EuroCert Sp. z o.o.
Centrum EUROCERT

# The Certificate policy
for EuroCert qualified certificates

Version 3.0
Date: 15 November 2017
Status: invalid

EuroCert Sp. z o.o.
“Centrum EUROCERT”
ul. Puławska 474
02-884 Warsaw
https://eurocert.pl

TABEL OF CONTENTS

1 Introduction

Certificate policy for EuroCert qualified certificates, hereinafter: the "Policy", specifies the rules applied by the organisational unit of EuroCert Sp. z o.o. acting under the name "Centrum EuroCert" (hereinafter: "EuroCert") during the performance of certification services that involve issuing certificates used for verifying qualified electronic signatures, revoking or suspending certificates and verifying certificates' status on-line.

EuroCert acts in line with the laws applicable in the Republic of Poland, with the principles applicable to qualified providers of trust services, set out in the eIDAS Regulation, the Trust Services Act, 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 and in line with this Policy.

EuroCert is a qualified trust service provider performing qualified certification services, entered in the register of qualified provider of trust services under number 13 pursuant to the decision of the Ministry of Economy No 1/10573-13/13 dated 23 December 2013.

The Policy applies for the Certification Authority Centrum Kwalifikowane EuroCert, after updating the EuroCert's certificate dated 14.02.2017 performed in line with Article 10 Paragraph 1 items 1 and 2 in connection with Article 4 Paragraph 1 item 2 of the Trust Services Act. The previous EuroCert's certificate will be used only in order to create and publish CRLs until 15.01.2019.

The Certification policy statement is closely related to the Policy which is defined as the declaration of procedures applied by the CA in the process of issuing certificates and performing additional certification services.

The document's structure was created based on recommendations RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework[1]".

1.1 Overview

The Policy describes the scope of business of EuroCert and registration authorities, subscribers and relying parties related to it. The policy defines also parties participating in the process of performing qualified certification services by EuroCert, their obligations and responsibility, types of certificates, procedures of subscribers' identity verification applied during issuing certificates and certificate application areas.

The rules presented in this document should shape the activities of the entities and services providers using certificates issued by EuroCert.

1.2 Document name and identification

The Policy is assigned its own name and an Object Identifier – OID, presented in Tab. 1.

Tab.1. Document card

Own name	Certificate policy for EuroCert qualified certificates
Owner	EuroCert Sp. z o.o.
Version	3.0
Status	invalid
Date of approval	15.11.2017

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

Approved by	Management Board of EuroCert Sp. z o.o.
Valid from	20.11.2017
Object Identifier – OID	1.2.616.1.113791.1.2
Expiry date	01.10.2018

All versions of the Policy are available in electronic form at: https://www.eurocert.pl/repozytorium.

Certificates issued by EuroCert contains certificate policy identifiers, which enable relying parties to define if certificate usage is correct (regarding restrictions of the keyUsage and certificatePolicies: see § 1.3.1 and § 7.1.2). Certificate policy identifiers, published in the certificate, are described in § 1.3.1 and 7.1.2.

1.3 PKI participants

EuroCert public key infrastructure for qualified certificates comprises the following elements:

a) qualified CA: EuroCert Qualified Centre,
b) registration authorities, notaries and other persons confirming subscribers' identity,
c) subscribers,
d) relying parties.

Recipients of certification services provided by EuroCert are obliged to read this document. A subscriber is obliged to read the Policy before signing an agreement for providing trust services while the relying party is obliged to read it before using any certificate issued in line with the Policy.

1.3.1 CA

EuroCert comprises one CA – EuroCert Qualified Centre that issues certificates for end users (subscribers) and discloses information necessary for verifying the validity of certificates issued by it. The authority 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 services of EuroCert. This means that each certification path developed by them should start with the NCC's certificate to certification for EuroCert Qualified Centre issued from NCC and the last: subscriber's certificate

EuroCert does not issue certificates for any subordinate certification authorities.

EuroCert Qualified Centre issues qualified certificates in line with certificate policies with identifiers specified in Table 2 below and in § 7.1.2.

Tab.2. Certificate policies identifiers included in certificates issued by EuroCert

Certificate Name	Certificate policy identifiers
Qualified certificate (RSA, SHA-1)	1.2.616.1.113791.1.2.1
Qualified certificate (RSA, SHA-2)	1.2.616.1.113791.1.2.2
Qualified certificate (ECDSA, SHA-2)	1.2.616.1.113791.1.2.3

Tasks related to accepting applications for issuing certificates are performed by registration authorities.

1.3.2 Registration authorities

While performing its tasks, EuroCert may act alone or through registration authorities. Registration authorities may be individuals, companies and organisational units having no legal personality, upon signing an applicable agreement for certification services with EuroCert. Registration authorities supervised by EuroCert cannot accredit these registration authorities nor accept applications for revoking/suspending a certificate.

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

a) accepting certificate application,
b) confirming identity,
c) signing agreements with subscribers,
d) creating certification requests,
e) generating subscribers' keys pairs,
f) delivering certificates to subscribers,
g) informing about qualified electronic signature including its effects,
h) the sale of sets affixing an electronic signature.

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

Registration authorities competences cannot include particularly the use of a private key used for generating certificates and CRLs.

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

1.3.3 Subscribers

Each individual may be a subscriber of a certificate issued within the Policy, if their distinguished name is included in the field "subject" of the certificate and if they do not issue any further certificates to other entities.

1.3.4 Relying parties

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

The relying party is liable for verifying the current status of the subscriber's signature (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. Information included in a qualified certificate (for instance identifiers and 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.

1.4 Certificate usage

Certificates of keys verifying signatures, issued by EuroCert in line with the Policy are qualified certificates for electronic signatures within the meaning of eIDAS Regulation. They ensure very high level of identity reliability for the subject of the certificate.

Private keys connected with certificates should be used for creating qualified electronic signatures, 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.

Qualified electronic signatures issued by EuroCert have a legal effect identical to handwritten signatures.

Certificates may be used in financial transactions or in transactions with a significant risk of fraud, also in events when a handwritten signature is often 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 devices for creating electronic signatures is published in the repository (See Chapter 2).

Certificates issued under the Policy 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).

1.5 Policy administration

Each amendment in the Policy, 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 current version is approved and published.

A new version of the Policy is published in the repository (see Chapter 2). Subscribers and other interested persons (listed in § 1.3) are obliged to act accordingly to the current version of the Policy, based on which a certain certificate was issued.

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

In order to obtain further information, regarding services and business of EuroCert please contact:

EuroCert Sp. z o.o.
Centrum EUROCERT
ul. Puławska 474
02-884 Warsaw
+48 22 490 36 45
biuro@eurocert.pl

1.6 Definitions and acronyms

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

Tab. 3. Terms and acronyms used in the Policy

Term/acronym	Description
CA	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 policy.
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

All information important for subscribers, registration authorities, relying parties are published at:

https://eurocert.pl/repozytorium

These include following information:

a) current certificates issued by NCC for EuroCert used for verifying public key certificates,

b) current CRL,

c) current and previous versions of the Certification policy statement and the Certificate policy, together with the term of their validity,

d) description of suspending/revoking certificates,

e) a list of recommended applications and devices for creating and verifying electronic signatures,

f) a document specifying exact conditions for the use of a certificate (PKI Disclosure Statement) including but not limited to:

   - methods of resolving complaints and disputes;
   - the scope of limitations for the use of certificates that comply with the Policy;
   - legal consequences of creating qualified electronic signatures verified with the use of certificates complying with the Policy.

EuroCert does not publish subscribers' certificates.

The CRL is generated and published automatically, at least every 24 hours or within 1 hour from the demand to suspend or revoke a certificate, while other information each time upon their updating or amending.

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

3 Identification and authentication

This Chapter presents the principles of verifying the identity of potential subscribers while issuing, suspending or revoking certificates. The principles contain measures which must be undertaken in order to ascertain that information submitted by a potential subscriber in a certificate application is exact and credible at the moment of issuing the certificate.

3.1 Naming

The identification of each entity holding a certificate issued by EuroCert is performed based on the distinguished name (DN), included in the subject identification field (subject).The subscriber's DN profile and the certificate's issuer profile comply with ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part: 1,2,5 as well as with ITU series X.500 recommendations.

Subscriber's DN comprises some or all attributes included in the set of attributes presented in Table 4, while it must contain at least the country name, name(s), surname and serial number (SN).

Tab. 4. DN profile

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

SN	The subscriber's passport number, identity card number, personal identification number (e.g. PESEL), the subscriber's tax identification number (e.g. NIP) or local identifier of the subscriber, recognisable on the European Union's level
O	Organisation name where the subscriber is employed or which is represented by the subscriber
T (Title)	The subscriber's position name in a certain organisation
ST	province
L	City/ locality
A	Address

The subscriber may hold any number of certificates containing the same DN identifier.

With regard to a subscriber who uses PESEL number the Serial Number attribute has the format "PNOPL-XXXXXXXXXXX" in compliance with ETSI EN 319 412-2.

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

Address (province, city name, postal address) of the entity the name of which is placed in the "Organisation" 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'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

An individual's identity verification procedure is performed by the operator of a registration authority, the registration officer or by other person verifying the identity. This involves a detailed verification of documents and application submitted by the subscriber and optionally, on verifying the correctness of DN.

Confirming the data in the event when the potential subscriber does not hold a valid qualified certificate issued by the qualified provider of trust services takes place through their physical presence at the registration authority or a personal contact of the registration authority operator with a potential subscriber at any other location.

EuroCert and registration authorities supervised by it confirm the identity of a potential subscriber 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.

An individual verifying the identity of the potential subscriber on behalf of EuroCert certifies the performance of the verification by affixing 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 (PESEL),
e) series and number and type of the identity document and description of the body issuing an identity card or a passport, based on which the applicant's identity was confirmed.

EuroCert may also confirm the identity of an individual applying for the certificate through a notary. In this event, 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 the Certificate policy, the Certification policy statement, the terms and conditions for the use, scope and limits for the use of the certificate, legal consequences of affixing a qualified electronic signature by way of signing the agreement for certification 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 issuing the certificate, the subscriber is aware of what information is contained in the certificate and agrees for making it public.

3.3 Identification and authentication for re-key requests

If a party applying for issuing a qualified certificate holds a valid qualified certificate, the confirmation of their identity 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 of this person if information is the same as data included in the certificate related to the qualified electronic signature used for signing the data. Then, the subscriber's verification is performed based on information included in EuroCert databases and it involves verifying an electronic signature affixed under the application for the certificate immediately upon confirming the authenticity of the certificate bound to the signature (based on the certification path). However, this does not mean that it is impossible to apply the procedure described in § 3.2.

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

A certificate may be revoked:

a) at the subscriber's (an individual's) request,
b) at the request of the ordering party (an organisation represented by the subscriber) whose data was contained in the certificate,
c) at the request of the Ministry of Digital Affairs,
d) under the initiative of EuroCert.

A certificate may be revoked in the following manner:

a) in person at EuroCert, with its address given in § 1.5, during working hours, namely from 9.00 to 17.00, after verifying the identity of the party applying for revoking the certificate by the Registration officer in line with the procedure described in § 3.2,
b) by phone under hotline number 22 490 49 86, during the whole day, based on the password for invalidating the certificate agreed while issuing it, and personal data given while issuing the certificate,
c) by e-mail using an on-line form available at https://eurocert.pl/uniewaznienia/ or by sending an application for revoking (published in the repository) containing a valid qualified electronic signature submitted to: uniewaznienia@eurocert.pl.

In the last case the Registration Officer calls the phone number given in the application and verifies data from the certificate against the data in the application for revoking the certificate.

In the case of any irregularities in verified data, the certificate is suspended until the irregularities are explained or the application for revoking the certificate is rejected.

Identification and verification of a third party whose data is included in the certificate takes place in line with the procedure described in § 3.2. The application is admitted in this case on the basis of a successful verification of the right of a third party to apply for revoking the certificate.

The terms of suspending, reinstating and invalidating the certificate, in particular at the request of the ordering party or the subscriber are set out in § 4.9.

4 Certificate life-cycle operational requirements

This Chapter describes the method of performing the service of issuing qualified certificates, including, their modifying, revoking and suspending/ reactivating, issuing consecutive certificates.

4.1 Certificate application

An application for generating keys and a certificate is submitted in person in the registration authorities in hard copy (with a handwritten signature) or by e-mail (signed with the qualified electronic signature). The application is always signed by an individual for whom the certificate is to be issued. The applicant certifies in the application that all data submitted by him/her, necessary for issuing the certificate is true.

Before commencing the potential subscriber's identity verification procedure, an authorised representative of EuroCert in the registration authority, collects from him/her a written declaration on becoming familiar with the document describing the conditions for using the certificate, including, but not limited to:

a) methods of resolving complaints and disputes,

b) the scope of limitations for the use of certificates that comply with the Policy,
c) legal consequences of affixing electronic signatures verified by certificates complying with the Policy,
d) information on the system of voluntary registration of qualified trust service providers and their significance.

4.2 Certificate application processing

The registration authority verifies the identity of a potential subscriber in line with the provisions of § 3.2 or 3.3. This is followed by generating a certificate request, containing all data necessary for issuing the certificate in line with the certificate profile included in § 7.1.

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

EuroCert issues a certificate each time on the basis of a certification request, signed electronically by an authorised individual acting as the Registration Officer.

EuroCert issues certificates each time generating a new pair of keys.

The registration officer signs electronically a certification request described in § 4.2, followed by sending the signed certification request to the system generating certificates, launching the subscriber's certificate generating procedure on a qualified signature creation device, with the function of generating keys through a technical component, the construction of which:

a) disables copying the private key from a technical component on which the keys were generated or
b) disables copying the private key from a key module cooperating with the component on which the keys were generated or
c) enables recording in the key module or other technical component of a generated private key, or data used for opening the key while simultaneously it guarantees deleting the private key from the technical component not delivered to the subscriber in the manner disabling the reconstruction of the key.

The new certificate will contain, among other things, the public key and subscriber's data submitted by him in the certificate application.

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 CA, 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.

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 it from EuroCert's system.

Certificates are not published outside EuroCert internal network.

4.5 Key pair and certificate usage

This Chapter presents the obligations of subscribers and relying parties related to the use of pairs of keys and certificate.

4.5.1 Subscriber's obligations

The subscriber undertakes to:

a) observe the obligations under the agreement entered into with EuroCert,

b) submit to EuroCert only true and complete data within the scope required under the agreement or the certification request,

c) submit documents confirming that the data contained in the certificate application is true,

d) 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,

e) 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 values of fields 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,

f) immediately notify EuroCert about any circumstances causing the fact that the subscriber's private key was disclosed to third parties or as a result of which the subscriber may suspect that the private key could have been disclosed to third parties (e.g. the loss of a private key),

g) immediately commence the procedure of revoking the certificate, in the event of a breach of protection (or a suspected breach of protection) of their private key,

h) consider the loss or disclosure of the password (by sharing it with other unauthorised party) the same as the loss or disclosure of the private key (by sharing it with other unauthorised party),

i) 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,

j) do not create an electronic signature using the private key held by them, if the certificate connected to the private key is out of date (its validity date has expired), is revoked or suspended,

k) use private keys and certificates in line with their purpose set out in § 1.4 and indicated in the certificate (in the “keyUsage” and “CertificatePolicies” field, see § 7.1.2),

l) immediately notify EuroCert about the demand of revoking the certificate in the cases provided for in § 4.9.1.

4.5.2 Relying party’s obligations

Relying parties are obliged to:

a) rely only on the qualified certificates that are used in line with the declared purpose and can be used in the areas specified earlier by the relying party,

b) use public keys and certificates only upon verifying their status and validity of the certificate of the CA that issued the subscriber’s certificate,

c) verify the electronic signature using the CRL and the accurate certification path,

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 path are present in the set of acceptable identifiers specified by the verifying 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,

g) test types of a certificate and policy, according to which it was issued; in the event of any doubts whether a certain certificate was issued properly and whether it is used by an entity authorised to do so, the relying party is obliged to notify EuroCert about any doubts,

h) use certificates in accordance with their purpose set out in § 1.4 and indicated in the certificate (in “keyUsage” and “CertificatePolicies”field, see § 7.1.2).

4.6 Certificate renewal

It is not possible to renew a subscriber’s certificate. EuroCert issues certificates each time generating a new pair of keys. If the subscriber holds a valid qualified certificate, he/she can apply for issuing a new certificate for a new pair of keys under a simplified procedure (see § 4.7).

4.7 Certificate re-key

Issuing a consecutive certificate takes place always at the request of the subscriber who applies for an additional certificate of the type held for a new pair of keys within the validity term of the existing certificate.

Issuing a consecutive 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 of the subscriber affixed in the certificate application.

The procedure of issuing a consecutive certificate, upon revoking the previous one or issuing a consecutive certificate in the case when the certificate held by a subscriber has expired takes place in the analogical manner as the process of issuing the first certificate.

Issuing a consecutive certificate takes place always at the subscriber's initiative. The subscriber may at any time apply for issuing a new certificate, for instance when the existing certificate expires.

Prior to issuing a consecutive certificate, 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.

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 first certificate. The current certificate – if data contained therein became invalid and contain false information about the subscriber – is invalid.

Certificate modification may apply only to a certificate before its expiry date which was not revoked.

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).

4.9 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 a day.

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

4.9.1 Circumstances for revocation

A certificate may be revoked in the following circumstances:

1) information contained in the certificate became invalid or is false,
2) at each request of a subscriber or – in the event of notifying about business certificate revoking – at the request of an authorised representative of an entity or other authorised party,
3) at the request of the Minister of digital affairs,
4) 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 or a suspicion of an unauthorised access to a private key, the loss or a suspicion of the loss of a private key, a theft or a suspicion of a theft of a private key, an accidental destruction of a private key),
5) 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.),
6) by the certificate issuer, namely by EuroCert, e.g. as a result of a gross infringement of the Certificate policy or the Certification policy statement by the subscriber, in particular the obligations set out in § 4.5.1,
7) EuroCert ceases to perform services with regard to certificates and no other entity takes over providing services of providing information about the certificate's status,
8) EuroCert receives a proof that the certificate was used contrary to its purpose,
9) EuroCert receives information that certificate together with keys is potentially insecure,
10) the certificate was issued in conflict with the Certificate policy,

11) a private key of the CA was compromised or EuroCert obtains the information that it could have been compromised.

4.9.2 Who can request revocation

EuroCert observes the general rule that only the individual indicated in a certificate may demand the certificate be revoked, as well as the certificate owner or the entity represented by the owner. However, the situations may occur when the application for revoking may by submitted by other interested parties. The list of such parties and situations when it may occur are presented in the Certification policy statement.

4.9.3 Procedure for revocation request

The certificate is revoked upon successful verification of the application for revoking the certificate 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.

New CRL is generated published within one hour after the receipt of the revocation request. EuroCert submits the confirmation of the certificate revoking or the refusal decision indicating the reasons of the refusal, to the certificate subscriber and to the party applying for revoking the certificate by e-mail.

4.9.4 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.

4.9.5 Who can request suspension

A certificate is suspended at EuroCert's suspicion 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).

4.9.6 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 § 4.9.4, 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 certificate suspension 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.

4.10 Certificate status services

Verifying status of certificates issued by EuroCert may take place based on CRL. CRLs are generated at least every 24 hours or after every suspension/revocation a certificate, and are published

automatically in the repository (See Chapter 2). EuroCert checks the availability of CRLs at least once a day.
The status of a certificate issued by EuroCert may be also verified using the OCSP service, as long as this information is included in the issued certificate. If the address of OCSP service was included in a certificate, it means that this service is available for this certificate.

4.11 End of subscription

The agreement for providing certification services between EuroCert and the subscriber expires at the moment of the expiry of the certificate. 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. The Certification policy statement contains an extended description of these requirements.

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 providers of trust services and under the Personal Data Protection Act. Applied methods of physical protection for premises include, but are not limited to:

a) access control system for premises,
b) fire protection system,
c) flooding protection system,
d) break-in and robbery signalling system,
e) cooling system,
f) emergency power supply system.

Physical access to buildings with these premises is controlled and supervised by an integrated alarm system. External security in the buildings operates 24 hours every day.

Information systems used for providing trust services are located in two independent places (the primary centre and the backup centre) distanced from each other. In the case of the primary system's failure, the other system takes over the operations related to revoking, suspending certificates and CRLs publication, on an ongoing basis.

5.2 Procedural controls

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 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*.

Tab. 5. Trusted roles in EuroCert

Role	Scope of duties
Security officer	supervising the implementation and application of all safety procedure for information systems exploitation, used while providing trust services, managing system administrators, initiating and supervision over the process of generating keys and shared secrets, granting authorisation with regard to protection and access rights to users, assigning passwords to new accounts, supervising servicing works.
System Administrator	installing, configuring and managing systems and information networks used while performing certification services, managing the authorisations for system operators
System operator	permanent 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	analysing records in registers of events occurring in EuroCert’s information systems

The role of security officer cannot be connected with the System Administrator and the System Operator. The system auditor cannot be connected with any of the other mentioned roles.

Extended description of organised security and protection systems is included in the Certification policy statement and in internal documents of EuroCert.

5.3 Personnel controls

EuroCert guarantees that individuals performing their obligations resulting from the functions performed by the CA:

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 § with regard to sensitive information for the CA’s safety or confidentiality of the subscriber’s data,
e) they do not perform obligations that may cause conflict of interests between the CA 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.

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.

5.4 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 system 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

Types of event logs are listed in the Certification policy statement.

5.4.2 Frequency of processing log

Records of events are analysed by the system auditor and the system administrator each time upon the occurrence of an alarm in the monitoring system for key elements of the CA system in order to recognise possible unauthorised activities or other anomalies 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 only to the System auditor. 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 safe available only to system auditor 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.

5.4.6 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 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 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.

5.5 Records archival

Hard copy documents and electronic data directly related with provided certification services such as:

- Certification services agreement referred to in Article 14 item 1 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,
- the CA's keys history, from generation to destruction, inclusively,
- certificate policies,
- documents issued by the registration authority's 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.

According to Article 17 Paragraph 2 of the Trust Services Act above documents are stored and archived for 20 years from their creation.

Archive data in electronic form is stored in the principal centre in safes, while hard copy archive data is stored in the registered office of EuroCert Sp. z o.o. in metal lockers locked with keys.

5.6 Key changeover

The key changeover procedure refers to CA keys used for signing certificates and CRLs.

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

A new CA'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

This subchapter contains the description of procedures implemented by EuroCert in special events (including natural disasters) in order to reinstate the CA's functionalities. These procedures are implemented according to the prepared business continuity plan.

5.7.1 Compromise handling procedures

Eurocert has relevant procedures applicable in the event of the loss of confidentiality (compromise) of EuroCert's private key or a justified suspicion that such event occurred (see § 5.4.6). These procedures 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 related to the revealed private key and all currently valid certificates signed using the compromised private key,
d) notification about revoking the CA's certificate using available information channels,
e) creating new CA's keys and notifying the Minister of Digital Affairs about them in order to issue a new certificate by NCC 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 and keys for subscribers , based on new EuroCert keys, with their expiry date at least the same as the date of revoked certificates, without charging them with any costs for this operation.

5.7.2 Disaster recovery

EuroCert has implemented procedures ensuring the security and continuity in providing critical services of the CA 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.

Technical infrastructure of the CA is protected in order to enable continuous work in the event of any failure, while in the event of a disaster, equipment or infrastructure failure exceeding the capacities of the protection, the CA 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 CA 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).

Detailed procedures in this case are included in the termination plan for a qualified provider of trust services, referred to in Article 24 § 2 letter and eIDAS Regulation and in Article 19 § 3 of the Trust Services Act, held by EuroCert.

If other qualified supplier fails to take over EuroCert's business including especially processing of applications for revoking and suspending certificates and publishing CRLs it is necessary to revoke certificates of subscribers, who are entitled to return of the part of remuneration for the certificate's use in proportion to the period of its use.

Otherwise it is necessary to revoke certificates of subscribers, who are entitled to return of the part of remuneration for the certificate's use in proportion to the period of its use.

If no other qualified entity takes over the business of EuroCert, documents and records with regard to which archiving is requires are transferred to the supervisory body or to an entity indicated by it, upon closing the business.

6 Technical security controls

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

The CA 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), including the Security Officer. A report is prepared from the ceremony of keys generating.

The keys of certification services providing offices, operating within EuroCert are generated using a separated, credible workstation and a cryptographic module operating in unison with this station, holding Common Criteria EAL4+ certificate. 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.

6.1.2 Private key delivery to subscriber

A pair of keys and subscriber's certificate are issued in line with the rules described in § 4.4. The subscriber's keys together with the certificate are supplied to the subscriber in person together with information allowing for activating a private key for immediate change of data allowing for activating the private key. It is necessary to change PINs by the subscriber before commencing the certificate exploitation period.

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

6.1.3 CA public key delivery to relying parties

Public keys of the CA issuing certificates to end users are distributed only in the form of certificates in line with recommendation ITU-T X.509 v.3. Public key of EuroCert Qualified Centre has the form of a certificate issued by the NCC.

Public keys of the CA are distributed by publishing in the generally available repository (see Chapter 2) and listed on the TSL.

6.1.4 Key sizes

The minimum parameters of cypher algorithms accepted for use by EuroCert and by certification services recipients, within the policy, are as follows:

1) for RSA algorithm:
   - the minimum length of the key, understood as p*q module amounts to 2048 bits,
   - the length of the first p and q numbers comprising the module cannot differ by more than 30 bits;
2) for ECDSA and ECGDSA algorithm:
   - the minimum length of g parameter, amounts to 256 bits,
   - the minimum r0 indicator is 10000,
   - the minimum class is 200.

For executing an electronic seal under the subscriber's certificate, RSA/ECDSA algorithm is used in combination with SHA-1/SHA-512 hash function.

The CA keys' length is min. 2048 RSA bits or 384 bits ECC. Subscribers' keys' length is min. 2048 RSA bits or 384 bits ECC.

6.1.5 Key usage purposes

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

The private key of the CA may be used only for signing certificates and CRLs. A public key corresponding to it is used exclusively for verifying certificates (keyCertSign) and CRLs (cRLSign).

Subscribers' certificates may be used exclusively for affixing qualified electronic signatures and they are designated for ensuring non-repundation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Each subscriber, as well as CA personnel and operators of registration authorities, use and destroy their private key in the manner preventing its loss, disclosure, modification or unauthorised use.

6.2.1 Cryptographic module standards and controls

Private keys of subscribers related to qualified certificates are processed exclusively in qualified signature creation device, that fulfil the requirements set out in Attachment II to the eIDAS Regulation. This device as well as the cryptographic module (Hardware Security Module – HSM), in which the private key of EuroCert is stored, hold Common Criteria EAL4+ compliance certificate.

6.2.2 Private key escrow

Private key of EuroCert is not transferred (or forwarded) to other entities. EuroCert does not perform services of depositing and storing private keys of subscribers.

6.2.3 Private key backup

The mechanism of entrusting a backup copy of the private key of the CA is performed by dividing the key in parts (i.e. secrets) with 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

CA	Total number of secrets [n]	Number of secrets necessary for using the key [m]
EuroCert Qualified Centre	3	2

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 CA.

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 § 6.2.5.

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

6.2.4 Private key archival

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

Private keys of CA 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.

6.2.5 Private key transfer into or from a cryptographic module

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

1) commissioning the CA, during the system starting,
2) recovery of the CA’s key in a backup centre,
3) exchanging the cryptographic module.

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 § 6.2.3. 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 a cryptographic module 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.

6.2.6 Private key storage on cryptographic module

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

Keys from the CA and subscribers are stored on cryptographic cards protected by PIN and PUK cards.

6.2.7 Method of activating private key

A private key of the CA 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 carrier.

6.2.8 Method of deactivating private key

Deactivating EuroCert CA'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 CA server. Deactivating a key involves cleaning the cryptographic module's 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.

6.2.9 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 CA means a physical destruction of cryptographic cards, on which shared secrets are stores or their safe removal from a carrier (from a cryptographic card, a cryptographic equipment module etc.). Destroying private keys of the CA 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 and a witness. Cards must be identified before being destroyed. A report is prepared from the destruction procedure.

6.3 Other aspects of key pair management

The following points describe aspects related with the certificates validity periods and archiving the keys.

6.3.1 Public key archival

EuroCert implements a long term archiving process for its 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 upon the expiry of the validity period of CA's certificate and completing its operations.

Archiving is performed by the Security Officer. Archiving is performed by saving files with certificates on optical carriers. The archive files are subscribed with an electronic signature of the Security Officer. Details regarding creating an electronic archive are included in § 5.5. The archiving period for public keys of the CA is 20 years.

6.3.2 Certificate operational periods and key pair usage periods

Validity period for private keys and certificates of subscribers, according to the Policy does not exceed 2 years and it is set out in the validity field of each certificate. “Valid from” date for each certificate is the same as its date of issue.

6.4 Activation data

Immediately upon generating the certificate and a pair of keys on cryptographic card, using the card managing application delivered by EuroCert PIN and PUK securing codes are given, securing the access to the card, confirming the performance of the operation by affixing own signature in a written declaration.

The PIN and PUK keys assigned by the subscriber are known only by the 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. 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.

Activating EuroCert CA’s key is described in § 6.2.7.

6.5 Computer security controls

The safety assessment of a single computer and software installed in this computer is performed based on norms requirements described 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.

6.6 Life cycle technical 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.

The policy 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 including issuing certificates by a qualified supplier of these services.

Supervision over the security of EuroCert’s computer systems is performed by EuroCert.

6.8 Time-stamping

All timers functioning in EuroCert system and used while performing the services are synchronised with the Coordinated Universal Time with an accuracy of 1 second.

7 Certificate and CRL profiles

Profiles of certificates and CRLs issued in line with the Policy comply with recommendations of ITU-T X.509 v3 and ITU-T X.509 v2 norms as well as with the profiles included in: ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Parts 1,2,5.

According to the opinion issued by the Ministry of Development, Electronic Economy Department, during the transition period, indicated in Article 51, § 2 of the eIDAS Regulation, EuroCert uses SHA-1 algorithm in qualified services performed by it.

Information presented below describe the meaning of certain certificate fields, CRLs, applied extensions.

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, defined respectively in § 7.1.1 and 7.1.2 below.

7.1.1 Basic fields

EuroCert operates basic fields of the certificate described in Table 7.

Tab. 7. Profiles 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		Explicit serial number (product key) of the certificate, assigned by EuroCert
SignatureAlgorithm	cryptographic algorithm identifier, describing the algorithm used for the performance of an electronic seal made by the CA on the certificate.		SHA1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or SHA512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) or ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Issuer (certificate issuer's DN)	Profile 1	Common Name	CN = Centrum kwalifikowane Eurocert
		Organization	O = EuroCert Sp. z o.o.
		Country	C = PL
		Organization Identifier	2.5.4.97 = VATPL-9512352379
	Profile 2	CN	Centrum Kwalifikowane EuroCert
		O	EuroCert Sp. z o.o.
		C	PL
		SerialNumber	Nr wpisu: 14

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 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1,2,5.*	Subscriber's DN (see § 3.1)	
SubjectPublicKeyInfo	The field is coded in line with requirements specified in RFC 5280 and it may contain information on RSA, DSA or ECDSA public keys (namely on the key identifier, the key length in bits and on the public key's value). The public key's value of an entity with the algorithm identifier associated with the key.	Public Key Algorithm	sha1WithRSAEncryption or SHA512WithRSAEncryption or ecdsa-with-SHA512
		RSA Public Key (the length of the key)	Min. 2048 bits or ECC 384 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).	

7.1.2 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	160 bit SHA-1/SHA-512 hash function on the value of the public key for the CA's certificate
SubjectKeyIdentifier	NO	Certificate identifier containing the hash public key contained in the certificate	160 bit SHA-1/ SHA-512 hash function on the value of the public key for the CA's 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: 1.2.616.1.113791.1.2.1 or 1.2.616.1.113791.1.2.2 or 1.2.616.1.113791.1.2.3
CRLDistributionPoints	NO	CRL distribution point (specifies the URL address on which the current CRL is published)	http://crl.eurocert.pl/qca03.crl or http://crl.eurocert.pl/qca02.crl or http://crl.eurocert.pl/qca04.crl
Authority Info 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}
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}

7.2 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) or SHA512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) or ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Issuer CRL's issuer identifier, compliant with the identifier set out in the certificate's profile	See table 7 (Issuer)

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	serial number (product key) of a revoked certificate
revocationDate	date and hour of certificate revoking
reasonCode	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.

7.3 OCSP profile

Certificate status token profile is described in internal classified 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 providers of trust services described in the eIDAS Regulation and procedures and processes described in EuroCert's documentation (including the Certificate Policy and the Certification policy statement).

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 e) of the eIDAS Regulation.

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

Issues covered by the audit and the procedure applicable in the event of irregularities of functioning of the CA are presented in the Certification policy statement.

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.

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.

Services related to suspending and revoking certificates and access to the CRLs are free of charge.

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 the Certificate policy or the Certification policy statement.

9.2 Financial responsibility

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 supplier of trust services.

The financial liability of EuroCert Sp. z o.o 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.

9.3 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.

9.4 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 Personal Data Protection Act of 29 August 1997.

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

a) Certificate policy and the Certification policy statement,
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.

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 § 7.1.1) or – with regard to a business certificate subscriber – the property of the subject represented by the subscriber.

9.6 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:

   i. ITU-T X.509 (ISO/IEC 9594-8 corresponds to it),
   ii. ISO/IEC 15945 (CMP protocol),
   iii. *in fact* PKCS#10, PKCS#7, PKCS#12,
   iv. ETSI EN 319 401,
   v. ETSI EN 319 411-1,
   vi. ETSI EN 319 411-2,
   vii. ETSI EN 319 412-1,
   viii. ETSI EN 319 412-2,
   ix. 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.

The registration authority and persons confirming identity also undertake to:

1) observing procedures of identity confirmation while issuing certificates in line with the rules set out in this document and in the Certificate policy, 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 this Certificate policy,
7) undergoing planned audits performed at EuroCert's order or by EuroCert.

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

9.7 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

This Certificate Policy applies to certificates issued in line with this policy until the expiry of these certificates (due to the expiry or revoking a certificate).

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

OID change for the Policy may take place only in the event of the change of the entity supervising the EuroCert Qualified Centre and in the case of changes that may have actual effect on a significant group of the Policy users.

9.13 Dispute 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 Certification policy statement and agreements entered into.

Disputes or complaints arising from using the certificates, certificates status verification 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 this Certificate policy, in the Certification policy statement and in the applicable provisions of law. In order to interpret the terms included in the Policy, they must be considered in line with eIDAS 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:

1) 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,
2) The Act on Trust Services and Electronic Identification of 5 September 2016,
3) The Personal Data Protection Act of 29 August 1997,
4) The Criminal Code of 6 June 1997,
5) The Identity Cards Act of 6 August 2010,
6) The Passports Act of 13 July 2006,

7) The Foreigners Act of 12 July 2013,
8) The Copyright Law of 4 February 1994.

9.16 Miscellaneous provisions

See: Certification policy statement

9.17 Other provisions

No other provisions exist.

Document history

Version	Approval date	Description of amendments
1.0	01.08.2013	creating a document
1.1	27.11.2015	Submitting to the Supervisory body
1.2	15.03.2015 r.	Changes in the address of contact data
1.3	20.11.2015 r.	Changes in the address of contact data
2.0	14.06.2017	Conforming to eIDAS Regulation (EU) and Trust services act (PL)
3.0	15.11.2017	Changes regarding new profile of certificate (added 3072 RSA bit keys and ECDSA keys).