Certificate Policy
and
Certification Practice Statement
of EuroCert's Qualified Trust Services

Version 4.1

Approved by:	
Position	CEO
Name and surname	Łukasz Konikiewicz
Date of approval	21.06.2023
Valid from	21.06.2023

EuroCert Sp. z o.o. „CENTRUM EUROCERT"
ul. Puławska 474
02-884 Warszawa
https://eurocert.pl

Table of contents

1 Introduction

1.1 Overview

This document, hereinafter referred to as the "Policy" is used by EuroCert Sp. z o.o. – "Centrum EuroCert" (hereinafter: the „EuroCert" or "Primary Registration Authority"), to provide qualified trust services, comprising issuing:

a) qualified certificates for electronic signature;
b) qualified certificates for electronic seal,
   hereinafter referred to as "certificates", including revoking, suspending and unsuspending certificates as well as publishing the CRLs;
c) qualified certificates for website authentication;
d) qualified electronic time stamps, hereinafter referred to as "time stamps".

EuroCert is a reliable service provider respecting:

a) The Act on Trust Services and Electronic Identification of 5 September 2016 (Journal of Laws of 2016, item 1579), hereinafter the "Trust Services Act";

b) 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, hereinafter the "eIDAS";

c) The Personal Data Protection Act of 10 May 2018 (Journal of Laws item 1000), hereinafter the "Personal Data Protection Act";

d) Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the "GDPR";

e) Appropriate Executive (implementing) provisions to these above regulations.

The structure of this document complies with the RFC 3647 Internet standard "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practice Framework".

This Policy also fulfils the role of the Certification Practice Statement.

1.2 Document name and identification

The Policy holds the following registered object identifier: 1.2.616.1.113791.1.2.
The valid Policy and its previous versions are available in an electronic form at: https://www.eurocert.pl/repozytorium.

1.3 PKI participants

The Policy applies to the following entities:

a) qualified CA: “Centrum Kwalifikowane EuroCert”,
b) qualified time-stamping authority: “EuroCert QTSA”,
c) Registration Authorities,
d) Primary Registration Authority,
e) subscribers,
f) relying parties.

Public keys to verify trust services:

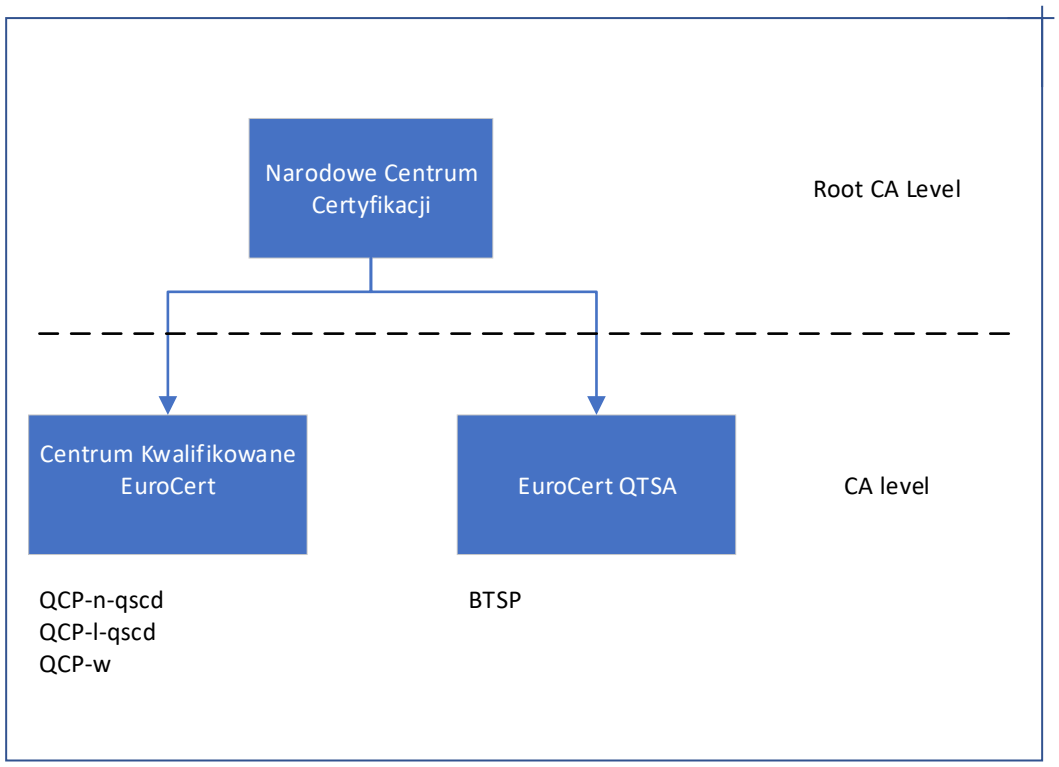
a) key for signing certificates and CRLs,
b) key for signing time stamps

are available as certificates of trust services provider issued by the Ministry of Digital Affairs or an entitled subject (National Certification Centre) acting by virtue of § 10.1 of the Trust Services Act.

EuroCert does not issue certificates for any subordinate trust services providers.

Figure 1 shows PKI set-ups for qualified trust services. It always consists of a chain which begins with a root CA (root authority or trust anchor) which is followed by further sub-CAs (intermediate CAs). The last sub-CA of this chain is the issuing CA which issues end entity certificates.

Fig. 1 PKI hierarchy for qualified trust services.



Depending on their features, the certificates can be assigned to the requirements of the different policies (certification level) within EN 319 411-2:
QCP-n-qscd – EU qualified certificates issued to a natural person with private key related to the certified public key in a QSCD,

QCP-l-qscd – EU Qualified certificates issued to legal person with private key related to the certified public key in a QSCD,
QCP-w – EU qualified website certificates issued to legal persons.

Depending on their features, the service certificates for time stamps can be assigned to the requirements of EN 319 421:
BTSP - Qualified time stamp service.

1.3.1 Certification authorities

CA – "Centrum Kwalifikowane EuroCert" issues certificates and publishes CRLs.

The CA is supervised by the Ministry of Digital Affairs who entrusted the role of the root CA to the National Certification Centre (NCCert). NCCert is a trust point for all subscribers and relying parties for qualified trust services of EuroCert. This means that each certification path developed by them should start with the certificate of NCCert to certificate for CA "Centrum Kwalifikowane EuroCert" issued by NCCert and end up with the end entity certificate.

Certificates are issued by CA according to the policy set forth in point 5.3 of the ETSI EN 319 411-2.

Tab. 1 The Certificate policy identifiers included in the certificates

Name of certificates	Policy type acc. To ETSI EN 319 411-2	Certificate policy identifiers
Certificate for electronic signature	QCP-n-qscd	1.2.616.1.113791.1.2.2
Certificate for electronic seal	QCP-l-qscd	1.2.616.1.113791.1.2.3
Certificate for website authentication	QCP-w	1.2.616.1.113791.1.2.1

1.3.2 Time-stamping authority

The time-stamping authority "EuroCert QTSA" issues time stamps in line with the recommendations of ETSI EN 319 422. Each time stamp contains a certificate policy identifier (tab. 2), according to which it was issued and it is certified exclusively with the use of a private key created especially for the time-stamping service.

Tab. 2 The identifier for the included in timestamp issued by EuroCert QTSA

Name of the token	Certificate policy identifiers
Timestamp from EuroCert QTSA	1.2.616.1.113791.1.4

While performing services of electronic time-stamping, the time-stamping authority "EuroCert QTSA" uses solutions which enable synchronization with the Coordinated Universal Time – UTC with 1-second accuracy.

The policy of EuroCert QTSA is in compliance with the norm ETSI EN 319 421 and indicates the qualified time stamp in the meaning of eIDAS. The key of this CA is available on the TSL list and is defined as a qualified trust service.

1.3.3 Registration Authorities

RAs operate on the basis of the authorization by the EuroCert. The authorization concerns the registration and identification of the identity of subscribers.

RAs may be natural and legal persons and organisational units having no legal personality, upon signing an agreement with EuroCert on cooperation in providing trust services.

RAs which are supervised by EuroCert cannot accredit other RAs.

RAs represent the EuroCert in contacts with subscribers and act within the scope of authorisation given by the EuroCert, including:

a) collecting and accepting certificate applications, terms of provision of trust services, accepted by Subscribers,
b) verification of subscribers' identity,
c) creating certification requests and submitting them to the CA,
d) delivering certificates along with an smart card to subscribers,
e) accepting and processing revocation, suspension or unsuspension requests,
f) registration of subscribers who use time-stamping service.

The Tasks e) and f) can be only performed by the Primary Registration Authority.

The tasks assigned to the RAs are executed only by persons authorised by EuroCert, hereinafter referred to as "Operators".

Detailed scope of duties of RAs is set out by the agreement between EuroCert and a certain RA.

Primary Registration Authority is prepared to handle notary's confirmation of the identity of a subscriber or confirmation issued by a qualified person, without the need for a subscriber to appear at the RA.

A list of current authorised RAs is available at http://eurocert.pl/PunktyPartnerskie.

Majority of RAs offers a service of certificate issuance on the subscriber's premises or in the workplace.

1.3.4 Subscribers

A subscriber of a certificate for electronic signature may solely be an individual person.

A subscriber of a certificate for electronic seal may solely be a legal person or organizational unit without legal personality.

A natural person, a legal person, or an organisational unit without corporate existence whose data has been entered or is to be entered into a certificate may be a subscriber in case of qualified certificates of websites.

A subscriber of a qualified timestamp may be each natural person, legal person in the meaning of the national law and other entity of a similar nature (organizational unit without legal personality, partnership etc.).

In case of qualified certificates for electronic seal and certificates for websites authentication issued to entities other than a natural person actions provided for in the Policy for a subscriber, shall be carried out by a person authorised by these entities. This person has also been charge with responsibilities relating to the protection of a private key.

1.3.5 Relying Parties

A relying party is an entity using the certificate in order to verify an electronic signature or seal.

The relying party is liable for verifying the current status of the certificate. This decision must be made by the relying party each time when the certificate is to be used for verifying an electronic signature (seal) or authentication of websites. Information included in a qualified certificate (for instance certificate type, object identifiers of the certificate policy, content of keyUsage field) should be used by the relying party for the assessment whether the certificate was used in line with its declared designation.

Obligations of relying parties are listed in chapter 4.5.2 of the Policy.

1.4 Certificate usage

The declared purpose might be specified on the basis of values set in PolicyInformation structure of the extension certificatePolicies (see chapter 7.1.2) of every certificate issued by EuroCert.

Subscribers private keys related to qualified certificates may be processed exclusively in the qualified electronic signature (seal) creation devices (QSCD) meeting the requirements set out in 6.2.1. The list of these devices used by EuroCert is published in the repository (see chapter 2).

EuroCert makes regular reviews of the validity of certificates for these devices.

1.4.1 Appropriate certificate uses

Qualified certificates for electronic signature may be used only to verify secure electronic signatures which are proofs of act of will and proof of connection with the data.

The qualified electronic signature created by a qualified certificate has equivalent legal effect of handwritten signatures.

Qualified certificates for electronic seal may be used only to verify qualified seals which guarantee origin authenticity and integrity of associated data. Qualified electronic seal is not used to express the will of subjects who create the seal.

Qualified certificates for websites authentication are used to confirm reliability of servers and to confirm their authenticity. They allow setting up a TSL encrypted connection among servers with such certificates, and also providing clients with safe logging in. Certificates of that type may be issued only for servers operating in public networks and that have a full, clear domain name defining location of a specific nod in DNS (FQDN - Fully Qualified Domain Name).

1.4.2 Prohibited certificate uses

The certificates cannot be used contrary to their designation and limitations in the usage of a certain certificate indicated in the certificate.

It is also prohibited for unauthorised individuals to use a certificate.

1.5 Policy administration

Each amendment to the Policy, except for those replacing obvious clerk or style errors, must be approved by the management board of EuroCert Sp. z o.o in the new version of the Policy. The version valid at a certain time has a current status. Each version is valid until a new version is approved and published.

A new version of the Policy is published in the repository. Subscribers, relying parties and RAs are obliged to use only the valid Policy.

1.5.1 Organization administering the document

EuroCert Sp. z o.o. is an entity in charge of managing the Policy (including the approval of amendments etc.).

1.5.2 Contact person

All correspondence regarding trust services must be addressed to:

EuroCert Sp. z o.o.
Centrum EuroCert
ul. Puławska 472
02-884 Warsaw
+48 22 490 36 45
biuro@eurocert.pl

1.5.3 Approval procedures

The management board of EuroCert Sp. z o.o approves the Policy. Upon an approval, the document receives the valid status indicating the date of entering into force. It is published in the repository no later than on the same date.

1.6 Definitions and acronyms

The terms used in the Policy and not defined below should be interpreted in line with definitions included in the Trust Services Act and in the eIDAS.

1) DN – Distinguished Name – an identifier of the PKI entity in line with the syntax defined for ITU X.500 series recommendations as well as ETSI TS 119 412-1 and ETSI EN 319 412 norms,
2) CA – Certification Authority,
3) QSCD – Qualified Signature/Seal Creation Device - a qualified electronic signature or seal creation device that meets the requirements laid down in Annex II of the eIDAS,
4) Applicant – the Subscriber in the period between submission of a request (application) to a certification authority and the completion of certificate issuance procedure,
5) Subscriber – the subject for which certificate was issued or is going to be issued,
6) CRL – Certificate Revocation List,
7) PKI – Public Key Infrastructure - a system covering Keys Certification Centres, Registration authorities and end users, controlled by trust service providers,
8) HSM - Hardware Security Module – a device with the functionality of generating cryptographic keys and using a private key for generating electronic signatures/seals (e.g. while issuing certificates, CRLs),

9) Private key - data used for creating an electronic signature (seal),
10) Public key - data used for verifying an electronic signature (seal), usually distributed in the form of a certificate,
11) Remote signature/seal – a service of creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory.
12) TSL EU Trust service Status List – lists issued by the European Commission (a list of lists) and the EU member states, containing information about entities providing trust services, their status (whether “qualified”) and data allowing for verifying tokens issued by trust services providing entities (namely the verification of qualified certificates, time stamps etc.),

2 Publication and repository responsibilities

2.1 Repositories

Repository is a public collection of documents concerning designed for external parties (subscribers, RAs, relying parties) which is available 24/7 and published at: https://eurocert.pl/repozytorium.

2.2 Publication of certification information

The following information is published in the repository:

a) certificate policy,
b) certification practice statement,
c) certificates of trust service providers (CA certificates),
d) terms and conditions of providing trust services by EuroCert,
e) CRLs,
f) a list of qualified signature (seal) creation devices,
g) contract templates, application forms, order forms, regulations, instructions, procedures.

Information concerning qualified trust services provided by EuroCert is published automatically in the repository (CRLs) or upon acceptance by authorized parties (e.g. certificate policy, certification practice statement, CA certificates and other documents).

2.3 Time or frequency of publication

CRLs are generated and published automatically, while other information each time upon their updating or amending.

2.4 Access control on repositories

The information published in the repository is secured against unauthorised amending, supplementing and removing and is stored with back-up copies.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The certificates generally contain information regarding the issuer and the subject. In line with the [X.509] standard, these names are given as distinguished name.

Alternative names can be registered and included in the subjectAltName extension of the certificates (see section 7.1.2).

3.1.2 Need for names to be meaningful

Mandatory data in the certificate enabling unambiguous identification of the subscriber has been pointed out in 3.1.4.

3.1.3 Anonymity or pseudonymity of subscribers

EuroCert does not issue anonymous certificates (in particular those containing only a pseudonym) i.e. the ones which contain insufficient data to identify the subscriber in an unambiguous way. Each subscriber's identifier contains at least the information marked as mandatory in 3.1.4.

3.1.4 Rules for interpreting various name forms

The interpretation of names of fields included in certificates complies with ETSI TS 119 412-1 and ETSI EN 319 412 (Part: 2,3,4,5).

The attributes of the *distinguished name* (DN components) of certificates are interpreted as follows:

Tab. 3. Subscriber's DN in the certificate for electronic signature

Fields	**Values**
C*	a two-letter international acronym for a country (PL for Poland)
G*	the subscriber's first name(s)
S*	the subscriber's surname plus possibly surname at birth
CN	(common name) contains the subscriber's first name(s) and surname or pseudonym.
SERIAL NUMBER*	passport number, identity card number, personal identification number (e.g. PESEL), the subscriber's tax identification number or local identifier of the subscriber, recognisable on the European Union's level according to point 5.1.3 of ETSI TS 119 412-1. When a subscriber is identified by PESEL number, serial number should be in the following format: „PNOPL-XXXXXXXXXXX" in accordance with the point 5.1.3 of ETSI TS 119 412-1
O	Organisation name where the subscriber is employed or which is represented by the subscriber
OU	Name of an organizational unit
T	The subscriber's position name in a certain organisation, professional position
Postal Address	Postal Address: city, street and number, zip code

*mandatory field

Tab. 4. Subscriber's DN in the certificate for electronic seal

Fields	Values
C*	a two-letter international acronym for a state (PL for Poland)
CN	common name. The common name shall contain the name most frequently used by an organisation. It does not have to be the official name, the same as in the register or the statute.
ORGANIZATION IDENTIFIER*	Organization identifier: tax identification number, register number in the national commercial register or local identifier, recognisable on the European Union's level according to point 5.1.4 ETSI TS 119 412-1
O*	Official name of the organisation
OU	Name of an organizational unit
Postal Address	Postal Address: city, street and number, zip code

*mandatory field

Tab. 5. Subscriber's DN in the certificate for website authentication

Fields	Values
C*	a two-letter international acronym for a state (PL for Poland)
L*	Locality (city/town)
CN	common name. The common name shall contain the name most frequently used by an organisation.
ORGANIZATION IDENTIFIER*	Organization identifier: tax identification number, register number in the national commercial register or local identifier, recognisable on the European Union's level according to point 5.1.4 ETSI TS 119 412-1
O*	Official name of the organisation
OU	Name of an organizational unit
Postal Address	Postal Address: city, street and number, zip code
subjectAltName	Name of the Internet domain registered in the DNS system for which a certificate is issued

*- mandatory field

3.1.5 Uniqueness of names

Each certificate has its own unique serial number (product key) given by the CA. In connection with the DN of a subscriber, it guarantees an explicit identification of the subscriber.

EuroCert ensures that the subscriber's name ("Subject" field) (DistinguishedName) used in certificates is always assigned within this PKI to the same subscriber, respectively.

The serial number ensures the unambiguity of the certificate.

The TSP ensures the unambiguity of distinguished names in CA certificates.

3.1.6 Recognition, authentication, and role of trademarks

The subscriber's DN should contain exclusively the names to which the subscriber is entitled. EuroCert does not verify the rights to use reserved trademarks, and it is not liable for unauthorised use of trademarks and it is not a party in the event of any dispute related to it. In the case of the subscriber

losing the right to use a certain name or other mark included in the certificate, it is obliged to notify about this fact in order to revoke the certificate due to the invalidity of data contained in the certificate.

3.2 Initial identity validation

EuroCert registers only this data which is needed to issue a certificate of a given type as well as detailed attributes of the subscriber, including the date and place of birth, the type, expiry date and the reference number of the identity document presented.

Subscribers are obliged to provide their contact address, in particular e-mail.

EuroCert gathers only this information which is necessary to issue a certificate for a specified purpose.

RAs verify the identity and if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued:

a) by the physical presence of the natural person or of an authorised representative of the legal person; or
b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 eIDAS with regard to the assurance levels 'substantial' or 'high'; or
c) remotely, by using a remote identification method; or
d) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b) above.

In case of the item (a), verification of identity requires physical presence in front of an authorised representative of EuroCert or Registration Authority, notary or any other person authorised by EuroCert.

Item (d) is described in point 3.3.1 and 4.7 of this Policy.

In case of the item (c), EuroCert uses a method which has been certified for conformity to the requirements of eIDAS Regulation by the authority for verifying conformity, giving the same degree of security as personal appearance, pursuant to Art. 24, par. 1 item d of the eIDAS Regulation.

3.2.1 Method to prove possession of private key

The certificate may be issued with a pair of keys generated by EuroCert or to a public key from a pair of keys generated by the subscriber.

If a pair of keys is generated by the subscriber it shall be done under supervision of EuroCert, except for the certificates for website authentication.

If the subscriber generates a pair of keys it should meet the requirements specified in sections 6.1.5 and 6.2.1. Then it is required to present the file with request for certificate issuance in order to issue the certificate. Such file contains a public key for which the certificate is to be generated, the subscriber's data, and electronic signature or electronic seal generated with the use of a private key which constitute one pair with the public key. Provision of a request containing a public key and signed with a private key is to establish whether a private key making a single pair with a public key is under control of the subscriber. The file with the request shall be delivered personally to EuroCert by the

subscriber or shall be send by email in the form of an electronic file with the request signed with qualified electronic signature of the subscriber.

3.2.2 Authentication of organization identity

The identification of a legal person or an organisational unit not having legal personality as well as an authorised representative of this entity is established by verification of:

- The entries in The National Court Register or Central Register and Business Activity Register; and
- Power of attorney or other authorisation issued by a legally authorised representative of a given entity (in the case when the person is not mentioned in the public register).

An authorised representative of an organisation applying for a certificate is subject to verification according to point 3.2.3. The issued certificate is in such a case a proof that a natural person can use a private key acting on behalf of the entity.

In case of the qualified certificate for websites authentication verification checks if the ordering party has the right to use the domain name and if the domain remains under its control. Verification carried out by EuroCert covers:

1) checking in the publicly available WHOIS services or directly with entities registering domains, if the ordering party is registered as a domain owner or has the right to use the domain name during a period of submission of an order for the certificate;
2) confirming control over the requested Domain Name by placing indicated by EuroCert random data in file ecdv.txt under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation. The file with random data has to be accessible by EuroCert via HTTP or HTTPS. Random data in file is unique for every certificate request, does not appear in the request HTTP nor HHTPS and data is not older than 30 days;
3) checking, if verification data indicated by EuroCert has been put on a server or a TXT type record in DNS for the domain;
4) the alternative way of checking the control over the requested Domain Name is placing the random data given by EuroCert in DNS record TXT, CAA or CNAME type. Random data sent by EuroCert is unique for each validation and is not older than 30 days;
5) in case of Wildcard Certificates checking if in the “public suffix list” (PSL) register http://publicsuffix.org/ (PSL), the sign “*” is not put in the first place on the left-hand side of the suffix of gTLD domains delegated by ICANN. EuroCert may issue a Wildcard Certificate for gTLD domains, if the subscriber properly proves its right to manage the entire space of names under the gTLD domain;
6) checking if the DNS of the domain does not contain restriction as a CAA (Certification Authority - Authorization) record describing which entities can issue certificates for a given domain. This check is performed by the dedicated tool by querying a CAA record. To minimise the risk of using wrong data, EuroCert shall use data presented in the WHOIS service in combination with the IANA data and the WHOIS data provided by entities approved by ICANN that register domains.

If the Subscriber Identifier of the qualified certificate for websites authentication containing the domain name is also to contain a name of the country, then prior to issuance of the certificate EuroCert shall verify if the indicated name of the country is linked with the subscriber. Verification is carried out according to one of the methods described below and it consists in checking:

1) if an IP address of the domain indicated in DNS is within a range of IP addresses assigned for a country for entering of which into the Subscriber Identifier the applicant applies;
2) if the name of the country included in information provided by an authority registering the domain the name of which is to be placed in the certificate is compliant with the name of a country for entering of which into the Subscriber Identifier the applicant applies;
3) By verifying the name of the country EuroCert shall examine if the ordering party does not use a proxy server to substitute an IP address from another country than in which it is actually located.

3.2.3 Authentication of individual identity

The identity of the applicant is checked against an official identity document. Either valid ID card, passport or permanent residence card can be used.

If a certificate is to contain additional data, e.g. detail of an organization, profession, job position, professional qualifications, a document is required to confirm these.

In the event of verifying the identity through a notary, the applicant accepts the terms of provision of trust services in the presence of a notary and provide the original copy to EuroCert. Then this document is accepted by the registration officer and sent back to the address indicated by the applicant.

Before certificate issuance Subscriber is obligated to familiarize themself with "Terms & conditions of EuroCert Qualified Trust Services" and the terms of provision of trust services set out in this document available at https://eurocert.pl/repozytorium/.
The subscriber is obliged to confirm themself familiarization with the rules described above by accepting the terms of provision of trust services.

EuroCert guarantees documents in Polish and English language of information listed above which cover an area of interest in the language of our customers. The documents are downloadable in PDF format through the repository of EuroCert https://eurocert.pl/repozytorium/.

Acceptance of the terms of provision of trust services (consisting of the terms and conditions for the use, scope and limits for the use of the certificate, legal consequences of creating a qualified electronic signature/seal) also means that:

a) the subscriber agrees for the processing of his/her personal data by EuroCert Sp. z o.o for the purposes necessary for the certification procedure,
b) the subscriber declares that information given by it is true and was given voluntarily,
c) the subscriber confirms collecting in person the certificate and private key on cryptographic card (QSCD) and, if applicable, a safe envelope containing PIN and PUK codes,
d) the subscriber agrees to make their certificate public in the repository of certificates run by EuroCert.

The applicant declares the contract conclusion of and the issuance of a qualified certificate by accepting the terms of provision of trust services set out in the "Terms & conditions of EuroCert Qualified Trust Services" and the „Certificate policy and certification practice statement of EuroCert's qualified trust services" available at https://eurocert.pl/repozytorium/.

3.2.4 Non-verified subscriber information

EuroCert verifies all the data which shall be placed in the certificate (see 3.1.4).

3.2.5 Validation of authority

In the case of natural persons, the identity and, if necessary or applicable, the affiliation with the organization concerned is determined and verified and/or confirmed using procedures according to section 3.2.3. In the case of organizations, proof of their existence and the applicant's right to represent the organization in question is verified and/or confirmed according to section 3.2.2. Furthermore, at least one representative is identified in person or using a remote identification procedure.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Re-key requires reverification of the subscriber's identity in line with the description in 3.2 or using the simplified method presented in 3.3.1 compliant with the Article 24 Paragraph 1 item c of the eIDAS.

3.3.1 Identification and authentication for routine re-key

The confirmation of the identity of a subscriber holding a valid qualified certificate does not require presenting a valid identity card or passport (and other identity documents) and information necessary for certification request may contain a qualified electronic signature/seal of this person if information is the same as data included in the certificate related to the qualified electronic signature/seal used for signing the data. Then, the subscriber's authentication is performed by verifying an electronic signature/seal created under the certificate request and confirming the authenticity of the certificate bound to the signature/seal (based on the certification path). However, this does not mean that it is impossible to apply the procedure described in 3.2.2.

Re-keying is not offered for certificates for website authentication (according to QCP-w). In the case of these certificates, the complete identification and registration process which also applies to first-time applications must be carried out (as shown in point 3.2.2).

3.3.2 Identification and authentication for re-key after revocation

In the case of expiration or revocation and in the event of changing any identification data contained in the certificate should be followed procedure applicable for issuing the first certificate (see 3.2).

3.4 Identification and authentication for certificate's change of status

The certificate may be revoked or suspended:

a) in person at EuroCert, with its address given in 1.5.2, during working hours, namely from 8.00 to 16.00,
b) by phone under hotline number 22 490 49 86, during the whole day, based on the revocation password for the certificate,
c) by sending a completed and electronically signed revocation/suspension request to uniewaznienia@eurocert.pl. The form can be downloaded at: https://eurocert.pl/index.php/en-us/documents/suspend-or-revoke-of-the-certificate,
d) by e-mail filling an on-line form available at https://eurocert.pl/uniewaznienia/.

The basis for acceptance of the revocation/suspension request is a positive verification by the EuroCert registration officer:

a) the applicant's identity and their rights to apply for revocation/suspension of the certificate,

b) the data contained in the revocation/suspension application.

In case when it is impossible to completely verify the revocation request by the registration officer the certificate is suspended until the irregularities are explained or the request is rejected.

Verification of requests for cancellation of suspension proceeds in accordance with subchapter 3.2.

Revocation, suspension and cancellation of suspension is performed by the Primary Registration Authority.

In the case of submission of revocation request (personally by the subscriber) in RA, the operator of RA carries out identification and authentication of the subscriber in accordance with section 3.2 and request for revocation on behalf of subscriber by one of the methods from a to d above. The revocation request and confirmation of identity is transferred to Primary Registration Authority.

EuroCert confirms the revocation or the refusal thereof along with the justification to the subscriber and the party applying for revocation/suspension via an e-mail.

4 Certificate life-cycle operational requirements

The procedure of obtaining a certificate is initiated with submission of an application at a RA, which is addressed to certification authority or time-stamping authority. Applications shall contain information which is necessary to accurately identify the subscriber.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Legal persons and organisational units without legal personality apply for issuing the certificate only via authorized representatives, whereas individual subscribers (natural persons) always request a certificate by themselves (on their own behalf).

The detailed scope of the powers to act on behalf of someone else should define the power of attorney or other document authorizing to act on someone else's behalf.

4.1.2 Enrolment process and responsibilities

Certificate application shall be submitted in the RA in person or (in the case of a renewal, when a certificate has not expired) via an electronic form.

4.2 Certificate application processing

A certificate application and certification request file (pkcs#10) is subject to mandatory authentication by the RA operator in line with 3.2 or 3.3.

4.2.1 Performing identification and authentication functions

Identification and authentication functions of all required subscriber’s data are performed as set out in chapter 3.

The registration process can be carried out by partners or external providers (RAs) under a corresponding agreement if such partners or external providers fulfil the requirements of the Policy.

4.2.2 Approval or rejection of certificate applications

EuroCert may reject the certificate application if:

1) the DN name of the subscriber applying for the certificate is identical as the name of another subscriber,
2) there is a justified suspicion that the subscriber forged the application or provided false information in the application,
3) the subscriber failed to submit a complete set of required documents,
4) it has been signed by a person who is unauthorised to represent the subscriber,
5) A public key included in the certification request file does not meet requirements specified in section 6.1.5,
6) A Qualified certificate used for identification of the subscriber does not contain data unambiguously identifying the subscriber,
7) PESEL number is incorrect, the identity document is not valid (is registered in Restricted Document Database as restricted, in case of certificates for website validation the domain is not under control of the principal or subscriber),

8) data released as part of the electronic identification means has not been confirmed by the subscriber or the order does not contain the required data.
9) due to other important reasons not listed above, upon consulting the security officer in order to agree on the rejection.

EuroCert may refuse to grant the certificate to any applicant without contracting any obligations or without exposing itself to any liability that may arise from the loses or costs incurred by the applicant (as a result of the refusal). In this case, EuroCert returns to the applicant the fee for issuing the certificate (if the fee was prepaid), unless the applicant included forged or false data in the certificate application.

The notice about the refusal to issue the certificate is sent to the applicant in the form of a relevant decision with the statement of grounds for the refusal. The applicant may appeal against the decision of EuroCert within 14 days from the date of its receipt.

4.2.3 Time to process certificate applications

If there are no reasons beyond EuroCert's control, the certificate application processing time should not exceed 7 days from the moment of submitting an order to the RA, unless the agreement entered into between EuroCert and the subscriber provides for a longer time limit.

4.3 Certificate issuance

The certificate may be issued for a pair of keys generated by EuroCert on QSCD or on the basis of a certification request presented by the subscriber for key pair generated by themself (see 3.2.1).

EuroCert shall place, in a relevant certificate extension **esi4-qcStatement-4 (0.4.0.1862.1.4** QcSSCD), referred to in point 7.2, information about storage of a private key in the QSCD, if the certificate is issued:

1) for a pair of keys generated by EuroCert on QSCD, or
2) when a pair of keys, which meets the requirements specified in section 6.1.5, is generated by Subscriber in the presence of Operator in QSCD controlled by the subscriber.

If the above requirements (including lack of QSCD certification) are not fulfilled, EuroCert will not issue the certificate.

If a pair of keys is generates by a subscriber on their own (without supervision of EuroCert), EuroCert does not check if the keys are stored in a QSCD, and do not place qcStatement extension – qcSSCD in the certificate. Operator of RA after checking certification request in accordance with paragraph. 3.2.1 generates a certificate.

If pair of keys was generated by EuroCert on cryptographic card, Operator issues also secure envelop with PIN and PUK codes.

4.3.1 CA actions during certificate issuance

If the certificate application together with the data contained therein was verified correctly then RA Operator proceeds to generate the certificate.

RA operator prepares a certification request token and submits to the certification authority in order to generate a certificate by the registration officer.

The registration officer signs electronically a certification request token followed by sending the signed certification request to the system generating certificates, launching the certificate generating procedure.

When a key pair is generated by EuroCert on a cryptographic card the RA operator personifies the card by securing it with generating PIN and PUK codes to the card in a sealed envelope. Certificates are given directly to a subscriber.

If the subscriber generates a pair of keys himself, Registration officer after checking in accordance with paragraph. 3.2.1 certification request generates a certificate.

If a pair of keys is generated by EuroCert, the transfer of private key to the subscriber is confirmed with a document confirming the issuance of the certificate and signed by the subscriber.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The subscriber is notified in person about issuing the certificate by the person who verifies their personal data, as the key pair and certificate are generated in the subscriber's presence immediately after a successful completion of identity verification. If in the certificate the data of the third party are contained (e.g. data of a subject represented by the subscriber) this person is also notified about the certificate issuance.

If the request file was delivered to EuroCert in the form described in section 3.2.1, the certificate generated by EuroCert can be send back to the subscriber on the email address indicated in the order.

4.4 Certificate acceptance

Upon collecting the certificate, the subscriber is obliged to immediately check its content, no later than before the first use of the private key connected with the certificate. If data included in the certificate is incorrect, it is obliged to notify EuroCert about this fact immediately, in order to revoke the certificate in line with applicable procedures (see 3.4 and 4.9) and to receive a new certificate containing correct data. Using a certificate containing false data poses a risk of criminal liability to the subscriber, as set out in Article 42 Paragraph 2 of the Trust Services Act.

An initial acceptance of the certificate is performed by the RA immediately upon issuing the certificate by the certification authority, and before saving it on any carrier. The RA checks whether data included in the certificate is correct. If the certificate contains any defects it should be immediately revoked and a new certificate, free of any defects, should be issued instead without charging the subscriber with any costs for this operation. In this case, it is not required to sign an agreement and/or deliver additional documents.

4.4.1 Conduct constituting certificate acceptance

Certificate acceptance means occurrence of one of the following things within 7 days of the reception of a certificate:

1) subscriber's submission of certificate acceptance, or
2) lack of certificate revocation in above mentioned period.

4.4.2 Publication of the certificate by the CA

Certificates are not published outside EuroCert's internal network.

4.4.3 Notification of certificate issuance by the CA to other entities

EuroCert may notify other entities about issuing the certificate, if the certificate referred to them or contained their data (e.g. an entity represented by the subscriber).

4.5 Key pair and certificate usage

Certificates may be used exclusively for verification of electronic signatures or electronic seals, in line with this Policy and taking into account possible limitations stated in the certificate.

Private key linked to the certificate may be exclusively used for purposes related to uses stated in the certificate.

Private key for electronic signature shall remain at the sole disposal of the subscriber – a natural person whose data have been placed in the certificate. The use of the key is not allowed by any other person.

Private key for electronic seal shall remain at the sole disposal of the authorised person (s).

In the case of remote signature/seal – the private key used to create the signature/seal is stored on an HSM at EuroCert's premises and is used by EuroCert exclusively for the purpose of electronic signature/seal on behalf of the subscriber.

4.5.1 Subscriber private key and certificate usage

The subscriber undertakes to:

a) notify EuroCert about any changes in information contained in its certificate in order to revoke the certificate and possibly to issue a new one, containing correct information,
b) testing the correctness of information included in the certificate, immediately upon its receipt; in the event of the occurrence of any irregularities, in particular irregular data specifying the subscriber's identity, the subscriber is obliged to immediately notify EuroCert about this fact in order to revoke the certificate and to generate a new certificate with correct data,
c) immediately submit a revocation request in the event of a reasonable suspicion that an unauthorised person has access to the private key (e.g. loss of the private key, disclosing access passwords) and when circumstances have invoked as set out in 4.9.1,
d) undertake all possible security measures in order to store the private key safely, including
    - the control and protection of access to devices containing their private keys;
    - refraining from storing the cryptographic card containing a private key together with their personal identification number (PIN);
    - refraining from disclosing and sharing their private keys and used passwords to and with any third parties,
e) use private keys and certificates only within their validity period and in line with their purpose set out in this Policy and indicated in the certificate (in the "keyUsage" or "extendedKeyUsage" field, see section 7.1.2),
f) refrain from using the private key in the period of certificate suspension.

4.5.2 Relying party public key and certificate usage

Relying parties are obliged to:

a) use private keys and certificates only within their validity date and in line with their intended purpose set out in this Policy and indicated in the certificate (in the "keyUsage" or "extendedKeyUsage" field, see section 7.1.2),
b) rely only on the certificates that are used in line with the declared purpose and can be used in the areas specified earlier by the relying party,
c) use public keys and certificates only upon verifying their status and validity of the trust service provider certificates,
d) notify EuroCert about all cases of the certificate's use by unauthorised persons and about suspicions that the certificate was issued to an improper entity,
e) check whether certificate policy identifiers contained in certificates located on the certification path are present in the set of acceptable identifiers specified by the relying party,
f) consider a signature invalid if it is impossible to verify using the available software and equipment, whether the signature is valid or the obtained verification result is negative.

4.6 Certificate renewal

It is not possible to substitute a certificate with a new certificate without changing the public key or any other information (except for a new validity date, serial number and a signature of the certificate issuer) contained in the certificate (see 4.7).

4.7 Certificate re-key

When certificate is renewed as specified in 3.3, a new key pair is generated.

Subscribers who hold the certificate on their cryptographic cards and want to renew it, may generate another key pair remotely. Then EuroCert provides to them a dedicated application that generates the keys directly on the subscriber's cryptographic card.

Renewal of the certificate may be performed by the subscriber from time to time, based on parameters of an indicated certificate already held by the subscriber. As a result, a new certificate is created with its parameters being the same as the parameters of the certificate indicated in the application, except for the new public key contained therein, the certificate serial number (product key) and different expiry date.

The new certificate will contain the same DN of the user contained in the subscriber's certificate which is used for verifying the electronic signature/seal of the subscriber created in the certificate application.

In the case of certificates for website authentication the same requirements as those in the initial identity validation apply.

4.7.1 Circumstance for certificate re-key

The subscriber may at any time apply for a certificate's renewal before the certificate validity date has expired.

Prior to issuing a certificate's renewal, necessary formal documents must be submitted in electronic form, signed (certified) using a valid private key connected with a certificate which has not expired. There is no need to revoke current certificate.

The subscriber's identity verification in this case takes place based on an electronic signature/seal, created under the certificate application.

4.7.2 Who may request certification of a new public key

Renewal of a certificate takes place at the initiative of the subscriber holding a certificate issued by the EuroCert.

4.7.3 Processing certificate re-keying requests

The procedure for processing re-keying requests is the same as the one specified in 3.3.1.

4.7.4 Notification of new certificate issuance to subscriber

Information about generating the certificate is submitted to the subscriber electronically.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.8 Certificate modification

Modifying the certificate's content requires issuing a new certificate. Issuing a certificate for modified data takes place in the same manner as in the event of issuing the certificate for the first time. The current certificate – if data contained therein became invalid and contain false information about the subscriber – is revoked.

4.8.1 Circumstance for certificate modification

When it is necessary to change the data in the certificate a new certificate shall be issued.
The new certificate contains a new public key, new serial number (product key) and it differs with at least one other certificate field.

4.8.2 Who may request certificate modification

The subscriber is responsible for notifying about the necessity of updating data contained in the certificate and for specifying whether the change of data requires revoking the existing certificate (see 4.5.1).

4.8.3 Processing certificate modification requests

The procedure for processing certificate modification requests is the same as the procedure for issuing a new certificate and it requires that all data shall be verified in line with 3.2.

4.8.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.9 Certificate revocation and suspension

According to Article 16 Paragraph 4 of the Trust Services Act EuroCert ensures the possibility of submitting demands to revoke/suspend certificates for 24 hours each day.

4.9.1 Circumstances for revocation

A certificate can be revoked in the following circumstances:

a) information contained in the certificate is not valid or is false,
b) loss (or there is a justified suspicion that this loss could take place) of control of a private key(e.g. the loss of a private key, an unauthorised access to a private key, a theft of a private key, an accidental damage of a private key),
c) subscriber resigns from services,
d) circumstances justifying publishing the organisation's data in the certificate have expired (e.g. terminating contract with an employee, change in the scope of duties etc.),
e) EuroCert ceases to perform trust services,
f) a proof exists that the certificate was used contrary to its purpose,
g) the certificate was issued in conflict with this Policy,
h) a private key of the certification authority was compromised or there is a justified suspicion that it could have been compromised.

4.9.2 Who can request revocation

The certificate can be revoked upon the request of:

a) the subscriber, for any reason,
b) an authorised representative of an organisation, whose data has been contained in the certificate (in the event of a certificate for an electronic signature containing organisation details), in the case of a terminating contract with an employee, change in the scope of duties etc.,

c) other person if so stipulated in the contract of providing of trust services or other documents, for specific reason (e.g. those in point 4.9.1).

In special cases certificate revocation/suspension may be requested by:

a) a supervisory body (ministry of digital affairs) or an entity authorised by it,
b) Registration officer of EuroCert, who can act on behalf of a subscriber or on their own, if they hold any information justifying the revocation (e.g. an infringement by the subscriber of the obligations set out in point 4.5.1., indicators from point 4.9.1 has occured).

4.9.3 Procedure for revocation request

The certificate is revoked upon successful verification of the revocation request by the registration officer, in line with the provisions of 3.4.

The information about certificate revocation is published on the CRL within 24 hours after the receipt of the request (see 4.9.7 and 7.2).

EuroCert submits the confirmation of the certificate revoking or the refusal decision indicating the reasons of the refusal, to the certificate subscriber and to the party applying for revoking the certificate by e-mail.

4.9.4 Revocation request grace period

The information about certificate revocation is published on the CRL within 24 hours after the receipt of the correct revocation request.

4.9.5 Time within which CA must process the revocation request

The maximum admissible time limit for processing a revocation request amounts to 24 hours.

4.9.6 Revocation checking requirement for relying parties

The party relying on data contained in the certificate is obliged to each time check whether the certificate is not listed on the CRL before its use to verify an electronic signature/seal or website.

4.9.7 CRL issuance frequency

CRLs are published automatically at least every 24 hours or after each revocation and published in the repository.

4.9.8 Maximum latency for CRLs

Current CRLs are published without undue delay, immediately after they have been created. EuroCert stipulates that any delay in publishing CRLs may not be longer than 60 minutes.

4.9.9 On-line revocation/status checking availability

Does not apply.

4.9.10 On-line revocation checking requirements

Does not apply.

4.9.11 Other forms of revocation advertisements available

In the case of security breach (disclosure) of the CA private key, the information about this fact is published immediately on CRLs and it is obligatory to send it by e-mail to all subscribers of that given CA. All subscribers whose interests may be in any manner (directly or indirectly) at risk are notified.

4.9.12 Special requirements re key compromise

If the CA's key is compromised, EuroCert is obliged to notify ASAP the supervisory body, subscribers and relying parties about this fact by way of publishing the notice on the EuroCert website and, if possible, in the mass media.

4.9.13 Requirements for suspension

A certificate can be suspended in the following circumstances:

a) information contained in the revocation request cause justified suspicions,
b) in the event of justified suspicion that there are premises for revoking the certificate indicated in 4.9.1 but the registration officer is unable to explain all doubts regarding the revoking of the certificate within 24 hours from receiving a complete request,
c) the revocation request was submitted by phone or electronically and the identity of the applicant cannot be confirmed within 24 hours from the moment of the request receipt as well as request can't be rejected,
d) the certification authority may immediately suspend a certificate in the case of a justified suspicion that the certificate was issued while failing to observe the provisions of this Policy,
e) other circumstances that require an explanation by the subscriber or by the applicant.

4.9.14 Who can request suspension

See section 4.9.2.

4.9.15 Procedure for suspension request

The suspension procedure takes place similarly as in the case of revoking a certificate. Upon successful verification of an application for the suspension by the registration officer which takes place in line with 3.4, the status of the certificate on CRL is changed into suspended (together with the suspending reason "certificateHold").

In the event of failing to confirm the premises justifying suspending a certificate, described in 4.9.13, EuroCert cancels the certificate's suspension. In the case of confirming the suspicion and in the event when EuroCert is not in the position to explain the doubts regarding the suspension of a certificate within 7 days from suspending the certificate, the certificate is revoked.

Upon reinstating the certificate, information about the certificate is removed from the CRL.

If a certificate is revoked after its prior suspending, the date of revoking the certificate is the same as the date of suspending the certificate.

4.9.16 Limits on suspension period

A certificate's suspension is temporary (usually until the moment of explaining all doubts causing the suspension). Possible reinstating the certificate, however, must take place no later than 7 days from the date of suspension (otherwise the certificate is revoked).

EuroCert guarantees the grace period in suspension request processing, as well as availability of certificate status verification to be the same as the in case of certificate revocation (see chapter 4.9.4).

4.10 The status of certificate

The status of certificates issued by EuroCert is verified on the basis of published CRLs.

4.11 End of subscription

The agreement for providing trust services between EuroCert and the subscriber expires at the moment of the expiry of the certificate or its revocation which has been issued on the basis of this agreement.

4.12 Key escrow and recovery

EuroCert does not entrust its private key to other entities.

In the case of a service of remote signature/seal the Subscriber provides EuroCert with their private key. EuroCert does not hand this key over to anyone, including the subscriber.

5 Facility, management, and operational controls

This chapter describes the requirements of supervision over physical, organisational protection and personnel activities applied in EuroCert, including but not limited to during generating keys and certificates, authorising entities, revoking certificates, audit and making backup copies.

5.1 Physical controls

5.1.1 Site location and construction

Information systems used for providing trust services are located in two independent places (the primary centre and the backup centre) distanced from each other.

5.1.2 Physical access

Physical access to the building is monitored 24 hours a day. Access to EuroCert premises is controlled and supervised by Access Control System and alarm system.

The computer system premises, in which the cryptographic module HSM is kept with the certification authority's keys are stored in the Zone of Limited Access. Access to these premises is subject to constrains, it is monitored by the access control system and the system signalling robbery and burglary. Access to the premises is limited to a narrow group of authorized individuals of the trusted EuroCert personnel. Execution of access rights is performed on the basis of access cards held by the personnel.

5.1.3 Power and air conditioning

In the event of a power cut the computer systems switches to the emergency power supply provided through UPS.

The environment in the computer systems premises is controlled permanently. All premises are air-conditioned.

5.1.4 Water exposures

Flood sensors are installed in the server room. Flooding alarms are automatically transferred to the security and building's administrator and they undertake suitable actions, notify relevant city services, the security officer and the system administrator.

5.1.5 Fire prevention and protection

Fire protection system is installed in the computer systems premises, meets the requirements of applicable provisions and fire protection norms. Fire extinguishing (gas) devices were installed in the server room, and they switch on automatically in the event of sensors discovering fire in the protected area.

5.1.6 Media storage

Carries on which archaic data are stored and back-up of data are stored in fireproof safes located in the primary centre. Access to the safes is granted to employees authorized in the procedure set out internally.

5.1.7 Waste disposal

EuroCert executes the security policy aimed at protection of data confidentiality. Internal regulations introduce data classification with respect to their confidentiality and set forth security requirements as well as methods of data handling in order to prevent data security infringements. Obsolete carriers containing data which may affect the security of EuroCert are destroyed to prevent data recovery or to make the data recovery economically unfeasible. For example with regard to carriers where cryptographic keys or PIN numbers were stored, they are destroyed only in devices which ensure at least DIN-3 class security or in other manner which ensures at least the same security level.

5.1.8 Back-up copies

All data significant for the safety of EuroCert and of services performed by it (in particular copies of passwords, PIN numbers and cryptographic keys applied in EuroCert system, archives, copies of current information, full installation software version) are stored in the primary centre in safes or in security containers depending on the security class of the data.

5.1.9 Off-site backup

In the event of a failure of the primary centre disabling the performance of trust services, the system's operation is taken over by the backup system located in the backup server room. In the case of a failure, the backup system takes over the operations related to revoking, suspending certificates and CRLs publication, on an ongoing basis.

5.2 Procedural controls

EuroCert ensures the performance of organisational securities by specifying the following:

a) entrusted roles that may be performed by one or more individuals in the certification authority,
b) ban of cumulation of specified roles,
c) the scope of obligations and responsibilities of individuals performing specific roles,
d) number of individuals necessary for the performance of specific tasks,
e) identification and verification of personnel.

5.2.1 Trusted roles

Individuals supervising the system used for performing trust services at EuroCert perform certain roles, listed in Table 6. The presented division of roles complies with the requirements of ETSI EN 319 401

Tab. 6. Trusted roles

Role	Scope of duties
Security officer	preparation and participation in the preparation, implementation and application of security regulation for information systems exploitation, used while providing trust services. Implementation of this Policy provisions. Supervision over the actions of system administrators according to existing regulations. Initiating and supervision over the process of generating keys and shared secrets. Participation in the process of internal control. Controlling the execution of security processes.

System administrator	the installation, configuration and management of systems and ICT networks used for the purposes of provision of trust services; managing the authorisations for system operators
System operator	operating information system, including making backup copies, managing the authorisations of registration officers
Registration officer	signing certification requests and accepting applications for revocation, suspension, or reinstating certificates and generating and publishing new CRLs.
System auditor	conducting planned and ad hoc audits in line with existing regulations. Analysing the event log; analysis the records in the registers of events that happen in the IT systems used while providing trust services
Data protection officer	supervision over the compliance with requirements set forth in the GDPR.

5.2.2 Number of persons required per task

EuroCert observes the rules set out in the internal regulations with respect to minimal staffing. Compliance with these rules ensures business continuity in critical situations even in the event of availability of 50% of the staff.

5.2.3 Identification and authentication for each role

EuroCert's personnel is subject to the procedures of:

- placing on the list of individuals with access to EuroCert's premises,
- placing on the list of individuals with logical access to EuroCert's system or network,
- assigning access and password in the EuroCert's computer systems.

Execution of the above procedures results in assigning individual identifiers to subjects who become the system users. These identifiers allow for unambiguous identification of users. Each of these identifiers :

- must be unique within the system and assigned directly to a consecutive person,
- cannot be shared with other persons,
- must be linked to the eligibility (resulting from the role performed by a certain individual) and alternatively with a user.

While managing the users eligibilities the rule must be observed of assigning minimal eligibilities necessary for employees to execute their roles and duties. Operations performed by EuroCert which do not require access through the co-shared network, are secured thanks to implemented mechanisms of verification (certification) and cyphering sent information.

Eligibilities of individuals who have already left the work at EuroCert or lost the right to represent EuroCert are blocked immediately. Accounts of a blocked user may be deleted only after the statutory time prescribed for data archiving has elapsed.

EuroCert's Security officer execute regular, planned once every quarter internal controls of access and accounts of system users The security officer is eligible to run ad hoc controls within existing internal regulations.

5.2.4 Roles requiring separation of duties

The roles of:

- the chairman of the board,
- security officer,
- audit officer

cannot be cumulated with any other functions in EuroCert.

The positions, roles and rules for position separation at EuroCert prevent the abuse while using EuroCert systems. Everybody who is responsible for the exploitation of EuroCert systems, used for providing certification services is granted the rights limited to the position held by them and to the liability related to the held position.

5.3 Personnel controls

EuroCert personnel, particularly persons holding trusted roles, are obliged to act in line with the provisions of the eIDAS, the Trust Services Act, the Data Protection Act and in line with provisions of existing internal regulations.

5.3.1 Qualifications, experience, and clearance requirements

Parties dealing with providing trust services have relevant qualifications provided for qualified trust service providers, in particular the knowledge and skills regarding the public key infrastructure and personal data processing as well as:

a) they have the full capacity for executing legal transactions,
b) they were not convicted with a valid judgement for a crime against documents' credibility, economic turnover, money and securities turnover, a treasury crime, a crime described in chapter VI of the Trust Services Act,
c) they have at least secondary school education,
d) they signed a confidentiality clause with regard to sensitive information for the Certification authority's safety or confidentiality of the subscriber's data,
e) they do not perform obligations that may cause conflict of interests between the Certification authority and RAs acting on its behalf,
f) have undergone on-the-job training including the content of EuroCert procedures and regulations.

5.3.2 Background check procedures

Before entrusting any role described in 5.2.1 to an employee the following documents are verified:

a) employment certificates from previous places of employment (applies to a new employee),
b) the diploma and certificates confirming the employee's education,
c) qualifications and professional experience,
d) employee's declarations on clear criminal record.

5.3.3 Training requirements

The personnel of EuroCert and RAs operators must participate in on-the-job training before receiving the authorisation to perform their positions. The training concerns:

- "Certificate policy and certification practice statement of EuroCert's qualified trust services",
- Internal regulations, procedures, statutes applied at EuroCert

- personal data protection and information protection,
- the public key infrastructure,
- verification of identity based on documents confirming identity,
- criminal liability pertaining to trust services and the function performed therein,
- the certification authority's computer system software,
- the scope of obligations and access rights resulting from the preformed function.

After completing the training its participants sign a document confirming that they became familiar with presented documentation and that they accept limitations resulting from it.

5.3.4 Retraining frequency and requirements

Trainings described in 5.3.3 are repeated or supplemented if needed and always when significant changes of rules in providing trust services by EuroCert were implemented, as well as in the functioning of EuroCert, organization of the system and essential internal and external regulations.

5.3.5 Job rotation frequency and sequence

This Policy does not set out any requirements in this regard.

5.3.6 Sanctions for unauthorized actions

In the case of discovering an unauthorised action or a suspicion of such action, the System Administrator in agreement with the Security officer may block the perpetrator's access to EuroCert systems. Further proceedings are performed in agreement with the management of EuroCert Sp. z o.o.

5.3.7 Independent contractor requirements

EuroCert allows for performing activities related to the performance of the role among those listed in 5.2.1 by individuals who are not employed under an employment contract (contract employees).

In this event, EuroCert includes in an agreement with the individual or with the company employing them the possibility of EuroCert pursuing all damages that may be incurred by them in the event of an undue performance of obligations under the performed role or as a result of failing to observe applicable provisions of the law, as well as the rules and regulations applicable at EuroCert.

Notwithstanding possible financial liability, individuals who perform their obligations related to providing certification services without due care or fail to observe the requirements imposed by the regulations regarding trust services (in particular the confidentiality requirements, certificates issuing and revoking requirements) are subject to penalties set out in the Trust Services Act.

5.3.8 Documentation supplied to personnel

EuroCert gives its personnel and operators of RAs access to the following documents:

- the Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services, Terms and conditions of rendering trust services by EuroCert,
- template contracts and application and order forms,
- External and internal regulations, norms, standards, procedures, statutes applied at EuroCert.

5.4 Audit logging procedures

EuroCert maintains a register of all security relevant events related to the performed trust services in order to ensure safety, supervision over the efficient operation of the systems and in order to hold users and personnel accountable for their activities. The security officer is responsible for keeping the register of events. The register is stored in the manner ensuring its integrity.

5.4.1 Types of events recorded

Event log includes the following events:

a) events directly related with providing trust services and in particular: generating CA's keys, accepting an application for issuing a certificate, generating keys and certificates to subscribers, revocation/suspension of certificates/cancellation of suspension, generating and publishing CRLs, acceptance of a request for a time-stamp,
b) activities related with servicing customers and subscribers: accepting and signing orders, agreements, applications, issuing certificates, delivering certificates, invoicing, etc.,
c) system logs from servers and work stations included in the system generating certificates,
d) events related to technical servicing the system: errors and alarms, register of changes introduced in the system, users support.

The event logs are recorded electronically. Records include an event identifier, date and time of the occurrence, type of the event, detailed description. A log is subject to archiving.

5.4.2 Frequency of processing log

Records of events are subject to regular control by the System Administrator and planned control by the Security Officer. Each time upon the occurrence of an alarm in the monitoring system for key elements of the certification authority system this occurrence is analysed by the System Administrator in co-operation with Security Officer in order to recognise possible unauthorised activities or other irregularities posing risk for the security of EuroCert.

5.4.3 Retention period for audit log

After archiving the event logs they are stored for at least 20 years, same as other information and documents related to performing trust services, in line with Article 17.2 of the Trust Services Act.

5.4.4 Protection of audit log

Access to event logs is given to the system auditor and security officer. The logs are protected against modifying, they are subject to procedures regarding creating backup copies and they are archived. The event logs archives are stored in the archive available to system auditor, security officer and the Management Board.

5.4.5 Audit log backup procedures

Event logs are copied in line with the system backup copies schedule. The copies are stored in the primary centre in safes or in secured network resources in a secured internal logic network of EuroCert.

Backup copying activities are performed automatically or manually depending on the type and intended use of the copy. Manual backup copying is performed by the system administrator under the supervision of security officer. Automatic backup copying is subject to regular control by the system

administrator and planned control by the security officer. In the event of detection of irregularities the control is run ad hoc.

5.4.6 Audit collection system

The program modules of the keys certification system create logs in the event logs automatically. Other events are logged manually in relevant databases. For the needs of the internal audit, data is available on-line or from the archive logs kept in safes.

5.4.7 Notification to event-causing subject

Elements of the certification system and supporting systems are subject to permanent supervision by monitoring systems and trusted technical personnel. Information on the discovered risk or security breach is directly sent to the system administrator and the Security officer. Depending on the level and importance of the risk, individuals in charge of operating components to which the event pertains must be notified. Notifying may take place by e-mail and by phone.

In the event of a security breach or the loss of integrity that significantly affect the performed trust service or personal data processed and secure within the service, no later than within 24 hours from the occurrence of the event, EuroCert notifies the supervision body and, in relevant cases, other relevant entities in line with Article 19.2 of the eIDAS (see 5.7.1).

5.4.8 Vulnerability assessments

EuroCert is required to perform the analysis of vulnerability to hazards with regard to all held assets, in particular with regard to software and computer systems.

The risk analysis is performed at least once a year or during performing new services, major changes in systems or as a result of a security incident. The audit officer is responsible for internal audit and he is in charge of controlling the compliance of records in the safety register, proper storage of its copies, controlling actions undertaken in risk situations and controlling the observance of provisions hereof.

5.5 Records archival

Data archiving is conducted in line with regulations of "Policy of backup creation and archiving, management of event logs" and documentation of EuroCert trust services"

5.5.1 Types of records archived

Subject to archiving are:

- trust services agreement referred to in Article 14 of the Trust Services Act,
- received applications and issued decisions, in hard copy and in electronic version,
- all information on subscribers collected during the certificate issuing process,
- certificates database,
- issued CRLs,
- certificates for trust services provider,
- the CA's keys history, from generation to destruction, inclusively,
- policies, internal regulations, procedures, statutes,

and other documents subject to archiving as set out individually in other subchapters of this Policy, in particular in 5.4.1.

5.5.2 Retention period for archive

Hard copy documents and electronic information described in 5.5.1, directly related with used trust services are stored for 20 years from their creation date (according to the Trust Services Act, Article 17 § 2).

5.5.3 Protection of archive

Archive data in electronic external carriers is stored in the primary centre in safes. Electronic data in files is stored in secure resource dedicated to electronic archive materials. Hard copy archive data is stored in the registered office of EuroCert Sp. z o.o. in access control rooms, in metal lockers locked with keys.

5.5.4 Archive backup procedures

Backup copies are created in order to protect data and to enable restoring the system after a failure. For this purpose the following is copied:

- installation discs with system software, including operating systems,
- installation discs with Certification authority applications and RA applications,
- history of the CA keys, certificates and CRLs,
- data from the repository of the Certification authority,
- information about subscribers and EuroCert personnel,
- events registers.

Detailed procedures of performing backup copies are regulated by internal EuroCert policies.

5.5.5 Requirements for time-stamping of records

Archived data is not subject to time stamping.

5.5.6 Archive collection system (internal or external)

EuroCert archives data by its own means, in access control rooms, using metal lockers, with key locks, fireproof safes and dedicated secure network resource. Archive copies of electronic data are stores in the primary centre. Detailed procedures of creating archives are regulated by internal EuroCert policies.

5.5.7 Procedures to obtain and verify archive information

In order to check the integrity, verified data is, when applicable, from time to time tested and compared with original data. This activity is performed under the procedure of internal planned control.. In the event of discovering damages or destruction of original data or archived data, discovered damage is removed as soon as possible.

5.6 Key changeover

The key exchange procedure refers to Certification authority keys used for signing certificates, CRLs, time stamps.

The exchange of keys of certification authorities is performed in the manner ensuring keeping the agreed minimum certificates validity period. Before the expiry of the certificate of a certain authority a new, independent public key infrastructure is created under which a new pair of keys and a certificate

of the new Certification authority is generated. Until the expiry of the old certification authority's certificate, both centres operate. The new Certification authority takes over the role of the expiring one, performs all activities related with servicing certificates: generating, suspending and revoking certificates, generating CRL. The expiring certification authority processes only revoking and suspending certificates issued within its own infrastructure and generate CRLs until its operating activity ceases (the certificate expires).

A new Certification authority's certificate is published in the repository (chapter 2). Information on changing keys may be published in the mass media.

The procedure of exchanging a pair of keys goes as follows:

- an application to the supervisory body for issuing a new certificate,
- creating new keys of the CA and notifying the Minister of digital affairs about hem, in order to issue a new certificate from NCCert and placing on TSL,
- the receipt of certificate from NCCert and issuing by NCCert a new TSL,
- publication of a new certificate in the repository.

5.7 Compromise and disaster recovery

EuroCert has implemented procedures of conduct t in critical situations (including natural disasters) which make it possible to reinstate business operations at least covering the minimal service level. The Business Continuity Plan (BCP) is reviewed annually and updated when necessary. The BCP is to prepare EuroCert for critical situations.

In the event of a critical situation the Disaster Recovery Plan (DRP) is implemented. DRP is part of BCP and contains scenarios of acting in critical situations. It is reviewed alongside the BCP's reviews. The BCP and DRP are subject to at least yearly technological and business tests. Technological tests include disaster recovery. Business tests allow to verify the performance of business processes in such a situation. Moreover, call tree tests are performed concerning the event notification of members of emergency teams.

5.7.1 Incident and compromise handling procedures

The procedures in the event of any threats of system security breach are described in the safety incident management procedure and business continuity plan, applicable at EuroCert. These procedures and BCP are in line with the requirements of Article 19.2 of the eIDAS .

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

EuroCert has a set of operating procedures should recovery of resources be necessary. In each location there are resources allowing for the recovery of basic functionalities of the Certification authority. In particular they include:

a) data back-up;
b) back-up keys of certification authorities;
c) cryptographic cards' copies with divided secrets and administration cards;
d) carriers with keys certification system software;
e) procedures and architecture of the certification authority.

The DRP is within the business continuity plan and it is tested on a regular basis. A report is created after the tests.

5.7.3 Entity private key compromise procedures

Eurocert has relevant action plans applicable in the event of the loss of confidentiality of EuroCert's private key or a justified suspicion that such event occurred (see 5.4.7). These plans provide for the following, but not limited to:

a) notifying the supervisory body about the occurrence of the safety incident in the "incident notification form by trust service provider" in line with Article 19.2 of the eIDAS,
b) notifying subscribers about the existing situation and about further action plan,
c) addressing the supervisory body with a request for revoking the certificate of the trust services provider related to the revealed private key and all currently valid certificates signed using the compromised private key,
d) notification about revoking the qualified authority's certificate using available information channels,
e) creating new qualified authority's keys and notifying the Ministry of Digital Affairs about them in order to issue a new certificate of the trust services provider and to put it on the TSL,
f) if it is possible in a certain situation (in particular if databases of EuroCert remain credible) – issuing new certificates for subscribers for the keys based on new authority keys, with their expiry date at least the same as the date of revoked certificates, without charging the subscribers with any costs for this operation.

In the event of loss of the confidentiality of the private key passed on by subscribers (service of remote signature/seal) EuroCert immediately revokes the key certificates and informs subscribers about this event.

When it happens that the certification authority's or subscribers' cryptographic algorithms or their parameters are insufficient for an intended period of their usage, EuroCert informs all the subscribers, makes this information public as well as facilitates revocation of affected certificates. If possible, certificates will be replaced with new ones, using new cryptographic algorithms and/or their parameters.

5.7.4 Business continuity capabilities after a disaster

EuroCert has implemented plans ensuring the security and continuity in providing critical services of the certification authority in the event of a physical damage of the computer system, software failure and telecommunication network and power supply failures, disasters and other unpredicted circumstances.

The EuroCert's technical infrastructure is protected in order to enable continuous work in the event of failure, while in the event of a disaster, equipment or infrastructure failure exceeding the capacities of the protection, the certification authority will be launched in a backup centre within 1 hour from the moment of finding the failure in line with the centres switch-over procedure applicable at EuroCert.

The backup centre ensures business continuity of the certification authority within the scope of revoking or suspending certificates and publishing the CRLs.

5.8 CA or RA termination

EuroCert is obliged to notify all subscribers holding valid certificates and a supervision body at least ninety days in advance about the intention to cease the operations including providing qualified trust services (see Article 7 of the Trust Services Act).

The termination plan for a qualified trust service providers, referred to in Article 24 Clause 2 letter i eIDAS and in Article 19 Clause 3 of the Trust Services Act, held by EuroCert is prepared in the event described above.

Upon issuing the last CRL list, the private key of the qualified authority is destroyed. On termination of EuroCert operations documents subject to archiving are submitted to the supervisory body or a body appointed by it.

6 Technical security controls

Below are presented rules of creating and managing (e.g. storage and use) in pairs cryptographic keys under the control of their owners (the certification authority or subscribers) together with technical conditions related to it.

6.1 Key pair generation and installation

EuroCert holds at least one certificate which is used in the process of electronic certification of qualified certificates and CRLs.
Private keys of Certification Authority Centrum Kwalifikowane EuroCert are uses for signing certificates and CRLs. The RSA algorithm combined with SHA-256 is used while affixing an electronic signature.

6.1.1 Key pair generation

The Certification authority keys are generated by EuroCert personnel in line with an internal procedure, in the presence of at least two individuals whose functions are directly related with the performance of qualified certification services (see 5.2.2), including the Security officer. A report is prepared from the ceremony of keys generating.

The keys of certification authorities are generated using a separated, credible workstation and an HSM cryptographic module operating in unison with this station, holding the certificate of Common Criteria EAL4+ level. Generating keys and operations related with the use of a private key take place exclusively in the cryptographic module and they are registered.

Private keys of subscribers can be generated by EuroCert on the cryptographic card or hardware cryptographic mode (HSM). In case of an cryptographic card the private key is under the sole supervision of the subscriber (or his/her proxy when a legal person) and it cannot be escrowed. In case of HSM subscribers have a sole access to its private key contained therein upon login to and individual service account or remote signature/seal.

A subscriber may generate a pair of keys themselves and present a public key for certification in the form of the PKCS#10 request (see 3.2.1).

If the subscriber generates a pair of keys on their own it should meet the requirements specified in section 6.1.5.

6.1.2 Private key delivery to subscriber

Keys of the Subscribers which was generated by EuroCert are provided to the Subscriber personally (in case of qualified certificates for electronic signature) or to the eligible person (in case of other certificates) together with the public key certificate.

If the keys are issued on a cryptographic card, access to the private key is secured with the PIN/PUK codes.

When EuroCert generates keys on behalf of subscriber and manages these keys on behalf of a subscriber, the private key is not delivered to the subscriber. The subscriber has access to the private key based on:

1) identification with login and password,
2) one time password (OTP) SMS.

EuroCert ensures that procedures applied in the authority at no time after generation of a private key on the subscriber's request allow to use it for electronic signatures or seals by any other person than the key owner only.

6.1.3 Public key delivery to certificate issuer

If a pair of keys is generated by the certification authority, it is not necessary for the subscriber to deliver the public key.

If the keys are generated by the subscriber, they deliver their public key to the RA in the form of electronic request signed with the private key which complies with the PKCS#10 standard.

6.1.4 CA public key delivery to relying parties

Public keys of the Certification authority are publicly available in the form of certificates of trust services providers issued by the National Certification Authority in line with recommendation ITU-T X.509 v.3.

The keys are distributed by publishing in the publicly available repository (see chapter 2) and listed on the national TSL.

6.1.5 Key sizes

The keys of all certification authorities of EuroCert have 4096 RSA bits.

Keys of the subscribers have at least 2048 RSA bits.

EuroCert uses algorithms of SHA-256 hash function to sign certificates, time stamps and other tokens.

6.1.6 Public key parameters generation and quality checking

Public key generating parameters meet the requirements specified in the ETSI EN 319 401, ETSI EN 319 411 and ETSI TS 119 312 norms.

6.1.7 Key usage purposes

The private key usage is specified in the field "keyUsage" (OID: 2.5.29.15) which is one of the basic fields of certificates (see 7.1.2). This field is subject to obligatory verification by the relying parties and applications using the certificate.

Certificates for electronic signature/seal may be used exclusively for electronic signing (sealing). Generation and management of the certificates is subject to requirements defined for certificates used exclusively in providing the service of nonrepudiation (nonRepudiation defined bit).

EuroCert has keys to electronic certification of certificates and CRLs (keyCertSign and cRLSign). Respective public key may be exclusively used for verification of certificates and CRLs.

EuroCert QTSA has keys used for electronic certification of time stamp tokens (digitalSignature and nonRepudiation).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

EuroCert enables subscribers to use the keys exclusively on QSCD.

Pair of keys generated by EuroCert on cryptographic card is secured by EuroCert with PIN and PUK codes generated by EuroCert and printed in the secure envelope. Before the first usage of card subscriber shall change PIN code on his own code.

For more information see the section 6.1.2.

6.2.1 Cryptographic module standards and controls

Private keys of subscribers related to qualified certificates for electronic signature/seal are processed exclusively in qualified signature/seal creation devices (QSCD).

Hardware security modules (HSM) used by EuroCert and subscribers are compliant with Common Criteria EAL 4+.

6.2.2 Private key (n out of m) multi-person control

The private key of all of the EuroCert's certification authorities is secured by dividing the key in parts (namely secrets) in their number exceeding the number required for opening the key. The assumed number of key division into secrets and the threshold value allowing for restoring this key are presented in Table 7.

Tab. 7. Private key division scheme

Certification authority	Total number of secrets [n]	Number of secrets necessary for using the key [m]
Centrum Kwalifikowane EuroCert	4	3
EuroCert QTSA	4	3

Secrets are recorded on cryptographic cards secured with PIN known only to the person to whom it was handed over during the key generating ceremony. Secrets as well as PINs protecting them are stores in various, physically protected places. None of this locations are used for storing the set of cards and PINs that allows for recovering the key of the Certification authority.

If it is necessary to recover the key from backup copies, a procedure of introducing the key to the module is performed, as described in 6.2.6.

6.2.3 Private key escrow

Private keys of a subscriber cannot be escrowed apart from the keys which are used in remote signature/ seal service.
Private keys of certification authorities of EuroCert are not escrowed.

6.2.4 Private key backup

The mechanism of entrusting a backup copy of the private key of the certification authority is performed by dividing the key in parts (see 6.2.2).

EuroCert does not keep copies of subscriber's private keys.

6.2.5 Private key archival

Private keys of Certification authorities used for performing electronic seals are not archived and are destroyed immediately upon ceasing signing operations or upon the lapse of the validity period of a certificate complementary with them or upon its invalidation.

EuroCert does not archive subscribers' private keys.

6.2.6 Private key transfer into or from a cryptographic module

Private key is uploaded to the cryptographic modules in the following situations:
1) launch of the certification authority or time-stamping authority, during the system start-up;
2) recovery of the key of the certification authority or time-stamping authority in the backup location;
3) replacement of the HSM.

The key is uploaded to the module in the presence of holders of co-shared secrets. To upload the key it is necessary to have present the number of secrets described in point 6.2.2. Uploading is carried out in a closed security environment. A private key is made up of elements. Fragments of the secret key are provided in sequence from the cards, enciphered files are uploaded to the module memory, and then deciphered. The private key is ready to use. Uploading the key to the module is recorded in the register of events.

6.2.7 Private key storage on HSM

After deciphering and uploading the private key to the memory of the cryptographic module, it is hardware protected. It is not possible to read the value of the private key from the module, as this key never leaves the module. Operations that require the use of a private key are performed in the cryptographic module.

6.2.8 Method of activating private key

A private key of the Certification authority uploaded to a HSM device upon its generating, transferring in cyphered form from another module or recovering from parts shared by relying parties, remain active until their physical removal from the module or until the HSM is switched off.

Subscribers private keys stored on a QSCD are activated only after authorisation (upon inserting PIN) and only for the duration of a single cryptographic operation with the use of the key. Upon completing the operation the private key is automatically deactivated and it must be activated again before the performance of another operation, notwithstanding whether the keys are stored on an cryptographic card or other qualified signature (seal) creation (e.g. HSM).

6.2.9 Method of deactivating private key

Deactivating EuroCert Certification authority's keys is performed by the Security officer only in the event when the key expiry date has lapsed and the key was revoked or there is a necessity of timely suspend the operations of the signing server. Deactivating a key involves cleaning the HSM memory from uploaded keys. Each deactivation of a private key is recorded in the events log.
Deactivating a subscriber's private key takes place immediately upon affixing an electronic signature/seal.

6.2.10 Method of destroying private key

Destroying subscribers' private keys is performed by the holder of an cryptographic card by logical removal of the key (from an electronic card.) or the physical destruction of an electronic card).

In the case of remote seal service destroying the key takes place by removal of encrypted key from the HSM device and from the key storage area in an encrypted form.

The destruction of the private key of the certification authorities means a physical destruction of cryptographic cards and/or other media, on which copies or archives of shared secrets are stores or their safe removal from the media (from a cryptographic card, or HSM, etc.). Destroying private keys of the Certification authorities takes place in the presence of a committee, by the EuroCert's personnel, in line with a documented procedure. The presence of at least two persons is required, including the Security officer. Cards must be identified before being destroyed. A report is prepared from the destruction procedure.

6.2.11 Cryptographic Module Rating

See 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

EuroCert implements a long term archiving process for public keys in the form of certificates of Subscribers or trust service providers, subject to the principles applicable to other archived data (see 5.5).

Archiving public keys aims at the possibility of verifying electronic signatures/seals/time stamps upon the expiry of the validity period of certificate of Subscriber or CA.

6.3.2 Certificate operational periods and key pair usage periods

Validity period for private keys and certificates of subscribers does not exceed 3 years and it is set out inside each certificate. "Valid from" date for each certificate cannot be earlier than its generation date.

A time stamp issued by EuroCert is valid till the end of validity period of the certificate issued for time stamping authority.

6.4 Activation data

Activation data is used for activation of private keys used by certification authorities and subscribers. It is used most often at the stage of authentication of the subject and the access control to the private key.

6.4.1 Activation data generation and installation

If the certificate and the pair of keys have been generated on a cryptographic card, the subscriber receives PIN and PUK codes securing access to the card in a safe envelope.

The subscriber should assign the new codes to secure the card with a pair of keys and the certificate with the use of the application for card management that has been provided by EuroCert together with the card.

Shared secrets used to protect private keys of all CAs providing trust services are generated in line with requirements specified in 6.2.2.

6.4.2 Activation data protection

Only the subscriber should know the access code to the private key assigned by this subscriber. The subscriber is responsible for protecting the PIN and PUK. Disclosing PIN and PUK should constitute the grounds for a demand that the certificate be revoked or suspended.
Multiple failures to access the private key result in blocking the electronic card. Activation data which is saved can never be stored together with the card.

6.4.3 Other aspects of activation data

Copies of passwords for securing access to private keys are not stored at EuroCert. EuroCert does not hold any codes or date allowing for restoring PIN and PUK codes securing access to the private key, assigned by the subscriber.

6.5 Computer security controls

Certification authority is not required to use servers holding security certificates for hardware or operational system software.

All operations planned to be performed on the computers and servers of the certification authority can be run upon prior authentication and eligibility control. Performed operations are stored in event logs.

6.6 Life cycle technical controls

6.6.1 System development controls

Introducing modifications or changes in the EuroCert system is performed by the Security officer. He/she approves the system configuration and all changes in the software and hardware. Tests of new software versions and/or using the existing databases for this purpose takes place in the testing environment. The procedures applied by EuroCert during the performance of these tests guarantee uninterrupted work of the EuroCert system, integrity of its resources and the confidentiality of information.

Hardware exchange in the system is registered and monitored. In particular:

a) hardware is delivered in a manner which enables tracking of the whole route travelled by the hardware from the supplier to the installation premises,
b) delivery of exchange hardware is performed in the same way as the delivery of the original hardware; exchange works are performed by trusted and qualified personnel.

EuroCert accepts however only these cryptographic modules which meet the requirements specified in 6.2.1.

Cryptographic hardware modules delivered to EuroCert are each time checked in terms of breach of delivery and physical and logical integrity of the module. Verification followed by a report is performed exclusively by EuroCert trusted personnel. Cryptographic hardware modules which are not used are secured in a packaging which is impossible to stay undetected when opened. The modules prepared in this manner are stored in safes located in surveillance rooms accessible only by an appointed group of EuroCert trust personnel.

6.6.2 Security management controls

The security management control aims at the supervision of EuroCert system operations ensuring that the system works properly and its functions are in line with the planned and implemented configuration.

Despite the fact that administration works and changes in EuroCert systems are registered, each of them requires additional verifying and acceptance by at least two EuroCert administrators. The change control system notifies authorised employees about the occurrence of a modification in EuroCert system and it requires it be verified by a person other than the one who introduced the change. Current configuration of EuroCert system as well as any modifications and updates of the system are documented and supervised. Mechanisms applied in EuroCert allow for constant verification of the system integrity, versions control as well as authorising and verifying sources of the origin.

6.6.3 Life cycle security controls

The Policy does not impose any life cycle for the applied security measures. Security measures are replaced in the event of necessity to apply other measures than those that are currently used, amendments in legal regulations or if they are technologically outdated and do not comply with the current standards and norms.

6.7 Network security controls

Access to EuroCert system under which qualified trust services are performed, is secured on the level specified for performing qualified trust services.

Detailed description of EuroCert network configuration and its securities is presented in the documentation of technical infrastructure of EuroCert system. This document is classified and is made accessible only to security officer, system administrator and audit officers.

6.8 Time-stamping

Electronic time stamps are compliant with the ETSI EN 319 422.

The primary objective of electronic timestamp service, provided by the electronic timestamp authority EuroCert QTSA is to mark an electronic documents, electronic signatures, electronic transactions, etc. with a reliable time. Electronic timestamp is proof that data object existed before the date placed in this electronic timestamp. Thanks to this:

- electronic timestamp authority confirms the existence of data,
- electronic timestamp authority allows to prove that an electronic signature was made prior to the revocation of the key used to signing a document or a message.

Electronic timestamp authority EuroCert QTSA is not a party of transactions referred to and marked with a reliable time.

Procedure of obtaining a time – stamp issued by electronic timestamp authority is carried out as follows:

- applicant sends a request containing the value of the digest (associated with document, message etc.), the identifier of the hash function and the session identifier (nonce); the request shall contains OID policy used for the electronic timestamp token issuance; the format of issuance is default in the case of lack of identifiers,
- electronic timestamp authority verifies completeness and correctness of application,
- electronic timestamp authority generates an electronic timestamp (electronic timestamp token – TST), which contains serial number, protocol identifier, time from reliable source, application data, data generated by electronic timestamp authority, binding in a cryptographic manner the time with the digest value, the identifier of the hash function and the session identifier,
- electronic timestamp authority submits an electronic timestamp token to the requesting entity,
- requesting entity verifies the correctness of electronic timestamp token.

Electronic timestamps are issued in accordance with the following requirements:

- trusted time source is synchronized with International Atomic Time (TAI) with an accuracy of 1 second,
- serial number of electronic timestamp token is unique within certification authority domain EuroCert QTSA; this feature is also retained in the event of a resumption of service after a failure,
- the electronic timestamp authority EuroCert QTSA owns private key used for creating electronic confirmations of electronic timestamp tokens.

7 Certificate and CRL profiles

Profiles of certificates and CRLs are issued in line with norms of ETSI TS 119 412-1 and ETSI EN 319 412 (Parts 2,3,4,5).

7.1 Certificate profile

A certificate is a sequence of value of basic fields and extensions. Basic fields of the certificate are described in Table 8.

Tab. 8. Basic fields of a certificate

Field Name	Description		Value
Version	certificate complies with X.509 standard, version 3		V3
SerialNumber	Certificate number, unique in the CA		Serial number (product key) of the certificate
SignatureAlgorithm	cryptographic algorithm identifier used for the performance of an electronic seal made by the CA on the certificate.		sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer (certificate issuer's DN)	Common Name		CN = Centrum Kwalifikowane Eurocert
	Organization		O = EuroCert Sp. z o.o.
	Country		C = PL
	Organization identifier		2.5.4.97 = VATPL-9512352379
NotBefore	certificate issuing date	certificate issuing date	
NotAfter	certificate expiry date	certificate expiry date	
Subject	The subscriber's name complies with the requirements of ETSI TS 119 412-1, *ETSI EN 319 412 (Parts 2,3,4,5).*	Subscriber's DN (see 3.1)	
SubjectPublicKeyInfo	Algorithm identifier of the public key, the key length in bits and the public key's value.	Public Key Algorithm	SHA256WithRSAEncryption
		RSA Public Key (the length of the key)	2048/3072 bits
SignatureValue	electronic seal is produced on the certificate by the CA.	The value in the electronic certification field (signatureValue) results from applying the algorithm of a hash function to all fields of certification, specified by its content fields (tbsCertificate) followed by cyphering the result using the private key of the CA (publisher).	

7.1.1 Version number

Certificates are issued in line with version 3 of X.509 standard.

7.1.2 Certificate extensions

EuroCert operates extension fields described in Table 9.

In the field "certificate policies" of certificates issued by EuroCert there are certificate policy object identifiers, which enable relying parties specifying whether the use of a certificate verified by them complies with the declared purpose of the certificate. Certificate policies object identifiers are also included in the time stamps.

Tab. 9. Certificate extensions

Extension name	Critical?	Description	Value
AuthorityKeyIdentifier	NO	public key identifier of the issuer used for verifying the issued certificate	Public key hash function of the certification authority
SubjectKeyIdentifier	NO	Certificate identifier containing the hash public key contained in the certificate	Public key hash function of the subscriber
KeyUsage	YES	specifies the scope of used public key used by the subscriber.	nonRepudiation (a key for non-repudiation function)
ExtendedKeyUsage	NO	Applies only to certificate for website authentication	clientAuthentication serverAuthentication
SubjectAltName	NO	Applies only to certificate for website authentication	Fully Qualified Domain Name
cabfOrganizationIdentifier	NO	Applies only to certificate for website authentication	Identifier of an organization
CertificatePolicies	NO	indicating certificate policies with the certificate issued in line with it	a.Certificate Policy identifier compliant with 7.1.6, and depending on the type of certificate: b. NCP+, c. qcp-l / qcp-l-qscd, d. qcp-n / qcp-n-qscd, e. qcp-w, f. qcp-w-psd2, g. 2.23.140.1.1, h. 0.4.0.19431.1.1.3.
CRLDistributionPoints	NO	CRL distribution point (specifies the URL address on which the current CRL is published)	http://crl.eurocert.pl/qca03.crl
Authority Information Access	NO	Access to information on the certification authority – issuer	1) URL address, issuing certificates of trust services providers; 2)address URL of OCSP service: http://crl.eurocert.pl/OCSP/
BasicConstraints	YES	allows for checking whether the certificate entity is an end user or an entity issuing certificates	Entity type=none (end user) Limit on the certification path's length=none

qcCompliance	NO	Certificate issuer's declaration	A declaration that the certificate is a qualified certificate within the eIDAS meaning; OID: {itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) 1 1}
qcSSCD	NO	Certificate issuer's declaration Don't apply to website certificate	indication that a private key is stored in a device qualified for affixing signatures; OID: {0.4.0.1862.1.4}
qcType	No	Indication of a certificate type	Indication of one out of two types of certificates: Certificate for an electronic signature (OID: 0.4.0.1862.1.6.1), Certificate for an electronic seal (0.4.0.1862.1.6.2), Certificate for website authentication (0.4.0.1862.1.6.3).
qcPSD2	NO	Applies only to certificate for electronic seal and website authentication acc. to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2).	Roles of Payment Service Providers (PSP), Name of the National Competent Authority (NCA), ID of the National Competent Authority

7.1.3 Algorithm object identifiers

The certification authority seals the certificates with the RSA algorithm having 4096 bit keys and the SHA-256 hash function.

The subscribers' certificates are issued for the RSA keys with the length of 2048/3072 bits and the SHA-256 hash function.

7.1.4 Name forms

See 3.1.1 and Tab 8 in 7.1.

7.1.5 Name constraints

See 7.1.4.

The qualified certificates may not contain IP addresses in the subject and subjectAltName fields.

Domain names may be included only in the qualified certificates for certification of websites. In the subject and subjectAltName fields those certificates may not contain domain names that are not registered in the online DNS system.

7.1.6 Certificate policy object identifier

See 1.3.1.

7.1.7 Usage of Policy Constraints extension

EuroCert does not anticipate using in certificates any other extensions that the ones indicated in 7.1.2.

7.1.8 Policy qualifiers syntax and semantics

EuroCert does not set out any requirements in this regard.

7.2 CRL profile

The list of revoked and suspended certificates is a sequence of fields presented in Table 10. The CRL list profile is compliant with the X.509 V2 standard.

Tab. 10. CRL's profile in the format complying with X.509 V2

Attribute	Value
version	V2
SignatureAlgorithm cryptographic algorithm identifier, describing the algorithm used for the performance of an electronic authorisation made by the CA on the CRL	sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer CRL's issuer distinguishing name, compliant with the name set out in the certificate's profile	See table 8 in 7.1.
thisUpdate	date and hour of the list issuing
nextUpdate	date and hour of the consecutive list issuing (thisUpdate + not exceeding 24 hours)
SignatureValue	Electronic certification of the CRL's issuer
revokedCertificates (revoked certificates list) userCertificate revocationDate reasonCode	 serial number (product key) of a revoked certificate date and hour of certificate revoking reasons for listing the certificate on the CRL: a) unspecified, b) keyCompromise – key compromise, c) cACompromise – CA key comprimise, d) affiliationChanged – Subscriber's data change, e) superseded – key is superseded (replaced), f) cessationOfOperation – cessation of the key operation for purposes for which it was issued g) certificateHold – the certificate was suspended.

7.2.1 Version number

CRL format complies with version 2 of X.509 standard.

7.2.2 CRL and CRL entry extensions

EuroCert serves non-critical extension for CRL named reasonCode (see table 10), containing the code for the reason of revoking a certificate.

7.3 OCSP profile

The Service Provider operates an online certificate status service according to the IETF RFC 6960.

8 Compliance audit and other assessments

Audits are performed at EuroCert in order to check the compliance of the EuroCert procedure with requirements imposed on qualified trust service providers described in the eIDAS and procedures and processes described in EuroCert's documentation (including this Policy).

8.1 Frequency or circumstances of assessment

The audit is performed by EuroCert individually (an internal audit) in line with the internal audit policy, or once every two years by a third party unit that assesses the compliance under Article 20 (1) of the eIDAS (an external audit).

The external audit may be performed also at any time at the request of the supervisory body under Article 31 of the Trust Services Act in connection with Articles 20.2 and 17.4 lit e) of the eIDAS .

8.2 Identity/qualifications of assessor

The internal audit is performed by an authorised national or European institution authorised for this type of business, holding the accreditation for performing audits of compliance of trust services providers meeting the requirements specified by norm ETSI EN 319 403.

8.3 Assessor's relationship to assessed entity

Auditors cannot perform business operations with regard to trust services, perform trust services, be partners or shareholders of a provider of trust services nor perform obligations of a person representing or a member of a supervisory board or an audit committee of the provider, as well as to remain in the employment relationship with the provider, enter into the contract of mandate or into any other legal relationship of similar character.

8.4 Topics covered by assessment

Issues covered by the audit include:

a) testing organisation and legal requirements under the eIDAS and issued executive decisions for this purpose,
b) monitoring and ensuring the compliance of operations with procedures,
c) subscribers' identity verification procedures,
d) physical securities at EuroCert,
e) information security management,
f) personnel security,
g) certification services and procedures for their provision,
h) software and network access protection,
i) event logs and system monitoring procedures,
j) back-up copies preparing procedures and their restoring,
k) archiving procedures implementing,
l) documenting changes in EuroCert configuration parameters,
m) documenting inspections and maintenance of hardware and software.

8.5 Actions taken as a result of deficiency

Internal and external audits reports are submitted to managing parties at EuroCert who appoint a team of employees listed in 5.2.1 in order to prepare within the time limit set out in the report, a written

opinion of EuroCert regarding all failures indicated in the reports. The response must specify also methods and dates for removing defects. Information on removing defects is forwarded to the auditing authority.

With regard to an audit order by the Minister of Digital Affairs, upon reviewing the report and reservations, as well as with explanations submitted by EuroCert, the minister notifies this entity about the results of control and in the event of finding irregularities, it sets out the time limit for their removal, of at least 14 days (Article 34 of the Trust Services Act).

8.6 Communication of results

Information about audit results in the form of a report from its performance or the report summary are shared only internally.

9 Other business and legal matters

9.1 Fees

EuroCert collects fees for provided trust service in line with the price list published at https://sklep.eurocert.pl.

9.1.1 Certificate issuance or renewal fees

EuroCert collects fees for issuing a certificate and its renewal.

9.1.2 Certificate access fees

Eurocert does not collect any fees for access to certificates of trust service providers.

9.1.3 Revocation or status information access fees

EuroCert does not collect fees for revoking, suspension or cancellation of suspension of a certificate and for sharing CRLs.

9.1.4 Fees for other services

EuroCert can collect also other fees if they are introduced to the price list These fees may include, for instance the payment for

a) trainings and consultations,
b) cards,
c) card readers,
d) software licences,
e) performing developer, launching and installation works.

9.1.5 Refund policy

Return of payments is possible under the provisions of the Polish law in the event of EuroCert failing to perform the agreement or if the service is performed contrary to the provisions of this Policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

Eurocert sp. o.o. holds an third party liability insurance in line with the requirements of the Regulation of the Minister of Development and Finance of 19 December 2016 on the obligatory third party liability insurance for a qualified trust service providers.

The financial liability of EuroCert with regard to one event amounts to the equivalent of EUR 250,000 in PLN, but not exceeding EUR 1,000,000 with regard to all such events.

9.2.2 Other assets

EuroCert holds sufficient financial measures necessary for conducting its business and for performing its obligations.

9.2.3 Insurance or warranty coverage for end-entities

This Policy does not set out any requirements in this regard.

9.3 Confidentiality of business information

EuroCert and persons employed by it or entities acting on its behalf, are obliged to keep confidential all information obtained during the employment or during the performance of the activities described above, also upon the expiry of their employment or of the authorisation to perform these activities.

9.3.1 Scope of confidential information

This Policy does not set out any requirements in this regard.

9.3.2 Information not within the scope of confidential information

This Policy does not set out any requirements in this regard.

9.3.3 Responsibility to protect confidential information

This Policy does not set out any requirements in this regard.

9.4 Privacy of personal information

Personal data submitted to EuroCert by subscribers of certification services and by parties ordering certificates are subject to the protection set out in the Act of 10 May 2018 on data protection (Journal of Laws as of 24 May 2018, no. 1000).

9.4.1 Privacy plan

All personal data (in particular the subscribers' data) held by EuroCert is gathered, stored and processed in compliance with applicable provisions of law, in particular with the Act of 10 May 2018 on data protection (Journal of Laws as of 24 May 2018, no. 1000).

9.4.2 Information treated as private

EuroCert considers private all information related to rendering trust services except for the following information:

a) This Policy,
b) Certificates,
c) CRLs,
d) Infrastructure certificates,
e) Current information designated for publishing (such as price lists, commercial offer, current communications, contact details),
f) Information contained in the certificate content, if the subscriber agreed for their publication.

Only the information available in the public domain are shared with third parties in the certificate, upon receiving the subscriber's consent for their publication.

9.4.3 Information not deemed private

All information not designated as private and confidential by subscribers, relying parties or by EuroCert is non confidential information. Data entered in the certificate is considered non-confidential information.

All information necessary in the process of proper operation of certification services is considered public information. In particular, information included in a certificate by certificate issuing bodies in line with the description presented in chapter 7 is considered public. While applying for issuing the certificate, the subscriber agrees for making public the information contained in the certificate.

Part of information submitted by and shared with users may be shared to other entities exclusively at the user's consent.

9.4.4 Responsibility to protect private information

EuroCert Sp. z o.o., ul. Puławska 474, 02-884 Warszawa is a personal data controller for the subscriber, within the meaning of the Personal Data Protection Act and it is liable for the protection of personal date and other confidential information entrusted to it.

9.4.5 Notice and consent to use private information

EuroCert may entrust the personal data processing to a third party, in line with the requirements of the Personal Data Protection Act.

9.4.6 Disclosure pursuant to judicial or administrative process

EuroCert is obliged to disclose personal data to entities that may submit a demand to do so under mandatory provisions of law, in line with the requirements of the Personal Data Protection Act.

9.4.7 Other information disclosure circumstances

This Policy does not set out any requirements in this regard.

9.5 Intellectual property rights

Copyrights to this document are held by EuroCert Sp. z o.o and it may be used only for the purposes of using certificates. Any other application, including the use of total or fragment of the document requires a written consent of Eurocert Sp. z o.o., while Eurocert Sp. z o.o. agrees for copying and publishing this document in whole.

Subscribers are fully liable for data provided by them in certificates. EuroCert does not verify the rights to use reserved trademarks, and it is not liable for unauthorised use of trademarks and it is not a party in the event of any dispute related to it. In the case of the subscriber losing the right to use a certain name or other mark included in the certificate, it is obliged to notify about this fact in order to revoke the certificate due to the invalidity of data contained in the certificate.

A certificate by Centrum Kwalifikowane EuroCert is the property of EuroCert Sp. z o.o and EuroCert grants a licence for making a copy of this certificate and for including it in software, in particular in certificates warehouses or on hardware to software or hardware producers.

Each pair of keys to which a public key certificate is related, issued by EuroCert is – with regard to a personal certificate subscriber – the property of the subject of the certificate, described in the certificate subject field (see 7.1) or – with regard to a business certificate subscriber – the property of the subject represented by the subscriber.

9.6 Representations and warranties

9.6.1 CA representations and warranties

EuroCert guarantees that:

a) for generating subscriber's keys, it uses credible equipment in line with the norms set out in the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of the eIDAS ,
b) acts in line with the provisions of law, in particular it does not infringe the provisions of the *eIDAS and of the Trust Services Act* together with application regulations and it does not infringe any copyrights and licences of third parties,
c) performed services comply with generally accepted norms and standards, including:
   - ITU-T X.509 (ISO/IEC 9594-8 corresponds to it),
   - ISO/IEC 15945 (CMP protocol),
   - *in fact* PKCS#10, PKCS#7, PKCS#12,
   - ETSI EN 319 401,
   - ETSI EN 319 411-1,
   - ETSI EN 319 411-2,
   - ETSI TS 119 412-1,
   - ETSI EN 319 412-2,
   - ETSI EN 319 412-3,
   - ETSI EN 319 412-4
   - ETSI EN 319 412-5,
   - TS 119 312,
   - CA/Browser Forum.
d) observes and executes the certification procedures described in this document,
e) issued certificates contain data that is true and the data was updated at the moment of their confirmation,
f) issued certificates contain no errors resulting from any omissions or infringements of procedures by individuals approving the applications for issuing certificates or individuals issuing the certificates,
g) subscriber's DN included in certificates are unique,
h) ensures subscriber's personal data protection in line with the Act of 10 May 2018 on data protection (Journal of Laws as of 24 May 2018, no. 1000)and with application documents for this Act,
i) does not copy or store private keys of its customers, used for affixing electronic signatures (seals), with the exception of remote signature (seal) service,

j) employs employees who have the knowledge, qualifications and experience corresponding to the performed functions related with certification services, in particular including the following fields of expertise:
   i. automatic data processing in networks and in information systems,
   ii. networks and information systems protection mechanisms,
   iii. cryptography, electronic signatures and public key infrastructure,
   iv. hardware and software used for electronic data processing.

9.6.2 RA representations and warranties

The RA and persons confirming identity undertake to:

1) observing procedures of identity confirmation while issuing certificates in line with the rules set out in this document, internal procedures an in applicable laws and the principles of social co-existence, particularly taking into account the require due diligence,
2) issuing necessary certification requests tokens, authorising for using a certain EuroCert service,
3) sending to EuroCert confirmed data of subscribers,
4) submitting to EuroCert's recommendations,
5) protecting private keys of the RA's operators,
6) refraining from the use of keys of private operators for other purposes than the ones specified in the Policy,
7) undergoing planned audits performed at EuroCert's order or by EuroCert.

Obligations of subscribers and relying parties were presented respectively in 4.5.1 and 4.5.2.

9.6.3 Subscriber representations and warranties

See 4.5.1.

9.6.4 Relying party representations and warranties

See 4.5.2.

9.6.5 Representations and warranties of other participants

This Policy does not set out any requirements in this regard.

9.7 Disclaimers of warranties

EuroCert is not liable for any damages that were incurred or could be incurred by certification services recipients or third parties, resulting from other reasons than non-performance undue performance of obligations by EuroCert or entities acting on its behalf. In particular, EuroCert is not liable for the effects of infringing the obligations imposed on a subscriber and relying parties, listed respectively in 4.5.1 and 4.5.2.

In particular cases, EuroCert is also not liable for damages caused by failing to perform or by improper performance of its obligations, if failing to perform or the improper performance of these obligations results from circumstances not attributable to EuroCert that could not have been prevented despite exercising due diligence.

9.8 Limitations of liability

EuroCert is not liable for damages resulting from infringing the obligations imposed on the recipients of its services, listed respectively in 4.5.1 and 4.5.2.

In the event of shortening of validity period of certificates through EuroCert's fault, EuroCert's liability is limited to refunding the costs of issuing the certificates, proportionately to the period being shortened.

9.9 Indemnities

EuroCert may demand compensation from a subscriber for damages incurred by EuroCert as a result of the subscriber giving false information which despite due diligence performed by EuroCert was included in the issued public key certificate.

9.10 Term and termination

9.10.1 Term

This document is valid from the moment of being given the "valid" status and publishing it in the EuroCert repository, until the consecutive valid version is published.

9.10.2 Termination

The consecutive version of the Policy indicates its validity date which is also the expiry date of the current Policy. At the same time the previous Policy loses its "valid" status.

9.10.3 Effect of termination and survival

Subscribers observe only the valid Policy.

9.11 Individual notices and communications with participants

All letters related to EuroCert's business should be delivered to the address given in 1.5.

9.12 Amendments

9.12.1 Procedure for amendment

See 1.5.4.

9.12.2 Notification mechanism and period

Not applicable.

9.12.3 Circumstances under which OID must be changed

OID change for the Policy may take place only in the event of the change of the entity supervising CA and in the case of changes that may have actual effect on a significant number of subscribers.

9.13 Disputes resolution provisions

Disputes resolution may apply only to discrepancies or conflicts arising between parties with regard to issuing and revoking qualified certificate based on the provisions of the Policy and agreements entered into.

Disputes or complaints arising from using the certificates, certificates status verification tokens, time stamp tokens issued by EuroCert will be resolved based on written information following mediations. Complaints processing is reserved exclusively to the president of the management board. They are subject to a written review within 10 days.

Disputes related to qualified certification services performed by EuroCert will be first of all resolved under conciliation proceedings.

If the dispute is not resolved within 30 days from commencing conciliation proceedings, the parties are entitled to bring the case to the court. The applicable court for reviewing the case will be a common court with its jurisdiction over the defendant's address.

If any other disputes arise as a consequence of using a certificate issued or other qualified services rendered by EuroCert, the subscriber undertakes in writing to notify EuroCert about the subject matter of the dispute.

9.14 Governing law

EuroCert's business operations are based on the rules included in the Policy s and in the applicable provisions of law. In order to interpret the terms included in the Policy, they must be considered in line with eIDAS and with Trust Services Act.

9.15 Compliance with applicable law

EuroCert business principles comply with the applicable laws, in particular with the provisions contained in the following legal acts:

a) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 October 2014 and executive decisions of the Commission (EU) issued on the basis of this Policy,
b) The Act on Trust Services and Electronic Identification of 5 September 2016,
c) Act of 10 May 2018 on data protection (Journal of Laws as of 24 May 2018, no. 1000),
d) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,
e) The Criminal Code of 6 June 1997,
f) The Identity Cards Act of 6 August 2010,
g) The Passports Act of 13 July 2006,
h) The Foreigners Act of 12 July 2013,
i) The Copyright Law of 4 February 1994.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The terms and conditions of the agreement entered into between the parties and the Policy are binding for the parties.

9.16.2 Assignment

No third party can take over the rights and obligations of the party to the agreement without the consent of the other party. In the case of cessation of the operations involving providing services

covered by this document, EuroCert may transfer the authorisation to use the private key and to issue and publish the CRL to another entity without the consent of the ordering party, subscriber or the relying party.

9.16.3 Severability

In case of any doubts, or if there is a conflict between provisions of the agreement and the Policy, the agreement prevails over the Policy.

In the event of illegality of any provision of any of these documents resulting it is invalidity, the provisions included in other documents remain valid.

9.16.4 Enforcement

Temporary non-performance of EuroCert's rights as well as failing to exercise them with regard to one or many subscribers cannot be interpreted as a waiver or permanent resignation from exercising these rights and it has no effect on the content and interpretation of the Policy.

9.16.5 Force Majeure

The occurrence of force majeure is understood as all extraordinary events that are external, impossible to predict, such as disasters, fires, floods, explosions, social unrests, acts of war, acts of state authorities, power supply failure or failure of a telecommunication connection which in part or in total disable the performance of obligations included in the agreement or in Policy or make difficult the performance of these obligations on terms and conditions set out therein. EuroCert shall not be liable for any infringement of its obligations if it results from an occurrence of force majeure.

10 Final provisions

n/a.

Document history

General information			
Signature			0-PT-025-04.01
Class of data protection			0 Public
Status			valid
Modification history			
Date of approval	Valid from (Effective date of implementation)	Version	Amendments
16.07.2018 r.	02.10.2018 r.	1	Creation of the document. This document covers the following previous documents: 1. Certification policy statement for qualified trust services v. 2.0, 2. The Certificate policy for EuroCert qualified certificates v. 3.0, 3. Policy for EuroCert qualified time-stamps v. 1.0.
10.06.2019	19.06.2019	2	- remote seal/signature provisions, - extension of the time within which CA must process the revocation request to 24h, - allowing the subscriber to generate the keys themselves.
20.08.2019	21.08.2019	3	- inclusion of provisions concerning certificates for website authentication.
22.04.2020	22.04.2020	3.1	- change of the way of conclusion of agreement by accepting terms of service provision, - correction of QSCD definition.
05.06.2020	31.03.2021	4.0	- inclusion of provisions concerning remote identification in chapter 3.2.
21.06.2023	21.06.2023	4.1	Added OCSP service in addition to CRL.