Practice Statement
for Providing electronic identification
KIBSTrust OneID

Version: 1.0
Effective date: 24.09.2021

Designation: 111.02
OID: 1.3.6.1.4.1.16305.1.1.6

KIBS AD Skopje

https://www.kibstrust.com/

Trademark notice

KIBS, KIBSTrust and OneID are registered marks of KIBS AD Skopje. Other names mentioned in the document may be trademarks of other owners. The Trust Service Provider is organizationally part of KIBS, but operates under the brand name KIBSTrust, hence the term "KIBS Trust Service Provider" is identified with "KIBSTrust".

Contents

1. INTRODUCTION

This document contains the Practices applied by KIBSTrust for remote check and verification of the existence of a natural person, the authenticity of the attached documents for personal identification of the natural person, issuance of Electronic Identification Means according to a registered Electronic Identification Scheme with a high level of security.

It sets out the general requirements and security measures used by KIBSTrust in providing Electronic Identification Services and issuing a Qualified Certificate for Electronic Signature as one of the components of Electronic Identification Means. All this is according to MK-eIDAS[1], Articles 11 to 20 (related to electronic identification), Articles 24, 29, 38, 39, 40, 55 (related to Qualified Trust Services), relevant bylaws and Articles 19, 24, 26, 27, 28, 36, 37, 38 and 45 of Regulation (EU) no. 910/2014 (eIDAS)[2]. Additionally, in terms of personal data protection, this document complies with MK-GDPR[3] и GDPR[4].

As a confirmation of the compliance with MK-eIDAS and eIDAS, KIBSTrust is subject to conformity assessment verification by an independent organization, accredited Conformity Assessment Body, accepted by the Macedonian national regulator Ministry of Information Society and Administration (MISA). Based on this Certificate of Conformity, KIBS as a Qualified Provider of Trust Services and Electronic Identification Services is entered in the Register of Trust Service Providers and Electronic Identification Schemes.

This document is made public to inform the Subjects, Relying Parties, auditors, and regulatory bodies about the business, legal, technical, and organizational measures in requesting, issuing, managing, using, renewing, replacing, suspending, revoking, and reactivating the Electronic Identification Means of the Subject.

1.1. Overview

KIBSTrust applies procedures and standards, according to regulatory requirements, for issuing and managing the life cycle of Electronic Identification Means consisting of a mobile device, an application solution installed on the mobile device, natural person identification data, and a Qualified Certificate for Electronic Signature as a means for electronic signing.

Policies and procedures for issuing a Qualified Certificate as part of Electronic Identification Means are in accordance with the ETSI EN 319 411-2 standard and the QCP-n-qscd profile for Qualified Certificates for Electronic Signature issued on a Qualified Signature Creation Device (QSCD), and are published in the public repository of documents under the name "Rules and Procedures for Issuing Qualified Certificates for Electronic Signatures and Electronic Seals" (with internal designation 111.01). This document shall hereinafter be referred to as: CP / CPS.

The Qualified Signature Creation Device (QSCD) used by KIBSTrust is included in the list of Qualified Electronic Signature and Electronic Seal Creation Means maintained by MISA according to MK-eIDAS.

KIBSTrust has secure storage capacity for, inter alia, Certificate issuing systems, including cryptographic modules with private keys used for issuing Certificates. KIBSTrust as a Trust Service Provider for issuing Certificates performs all services regarding the life cycle of Certificates in terms of issuing, managing, revoking, and renewing Qualified Certificates.

CP /CPS is particularly applicable to issuing Certificates of KIBSTrust, which issues Qualified Certificates for Electronic Signatures and Electronic Seals. KIBSTrust publishes CP /CPS to comply with the specific requirements of the applicable legislation or other industry standards and requirements.

---

[1] Law on Electronic Documents, Electronic Identification and Trust Services (Official Gazette of the Republic of North Macedonia 101/19, 215/19)) (MK-eIDAS)

[2] Regulation (EU) 910/2014 of the European Parliament and the Council of 23 July 2014 on Electronic Identification and Trust Services for electronic transactions on the internal market and repealing Directive 1999/93 / EC (eIDAS)

[3] Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia (MK-GDPR)

[4] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and free movement of such data and repealing Directive 95/46 / EC (GDPR)

The requirements in this document derived according to those listed in CP / CPS shall be referenced to the corresponding item of CP / CPS.

1.2. Document name and Identification

KIBSTrust assigned the following value of object identifier (OID): **1.3.6.1.4.1.16305.1.1.6** to this document entitled "Practices for Providing Electronic Identification Service"

1.3.6.1.4.1.16305	Identification number (OID) of KIBS, registered in IANA
1.3.6.1.4.1.16305.1	Trust Services Provider
1.3.6.1.4.1.16305.1.1	Certificate Policy and Certification Practice Statement (CP/CPS)
1.3.6.1.4.1.16305.1.1.6	Practices for Providing a Qualified Electronic Identification Service

1.3. Participants

1.3.1. Issuer of Electronic Identification Means

The issuer of Electronic Identification Means is a legal entity that meets the requirements set out in MK-eIDAS and the relevant bylaw[5] (Rulebook) and has full responsibility for providing the services for which it is registered.

KIBSTrust is a registered issuer of Electronic Identification Means and meets the standards and technical security measures of its Electronic Identification Scheme, related to the characteristics and design of the Electronic Identification Means at a high level.

KIBSTrust is the owner of the Electronic Identification Scheme and applies standard authentication protocols (OpenID connect, SAML 2, WS federation) and initiates signature creation and creation of Electronic Identification Means, which ensures easy interoperability with any system or application.

KIBS is also a registered provider of Qualified Trust Services that include the issuance of Qualified Certificates for Electronic Signature.

The Qualified Certificate profile issued on remote QSCD as part of the Electronic Identification Means is described in CP / CPS (item 7.0).

1.3.2. Registration Authorities

Registration Authority (RA) is an entity that verifies the entity's identification data before issuing a Certificate and Electronic Identification Means, initiates or forwards applications for revocation of Certificates /revocation of Electronic Identification Means, and approves key renewal applications. KIBSTrust acts as a RA for the Qualified Certificates and Electronic Identification Means it issues.

KIBS may enter into a contractual relationship with one or more third parties for the performance of part or all of the obligations (outsourcing) of RA. In this case, the third party is a Registration Authority (RA) and it performs its obligations in full compliance with these Practices and CP / CPS, the relevant procedures for authentication and verification of identity, and the terms of the RA agreement, signed between RA and KIBS.

Verification of the e-mail address cannot be delegated to a third party and is verified only by the CA RA system.

Before launching RA-related operations, KIBS trains authorized RA personnel for the verification process and security procedures and then conducts annual retraining.

KIBS conducts annual audits of the operation and procedures of RA to ensure compliance with these Practices, validation plans, and the agreement with the RA (if the RA is an external company).

1.3.3. Subject of Electronic Identification

Subject of Electronic Identification (Subject) means a natural person to whom KIBSTrust provides services according to these Practices, that is, issues an Electronic Identification Means based on its application.

[5] Rulebook on the Procedures and Standards for Compliance with the Technical, Physical and Organizational Measures for Security of Electronic Identification Schemes (Official Gazette of RSM 53/20)

1.3.4. Relying Parties

Relying Party is a legal entity that, to provide electronic services to its customers, relies on the trust in the Electronic Identification Means issued by KIBSTrust. Relying Parties have entered into an agreement for the integration of their services with the KIBSTrust OneID service to download a set of data - attributes for the Subject and /or to rely on that data contained in the Electronic Identification Means of their clients.

Downloading attributes from the Electronic Identification Means by the Relying Party is performed only with the explicit consent of the Subject.

The Relying Party publishes a Privacy Policy with which it is bound to treat personal data of the Subjects for electronic identification according to the requirements of the Law on Personal Data Protection. By giving its consent to the transfer of attributes from its Electronic Identification Means, the Subject also accepts the Privacy Policy of the Relying Party.

The Relying Party must verify the validity of the Certificate through the appropriate Certificate validation services provided by KIBSTrust, before relying on the information contained in the client's Electronic Identification Means.

1.3.5. Other Participants

Other participants include:

- Confidential data source, such as the Central Population Register (CPR).
- External companies with which, based on an agreement, KIBSTrust conducts business and technical relations such as automated services for verification of personal identification documents; outsourcing the need for means, trust systems, and procedures to generate, securely store, and provide other parts of the life cycle of KIBSTrust root and issuing Cas.

1.4. Electronic Identification Usage

When issuing an Electronic Identification Means, remote authentication and verification of personal and other data of natural persons, which shall be included in the Qualified Certificate issued by KIBSTrust, are applied.

Electronic Identification Means enables the entity participating in the electronic transaction to prove its identity to the other participants in such transaction.

The Relying Parties, providers of electronic service for their clients, apply electronic identification to verify the identity of their client, that is, they rely on the data from the Electronic Identification Means to enable authentication and authorization of their clients.

1.4.1. Appropriate Electronic Identification Service Usage

1.4.1.1. Subject of Electronic Identification

The Subject agrees to the Terms and Conditions for using the Electronic Identification Service. Personal data obtained in the electronic identification process are used in the process of online signing a consent for the issuance of a Certificate for Qualified Signature. The signing of the consent is done with a one-time Certificate issued only once based on the correct identification of the user in the process of registration and creation of the electronic identity. A registered user can use the electronic identity multiple times until the expiration of the Qualified Certificate validity.

The Electronic Identification Means is used by the Subject for authentication and can also be used for signing electronic documents, provided that the use is not otherwise prohibited by law, with these Practices, Terms and Conditions of Use, and other agreements with the users.

1.4.1.2. Relying Parties

After the consent of the Subject, the Relying Parties will use the Subject's data from the Electronic Identification Means. In accordance with the contractual provisions between KIBSTrust and the Relying Party, and with the consent of the Subject, the Relying Party can confidently rely on the accuracy of the electronic identification attributes by taking a minimum or additional set of personal identification data which in a unique way represent specific natural person.

The minimum and additional set of personal identification data are according to the requirements of the Rulebook resulting from the MK-eIDAS law, the Law on Prevention of Money Laundering and Financing of Terrorism.

For a minimum set of attributes for identification of persons using Electronic Identification Means, the following is determined: name, surname, date of birth, personal identification number, or identification number. An additional set of attributes may be: name and surname at birth, place of birth, current address, gender, number of the identification document or serial number of the Electronic Identification Means, the authority that issued the document and date of validity, that is, name of the issuer of the Electronic Identification Means and the period of validity of the Electronic Identification Means.

Relying Parties that enable electronic signing with the Electronic Identification Means should check the validity of the Certificate by confirming the status of the Certificate and the Electronic Signature of the CA that issued the Certificate. KIBSTrust shall not be liable if the Relying Party fails to make such checks, if it does not have the right to process the user's personal data or if it processes them in violation of the applicable law.

Relying Parties may use KIBSTrust CP OID, identified in the Certificate, to approve or refuse the use of the Certificate.

1.4.2. Prohibited Usage

The Electronic Identification Service will only be used to the extent that its use is according to the applicable laws, and in particular according to the Anti Money Laundering (AML) and Know Your Customer (KYC) requirements.

The Electronic Identification Service should not be used in a way that could compromise the confidentiality, integrity, and security of the data.

1.5. Administration of this Document

1.5.1. Organization Administrating the Document

These Practices, the CP / CPS of CA and the relevant documents listed here are maintained by the Policy Management Authority (PMA) of KIBSTrust - PMA, which can be contacted at:

KIBS AD Skopje
Kuzman Josifovski Pitu 1
1000, Skopje, Republic of North Macedonia

1.5.2. Contact Information

KIBSTrust PKI Policy Manager

E-mail: pma@kibstrust.com

tel. +389 2 5513401, +389 2 3297401

1.5.3. Person Determining Suitability of this CPS

The Coordinator of KIBSTrust Policy Management Authority determines the appropriateness and applicability of these Practices based on the results and recommendations of the compliance audits.

1.5.4. Practice Approval Procedure

Approval of these Practices and subsequent amendments are made by PMA. Amendments represent a document that contains a modified form of Practices or a note for a revised text. Modified versions or updates are linked to the updates and practices notifications section of KIBSTrust repository located at: https://pki.kibstrust.com/repository. Even if there is no compelling reason to amend these Practices, PMA conducts a review process at least once a year to improve.

1.6. Definitions and Acronyms

Refer to Appendix A for a table of acronyms and definitions.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Public Information Repository

At a minimum, KIBSTrust publishes the following information related to the issuance of Electronic Identification Means in its information repository:

- Practice for providing Electronic Identification Service,
- CP / CPS for issuing Certificates,
- Certificate Policies,
- Overview of the Certificate hierarchy,
- Audit results,
- Insurance Policy,
- Certificates, including root and issuing Certificates,
- Certificate profiles,
- Terms and Conditions for using Qualified Trust Services,
- Privacy Policy,
- Certificate Revocation List,
- Browsing for a Certificate for which the Subject has given consent for publication.

KIBSTrust shall ensure that its repository is available 24 hours a day, 7 days a week, with a minimum of 99.00% availability per year and a scheduled downtime of no more than 0.4% per year.

Upon system failure, service, or other factors that are not under the control of KIBSTrust, every effort will be made to prevent the unavailability of this information service from exceeding the abovementioned time.

2.2. Publication of Information

KIBSTrust maintains a web-based repository in the public data communication network (https://pki.kibstrust.com/repository) that allows Relying Parties to request online information about revoked or another Certificate status. KIBS provides Relying Parties information on how to locate the repository to verify the status of a Certificate and how to find the right OSCP Responder.

2.2.1. Publication and Notification Policies

These Practices and the referenced KIBSTrust CP / CPS are published in the public repository located at: https://pki.kibstrust.com/repository . KIBSTrust documents are published along with the enforcement date no less than 10 days prior to taking effect.

2.2.2. Items not Published

Refer to Section 9.3.1 of this document.

2.3. Time and Frequency of Publication

Certificate status information is published according to the provisions of the CA CP / CPS.

Updated Terms and Conditions are published as required. Certificates are released immediately after issuance if the Subject has given consent for release of the Certificate in the public directory of issued Certificates.

2.4. Repository Access Control

The information published in the repository section of the KIBSTrust website is publicly accessible. Access to such information with a read-only option is not restricted. KIBSTrust requires individuals to agree to the Terms and Conditions as a condition to accessing Certificates, Certificate status information, or CRL. KIBSTrust has

implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying content in the repository, according to KIBS Security Policies. KIBSTrust makes its repository publicly available in a read-only manner, specifically at the link https://pki.kibstrust.com/repository .

3. IDENTIFICATION AND AUTHENTICATION

In line with the positively conducted check by an external certification body for conformity assessment, KIBSTrust applies an Electronic Identification Scheme with a high level of security in the phase of logging and

registration of the Electronic Identification Subject and the phase of identity check and verification of natural persons.

The Electronic Identification Scheme provides:

- verification of the natural person's identity should be carried out using biometric data or physical characteristics that uniquely connect the person with the personal identification document for which there is a confirmation from a confidential source, or
- verification of the natural person for whom an equivalent valid means has already been issued, that is, a Qualified Electronic Signature issued by a registered or recognized provider of Qualified Trust Services.

The personal data of the Subjects are processed in a way that guarantees a high level of security, including protection against unauthorized or illegal processing and accidental loss, destruction, or damage, by applying appropriate technical and organizational measures.

The content of some of the items in this Chapter, related to the Qualified Certificate issued as part of the Electronic Identification Means, refers to the corresponding item in the CP / CPS above.

3.1. Naming

Refer to item 3.1 of CP/CPS.

3.2. Initial Identity Validation

KIBSTrust uses the methods described in this Section to establish the identity of the Subject of electronic identification. KIBSTrust may refuse to issue Electronic Identification Means at its discretion if the authentication is not successful.

KIBSTrust applies remote proofing and automatic verification of the identity of the person requesting the issuance of an Electronic Identification Means. In the event of a failed automatic verification, KIBSTrust RA agent may be activated.

The second way of verifying the identity is with a Qualified Electronic Signature if the Subject of Electronic Identification already has a valid Qualified Certificate for Electronic Signature issued by a registered provider of Qualified Trust Services.

In both cases, the process starts with registration and data entry for creating an account, whether initiated through an entry form in an installed mobile application or through a web form on the portal of the Relying Party (company) whose user registration system is integrated with the KIBSTrust OneID Electronic Identification Service.

3.2.1. Application and Registration of the Subject

In the process of registering a user on the mobile application:

1. name, surname, e-mail address (username), password, and password confirmation are entered,
2. the Terms and Conditions of Use and the Privacy Policy for the Service are accepted,
3. an OTP code is received on the entered e-mail address. The OTP code is a 6-digit number valid for 60 minutes. The user can request a new OTP code,
4. the received OTP code is entered. The user has 3 attempts to complete the confirmation at the reported e-mail address. After the third failed attempt, all entered data for the new user will be destroyed and the registration process will start from the beginning.

The user account has been created and can be used. If the process is initially started through the website of the Relying Party, the registered user is shown a QR code. The user captures the QR code with the camera on their mobile phone. The link leads the user to one of the repositories for the distribution of mobile applications for the operating system (such as iOS, Android, HarmonyOS). The mobile application KIBSTrust OneID Mobile is downloaded and installed from these repositories.

Mobile device activation follows:

1. The OneID Mobile user logs in to the mobile application with their credentials (username and password).
2. After successful authentication, a new PIN code that will be used for authentication of the mobile application is entered.

3. The user is offered to use the highest degree of authentication that is supported by the operating system of the mobile device. Optionally the user can enable biometric authentication so-called FaceID or TouchID which will be used to activate the mobile application.
4. A security software token is created and placed in a secure location on the mobile device, indicating that the device is activated.

Note: The user is allowed to have only one active mobile device when using the OneID service. If the user has previously activated another mobile device, he needs to disable that device through the security settings of the OneID.com web application.

3.2.2. Remote Identity Verification

A registered user can request creation of an Electronic Identification Means and the issuance of a Certificate on a remote QSCD, for which he will need to present a valid identity document (ID card or passport).

The application process for creating an Electronic Identification Means and remote Certificate for Electronic Signature consists of the following steps:

1. Authenticated user of the mobile application selects the option for OneID electronic identity.
2. Accepts the Terms and Conditions of Use and Privacy Policy for the KBSTrust OneID Service.
3. Enters name and surname as stated in the personal identification document, personal identification number, and number of the personal identification document (identity card or passport).
4. The entered data are compared with the data from a trusted data source - Central Population Register (CPR).
5. After a positive check, the process of verification of the personal identification document begins:
   a. the user scans the appropriate pages depending on the type of identity document (ID card or passport).
   b. takes a selfie with the registered mobile device.
   c. based on generated instructions on required movement from the mobile application makes a video that serves to confirm his liveliness.
6. The system makes background checks whether the personal identification document is original and issued by state authority of the Republic of North Macedonia, makes a biometric comparison of the document photo and the photo of the person taken with the camera of the registered mobile device, compares the extracted data from the document for personal identification with the CRP data.
7. In case of a problem with the identity check, an agent in the KIBS RA is notified, who can check and verify the identity in the process of electronic identification.
8. After positive verification, an automated process of the application for issuance of a Certificate, verification and issuance of a Certificate for Electronic Signature is initiated.
9. The application for issuance of a Certificate is signed with a one-use Certificate that is created with the data of the user and the issuance of a Qualified Certificate is approved.
10. With the issuance of the Certificate, the process of issuing an Electronic Identification Means is completed.

All personal data extracted from the document and the result of the identity verification are stored by KIBSTrust as a proof of remote electronic identification transaction.

3.2.3. Verification of Identity with Issued Equivalent Valid Means

A registered user can request creation of an Electronic Identification Means and issuance of a Certificate on a remote QSCD, by presenting that he /she has a valid Qualified Certificate for Electronic Signature (for the issuance of which an identity verification has been made previously).

The process of applying for and creating an Electronic Identification Means and remote Certificate for Electronic Signature consists of the following steps:

1. An option to create OneID electronic identification is selected by the user of the mobile application.
2. Completed form with data for the Certificate Application with name and surname (from the already registered user account) follows and the personal identification number and the number of the personal identification document (ID card /passport number) of the user is entered, the Terms and Conditions for using the service are accepted.
3. From the offered two methods, the option of possessing a Qualified Certificate issued by KIBSTrust is selected, whereby an e-mail to the previously registered e-mail address of the user is sent.
4. The e-mail contains a unique temporary link to the web application www.OneID.mk. www.OneID.mk. The link expires in 24 hours.

5. An initial check is made on the type of device used to open the link. It is necessary to open the link from a desktop computer, as it will be offered to sign the application with a Qualified Certificate issued on a local QSCD. An XML document that contains data to be verified is created.
6. XML document with a valid Qualified Certificate issued by KIBSTrust is signed by the user. The Qualified Certificate with which the XML document has been signed is verified and the link between the Certificate and the personal identification number contained in the XML verification data is checked.
7. If the check is in order, the application for issuance of Electronic Identification Means is approved and a new Certificate is issued on remote QSCD. The user is informed that the data for the issued Certificate are saved in his mobile application KIBSTrust OneID Mobile.
8. The issued Certificate is recorded in the mobile application.

3.3. Identification and Authentication of the Renewal or Re-key Applications

Before the expiration of an existing Certificate, it is necessary for the Subject to obtain a new Certificate to maintain the continuity of the Certificate use within the Electronic Identification Means. The process of renewing the electronic identity of the Subject means generating a new pair of keys to replace the pair that is expiring (technically defined as "re-key").

The user can request renewal 30 days before the expiration of the Certificate. Authentication of the renewal application is done by Electronic Signature with the still valid Certificate.

The user can renew only once without re-identification. At the next application for renewal, the identification procedure must be passed, as well as at the initial verification of the identity.

The renewal process can be initiated by the Subject in case of replacement of the mobile device.

If a user who has an active OneID Certificate wants to continue using it on a new mobile device or in case the OneID Mobile application is deleted from an existing device, the following steps should be followed:

1. Installing the OneID Mobile Mobile application,
2. Authentication with a username for which there is an active Certificate. The mobile application notifies that there is an active Certificate with data to activate another device and in order to make a replacement, the revocation of the old Certificate must be confirmed.
3. Confirmation of the revocation application of the old Certificate:
   (1) with approval from the mobile device where the old Certificate is registered (if the user is still in possession of the old device with an active application), or
   (2) using the OTP code sent to the mobile number that was verified upon issuance of the Certificate to be revoked.
4. Initiating an application for issuance of a new Certificate which is signed with a one-use Certificate that is created with the user data checked in the CRP.

With the issuance of a new Qualified Certificate, the process of replacing an Electronic Identification Means is completed.

3.4. Identification and Authentication of Revocation Applications

All revocation applications of the Electronic Identification Means and revocation of the Qualified Certificate must be authenticated.

Before a Certificate is revoked, it is verified that the revocation was requested by the Subject of the Certificate or the entity that approved the Certificate Application.

Acceptable procedures for authenticating cancelation /revocation application by the Subject include one or more of the following procedures:

1. The Subject submits an electronic revocation form through the KIBSTrust web portal authenticated as a registered user with an additional security level, provided with two-factor authentication;
2. Receiving an e-mail from the e-mail address of the Subject requesting revocation, which contains an Electronic Signature that can be verified with a Qualified Certificate to be canceled;
3. Communication with the Subject that will provide reasonable assurances confirming with certainty that the person seeking revocation is indeed the Subject or is duly authorized to claim it. Such communication,

depending on the circumstances, may involve one or more of the following: telephone or personal presence of the Subject, or delivery of the proper authorization by standard post or courier service.

KIBSTrust RA Administrators are authorized to request revocation of Certificates within the KIBSTrust domain. Before the administrator is allowed to perform the revocation function, the administrator identity will be authenticated by access control using SSL and client authentication.

Revocation of the Electronic Identification Means can be done in several ways depending on the need of the user, such as lost or damaged mobile device of the user or the user wants to revoke the service due to other reasons.

If the user's device is functional, the user can revoke the Electronic Identification Means through the OneID Mobile mobile application from the user profile menu, where there is an option to close the account. This option will erase all device data, deactivate the device, revoke the Certificate, and delete all device activation data.

If the user does not own his device (lost or stolen), the revocation procedure through alternative channels may be used (support call center, web portal for OneID service users).

The user can authenticate himself on the web portal for the OneID service and choose the option to revoke the Electronic Identification Means, which will mean deleting the data from the mobile device and revoking the Qualified Certificate for Electronic Signature.

If the user calls the number of the support center for authentication of the application for revocation of the Electronic Identification Means /revocation of the Certificate, in addition to the personal data, the user must have access to the e-mail address through which the application is verified. The agent from the support center checks the data and verifies the e-mail address by activating the generation and sending the OTP code to the user's e-mail. The user reads the OTP code and communicates it to the call center over the phone.

Once the user is identified, the serial number of the active OneID Certificate can be unambiguously found in the OneID Backoffice system. Note: for one e-mail address (username) there is only one active Certificate.

Within the PKI system, based on the determined serial number, the Certificate is revoked and the activation data for the Electronic Identification Means are deleted.

After the Certificate and the issued Electronic Identification Means are revoked, the user should follow the same procedure for issuing a new Electronic Identification Means by submitting a new application and going through the process of identity verification again (item 3.2.2).

3.5. Identification and Authentication on the Application of the Relying Party

When the Relying Party for its Electronic Service, which is integrated with KIBSTrust OneID, needs to download the electronic identification data of its client - Subject of the Electronic Identification Means, the user is asked

to perform authentication with his user account. After successful basic authentication, the OneID Backend background system sends the so-called Push notification to the mobile application for secondary authentication (2FA). The web application of the Relying Party is in a state of waiting for the authentication status to be verified. The Subject receives a Push notification on his OneID Mobile application and enters his PIN or uses biometric data (FaceID / TouchID) to open the notification. The user is shown details about the consent request (name of the Relying Party and set of data that are required) and is offered options to accept or cancel the consent. If he approves the download, a software access token is created, which remotely activates the private key of the Qualified Certificate stored on the remote QSCD in the KIBSTrust system, to create a Qualified Electronic Signature of the consent for downloading the personal identification data. The system of the Relying Party receives the electronic identification data of the user.

4. OPERATIONAL LIFE CYCLE OF THE CERTIFICATE AS A PART OF THE ELECTRONIC IDENTIFICATION MEANS

4.1. Application for a Certificate as Part of the Electronic Identification Means

4.1.1. Who can Submit a Certificate Application

An application for a Qualified Certificate can be submitted by the Subject of electronic identification within the process of creating an Electronic Identification Means which is also a Subject of the Certificate if it is legally qualified.

Issuance of an Electronic Identification Means can be requested by all natural persons over 15 years of age who have a valid personal identification document issued by state authority of the Republic of North Macedonia.

4.1.2. Registration Process and Responsibilities

The Subject of electronic identification agrees with the Terms and Conditions for issuance of Certificates, which contain representations and warranties described in Section 9.6.3, and go through the registration process which consists of:

- Acceptance of the Terms and Conditions regarding the use of the Certificate;
- Automatic completing data required for issuance of a Certificate collected during the process of identification and electronic signing of the form "Order and Agreement" and providing accurate and true information according to the requirements of this Policy;
- Providing relevant validation documents;
- Generating or organizing generation keys pairs;
- Obtaining his / her Certificate, directly or through RA;
- Proof that they possess and /or have exclusive control of the private key corresponding to the public key;
- Payment of all applicable fees, if required.

4.2. Processing of the Certificate Application

4.2.1. Performing Identification and Authentication Function

KIBSTrust performs identification and authentication of all necessary information about the Applicant:

(1) remotely with a Qualified Certificate, or
(2) using a method equivalent to physical presence, in line with Section 3.2.

If RA assists in the verification, then KIBS RA must create and maintain sufficient records to establish that it has performed its required verification tasks and communicates the completion of such tasks to KIBSTrust.

As part of this evaluation, KIBSTrust RA may check the Certificate against the internal database of previously revoked Certificates and rejected Certificate Applications to identify suspicious Certificate Applications.

4.2.2. Approval or Rejection of the Certificate Applications

After successful remote verification of the identity of the person and automatic validation of the data, the

application for issuance of a Certificate within the Electronic Identification Means is automatically approved.

4.2.3. Certificate Application Processing Time

KIBS starts processing Certificate Applications immediately after successful electronic verification of the Applicant's identity. Certificate Application remains active until it is rejected, issued, or automatically expired within 30 days.

4.3. Certificate Issuance

4.3.1. Actions During the Issuance of the Certificate

The Certificate is created and issued after successful verification of the Applicant’s identity, registered user of the mobile application as part of the Electronic Identification Means.

KIBSTrust databases and certification processes are protected from unauthorized modification. Upon completion of the issuance, the Certificate is stored in the database and sent to the Subject.

4.3.2. Certificate Issue Notification for the Subject

KIBSTrust notifies Subjects that the Certificates have been created and allows the Subjects to access Certificates by notifying them that they are available. The Certificates are made available to the Subjects through the mobile application for electronic identity management.

4.4. Certificate Acceptance

4.4.1. Actions that Constitute Acceptance of the Certificate

The following procedures represent acceptance of the Certificate:

- Downloading a Certificate constitutes an acceptance of the Certificate by the Subject,
- Failure of the Subject to submit an objection to the Certificate or its content within 5 days constitutes an acceptance of the Certificate.

4.4.2. Publication of the Certificate

KIBSTrust publishes information about the Certificates it issues in a publicly available repository. The Subject is entitled to choose whether the information on the Certificate and the Certificate itself will be published in the KIBS CA Public Directory for issued Certificates.

4.4.3. Notification of Certificate Issuance by KIBSTrust to Other Entities

RA may receive notification of the Certificate issuance which is a result of a positively completed remote electronic identification.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Refer to item 4.5.1 of the CP/CPS document.

4.5.2. Relying Party Public Key and Certificate Usage

Refer to item 4.5.2 of the CP/CPS document.

4.6. Certificate Renewal

Certificate renewal with the same key pair does not apply.

4.7. Renewed Certificate with New Key Pair (Certificate Re-key)

Refer to item 4.7 of the CP/CPS document.

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 the change of information in the existing Certificate (different from the public key of the Subject).

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

4.8.2. Who may Application Certificate Modification

Refer to Section 4.1.1.

4.8.3. Processing Certificate Modification Applications

KIBSTrust performs identification and authentication of all required information of the Subject in line with Section 3.2.

4.8.4. Notification of New Certificate Issuance to Subscriber

Refer to Section 4.3.2.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Refer to Section 4.4.1.

4.8.6. Publication of the Modified Certificate by CA

Refer to Section 4.4.2.

4.8.7. Notification of Certificate Issuance by CA to Other Entities

Refer to Section 4.4.3.

4.9. Certificate Revocation and Suspension

Revocation of a Certificate permanently terminates the operational period of the Certificate before the Certificate reaches the end of the specified period of validity. By revoking the Certificate, the electronic identity of the user is also revoked.

The revocation application is authenticated according to Section 3.4. before the revocation process of the Certificate is performed.

Revocation of Certificates is performed as stated in the following items.

For Certificates that include an e-mail address, revocation and suspension of the Certificate are according to the requirements of the CA / B Forum.

4.9.1. Circumstances for Revocation

KIBSTrust Terms and Conditions provide an obligation and /or right of the Subject to apply for revocation of a Certificate. Only in the circumstances listed below, the Certificate relating to the Electronic Identification Means will be revoked by KIBSTrust or the Subject and published in the CRL.

The Subject's Certificate is revoked if:

- KIBSTrust or the Subject has reason to believe or suspect that the Subject's private key has been compromised. If a third party reports a compromise, KIBSTrust shall request appropriate confirmation from the Subject;
- KIBSTrust has reason to believe that the Subject has breached a material obligation, representation, or warranty of the applicable Terms and Conditions for the use of Qualified Trust Services;
- KIBSTrust has reason to believe that the Certificate was issued contrary to CP / CPS procedures, to a person other than what is stated as a Subject in the Certificate, or the Certificate was issued without the authorization of the person named as a Subject in the Certificate;
- KIBSTrust is aware of the changes affecting the validity of the Certificate;
- The used cryptography no longer provides a link between the Subject and the public key;
- KIBSTrust has reason to believe that any of the material facts in the Certificate Application are incorrect;
- KIBSTrust established that the material precondition for issuing the Certificate was neither satisfied

nor waived;

- The Subject loses the legal qualification, is declared absent or deceased, having in mind that the Certificate is in any case non-transferable;
- The Subject loses the ability to use the local QSCD or mobile device required to access the remote QSCD;
- In case when the Subject of the Certificate is a natural person associated with a Subject - legal entity and the Subject requests revocation;
- In case of a court decision without right to appeal ordering revocation of the Certificate;
- KIBSTrust private key is compromised;
- The Supervisory Body requests revocation under the law;
- The identity of the Subject has not been successfully re-verified;
- The Subject did not make a due payment;
- Continuing to use that Certificate is harmful to KIBSTrust;
- There have been changes in the standards and technical requirements adopted by the CA / B Forum and / or the regulations and laws of the EU and the Republic of North Macedonia.

When considering whether the use of a Certificate is harmful to KIBSTrust, KIBSTrust shall consider, inter alia:

- The nature and number of complaints received;
- The identity of the person who made the complaints;
- Relevant regulations in force;
- The responses to the alleged harmful use by the Subject.

KIBSTrust may also revoke an administrator Certificate if the administrator's authorization to act as an administrator has been terminated or otherwise ended.

Under the KIBSTrust Terms and Conditions, the Subject of electronic identification is obliged to immediately notify KIBSTrust of any knowledge or presumption that its private key has been compromised.

Upon approval of the revocation application by KIBSTrust, the revoked Certificate may not take effect again.

4.9.2. Who may Request Revocation

An application for revocation of a Qualified Certificate can be submitted by:

- RA;
- the Subject of the electronic identification, or its legal representative, or successor who wishes to request revocation in case of a deceased Subject (natural person) provided that it is legally qualified;
- Competent court or body;
- Supervisory body.

An application for revocation of a CA Certificate (root or issuing) can be submitted by:

- KIBS, which is a Subject of the Certificate, legally qualified;
- Competent court or body;
- Supervisory body.

4.9.3. Procedure for Revocation Application

The Subject requesting revocation is required to communicate the request to KIBSTrust in one of the following ways: via the online revocation service, by e-mail to revoke@kibstrust.com, or a form in a printed copy of the Certificate revocation which is submitted personally to the RA, whereupon the revocation of the Certificate will be initiated immediately.

The submission of such an application for revocation shall be according to Section 3.4.

4.9.4. Revocation Application Grace Period

Revocation applications shall be submitted in the shortest possible time, within a commercially reasonable time.

4.9.5. Time within which KIBS CA must Process the Revocation Application

KIBSTrust shall take commercially reasonable steps to process revocation applications without delay and in any case, the maximum delay from the moment KIBSTrust receives a revocation application, according to Section 4.9.3, until the decision to change the status information available to all Relying Parties shall be 24 hours at the most. If the revocation application cannot be confirmed within 24 hours, then the status should not be changed.

Immediately after the approval of the revocation application, KIBSTrust shall notify the Subject for the realization of the revocation via e-mail.

4.9.6. Revocation Verification Requirements for Relying Parties

Relying Parties shall check the status of the Certificate they wish to rely on. One method Relying Party may verify the Certificate status is to consult the latest KIBSTrust CRL that issued the Certificate on which the Relying Parties wish to rely. Alternatively, Relying Parties may check the Certificate status using the KIBSTrust web-based repository or by using technology provided by OCSP Responder. KIBSTrust will provide the Relying Parties with information on how to find the appropriate CRL, web-based repository or OCSP Responder to check for the revocation status. Due to the numerous and different locations for CRL repositories, the Relying Parties will be notified to access CRL using the URL embedded in the extension for CRL Certificate Distribution Points.

The appropriate OCSP Responder for the given Certificate is included in its extension for accessing Issuer's information.

Revocation status information is made available after the validity period of the Certificate.

4.9.7. CRL Issuance Frequency

CRL for Subject - end user Certificates are issued at least once a day. CRLs for KIBSTrust Certificates are issued at least annually, but also whenever a CA Certificate is revoked. If the Certificate listed in the CRL expires, it can be removed in the next issued CRL, after the Certificate's expiration.

4.9.8. Maximum Latency for CRLs

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

4.9.9. Availability for On-line Verification of Revocation Status

Online revocation information, as well as other Certificate status information, are available through the web-based repository and OCSP. In addition to publishing the CRL, KIBSTrust provides Certificate status information through query functions in the KIBSTrust repository. Certificate status information for Qualified Certificates is available in the KIBSTrust repository at: https://pki.kibstrust.com/repository.

OCSP responses are provided within a commercially reasonable time upon receipt of the application, which is subject to delayed transmission over the Internet. OCSP responses are according to RFC 5019 and /or RFC 6960. OCSP responses are:

1. Signed by the CA that issued the Certificates whose revocation status is being checked, or
2. 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 id-pkix-ocspnocheck extension, as defined by RFC 6960.

The maximum delay between the verification of the Certificate revocation to become effective and the actual

change of the status information of this Certificate being made available to the Relying Parties is at the most 60 minutes. If, however, the revocation application requires revocation in advance (e.g., Subject's planned cessation of duties on a specific date), then the scheduled date may be considered as confirmation time.

4.9.10. On-line Revocation Checking Requirements

Relying Party must check the status of the Certificate on which it wishes to rely. If the Relying Party does not verify the status of the Certificate on which the Relying Party wishes to rely by consulting the latest relevant CRL, the Relying Party shall check the status of the Certificate by consulting the KIBS repository or by requesting Certificate status using the appropriate OCSP Responder.

4.9.11. Other Available Forms of Revocation Publishing

Not applicable.

4.9.12. Special Requirements Regarding Key Compromise

KIBS makes a commercially reasonable effort to notify potential Relying Parties if it discovers, or has 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 may Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Application

Not applicable.

4.9.16. Limits on the Suspension Period

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Certificate status information is available through CRL and OCSP Responder. The serial number of the revoked Certificate remains in the CRL until another additional CRL is issued after the expiration date of the Certificate. OCSP information on subscriber Certificates is updated according to Section 4.9.9.

4.10.2. Service Availability

KIBS provides 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% per year.

4.10.3. Optional Characteristics

Not applicable.

4.11. End of Subscription

Subject may terminate the subscription for a KIBS Qualified Certificate:

- by allowing his / her Qualified Certificate to expire without re-keying that Certificate;
- by revoking the Qualified Certificate before its expiration, without making a replacement.

4.12. Key Escrow and Recovery

Not applicable.

4.12.1. Kew 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

Refer to item 5.1. from the CP / CPS document.

5.1.1. Site Location and Construction

Refer to item 5.1.1 from the CP/CPS document.

5.1.2. Physical Access

Refer to item 5.1.2 from the CP/CPS document.

5.1.3. Electric Power and Air Conditioning

Refer to item 5.1.3 from the CP/CPS document.

5.1.4. Water Exposure

Refer to item 5.1.4 from the CP/CPS document.

5.1.5. Fire Prevention and Protection

Refer to item 5.1.5 from the CP/CPS document.

5.1.6. Media Storage

Refer to item 5.1.6 from the CP/CPS document.

5.1.7. Waste Disposal

Refer to item 5.1.7 from the CP/CPS document.

5.1.8. Off-site Backup

Refer to item 5.1.8 from the CP/CPS document.

5.2. Procedural Controls

5.2.1. Trusted Roles

Refer to item 5.2.1 from the CP/CPS document.

5.2.2. Number of Persons Required per Task

Refer to item 5.2.2 from the CP/CPS document.

5.2.3. Identification and Authentication for Each Role

Refer to item 5.2.3 from the CP/CPS document.

5.2.4. Roles Requiring Separation of Duties

Refer to item 5.2.4 from the CP/CPS document.

5.3. Personnel Controls

Refer to item 5.3 from the CP/CPS document.

5.3.1. Qualifications, Experience and Clearance Requirements

Refer to item 5.3.1 from the CP/CPS document.

5.3.2. Background Check Procedures

Refer to item 5.3.2 from the CP/CPS document.

5.3.3. Training Requirements

Refer to item 5.3.3 from the CP/CPS document.

5.3.4. Retraining Frequency and Requirements

Refer to item 5.3.4 from the CP/CPS document.

5.3.5. Job Rotation Frequency and Sequence

No rotation is performed.

5.3.6. Sanctions for Unauthorized Actions

Refer to item 5.3.6 from the CP/CPS document.

5.3.7. Independent Contractor Prerequisites

Refer to item 5.3.7 from the CP/CPS document.

5.3.8. Documentation Provided to Personnel

Refer to item 5.3.8 from the CP/CPS document.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

KIBS shall ensure that all relevant information relating to the operation of Trust Services is recorded to provide evidence intended for legal proceedings. This information includes the archival records required to prove the validity of the Trust Service operation.

KIBS manually or automatically logs the following significant events:

- CA certificates and keys life cycle management events, including:
  - Key generation, backup, storage, renewal, archiving, and destruction,
  - Modifications to CA details or keys,
  - Events related to the life cycle management of cryptographic devices.
- Subscriber Certificates and keys life cycle management events, including:
  - Certificate Applications, issuance, renewal of a new key pair and revocation,
  - Key generation, backup, storage, recovery, archiving and destruction;
  - Successful or unsuccessful processing of applications,
  - Changes in Certificate creation policies,
  - Generation and issuance of Certificates and CRL,
  - Using the Certificate for Electronic signing,

  - Attempts to login of a registered user.
- Events related to Electronic Identification Services
  - Registration of a new user to a mobile application,
  - Verification of personal identification documents,
  - Verification of the liveliness of the person,
  - Confirmation of biometric data from liveliness detection and photography of the personal identification document,
  - Checking someone's electronic identity from the Relying Party systems,
  - Use of the electronic identity for authentication of the holder.
- Events for trusted employees, including:
  - Login and logout attempts,
  - Attempts to create, remove, set passwords or change system privileges for all privileged users,
  - Personnel changes.
- All important safety-related events, which include:
  - Successful or unsuccessful attempts to access the PKI system,
  - Starting and shutting down systems and closing applications,
  - Possession of activation data for CA private key operations,
  - PKI and security system activities carried out by KIBS personnel,
  - Security sensitive documents or records that have been read, written, or deleted,
  - Changes in the rules in the Security Policy,
  - System crashes, hardware failures, and other anomalies,
  - Activities related to firewalls and routers,
  - Entry /exit of visitors in the premises of the CA,
  - Input /output for remote QSCD access.

Log entries include the following elements:

- Date and time of entry,
- Series or consecutive number of records,
- Identity of the entity making the journal entry,
- Entry type.

Certificate Application information from the KIBS RA logbook, including:

- Type of identification document (s) presented by the Certificate Applicant;
- Records of unique identification data, numbers, or a combination thereof (for example, ID card number of the Certificate Applicant) of identification documents, if applicable. Storage location of application copies, and identification documents for Qualified Certificates,
- All special choices in the Certificate Application,
- Identity of the Subject that accepts the application and in case of Qualified e-Seals, the identity of the natural person representing the legal entity to which the Qualified Certificate for Electronic Seal is issued,
- Method used to verify (validate) identification documents, if any,
- Name of receiving CA or submitting RA, if applicable.

5.4.2. Frequency of Audit Log Review

Refer to item 5.4.2 from the CP/CPS document.

5.4.3. Retention Period for Audit Log

Refer to item 5.4.3 from the CP/CPS document.

5.4.4. Protection of Audit Log

Refer to item 5.4.4 from the CP/CPS document.

5.4.5. Audit Log Backup Procedures

Refer to item 5.4.5 from the CP/CPS document.

5.4.6. Audit Collection System (Internal vs. External)

Refer to item 5.4.6 from the CP/CPS document.

5.4.7. Notification to Event-Causing Subject

Refer to item 5.4.7 from the CP/CPS document.

5.4.8. Vulnerability Assessment

Refer to item 5.4.8 from the CP/CPS document.

5.5. Records Archival

5.5.1. Types of Records Archived

KIBS archives:

- All audit data collected according to the requirements of Section 5.4.,
- Certificate Application information,
- Documentation attached to the Certificate Applications,
- Data from the electronic verification of the identity of the Applicant,
- Certificate life cycle information,
- Approval and rejection of the revocation application,
- CP and CP / CPS versions,
- Audit reports of the conformity assessment,
- KIBS certification,
- Appointment of an individual for a trusted role.

5.5.2. Archive Retention Period

The storage period in the archive is described in Section 5.4.3.

5.5.3. Protection of Archive

Refer to item 5.5.3 from the CP/CPS document.

5.5.4. Archive Backup Procedures

Refer to item 5.5.4 from the CP/CPS document.

5.5.5. Requirements for Time-Stamping of Records

Refer to item 5.5.5 from the CP/CPS document.

5.5.6. Archive Collection System

Refer to item 5.5.6 from the CP/CPS document.

5.5.7. Procedure for Obtaining and Verifying Archived Information

Refer to item 5.5.7 from the CP/CPS document.

5.6. Key Changeover

Refer to item 5.6 from the CP/CPS document.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Refer to item 5.7.1 from the CP/CPS document.

5.7.2. Compromised Computer Resources, Software and/or Data

Refer to item 5.7.2 from the CP/CPS document.

5.7.3. CA Private Key Compromise Procedures

Refer to item 5.7.3 from the CP/CPS document.

5.7.4. Business Continuity Capabilities after a Disaster

Refer to item 5.7.4 from the CP/CPS document.

5.8. CA or RA Termination

Refer to item 5.8 from the CP/CPS document.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Refer to item 6.1.1 from the CP/CPS document.

6.1.2. Private Key Delivery to Subject

Subject – end user key pair is generated on a Subject-operated remote QSCD and no physical delivery of the Subject's private key is applicable. The private key is activated by the holder and only he can use it for Electronic Signature using his credentials and applying strict authentication.

6.1.3. Public Key Delivery to the Certification Authority

This requirement does not apply when the Subject key pair has previously been generated by KIBS.

6.1.4. CA Public Key Delivery to the Relying Parties

Refer to item 6.1.4 from the CP/CPS document.

6.1.5. Key sizes

Refer to item 6.1.5 from the CP/CPS document.

6.1.6. Public Key Parameters Generation and Quality Checking

Refer to item 6.1.6 from the CP/CPS document.

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

Refer to item 6.1.7 from the CP/CPS document.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Refer to item 6.2 from the CP/CPS document.

6.2.1. Cryptographic Module Standards and Controls

Refer to item 6.2.1 from the CP/CPS document.

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

Refer to item 6.2.2 from the CP/CPS document.

6.2.3. Private Key Escrow

Refer to item 6.2.3 from the CP/CPS document.

6.2.4. Private Key Backup

Refer to item 6.2.4 from the CP/CPS document.

6.2.5. Private Key Archival

Refer to item 6.2.5 from the CP/CPS document.

6.2.6. Private Key Transfer to or from a Cryptographic Module

Refer to item 6.2.6 from the CP/CPS document.

6.2.7. Private Key Storage on Cryptographic Module

Refer to item 6.2.7 from the CP/CPS document.

6.2.8. Method of Activating Private Key

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

The private keys for the electronic identity of the Subject that are on remote QSCD are protected with username, password, OTP codes, and inclusion of biometric protection on the user's mobile application. The following rules apply:

- Username, password, and OTP code on QSCD are required for each transaction,
- The Subject is obliged to create PIN code for access to the mobile application in which his username and password are safely stored,
- PIN code is required to create an OTP for each transaction,
- The user of the mobile application can set up biometric authentication so that he does not have to enter the PIN code,
- In case of incorrect username, password, and OTP code 5 times in a row, the remote account of QSCD is locked,
- The QSCD remote account cannot be reset with a password,
- The user can change the PIN-code on the mobile application.
- The user can change the password through the web portal after authentication.

The CA private key shall be activated online with a limited number of Shareholders, as defined in Section 6.2.2 of the CP / CPS, by submitting their activation data (stored on secure media). Once the private key is activated, it may be active for an indefinite period until it is deactivated when the CA is disconnected from the network (goes offline). Similarly, a threshold number of Shareholders shall be required to submit their activation data to activate an offline CA's private key. Once the private key is activated, it shall only be active once.

6.2.9. Method of Deactivating Private Key

KIBS CA private keys are deactivated by shutting down the cryptographic module.

Subjects' private keys may be deactivated after each operation, after logging off from the system or by removing the local QSCD from the system, or after logging off from the remote QSCD. In any case, Subjects should adequately protect their private key (s) according to CP / CPS.

6.2.10. Method of Destroying Private Key

Where required, KIBS destroys the CA private keys and Subject's private keys in a manner that provides reasonable assurance that there are no key residuals that could lead to key reconstruction. KIBS uses the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. In the course of destruction, records of the activities are made.

6.2.11. Cryptographic Module Rating

Refer to Section 6.2.1

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to item 6.3.1 from the CP/CPS document.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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

Certificate issue by:	Use of private key	Validity period
Root CA	No stipulation	Normally up to 20 years
Issuing CA	No stipulation	Normally up to 10 years
Certificate with Long Lived Validity	No stipulation	Normally 1-3 years
Certificate on remote QSCD	Authentication and Electronic Signature	2 years

Table: Certificate Operational Period

In addition, KIBS CA ceases to issue new Certificates on an appropriate date (60 days plus the maximum validity period of the issued Certificates) before the expiration of the CA Certificate, so that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates. The lifetime of the Subject's Certificates will not exceed the lifetime of the CA's signing certificate.

Subjects will stop using all key pairs after their periods of use have expired.

If the algorithm or the corresponding key length offers no sufficient security during the validity period of the Certificate, the concerned Certificate will be revoked and an application for a new Certificate will be initiated.

The applicability of cryptographic algorithms and parameters is constantly supervised by KIBS management.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Refer to item 6.4.1 from the CP/CPS document.

6.4.2. Activation Data Protection

Refer to item 6.4.2 from the CP/CPS document.

6.4.3. Other Aspects of Activation Data

Refer to item 6.4.3 from the CP/CPS document.

6.5. Computer Security Controls

6.5.1. Special Computer Security Technical Requirements

Refer to item 6.5.1 from the CP/CPS document.

6.5.2. Computer Security Rating

Not applicable.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Refer to item 6.6.1 from the CP/CPS document.

6.6.2. Security Management Controls

Refer to item 6.6.2 from the CP/CPS document.

6.6.3. Life Cycle Security Controls

Refer to item 6.6.3 from the CP/CPS document.

6.7. Network Security Controls

Refer to item 6.7 from the CP/CPS document.

6.8. Time-Stamping

Refer to item 6.8 from the CP/CPS document.

7. CERTIFICATE, CERTIFICATE REVOCATION LIST (CRL) AND ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) PROFILES

7.1. Certificate Profile

The Certificate profile is according to X.509 v.3, IETF RFC 5280, and clause 6.6.1 of ETSI EN 319 411-1.

For more details refer to item 7.1 from the CP/CPS document.

7.2. CRL Profile

CRL profile is according to X.509 version 2 and IETF RFC 5280.

For more details refer to item 7.1 from the CP/CPS document.

7.3. OCSP Profile

OCSP profile of KIBSTrust complies with IETF RFC 6960. For more details refer to item 7.1 from the CP/CPS document.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The conformity of the information system, policies and practices, facilities, personnel, and assets of KIBS is assessed by a Conformity Assessment Body according to MK-eIDAS law and eIDAS regulations, relevant laws, and standards or whenever a major change in the Trust Service operations is made, based on the ETSI standards listed in Section 9.15.

In addition to compliance audits, KIBS is entitled to conduct other reviews and surveys to ensure the trustworthiness of KIBSTrust certification services. KIBS is entitled to delegate the performance of these audits, reviews, and investigations to a third-party audit company.

KIBS is entitled to conduct external audits of KIBS-related contractors to act as authentication agents.

8.1. Frequency and Circumstances of Assessments

The KIBSTrust Conformity Audit is performed at least annually. The audits are performed in continuous series of audit periods, and each period lasts no longer than one year.

8.2. Identity and Qualification of Audit

The KIBS CA Compliance Audit is performed by:

- Internal auditors,
- Conformity Assessment Body accredited according to EC Regulation no. 765/2008, ETSI standards (that is, ETSI EN 319 403),
- Supervisory Body.

8.3. Assessor's Relationship to Assessed Subject

The auditor of the Conformity Assessment Body shall be independent of KIBS and KIBS assessed systems. The internal auditor shall not audit his areas of responsibility.

8.4. Topics Covered by Assessment

The conformity assessment covers the compliance of the information system, policies and practices, facilities, personnel and assets of KIBS with MK-eIDAS and eIDAS regulations, relevant laws, and standards. The

Conformity Assessment Body audits parts of the information system used to provide Trust Services.

Areas of activity subject to internal auditing are as follows:

- Quality of service;

- Security of the service;
- Security of operation and procedures;
- Data protection of Subjects and Security Policy, execution of work procedures and contractual obligations, as well as compliance with CP and service-based Policies and Practices Statements.

The Conformity Assessment Body and the Internal auditor also audit these parts of the information system, policies and practices, facilities, personnel, and assets of the subcontractors related to the provision of KIBS Trust Services.

8.5. Actions Taken as a Result of Deficiency

Concerning 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 by entering data 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 Trust Services, a corrective action plan will be developed within 30 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 case of established deficiency by the Conformity Assessment Body, the Supervisory Body shall request KIBS to eliminate any non-compliance with the requirements within a timeframe (if applicable) determined by the Supervisory Body. KIBS shall make efforts to remain consistent and meet all deficiency requirements in a timely manner. KIBS management is responsible for implementing the corrective action plan. KIBS shall assess the significance of deficiencies and prioritize appropriate actions to be taken at least within the time limit set by the Supervisory Body or within a reasonable period of time.

When personal data protection rules appear to be violated, the Supervisory Body shall notify the Data Protection Authority of the compliance audit results.

8.6. Communication of Results

The conclusions of the audit or Certificate (s) for Trust Services, based on the audit results of the Conformity Assessment Body, conducted according to MK-eIDAS law and eIDAS regulations, relevant laws, and standards, may be published on the web -KIBS website https://pki.kibstrust.com/repository .

In addition, KIBS shall submit the received conformity assessment report to the Supervisory Body within three (3) working days from its receipt. KIBS shall submit the audit conclusions or Certificate (s) for Trust Services to the Root Browsers program maintainers in which KIBS and other interested parties participate.

Results of the compliance audit of KIBS CA operations may be released at the discretion of KIBS management.

8.7. Self-audits

KIBS shall conduct regular internal audits to determine compliance according to Section 8.4.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Electronic Identification Means Issuance Fee

KIBSTrust charges customers for its Electronic Identification Services. Clients are primarily legal entities – Relying Parties but depending on the needs, clients can also be natural persons. The fee includes but is not limited to the number of electronic remote recognitions, number of consents for transfer of the attributes from the Electronic Identification Means, and number of uses of the Qualified Certificate for Electronic Signatures.

9.1.2. Certificate Access Fees

KIBSTrust may charge a fee as a condition of making the Certificates available in the repository or otherwise making the Certificates available to the Relying Parties.

9.1.3. Certificate Revocation or Status Information Access Fees

KIBSTrust does not charge any fee for accessing the Certificate revocation or status information. The Certificate status information is available through OCSP and CRL which are available through the repository or otherwise available to the Relying Parties. KIBSTrust does not permit access to the Certificates status information in its repositories to third parties that use such Certificate status information when providing products or services, without Subject's prior express consent.

9.1.4. Fees for Other Services

KIBSTrust does not charge any fees for accessing this document. Any use other than simply viewing the document, such as reproduction, redistribution, modification, or creation of texts resulting therefrom shall be subject to a license agreement with KIBS.

9.1.5. Refund Policy

9.1.5.1. Remote Sales

KIBS shall not accept any claims for Certificate's deficiencies and damages caused by fault or activities undertaken by the Subject.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

KIBS maintains a commercially reasonable level of professional liability insurance for errors and omissions through the error and omission program with the Insurance Company. Insurance Policy Certificate is available in the KIBS public repository at http://www.kibstrust.com/repository .

The rules of indemnification according to the Professional Liability Insurance of the Trust Service Provider KIBS (hereinafter: Rules) follow the MK-eIDAS law. Under MK-eIDAS bylaw[6], TSP KIBS is fully adapted to the established requirements for the risk coverage amount of liability for damages. For each trust 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 Trust Service Provider.

9.2.2. Other Assets

KIBS has sufficient financial resources to maintain its operations and perform its duties, as well as a reasonable ability to bear the risk of liability to Subjects and Relying Parties. Proof of financial resources is not publicly available.

9.2.3. Insurance or Warranty Coverage for End-Entities

Refer to section 9.2.1. of these Practices.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

All information that has become known when providing services that is not intended to be disclosed (e.g. information known to KIBSTrust for operation and provision of its services) is confidential. The Subject is entitled to obtain information from KIBSTrust about itself, according to the applicable laws.

9.3.2. Information Considered to be non-Confidential

Any information not listed as confidential or intended for internal use is public. Information considered public in KIBSTrust is listed in Section 2.2 of these Practices.

In addition, non-personalized statistical data about KIBSTrust services is considered public information. KIBS may publish statistical data regarding its non-personalized services.

9.3.3. Responsibility to Protect Confidential Information

[6] Rulebook on determining the minimum 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 Qualified Trust Services Provider

KIBSTrust protects confidential information and information intended for internal use from compromise and disclosure to third parties by implementing various security controls.

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

9.4. Privacy of Personal Information

9.4.1. Privacy Policy

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

9.4.2. Information Treated as Private

Any information about the Subject that is not publicly available through the content of the issued Certificate, Certificate Directory, and online CRL is treated as private.

9.4.3. Information not Deemed Private

Subject to applicable laws, all information made public in a Certificate is not considered private.

9.4.4. Responsibility to Protect Private Information

KIBS shall protect personal data from compromise and disclosure to third parties and shall comply with applicable laws on personal data protection.

9.4.5. Notice and Consent to Use Private Information

According to the relevant Law on Data Protection, the applicable Privacy Policy, and the accepted Terms and Conditions of use, personal data are not used without the consent of the party to which the information refers.

9.4.6. Disclosure According to Judicial or Administrative Process

KIBS is entitled to disclose confidential information if, in good faith, KIBS believes that:

- Disclosure is necessary in response to a subpoena and a search warrant;
- Disclosure is necessary in response to court, administrative, and other legal proceedings during investigative proceedings in a civil or administrative proceedings, such as a subpoena, interrogation, request for admission, and a request for production of documents.

This Section is subject to the applicable laws on the territory of the state.

9.4.7. Disclosure upon Owner's Request

The Privacy Policy contains provisions relating to the disclosure of personal data of the person who provided that information to KIBS. This section is under the applicable Law on Personal Data Protection.

9.4.8. Other Information Disclosure Circumstances

Not applicable.

9.5. Intellectual Property Rights

The allocation of Intellectual Property Rights among KIBS partners, other than Subjects and Relying Parties, is governed by the applicable agreements entered into between those participants and KIBS. The following sub-sections refer to the Intellectual Property Rights related to the Subjects and Relying Parties.

9.5.1. Property Rights of Information in Certificates and Revocation Information

KIBS reserves all Intellectual Property Rights in and to the Certificates and revocation information it issues. KIBS grants permission to reproduce and distribute Certificates on a non-exclusive royalty-free basis, provided that they are reproduced in full and the use of the Certificates is governed by the Terms and Conditions outlined in the Certificate. KIBS grants permission to use the revocation information to perform the Relying Parties functions subject to the applicable Terms and Conditions, or any other applicable agreements.

9.5.2. Property Rights in this Practice

Subjects acknowledge that KIBS reserves all Intellectual Property Rights in these Practices and the relevant CP / CPS.

9.5.3. Property Rights in Names

Certificate Applicant reserves all rights (if any) to the trademark, service mark, or trade name contained in the Certificate Application and the distinguished name in the Certificate issued to such Certificate Applicant.

9.5.4. Property Rights in Keys and Key Material

The key pairs corresponding to Certificates of CA and Subjects – end users are the property of CA and the Subjects

– end users that are Subjects of those Certificates, regardless of the physical medium in which they are stored and protected, and those persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, KIBS root public keys and root Certificates containing them, keys, and self-signed Certificates are the property of KIBS. Finally, the Secret Shares of the CA private keys are the property of CA and CA retains all Intellectual Property Rights to those Secret Shares, although it may not acquire physical ownership of those shares or the CA from KIBS.

9.5.5. Violation of Property Rights

KIBS intentionally does not infringe the Intellectual Property Rights of any third party.

9.6. Representations and Warranties

9.6.1. Representations and Warranties of the Issuer of Electronic Identification Means

KIBSTrust warrants that:

- Provides its services according to the requirements and procedures defined in these Practices and related documents;
- Complies with MK-eIDAS, eIDAS, and related legal acts set out in these Practices and related documents;
- Publishes its Practices and related documents and guarantees their availability in the public data communication network;
- Publishes and meets the requirements of the Terms and Conditions for Subjects and guarantees their availability and access to the public data communication network;
- Maintains confidentiality of the information received during the supply of the service and which is not subject to publication;
- Keeps account of the Electronic Identification Means issued by it and their validity, and provides an opportunity to check the validity of the Certificates;
- Provides access to the private keys of the remote QSCD to the authorized Subject of the key;
- Ensures proper management and compliance of the remote QSCD;
- Informs the Supervisory Body of any changes to the public key used to provide Trust Services;
- Without undue delay, but in any case, within 24 hours after learning of any security breach or loss of integrity that has a significant impact on the provided service or the personal data contained therein, it shall notify the Supervisory Body and, where appropriate, other relevant bodies such as the national CERT or the Data Inspectorate.
- When security breach or loss of integrity is likely to adversely affect a natural or legal person to whom service has been provided, it shall notify the natural or legal person of the security breach or loss of integrity without undue delay;
- Keeps all documentation, records, and logs related to the services according to items 5.4 and 5.5;
- Provides conformity assessment according to the requirements and presents the conclusion of the Conformity Assessment Body to the Supervisory body to ensure the continuous status of services registered in the Register of MISA;
- Has the financial stability and resources required to operate according to these Practices;
- Publishes the conditions of the compulsory insurance policy and the conclusion of the Conformity Assessment Body in the public data communication network;
- Provides access to its services for persons with disabilities, if possible;
- There is no material misrepresentation of a fact in the Electronic Identification Means, known or originating from the entities through which the application for issuance of Electronic Identification Means is approved.

Terms and conditions for using KIBS services may include additional statements and warranties.

9.6.2. CA Representations and Warranties

KIBSTrust warrants that:

- The identity of the Subject is verified through procedures approved by KIBSTrust,
- There is no material misrepresentation of a fact in the Certificate that is known or originating from the Subjects approving Certificate Application or issuing Certificate,
- There are no errors in the Certificate information provided by the entity approving the Certificate Application as a result of failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of the applicable CP / CPS, and
- Revocation services (where applicable) and repository use are compliant with the applicable CP / CPS in all material aspects.

KIBS Terms and Conditions may include additional statements and warranties.

9.6.3. Subject Representations and Warranties

Subjects warrant that:

- All statements made by the Subject in the application to create an Electronic Identification Means are true, and the Subject is aware that KIBSTrust may refuse to provide the service if the Subject intentionally provided false, inaccurate, or incomplete information in the service application;
- The Subject complies with the requirements given by KIBSTrust in these Practices and related documents;
- All information submitted by the Subject and contained in the means is true and in case of change of the submitted data, the Subject should report the correct data according to the rules established by these Practices and related documents;
- The means is used exclusively for authorized and legal purposes, according to these Rules;
- Any e-Signature or e-Seal created using the private key corresponding to the public key specified in the Qualified Certificate is a Qualified e-Signature or e-Seal of the Subject and the Qualified Certificate is accepted and operational (not expired or revoked) at the time the Qualified e-Signature or e-Seal is created,
- Credentials such as PIN, username, password, OTP, etc. that access the private key are protected and no unauthorized person has ever had access to them,
- Qualified e-Signature is only created on QSCD,
- The Subject is not a CA, and does not use the private key corresponding to the public key specified in the Certificate to digitally sign any Certificate (or any other form of the certified public key) or CRL, as a CA or otherwise;
- The Subject will notify KIBS without delay if the Subject's private key is stolen or potentially compromised, or the control over it has been lost.

KIBS Terms and Conditions for use of Qualified Trust Services may include additional statements and warranties.

9.6.4. Representations and Warranties of the Relying Party

According to the KIBS Terms and Conditions for the use of the service, the Relying Party is required to confirm that it has sufficient information to decide on the extent to which it will choose to rely on the information in the Certificate which is part of the Electronic Identification Means, that it is solely responsible for deciding whether or not to rely on such information, and that it shall bear the legal consequences of the failure to perform the obligations of the Relying Party according to these Practices.

KIBS Terms and Conditions for use of Qualified Trust Services may include additional statements and warranties of the Relying Parties.

9.6.5. Representations and Warranties of Other Participants

Not applicable.

9.7. Disclaimer of Warranties

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

KIBS is not responsible for:

- The secrecy of the credentials (PIN, username, password, OTP) that grant access to the private keys of the Subjects, possible misuse of Certificates or improper Certificate checks or wrong decisions of the Relying Parties, or any consequences due to errors or omissions in Trust Service validation checks;
- The non-performance of its obligations, if such non-performance is due to errors or security problems of the Supervisory Body, the Data Protection Supervisory Authority, Trusted List or any other public authority;
- The non-fulfillment of its obligations or creation of additional expenses for its service users as a consequence of technical standards change;
- The non-performance of the obligations arising from these Practices and related documents, if such non-performance is caused by Force Majeure.

9.8. Limitations of Liabilities

KIBS liability is limited by KIBS Terms and Conditions for the use of Qualified Trust Services. Limitations of liability include the exclusion of indirect, special, incidental, and consequential damages. They also include limitation of liability in the amount of five hundred euros (€ 500.00) expressed in denar counter-value according to the NBRSM middle exchange rate, limiting KIBS damages concerning a Qualified Certificate.

The liability (and/or limitation thereof) of Subjects and Relying Parties is set forth in the relevant Subscriber Agreements for the use of Qualified Trust Services.

9.9. Indemnities

9.9.1. Indemnification by Subjects

To the extent prescribed by the applicable law, Subjects are expected to indemnify KIBS for:

- Forgery or misinterpretation of facts by the Subject in the Certificate Application,
- Failure by the Subject to present a material fact in the Certificate Application, if the misinterpretation or omission is made by negligence or with intend to deceive any party,
- Failure of the Subject to protect Subscriber's private key, use of the Trust System or otherwise fail to prevent compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The use of a name (including without limitation within a common name, domain name, or e-mail address) by the Subject that infringes the Intellectual Property Rights of a third party.

The Subscription agreement may include additional indemnity obligations.

9.9.2. Indemnification by Relying Parties

To the extent prescribed by the applicable law, KIBS Terms and Conditions for the use of Qualified Trust Services require the Relying Party to indemnify KIBS in the event:

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

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

9.10. Term and Termination

9.10.1. Term

These Practices become effective upon publication in the KIBS repository. Amendments to these Practices become effective upon publication in the KIBS repository.

9.10.2. Termination

These Practices as amended from time to time remain in force until they are superseded with a new version.

9.10.3. Effects of Termination and Extension

Notwithstanding the termination of the validity of these Practices, KIBS PKI Participants are bound by all the conditions for all issued Certificates for the remainder of the validity period of such Certificates.

9.11. Individual Notices and Communication 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 available means of communication.

9.12. Amendments

9.12.1. Procedure for Amendments

Amendments to these Practices are made by KIBSTrust's Policy Management Authority (PMA). Amendments are in the form of a document containing an amended form of the document or an update. Versions with the amendments or updates associated with the KIBS repository are published at https://pki.kibstrust.com/repository/ .

Updates supersede any specified or conflicting provisions of the specified version of the document.

9.12.2. Notification Mechanism and Period

KIBS PMA reserves the right to amend these Practices and /or CP / CPS without notice for the amendments that are not material, including without limitation correction of typographical errors, changes of URLs, and changes in contact information. The decision of PMA to designate amendment as material or non-material is at the discretion of PMA.

Proposed amendments to these Practices and related CP / CPS are published in the KIBS repository located at: https://pki.kibstrust.com/repository/.

Notwithstanding anything contained in these Practices and CP / CPS to the contrary, if PMA believes that material amendments to these Practices and CP / CPS are necessary to immediately stop or prevent a breach of the security of KIBS as an Issuer of Electronic Identification Means and as a Trust Service Provider (TSP) or any part thereof, KIBS and PMA shall be entitled to make such amendments by publication in the KIBS repository. Such amendments shall enter into force immediately upon publication. At a reasonable time after publication, KIBS shall notify KIBS PKI participants of such amendments.

At a minimum, KIBS and PMA will update these Practices annually, in compliance with the CA / Browser Forum guidelines.

Amendments that do not change the meaning of these Practices, such as spelling corrections, translation, and contact details updates, are documented in the Version History section of this document. In this case, the selected portion of the document version number is increased.

In case of substantial changes, the new version of CP / CPS is clearly distinguished from the previous ones and the serial number has been increased by one.

9.12.3. Circumstances that Require Changing the Object Identifier (OID)

If PMA determines that a change in the object identifier corresponding to the Certificate Policy is necessary, the amendments will contain a new object identifier for the Certificate Policies. Otherwise, amendments do not require a change in the object identifier of the Certificate Policy.

9.13. Dispute Resolution Provisions

9.13.1. Disputes among KIBS, Affiliates, and Clients

Disputes among participants in KIBS PKI are resolved under the provisions of the applicable agreements among the parties.

9.13.2. Disputes with Subjects -End Users 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 a court dispute in the competent court in Skopje.

9.14. Governing Law

The laws of the Republic of North Macedonia govern the execution, compilation, interpretation, and validity of these Practices, regardless of the agreement or the choice of other legal provisions and without a request to establish a commercial liaison in the country. This choice of law is made to ensure uniform procedures and interpretation for all KIBS PKI participants, regardless of where they are located.

This governing law provision applies only to these Practices. Agreements incorporating these Practices only by reference may have their governing law provisions, provided that Section 9.14 governs the execution, composition, interpretation, and validity of the terms of these Practices separate and apart from the other provisions of any such agreement subject to any limitations that arise in the applicable law.

9.15. Compliance with Applicable Law

KIBS ensures compliance with the legal requirements to meet all applicable legal requirements for the protection of records against loss, destruction, and forgery and the requirements of the following:

- MK-eIDAS - Law on Electronic Documents, Electronic Identification and Trust Services (Official Gazette of the Republic of Northern Macedonia 101/19 ... 215/19);
- ID eIDAS - Regulation (EU) no. Regulation (EC) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions on the internal market and repealing Directive 1999/93 / EC;
- Laws on Personal Data adopted in the Republic of North Macedonia and the associated 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 Services Providers issuing Certificates; Section 1: General Requirements;
  c. ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Certificates; Section 2: Certification Authorities Requirements for issuing Qualified Certificates;
- Basic requirements of the CA/Browser Forum/ Browser.

These Practices are subject to Macedonian laws.

9.16. Miscellaneous Provision

9.16.1. Entire Agreement

Not applicable.

9.16.2. Assignment

All Subjects operating under these Practices may not assign their rights or obligations without the prior written consent of KIBSTrust. Unless specified otherwise in the agreement with a party, KIBS does not give notice of assignment.

9.16.3. Severability

If an article or clause of these Practices is held unenforceable by an appropriate court or other competent authority, the remainder of these Practices shall remain valid.

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

KIBS may claim damages and attorney's fees from the party for damages, losses, and expenses associated with that party's conduct. The failure of KIBS to enforce a provision of these Practices does not waive the right of KIBS to enforce the same provision later or the right to enforce any other provision of these Practices. To be effective, waivers must be in writing and signed by KIBS.

9.16.5. Force Majeure

Non-fulfillment of the obligations arising from CP / CPS and /or related documents shall not be considered a violation if such non-fulfillment is caused by a Force Majeure. Neither party shall claim damages or other compensation from the other parties for delays or non-fulfillment of these Practices and /or related documents caused by Force Majeure.

9.17. Other Provisions

Not applicable.

Appendix A. Table of acronyms and definitions

Table of acronyms

Term	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OTP	One Time Password
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RFC	Request for Comment
TSP	Trusted Service Provider

Table of definition

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.
Certificate for Electronic Signature	Electronic verification that links the data for validation of the Electronic Signature with a natural person and verifies at least the name or pseudonym of that person. Technically it is a user's public key, along with some other information, that is encrypted with the private key of the CA that has issued it, so that it cannot be forged.
Certificate Revocation List (CRL)	A signed list indicating a set of Certificates revoked by the Certification Authority.
Certification Authority (CA)	Authority authorized to create and assign Certificates.
CP/CPS	Rules for the Practices used by the Certification Authority in issuing, managing, revoking, and renewing Certificates or renewing Certificates with re-keying.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure 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	EU Regulation no. 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 on the internal market and abolition of Directive 1999/93 / EC.

Electronic Signature	Data in electronic form that are attached or logically linked to other electronic data, and which the signatory uses to sign.
Terms and Conditions for Using Services	A binding document stating the Terms and Conditions under which a natural or legal person acts as Subject or as Relying Party for the relevant trust services provided by KIBS.
Repository	Website for public information on Policies and Practices for issuing Certificates and Electronic Identification Means and other relevant KIBS information available online.
Certificate with Long-Lived Validity	Qualified Certificate that is valid for 1 to 3 years.
MK-eIDAS	Law on Electronic Documents, Electronic Identification, and Trust Services. (Official Gazette of the Republic of North Macedonia 101/19… 275/19).
KIBSTrust Policy Management Authority (PMA)	A group within KIBS, responsible for publishing this Practice and related documents.
Private Key	A key of a key pair securely held by the key holder, used to create a Qualified Certificate or to decrypt electronic records or files that have been encrypted with the appropriate public key.
Public Key	The key of the key pair that can be publicly disclosed by the holder of the relevant private key and used by the Relying Party to verify a Qualified Certificate, that is, the Electronic Signature created by the appropriate private key of the holder.
Public Key Infrastructure (PKI)	Architecture, organization, techniques, practices, and procedures that jointly support the implementation and operation of a Certificate-based public key cryptographic system. KIBS PKI consists of systems that work together to provide and implement a Certificate-based public key cryptographic system.
Qualified Electronic Signature	Advanced Electronic Signature created by a Qualified Electronic Signature Creation Device based on a Qualified Certificate for Electronic Signature.
Qualified Certificate	A Qualified Certificate is a Certificate issued by CA, which is accredited and supervised by authorities designated by an EU Member State.
Qualified Certificate for Electronic Signature	Certificate for Electronic Signature, issued by a Qualified Trust Service Provider that meets the requirements set out in eIDAS Annex I.
Qualified Trust Service Provider	Trust Service Provider that provides one or more Qualified Trust Services and has been granted qualified status by the Supervisory Body.
Registration Authority (RA)	Entity approved by a TSP to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	Individual or organization that acts in reliance on a Certificate and/or an Electronic Signature.
Remote QSCD	Server-based HSM used to centrally generate and use Subscriber's Private Keys.
Remote Identity Verification	Method /process by which the Subject is identified through a video call session and is equivalent to physical presence validation.
Secret shares	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.

Subordinate CA (Sub CA)	Certification Authority whose issuing Certificate is signed by a Superior CA.
Subject	It may be: - natural person; - natural person identified as being associated with a legal entity; - legal entity (it can be an organization or a unit or department identified as being affiliated with an organization);
Electronic Identification Subject	The natural or legal person initiating an application procedure for issuing Electronic Identification Means before the Issuer of Electronic Identification Means.
Supervisory Authority	Authority designated by a Member State to carry out the supervisory activities of Trust Services and Service Providers under eIDAS. According to MK-eIDAS, it is the Ministry of Information Society and Administration (MISA).
Trust Service	According to the MK-eIDAS law, Trust Services are: - Issuance of Certificates for Electronic Signature, - Issuance of Certificates for Electronic Seal, - Issuance of Certificates for Web pages authenticity, - Electronic Signature storage and validation, - Electronic Seal storage and validation, - Electronic Time Stamps issuance, - Electronic registered delivery, - Trust service for document electronic storage.
Trust Service Provider	A legal entity that provides one or more Trust Services.
Qualified Trust Service Provider	Trust Service Provider supplying one or more Qualified Trust Services and whose status as a Qualified Trust Service Provider is granted by the Minister of Information Society and Administration by registration in the Register of Electronic Identification Schemes and Trust Services. Qualified Trust Service Provider is a legal entity with granted public authorizations, according to the provisions of the MK-eIDAS law.
Trusted person	Employee, contractor, or consultant of an entity responsible for managing the entity's infrastructure security, its products, services, its facilities and /or practices as further defined in CP / CPS Section 5.2.1.
Trusted Role	Position in KIBSTrust that must be held by Trusted Person.
Valid Certificate	Certificate passing the validation procedure specified in RFC 5280.
Validity	The period measured from the date of Certificate issuance to the expiration date.
Electronic Identification	Process of using data for identification of persons in electronic form which represent the natural person or legal entity or authorized person of a legal entity in a unique way.
Electronic Identification Means	Material or non-material means that contain personal identification data used for authentication in electronic services.
Issuer of Electronic Identification Means	A legal entity that meets the requirements set out in the Law on Issuers of Electronic Identification Means.

Electronic Identification Scheme	An electronic identification system according to which the Electronic Identification Means is issued to natural persons or legal entities, or authorized person of a legal entity.

End of document