Certificate Policy & Certification Practice Statement
(CP/CPS) for Qualified Certificates
for electronic signatures and electronic seals

KIBSTrust Verba

Version: 2.0

Effective Date: 15.11.2024

111.01

OID 1.3.6.1.4.1.16305.1.1.5.

KIBS Certificate Policy & Certification Practices Statement for Qualified certificates for electronic signatures and electronic seals

Trademark Notices

Version history

version	date	author	цел на промената
2.0	15.11.2024	Kristina Radomirovikj Isidora Martinovska	Changes according to new issuing certificates from generation G3 and changes in end user certificate profiles. Changes in the following chapters: 1.3.1, 7.1, 7.3
1.0	01.04.2021	Policy Management Authority	New document. Certificate Policy & Certification Practice Statement for Qualified Certificates for electronic signatures and electronic seals in the hierarchy of **KIBSTrust Root CA G2** according to the requirements of MK-eIDAS and eIDAS.

Table of Contents

1. INTRODUCTION

This document is the KIBS Certificate Policy & Certification Practices Statement (CP/CPS) for Qualified Certificates. It states the practices that KIBS as Trusted Service Provider (TSP) employs in providing certification services for Qualified Certificates for electronic signatures and Qualified Certificates for electronic seals in accordance, but not limited to Articles 24, 29, 38, 39, 40, 55 of the MK-eIDAS[1] and Articles 19, 24, 26, 27, 28, 36, 37, 38 and 45 of Regulation (EU) N° 910/2014 (eIDAS)[2].

Qualified Certificates for electronic signatures may be issued either on a Local Qualified Signature Creation Device (Local QSCD) or a Remote QSCD. Qualified Certificates for electronic seals may be issued either on a Local QSCD or a Remote QSCD.

This document establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing Certificates and providing associated trust services. These requirements apply to all the Certification Authorities (CA), Registration Authorities (RA), Subscribers, Relying Parties, and other PKI entities that interoperate with KIBS's PKI.

This document describes the practices that KIBS employs for:

- Securely managing the related infrastructure that supports KIBS's PKI, and
- Issuing, maintenance, managing, revoking and renewing (life cycle management) of Qualified Certificates as defined in MK-eIDAS and Regulation (EU) N° 910/2014.

This CP/CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

1.1. Overview

This CP/CPS describes the practices and procedures used to address all the requirements identified by MK-eIDAS and Regulation (EU) N° 910/2014, for issuing, maintenance and lifecycle management of Qualified Certificates for electronic signatures and Qualified Certificates for electronic seals.

These practices and procedures are compliant with:

- ETSI EN 319 411-2 Policies:
  - QCP-n / QCP-n-qscd for Qualified Certificates for electronic signatures; and
  - QCP-l / QCP-l-qscd for Qualified Certificates for electronic seals,

KIBS has established a secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates. KIBS acts as a CA under umbrella of registered trademark KIBSTrust. KIBSTrust performs all Certificate lifecycle services of issuing, managing, revoking, and renewing Qualified Certificates.

This CP/CPS is specifically applicable to KIBS's Issuing CAs, who issue Qualified Certificates for electronic signatures and electronic seals.

Private CAs and other hierarchies that are managed by KIBS or services provided by KIBS to other Organizations are also within the scope of this CP/CPS. The practices relating to services provided by other Organizations are beyond the scope of this CP/CPS.

KIBS publishes this CP/CPS to comply with the specific policy requirements of the applicable legislation, or other industry standards and requirements.

The CP/CPS is only one of a set of documents relevant to KIBS's Trust Services. These other documents include:

- Ancillary confidential security and operational documents that supplement the CP/CPS by providing more detailed requirements, such as:

[1] Law for electronic documents, electronic identification, and trusted services (Official Gazette of Republic of North Macedonia 101/19, 215/19)

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

- Key Ceremony Reference Guide, which presents detailed key management operational requirements.
- KIBS Cryptographic Key Management Policy, which presents detailed key management operational requirements.
- The KIBS Physical Security Policy which sets forth security principles governing KIBS infrastructure,
- The KIBS Information System Security Policy that states the requirements for Information System infrastructure in order to operate securely and according to relative legislative and contractual requirements.

(Although these documents are not publicly available, their specifications are included in KIBS's Conformity Assessment Report and may be made available under special agreement)

- KIBS Terms and Conditions for the Use of Qualified Trust Services. These Terms and Conditions bind Customers, Subscribers and Relying Parties with a broad range of commercial and other specific terms or KIBS Trust Services.

In many instances, the CP/CPS refers to these ancillary documents for specific, detailed practices implementing KIBS Policies where including the specifics in the CP/CPS could compromise the security of KIBS's CA.

KIBS also offers Web Site certificates (Secure Server IDs).

Web Site Certificates are offered by KIBS in a special cooperation with third party Trusted service providers and not under KIBS CA. For this line of business KIBS shall apply to the terms and conditions of this third party Trusted service providers.

1.2. Document name and Identification

This document is the KIBS Certificate Policy & Certification Practice Statement for Qualified Certificates. KIBS has assigned this CP/CPS the following object identifier (OID) value.

1.3.6.1.4.1.16305.1.1.5

1.3.6.1.4.1.16305	Identification Number (OID) of KIBS, registered to IANA
1.3.6.1.4.1.16305.1	Trust Service Provider
1.3.6.1.4.1.16305.1.1	Qualified Certificate Policies
1.3.6.1.4.1.16305.1.1.5	Applicable and current version of the CP/CPS

The applicable and current CP/CPS (OID) shall be inserted by reference within each and every Certificate Policy ruled by the KIBS CP/CPS.

1.3. PKI Participants

1.3.1. Certification Authorities

The authority trusted by the users of the certification services (i.e. Subscribers as well as Relying parties) to create and assign certificates, is called the Certification Authority (CA). The CA has overall responsibility for the provision of the certification services.

KIBS is currently using the following certificate hierarchy:

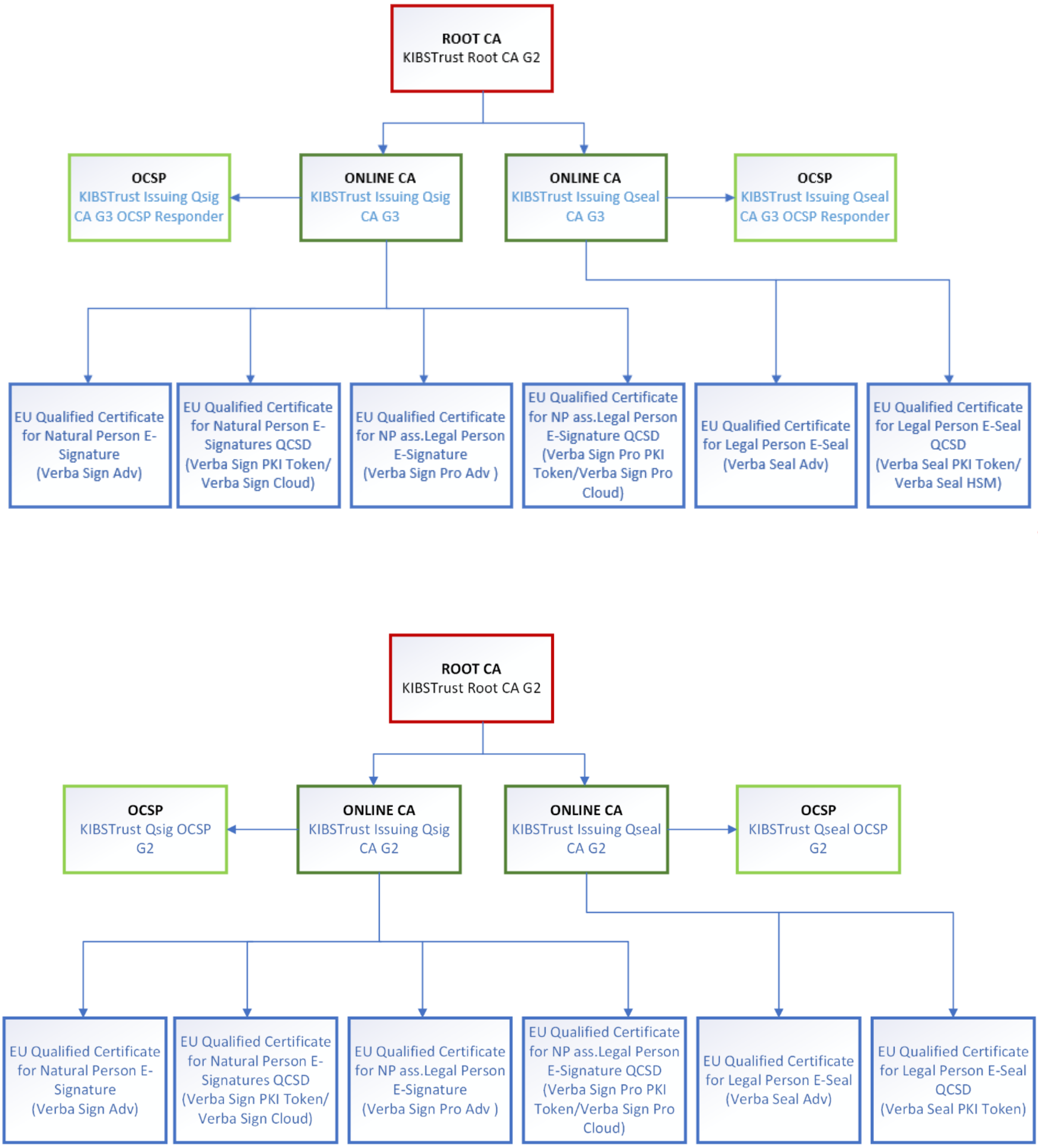
ROOT CA
KIBSTrust Root CA G2
OCSP
KIBSTrust Issuing Qsig CA G3 OCSP Responder
ONLINE CA
KIBSTrust Issuing Qsig CA G3
ONLINE CA
KIBSTrust Issuing Qseal CA G3
OCSP
KIBSTrust Issuing Qseal CA G3 OCSP Responder
EU Qualified Certificate for Natural Person E-Signature (Verba Sign Adv)
EU Qualified Certificate for Natural Person E-Signatures QCSD (Verba Sign PKI Token/ Verba Sign Cloud)
EU Qualified Certificate for NP ass.Legal Person E-Signature (Verba Sign Pro Adv)
EU Qualified Certificate for NP ass.Legal Person E-Signature QCSD (Verba Sign Pro PKI Token/Verba Sign Pro Cloud)
EU Qualified Certificate for Legal Person E-Seal (Verba Seal Adv)
EU Qualified Certificate for Legal Person E-Seal QCSD (Verba Seal PKI Token/ Verba Seal HSM)
ROOT CA
KIBSTrust Root CA G2
OCSP
KIBSTrust Qsig OCSP G2
ONLINE CA
KIBSTrust Issuing Qsig CA G2
ONLINE CA
KIBSTrust Issuing Qseal CA G2
OCSP
KIBSTrust Qseal OCSP G2
EU Qualified Certificate for Natural Person E-Signature (Verba Sign Adv)
EU Qualified Certificate for Natural Person E-Signatures QCSD (Verba Sign PKI Token/ Verba Sign Cloud)
EU Qualified Certificate for NP ass.Legal Person E-Signature (Verba Sign Pro Adv)
EU Qualified Certificate for NP ass.Legal Person E-Signature QCSD (Verba Sign Pro PKI Token/Verba Sign Pro Cloud)
EU Qualified Certificate for Legal Person E-Seal (Verba Seal Adv)
EU Qualified Certificate for Legal Person E-Seal QCSD (Verba Seal PKI Token)

Figure 1 Certificate hierarchy

This CA hierarchy is constituted by the following entities:

List of Root CAs

#	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	**CN** = KIBSTrust Root CA G2 **O** = KIBS AD Skopje **2.5.4.97** = NTRMK-5529581 **OU** = KIBSTrust Services **C** = MK	9E0D33A6B826F84030A8110 11E92217731C40CD28DBC23 37931286D8A4951235

List of Issuing CAs

#	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	**CN** = KIBSTrust Issuing Qsig CA G3 **2.5.4.97** = NTRMK-5529581 **OU** = KIBSTrust Services **O** = KIBS AD Skopje **C** = MK	410CF3BEFD8B711C1AE 06AB81778CC3F85B7D BE9BEC4F19F9EB38E97 554DB1E2
2	**CN =** KIBSTrust Issuing Qseal CA G3 **2.5.4.97 =** NTRMK-5529581 **OU =** KIBSTrust Services **O =** KIBS AD Skopje **C =** MK	B3EADB5037E5C6785D E190D3061F296848C61 7AECAB006BA6A057E5 F1DB0FC0C
3	**CN** = KIBSTrust Issuing Qsig CA G2 **2.5.4.97** = NTRMK-5529581 **OU** = KIBSTrust Services **O** = KIBS AD Skopje **C** = MK	C2F8EAF1ECF16467782 23B45D1DEFDF67932A 8352CC8303176DF5F4B 627D2B41
4	**CN =** KIBSTrust Issuing Qseal CA G2 **2.5.4.97 =** NTRMK-5529581 **OU =** KIBSTrust Services **O =** KIBS AD Skopje **C =** MK	086ABDC02F432448654 36EF125141DA731F7B3 EABCABEBA8531FF2FA7 AAECF65

1.3.2. Registration Authorities

A Registration Authority (RA) is an entity that performs identification and validation of Subscribers for issuing certificates, initiates or passes along revocation requests for Certificates and approves applications for re-keying certificates on behalf of the CA. KIBS act as an RA for the Qualified Certificates it issues.

KIBS may enter into a contractual relationship with one or more third parties, in order to outsource part or all of RA responsibilities. In this case, the third party becomes KIBS's RA and performs its responsibilities in full compliance with this CP/CPS, the respective validation plans, and the terms of the RA Agreement signed between RA and KIBS.

Validation of the email address cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

KIBS trains RA's authorized employees on validation process and security procedures, prior starting RA's related operations and performs yearly re-training thereafter.

KIBS performs yearly audits to the RA operations and procedures in order to ensure compliance with this CP/CPS, the validation plans and the RA Agreement (If RA is outsourcing company).

1.3.3. Local Registration Authorities

A Local Registration Authority (or LRA) is an entity that performs the identification and validation of Subscribers and Subjects and the initial examination of their respective documents for the issuance, re-keying and revocation of Certificates.

KIBS may enter a contractual relationship with one or more third parties, to outsource part of RA responsibilities, especially regarding the validation of the Subscriber. In this case, the third party constitutes a LRA. LRA performs its responsibilities in full compliance with this CP/CPS, the respective Validation plans and the terms of the LRA Agreement signed between LRA and KIBS.

The relationship between KIBS, LRA and RA is described in the LRA's contract agreement and includes, but not limited, the following:

- Full details of LRA's authorized employees, that will perform LRA's duties and activities;
- LRA's obligation to receive yearly training of LRA's authorized employees from KIBS regarding LRA's duties and activities and to accept yearly audits by KIBS regarding LRA operations and procedures;
- LRA's authorized employee's obligation to use credentials issued by KIBS RA to ensure secure communications between both parties;
- LRA's obligation to process Subscriber's applications exclusively through LRA's authorized employees.

Local Registration Authority is responsible for delivering the Qualified Signature Creation Device (QSCD) or authentication credentials in case of Remote Qualified Certificate to the Subscriber or Subject.

LRA passes all Subscriber's applications or requests accompanied by the related documents to the Registration Authority for approval or rejection of Certificate issuance, re- keying, or revocation.

KIBS trains LRA's authorized employees on validation process and security procedures, prior starting LRA's related operations and performs yearly re-training thereafter.

KIBS performs yearly audits to the LRA operations and procedures to ensure compliance with this CP/CPS, the Validation Plans and the LRA Agreement

1.3.4. Subscribers

Two different terms are used in this CP/CPS to distinguish between these two roles:

- "**Subscriber**" is the entity, which contracts with KIBS for the issuance of credentials, and;
- "**Subject**" is the person to whom the credential is bound.

The Subscriber bears ultimate responsibility for the use of the credential, but the Subject is the individual that is authenticated when the credential is presented.

The Subscriber means a natural or legal person to whom KIBS provides the Trust Services according to this CP/CPS.

The **Subject** means:

- a natural person
- a natural person who is identified in association with a legal person
- a legal person

The **Subscriber** may or may not be the Subject of a certificate. The link between the subscriber and the subject is one of the following:

- To request a certificate for natural person the subscriber is:

  a) the natural person itself;

b) a natural person mandated to represent the subject; or
c) any entity with which the natural person is associated.

- To request a certificate for legal person the subscriber is:

a) any entity as allowed under the relevant legal system to represent the legal person; or
b) a legal representative of a legal person subscribing for its subsidiaries or units or departments.

1.3.5. Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the CA. A Relying party may or may not also be a Subscriber. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate.

1.3.6. Other Participants

Other Participants include:

- The KIBS Policy Management Authority (PMA) which is responsible for amendments to this CP/CPS.
- The company "ADACOM S.A." with which KIBS had signed an agreement, having in mind that ADACOM is a QTSP that is properly audited under the eIDAS regulation and complies with the requirements of Article 20 of Regulation (EU) 910/2014 (eIDAS). Under this agreement KIBS outsourced need of facilities, trustworthy systems, and procedures for generating, keeping secure, and providing other parts of the life cycle of KIBS's Root and Issuing Certificates (KIBS CA's) to ADACOM.

  Upon this agreement, KIBS accepts that in frame of this CP/CPS, facilities, ADACOM's systems and procedures are referred as its own.

1.4. Certificate Usage

A digital Certificate is formatted data that cryptographically binds an identified Subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1. Appropriate Certificate Usage

1.4.1.1. Certificates Issued for electronic signature

Qualified Certificates for electronic signatures are normally used by individuals to sign electronic documents, to sign email messages and for authentication purposes, provided that the usage is not otherwise prohibited by law, by this CP/CPS, the Terms and Conditions, and any other agreements with Subscribers.

Certificates are compliant with QCP-n and QCP-n-qscd.

Certificates issued under these requirements are aimed to support qualified electronic signatures with the use of a Qualified Signature Creation Device (QSCD) such as defined in article 3 (29) of MK-eIDAS and article 3 (12) of the eIDAS and advanced electronic signatures without the use of a Qualified Signature Creation Device (QSCD) such as defined in article 3 (28) of MK-eIDAS and article 3 (11) of the eIDAS.

1.4.1.2. Certificates Issued for electronic seals

Qualified Certificates for electronic seal is normally used to ensure the integrity and the origin of that data to which it is linked, or for other purposes, provided that the usage is not otherwise prohibited by law, by this CP/CPS, the Terms and Conditions, and any other agreements with Subscribers.

Certificates are compliant with QCP-l and QCP-l-qscd.

Certificates issued under these requirements are aimed to support qualified electronic seals with the use of a Qualified Signature Creation Device (QSCD) such as defined in article 3 (33) of MK-eIDAS and article 3 (27) of the Regulation (EU) N° 910/2014 and advanced electronic seals without the use of a QSCD such as defined in article 3 (32) of MK-eIDAS and article 3 (26) of the Regulation (EU) N° 910/2014.

1.4.2. Prohibited Certificate Usage

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

CA Certificates may not be used for any functions except CA functions. In addition, Subscriber Certificates shall not be used as CA Certificates. Usage of Certificates, other than to support applications identified in Section 1.4.1 of the present CP/CPS, is prohibited.

Relying Parties shall use the KIBS Certificate Policy OIDs as identified in the Certificate to appropriately accept or reject a Certificate usage.

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CP/CPS and the relevant documents referenced herein are maintained by the KIBS Policy Management Authority (PMA), which can be contacted at:

KIBS AD Skopje
Kuzman Josifovski Pitu 1,
1000, Skopje, Republic of North Macedonia
tel. +389 2 5513401, +389 2 3297401
E-mail: pma@kibstrust.com

1.5.2. Contact Person

PKI Policy Manager
KIBS AD Skopje
Kuzman Josifovski Pitu 1,
1000, Skopje, Republic of North Macedonia
tel. +389 2 5513401, +389 2 3297401
E-mail: pma@kibstrust.com

1.5.2.1. Revocation contact person

For Certificate revocation requests, refer to Section 4.9.3.

1.5.3. Person Determining CP/CPS Suitability for the Policy

The KIBS Policy Management Authority (PMA) determines the suitability and applicability of this CP/CPS based on the results and recommendations from compliance audits.

1.5.4. CP/CPS Approval Procedure

Approval of this CP/CPS and subsequent amendments are made by the PMA. Amendments are either in the form of a document containing an amended form of the CP/CPS or an update notice. Amended versions or updates are linked to the Practices Updates and Notices section of the KIBS Repository located at:

https://www.kibstrust.com/repository/cps.

Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS. The PMA shall determine whether changes to the CP/CPS require a change in the Certificate policy object identifiers of the Certificate policies.

Even if there is no compulsory reason for a change in this CP/CPS, the PMA performs a review process at least annually in an effort for improvement.

1.6. Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

KIBS is responsible for the repository functions for its own CAs. KIBS publishes the issued end-user Subscriber's Certificates in the repository in accordance with Section 2.2.

Upon revocation of a Subscriber's Certificate, KIBS publishes notice of such revocation in the repository and issues Certificate Revocation List (CRL) and provides OCSP services pursuant to the provisions of this CP/CPS.

KIBS shall ensure that its repository is available 24 hours a day, 7 days a week, with a minimum of 99,00% availability overall per year with a scheduled down-time that does not exceed 0,4% annually.

Upon system failure, service or other factors which are not under the control of KIBS, KIBS shall apply best endeavors to ensure that this information service is not unavailable for longer than above time.

2.2. Publication of Certificate Information

KIBS maintains a web-based repository in a public data communications network (https://pki.kibstrust.com/repository) that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. KIBS provides Relying Parties with information on how to find the appropriate repository to check Certificate status and how to find the right OCSP responder.

KIBS publishes in its public information repository at least the following information:

- Overview of the certification hierarchy,
- Certificate practice statement,
- Audit results,
- Insurance Policies,
- Certification policies,
- Certificates, including root and issuing CAs
- Certificate Profiles,
- Terms and Conditions for use of Qualified Trust Services,
- Certificate Revocation Lists
- Certificate search
- Privacy Policy.

2.2.1. Publication and Notification Policies

This KIBS CP/CPS is published in KIBS's public information repository:

https://www.kibstrust.com/repository/CPS

KIBS CP/CPS is published along with the enforcement dates no less than 10 days prior taking effect.

2.2.2. Items not published in the Certification Practice Statement

Refer to Section 9.3.1 of this CP/CPS.

2.3. Time or Frequency of Publication

Certificate status information is published in accordance with the provisions of this CP/CPS.

Refer to Section 2.2.1 of current CP/CPS for updates to this CP/CPS. Updates to Terms and Conditions are published as necessary. Certificates are published upon issuance.

2.4. Access Controls on Repositories

Information published in the repository portion of the KIBS web site is publicly accessible information. Read only access to such information is unrestricted. KIBS requires persons to agree to the Terms and Conditions as a condition to accessing Certificates, Certificate status information, or CRLs. KIBS has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries according to the applicable KIBS security policies. KIBS makes its repository publicly available in a read only manner, and specifically at the link https://pki.kibstrust.com/repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

Naming in certificates are as specified in Recommendation ITU-T X.509 or IETF RFC 5280 and the appropriate part of ETSI EN 319 412.

3.1.1. Type of Names

Type of names assigned to the CA and to the Subscriber is described in the relevant Certificate Profile documentation published in KIBS's repository.

KIBS CA and Subscriber Certificates contain X.501 Distinguished Names in the Issuer and Subject fields.

3.1.2. Need for Names to be Meaningful

Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual that is the Subject of the Certificate.

KIBS CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3. Anonymity or pseudonymity of Subscribers

The use of anonymity or pseudonymity is not permitted.

3.1.4. Rules for Interpreting Various Name Forms

Fields contained in Digital Certificates are in compliance with this CP/CPS and the Digital Certificate Profiles detailed in Section 7. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

RFC-822 names may be used as Alternate Subject Names by indicating the e-mail address of the Certificate Subject.

3.1.5. Uniqueness of Names

KIBS ensures that Subject Distinguished Names (DN) of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the similar Subject Distinguished Name.

The uniqueness of the Distinguished Name for electronic signatures and authentication is ensured by the Serial Number attribute value in the Subject field of the certificate. For electronic seals it is ensured by the Organizational Identifier attribute value in the Subject field of the certificate.

3.1.6. Recognition, Authentication, and Role of Trademarks

Certificate applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual property rights of others. KIBS, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrates, mediates, or otherwise resolves any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. KIBS is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2. Initial Identity Validation/Authentication

KIBS may use methods described in this Section to ascertain the identity of a Subscriber. KIBS may refuse to issue a Certificate at its sole discretion if identity validation is not successful.

Identity validation is part of the process of the certificate application, certificate issuance and device provisioning.

3.2.1. Method to Prove Possession of Private Key

The key generation process is ensured by this CP/CSP in compliance with the ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 technical standards.

The Certificate applicant must demonstrate that he/she rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration or another approved method by KIBS. This requirement does not apply where a key pair is generated by KIBS on behalf of a Subscriber, for example where pre-generated keys are placed on a QSCD.

For Qualified Certificates associated with private keys in a Qualified Signature/Seal Creation Device (QSCD):

- In the case of a Local QSCD, Private Keys are generated and stored on the Local QSCD. Generation of private keys can be in the presence of the certificate holder (in case of face-to-face recognition) or without presence of the certificate holder (in case of remote recognition). The certificate holder is responsible for securing the Local QSCD with a out of band given Personal Identification Number (PIN) for accessing QSCD.
- In the case of a Remote QSCD, Private Keys are generated and stored under the control of the Certificate Holder on a Hardware Security Module that is located in a KIBS data center. Access by the Certificate Holder to the keys is protected using multifactor authentication aimed to achieve the same level of assurance of sole control as achieved by a Local QSCD.

3.2.2. Authentication of Organization identity (Legal Person)

3.2.2.1. Legal person’s identity verification

The legal person’s identity who is the Subscriber of an Qualified Certificate is verified pursuant to current legislation is performed in one of the following ways :

To issue a certificate, it is necessary to identify the subscriber – **legal person** and **the legal representative** (items 1 and 2):

1) Confirmation of the **subscriber's** identity (legal person) is performed in one of the following ways:
    - For a legal person registered in Macedonia, the data entered for the legal person in the Purchase Order and Agreement form are cross-checked with the data for that legal person stored in register of legal entities and other entities maintained by the Central Register Republic of North Macedonia, including the legal representative name.
    - For a legal person registered outside Macedonia, it is necessary to bring the evidence from a trade register or a similar body that has the right to confirm that the subscriber is registered as a legal person in the domicile country including the name of legal representative. The certificate is submitted in the original document, and the document translated by court sworn translator into Macedonian or English language.
2) Confirmation of the identity of the **legal person’s representative**

- who **sign by hand** the Purchase Order and Agreement form is performed as follows:
    - For a legal person registered in Macedonia, a notarized certified copy of the Certified signature form (ZP form) is attached, on which the handwritten signature of the legal representative is registered, or
    - For a legal person registered outside Macedonia: by submitting the appropriate form, where the connection of a bank account with the handwritten signature of the legal representative has been certified, or
    - The legal representative signs Purchase Order and Agreement form in front of a public notary. Public notary will certify this
    - The legal representative shows a personal identification document and signs Purchase Order and Agreement form in front of an LRA/RA officials.

- who **digitally sign** the Purchase Order and Agreement form with Qualified Certificate for electronic signature or electronic seal issued by a Qualified Trust Service Provider, which validates the Legal Representative's identity,

In case of a third person to apply for the issuance of the Qualified Certificate, copy of power of attorney from the legal representative to that third person or any other equivalent document, which shows that the third person is able to sign on behalf of the legal representative have to be showen.

3.2.3. Authentication of Individual Identity (Natural Person)

3.2.3.1. Natural person identity verification

The natural person's identity who is the Subscriber and the Subject of an Qualified Certificate is verified pursuant to current legislation, is performed in one of the following ways:

- With the physical presence of the Subscriber in LRA/RA of KIBS CA, at the address published on https://www.kibstrust.com/en-GB/Home/Contact/, where they:
  - shows a personal identification document (ID card or passport),
  - signs the Purchase Order and Agreement form in front of LRA/RA official.
- If the subscriber is not able to come in person to the LRA/RA of KIBS CA he/she must personally go to a notary public and in front of the notary public to sign the Purchase Order and Agreement form for which the notary public will make a notary certification,
- Remotely, by means of using Qualified Certificate for electronic signature issued by a Qualified Trust Service Provider, which validates the personal identity, or
- by Remote ID verification, equivalent to physical presence, by which the natural person is identified through a liveness detection session managed automatically or by an authorized LRA/RA employee.

The natural person shall provide acceptable identification documents: National ID Card for resident of Republic of North Macedonia, temporary ID Card for foreign citizen with temporary residence in Republic of North Macedonia, foreign citizens ID Card for citizens from countries that Government of Republic of North Macedonia accept as legal travel document and passport for all citizens. Identity document includes a unique number assigned to the applicant by the above-mentioned identity document issuing country.

3.2.3.2. Natural person associated with legal person identity verification

In case of a natural person who is the Subject of a Qualified Certificate associated with a legal person who is the Subscriber :

1. by the physical presence of the natural person associated with legal person (Subject) and legal person's representative, in LRA/RA of KIBS CA, at the address published on https://www.kibstrust.com/en-GB/Home/Contact/, who submits to an KIBS's RA or an LRA's authorized employee the following documents:
   - Proof of the Subject's and legal person's representative identity [full name, date and place of birth] on the basis of a National ID Card for resident of Republic of North Macedonia, temporary ID Card for foreign citizen with temporary residence in Republic of North Macedonia, foreign citizens ID Card for citizens from countries that Government of Republic of North Macedonia accept as legal travel document and passport for all citizens, given that the document includes a unique number assigned to the applicant by the above mentioned identity document issuing country.
   - Written and dully signed Purchase Order and Agreement form, by the legal person's representative and the natural person that the subject attributes also identify such organization.
2. If the Subject and legal person's representative are not able to come in person to the LRA/RA of KIBS CA they must personally go to a notary public and in front of the notary public to sign the Purchase Order and Agreement form for which the notary public will make a notary certification. The documents are delivered to KIBS's RA by the physical presence of a dully authorized representative of the Subscriber provided that the representative is duly mandated by the Subscriber to represent him/her.

3. Remotely, by means of using Qualified Certificate for electronic signature or electronic seal issued by a Qualified Trust Service Provider, which validates the Legal Representative's identity, and by sending all the documents listed in paragraph 1 above via email to KIBS's RA/LRA.
4. By Remote ID verification, equivalent to physical presence of the natural person associated with legal person (Subject) and legal person's representative. Remote ID verification is based on National ID Card for resident of Republic of North Macedonia, temporary ID Card for foreign citizen with temporary residence in Republic of North Macedonia, foreign citizens ID Card for citizens from countries that Government of Republic of North Macedonia accept. Online created Purchase Order and Agreement form must be accepted by the natural person and legal person's representative.

3.2.3.3. Domain e-mail validation

KIBS verifies a Subscriber's right to use or control an email address to be contained in a Certificate by sending an approval email message to the email address to be included in the Certificate.

3.2.4. Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU) attributes
- Any other information designated as non-verified in the Certificate (like "Title" addressing job position).

3.2.5. Validation of Authority

Whenever a natural person's name is associated with an legal person's name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the legal person.

KIBS RA:

- determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, when appropriate, his/her authority to act on behalf of the Organization.

3.2.6. Criteria of Interoperation

Not applicable.

3.3. Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. KIBS generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

Please refer to Sections 3.2.2 and 3.2.3 of this CP/CPS.

In addition, all documents required can be sent electronically digitally signed by an existing Qualified Certificate for electronic signatures.

3.3.1. Identification and Authentication for Routine Re-key

Not applicable.

3.3.2. Identification and Authentication for Re-key After Revocation

Subscriber must undergo the initial registration process as per Sections 3.2.2 and 3.2.3 of this CP/CPS.

3.4. Identification and Authentication for Revocation Request

RA authenticates all revocation requests.

Prior to the revocation of a Certificate, RA verifies that the revocation has been requested by the Certificate's Subscriber or the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include one or more of the following:

- Having the Subscriber submit the Subscriber's Challenge Phrase, and revoking the Certificate automatically if it matches the Challenge Phrase on record.
- The Subscriber signs paper based revocation form of the request for revocation.
- The Subscriber submit electronic revocation form via KIBS web portal authenticate as registered user with additional security level provided by two-factor authentication.
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked.
- Communication with the Subscriber providing reasonable assurances, ensuring that the person or organization requesting revocation is, in fact the Subscriber or has the dully authorization to do so. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

KIBS RA Administrators are entitled to request the revocation of Certificates within KIBS's domain. KIBS authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Application for Qualified Certificate may submit the natural (physical) person or legal person, who is the Subscriber of the Certificate, if they are legally eligible. Applicants are responsible for any data that the Applicant or any authorized person by the Applicant supplies to KIBS.

4.1.2. Enrollment Process and Responsibilities

All Certificate Subscribers shall manifest assent to the relevant Terms and Conditions that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- Accept the Terms and Conditions regarding the use of the certificate
- Completing and signing a Certificate Purchase Order and Agreement form by providing true and correct information in accordance with the requirements of this policy.
- Provide relevant validation documents.
- Generating or arranging to have a key pair generated.
- Receiving his, her, or its certificate, directly or through the RA / LRA.
- Demonstrating possession and/or exclusive control of the private key corresponding to the public key.
- Paying any applicable fees if required.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

KIBS performs identification and authentication of all required Subscriber information either:

a) by physical presence,
b) remotely by means of a Qualified Certificate, or
c) by using a method equivalent to physical presence in accordance with Section 3.2.

If an LRA/RA assists in the verification, the LRA/RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to KIBS. After verification is complete, KIBS evaluates the information and decides whether to issue the Certificate.

As part of this evaluation, KIBS RA may check the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

4.2.2. Approval or Rejection of Certificate Applications

KIBS approves an application for a certificate only if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2,
- Payment has been received.

KIBS rejects a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request,
- The Subscriber fails to respond to notices within a specified time,
- Payment has not been received, or
- KIBS believes that issuing a certificate to the Subscriber may bring KIBS into disrepute.

In case KIBS rejects a certificate for application related to a Remote QSCD, the relevant Subscriber account is not created, and no other actions are required from Subscriber.

4.2.3. Time to Process Certificate Applications

KIBS begins processing certificate applications within a reasonable time upon receiving complete documentation. A certificate application remains active until is rejected, issued, or automatically expired in 30 days. The expired certificate's Purchase Order and Agreement forms are automatically deleted from KIBS's user's database.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application (Purchase Order and Agreement form) by KIBS based on information that the Purchase Order and Agreement form contains.

Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

KIBS notifies Subscribers that the Certificates have been created and provides Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates are made available to Subscribers, by informing them via an e-mail message or directly in premises of RA/LRA. Notification contains information how Subscriber can pick up certificate.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object, within 5 days, to the certificate or its content constitutes certificate acceptance.

4.4.2. Publication of the Certificate by the CA

KIBS publishes information about the Certificates it issues in a publicly accessible repository. The Subscriber has the right to choose whether the certificate information and the certificate itself will be published in a publicly accessible repository for issued KIBS IS certificates.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RAs and LRAs may receive notification of the issuance of certificates they approve.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate is only permitted once the Subscriber has agreed to the Terms and Conditions and accepted the certificate. The certificate shall be used lawfully in accordance with KIBS's Terms and Conditions, and this CP/CPS. Certificate usage must be consistent with the KeyUsage field extensions included in the certificate. Certificate key usage is of type B as specified in clause 4.3.2 of ETSI EN 319 412-2.

Subscribers shall maintain their private keys under their sole control, protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the KIBS Terms and Conditions as a condition of relying on the Certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CP/CPS. KIBS is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate.
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6. Certificate Renewal

Not applicable.

4.7. Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

4.7.1. Circumstances for Certificate Re-Key

Minimum 30 days prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to Re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2. Who May Request Certification of a New Public Key

Only the Subscriber may request Certificate re-keying.

4.7.3. Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

The Subscriber submits a digitally signed re-key application (with his existing valid certificate) to KIBS RA/LRA.

KIBS RA/LRA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements, as described in Section 3.3.

Other than this procedure or another KIBS-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4. Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6. Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in KIBS's publicly accessible repository.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

RAs and LRAs may receive notification of the issuance of Certificates they approve.

4.8. Certificate Modification

4.8.1. Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2. Who May Request Certificate Modification

See Section 4.1.1.

4.8.3. Processing Certificate Modification Requests

KIBS performs identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6. Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9. Certificate Revocation and Suspension

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, all revocation requests are authenticated as per Section 3.4.

Revocation of certificates is performed according to the following sections.

For certificates including email address, certificate revocation and suspension is compliant with CA/B Forum Requirements.

4.9.1. Circumstances for Revocation

The KIBS's Terms and Conditions provide the obligation and/or right of the Subscriber to request revocation of a Certificate. Only in the circumstances listed below, Subscriber Certificate will be revoked by KIBS (or by the Subscriber) and published on a CRL.

An Subscriber Certificate is revoked if:

- KIBS or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key. In case a compromise is reported by a third party, KIBS requires respective confirmation from the Subscriber;
- KIBS has reason to believe that the Subscriber has breached a material obligation, representation, or warranty under the applicable Terms and Conditions for Use of Qualified Trust Services;
- KIBS has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CP/CPS, was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate;
- KIBS is aware of changes which impact the validity of the certificate.
- The used cryptography is no longer ensuring the binding between the Subject and the public key.
- KIBS has reason to believe that a material fact in the Certificate Application is false,
- KIBS determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- Subscriber loses the legal eligibility, is declared in absence or death, taking into account that a certificate is nontransferable in any case;
- Subscriber loses ability to use the local QSCD or mobile device required to access a remote QSCD;
- In case the Subject of the Certificate is a natural person associated with the Subscriber- legal person and the Subscriber requires the revocation;
- A final court judgment requires the relevant revocation;
- The private key of the CA has been compromised;
- The Supervisory Body requests the revocation according to the law;
- The Subscriber identity has not been successfully re-verified;
- The Subscriber has not submitted payment, when due;
- The continued use of that certificate is harmful to KIBS;
- For Certificates including an email address, if they no longer comply with the requirements of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy.

When considering whether certificate usage is harmful to KIBS, KIBS considers, among other things, the following:

- The nature and number of complaints received,
- The identity of the complainant(s),
- Relevant legislation in force,
- Responses to the alleged harmful use from the Subscriber.

KIBS may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

KIBS Terms and Conditions require end-user Subscribers to immediately notify KIBS of a known or suspected compromise of its private key.

After the approving of a revocation request by the CA, the revoked certificate cannot be re-entered into force.

4.9.2. Who Can Request Revocation

Request for revocation of a Qualified Certificate may be submitted by:

- RA or LRA

- a natural or legal person, or their legal representatives, who is the Subscriber of the Certificate, or a successor who wishes to request revocation in case of a deceased Subscriber (natural person), provided that is legally eligible
- a competent court or authority
- the Supervisor Body

Request for revocation of a CA Certificate may be submitted by:

- a legal person, who is the Subscriber of the Certificate, provided that is legally eligible,
- a competent court or authority
- the Supervisor Body.

4.9.3. Procedure for Revocation Request

An Subscriber requesting revocation is required to communicate the request to the KIBS by: online procedure for revocation, e-mail at revoke@kibstrust.com or paper based form for revocation send to RA office, which in turn will initiate revocation of the certificate promptly.

Communication of such revocation request shall be in accordance with Section 3.4.

4.9.4. Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5. Time within which CA must process the Revocation Request

KIBS takes commercially reasonable steps to process revocation requests without delay and in any case the maximum delay from the time KIBS receives a revocation request in accordance with Section 4.9.3. and the decision to change its status information being available to all relying parties shall be at most 24 hours. If though the revocation request cannot be confirmed within 24 hours, then the status need not be changed.

Right after the approval of a revocation request, the CA informs the Subscriber and the Subject of the certificate for the revocation via e-mail for this event.

4.9.6. Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement by checking Certificate status using the KIBS web-based repository or by using OCSP. CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository or OCSP responder to check for revocation status. Due to the numerous and varying locations for CRL repositories, relying parties are advised to access CRLs using the URL(s) embedded in a certificate’s CRL Distribution Points extension.

The proper OCSP responder for a given certificate is placed in its Authority Information Access extension.

Revocation status information shall be made available beyond the validity period of the certificate.

4.9.7. CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once daily. CRLs for CA Certificates are issued at least annually, but also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate’s expiration.

4.9.8. Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9. On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository an OCSP. In addition to publishing CRLs, KIBS provides Certificate status information through query functions in the KIBS repository. Certificate status information for Qualified Certificates is available KIBS Repository at:

https://pki.kibstrust.com/repository OCSP responses are provided within a commercially reasonable time after the request is received, subject to transmission latencies over the Internet. OCSP responses conform to RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp- nocheck, as defined by RFC 6960.

The maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the status information of this certificate being made available to relying parties is at most 60 minutes. If though the revocation request requires revocation in advance (e.g. Subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time.

4.9.10. On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the KIBS repository or by requesting Certificate status using the applicable OCSP responder.

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements regarding Key Compromise

KIBS uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of its own CAs.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate’s validity period. OCSP information for subscriber Certificates is updated as per Section 4.9.9.

4.10.2. Service Availability

KIBS ensures the availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.4% annually.

4.10.3. Optional Features

Not applicable.

4.11. End of Subscription

A subscriber may end a subscription for a KIBS Qualified Certificate by:

- Allowing his/her/its Qualified Certificate to expire without re-keying that Certificate,
- Revoking of Qualified Certificate before certificate expiration without replacing it.

4.12. Key Escrow and Recovery

Not applicable.

4.12.1. Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

KIBS has implemented a set of Security Policies, which supports the security requirements of this CP/CPS. Compliance with these policies is included in KIBS's audit requirements described in Section 8. The KIBS Security Policies contain sensitive security information and is only available upon agreement with KIBS. An overview of the requirements is described below.

5.1.1. Site Location and Construction

KIBS CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, prevents, access to, or disclosure of sensitive information and systems whether covert or overt.

KIBS also maintains disaster recovery facility for its CA operations. KIBS's Disaster Recovery facilities are protected by multiple tiers of physical security comparable to those of KIBS's primary facility.

5.1.2. Physical Access

KIBS systems are protected by five (5) tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged, and video recorded. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes tiers for key management security which serves to protect both online and offline storage of Cryptographic Signing Unit (CSUs) and keying material. Areas used to create, and store cryptographic material enforce dual control, each through the concurrent use of proximity cards and biometrics. Online CSUs are protected using locked cabinets. Offline CSUs are protected using locked safes, cabinets, and containers. Access to CSUs and keying material is restricted in accordance with KIBS's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers are logged for audit purposes.

KIBS RA operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system.

Access card logs and video records are reviewed on a regular basis. KIBS securely stores all removable media and paper containing sensitive plain-text information related to its RA operations in secure containers.

KIBS securely stores the Cryptographic Signing Units (CSU) used to generate and store the Subscribers Private Keys for remote signature. Access to the rooms used for key storage and key generation activities is controlled and logged by the building access card system. Access card logs and video records are reviewed on a regular basis.

5.1.3. Power and Air Conditioning

KIBS's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power, and
- heating / ventilation / air conditioning systems to control temperature and relative humidity.

5.1.4. Water Exposures

KIBS has taken reasonable precautions to minimize the impact of water exposure to its systems.

5.1.5. Fire Prevention and Protection

KIBS have taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6. Media Storage

All media containing production software and data, audit, archive, or backup information is stored within KIBS's facilities and in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire).

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with KIBS's normal waste disposal requirements.

5.1.8. Off-Site Backup

KIBS perform routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a secure off-site Disaster Recovery facility in accordance with KIBS's "Continuous operation plan".

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted Persons include all employees that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications,
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information,
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository,
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,

- RA/LRA personal,
- cryptographic business operations personnel,
- security personnel,
- internal auditors,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

KIBS considers the categories of personnel identified in this Section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CP/CPS.

The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

Contractors and consultants that have access to or control authentication or cryptographic operations can conduct these operations only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.2.2. Number of Persons Required per Task

KIBS has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

The validation and issuance of Qualified Certificates require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process.

5.2.3. Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing KIBS HR or security functions and a check of well-recognized forms of identification (e.g., passports and identification cards). Identity is further confirmed through the background checking procedures in Section 5.3.2.

KIBS ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities,
- issued electronic credentials to access and perform specific functions on KIBS, RA, or other IT systems.

KIBS has implemented an access control system, which identifies authorities and registers all the KIBS information system users in a trustworthy manner.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with dedicated account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use.

User accounts are locked as soon as possible when the role change dictates. Access rules are audited annually.

5.2.4. Roles Requiring Separation of Duties

Roles requiring Separation of duties include but are not limited to those performing:

- the validation of information in Certificate Applications,
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information,
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository,
- the generation, issuing or destruction of a CA certificate;
- the loading of a CA to a Production environment.
- the access to the Remote QSCD
- backups, recording, and record keeping functions;
- audit, review, oversight, or reconciliation functions.

To accomplish this separation of duties, KIBS designates individuals to the trusted roles, restricting an employee from assuming multiple roles, and thus preventing an employee from having more than one identity.

5.3. Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1. Qualifications, Experience and Clearance Requirements

KIBS requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities, as specified in the employment contract, job description and Roles and Responsibilities documents, competently and satisfactorily as well as proof of any government clearances, if any, necessary to perform certification services under government contracts, before they perform any operational or security functions.

The employment contracts signed by the employees of KIBS provide for the following obligations:

- To maintain the secrecy of confidential information that has come to their knowledge during their performance,
- To prevent them from holding business interests in a company, which may affect their judgment in the supply of the service and - to ensure that they have not been punished for a willful crime.
- All personnel in Trusted Roles are free from any interests that may affect their impartiality regarding KIBS operations.

5.3.2. Background Check Procedures

Prior to commencement of employment in a Trusted Role, KIBS conducts background checks which include the following:

- Verification of identity,
- Check of previous employment and professional reference (if available),
- Confirmation of the highest or most relevant educational degree obtained,
- Search of national criminal records,
- Check of financial records.

To the extent that any of the requirements imposed by this Section cannot be met due to a prohibition or limitation in local law or other circumstances, KIBS will utilize a substitute investigative technique permitted by law that provides substantially similar information.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for acting against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,

- Highly unfavorable or unreliable professional references,
- Certain criminal convictions.
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action considering the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable laws.

5.3.3. Training Requirements

KIBS provides its personnel with training upon hire or the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. KIBS maintains records of such training. KIBS periodically reviews and enhances its training programs, as necessary.

KIBS’s training programs are tailored to the individual’s responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- KIBS security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling,
- Disaster recovery and business continuity procedures.

5.3.4. Retraining Frequency and Requirements

KIBS provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5. Job Rotation Frequency and Sequence

No rotation used.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for employees and agents failing to comply with this CP/CPS, unauthorized actions or other violations of KIBS policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7. Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a KIBS employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in Section 5.3.2 are permitted access to KIBS ’s secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8. Documentation Supplied to Personnel

KIBS provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily, including a copy of this CP/CPS and other technical and operational documentation needed to maintain the integrity of KIBS's CA operations. Employees are also given access to information on internal systems and security documentation, identity verification procedures and other relevant information.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

KIBS ensures that all relevant information concerning the operation of the Trust Services is recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of the Trust Service operation.
KIBS manually or automatically logs the following significant events:

- CA certificate and key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction,
  - Changes to CA details or keys.
  - Cryptographic device life cycle management events.
- Subscriber certificate and key life cycle management events, including:
  - Certificate Applications, issuance, re-key, and revocation,
  - Key generation, backup, storage, recovery, archival, and destruction,
  - Successful or unsuccessful processing of requests,
  - Changes to certificate creation policies,
  - Generation and issuance of Certificates and CRLs.
- Trusted Employee Events, including:
  - Logon and logoff attempts,
  - Attempts to create, remove, set passwords or change the system privileges of any privileged users,
  - Personnel changes
- All significant security-related events including:
  - Successful and unsuccessful PKI system access attempts,
  - Start-up and shutdown of systems and applications,
  - Possession of activation data for CA private key operations,
  - PKI and security system actions performed by KIBS personnel,
  - Security sensitive files or records read, written or deleted,
  - Security policy settings changes,
  - System crashes, hardware failures and other anomalies,
  - Firewall and router activity,
  - CA facility visitor entry/exit.
  - Remote QSCD facility access entry/exit

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

KIBS RA and LRA log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant’s identification card number) of identification documents, if applicable. Storage location of copies of applications and identification documents for Qualified Certificates,
- Any specific choices in the Certificate Application,
- Identity of entity accepting the application and in case of Qualified e-Seals identity of the natural person representing the legal person to whom the Qualified Certificate for the electronic seal is provided,
- Method used to validate identification documents, if any,
- Name of receiving CA or submitting RA and LRA, if applicable..

5.4.2. Frequency of Processing Log

KIBS systems are continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

5.4.3. Retention Period for Audit Log

Audit logs shall be retained for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.

Physical or digital archive records about certificate applications, registration information and requests or applications for revocation are retained ten (10) years after any certificate based on these records ceases to be valid.

In case of CA termination KIBS audit logs and archive records are retained and accessible until abovementioned term for retention in accordance with Section 5.8.

The individuals who remove audit logs from KIBS's CA systems are different than the individuals who control signature keys.

5.4.4. Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5. Audit Log Backup Procedures

Incremental backups of audit logs are created daily, and full backups are performed weekly.

5.4.6. Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by KIBS personnel in Trusted Roles.

5.4.7. Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event unless such notice is compulsory according to the law.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons who have a legal right of access.

5.4.8. Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Vulnerability assessments are performed and reviewed annually in order to identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access.

KIBS also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that it has in place to control such risks. The Vulnerability Assessment and Risk Assessment are an input to KIBS's annual conformity assessment audit.

5.5. Records Archival

5.5.1. Types of Records Archived

KIBS archives:

- All audit data collected in terms of section 5.4,
- Certificate application information,
- Documentation supporting certificate applications,
- Certificate lifecycle information,
- Approval or rejection of a revocation request,
- CP and CP/CPS versions,

- Conformity assessment audit reports,
- KIBS Certifications,
- Appointment of an individual to a trusted role.

5.5.2. Retention Period for Archive

The retention period for archive is described in Section 5.4.3.

5.5.3. Protection of Archive

KIBS protects the archive so that only authorized Trusted Persons can obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP/CPS.

5.5.4. Archive Backup Procedures

KIBS incrementally backs up electronic archives daily and performs full backups on a weekly basis. Electronic copies of paper-based records are maintained on KIBS's off- site secure facility.

5.5.5. Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information is not cryptographic based.

5.5.6. Archive Collection System (Internal or External)

KIBS uses an internal archive collection system.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel can obtain access to the archive. The integrity of the information is verified when it is restored.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons who have a legal right of access.

5.6. Key Changeover

KIBS CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CP/CPS. KIBS CA Certificates may be renewed if the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs are generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Towards the end of a CA Private Key's lifetime, KIBS ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

Where KIBS has cross-certified another CA that is in the process of a key rollover, KIBS obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA cross Certificate following the procedures described above.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Backups of the following CA information are kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys are generated and maintained in accordance with this CP/CPS.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to KIBS's or ADACOM's Security and incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, key compromise or disaster recovery procedures will be enacted.

5.7.3. 5Entity Private Key Compromise Procedures

Upon the suspected or known compromise of a KIBS CA, KIBS follows the plan of actions as described within the Security Incident Management procedure.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the KIBS repository in accordance with Section 4.9.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected Participants, and
- The CA will generate a new key pair in accordance with Section 5.6, except where the CA is being terminated in accordance with Section 5.8.

This paragraph is also applicable in case PKI algorithms or associated parameters become insufficient for its remaining intended usage.

5.7.4. Business Continuity Capabilities after a Disaster

KIBS maintains a Business Continuity Plan (BCP) to establish procedures to recover the KIBS critical business functions following a disaster.

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - Notification/Activation phase to detect and assess damage and activate the plan.
  - Recovery phase to restore temporary IT operations and recover damage done to the original system.
- Identify the activities, resources, and procedures needed to carry out KIBS CA and Certificate functions during prolonged interruptions to normal operations.
- Assign responsibilities to designated KIBS personnel and provide guidance for recovering KIBS procedures during prolonged periods of interruption to normal operations.
- Ensure coordination with other KIBS staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

KIBS has the capability to restore or recover essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- Publication of revocation information.

ADACOM maintains redundant hardware and backups of its CA and infrastructure system software at its Disaster Recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with Section 6.2.4.

5.8. CA or RA Termination

The CA is terminated:

- with a decision of the KIBS's Board of Directors.
- with a decision of the authority exercising supervision over the supply of the service.
- with a judicial decision.
- Upon the liquidation or termination of the operations of KIBS.

KIBS ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of KIBS's services, and in particular, it ensures the continued maintenance of information required to verify the correctness of Trust Services.

If it is necessary for an KIBS CA, to cease operation, KIBS makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, where applicable, KIBS will transfer its obligations to another TSP and will activate the documented "KIBS Termination Plan" to minimize disruption to Customers, Subscribers, and Relying Parties. This termination plan may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by KIBS,
- The preservation of the CA's archives and records for the time periods required in this CP/CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and issuing CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key, including backup key, and the hardware tokens containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA where possible,
- Provision notice to relevant authorities such as supervisory bodies,
- Transfer of obligations to a reliable party for maintaining all information necessary to provide evidence of the Trust Services operation for a reasonable period, unless it can be demonstrated that KIBS does not hold such information,
- The submission of the KIBS CA's archives and records to another contracting Certification Service Provider for Qualified Certificates, for the time periods required by the law.

Upon termination of KIBS CA's operations, or termination of RA's services, for any reason, any contracts assigning part of the TSP responsibilities to third parties, i.e. outsourced Subscriber validation responsibilities to a Registration Authority, shall expire automatically. To this end, third parties shall secure the transfer of the records and documents related to the assigned responsibilities, according to applicable law.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained, and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for key generation meet the requirements of FIPS 140-2 level 3.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide. The activities performed in each key generation ceremony are recorded, dated, and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by KIBS Management.

Generation of end-user Subscriber key pairs is generally performed by KIBS's operator, using the card management software, in front of the Subscriber. on a QSCD certified cryptographic module compliant with eIDAS Regulation requirements.

For Remote Qualified Certificates, the generation of keys, their storage and subsequent use, is performed by KIBS using exclusively devices certified specifically in accordance with the applicable requirements per Article 30.3 of the eIDAS and, thus included in the list of qualified devices maintained by the European Commission in compliance with Articles 30, 31 and 39 of eIDAS. The above devices aimed to be managed on behalf of the signatory by a QTSP may be duly operated by a third QTSP in accordance with eIDAS Regulation (EU) 910/2014.

6.1.2. Private Key Delivery to Subscriber

When Subscriber key pairs are generated on QSCD by the Subscriber, private key delivery to a Subscriber is not applicable.

When Subscriber key pairs are pre-generated by KIBS on QSCD, such device is delivered to the Subscriber using a commercial registered mail delivery service. The data required to activate the device is communicated to Subscriber using an out of band process. The distribution of such devices is monitored by KIBS.

When Subscriber key pairs are generated on a remote QSCD by the Subscriber, private key delivery to the Subscriber is performed inside the remote QSCD.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers submit their public key to KIBS for certification electronically using a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where Subscriber key pairs are pre-generated by KIBS, this requirement is not applicable.

6.1.4. CA Public Key Delivery to Relying Parties

KIBS makes the Root and Issuing CA Certificates available to Subscribers and Relying Parties through its repository. KIBS generally provides its own full certificate chain (including the issuing CA and any CAs in the chain) to the Subscriber upon Certificate issuance.

Subscribers, during the certificate pick-up process, automatically download and install into their computer, the issuing CA's public keys. In any case if a user needs to verify and/or download the public key of the CA, he can do so by accessing the KIBS's web-based repository: https://pki.kibstrust.com/repository.

6.1.5. Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The KIBS Standard for minimum key sizes is the use of key pair equivalent in strength to 4096-bit RSA for CAs and 2048-bit RSA for RAs keys and Subscriber certificates.

Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 119 312, for signing Certificates, CRLs, and certificate status server responses.

All CAs and Subscriber certificates use SHA-256 for digital signature hash algorithm.

6.1.6. Public Key Parameters Generation and Quality Checking

The quality of Public Keys is guaranteed by using secure random number generation and onboard generation of Public Keys. Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 119 312.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to Section 7.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

KIBS has implemented a combination of physical, logical, and procedural controls to ensure the security of KIBS CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1. Cryptographic Module Standards and Controls

For CA key pair generation and CA private key storage, KIBS uses cryptographic modules that are certified at or meet the requirements of FIPS 140-2 Level 3.

Subscriber Private Keys are generated on QSCD compliant to eIDAS Regulation requirements.

KIBS monitors QSCD certification status until the end of the validity period of the certificate associated with the relevant QSCD. In case of a modification of the certification status of the QSCD, KIBS will stop issuing certificates on these devices.

6.2.2. Private Key (m out of n) Multi-Person Control

KIBS uses ADACOMs trustworthy services that incorporates technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. ADACOM uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is three (3). Secret Shares are protected in accordance with this CP/CPS.

6.2.3. Private Key Escrow

KIBS CA and end user’s private keys are not escrowed.

6.2.4. Private Key Backup

ADACOM creates backup copies of KIBS CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CP/CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CP/CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CP/CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CP/CPS.

ADACOM does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12.

6.2.5. Private Key Archival

Upon expiration of a KIBS CA Certificate, the key pair associated with the certificate is securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this and ADACOM’s CP/CPS. These CA key pairs are not used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of this CP/CPS.

KIBS does not archive copies of Subscriber private keys.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

ADACOM generates KIBS CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ADACOM makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7. Private Key Storage on Cryptographic Module

Private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8. Method of Activating Private Key

All KIBS Subscribers shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

The Subscriber Private Keys on Local QSCD are protected by PIN codes. The following rules apply:

- Subscriber needs to enter the PIN code to the QSCD for each transaction.
- Subscriber is obligated to change the PIN code prior the initial registration process
- In case the Subscriber enters a wrong PIN code 5 times in a row, the QSCD is blocked
- PIN can be unblocked using an admin PIN code only in RA
- The usage of admin PIN code will be blocked after 3 consecutive incorrect tries
- User can change the PIN code.

The Subscriber Private Keys on Remote QSCD are protected by username, password and OTP codes. The following rules apply:

- Subscriber needs to enter the username, password and OTP code to the QSCD for each transaction.
- In case the Subscriber enters a wrong username, password and OTP code 5 times in a row, the Remote QSCD account is locked
- Remote QSCD account cannot be password reset
- User can change the password.

An online CA’s private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA’s private key. Once the private key is activated, it shall be active only for one time.

6.2.9. Method of Deactivating Private Key

KIBS CA private keys are deactivated upon power off of the cryptographic module.

Subscriber private keys may be deactivated after each operation, upon logging off their system, upon removal of the Local QSCD from the system, or upon logging off of the Remote QSCD. In all cases, Subscribers have an obligation to adequately protect their private key(s) in accordance with this CP/CPS.

6.2.10. Method of Destroying Private Key

Where required, KIBS destroys CA and Subscriber private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. KIBS utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, key destruction activities are witnessed.

The Subscriber Private Keys of a Local QSCD can be destroyed by physically destroying or damaging the QSCD.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

KIBS CA certificates are backed up and archived according to agreement with ADACOM in its trustworthy services.

KIBS RA and end-user Subscriber Certificates are backed up and archived as part of KIBS ’s routine backup procedures.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum Operational Periods for KIBS Certificates for Certificates issued on or after the effective date of this CP/CPS are set forth in Table "Certificate Operational Periods" below.

Certificate Issued By:	Private Key Use	Validity Period
Root CA	No stipulation	Normally up to 20 years
Issuing CA	No stipulation	Normally up to 10 years
Long-lived Certificate	No stipulation	Normally 1-3 years

Table: Certificate Operational Periods

In addition, KIBS CAs stop issuing new Certificates at an appropriate date (60 days plus maximum validity period of issued Certificates) prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates. The lifetime of Subscriber's certificates will not exceed the lifetime of the CA's signing certificate

Subscribers shall cease all use of their key pairs after their usage periods have expired.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by the KIBS management.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Activation data (Secret Shares) used to protect HSM containing KIBS CA private keys are generated in accordance with the requirements of Section 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

Activation data used (PINs) to protect Local QSCD containing Subject's private keys are generated in accordance with the user manual of the QSCD.

– Where Subscriber key pairs are pre-generated by KIBS, activation data are delivered to the Subscriber using a commercial registered mail delivery service.
– Where Subscriber key pairs are generated by the Subscriber, pre-defined activation data must be changed immediately before the key generation. Activation data used (username, password and OTP code) to protect Remote QSCD containing Subject's private keys are generated in accordance with the compliance requirements of the QSCD.

Activation data used (username, password and OTP code) to protect Remote QSCD containing Subject's private keys are generated in accordance with the compliance requirements of the QSCD.
KIBS will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

6.4.2. Activation Data Protection

KIBS protects data used to unlock Private Keys from disclosure using a combination of control mechanisms. KIBS Shareholders are required to safeguard their Secret Shares and remote QSCD Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

KIBS personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. Subscribers are also instructed to memorize their activation credentials (PIN, PUK, username, password, OTP) and not share them with anyone else.

KIBS enforces multi-factor authentication for all accounts capable of causing certificate issuance or performing Registration Authority or delegated third party functions, or implement technical controls operated by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.

6.4.3. Other Aspects of Activation Data

6.4.3.1. Activation Data Transmission

To the extent activation data for private keys are transmitted, Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3.2. Activation Data Destruction

Activation data for CA private keys are decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, KIBS destroys activation data by overwriting and/or physical destruction.

6.5. Computer Security Controls

KIBS performs all CA and RA functions using Trustworthy Systems that meet the requirements of KIBS's Information Security Management System (ISMS).

6.5.1. Specific Computer Security Technical Requirements

KIBS ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, KIBS limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

KIBS's production network is logically separated from other components. This separation prevents network access except through defined application processes. KIBS uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

All critical software components are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorized software.

KIBS personnel are authenticated before using critical applications related to the services. User accounts are created for personnel in specific roles that need access to the system in question. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

KIBS requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. KIBS requires that passwords be changed on a periodic basis.

Direct access to KIBS databases supporting KIBS's CA Operations is limited to Trusted Persons in KIBS's Production Operations group having a valid business reason for such access.

The KIBS certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All media containing production environment software and data, audit, archive, or backup information are stored within KIBS with appropriate physical and logical access controls. Media containing Sensitive Information are securely disposed of when no longer required.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

RAs must ensure that the systems maintaining software and data files are trustworthy systems, secure from unauthorized access and logically separated from other components. RAs must use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information.

6.5.2. Computer Security Rating

Not applicable.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

KIBS software goes through secure development procedures before being published to the production environment.

New versions of software are developed and implemented in accordance to change management procedure.

6.6.2. Security Management Controls

KIBS has mechanisms and/or policies in place to control and monitor the configuration of its CA systems.

KIBS follows the network security guidelines of Section 7.8 of ETSI EN 319 401. KIBS also follows the security guidelines of "Network and Certificate System Security Requirements" of the CA/Browser Forum.

Upon installation and periodically thereafter, KIBS validates the integrity of its CA systems. Only the software directly used for performing the tasks is used in the information system.

6.6.3. Life Cycle Security Controls

KIBS policies and assets are reviewed at planned intervals, or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

The configurations of KIBS systems are checked at least annually for changes that violate the KIBS security policies. Changes that have an impact on the level of security provided are reviewed by the Security Officer and approved by the Management.

KIBS has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

KIBS manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment.

6.7. Network Security Controls

KIBS performs all its CA and RA functions using networks secured in accordance with the KIBS ISMS to prevent unauthorized access and other malicious activity. KIBS protects its communications of sensitive information through the use of encryption and digital signatures.

The security level of the internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

KIBS performs a vulnerability assessment periodically on public and private IP addresses as long as penetration tests on the certification systems.

6.8. Time-Stamping

Certificates, CRLs, and other revocation database entries contain time and date information.

The system time on KIBSs computers is updated using the Network Time Protocol (NTP) which synchronizes system clocks at least once every one hour.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

Certificate profile is in accordance with the X.509 v.3, the IETF RFC 5280 and clause 6.6.1 of ETSI EN 319 411-1.

7.1.1. Version Number

All Certificates are X.509 version 3.

7.1.2. Certificate Extensions

Every issued certificate includes extensions as they are defined for X.509v3 Certificates.

KIBS's Technically Constrained Issuing CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Issuing CA Certificate is authorized to issue certificates. The **anyExtendedKeyUsage KeyPurposeId** does not appear in the EKU extension of KIBS trusted certificates.

Below is a list of extensions used by KIBS for each type of certificate.

7.1.2.1. For Root CAs

Root certificate has the name KIBSTrust Root CA G2, which is the same for Issuing CA from G2 and G3 generation.

Standard Extension	Field	Value
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**None**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.15976.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Subject Key Identifier	Key Identifier	D4E9C6758EDBFEA63227A1C4DA9A0435AE4CBC58 *(This field contains the ID of the Certificate Holder's key.)*

7.1.2.2. For Issuing CAs for electronic signatures

The names of CAs for electronic signatures are: KIBSTrust Issuing Qsig CA G2 and KIBSTrust Issuing Qsig CA G3

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	D4E9C6758EDBFEA63227A1C4DA9A0435AE4CBC58 *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.kibstrust.com/rootg2.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information	Access Method	**1.3.6.1.5.5.7.48.2**

Access	Access Location	http://pki.kibstrust.com/repository/certs/rootg2.crt
Subject Key Identifier	Key Identifier	1FF18B5F563D2C9002089867B03B46259146C869 *(for G3)* 8A7748F3F4E03221EA9ED52BC9633D25A8CE24B5 *(for G2)* *(This field contains the ID of the Certificate Holder's key.)*
Subject Alternative Name	Directory Address	N/A *(for G3)* CN=PRIVATE-4096-11 *(for G2)* *(This field contains the Key identification)*

7.1.2.3. For Issuing CAs for electronic seals

The names of CAs for electronic seals are: KIBSTrust Issuing Qseal CA G2 and KIBSTrust Isssuing Qseal CA G3

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	D4E9C6758EDBFEA63227A1C4DA9A0435AE4CBC58 *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.16503.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.kibstrust.com/rootg2.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.kibstrust.com/repository/certs/rootg2.crt**
Subject Key Identifier	Key Identifier	E0B0E64BB05E5F53CF95DBFF17B747C4227432A9 *(for G3)* 264AABD306A8E9D270DA7104B631504785A9094D *(for G2)* *(This field contains the ID of the Certificate Holder's key.)*
Subject Alternative Name	Directory Address	N/A *(for G3)* CN=PRIVATE-4096-12 *(for G2)* *(This field contains the Key identification)*

7.1.2.4. For Natural Person electronic signatures

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	1FF18B5F563D2C9002089867B03B46259146C869 *(for G3)* 8A7748F3F4E03221EA9ED52BC9633D25A8CE24B5 *(for G2)* *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://www.kibstrust.com/repository/cps**
	Cert Policy ID	**0.4.0.194112.1.0** (QCP-n), or **0.4.0.194112.1.2** (QCP-n-qscd)
	Cert Policy ID	***For G3:*** **1.3.6.1.4.1.16305.1.2.5.4.2** (QCP-n), or **1.3.6.1.4.1.16305.1.2.5.4.3** (Local QSCD), or **1.3.6.1.4.1.16305.1.2.5.4.4** (Remote QSCD) ***For G2:*** **1.3.6.1.4.1.16305.1.2.5.1.2** (QCP-n), or **1.3.6.1.4.1.16305.1.2.5.1.3** (Local QSCD), or **1.3.6.1.4.1.16305.1.2.5.1.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl3.kibstrust.com/KIBSTrustIssuingQsigCAG3.crl** *(for G3)* **http://crl.kibstrust.com/qSigG2.crl** *(for G2)*
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-n)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (EN)	**https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf** *(for G3)* **https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf** *(for G2)*
	PDS Location (MK)	**https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf** *(for G3)* **https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf** *(for G2)*
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information	Access Method	**1.3.6.1.5.5.7.48.1**

Access	Access Location	http://ocsp3.kibstrust.com/ *(for G3)* http://ocsp2.kibstrust.com/ *(for G2)*
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://cacerts.kibstrust.com/KIBSTrustIssuingQsigCAG3.crt *(for G3)* https://www.kibstrust.com/repository/certs/CA-qSig-G2.crt *(for G2)*
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.2.5. For Natural Person in association with a Legal Person electronic signatures

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	1FF18B5F563D2C9002089867B03B46259146C869 *(for G3)* 8A7748F3F4E03221EA9ED52BC9633D25A8CE24B *(for G2)* *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://www.kibstrust.com/repository/cps
	Cert Policy ID	**0.4.0.194112.1.0** (QCP-n), or **0.4.0.194112.1.2** (QCP-n-qscd)
	Cert Policy ID (N/A for QCP-n)	***For G3***: **1.3.6.1.4.1.16305.1.2.5.4.2** (QCP-n), or **1.3.6.1.4.1.16305.1.2.5.4.3** (Local QSCD), or **1.3.6.1.4.1.16305.1.2.5.4.4** (Remote QSCD) ***For G2***: **1.3.6.1.4.1.136305.1.2.5.1.2** (QCP-n), or **1.3.6.1.4.1.16305.1.2.5.1.3** (Local QSCD), or **1.3.6.1.4.1.16305.1.2.5.1.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl3.kibstrust.com/KIBSTrustIssuingQsigCAG3.crl *(for G3)* http://crl.kibstrust.com/qSigG2.crl *(for G2)*
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate	**etsiQcsCompliance**	**0.4.0.1862.1.1**

Statements	**etsiQcsQcSSCD** (N/A for QCP-n)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (EN)	**https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf** *(for G3)* **https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf** *(for G2)*
	PDS Location (MK)	**https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf** *(for G3)* **https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf** *(for G2)*
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp3.kibstrust.com/** *(for G3)* **http://ocsp2.kibstrust.com/** *(for G2)*
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://cacerts.kibstrust.com/KIBSTrustIssuingQsigCAG3.crt** *(for G3)* **https://www.kibstrust.com/repository/certs/CA-qSig-G2.crt** *(for G2)*
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder'skey.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.2.6. For Legal Person electronic seals

Standard Extension	**Field**	**Value**
Authority Key Identifier	Key Identifier	E0B0E64BB05E5F53CF95DBFF17B747C4227432A9 *(for G3)* 264AABD306A8E9D270DA7104B631504785A9094D *(for G2)* *(This field contains the Subject Key Identifier of the issuer's Certificate.)*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://www.kibstrust.com/repository/cps**
	Cert Policy ID	**0.4.0.194112.1.1** (QCP-l), or **0.4.0.194112.1.3** (QCP-l-qscd)

	Cert Policy ID	***For G3:*** **1.3.6.1.4.1.16305.1.2.5.5.2** (QCP-l), or **1.3.6.1.4.1.16305.1.2.5.5.3** (Local QSCD), or **1.3.6.1.4.1.16305.1.2.5.5.4** (Remote QSCD) ***For G2:*** **1.3.6.1.4.1.16305.1.2.5.2.2** (QCP-l), or **1.3.6.1.4.1.16305.1.2.5.2.3** (Local QSCD), or **1.3.6.1.4.1.16305.1.2.5.2.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	Full Name
	Uniform Resource ID	**http://crl3.kibstrust.com/KIBSTrustIssuingQsealCAG3.crl** *(for G3)* **http://crl.kibstrust.com/qSealG2.crl** *(for G2)*
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-l)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf** *(for G3)* **https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf** *(for G2)*
	PDS Location (MK)	**https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf** *(for G3)* **https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf** *(for G2)*
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp3.kibstrust.com/** *(for G3)* **http://ocsp2.kibstrust.com/** *(for G2)*
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://cacerts.kibstrust.com/KIBSTrustIssuingQsealCAG3.crt** *(for G3)* **https://www.kibstrust.com/repository/certs/CA-qSeal-G2.crt** *(for G2)*
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder'skey.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.3 Algorithm Object Identifiers

The signature algorithms follow the specifications described in Sections 6.1.5 and 6.1.6. All algorithms used for CAs and Subscriber follow current research and industry standards to deliver reasonable security for the intended purposes they are being used.

7.1.4 Name Forms

Each Certificate includes a unique serial number that is never reused.

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, Section 4.1.2.4.

7.1.4.1 For Root & Issuing CAs

Field	Value	
Issuer	**CN = KIBSTrust Root CA G2** **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Root CA it is the same as SubjectDN; For Issuing CAs it is the SubjectDN of the Root CA)*	
Subject DN	Common Name	**KIBSTrust Issuing Qsig CA G3** *(for G3 Issuing CA for e-Signature)* **KIBSTrust Issuing Qseal CA G3** *(for G3 Issuing CA for e-Seal)* **KIBSTrust Issuing Qsig CA G2** *(for G2 Issuing CA for e-Signature)* **KIBSTrust Issuing Qseal CA G2** *(for G2 Issuing CA for e-Seal)* *(Is used for user-friendly representation of the CA name to represent itself. This name does not need to be exact match of the fully registered organization name)*
	Organization	**KIBS AD Skopje** *(for Root CA and Issuing CAs)*
	OrganizationIdentifier (2.5.4.97)	***NTRMK-5529581***
	Organization Unit	*For Root and Issuing CA it is "*KIBSTrust Services*"*
	Country	**MK**
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**4096**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.2 For Natural Person electronic signatures

Field	Value	
Issuer	**CN = KIBSTrust Issuing Qsig CA G3** *(for G3)* **CN = KIBSTrust Issuing Qsig CA G2** *(for G2)* **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.)*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surname in UTF8 format according to RFC5280*
	serialNumber	*Unique Identification Number according registration number in CA database with the following semantics:“123456789“*
		Random code as specified in clause 5.1.3 of ETSI EN 319 412-1
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.3 For Natural Person associated with Legal Person electronic signatures

Field	Value	
Issuer	**CN = KIBSTrust Issuing Qig CA G3** *(for G3)* **CN = KIBSTrust Issuing Qsig CA G2** *(for G2)* **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.)*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	Title	*Natural person position in Legal Person*
	serialNumber	*Unique Identification Number according to registration number in CA database with the following semantics: “123456789“*
		Random code as specified in clause 5.1.3 of ETSI EN 319 412- 1
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	Organizational Unit	*VAT- <VATNumber> (optional)*

	OrganizationIdentifier (2.5.4.97)	**NTR***<Country code>-NTRnumber Identification of the Subscriber organization different from the organization name* *Legal Entity's Identification Number from a national trade register with the following semantics: "***NTR***MK-1234567".*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.4 For Legal Person electronic seals

Field	Value	
Issuer	**CN = KIBSTrust Issuing Qseal CA G3** *(for G3)* **CN = KIBSTrust Issuing Qseal CA G2** *(for G2)* **2.5.4.97 = NTRMK-5529581** **OU = KIBSTrust Services** **O = KIBS AD Skopje** **C = MK** *(For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.)*	
Subject DN	Common Name	*Legal Person's name*
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier (2.5.4.97)	*Legal Entity's Identification Number from a national trade register with the following semantics: "***NTR***MK-1234567".*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.5 Name Constraints

KIBS may include name constraints in the **nameConstraints** field when appropriate.

If an Issuing CA Certificate includes the extended key usage "id-kp-emailProtection" it is treated as technically constrained and audited as described in Section 8.

7.1.6 Certificate Policy Object Identifier

According to each certificate type, the following recognized OIDs can be added in the **certificatePolicies** extension:

- **QCP-n**: 0.4.0.194112.1.0 as described in ETSI EN 319 411-2
- **QCP-l**: 0.4.0.194112.1.1 as described in ETSI EN 319 411-2
- **QCP-n-qscd**: 0.4.0.194112.1.2 as described in ETSI EN 319 411-2
- **QCP-l-qscd**: 0.4.0.194112.1.3 as described in ETSI EN 319 411-2

KIBS is also adding the following OIDs in the Certificate Policies extension, to identify when the private key of a qualified certificate resides on a Local QSCD device whose management for the creation of this private key has the Subscriber/Subject and when the private key of a qualified certificate resides on a Remote QSCD device whose management for the creation of this private key has the QTSP on behalf of the Subscriber:

- Qualified Electronic Signatures
  - **1.3.6.1.4.1.16305.1.2.5.4.3** The private key is on a Local QSCD for G3
  - **1.3.6.1.4.1.16305.1.2.5.1.3** The private key is on a Local QSCD for G2
  - **1.3.6.1.4.1.16305.1.2.5.4.4** The private key is on a Remote QSCD for G3
  - **1.3.6.1.4.1.16305.1.2.5.1.4** The private key is on a Remote QSCD for G2.
- Qualified Electronic Seals
  - **1.3.6.1.4.1.16305.1.2.5.5.3** The private key is on a Local QSCD for G3
  - **1.3.6.1.4.1.16305.1.2.5.2.3** The private key is on a Local QSCD for G2
  - **1.3.6.1.4.1.16305.1.2.5.5.4** The private key is on a Remote QSCD for G3
  - **1.3.6.1.4.1.16305.1.2.5.2.4** The private key is on a Remote QSCD for G2.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier is the URI which points to the published KIBS CP/CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

CRL profile is in accordance with the X.509 version 2 and the IETF RFC 5280.

7.2.3 Version number

KIBS issues version 2 CRL’s that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	KIBS Issuing CA SubjectDN
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Signature	The signature algorithm MUST follow the requirements described in Sections 6.1.5 and 6.1.6

7.2.4 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer

Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3 OCSP Profile

7.3.1 Version number

KIBSs OCSP profile is in accordance with version 1 of the IETF RFC 6960.

7.3.2 OCSP Extension

Extension for KIBSTrust Issuing Qsig and KIBSTrust Issuing Qseal CA G2 OCSP Responder:

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.16305.1.1.5**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.kibstrust.com/repository/cps**
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**https://www.kibstrust.com/repository/certs/CA-qSig-G2.crt**, or **https://www.kibstrust.com/repository/certs/CA-qSeal-G2.crt**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

Extension for KIBSTrust Issuing Qsig and KIBSTrust Issuing Qseal CA G3 OCSP Responder:

Standard Extension	Field	Value
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The conformity of information system, policies and practices, facilities, personnel, and assets of KIBS are assessed by a conformity assessment body pursuant to the MK-eIDAS law and eIDAS regulation, the corresponding legislation and standards or whenever a major change is made to Trust Service operations, based on ETSI standards listed in Section 9.15.

In addition to compliance audits, KIBS is entitled to perform other reviews and investigations to ensure the trustworthiness of KIBS's Certification Services. KIBS is entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm.

KIBS is entitled to perform second party audits to contractors that are under a relationship with KIBS to operate as Local Registration Authorities (LRAs).

8.1 Frequency and Circumstances of Assessment

KIBS Compliance Audits are conducted at least annually. Audits are conducted over unbroken sequences of audit periods with each period no longer than one-year duration.

8.2 Identity/Qualifications of Assessor

KIBS's CA compliance audits are performed by:

- Internal Auditors,
- A conformity assessment body which is accredited in accordance with Regulation EC no 765/2008, the ETSI standards (i.e. ETSI EN 319 403).
- The Supervisory Body.

8.3 Assessor's Relationship to Assessed Entity

The auditor of the conformity assessment body shall be independent from KIBS and KIBS's assessed systems. The internal auditor shall not audit his/her own areas of responsibility.

8.4 Topics Covered by Assessment

The conformity assessment covers the conformity of KIBS's information system, policies and practices, facilities, personnel, and assets with MK-eIDAS law and eIDAS regulations, respective legislation and standards. Conformity assessment body audits the parts of information system used to provide Trust Services.

The areas of activity subject to internal auditing are the following:

- Quality of service;
- Security of service;
- Security of operations and procedures;
- Protection of the data of Subscribers and security policy, performance of work procedures and contractual obligations, as well as compliance with the CP and service-based Policies and Practice statements.

The Conformity Assessment Body and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of sub-contractors that are related to providing KIBS Trust Services (e.g. including LRAs).

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of KIBS's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by KIBS management with input from the auditor. KIBS management is responsible for developing and implementing a corrective action plan. If KIBS determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Trusted Services, a corrective action plan will be developed within 30 (thirty) days and implemented within a reasonable period of time. For less serious exceptions or deficiencies, KIBS management will evaluate the significance of such issues and determine the appropriate course of action.

Additionally, in the event of a result of the assessment by the Conformity Assessment Body, showing deficiency, the Supervisory Body requires KIBS to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body. KIBS makes efforts to stay compliant and fulfil all requirements of the deficiency on time. KIBS's management is responsible to implement a corrective action plan. KIBS evaluates the significances of deficiencies and prioritizes appropriate actions to be taken at least during the time limit declared by Supervisory Body or reasonable period of time.

Where personal data protection rules appear to have been breached, the Supervisory Body shall inform the data protection authority of the results of the compliance audit.

8.6 Communications of Results

Audit conclusions or certificate(s) for trust service(s), which are based on audit results of the conformity assessment body conducted pursuant to the MK-eIDAS law and eIDAS regulation, corresponding legislation and standards, may be published on KIBS's website https://www.kibstrust.com/repository.

In addition KIBS submits the resulting conformity assessment report to the Supervisory Body within at period of three (3) working days of receiving it. KIBS submits the audit conclusions or certificate(s) for trust service(s) to maintainers of the Browsers Root Programs in which KIBS is participating and other interested parties.

Results of the compliance audit of KIBS CA's operations may be released at the discretion of KIBS Management.

8.7 Self-audits

KIBS performs regular internal audits to ascertain compliance as per Section 8.4.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

KIBS charges end-user Subscribers for the issuance, management, and re-key renewal of Certificates.

9.1.2 Certificate Access Fees

KIBS does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

KIBS does not charge a fee as a condition of OCSP and making the CRLs required by this CP/CPS available in a repository or otherwise available to Relying Parties. KIBS does not permit access to revocation information, Certificate status information, or certificate status information in their repositories by third parties that provide products or services that utilize such Certificate status information without KIBS 's prior express written consent.

9.1.4 Fees for Other Services

KIBS does not charge a fee for access to this CP/CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with KIBS.

9.1.5 Refund Policy

9.1.5.1 Distant sales

In case the sale of the Certificate is effected via the internet or a phone call the Subscriber has the right, under Article 89 from Consumer Protection Law[3], as amended, to withdraw from the sales contract without stating the reasons within an exclusive time limit of fourteen (14) calendar days from the date of purchase. The exercise of this right shall be made in writing by the Subscriber to KIBS, sending an email to helpdesk@kibstrust.com.

Subsequently, and following communication, KIBS is obliged to repay the money corresponding to the value of the sales contract to the Subscriber. Refund payment is effected with the same method as initial payment and

[3] Consumer Protection Law (Official gazette of Republic of North Macedonia 38/04…140/18)

the Subscriber is not entitled to use the Certificate if it is issued. After that period, the right of withdrawal expires and KIBS has no further obligation for the above cause.

The Subscriber has the right to withdraw from the online prepared Purchase Order and Agreement form before activation of the Certificate. If the Subscriber does not show or submit proper documentation with in thirty (30) days from his/her Purchase Order and Agreement form for Qualified Certificate for electronic signature or seal in/to RA/LRA of Trusted service provider, the Purchase Order and Agreement form will be automatically discarded from the system. In this case, if Subscriber has already paid for the Certificate for electronic signature or seal, KIBS will not refund payment, but will bind payment to a new procedure for purchasing a Certificate during the ongoing fiscal year.

If Certificate is issued, within the period of five (5) days starting from the day of the certificate activation, the Subscriber may submit claims regarding the Certificate or local QSCD in cases of its invalid functionality, merely caused by factory fault, due to which the Certificate or local QSCD does not match its description, the intended purpose and usage which are declared and published by KIBS.

In this case the subscriber only is entitled to request the purchased certificate to be replaced with new and functional certificate. In any case the subscriber is not entitled to terminate the contract for purchase of the certificate and to request reimbursement of the paid purchase amount.

Upon timely provided claim, KIBS undertakes to perform necessary examination of the certificate in order to determine its functionality correctness.

KIBS in any case will not accept any claims submitted upon the expiry of the prescribed period of 5 days from the day of the certificate activation.

KIBS will not accept any claims for the Certificate's defects and damages caused by fault or actions undertaken by the Subscriber.

9.1.5.2 Other cases

According to Section 9.1.5.1 KIBS handles refund case-by-case.

To request a refund Subscriber should send a written application to KIBS. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers handles refund case-by-case. In rare cases KIBS may refund Subscriber. The exercise of this right shall be made in writing by Subscriber to KIBS by sending an e-mail to helpdesk@kibstrust.com.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

KIBS maintains a commercially reasonable level of Professional liability insurance coverage for errors and omissions through an errors and omissions insurance program with an insurance carrier. A certificate of the insurance policy is available at the KIBS public repository: http://www.kibstrust.com/repository.

Rules for indemnification in accordance with the Professional Liability Insurance of Trusted Service Provider KIBS (hereinafter: Rules) follows the MK-eIDAS law[4]. Following MK-eIDAS by-law[5], TSP KIBS is fully adapted to the established requirements for risk coverage amount of liability for damages. For each trusted service, KIBS publicly issues "Terms and Conditions" for using the service. These Terms and Conditions incorporate appropriate information on the Professional Liability Insurance of the trusted service provider.

[4] Law on electronic documents, electronic identification and trusted services (MK-eIDAS)

[5] Rulebook on determination of the lowest amount of insurance against possible damage caused by the issuer and the minimum amount or type of insurance coverage against risk of liability for damages caused by the provider of qualified trusted service.

9.2.2 Other Assets

KIBS has sufficient financial resources to maintain its operations and perform its duties, and is reasonably able to bear the risk of liability to Subscribers and Relying Parties. Proofs of financial resources are not made publicly available.

9.2.3 Insurance or Warranty Coverage for End-Entities

See Section 9.2.1 of this CP/CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to KIBS because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from KIBS about him/herself according to the applicable laws.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential or intended for internal use is public information. Information considered public in KIBS is listed in Section 2.2 of this CP/CPS.

Additionally, non-personalised statistical data about KIBS's services is also considered public information. KIBS may publish non-personalised statistical data about its services.

9.3.3 Responsibility to Protect Confidential Information

KIBS secures confidential information and information intended for internal use from compromise and disclosure to third parties by implementing different security controls.

Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information on the basis of a court order or in other cases provided by law.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

KIBS has implemented a Privacy Policy, which is located at: http://pki.kibstrust.mk/repository in compliance with applicable laws.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to applicable laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

KIBS secures private information from compromise and disclosure to third parties and complies with all applicable privacy laws.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CP/CPS, the applicable Privacy Policy or by agreement, private information are not used without the consent of the party to whom that information applies, in accordance with applicable privacy law.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

KIBS shall be entitled to disclose Confidential Information if, in good faith, KIBS believes that:

- Disclosure is necessary in response to subpoenas and search warrants.

- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This Section is subject to applicable privacy laws.

9.4.7 Disclosure upon Owner's Request

KIBS's privacy policy contains provisions relating to the disclosure of private Information to the person disclosing it to KIBS. This Section is subject to applicable privacy laws.

9.4.8 Other Information Disclosure Circumstances

Not applicable.

9.5 Intellectual Property rights

The allocation of Intellectual Property Rights among KIBS Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such KIBS sub-domain Participants. The following subsections apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. KIBS grants permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Terms and Conditions referenced in the Certificate. KIBS grants permission to use revocation information to perform Relying Party functions subject to the applicable Terms and Conditions, or any other applicable agreements.

9.5.2 Property Rights in the CP/CPS

Subscribers acknowledge that KIBS retains all Intellectual Property Rights in and to this CP/CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, KIBS's root public keys and the root Certificates containing them, including all PRCA public keys and self-signed Certificates, are the property of KIBS. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of those shares or the CA from KIBS.

9.5.5 Violation of Property Rights

KIBS does not knowingly violate the intellectual property rights of any third party.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

KIBS CA warrants that:

- Provides its services consistent with the requirements and the procedures defined in this CP/CPS and related documents;
- Complies with MK-eIDAS and eIDAS regulation and related legal acts defined in this CP/CPS and related documents;
- Publishes its CP/CPS and related documents and guarantees their availability in a public data communications network;

- Publishes and meet its claims in terms and conditions for subscribers and guarantees their availability and access in a public data communications network;
- Maintains confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- Keeps account of the Trust Service Tokens issued by it and their validity and ensure possibility to check the validity of certificates;
- Ensures the access to the private keys on the Remote QSCD to the authorized Subscriber of the keys
- Ensures the proper management and compliance of the Remote QSCD
- Informs the Supervisory Body of any changes to a public key used for the provision Trust Services;
- Without undue delay but in any event within 24 hours after having become aware of it, notify the Supervisory Body and, where applicable, other relevant bodies as national CERT or Data Inspectorate, of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein;
- Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach of security or loss of integrity without undue delay;
- Preserves all the documentation, records and logs related to Trust Services according to Sections 5.4 and 5.5;
- Ensures a conformity assessment according to requirements and present the conclusion of conformity assessment body to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- Has the financial stability and resources required to operate in conformity with this CP/CPS;
- Publishes the terms of the compulsory insurance policy and the conclusion of conformity assessment body in a public data communications network;
- Provides access to its services for persons with disabilities where feasible.
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Revocation services and use of a repository conform to the applicable CP/CPS in all material aspects.

KIBS Terms and Conditions for Use of Qualified Trust Services may include additional representations and warranties.

9.6.2 RA Representations and Warranties

KIBS RAs warrant that:

- They have verified the Subsciber’s identity through procedures approved by KIBS
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CP/CPS, and
- Revocation services (when applicable) and use of a repository conform to the applicable CP/CPS in all material aspects.

KIBS Terms and Conditions may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each e-Signature or e-Seal created using the private key corresponding to the public key listed in the Qualified Certificate is the Qualified e-Signature or e-Seal of the Subscriber and the Qualified Certificate has been accepted and is operational (not expired or revoked) at the time the Qualified e-Signature or e-Seal is created,

- The credentials (PIN, username, password, OTP) accessing the private key are protected and that no unauthorized person has ever had access to them,
- Qualified e-Signature is only created on a QSCD, whereas a Qualified e-Seal can be created either on a QSCD or not.
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true, and the Subscriber is aware of the fact that KIBS may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- The Subscriber observes the requirements provided by KIBS in this CP/CPS and the related documents;
- All information supplied by the Subscriber and contained in the Certificate is true and in the event of a change in the data submitted, Subscriber shall notify the correct data in accordance with the rules established by this CP/CPS and the related documents
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP/CPS.
- The Subscriber is not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.
- The Subscriber shall notify KIBS without any reasonable delay, if subject’s private key or control to it has been lost, stolen, potentially compromised.

KIBS Terms and Conditions for Use of Qualified Trust Services may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

KIBS Terms and Conditions for Use of Qualified Trust Services require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP/CPS.

KIBS Terms and Conditions for Use of Qualified Trust Services may include additional representations and warranties of Relying Parties.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Terms and Conditions for Use of Qualified Certificates disclaim KIBS’s possible warranties, including any warranty of merchantability or fitness for a particular purpose.

KIBS is not liable for:

- The secrecy of the credentials (PIN, username, password, OTP) that have access to the private keys of the Subscribers, possible misuse of the certificates or inadequate checks of the certificates or for the wrong decisions of a Relying Party or any consequences due to errors or omission in Trust Service validation checks;
- The non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the data protection supervision authority, Trusted List or any other public authority;
- Non-fulfilment of the obligations arising from this CP/CPS and the related documents if such non-fulfilment is occasioned by Force Majeure.

9.8 Limitations of Liability

KIBS Terms and Conditions for Use of Qualified Trust Services limit KIBSs liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the liability cap of five hundred Euros (500.00 €) payable in denars according middle exchange rate of NBRSM, limiting KIBS’s damages concerning a Qualified Certificate.

The liability (and/or limitation thereof) of Subscribers and Relying Parties is as set forth in the applicable Terms and Conditions for Use of Qualified Trust Servicess.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify KIBS for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The Terms and Conditions may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, KIBS Terms and Conditions requires for Use of Qualified Trust Services require Relying Parties to indemnify KIBS for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The Terms and Conditions for Use of Qualified Trust Services may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

The CP/CPS becomes effective upon publication in the KIBS's repository. Amendments to this CP/CPS become effective upon publication in the KIBS's repository.

9.10.2 Termination

This CP/CPS as amended from time to time remains in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, KIBS PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, KIBS PKI Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

Section 1.5.1 provides all the available means of communication.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP/CPS are made by the KIBS's Policy Management Authority (PMA). Amendments are either in the form of a document containing an amended form of the CP/CPS or an update. Amended versions or updates are linked to the KIBS repository published at https://www.kibstrust.com/repository/cps.

Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS. The PMA shall determine whether changes to the CP/CPS require a change in the Certificate policy object identifiers of the Certificate policies

9.12.2 Notification Mechanism and Period

KIBS's PMA reserves the right to amend the CP/CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion.

Proposed amendments to the CP/CPS are linked to KIBS Repository located at: https://www.kibstrust.com/repository/cps.

Notwithstanding anything in the CP/CPS to the contrary, if the PMA believes that material amendments to the CP/CPS are necessary immediately to stop or prevent a breach of the security of the TSP or any portion of it, KIBS and the PMA shall be is entitled to make such amendments by publication in the KIBS's Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, KIBS provides notice to of such amendments to KIBS PKI Participants.

At a minimum KIBS and the PMA will update this CP/CPS annually in compliance with CA/Browser Forum guidelines.

Amendments which do not change the meaning of this CP/CPS, such as spelling corrections, translation activities and contact details updates are documented in the Versions history of the present document. In this case the fractional part of the document version number is enlarged.

In case of substantial changes, the new CP/CPS version is clearly distinguishable from the previous ones and the serial number is enlarged by one.

9.12.3 Circumstances under Which OID Must be Changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment contains new object identifiers for the Certificate policies. Otherwise, amendments shall not requiring a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among KIBS, LRA, representing offices and Customers

Disputes among KIBS PKI Participants are resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

KIBS Terms and Conditions contain a dispute resolution clause. Disputes involving KIBS require an initial negotiation period of sixty (60) days followed by litigation in the court of Skopje.

9.14 Governing Law

The law of Republic of North Macedonia governs the enforceability, construction, interpretation, and validity of this CP/CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in country. This choice of law is made to ensure uniform procedures and interpretation for all KIBS PKI Participants, no matter where they are located.

This governing law provision applies only to this CP/CPS. Agreements incorporating the CP/CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP/CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15Compliance with Applicable Law and Standards

KIBS ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- MK-eIDAS - Law for electronic documents, electronic identification, and trusted services (Official gazette of Republic of North Macedonia 101/19…215/19).
- eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- Personal Data laws in Republic of North Macedonia and related EU regulation;
- Related European Standards:

  a. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
  b. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
  c. ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;

- CA/Browser Forum Baseline Requirements

This CP/CPS is subject to Macedonian laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of KIBS. Unless specified otherwise in a contract with a party, KIBS does not provide notice of assignment.

9.16.3 Severability

In the event that a clause or provision of this CP/CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP/CPS shall remain valid.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

KIBS may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. KIBS's failure to enforce a provision of this CP/CPS does not waive KIBS's right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by KIBS.

9.16.5 Force Majeure

Non-fulfilment of the obligations arising from the CP/CPS and/or related documents is not considered a violation if such non-fulfilment is occasioned by Force Majeure. None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this CP/CPS and/or related documents caused by Force Majeure.

9.17Other Provisions

Not applicable.

Appendix A. Table of Acronyms and definitions

Table of Acronyms

Term	Definition
CA	Certification Authority
CP	Certificate Policy
CP/CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	***Certificate Signing Request***
FIPS	United State Federal Information Processing Standards
LRA	Local Registration Authority
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol.
OID	Object Identifier, a unique object identification code
PDS	PKI Disclosure Statement
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority
PRCA	Primary Root Certification Authority
QSCD	Qualified Electronic Signature/Seal Creation Device
RA	Registration Authority.
RFC	Request for comment.
SSL	Secure Sockets Layer.
TSP	Trust Service Provider

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center or Managed PKI Customer, that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Advanced electronic seal	An electronic seal that meets the following requirements: • it is uniquely linked to the creator of the seal. • it is capable of identifying the creator of the seal. • it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and • it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Advanced electronic signature	An electronic signature that meets the following requirements • it is uniquely linked to the signatory; • it is capable of identifying the signatory; • it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and • it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Certificate	Public key of a user, together with some other information, rendered un- forgeable by encipherment with the private key of the certification authority which issued it

Term	Definition
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Policy (CP)	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that have been revoked by the certificate issuer
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to create and assign certificates
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Compliance Audit	A periodic audit that a Processing Center, Service Center or Managed PKI Customer undergoes to determine its conformance with DigiCert PKI Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Electronic Signature	Data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign.
Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
Exigent Audit/Investigation	An audit or investigation by KIBS where KIBS has reason to believe that an entity failed to meet the CP/CPS requirements, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the PKI posed by the entity has occurred.
General Terms and Conditions for Use of Qualified Trust Services	A binding document setting forth the terms and conditions under which an a natural or legal person acts as a Subscriber or as a Relying Party and KIBS provides the corresponding Trust Services.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
KIBS Repository	KIBS's database of Certificates and other relevant KIBS's information accessible on-line.
Managed PKI	KIBS's fully integrated managed PKI service that allows enterprise Customers of KIBSTrust to distribute Certificates to individuals, such as employees, partners, suppliers, and customers. Managed PKI permits enterprises to secure messaging, and e-commerce applications.
Local QSCD	USB PKI token or PKI smart card of QSCD
Long-lived Certificate	A Qualified Certificate which is valid for 1 to 3 years.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
MK-eIDAS	Law for electronic documents, electronic identification, and trusted services.(Official gazette of Republic of North Macedonia 101/19…275/19)

Term	Definition
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a Qualified Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	PRCA Issuing Root CAs and other designated CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
OTP	One Time Password
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
Participant	An individual or organization that is either KIBS, a Customer, a Certification Authority, a Registration Authority, a Subscriber, or a Relying Party.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within KIBS responsible for promulgating this policy.
Practice Statement	A statement of the practices that a TSP employs in providing a Trust Service.
Primary Root Certification Authority (PRCA)	A CA that acts as a root CA and issues Certificates to CAs subordinate to it.
Private key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create a qualified certificate or to decrypt electronic records or files that were encrypted with the corresponding public key.
Processing Center	The KIBS site that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates.
Public Key	The key of a key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify a qualified certificate created with the holder's corresponding private key
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The KIBS PKI consists of systems that collaborate to provide and implement the certificate-based public key cryptographic system.
Qualified electronic seal	An advanced electronic seal that is created by a qualified electronic seal creation device and is based on a qualified certificate for electronic seals.
Qualified electronic Signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and is based on a qualified certificate for electronic
Qualified Certificate	Qualified Certificate is a Certificate issued by a CA which has been accredited and supervised by authorities designated by an EU member state
Qualified Certificate for Electronic Signature	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS

Term	Definition
Qualified Certificate for Electronic Seal	A certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of eIDAS
Qualified signature/seal creation device (QSCD)	A device that is responsible for qualifying digital signatures by using specific hardware and software that ensures that the signatory only has control of their private key.
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Remote QSCD	Server based HSM that is used for central generation and usage of Subscriber private keys.
Remote Identity verification	The method/process by which the Subscriber is identified through a live video call session and is equivalent to validation through physical presence.
Root CA	Certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s).
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under Section 6.2.2.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Subordinate CA (Sub CA)	Certification authority who's Certificate is signed by the Root CA, or another
Subject	The subject can be: – a natural person; – a natural person identified in association with a legal person; – a legal person (that can be an Organization or a unit or a department identified in association with an Organization);
Subscriber	An entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
Terms and Conditions	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber or a Relying Party.
Supervisory Body	The authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS
Trust Service	Electronic service for: – creation, verification, and validation of digital signatures and related certificates. – creation, verification, and validation of timestamps and related certificates. – registered delivery and related certificates. – creation, verification, and validation of certificates for website authentication; or – preservation of digital signatures or certificates related to those services
Trust Service Provider	An entity that provides one or more Trust Services.
Trusted Person	An employee, contractor, or consultant of an entity within the DigiCert PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a DigiCert PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.

Term	Definition
Validity Period	The period of time measured from the date when the Certificate is issueduntil the Expiry Date.

End of Document

Преодни одредби

Овие Правила и постапки влегуваат во сила со денот на нивното објавување на веб страницата на квалификуваниот давател на доверливи услуги КИБС: https://www.kibstrust.mk.

Генерален директор

Горан Анастасовски