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

Version 1

Approved	
Position	CEO
Name and surname	Łukasz Konikiewicz
Date of approval	16.07.2018 r.
Valid from	02.10.2018 r.

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

Table of contents

1 Introduction

The Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services, hereinafter the "Regulation" describes the terms and conditions of providing trust services by EuroCert Sp. z o.o. – "Centrum EuroCert" (hereinafter: the „EuroCert"), comprising issuing:

a) qualified certificates for electronic signature;
b) qualified certificates for electronic seal,
   hereinafter referred to as "certificates", including revoking and suspending certificates as well as informing about the certificate status based on the CRL list and OCSP service;
c) qualified electronic time stamps, hereinafter referred to as "time stamps".

The Regulation is the certificate policy for each of the services mentioned above.

EuroCert is a qualified trust service provider performing in compliance with:

a) The Act on Trust Services and Electronic Identification of 5 September 2016 (Journal of Laws of 1579), hereinafter: the "Trust Services Act" and the Regulation of the Ministry of Digital Affairs of 5 October 2016 on the national trust infrastructure (Journal of Laws item 1632),
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 and repealing Directive 1999/93/EC, hereinafter: the "eIDAS Regulation".

The Regulation's structure has been based on recommendations RFC 3647[1].

1.1 Overview

EuroCert issues certificates and time stamps via respectively the certification authority "Centrum Kwalifikowane EuroCert" and the time-stamping authority "EuroCert QTSA".

Public keys to verify trust services:

a) key for signing certificates and CRL lists,
b) key for signing time stamps

are available as certificates of trust services providers issued by the minister in charge of ICT development or an entitled subject acting by virtue of art. 10.1 of the Trust Services Act.

In the field "certificate policies" (see 7.1.2) 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.

1.2 Document name and identification

The Regulation is available in an electronic form at: https://www.eurocert.pl/repozytorium. The Regulation has the following registered Object Identifier: 1.2.616.1.113791.1.2.

1.3 PKI participants

The public key infrastructure of the EuroCert is used to render the service of qualified trust services and it comprises the following elements:

a) qualified certification authority: Centrum Kwalifikowane EuroCert,

[1] https://www.ietf.org/rfc/rfc3647.txt

b) qualified time stamping authority: EuroCert QTSA,
c) registration authorities,
d) subscribers of certificates and time stamps,
e) relying parties.

1.3.1 Certification authorities

Certification authority – Centrum Kwalifikowane EuroCert issues certificates for end users (subscribers) and discloses information necessary for verifying the validity of certificates. The CA is supervised by the Ministry of Digital Affairs who entrusted the role of the root CA to the National Certification Centre (NCC). NCC 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 NCC's certificate to certificate of "Centrum Kwalifikowane EuroCert" issued by NCC and subscriber's certificate.

Tasks related to receiving applications for issuing certificates, issuing certificates and receiving applications for revocation or suspension of certificates are performed by registration authorities.

Certificates are issued by Centrum Kwalifikowane EuroCert according to the NCP+ policy set forth in point 5.3 of the ETSI EN 319 411-1.

Private keys of subscribers can be placed on the electronic card. In case of an electronic 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.

1.3.2 Time-stamping authority

The time stamping authority issues time stamps in line with the recommendations of ETSI EN 319 422. Each time stamp token contains a certificate policy identifier, according to which it was issued (its value is 1.2.616.1.113791.1.4) and it is certified exclusively with the use of a private key created especially for the time stamping service.

The time stamping authority acts on the basis of EuroCert entry onto the list of qualified providers of trust services and by virtue of the certificate issued by the minister in charge of ICT development or a designated body (NCC).

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 one-second accuracy.

The policy of EuroCert QTSA is in compliance with ETSI EN 319 411-2 and uses the qualified time stamp in the meaning of eIDAS regulation. The key of this authority is available on the TSL list and is defined as a qualified service.

1.3.3 Registration authorities

Registration authorities perform services for subscribers. They may be individuals, companies and organisational units having no legal personality, upon signing an applicable agreement with EuroCert. Registration authorities supervised by EuroCert cannot accredit other registration authorities.

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

a) accepting certificate application,
b) confirming identity of subscribers and their eligibility to receive certificates,
c) signing agreements with subscribers,
d) creating certification requests which are submitted to certification authority,
e) delivering certificates to subscribers.

Detailed scope of duties of registration authorities is set out by the agreement between EuroCert and a certain registration authority.

A list of current authorised registration authorities is available at https://sklep.eurocert.pl/pl/i/Mapa-Punktow-Partnerskich/14.

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.

An organization seeking to obtain a certificate for electronic seal can do so via its authorised representatives.

A subscriber of a qualified time stamp 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.)

1.3.5 Relying parties

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

The relying party is liable for verifying the current status of the subscriber’s certificate (see 4.5.2). This decision must be made by the relying party each time when the certificate is to be used for verifying an electronic signature or seal. Information included in a qualified certificate (for instance object identifiers of the certificate policy) should be used by the relying party for the assessment whether the certificate was used in line with its declared designation.

1.3.6 Other participants

Not defined.

1.4 Certificate usage

Certificates for electronic signature are used to verify qualified electronic signatures and they are designated to ensure non-repudiation.

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

Qualified electronic seal enjoys the presumption of the integrity of all data and of correctness of the origin of that data to which the qualified seal is linked.

Tab.1. Types of certificates

Certificate type		Apply
Qualified certificates for electronic signature	personal	to verify qualified electronic signatures created by individuals; the certificate contains only the individual's personal data (at least: the country name, the subscriber's name and surname and a serial number.
	professional	to verify qualified electronic signatures created by individuals; apart from the individual's data the certificate contains the date of an organization represented by the subscriber; the certificate contains at least: the country name, the subscriber's name and surname, a serial number, own full official name of the represented entity.
Qualified certificates for electronic seal	to verify qualified electronic seals. Certificates for electronic seal ensure a high level of credibility of the identity of a certificate's subject. They are issued only for legal entities and organizational units not having legal personality. Certificates should be used to create qualified electronic seals to ensure integrity and authenticity of the document being signed.	

1.4.1 Appropriate certificate uses

Private keys connected with certificates should be used for creating qualified electronic signatures (seals), ensuring the integrity of signed information and giving the information the feature of non-repudiation in the environment, when there is a risk of infringing information as the results of the infringement may be significant.

Certificates may be used in financial transactions or in transactions with a significant risk of fraud, also in events when a handwritten signature is usually applied.

Private keys related to qualified certificates may be processed exclusively in the equipment meeting the requirements 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 Regulation. List of qualified signature (seal) creation devices is published in the repository (see chapter 2).

1.4.2 Prohibited certificate uses

The certificates cannot be used contrary to their designation and without observing possible limitations in the usage of a certain certificate included in the certificate.

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

Certificates cannot be used for cyphering data or cryptographic keys (generally, in operations aiming at making information confidential).

Qualified certificates for electronic seal are not used to express the will of subjects who use them.

1.4.3 Uses of time stamps

Time stamps are used to certificate the date and time as well as integrity of data to which the date and time are linked.

1.5 Policy administration

Each amendment in the Regulation, except for those replacing obvious clerk or style errors, must be given a new version name and the management board of EuroCert Sp. z o.o must approve this amendment. 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 Regulation is published in the repository. Subscribers, relying parties and registration authorities are obliged to use only the valid Regulation.

1.5.1 Organization administering the document

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

1.5.2 Contact person

All correspondence regarding qualified trust services must be addressed to EuroCert:

EuroCert Sp. z o.o.
Centrum EUROCERT
ul. Puławska 474
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 amendments in the Regulation. 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 Regulation and not defined below should be interpreted in line with definitions included in the Trust Services Act and in the eIDAS Regulation.

Tab. 2. Terms and acronyms used in the Regulation

Term/acronym	Description
Certification authority	Centrum Kwalifikowane EuroCert.
Registration authority	an organisational unit acting on behalf of EuroCert Sp. z o.o. performing some functions related to providing certification services, described in this Regulation.
DN	DN – Distinguished Name identifier – an identifier of the PKI entity in line with the syntax defined for X.500 series norms.
OCSP	Online Certificate Status Protocol – a protocol and name of the PKI service used for informing about the status of certain certificates, inquired about by the customer (whether the certificate is valid of revoked).
CRL	Certificate Revocation List.
PDS	PKI Disclosure Statement.
PKI	Public Key Infrastructure. A public key infrastructure (PKI) is a system covering Keys Certification Centres, Registration authorities and end users, used for distributing public key certificates and for ensuring the possibility of their reliable verification.
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).
NCC	Root of the national PKI system, maintained by the National Bank of Poland, based on an authorisation of a minister in charge of digitalisation.
Private key	Data used for affixing an electronic signature.
Public key	Data used for verifying an electronic signature, usually distributed in the form of a certificate.
Trust Services Act	The Act on Trust Services and Electronic Identification of 5 September 2016 (Journal of laws item 1579).
eIDAS Regulation	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.
QSCD	QSCD - Qualified Signature Creation Device – a certified device allowing for its use for qualified issuing of an electronic signature/stamp, pursuant to eIDAS.
Personal Data Protection Act	The Personal Data Protection Act of 29 August 1997 (Journal of Laws of 2016 item 922).
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 subscribers, registration authorities, 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) the Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services,
b) EuroCert certificates,
c) PKI Disclosure Statement,
d) CRL lists,
e) a list of qualified devices for creating electronic signatures (seals),
f) contract templates, applications for issuing a certificate, order forms etc.

Information concerning qualified trust services rendered by EuroCert is published automatically in the repository (CRL lists) or upon acceptance by authorized parties (e.g. this Regulation, certificates of trust service providers and other documents).

2.3 Time or frequency of publication

The CRL is generated and published automatically, at least every 24 hours and within 1 hour from the demand to suspend or revoke a certificate, 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

This chapter presents the general principles of verifying the subscribers' identity which EuroCert applies while issuing, suspending and revoking certificates. The principles are to ensure that information submitted in a certificate application is correct and is linked to an existing natural person and that the applicant is this natural person who has been stated in the application.

3.1 Naming

Certificates issued by EuroCert are compliant with X.509. The names of subscribers and certificate issuers placed on certificates are compliant with distinguished names (DN), created in accordance with ITU series X.500 recommendations and ETSI EN 319 412.

3.1.1 Types of names

A distinguished name is created basing on the data stated in the certificate application using the subset of the following attributes (Tab. 3 and Tab. 4).

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

Fields	Values
C*	a two-letter international acronym for a state (PL for Poland)
G*	the subscriber's first name(s)
S*	the subscriber's surname plus possibly surname at birth
CN	common name
SERIAL NUMBER*	The subscriber's 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 EN 319 412-1. When a subscriber is identified by their PESEL number, serial number should be in the following format: „PNOPL-XXXXXXXXXXX" in accordance with the ETSI EN 319 412-1 norm (point 5)
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
ST	province
L	City/ locality
A	Address

*mandatory field

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

Fields	Values
C*	a two-letter international acronym for a state (PL for Poland)
CN	common name
ORGANIZATION IDENTIFIER*	Organization identifier: tax identification number, register number in the company register or local identifier, recognisable on the European Union's level according to point 5.1.4 ETSI EN 319 412-1
O*	Official name of the subscriber
OU	Name of an organizational unit
ST	Province
L	City/ locality
A	Address

*mandatory field

Address (province, city name, postal address) of the entity the name of which is placed in the Organisation ("O") attribute comply with an entry in the relevant register (log), list, articles of association or other document of this type relevant for the type of an entity and they should have the form used on posted letters.

The subscriber can have any number of certificates containing the same distinguishing name.

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 3.1.1.

3.1.3 Anonymity or pseudonymity of subscribers

EuroCert does not issue anonymous certificates 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 3.1.1.

3.1.4 Rules for interpreting various name forms

The interpretation of names of fields included by EuroCert in certificates issued by it complies with ETSI EN 319 412 (Part: 1,2,3,5). While creating and interpreting distinguished names the recommendations set forth in 3.1.1. are applied.

3.1.5 Uniqueness of names

EuroCert guarantees the uniqueness of the subscriber's DN in domain of each EuroCert qualified trust service. Each issued certificate has its own unique serial number (product key) given by the certification authority. In connection with the DN identifier of a subscriber, it guarantees an explicit identification of the subscriber.

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

A subscriber identity verification procedure consists in certification of the data which identifies the subscriber and verification of their authorization to receive a certificate which is carried out by the operator of a registration authority or registration officer

EuroCert and subordinate registration authorities confirm the identity and other attributes of the natural person or legal entity applying for qualified certificate with a valid identity card, passport or entry in the business activity register in accordance with the provisions of the art. 24 (c) of the eIDAS Regulation.

In the case when the entity already possesses the qualified certificates issued by any trust service provider and has been already subjected to identity verification, further identity verification may be based on previous documents and data. This data may be electronically signed acc. with art. 24 (c) of the eIDAS Regulation.

3.2.1 Method to prove possession of private key

Certificates are issued exclusively for a key pair generated by EuroCert.

3.2.2 Authentication of organization identity

The registration officer and the registration authority operator are obliged to verify subscriber’s authorizations always in situation, when a subscriber submits the certificate application for:

a) qualified certificate for electronic signature, containing an indication of whether subscriber acts on behalf of another entity, whose data are included in the application,
b) qualified certificate for electronic seal.

Authentication is a part of procedures of processing of customers’ requests for the issuance of the certificate for electronic signature to the natural person representing another person (natural or legal) or certificate for electronic seal. In this case the issued certificate should be interpreted as confirmation of the rights of the natural person to use a private key on behalf of another person.

The process of checking the authorizations includes authentication of authorized person identity. The process of checking the authorizations consists in verification of submitted authorization on the basis of:

a) submitted documents (e.g. letter of attorney),
b) checking the signature created on these documents by entitled person,
c) checking of compliance of information in certificate application with data included in the submitted documents.

3.2.3 Authentication of individual identity

Verification of the individuals’ identity is performed by a person authorized by EuroCert in a registration authority based on a valid identity card or a passport and additionally – when the certificate, together with personal data of an individual is to contain data regarding a legal entity or other organisational unit – based on the following documents:

a) a power of attorney or other document authorising for acting on behalf of someone else, specifying clearly the scope of authorisation to act on somebody else's behalf,
b) relevant authorisation issued by a certain organisation for placing the organisation's date in the certificate,
c) current copy of an entry in the National Court Register or the copy of an entry in the Central Electronic Register and Information on Economic Activity,
d) other documents that are necessary for verifying the data contained in the application for the certificate, e.g. a certificate on the place of employment, certification of the right to exercise a given profession.

An individual verifying the identity of the individual on behalf of EuroCert certifies the performance of the verification by creating handwritten signature and providing their personal identification number (PESEL) in the written declaration on verifying the identity. Then this individual signs an agreement with the subscriber on behalf of EuroCert, and the agreement contains the following subscriber's personal data:

a) first name,
b) surname,
c) date and place of birth,
d) personal identity number (e.g. PESEL) or tax identification number (TIN),
e) series and number and type of the identity document and description of the body issuing this document,
f) e-mail address and phone number.

In the event of certifying the identity through a notary, the applicant signs the agreement with EuroCert unilaterally in the presence of a notary, and the agreement upon its submitting to EuroCert is signed by the registration officer and sent to the address indicated by the applicant.

Before issuing the certificate, the applicant is obliged to confirm the knowledge of this Regulation, PKI Disclosure Statement (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) by way of signing the agreement for trust services with a handwritten signature. Signing the agreement 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 the cryptographic card with the private key in person, from the individual verifying their data and granting PIN and PUK codes securing access to the card,
d) while applying for the certificate, the subscriber is aware of what information is contained in the certificate and agrees for making it public.

3.2.4 Non-verified subscriber information

EuroCert verifies all the data which shall be placed in the certificate (see 3.1.1).

3.2.5 Validation of authority

Before delivering the certificate for electronic signature (seal) to a subscriber, EuroCert verifies the identity of the subscriber (a subscriber's representatives) based on the identity document presented by her/his.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Re-key entails issuing a new pair of keys without modification of the certificate content certificate. It 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 Regulation.

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 certifying 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.

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 revocation request

Revocation or suspension of a certificate may be requested by:

a) the subscriber (in case of a certificate for electronic seal – natural person representing the subscriber),
b) an organisation represented by the subscriber (natural person) whose data was contained in the certificate,
c) a supervisory body,
d) EuroCert,
e) other person if so stipulated in the contract of rendering trust services or other EuroCert's obligations.

A certificate may be revoked or suspended in the following manner:

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 password for invalidating 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 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.

4 Certificate life-cycle operational requirements

The procedure of obtaining a certificate is initiated with submission of an application at a registration authority, 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

Certificate application is submitted in person in hard copy (with a handwritten signature) or by e-mail (signed with the qualified electronic signature or qualified electronic seal) in the registration authority. The application is always signed by the subscriber for whom the certificate is to be issued. Organisations wishing to obtain certificates for their employees may do so through their authorised representatives. On the other hand, an individual subscriber applies for a certificate on its own behalf.

4.1.1 Who can submit a certificate application

Natural persons may apply for issuing the certificate (on their own behalf) as well as legal persons and institutions without legal personality via authorized representatives.

4.1.2 Enrollment process and responsibilities

Certificate application shall be submitted by an applicant in the registration authority in person or via an electronic form (in which case it is necessary to authenticate the applicant by a notary or the registration authority operator). An application for renewal of the certificate which has not expired shall be submitted exclusively via an electronic form.

4.2 Certificate application processing

A certificate application is subject to mandatory authentication by the registration authority 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 by registration authorities as set out in chapter 3.

4.2.2 Approval or rejection of certificate applications

EuroCert may reject the certificate application if:

1) Identifier (DN) of the subscriber applying for the certificate is identical as the identifier 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 (in case of certificates for electronic seals),
5) 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 registration authority, unless the agreement entered into between EuroCert and the subscriber provides for a longer time limit.

4.3 Certificate issuance

Upon authentication of the identity of the subscriber, registration authority operator prepares a certification request token and submits to the certification authority in order to generate a certificate by the registration officer. EuroCert electronically certifies the public key along with the subscriber's data.

4.3.1 CA actions during certificate issuance

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 on an qualified electronic signature/seal creation device.

The registration authority 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 or via an authorised person in case of qualified certificates for electronic seal.

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.

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 registration authority immediately upon issuing the certificate by the certification authority, and before saving it on any carrier. The registration authority 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

The certificate is accepted by a subscriber by confirming the receipt of the certificate in person from the same operator of the registration authority who previously verified the identity of the subscriber. A document confirming this with a handwritten signature of the subscriber is archived by EuroCert. The second copy of the document is handed over to the subscriber.

With regard to certificates issued remotely (see 4.7) the certificate's acceptance by the subscriber takes place by downloading the certificate from EuroCert's system and installing it on a safe device.

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 Regulation 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).

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 Regulation and indicated in the certificate (in the “keyUsage” field),

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 Regulation and indicated in the certificate (in the “keyUsage” field),

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 certificate of the certification authority that issued the subscriber’s certificate,

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 (which is still valid) 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 certification authority) contained in the certificate (see 4.7).

4.7 Certificate re-key

Renewal of a certificate as specified in 3.3 is an integral part of a new key pair generation. 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.

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 valid certificate issued by the qualified trust service provider.

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 invalid.

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 may be revoked in the following circumstances:

a) information contained in the certificate became invalid or is false,
b) the private key of a subscriber related to a public key in a certificate was compromised or there is a justified suspicion that this fact could take place (for instance as a result of the loss of a private key, unauthorised access to a private key, the loss of a private key, a theft of a private key),
c) 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.),
d) EuroCert ceases to perform trust services and to continue providing services of providing information about the certificate's status,
e) a proof exists that the certificate was used contrary to its purpose,
f) the certificate was issued in conflict with this Regulation,
g) 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 following entities may demand revoking the certificate:

a) the subscriber who is the subject of the revoked certificate,
b) the entitled representatives of subject represented by the subscriber, whose data are contained in the certificate,
c) the subscriber's representative (in case of certificates for electronic seals),
d) EuroCert, as a result of gross breach by the subscriber of this Regulation, contract, PKI disclosure statement, and in particular responsibilities set out in 4.5.1,
e) a Supervisory Body,

f) the registration authority operator, the registration officer who may submit such application on behalf of the subscriber or at their own initiative, if they hold information justifying revoking the certificate.

EuroCert is particularly vigilant while reviewing the revocation request when the subscriber is not its author and they approve of only the certificates listed in 4.9.1 and if the risk of losing trust to the questioned certificate exceeds irregularities and potential losses of the subscriber, resulting from its revoking.

If the party applying for revoking the certificate is not the subject of the certificate (its subscriber), the certification authority:

- verifies whether certain applicant may demand revoking a certificate,
- send a notification to the subscriber about revoking or the intention to revoke its certificate.

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. If there are premises for revoking the certificate but the registration officer is unable to explain all doubts regarding the revoking of the certificate within one hour from receiving a complete application, the certificate is suspended.

The information about certificate revocation is published on the CRL within one hour 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.

The revoked certificate and complementary private key stored on the electronic identification card should be irrevocably removed from this carrier. This operation is performed by the card's owner – an individual or the representative acting under the authorisation from a legal person.

4.9.4 Revocation request grace period

EuroCert guarantees revoking a certificate within one hour from the receipt of a complete request.

4.9.5 Time within which CA must process the revocation request

The maximum admissible time limit for processing an application for revoking a certificate amounts to 1 hour from the moment of submitting a complete application.

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.

4.9.7 CRL issuance frequency

CRLs are published at least every 24 hours and are automatically published in the repository. In the case of revoking or suspending a certificate, a new CRL is published immediately upon processing the application for revoking the certificate (see 4.9.5).

4.9.8 Maximum latency for CRLs

CRLs are published immediately upon their creation.

4.9.9 On-line revocation/status checking availability

EuroCert QOCSP provides access to the online verification service for certificates. This type of service is performed on the basis of the OCSP protocol (On-line Certificate Status Protocol), presented in RFC 6960.The OCSP service makes it possible to obtain more updated information more frequently about the certificate status as compared to the CRL list.

The OCSP protocol operates on the basis of a question – answer (Q&A) model. Each question is answered by the qualified authority with the following standard, certified information on the certificate status:

- Good – means a positive answer to the question, which should be clearly interpreted as a certification that the certificate is valid,
- Revoked – means that the certificate was revoked,
- Unknown – means that the verified certificate has not been issued by the qualified certification authority.

The certificate’s status is given in actual time (i.e. immediately upon revoking a certificate). The information about the certificate status is publicly available. The service address is given in an issued certificate (see 7.1.2).

The certificate status is retrieved from the certification authority’s server and is available not later than 60 seconds after revocation of a given certificate.

The CRL lists issued by EuroCert and responses of the QOCSP are electronically signed by authorities issuing them owing to which EuroCert ensures their integrity and authenticity.

4.9.10 On-line revocation checking requirements

A relying party is not obligated to verify certificate status on-line on the basis of mechanisms and services laid down in 4.9.9. Notwithstanding above, it is recommended to employ OCSP service when the risk of forgery of the electronic documents utilizing electronic signature is high or if it is required by other regulations concerning such situations.

4.9.11 Other forms of revocation advertisements available

In the case of security breach (disclosure) of a private key of the certification authority functioning within EuroCert, the information about this fact is published immediately on CRLs and it is obligatory to send it by e-mail to all subscribers of the certification authority. 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 certification authority'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 Circumstances for suspension

A certificate is suspended immediately upon having a justified suspicion that there are premises for revoking the certificate indicated in 4.9.1, in particular at the request submitted by the subscriber.

Suspending a certificate may take place in the following circumstances:

a) information contained in the electronic or hard copy application for revoking the certificate cause justified suspicions,
b) the application for revoking a certificate was submitted by phone or electronically and the identity of the applicant cannot be confirmed within one hour from the moment of the application receipt but the submitted application's merits cannot be questioned either,
c) 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 Regulation; a certificate may be suspended until the moment the certification authority finds the basis for revoking the certificate, but no longer than for 7 days,
d) other circumstances that require an explanation by the subscriber or by the applicant.

The application for suspending the certificate contains similar information as in the case of the application for revoking a certificate.

4.9.14 Who can request suspension

A certificate is suspended at the initiative of employees authorized by EuroCert in the event of justified suspicion that there are premises for revoking the certificate indicated in 4.9.1, in particular at the request submitted by the subscriber (see 3.4).

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.

The suspended certificate can be reinstated exclusively at the initiative of EuroCert. 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).

4.10 Time stamping

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,
- electronic timestamp authority private keys are generated and stored inside hardware security module complying with FIPS 140-2 Level 3 requirements,
- the electronic timestamp authority EuroCert QTSA owns private key used for creating electronic confirmations of electronic timestamp tokens.

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 which has been issued on the basis of this agreement. In addition, the subscriber may also terminate the agreement at any time, by invalidating the certificate. Termination of the Agreement itself does not result in revoking or suspending the certificates issued under this agreement.

4.12 Key escrow and recovery

EuroCert does not perform services of depositing and storing private keys of subscribers. Neither does it entrust its private key to other entities.

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

Premises in which personal data are processed connected to issuing, suspending or revoking certificates and in which generating, suspending and revoking certificates takes place, are protected by security guards in line with the requirements for qualified trust service providers and under the Personal Data Protection Act.

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 safe cryptographic module 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 certain roles,
d) number of individuals necessary for the performance of certain 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 5. The presented division of roles complies with the requirements of ETSI EN 319 401

Tab. 5. 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 regulation 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	installing, configuring and managing systems and information networks used while performing certification 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 suspending, revoking or reinstating certificates and creating new CRLs.
System auditor	conducting planned and ad hoc audits in line with existing regulations

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 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 Regulation, the Trust Services 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 Registration authorities acting on its behalf,
f) they became familiar with internal EuroCert procedures,
g) they were informed about the criminal liability within the scope related to providing certification services.

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

Trusted personnel of EuroCert and registration authorities operators must participates in a range of trainings before receiving the authorisation to perform their positions:

- the rules regulated by documentation and the effective regulations, assigned position of a certain person,
- personal data protection and information protection,
- the public key infrastructure,
- verification of identity based on documents confirming identity,
- the rules and mechanisms of protection used in the Certification authority and Registration authorities,
- the certification authority's computer system software,
- the scope of obligations that will be performed by them,
- procedures implemented after failures or disasters of the Certification authority's system,

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 in providing services by EuroCert were implemented, as well as in the functioning of EuroCert or registration authorities, in the systems, this Regulation or other essential internal regulations.

5.3.5 Job rotation frequency and sequence

This Regulation 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 electronic signature (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 registration authorities access to the following documents:

- the Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services,
- template contracts and applications forms,
- necessary excerpts from documentation (relevant for the performed role), including emergency procedures,
- the scope of obligations and rights resulting from the performed position.

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, generating CRLs, acceptance of a request for a time-stamp,
b) activities related with servicing customers and subscribers: accepting and signing 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 Regulation (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

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, from a subscriber or forwarded to the subscriber,
- 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,
- certificate policies,
- documents issued by the registration authority system operator, a notary or other persons confirming the identity of the applicant on behalf of EuroCert,
- demands for revoking a certificate,
- other hard copy documents related to performing certification services,
- other documents subject to archiving as set out individually in other subchapters of this regulation.

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 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 registration authority 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, 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 and verified statuses of certificates.

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. 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 NCC and placing on TSL,
- the receipt of certificate from NCC and issuing by NCC a new TSL.

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 Regulation.

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) certification authorities, back-up keys;
c) cryptographic cards' copies with divided secrets and operator's cards;
d) carriers with keys certification system software;
e) regulations 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 Regulation,
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.

5.7.4 Business continuity capabilities after a disaster

EuroCert has implemented plans ensuring the security and continuity in providing critical services of the qualified 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 qualified 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 qualified 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 item 2 of the Trust Services Act).

The termination plan for a qualified trust service providers, referred to in Article 24 Clause 2 letter and eIDAS Regulation 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 qualified 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 EuroCert Qualified Centre are uses for signing certificates and CRLs. The RSA algorithm combined with SHA-1/SHA-512 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 trust services providing offices, operating within EuroCert are generated using a separated, credible workstation and a cryptographic module operating in unison with this station, holding the certificate of Common Criteria EAL4+ level or higher and FIPS PUB 140-2 for a 3 level or higher.. Generating keys and operations related with the use of a private key take place exclusively in the cryptographic module.

Registration officers keys are generated independently by themselves on the cryptographic card under the supervision of the Security officer. They are used for signing subscriber's demands for keys certification.

Subscribers' keys are generated exclusively by EuroCert in the registration authority on the cryptographic card meeting the requirements of SSCD/QSCD, in the subscriber's presence and followed by immediate transfer to this subscriber.

6.1.2 Private key delivery to subscriber

The subscriber's keys are generated by the certification authority on a cryptographic card. They can be supplied to the subscriber together with information allowing for activating a private key for immediate change of data allowing for activating the private key in person, by courier or remotely. It is necessary to change PINs by the subscriber before commencing the certificate exploitation period.

Data necessary to activate the card (PUK/PIN) is made available to subscribers irrespectively of issued certificates.

EuroCert enables subscribers to use the keys exclusively in listed certified devices for qualified signatures and qualified seals notified in compliance with the art. 30(2), 39(2) and 39(3) of the eIDAS Regulation.

Subscribers who want to renew the valid qualified certificate, held on a cryptographic card issued by EuroCert may generate remotely another pair of keys. EuroCert supplies to its subscribers a dedicated application which creates keys directly on the cryptographic card of the subscriber.

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

Not applicable.

6.1.4 CA public key delivery to relying parties

Public keys of the Certification authority issuing certificates to end users are distributed only in the form of certificates of trust services providers in line with recommendation ITU-T X.509 v.3 issued by the National certification authority.

Public keys of the certification authority are distributed by publishing in the publicly available repository (see chapter 2) and listed on the TSL.

6.1.5 Key sizes

All authorities operating in the domain of EuroCert qualified trust services use keys of 2048 and 4096 bit length with SHA-2 hash function.

All certificates issued to end users within the framework of the qualified certification authority have the key length of 2048 bits/3072 bits and SHA-2 hash function.

6.1.6 Public key parameters generation and quality checking

Public key generating parameters meet the requirements specified in the ETSI EN 319 401 i 319 411-2 norms.

6.1.7 Key usage purposes

The 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.

Qualified certificates issued to subscribers may be used for signing. 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 tokens (digitalSignature and nonRepudiation).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Each subscriber, as well as qualified authority operator store their private key in a reliable system to prevent from its loss, disclosure, modification or unauthorised use. Certification authority which generates a key pair on behalf of the subscriber is bound to deliver it in a safe manner and caution the subscriber about the security principles of private key protection (see 6.1.2).

6.2.1 Cryptographic module standards and controls

Private keys of subscribers related to certificates are processed exclusively in qualified signature/seal creation device, that fulfil the requirements of the FIPS 140 norm and Common Criteria EAL4+ .

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 6.

Tab. 6. Private key division scheme

Certification authority	Total number of secrets [n]	Number of secrets necessary for using the key [m]
EuroCert Qualified Centre	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

No private key of EuroCert is transferred (or forwarded) to other entities. EuroCert does not perform services of depositing and storing private keys of subscribers.

6.2.4 Private key backup

Private keys of a subscriber related to certificates used for verifying electronic signatures/seals cannot be subject to back up copies procedures. 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).

6.2.5 Private key archival

Private keys of Certification authorities used for performing electronic certification 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.

Private keys of a subscriber related to certificates used for verifying electronic signatures/seals private keys of registration officers used for signing certification requests cannot be subject to archiving procedures.

6.2.6 Private key transfer into or from a cryptographic module

Introducing a private key to the HSM takes place in the following situations:

a) commissioning the certification authority, during the system starting,
b) recovery of the Certification authority's key in a backup centre,
c) exchanging the HSM.

Uploading the key to the module is performed by the holders of co-shared secrets. It is necessary for the number of secrets be available for uploading the key, as described in 6.2.2. Uploading takes place within the closed safety environment. A private key is made of elements. The secret key's fragments are given consecutively, cyphered files are uploaded to the module's memory, which is followed by their deciphering. The private key is ready for use. Uploading the key to the module is recorded in the events register.

Introducing a private key to the HSM is a critical operation. Due to this fact, during its performance the measures and procedures are used to prevent disclosing the key, its modification or provisions.

6.2.7 Private key storage on HSM

Upon deciphering and uploading a private key to the HSM memory, it is protected by the equipment. It is impossible to read the value of a private key from the HSM, the key never leaves it. Operations that require the use of a private key are used in the HSM.

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 (the removal of the card from HSM) or until the HSM is switched off.

Subscribers private keys are activated 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 electronic card or other qualified device used for electronic signature/seal.

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 takes place respectively by logical removal of the key from the carrier (a cryptographic card, a HSM device, etc.), the physical destruction of a key carrier (e.g. from a cryptographic card).

The destruction of the private key of the Certification authorities means a physical destruction of cryptographic cards, on which shared secrets are stores or their safe removal from a carrier (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

The following chapter describes aspects related with the certificates validity periods and archiving the certificates and keys of private subscribers and certification authorities.

6.3.1 Public key archival

EuroCert implements a long term archiving process for certificate authorities' public keys in the form of certificates, subject to the principles applicable to other archived data (see 5.5).

Archiving public keys aims at the possibility of verifying electronic signatures/time stamps upon the expiry of the validity period of certification authority's certificate and completing its operations.

Certification authority stores public keys of these subscribers whom it provided with the keys in a form of certificates.

6.3.2 Certificate operational periods and key pair usage periods

Validity period for private keys and certificates of subscribers does not exceed 5 years and it is set out in the validity field of each certificate. "Valid from" date for each certificate cannot be earlier than its date of issue.

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

Providing PIN and PUK codes by a subscriber in order to secure an electronic card with a pair of keys and a certificate should take place using the application for card management delivered by EuroCert together with the card.

Shared secrets used to protect private keys of all certification authorities rendering 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 for the card. 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 cryptographic card. Activation data which is saved is never stored together with the cryptographic card.

6.4.3 Other aspects of activation data

Copies of passwords for securing access to a cryptographic card are not stored at EuroCert. EuroCert does not hold any codes or date allowing for restoring PIN and PUK codes securing access to the card, 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.

Certification authority regularly performs vulnerability assessments and penetration tests of the IT system in place not less frequently than every 6 months. Test results are not published.

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 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 Regulation does not impose the life cycle of applied securities. Securities are exchanged in the event if it is necessary to apply other securities to the ones used at the moment, following changes in legal regulations or if they are technologically out of date and they do not correspond to current norms and standards.

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 (see 1.3.2 and 4.10).

7 Certificate and CRL profiles

Profiles of certificates and CRLs are issued in line with recommendations of ITU-T X.509 v3 and ETSI EN 319 412 (Parts 1,2,3,5).

7.1 Certificate profile

Certificates issued by EuroCert in line with X.509 v3 norm are a sequence of value of basic fields and extensions. EuroCert operates basic fields of the certificate described in Table 7.

Tab. 7. Profile of certificate's basic fields

Field Name	Description		Value
Version	certificate complies with X.509 standard, version 3		V3
SerialNumber	Certificate number, explicit 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 EN 319 412 (Parts 1,2,3,5).*	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 8.

Tab. 8. Certificate extensions

Extension name	Critical?	Description	Value
AuthorityKeyIdentifier	NO	public key identifier of the issuer used for verifying the issued certificate	
SubjectKeyIdentifier	NO	Certificate identifier containing the hash public key contained in the certificate	
KeyUsage	YES	specifies the scope of used public key used by the subscriber. With regard to qualified certificates limited to non-repudiation.	nonRepudiation (a key for non-repudiation function)
CertificatePolicies	NO	indicating certificate policies with the certificate issued in line with it	Certificate Policy identifier compliant with 7.1.6
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	OCSP URL	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	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).
qcPDS	NO	Information on EuroCert services	URL to the document describing the basic conditions for performing trust services within the scope of issuing certificates (PDS – PKI Disclosure Statements); OID: {0.4.0.1862.1.5}

7.1.3 Algorithm object identifiers

EuroCert seals the certificates with RSA (4096 bit) algorithm and SHA-256 hash function. Subscribers' certificates are issued for keys of 2048/3072 bit length and SHA-256 hash function.

7.1.4 Name forms

See 3.1.1 and Tab 7 in 7.1.

7.1.5 Name constraints

See 7.1.4.

7.1.6 Certificate policy object identifier

Policy identifier for qualified certificate for electronic signatures is: 1.2.616.1.113791.1.2.2.
Policy identifier for qualified certificates for electronic seals is: 1.2.616.1.113791.1.2.3.

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 set of fields with their meaning presented below in Table 9.

Tab. 9. 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	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) and sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer CRL's issuer identifier, compliant with the identifier set out in the certificate's profile	See table 7 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 9), containing the code for the reason of revoking a certificate.

7.3 OCSP profile

Certificate status token profile is described in internal documents held by EuroCert.

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 Regulation and procedures and processes described in EuroCert's documentation (including this regulation).

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 Regulation (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 Regulation.

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 Regulation 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.

9.1.3 Revocation or status information access fees

EuroCert does not collect fees for revoking 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 Regulation.

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 Regulation 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 Regulation does not set out any requirements in this regard.

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

This Regulation 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 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 (General Data Protection Regulation).

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 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 (General Data Protection Regulation).

9.4.2 Information treated as private

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

a) This Regulation,
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 Article 7 (4) 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 Regulation 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 EuroCert Qualified Centre 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 Regulation,

b) acts in line with the provisions of law, in particular it does not infringe the provisions of the *eIDAS Regulation 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 EN 319 412-1,
- ETSI EN 319 412-2,
- ETSI EN 319 412-3
- ETSI EN 319 412-5;

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 Personal Data Protection Act of 29 August 1997 as amended and with application documents for this Act,

i) does not copy or store private keys of its customers, used for affixing electronic signatures,

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 registration authority 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 registration authority's operators,
6) refraining from the use of keys of private operators for other purposes than the ones specified in the Regulation,
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 Regulation 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.

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 Regulation indicates its validity date which is also the expiry date of the current Regulation. At the same time the previous Regulation loses its “valid” status.

9.10.3 Effect of termination and survival

Subscribers observe only the valid Regulation.

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 Regulation 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 Regulation 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 Regulations and in the applicable provisions of law. In order to interpret the terms included in the Regulation, they must be considered in line with eIDAS Regulation 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 Regulation,
b) The Act on Trust Services and Electronic Identification of 5 September 2016,
c) The Personal Data Protection Act of 29 August 1997,
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 Regulation 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 Regulation, the agreement prevails over the Regulation.

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 Regulation.

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 Regulation 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

This Regulation shall, from approval date, replace the following regulations:

a) Certification Practice Statement for Qualified Trust Services,
b) Certificate Policy for Qualified Certificates,
c) Certificate Policy for Qualified Time Stamps.

Document history

Modification history			
Approval date	Valid from	Version	Amendments
16.07.2018	02.10.2018	1	Creation of the document. This document covers the following previous documents: a) Certification policy statement for qualified trust services v. 2.0, b) The Certificate policy for EuroCert qualified certificates v. 3.0, c) Policy for EuroCert qualified time-stamps v. 1.0.