• LONDON • LUBLJANA • PRISHTINA

2023

UKITES BY PBC LIMITED
SLOTES

CPS - Certification Practice Statement

rTrust PKI Certificate PolicyVersion 1.1

Publication Date: 31.05.2023

Effective Date: 01.08.2023

info@ukites.co.uk | www.ukites.co.uk

Copyright statement

UKITES BY PBC LIMITED - SLOTES
Kotnikova Ulica 5,
1000
Ljubljana, SLOVENIA
Email: info@rTrust.org

Document History

Version	Date	Description
0.8	05.05.2022	Draft
0.9	12.05.2023	Corrections
0.92	19.05.2023	Corrections
0.95	20.05.2023	Directory Links Corrections Key Recovery Links Corrections
0.98	23.05.2023	Procedural Control Corrections Personnel and Security Controls Corrections Audit Logging Procedures Corrections Intellectual Property Rights
1.00	01.06.2023	Final Draft
1.1	01.08.2023	Updates for certification

Table of contents

Contents

1. Introduction

1.1 Overview

This document describes rTrust Certification Practice Statement (CPS), which is operated and maintained by the UKITES BY PBC LIMITED - SLOTES.

1.1.1 Certification service provider

The Certification Service Provider (CSP) is the

UKITES BY PBC LIMITED - SLOTES
Kotnikova Ulica 5,
1000
Ljubljana, SLOVENIA

Through its contracted partnership with PBC:
Address: Tirana St. no. 91
10000 Prishtina,
KOSOVO

The CSP currently offers its services via https://www.rTrust.org/, but it may entrust contractual partners or external contractors with parts of the production process, as long as all agreements are meticulously documented and a contractual relationship has been established prior to the provision of supplied services.

1.1.2 About this document

This CP provides binding regulations and requirements for rTrust and thereby defines the certification process throughout the validity period of the End-Entity certificates (EE-certificates) as well as the co-operation, rights and duties of other PKI-participants.

The CP is legally binding in its entirety, in as much as is permissible by the legislature of the Republic of Kosovo. It contains statements describing duties, guarantees and liabilities for PKI-participants. Unless expressly stated otherwise, no warranties or formal guarantees in a legal sense may be derived from this CP.

The knowledge of the certification methods and –rules as well as the knowledge of the legal operating framework allows relying parties to form an

informed decision about the components and PKI-participants as well as to decide if the trustworthiness imparted by the security-measures inherent in the PKI is sufficient for their applications.

The structure of this document is based on the internet-standard RFC 3647 *„Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“,* to facilitate understanding and comparisons with otherCertificate Policies.

1.1.3 PKI traits

The rTrust PKI hierarchical structure is multi-tiered. The constellation of the rTrust PKI is shown in Figure 1.

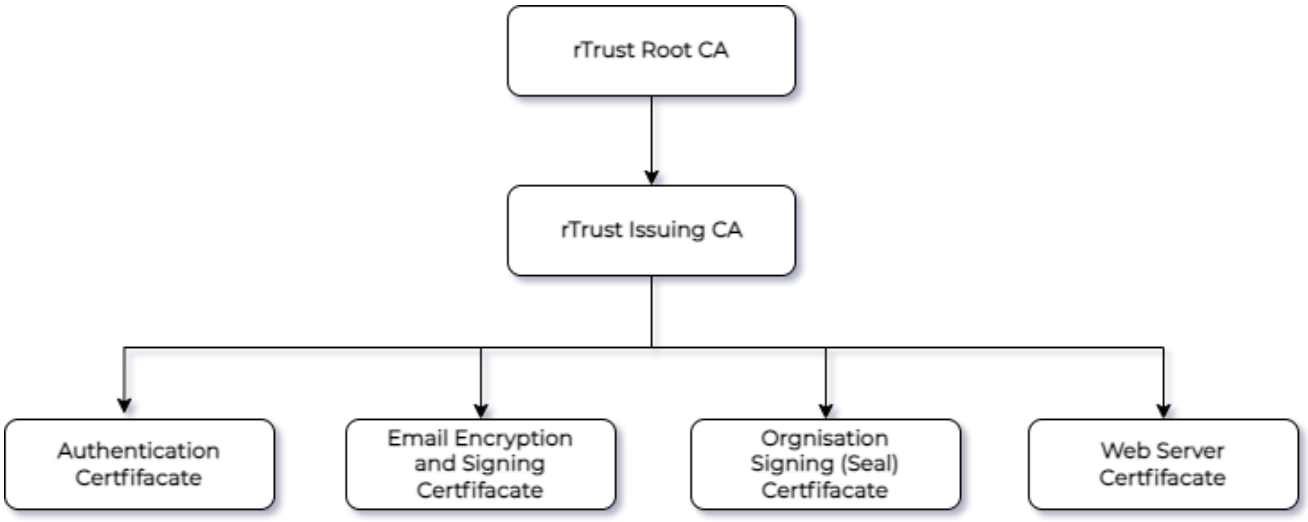

Figure 1: rTrust PKI architecture and certificate types

The EE-certificates, are described in separate document published in web site, can be categorized as follows:

1. Authentication Certificate (software based or qualified):
   Certificate for authentication under the holder's real identity.

2. Email Encryption and Signing Certificate (software based or qualified):
   Certificate for signing and encrypting/decrypting emails or files with respective email clients and tools.

3. Organization Signing (Seal) Certificate:
   Certificate for signing (electronic seal) documents to verify their authenticity by organization.

4. Web Server Certificate:
   Certificate for enabling secure communication (HTTP over TLS) between client and web server.

1.2 Document and Identification

Document name:	rTrust Certification Practice Statement (CPS)
Object Identification (OID):	This document's Policy-OID: 1.3.6.1.4.1.55084.100.1.1.100
Version	1.1

1.3 PKI-Participants

1.3.1 Certification Authority (CA)

CAs issue Certificate Revocation Lists (CRLs), certificates for natural entities (EE-certificates), legal entities or a group of individuals and certification authority certificates (CSP sub-CA-certificates). Certificates for functions and IT-processes are not issued.

Root-CAs only issue certificates with the extension basicConstraints: CA=TRUE (CA-certificate). Sub-CAs issue EE-certificates and/or further CA-certificates. The Certification Service Provider is named in the field issuer, which is part of the issued certificates and CRLs.

The digital certificate rTrust Root CA content is presented in Table 1:

Serial Number	140DDD17C6F5B50D
Issuer	rTrust Root CA
Subject	rTrust Root CA
Validity: Not Before	Friday, June 16, 2023 11:32:00 AM
Validity: Not After	Wednesday, June 16, 2038 11:32:00 AM
RSA Public Key	RSA (4096 bits): D3ED6080BDB446FCFA9BD2EFE30F3B0C...
Signature Algorithm	SHA256RSA
Key Identifier	A55D31EF15B9105E2D74052446D163B005062287
Authority Key Identifier	KeyID=A55D31EF15B9105E2D74052446D163B005062287
SHA-1 hash	9E1B9CBB668FD254B50FBFFA06140CDCC1A83209
SHA-256 hash	9BD8CB4F5E512F2CE439D136EB2A7896 FE43432D066C8BFE783001C8BCF42C92

Table 1: rTrust Root CA details

The rTrust Issuing CA digital certificate with details as presented in Table 2

Serial Number	4E00CAF4B919430A
Issuer	rTrust Root CA
Subject	rTrust Issuing CA
Validity: Not Before	Wednesday, July 19, 2023 6:09:00 PM
Validity: Not After	Tuesday, July 19, 2033 6:09:00 PM
RSA Public Key	RSA (4096 Bits): CD035DFA51B3996D33B080C8B1D2A3A3...
Signature Algorithm	SHA256RSA
Key Identifier	4579DE04B0A4C9EEAAD961E48A4EB02DC50189EA
Authority Key Identifier	KeyID= 55d31ef15b9105e2d74052446d163b005062287
SHA-1 hash	9417E36122B46A1767C15E2DF991C6327F182E5B
SHA-256 hash	9C5D77EDF18691BFDFBE5AB82A1A8B78 ED1E6B8D79032A5F0B37E6C2C55946B4

Table 2: rTrust Issuing CA details

These certificates, Root CA and Issuing CA, are available at https://pki.rTrust.org/

1.3.2 Registration Authority (RA)

Registration authorities (RAs) are responsible for checking the identity and authenticity of subscribers. The CSP provides the RA with suitable hard- and software, as well as work-flow processes that must be incorporated by the RA. Personal identification takes place online as described in the appropriate section.

1.3.3 Subscribers

Subscribers are individuals or legal entities, i.e. natural persons or organizations (legal entities). The subscriber can differ from the entry in the certificate's subject-field.

End-Entities (EU, subject) use the private End-Entity-Key (EE-key). End-Entities are identified in a certificate as the holder of the private key associated with the public key given in the certificate. Possible End-Entities are:

- Individuals
- Organizations (legal entities – under private law, public corporations or government owned)

who by concluding an agreement with rTrust as a Trust Service Provider, has undertaken the agreed obligations of a Subcriber.

1.3.4 Relying parties (RP)

Relying parties are individuals or legal entities that use the certificates of rTrust and have access to the services of the CSP. By means of the certificate, the Relying Party shall verify the identity of the Subject and shall validate electronic signatures.

1.4 Certificate Usage

1.4.1 Valid Usage of Certificates

CA-certificates are used exclusively in Issuing CA- or End-Entity certificates and CRLs in accordance with their extensions (BasicConstraints, PathLength-Constraint).

EE-certificates may be used for those applications in accordance with the intended certificate usage as stated in the certificates themselves.

Relying parties assume responsibility for estimating if this CP applies in the case of the application of interest. The relying party must also assess the suitability of utilizing certificates for a given scenario.

1.4.2 Invalid Usage of Certificates

It is prohibited to use certificates for applications other than those explicitly mentioned in the certificates themselves.

1.5 CP/CPS maintenance

1.5.1 Document Administrator

This CP is maintained by SLOTES and its partner PBC LLC. The head of the Quality Assurance Department (QAD) of PBC, is responsible for approving this CP and any following versions hereof.

1.5.2 Contact Address

UKITES BY PBC LIMITED, SLOTES
Kotnikova Ulica 5, Ljubljana,
Slovenia
Email: info@rTrust.org

More information about rTrust certificates can be downloaded from https://pki.rTrust.org/.

1.6 Definition of Terms, Abbreviations and Acronyms

1.6.1 Terms and names

Applicant	Subscriber, individual that applies for a certificate. Either for themselves or for others.
CA-certificate	A certificate for a Certification Authority's public key.
Certificate Policy (CP)	Compare Section 1.1
Certification Authority (CA)	Root PKI Authority, compare Section 1.3.1.
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking and renewing or re-keying certificates.
Certification Service Provider	Provider of certification services.
rTrust Root CA	Root Certification Authority, compare Section 1.3.1.
rTrust	UKITES BY PBC LIMITED, SLOTES
Directory Service	PKI-service for online access of information pertaining to certificates and CRLs; commonly realized through the Light Weight Directory Access Protocol (LDAP).
Distinguished Name	A sequence of data-fields describing the CA issuer and/or the subject uniquely. The format of a Distinguished Name is defined in the [X.501] standard.

End-Entity	End-Entitys make use of the private End-Entity -key and may differ from the Subject.
End-Entity-certificate	Certificate, that may not be used to certify and issue other certificates or CRLs.
EE-certificate	See “End-Entity -certificate”
Registration Authority (RA)	PKI-incorporated facility for participant-authentication; compare section 1.3.2.
Relying parties	Individual or legal entity that uses certificates; compare chapter 1.3.4.
Revocation Authority	Individual or legal entity that is entitled to revoke a certificate.
Status monitoring service	PKI-service for on-line inquiries concerning the status of a certificate (valid, revoked, unknown) through the Online Certificate Status Protocol-Responder.
Subscriber	Individuals or legal entities that own End-Entity certificates; compare chapter 1.3.3.
TrustCenter	The high-security area on the premises of the UKITES BY PBC LIMITED, SLOTES and Hetzner GmbH.
Qualified Certificate	Personal authentication certificate of standard security level whose corresponding private key shall be kept QSCD.
NCP	A Normalized Certificate Policy which meets general recognized best practice for Qualified TSPs issuing certificates used in support of any type of transaction.

Individual certificate (NCP)	Personal authentication certificate of standard security level whose corresponding private key shall be kept in software protected token. This type of certificate shall be compatible with "NCP" Certificate policy referred to in standard ETSI EN 39 411-1.

Business certificate (NCP)	Business authentication certificate of standard security level whose corresponding private key shall be kept in software protected token. This type of certificate shall be compatibile with "NCP" Certificate policy referred to in standard ETSI EN 319 411-1 [11].
Hetzner	Hetzner Online GmbH is a professional web hosting provider and experienced data center operator. Since 1997 the company has provided private and business clients with high-performance hosting products as well as the necessary infrastructure for the efficient operation of websites.

1.6.2 Abbreviations

AUTH	Authentication
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification service provider
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
ISO	International Organization for Standardization

LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment
URL	Uniform Resource Locator
PIN	Personal Information Number
NCP	Normalized Certificate Policy
BRG	Baseline Requirements Guidelines
GDPR	General Data Protection Regulation

1.6.3 References

[1] CP	Certificate Policy of the rTrust, UKITES BY PBC LIMITED, SLOTES, in its most recent version.
[2] CPS	Certification Practice Statement of the rTrust, UKITES BY PBC LIMITED, SLOTES, in its most recent version.
[3] Co-PKI	Common PKI Specification, Version 2.0, 20th of January 2009
[4] eIDAS	European Union Regulation, No 910/2014.
[5] RFC 2560	X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, June 1999.

[6] RFC 5280	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, May 2008.
[7]RFC 6960	X.509 Internet Public Key-Infrastructure Online Certificate Status Protocol, May 2008.
[8] X.501	ITU-T RECOMMENDATION X.501, Information technology – Open Systems Interconnection –The Directory: Models, Version August 2005.
[9] X.509	ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
[10] ETSI EN 319 401 v2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
[11] ETSI EN 319 411-1v2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
[12] ISO/IEC 27001:2013	Information technology-Security techniques-Information security management
[13] Hetzner Policy Document	Public available document „Technical and Organizational Measures in accordance with

Art. 32 GDPR from https://www.hetzner.com/AV/TOM_en.pdf.

[14] IETF RFC 5280 — Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

[15] IETF RFC 6960 — X.509 Public Key Infrastructure Online Certificate Status – OCSP (2013)

[16] ETSI TS 119 312 v1.1.1 (2014-11) — Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[17] CA/Browser Forum — Baseline Requirements – Certificate Policy for the Issuance and Management of Publicly-Trusted Certificate

2. Responsibility for Directories and Publications

2.1 Directories

The CSP does not publish CRLs and certificates into a LDAP-directory.

CA-certificates are published on the web-sites of rTrust and can be accessed through the URL https://pki.rtrust.org/.

The CSP provides an online certificate status-monitoring-service (OCSP) through which the revocation status of every certificate in rTrust may be checked. The address for the OCSP-service: http://pki.rtrust.org/ejbca/publicweb/status/ocsp is part of the certificate information. Any certificate's status may be checked up to a year after their expiration, after which time the entry will be removed from the service.

This CP, the CPS [2] CPS and the Subscriber's Obligation can be downloaded as PDF-documents from the CSP's web-site.

2.2 Publication of Certificate Information

Documents and information on certification services shall be available to the public and shall be published on the rTrust PKI repository.

The following shall be published on rTrust repository web pages:

- Certification Policy documents
- Public versions of the Certification Practice Statement
- Terms and Conditions and PKI disclosure statement
- Certification services price list
- Subscriber forms
- rTrust Root CA certificate and subordinated rTrust Issuing CAs certificates and End Entity certificate profiles
- CRL rTrust Root CA and CRLs subordinated rTrust Issuing CAs
- Notifications to Subscribers and Relying parties, related to Certification Service Provision
- Other information related to the work of rTrust Issuing CAsThe

CSP publishes the following information about rTrust:

- CA-certificates (Trust-Anchor),
- Certificate Revocation Lists (CRLs) and Certificate Status information,
- this CP [1],
- the CPS [2] CPS.

Confidential data shall not be published in the rTrust PKI repository.

2.3 Publication Frequency

EE-certificates are not published.

CA-certificates are published in the course of their creation and remain listed for at least until the CA has expired.

CRLs are published periodically and until the issuing CA-certificate expires. A new CRL of a SUB-CA is issued every 24 hours, even if no revocation has occurred in the meantime. A new CRL of the Root CA is published every 6 months. In case that the certificate of a Sub-CA is revoked the new CRL of the Root CA is published immediately. The CRLs are listed for at least until the CA has expired.

This CP and the CPS [2] CPS are published and remain listed and downloadable as long as they remain in effect (compare chapter 2.1).

2.4 Directory Access Control

Certificates, CRLs, CPs and the CPS are listed publically and can be downloaded free of charge. A read-only access is permitted for the general public.

The relevant parts of other, non-public documents can be made available on request, if a vested interest is in evidence.

3. Identification and Authentication

3.1 Naming Conventions

3.1.1 Types of Names

CA- and EE-certificates principally contain information on the issuer as well as on the Subscriber or End-Entity (subject). The names are listed in the fields issuer and subject and are formatted along the X.501[8] standard for DistinguishedNames.

Alternative names may be registered and would subsequently be displayed in the subjectAltName-extension of a certificate.

Details about the name, or the title of the certification Subject and details about the place of residence of a Natural person, or Business Entity registered office location shall be entered on each certificate. Details about the name or title entered in the certificate shall refer to the authentic name or title of the Subject. The Subject field in the certificate shall be aligned with the recommendation IETF RFC 5280 [14].

The Subject field in personal certificates and business certificates issued to Associated persons, shall contain the name and surname of the persons, and the serial number which shall ensure the uniqueness of the Subject field. In business certificates for Associated persons, the Subject field shall additionally contain the full registered name of the Business Entity and its identifier.

The Subject field in application certificates shall contain the name of the IT system, application or service (hereinafter referred to as: the application name). The Subject field in application certificates shall additionally also contain the full registered name of the Business Entity and its identifier.

The Subject field in certificates for electronic seal of Trusted List shall contain the full registered name and identifier of the central state administration authority competent for economic affairs.

3.1.2 Necessity for unambiguous names

A Subscriber's DistinguishedName is unique in rTrust.

An unambiguous, biunique correlation between certificate and subscriber is guaranteed.

3.1.3 Rules for the Interpretation of Different Naming Combinations

The provisions for inclusion and interpretation of names are defined in the Certificate Practice Statement CPS [2].

DN-components adhere to RFC 5280 [6] and Co-PKI [3] Co-PKI.

The interpretation of the name form in the Subject field according to the standard X.520 in rTrust PKI shall be determined in the following way:

- Serial Number

  The value of the attribute Serial Number in the Subject field shall guarantee the uniqueness of individual Subjects. The value of this attribute shall also guarantee the uniqueness of the Subject field in certificates within rTrust PKI production hierarchy founded on rTrust Root CA.

  In personal and business certificates issued to Natural persons, the Serial Number attribute shall consist of 10-digit unique identifier for Kosovar citizens or 11-12-digit unique identifier for EU or foreign citizens that have internal meaning for rTrust PKI.

- Common Name

  In personal certificates, these attributes shall contain the name and surname of the Natural persons as listed in the identification document.

  In certificates for the electronic seal this attribute shall contain the name determined by the central state administration authority competent for economic affairs, with which the Subject usually presents itself.

- Given Name

  The attribute Given Name shall contain the name of the Natural person as listed in the identification document.

- Surname

  The attribute Surname shall contain the surname of the Natural person as listed in the identification document.

- Country Name

  The attribute Country Name shall contain the two-letter

- Organization Name

In business certificates issued to Associated persons, the attribute Organization Name shall contain the full registered name of the Business Entity.

In certificates for e-seal of Trusted List, this attribute shall contain the full registered name of the central state administration authority competent for economic affairs.

In administrative certificates, the Organization Name attribute shall contain the full registered name of rTrust.

3.1.4 Uniqueness of Names

The CSP guarantees, that the DistinguishedName for a Subscriber or End-Entity employed in the subject field of rTrust EE-certificate will be unique, not only throughout the validity-period of the certificate, but throughout the entire existence of rTrust and will also stay strictly correlated with the same subscriber. DistinguishedName uniqueness may be achieved through the incorporation of a serial number, which guarantees the unambiguous identification[1] of the subscriber.

The CSP assures the uniqueness of its CAs' DistinguishedNames.

3.1.5 Acceptance, Authentication and Brand-Names

Not applicable.

3.1.6 Need for names to be meaningful

The names and titles of attributes of the Subject field that identify Natural persons and Business Entities shall be meaningful.

The following rules shall apply to attributes in the Subject field in certificates issued by rTrust Issuing CAs:

- identifiers must be meaningful,

[1] Identification in this instance means the identification of the subscriber's true name in combination with the data obtained through the initial application, notwithstanding any possible changes in possible consecutive applications. Identification in this instance neither includes the elicitation of possible changes in the initial application data nor locating a subscriber at a later point in time.

- the personal name and surname must be as listed in the identification document, that is, official competent registers,
- the full registered name of the Business Entity must be as listed in official competent registers,
- the name of the application must be as listed in applications for certificate issuance.

3.2 Initial Identity Inspection

3.2.1 Verifying Ownership of the Private Key

A subscriber's key-pairs are produced inside the facilities of the CSP. With the delivery of the token happening as soon as the password is given according to chapter 4.4.1 the transferal of the key-pairs is secured.

3.2.2 Identification and Authentication of Organizations (i.e. Service Providers)

The Service Provider must be identified by a "Qualified Independent Information Source".

A Qualified Independent Information Source (QIIS) is a regularly-updated database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information. The CA MUST check the accuracy of the database and ensure its data is acceptable.

The verification and authentication of a Business Entity's identity shall be conducted by verifying:

- the registered name of the Business Entity,
- the legal existence of the Business Entity,
- entry in the competent register,
- the company registration number in the competent register,
- the business number of the Business Entity, if one has been assigned,
- the address of the registered office of the Business Entity.

rTrust does not carry out verification and authentication of Business Entities when issuing Administrative certificates to rTrust 's authorized employees.

3.2.3 Identification and Authentication of Individuals

Personal identification takes place online by means of uploading and verifying identity documents. In case of businesses, the identity documents include the business certificate of that business. If no identifying documents are available, rTrust considers the identification process as failed and without having other means to verify that the applicant is a real person, will automatically deny the applicant.

The difference lies in the certificate content. The IDENT certificate contains personal information of the card holder that enables the service provider to identify him definitely:

- First and last name
- Citizen personal number (as serial number)
- Country code (KS for Kosovo, SI for Slovenia etc.)
- E-mail address (for SIG certificate only)
- Mobile phone number (optional)

When issuing business certificates being issued to Associated persons, rTrust shall also collect proof of the connection of the Associated person with the Business Entity.

3.2.4 Unexamined Statements concerning the Subscriber

Checks for validity or correctness of the email addresses will be performed. The email address will be submitted by the citizen during enrollment of the personal data. The email address has to be real, as it will serve as a channel to notify the applicant whether or not the application has been approved or denied.

3.2.5 Anonimity or pseudonymity of subscribers

Anonymity or pseudonyms of Subscribers shall not be supported.

3.2.6 Examination of Application Entitlement

Examination of application entitlement will be carried out by a person under the employee of UKITES BY PBC LIMITED, SLOTES, hereby known as the operator. The operator will confirm the data the applicant has submitted and based on that, will decide whether to approve the applicant request or not.

3.2.7 Criteria for Interoperability

Not applicable.

3.3 Identification and Authentication of Re-Keying Applications

Re-keying is not offered.

3.4 Identification and Authentication of Revocation Applications

The CSP validates the revoking party's entitlement for the intended action prior to revoking a certificate. The validation procedures intend a personal identification online based on valid identity documents; resp. in case of Service Providers, the Service Provider is identified by an "Qualified Independent Information Source" (cf. section 3.2.2).

Revocation procedures are described in chapter 4.9.

4. Operating requirements

4.1 Certificate Application and Registration

4.1.1 Application Eligibility

To be eligible to a rTrust certificate, certain conditions have to be met:

1. The applicant has to be a real person,

2. The applicant has given accurate information,

3. The applicant can be connected to a unique identifier, as used by the government,

4. The applicant has made the payment regarding the certificate that has been selected,

5. In select cases, such as the certificates used for organizations, several more conditions have to be met:

    5.1. The organization has to be registered in their respective government's business registry,

    5.2. The only person authorized to apply for an organization's certificate is the person listed in the respective government's business registry page about said organization.

4.1.2 Registration-Process and Administrative Responsibility

During the registration-process the applicants are made aware of the CP, the CPS, and further documents that inform the applicant of the restrictions and requirements in the usage of the different certificate-types.

The CSP ensures the correct observance of the registration-process.

4.2 Processing the Certificate Application

4.2.1 Identification and Authentication

The described procedures for identification and registration must be fully implemented in accordance with the provisions for the different categories; the necessary documents of proof must be impeccable.

Authentication of individuals or organizations, as well as the verification of relevant data may take place before or after application, but must be completed before certificates or, if applicable, keys and passwords are transferred to the subscriber.

The identification-process is described in Section 3.2.2. The applicable methods are defined in the [2] CPS.

4.2.2 Approval or Declination of Certificate Applications

The application will be declined if any of the criteria mentioned in 4.1.1 aren't met. Freely selectable content like email address may be rejected by operators.

Reasons for a declination may be:

- obviously wrong content,
- suspected misuse,
- duplicate requests that weren't automatically declined,
- failure to provide satisfactory proof of identity,
- suspicions concerning the violation of name rights

4.2.3 Time Limit for Application Processing

Application will be processed within 24 hours after submission, on the following weekdays: Monday, Tuesday, Wednesday, Thursday and Friday. On the two remaining weekdays: Saturday and Sunday, applications will be processed within 48 hours after submission.

4.3 Certificate Issuing

4.3.1 CSP Approach in Issuing Certificates

After a satisfactory validation of the application, the certificates are produced in the high-security CSP TrustCenter. The application documents are archived in their entirety. The personal data used for creating the certificates will remain, as per applicant's consent, securely stored on the servers.

4.3.2 Subscriber Notification Concerning Certificate Issue

Citizens are notified via e-mail about approval or denial of the data entered and are given further instructions regarding next steps.

4.4 Certificate Transfer

4.4.1 Certificate Transaction Procedures

After the operator approves the request, an email will be sent to the user using the provided email address. From there, the user is instructed to enter the password that they will be using to import the certificates, as well as the payment information.

After password is entered, a final automated comparison will be made between the entered data and the data in the provided identity documents, and if the comparison is satisfactory, the purchase is processed and certificates are be made available to the user for downloading.

4.4.2 Certificate Publication by the CSP

Certificates will not be made publicly available.

After certificate issuance, the status of the certificate will be available to any interested party either through the access of CRLs or by sending a status request to the OCSP-responder (compare chapter 2.1).

4.4.3 Notification of other PKI-participants about the Creation of the Certificate

The only person to be notified regarding creation of certificates is the operator, who in select cases (oragnization certificates), will contact the applicant, using the provided phone number if and only if that phone number matches the one listed in the respective government's business registry for that organization.

4.5 Certificate and Key-Pair Usage

4.5.1 Subscriber Certificate and Private-Key Usage

The subscriber may only use his private key for those applications that are explicitly described as the possible use-cases in the certificate.

4.5.2 Relying Parties' Certificate and Private-Key Usage

The certificates of rTrust can be employed by all relying parties. They retain their trustworthiness only, if

- the certificates are used according to the use-cases noted in the certificate (key-usage, extended key-usage, possible constraints),
- the certificate chain is successfully verified all the way up to – and including – a trust-worthy root-certificate,

- the certificate-status is successfully verified through the online status monitoring service (OCSP), and
- all further agreements and otherwise published precautions are metand that possible certificate constraints as well as any necessary provisions for the deployed applications are noted, considered and found to be in accordance with the use-case(s) by the relying parties.

4.6 Certificate Renewal

Certificate renewal is not offered.

4.7 Certificate Renewal with Key-Renewal

Key-renewal is not offered.

4.8 Certificate Changes

Certificate changes are not offered.

4.9 Revocation and Suspension of Certificates

4.9.1 Criteria for Revocation

Hosting a certificate revocation service is the CSP's lawful obligation towards the subscriber and affected third parties.

Subscribers or affected third parties are encouraged to apply for a revocation if there is a suspicion that the private key may have been compromised or the certificate data is no longer correct.

Revocations are fitted with a date and are not issued retroactively.

Revocation authorities must authenticate themselves according to chapter 3.4.

4.9.2 Eligibility for Revocation

The CSP is a revocation authority.

The subscriber is authorized to revoke any certificate made as a result of their request.

UKITES BY PBC LIMITED, SLOTES, reserves the right to revoke subscriber's certificates in case of citizen's death or if there is evidence of its misuse.

4.9.3 Processing a Revocation Application

Revocations are performed in the CSP's sphere of responsibility after the applicant is uniquely identified. The authentication follows the guidelines as laid-out in chapter 3.4.

4.9.4 Deadlines for a Revocation Application

The subscriber is obliged to revoke – or have the authorized third party revoke – the certificate as soon as reasons for a revocation become known.

4.9.5 CSP Revocation-Application Processing Time

On standard work days, revocation-applications are processed by the CSP from 09:00h to 17:00h.

4.9.6 Methods of Validating Revocation-Information

Topical revocation information is stored in certificate revocation lists that may be accessed through the light-weight directory-access protocol or downloaded via the link given in section 2.1. Additionally, the OCSP-service is provided. These services' reachability is noted in the form of URLs in the certificates themselves. Revocation-information can also be obtained from the websites of the CSP (http://pki.rtrust.org/ejbca/publicweb/status/ocsp). Delta-CRLs are not used. Integrity and authenticity of the revocation-information is ensured through a signature.

4.9.7 Revocation List Publication Frequency

Compare chapter 2.3.

4.9.8 Maximum Latency Period for Certificate Revocation Lists

Revocation lists are published with their production.

4.9.9 Online Accessibility of Revocation Information

An OCSP-service is provided for the online status check of certificates. This service's reachability is noted in the form of a URL in the certificates themselves.

4.9.10 Necessity of Checking Revocation Information online

There is no obligation to check revocation information online; the stipulations in section 4.5.2 stay in effect.

4.9.11 Other Forms of Publishing Revocation-Information

None.

4.9.12 Special Requirements for Compromised Private-Keys

None.

4.9.13 Conditions for a Suspension

Certificate suspensions are not offered.

4.9.14 Eligibility for Suspension

Not applicable.

4.9.15 Suspension-Application Procedure

Not applicable.

4.9.16 Time-Limitation for Suspensions

Not applicable.

4.10 Status Monitoring Service for Certificate

4.10.1 Mechanics of the Status Monitoring Services

The status monitoring service is implemented through the Online Certificate Status Protocol. The service's reachability is noted in the form of a URL in the certificates themselves.

4.10.2 Availability of the Status Monitoring Service

The status monitoring service is permanently (24/7) available.

4.10.3 Optional Services

None.

4.11 Withdrawal from the Certification Service

The certificate's validity ends according to the date noted in the certificate. A revocation request by the subscriber or an authorized third party results in the CSP revoking the certificate.

4.12 Key-Recovery

Key recovery is possible for users when the certificate has been deleted, or lostin any other way.

4.12.1 ConditionsandProceduresforKey-Recovery

A web service will be set up where the user has to authenticate themselves with their [IDENT] certificate. This web service can be accessed through user's dashboard https://sign.rtrust.org/

After successful authentication the user can select and download the PKCS#12 file containing the certificate(s) – the file is password-protected by the password the user chose when applying. This logon to the web service can only be performed using the [IDENT] certificate. Alternatively, support can be contacted by means of the contact form available on https://rtrust.org/contact, and if the identity gets confirmed in a satisfactory manner,key-recovery will be made possible.

4.12.2 ConditionsandProceduresforSession-Key-Escrowand-Recovery

Session keys are not offered.

5. Non-Technical Security Provisions

Physical protection measures, procedures implemented by rTrust within the context of system protection for certificate issuance (hereinafter referred to as: the certification system), as well as verification procedures of this system, management and operational procedures in rTrust PKI shall be of an internal nature and the details thereof shall not be publicly disclosed.

5.1 Confidentiality

5.1.1 Physical access control

As a certificate issuance service provider, rTrust shall implement physical protection measures for the certification system with the aim of minimizing risks related to physical protection and in accordance with rTrust 's business policy and valid legislation.

- Electronic physical entry control system with log
- High security perimeter fencing around the entire data center park
- Documented distribution of keys to employees and colocation customers for colocation racks (each Client only for his rack)
- Policies for accompanying and designating guests in the building
- Staff present 24/7
- Video monitoring at entrances and exits; security door interlocking systems and server rooms
- For people outside of the employment of Hetzner Online GmbH (data center visitors), entrance to the building is only permitted in the company of a Hetzner Online employee.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.1.2 Monitoring

- Electronic physical access control with log
- Video surveillance for all entrances and exits

Those conditions shall be carried out in accordance with Hetzner Document [13].

5.1.3 Electronic Access Control

For dedicated root server, colocation server, cloud server and storage box principal commissions:

- server passwords, which, after the initial deployment, can only be changed by Client and are not known to the Supplier
- the Client's password for the administration interface is determined by the Client himself; the password must comply with predefined guidelines. In addition, the Client may employ two-factor authentication to further secure his account.

For managed server, web hosting and storage share principal commissions:

- access is password-protected and only employees of the Supplier have access to the passwords. Passwords must meet a minimum length, and new passwords shall be changed on a regular basis.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.1.4 Internal Access Control

For the Supplier's internal administration systems:

- the Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
- a revision-proof, compulsory process for allocating authorization for Supplier employees

For dedicated root server, colocation server, cloud server and storage box principal commissions the responsibility for access control is incumbent upon the Client.

For managed server, web hosting and storage share principal commissions:

- the Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
- a revision-proof, compulsory process for allocating authorization for Supplier employees

- only the Client is responsible for transferred data/software with regard to security and updates.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.1.5 Transfer Control

- Drives that were in operation on canceled servers will be swiped multiple times (deleted) in accordance with data protection policies upon termination of the contract. After thorough testing, the swiped drives will be reused.

- Defective drives that cannot be securely deleted shall be destroyed (shredded) directly in the Falkenstein data center.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.1.6 Isolation control

For the Supplier's internal administration systems:

- data shall be physically or logically isolated and saved separately from other data

- backups of data shall also be performed using a similar system of physical or logical isolation

For dedicated root server, colocation server and storage box server principal commissions the client is responsible for isolation control

For managed server, web hosting and storage share principal commissions:

- data shall be physically or logically isolated and saved separately from other data.

- backups of data shall also be performed using a similar system of physical or logical isolation.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.2 Integrity

5.2.1 Data transfer control

- All employees are trained in accordance with Art. 32 Para. 4 GDPR and are obliged to ensure that personal data is handled in accordance with data protection regulations.
- Deletion of data in accordance with data protection regulations after termination of the contract.
- Encrypted data transmission options are provided within the scope of the service description of the principal commission.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.2.2 Data entry control

For the Supplier's internal administration systems:

- data is entered or collected by the Client
- changes in data are logged

For dedicated root server, colocation server and storage box server principal commissions the responsibility for input control is incumbent upon the client.

For managed server, web hosting and storage share principal commissions:

- data is entered or collected by the client
- changes in data are logged

Those conditions shall be carried as stated in Hetzner Policy Document [13].

5.3 Availability and Resilience

5.3.1 Availability Control

For the Supplier's internal administration systems:

- backup and recovery concept with daily backups of all relevant data

- professional employment of security programs (virus scanners, firewalls, encryption programs, spam filters)
- employment of disk mirroring on all relevant servers
- monitoring of all relevant servers
- employment of an uninterruptible power supply system or emergency power supply system
- permanently active DDoS protection

For dedicated root server, colocation server and storage box server principal commissions:

- data backup is incumbent upon the client
- employment of an uninterruptible power supply system or emergency power supply system
- permanently active DDoS protection

For managed sever, web hosting and storage share principal commissions:

- backup and recovery concept with daily backups of all relevant data depending upon the services booked for principal commission
- employment of disk mirroring
- employment of an uniterruptible power supply system or emergencypower supply system
- employment of software firewalls and restricted ports
- permanently active DDoS protection

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.3.2 Rapid recovery measures

- For all internal systems, there is a defined escalation chain which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.

Those conditions shall be carried as stated in the Hetzner Policy Document [13].

5.3.3 Training requirement

Employees carrying out tasks within rTrust PKI shall be provided with education and training in accordance with their trusted roles.

5.3.4 Retaining frequency and requirements

Awareness about IT security shall be conducted once annually for all rTrust PKI employees.

Education employees with trusted roles in rTrust PKI shall be carried out once annually with the aim of acquiring new knowledge and skills training.

Renewal of knowledge of rTrust RA Network employees, given the jobs they perform, shall be conducted regularly, at least once every two years.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Non-abidance of stipulated measures for authorised persons when working in rTrust PKI shall be subject to breach of work obligations, while possible penalties shall be determined through disciplinary proceedings.

In the event of unauthorised actions by external contractors, the provisions defined in the agreement with the external contractors shall apply.

5.3.7 Documentation supplied to personnel

The documentation required for the implementation of their work tasks according to the trusted role assigned and pertaining authorisations shall be supplied to each employee.

5.3.8 Vulnerability assessments

rTrust shall carryout regular risk assessments of IT assets, vulnerability assessments for recognized public and private addresses and penetration testing.

Risk assessment of IT assets shall be conducted once annually. rTrust PKIshall carryout vulnerability assessments of the system for recognised public and private addresses quarterly. Penetration tests shall be carried out once annually.

5.4 Key Changeover

rTrust shall ensure that rTrust CA continually provides trust services with its valid key pair and corresponding CA certificate. For this reason rTrust CA shall generate a new CA key pair sufficiently before the expiry of the CA certificate. Furthermore, rTrust CA shall generate a new CA key pair sufficiently earlier, even in the case when this change shall be required due to the level of security of cryptographic algorithms of the private CA key in use. In both cases, for a new public CA key, rTrust Root CA shall issue a CA certificate.

rTrust CA shall notify the participants of rTrust PKI about changes to its public key and new CA certificate in a timely manner.

5.5 Compromise and Disaster Recovery

5.5.1 Incident and compromise handling procedures

The business continuity plan for rTrust PKI shall regulate the procedures in the event of the occurrence of incidents or system compromise, which encompass procedures for system recovery and the establishment of security terms and conditions for providing certificate issuance services.

The business continuity plan shall be revised once annually.

5.5.2 Computing resources, software and/or data are corrupted

rTrust 's certification system was founded on reliable hardware and software components, while critical operations of the system shall be supported by redundant components.

Functionality, proper operation and timely elimination of damaged components of the certification system shall be secured through support and maintenance agreements with equipment suppliers.

The business continuity plan for rTrust PKI, shall regulate the procedure for recovery of the certification system in the event of malfunctions or damage to equipment and network resources and the return of data.

5.5.3 Entity private key compromise procedures

In the event that the private key of rTrust Issuing CA shall be compromised, the corresponding CA certificate shall be revoked by rTrust Root CA.

rTrust shall notify the following participants of rTrust PKI about the revocation of rTrust CA certificates:

- rTrust RA Network and External RAs,
- Subscribers,
- Relying parties.

After determining and eliminating the cause responsible for CA key compromise, rTrust shall if appropriate, undertake measures to prevent the recurrence of such an event. rTrust CA whose certificate has been revokedshall generate a new CA key pair. rTrust Root CA shall issue a new CA certificate for a new public CA key.

rTrust CA shall, by using the new private CA key, issue certificates to existing registered Subjects, and all subsequent information about revocation of certificates shall be signed using the new key. The new CA certificate shall be accessible to rTrust PKI participants in the same way as the previous CA certificate, and in accordance with the description in Section 2.2 of this Certificate Policy.

If the cryptographic algorithms and parameters used cease to provide the required security and protection, rTrust will, if possible, notify in due time:

- rTrust RA network and external RAs,
- Subscribers,
- Relying parties.

rTrust will consider using other appropriate recommended secure cryptographic algorithms and, if possible, make a decision about using another algorithm. rTrust will develop specific plans and procedures that will necessarily include the implementation of the revocation of all certificates that are affected by cryptographic algorithms and parameters whose security is compromised. About rTrust 's plans and deadlines will inform Subscribersand Relying parties.

5.6 Procedural Control

UKITES BY PBC LIMITED, SLOTES, follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the membersof the staff and of the satisfactory performance of their duties in the fields of theelectronic signature-related technologies.

The company obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

UKITES BY PBC LIMITED, SLOTES, conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determinetheir trustworthiness and competence.

Where dual control is required at least two trusted members of the company staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

5.7 Personnel Security Controls

5.7.1 Qualifications, experience and clearances

UKITES BY PBC LIMITED, SLOTES, through its subcontracted company PBC LLC in Prishtina, perform checks to establish the background, qualifications and experience needed to perform within the competence context of the specific job.

5.7.2 Training, requirements and procedures

UKITES BY PBC LIMITED, SLOTES, makes available training for their personnel to carry out their functions.

5.7.3 Retraining period and retraining procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.7.4 Sanctions against personnel

UKITES BY PBC LIMITED, SLOTES, sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate underthe circumstances.

5.7.5 Controls of independent contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as UKITES BY PBC LIMITED, SLOTES, personnel.

5.7.6 Documentation for training and retraining

UKITES BY PBC LIMITED, SLOTES, make available documentation to personnel, during initial training, retraining, or otherwise.

5.8 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment.

UKITES BY PBC LIMITED, SLOTES, implements the following controls:

The company audit records events that include but are not limited to

- Issuance of a certificate.
- Revocation of a certificate.
- Publishing of a CRL.

Audit trail records contain:

- The identification of the operation.
- The data and time of the operation.
- The identification of the certificate, involved in the operation.
- The identification of the person that performed the operation.
- A reference to the request of the operation.
- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

The company ensures that designated personnel review log files at regular intervals and detect and report anomalous events. Log files and audit trails are archived for inspection by the authorized personnel of UKITES BY PBC LIMITED, SLOTES. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up and must be available to independent auditors uponrequest.

6. Technical Security Provisions

This chapter shall describe protection measures undertaken with the aim of achieving the required level of security cryptographic key, activation data, critical security parameters, key management and other technical security measures for rTrust Issuing CAs, for rTrust OSCP services and for issuing subscribers certificates.

Subscribers and relying parties must only employ trustworthy computers and software.

6.1 Key Pair Generation

6.1.1 Key-pair generation

rTrust shall conduct generation for rTrust CA key pairs using algorithms for key generation in compliance with the standardized document ETSI TS 119312 [16].

6.1.2 rTrust CA Key Pair Generation

The procedure for generation of rTrust CA key pairs shall be carried out through a formal rTrust CA key pair generation ceremony for subordinated rTrust Issuing CAs.

The rTrust CA key pair generation ceremony shall be carried out following a key generation protocol documenting the steps performed during a ceremony. The protocol for key generation shall be in accordance with technical security measures according to the standard ETSI EN 319 411-1 [11] and with the requirements of CA/Browser Forum BRG [17].

The rTrust CA key pair generation ceremony procedure shall be video taped or the conducted procedure shall be witnessed by a Qualified auditor.

A transcript of the carried-out CA keys generation shall be recorded together with the attached audit logs.

rTrust shall possess the Qualified auditor's report witnessing that the rTrust CA key pair generation procedure has been carried out in compliance with the protocol and requirements for key generation.

6.1.3 Subscriber key pair generation for NCP certificates

Key pairs for the following certificates types issued by rTrust CA shall be generated by software modules:

- Individuals certificate
- Business certificate

In the event that the operator carries out key pair generation, the generation shall be carried out at the location of the Business Entity. Generating a key pair for the certificate application level 2 (NCP) is carried out in a controlled environment at the location of a business entity.

6.1.4 Private key delivery to subscriber

rTrust shall ensure the secure online delivery of a private key and corresponding certificate in software protected token to the Signatory or operator.

6.1.5 CA public key delivery to Relying parties

Public keys of rTrust Issuing CAs shall be accessible to Relying parties in rTrust CA certificates issued by rTrust Root CA. Hash of the rTrust RootCA certificate shall be delivered through trusted channel.

6.1.6 Key sizes

The key sizes in rTrust shall be as follows:

- rTrust Root CA shall use sha512WithRSA algorithm with 4096-bitlong keys,
- Subordinated rTrust Issuing CAs shall use sha256WithRSAalgorithm with 4096-bit long key,
- rTrust OCSP service shall use 2048-bit long RSA key,
- RA Network shall use 2048-bit long RSA key,
- Subscribers shall use 2048-bit long RSA key pairs.

6.1.7 Public key parameters generation and quality checking

rTrust shall carryout key pair generation using generation parameters in compliance with the standardized document ETSI TS 119 312 [16].

6.1.8 Key usage purposes (as per X.509 v3 key usage field)

Below follows a description of the purpose of key certificates within the scope of this Certificate Policy.

The rTrust CA certificate in the extension Key Usage shall have the set values keyCertSign and cRLSign. rTrust CA shall only use the corresponding private key for signing the corresponding CRL

6.2 Private Key Protection and Cryptographic Module EngineeringControls

6.2.1 Private key escrow

Private key escrow of rTrust Issuing CAs private keys shall not be applied. It is

not allowed to escrow private key associated with unqualified certificates.

6.2.2 Private key archival

rTrust shall not archive rTrust PKI private keys and shall not archiveSubcribers private keys.

6.2.3 Other aspects of activation data

Activation data for the private keys of Subscriber certificates may beperiodically modified to minimize the possibility of their disclosure.

This Certificate Policy shall not set any additional requirements on the life cycleof activation data of Subscriber certificates.

Additional rules about the terms and conditions, and life cycle of a Subject's activation data shall be specified in the Subscriber agreement.

6.3 Computer Security Controls

6.3.1 Specific computer security technical requirements

Only authorized persons after authentication shall have access to the IT systems and appliactions in rTrust PKI.

For all accounts that may directly initiate certificate issuance, two-factor authentication shall be necessary.

Modifications to and publication of the revocation status of certificates shall be carried out with two-factor authentication and mandatory control of access.

The rTrust PKI system shall carryout continuous monitoring and shall have a detection system for the purpose of detecting, recording and timely reactionto attempts at unauthorised access to system resources.

6.3.2 Computer Security Rating

With the aim of providing secure and quality trust service, rTrust has established an IT security management system in compliance with the standard ISO/IEC 27001[12].

6.4 Life Cycle Technical Controls

6.4.1 System development controls

When procuring development software from an external subcontractor, rTrust shall ensure the system development principles in the agreement with the supplier.

The analysis of security requirements shall be carried out in the design and specification phase of any development project of rTrust PKI systems, to ensure that security has been incorporated in information technology in rTrust PKI systems.

Software used to provide non-qualified certificate issuance services shall originate from a reliable source, and shall be approved by the person in charge of security in rTrust PKI. New versions of software shall be tested in a test environment. Implementation of software in production shall be carried out in accordance with documented procedures of change management.

6.4.2 Security management controls

rTrust shall carry out verification of all parts of the certification system in the rTrust production hierarchy, based on rTrust Root CA, with respect tosecurity, reliability and quality of operation.

In the event of a breach in certification system security or loss of its integrity which may have a significant impact on the provision of trust services or on the protection of personal data, rTrust shall within 24 hours notify the centralstate administration authority competent for economic affairs about this, as the authority competent for supervision of Trust Service Providers, and if necessary other competent authorities. In the event that the loss of integrity may have a negative impact on the Subscribers of rTrust trust services, rTrust shall

immediately notify all Natural persons citizens and Business Entities that may be impacted by the security breach thereof.

6.4.3 Life cycle security controls

rTrust shall carry out change management in rTrust PKI to ensure thatchanges occur for justified reasons, and in a controlled and formalised way.

The integrity of the certification and information systems shall be protected by antivirus protection and the use of authorised software.

Monitoring of available certification system capacities shall be carried out, and the compliance of existing capacities for future needs of the system shall be assessed to plan their expansion in a timely manner.

7. Profiles of Certificates, CRLs and OCSP

7.1 Certificate Profiles

Certificates issued by rTrust Issuing CAs comply with the stipulations detailed in the standards ITU [9] and IETF [6], as well as to the Common PKI 2.0 Co-PKI [3] Co-PKI pattern. Moreover, rTrust certificates are also eIDAS [4]compliant.

7.1.1 Version number(s)

Certificates shall be compliant with version 3 according to the X.509 [9] specification.

7.1.2 Certificate extensions

The document with a description of the certificate profile shall be available on the website of rTrust PKI repository to in Section 2.2 hereof.

7.1.3 Algorithm Object Identifier (OID)

Algorithms with pertaining OID identifiers for all certificates issued by subordinated rTrust Issuing CAs shall be shown in Table 3:

Algorithm	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Table 3: Algorithm pertaining OID identifiers

7.1.4 Name forms

Name forms for rTrust Root CAs are described in Section 1.3.2 of this Certificate Policy.

Names forms for certificates issued by subordinated rTrust Issuing CAs are described in Sections 3.1.1 and 3.1.4 of this Certificate Policy.

7.1.5 Name constraints

The extensions Name Constraints shall not be used.

7.1.6 Usage of policy constraints extension

The extension Policy Constraints shall not be used.

7.1.7 Policy qualifiers syntax and semantics

Policy qualifiers in the extension Certificate Policies shall contain two pointers in the form of a URI that contain the internet address of the Certification Practice Statement for Non-Qualified Certificates in English.

7.1.8 Processing semantics for the critical Certificate Policy extensions

No stipulations.

7.2 CRL Profiles

The issued CRLs conform to the stipulations detailed in the standards ITU [9] and IETF [6], as well as to the Common-PKI 2.0 Co-PKI [3] Co-PKI pattern.

7.2.1 Version number(s)

CRL shall be compliant with version 2 according to the X.509 specification.

7.2.2 CRL and CRL entry extensions

CRL extensions used in CRL lists and extensions used in entry elements of CRLs that are issued by rTrust Issuing CAs are defined in Table 4.

Extensions	Critical	Value
CRL Extensions		
CRL Number	NO	Monotonically increasing sequence number for CRL in the form of 20 octets.
AuthorityKeyIdentifier	NO	160 bits SHA1 hash
Reason Code	NO	Reason for the certificate revocation

Table 4: CRL and CRL Entry Extensions

7.3 Status Monitoring Service (OCSP) Profile

The status monitoring service conforms to the standard RFC 2560 [5] and fulfils the pattern requirements of Common PKI 2.0 Co-PKI[3] Co-PKI.

The CSP provides an online certificate status-monitoring-service (OCSP) through which the revocation status of every certificate in rTrust may be checked. The address for the OCSP-service (http://pki.rtrust.org/ejbca/publicweb/status/ocsp) is part of the certificate information

The rTrust OCSP service responders OCSP profile shall be in accordance with version 1 according to IETF RFC 6960 [15].

8. Verifications and other Assessments

Each CA within rTrust must design its processes in such a manner that they comply with this CP and its CPS. rTrust is entitled to review all processes of this CP and its CPS as well as its downstream CAs and RAs for compliance with the corresponding CP and CPS every year. (A conformity review can also be carried out by third parties.) Also the security concept of rTrust has to be reviewed.

Review results are documented and presented to the management of rTrust, but not published as a rule.

Defects detected must be eliminated in consultation between the management of rTrust and the UKITES BY PBC LIMITED, SLOTES as soon as possible.

9. Other Financial and Legal Regulations

9.1 Prices

rTrust shall reserve the right to price changes. Amendments to the price listshall be published on the website of the rTrust.

9.2 Financial Responsibilities

rTrust, as part of UKITES BY PBC LIMITED, SLOTES, shall possess financial stability and shall have at its disposal sufficient financial resources to ensure unhindered provision of certification services in accordance with this Certificate Policy.

UKITES BY PBC LIMITED, SLOTES, shall additionally insure property by means of an insurance policy coveringinsurance against the risk of fire, severe weather, floods, explosions, vehicle impact, aircraft fall or impact, demonstrations, insurance of equipment, machinery, electronic and communication devices, installations etc.

9.3 Confidentiality of Business Data

9.3.1 Definition of Confidential Business Data

The confidentiality of information may be agreed upon, in as much as it is not already defined by established law.

9.3.2 Non-confidential Business Data

All information that is contained explicitly (e.g., e-mail address) or implicitly (e.g., data on the certification) in the certificates and revocation lists issued or which can be derived therefrom is classified as non-confidential.

9.3.3 Responsibilities for the Protection of Confidential Business Data

The CSPs appointed employees are bound to secrecy through organizational measures within the limits of the applicable law.

9.4 Privacy of Personal Data

9.4.1 Data-Privacy Concept

The CAs and RAs must electronically store and process personal data for the provision of services. This must take place in compliance with the applicable laws.

9.4.2 Definition of Personal Data

As defined by Kosovar Law on the Protection of Personal Data, no.2010/03-L-172.

9.4.3 Non-Confidential Data

Information that is explicitly integrated into certificates, CRLs and status information is not considered confidential.

9.4.4 Responsibilities for the Protection of Privacy

The CSP ensures data protection. Every CSP employee is contractually compelled to adhere to the data protection rules. Internally, the adherence is supervised by the operational data security engineer.

9.4.5 Indication and Acquiescence for the Utilization of Personal Data

Upon application, the applicant is shown which personal data will be included in the certificate. Certificates will only be published after the applicant has given his consent during the application process.

Upon application, the applicant is informed that the RA only collects data that is necessary for the certificate creation and the operation of rTrust. He is additionally informed that his personal data is protected against third-party access, as per law, and that his data will only be passed on if the CSP is legally compelled to do so.

9.4.6 Data-Disclosure Following Legal or Governmental Directives

All CAs operating within rTrust are subject to the law of the Republic of Kosovo and must release confidential and personal information to government bodies in compliance with the applicable laws if corresponding decisions have been made.

9.4.7 Other Conditions for Data-Disclosure

Data is not disclosed for any other reasons than those described in section 9.4.6.

9.5 Industrial Trademark- and Copyrights

rTrust is a registered trademark of UKITES BY PBC LIMITED, SLOTES.

9.5.1 Intellectual Property Right

UKITES BY PBC LIMITED, SLOTES, owns and reserves all intellectual property rights associated with its databases, web sites, company certificates and any other publication whatsoever originating from UKITES BY PBC LIMITED, SLOTES including this CPS.

The distinguished names in use across UKITES BY PBC LIMITED, SLOTES, remain the sole property ofcompany, which enforces these rights.

Certificates are and remain property of UKITES BY PBC LIMITED, SLOTES. The company permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directorywithout the express written permission of the company. The scope of this restriction is also intended to protect subscribers against the unauthorized re- publication of their personal data featured on a certificate.

UKITES BY PBC LIMITED, SLOTES, owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Assurances and Guarantees

9.6.1 CSP Range of Services

The general terms and conditions apply. Insofar guarantees are not explicitly assured in this CP, the CSP grants no guarantees or assurances in the legal sense.

The CSP operates Registration Authorities (RA). The RA identifies and registers. The general terms and conditions, as well as the regulations in this CP apply.

9.6.2 Subscriber Confirmations and Guarantees

The general terms and conditions, as well as this CP apply.

9.6.3 Relying parties Confirmations and Guarantees

Confirmations and guarantees of the relying parties are not regulated in this CP. The CSP and the relying parties do not incur a contractual relationship. Apart from that, the general terms and conditions, as well as legal requirements apply.

9.7 Non-Liability

9.7.1 CSPs exclusion of liability

The general terms and conditions apply.

9.8 Limitation of Liability

The general legal terms and conditions apply as per ID cards.

9.9 Compensation

9.9.1 CSP Claims towards Applicants/Subscribers

If the applicant gives the RA fraudulent information, the CSP can claim compensation according to legal regulations.

9.9.2 Subscriber Claims towards the CSP

The general terms and conditions apply.

9.10 CP Validity Period and Expiration

This CP is valid from the date of publication and remains valid as long as certificates that have been issued on the basis of this CP remain valid.

9.11 Individual Announcements for and Agreements with PKI-participants

Not applicable.

9.12 Addendums

Addendums (if used) to this CP are incorporated into this document and published under the same OID.

9.13 Dispute-Mediation Regulations

Complaints regarding the fulfillment of this CP need to be submitted to the CSP in writing to UKITES BY PBC LIMITED, SLOTES, Kotnikova Ulica 5, 1000 Ljubljana, Slovenia, www.rTrust.org. If no redress has occurred within 5 weeks after the complaint has been filed, the following applies: Disputes may be addressed through legal action according to Slovenian law.

9.14 Competent Court of Jurisdiction

The general terms and conditions apply.

9.15 Abidance of Applicable Law

This CP is subject to the laws of the Republic of Slovenia.

9.16 Miscellaneous Regulations

9.16.1 Letter of Representation

All regulations contained in this CP or its CPS apply between a CA that operates within rTrust and its subscribers. The publication of a new version replaces all previous versions.

Verbal agreement or side agreements are not permitted.

9.16.2 Delimitations

Not applicable.

9.16.3 Severability Clause

If a regulation of this CP or its application is found null and void or not feasible for any reason and in any scope, the rest of the CP (as well as the application of the non-feasible or voided regulation in regard to other individuals or other circumstances) should be interpreted in such a way, that the agendas of the affected parties are taken into account to the maximum possible degree.

9.16.4 Enforcement (Attorney Fees and Waiver of Appeal)

Legal disputes resulting from the operation of a CA that operates within rTrust are subject to the laws of the Republic of Slovenia.

9.16.5 Acts of God

The general terms and conditions apply.

9.17 Other Regulations

9.17.1 Conflicting Regulations

The regulations under 9.16.1 are conclusive. They apply in the order as listed in 9.16.1.

9.17.2 Complying with Export Laws and -Regulations

The usage of the UKITES BY PBC LIMITED, SLOTES, public certification services is subject to multiple laws of the Republic of Slovenia. For any case of noncompliance with the public certification services, UKITES BY PBC LIMITED, SLOTES, reserves the right of filing charges for criminal prosecution.

UKITES by pbc
The way IT works

Well-known as the
House of Innovations and Optimizations with real competitive advantages

More than 500 bespoke SaaS platforms have been developed by more than 100 in-house software engineers, with an almost 100% satisfaction rate.