Terms and Conditions

Terms and Conditions for use of service KIBSTrust OneID

Last modified: 16.08.2022, (view archived versions)

1. General Terms

This document entitled "Terms and Conditions for Use of KIBSTrust OneID Service" (Terms and Conditions) describes the terms set and followed by KIBS AD Skopje when providing service for Electronic Identification and creating an Electronic Identification Means as well as the conditions according to which this service is delivered to the users. KIBS AD Skopje as a company has two main courses of operation: one as a clearing house for small-value interbank payments and a payment operations provider and on the other hand is a Trusted Services Provider (TSP) and Provider of electronic identification service both known under the trademark **KIBSTrust**.

The Terms and Conditions for the KIBSTrust OneID (OneID) Service are based on the document "Practice for Providing Electronic Identification Service" (Practice).

1.1. The "Practice for Providing Electronic Identification Service" regulates the remote identity check and the issuance of an Electronic Identification Means at a prior request of a natural or legal person who is a subject of identification (Subject) in front of an Issuer of electronic identification means.

1.2. The Subject must become familiar with the Practice and accept it. The Practice and the Terms and Conditions constitute a legally binding agreement between the Subject and KIBS.

1.3. The Subject shall voluntarily apply, based on an initiated need, for conducting an electronic identification (eID) by an Online Service Provider or by its own wish to obtain an electronic identification means.

1.4. For the issuance of an electronic identification means, the electronic identification scheme provides:

- remote check of the Subject's identity using a method that enables security equal to physical presence (Article 24, paragraph 1 d of the eIDAS Regulation and Article 31 of the MK-eIDAS). This identity check of the natural person is carried out by using biometric data or physical characteristics that in a unique way connect the person with the personal identification documents for which there is a verification from a trusted source, or
- identity check of the Subject for which a Qualified Electronic Signature has already been issued after its identification with physical presence by a recognized Qualified Trust Service Provider that presented acceptable official identification documents (Article 24, paragraph 1a of the eIDAS Regulation and Article 11 of MK-eIDAS).

1.5. Acceptable identification documents of the Subject are: national ID card for a resident of the Republic of North Macedonia, temporary ID card for foreign nationals with temporary residence in the Republic of North Macedonia, and passport issued by the Republic of North Macedonia.

1.6. KIBSTrust may outsource the whole or part of the process of identity verification to a third party.

1.7. KIBSTrust may refuse to issue an electronic identification means at its discretion if the identity validation using one of the methods listed in paragraph 1.5 is not successful.

1.8. The conditions stated in paragraph 5.4 shall be additionally applied for the Subject, whose identity is confirmed through the method of remote electronic identification. Remote identity verification is available and feasible only when the circumstances during the verification process are sufficient to provide an accurate proof of the Subject's identity.

1.9. The process of conducting electronic identification and issuing an Electronic Identification Means is related to the possession of a smart mobile device by the Subject, installation of OneID Mobile application on the same device, existence of a valid e-mail address and mobile line number accompanying the smart mobile device.

1.10. The Subject shall be legally eligible to initiate the procedure of conducting electronic identification.

1.11. The Subject agrees that the Qualified Certificate created in the process of creating the electronic identity will be placed on a Qualified Signature Creation Device (QSCD) provided by KIBSTrust is a remote means located in its cloud. The Subject is solely responsible for the proper use of the QSCD.

1.12. The Subject may request non-publication of the Certificate which is part of the Electronic Identification Means in the Public Directory of issued Certificates of KIBSTrust.

1.13. The Subject does not pay for the service of creating an electronic identity and using the Qualified Certificate, created in the electronic identification process, when a third-party online service provider initiates the process of electronic identification and / or use of the issued Qualified Certificate.

1.14. KIBS and consequently KIBSTrust as QTSP guarantees observance of the principle of equality and protection against discrimination in the exercise of human rights and freedoms[1].

1.15. KIBSTrust reserves the right, at its discretion, to amend its Practice and the present Terms and Conditions at any time and without notice when there is a justified need for such amendments, i.e. when it is mandatory according to regulatory requirements or changes in standards. Amendments shall be published 30 days before the enforcement. The present version and the previous version are published at https://www.kibstrust.com/repository. The Subject will be duly informed about the amendments to the document.

2. Type of qualified certificate as part of the electronic identification means and its acceptance

2.1. The type and purpose, and issuance procedure of the Qualified Certificate accompanying the Electronic Identification Means are given in the following table:

Certificate type	Purpose	Applied and published Certification Policy
Qualified Electronic Signatures according to МК-eIDAS и eIDAS. Cert Policy IDs: 1.3.6.1.4.1.16305.1.2.5.1.4 (Remote QSCD) and 0.4.0.194112.1.2 (QCP-n-qscd)	Data in electronic form that are attached to or logically associated with other data in electronic form and which are used by the signature to sign.	KIBS CP/CPS for Qualified Certificates for Electronic Signatures, Qualified Electronic Seals and Time-stamps are released at: https://www.kibstrust.com/repository According to ETSI EN 319 411-2 Certificate Policy: QCP-n-qscd Cert Policy ID: 1.3.6.1.4.1. 16305.1.1.5

Table 1

2.2. Qualified Certificates issued in the process of electronic identification and electronic identification means are valid 2 years.

2.3. The following procedure represents acceptance of the electronic identification means:

- Downloading Qualified Certificate as part of the electronic identification means represents acceptance of the electronic identification means by the Subject.
- The Subject will not submit an objection to the Qualified Certificate and its content within 5 days from the issuance of the electronic identification means.

3. Prohibited Electronic Identification Means Usage

3.1. The electronic identification means used for authentication by the Subject may also be used for signing electronic documents, provided that its use is not otherwise prohibited by law, Practice and these Terms and Conditions, as well as other agreements with the Subjects with third parties.

[1] Law on Prevention and Protection against Discrimination

3.2. The Qualified Certificate as part of the Subject's electronic identification means shall not be used outside the limits and context set forth in the "Applied and Published Certification Policy" given in the Table 1 above for Qualified Certificates for Electronic Signature for illegal purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of KIBSTrust that is, KIBS. Indicatively, the use of Qualified Certificate is prohibited for any of the following purposes:

3.2.1. Illegal activities (including cyber-attacks and attempts to misuse the Certificate).

3.2.2. Issuance of new Certificates and information regarding the validity of the Certificate.

3.2.3. Enabling other persons to use the Subject's Private Key.

3.2.4. Enabling the Certificate issued for electronic signature to be used in an automated way.

3.2.5. Use of the Certificate issued for electronic signing of documents which may lead to unwanted consequences (including signing such documents for testing purposes).

4. Validity of the Qualified Certificate and Audit Records

4.1. The information in the Qualified Certificate is correct. There are no errors or substantial misrepresentations of facts in the Certificate that are known or originate from the Subjects that approve the application.

4.2. The Certificate becomes valid on the date specified in the Certificate. The Certificate expires on the date stated on the Certificate or on the date and time the Certificate was revoked.

4.3. Audit records are stored locally for a period of at least 2 (two) months. Physical or digital archival records relating to Certificate applications, registration and revocation information are stored for a period of at least 10 (ten) years after the expiration of the relevant Certificate.

5. Rights and Obligations of the Subject of Identification and Indemnity

5.1. The Subject is entitled to apply for issuing a Certificate accepting the present Terms and Conditions and shall adhere to the requirements provided in the CP/CPS of KIBSTrust for Qualified Certificates for Electronic Signatures.

5.2. The Subject of electronic identification that possesses or should possess an Electronic Identification Means shall be:

5.2.1. solely responsible for the maintenance of access to his Private Key of the Qualified Certificate.

5.2.2. solely and fully responsible for all consequences of using his Electronic Identification Means both during and after the expiry of the validity of the Certificate accompanying the Electronic Identification Means.

5.2.3. solely responsible for any damage caused due to non-performance or improper performance of his obligations, specified in the present Terms and Conditions and / or the laws of the Republic of North Macedonia.

5.2.4. aware that the Electronic Signatures issued based on expired or revoked Certificates are invalid.

5.2.5. aware that he needs to provide accurate, truthful, and complete information that is essential to the creation of the Electronic Identification Means for Certificate issuance.

5.2.6. aware that he should not proceed with the procedure for creating an Electronic Identification Means if he/she is not legally eligible.

5.2.7. aware that the Private Key of his Qualified Electronic Signature is used only under his control and be cautious to avoid unauthorized use.

5.2.8. responsible for the confidentiality of the authentication credentials when accessing the Private Key (username, password, PIN) located on a remote QSCD (KIBSTrust cloud).

5.2.9. responsible for the proper use of the mobile device on which the OneID Mobile application has been installed to generate and use a Qualified Certificate located on a Remote QSCD. If the Subject loses or destroys the device or is unable to use the Qualified Certificate for any other reason beyond the control of KIBSTrust, the Subject shall contact KIBSTrust directly to request revocation of his Certificate.

5.2.10. responsible for using his Private Key and Certificate in accordance with the present Terms and Conditions, including the applicable agreements set out in Section 9 and the laws of the Republic of North Macedonia.
5.2.11. responsible for notifying KIBSTrust of the correct information within a reasonable time, in the event of a change in his personal data or any other inaccuracy in the content of the Certificate.
5.2.12. responsible for informing KIBSTrust of a possible unauthorized use of his Private Key or if his Private Key is lost, stolen, potentially compromised or he has lost control of his key due to compromising authentication credentials (e.g., PIN, PUK, username, password) or other reasons, and immediately revoke his Certificate.
5.2.13. responsible or his legal representative or successor to request revocation of the Certificate if the previously established relationships with the Subject terminated or ceased to exist.
5.2.14. responsible if he proceeds to use the Private Key even though the Certificate has been revoked or the Certificate issuer has been compromised.

5.3. The following terms additionally apply to the Subject whose identity has been verified using the method of remote identity verification:

5.3.1. The Subject shall follow the instructions exactly according to the documentation provided by KIBSTrust or the authorized employee who is conducting the validation process.
5.3.2. The Subject shall present the identification document (s) in good condition and good lighting conditions, to the extent that their authenticity can be verified.
5.3.3. At the beginning of the remote recognition and before initiation of the verification process, the Subject must provide his explicit consent regarding the use, recording and storage of the process of remote identity verification, photographing the face of the Subject, the verification method that provides security equal to physical presence, identification documents and, possibly, other necessary material.
5.3.4. If any third party other than the Subject appears in the process of remote identity verification, the session shall be terminated, all recorded data will be deleted and the process will be repeated, provided that no third parties appear.
5.3.5. KIBSTrust Remote Authentication System or authorized employee shall immediately terminate the remote identity verification process:

- When the identification document is inappropriate or raises doubts about its authenticity and security; or
- When the Subject behaves improperly to the automated remote authentication process or to the authorized KIBSTrust employee, or there are indications that the Subject is under duress, has a psychological or mental disorder or is abusing substances. In these cases, the process cannot be repeated, and the Subject must choose one of the other methods of identity verification referred to in part 1.4.
- When Subject is not legally eligible person.

5.3.6. The Subject shall submit to KIBSTrust a consent in which he will state his personal information in detail and his intention to proceed with the issuance of a Qualified Certificate.

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

5.4.1. False and misrepresentation of a fact by the Subject in the Purchase Order and Agreement form for the issuance of a Certificate.
5.4.2. Failure of the Subject to state a material fact in the Purchase Order and Agreement form if the misrepresentation or omission was made due to negligence or with the intention to deceive any party.
5.4.3. Failure of the Subject to protect its Private Key, use a secure system, or otherwise take precautionary measures to prevent compromise, loss, disclosure, modification, or unauthorized use of the Subject's private key.
5.4.4. Use of a name by the Subject that infringes the intellectual property rights of any third party.

6. OneID Service Provider Rights

6.1. Notwithstanding Section 8, KIBSTrust shall provide the Services in accordance with the Practice, CP/CPS for Qualified Electronic Signatures and Electronic Seals, CP/CPS of the KIBSTrust Time Stamp Issuer, and the relevant legislation.

7. Obligations of Relying Parties

7.1. Relying Party analyze the risks and obligations associated with accepting the Electronic Identification Means and thus the Qualified Certificate. The risks and obligations are listed in the Practices. The Relying Party acknowledges that it has access to sufficient information to ensure that it can make informed decision as to the extent to which it will chose to rely on the information from the Electronic Identification Means. THE RELYING PARTY IS RESPONSIBLE FOR THE DECISION WHETHER OR NOT TO RELY ON THE INFORMATION CONTAINED IN THE QUALIFIED CERTIFICATE.

7.2. Relying Party acknowledges and agrees that its use of the KIBSTrust repository, available at https://www.kibstrust.com/repository, and its reliance on a Qualified Certificate as part of its Electronic Identification Means shall be governed by applicable Practices which may be changed from time to time.

7.3. If insufficient evidence is attached to the Certificate for Electronic Signature regarding the validity of the Certificate, the Relying Party shall verify the validity or revocation of the Qualified Certificate using information on the current revocation status, based on the Certificate validation services provided by KIBSTrust, created with a Private Key corresponding to the Public Key contained in the Qualified Certificate, based on the Certificate verification services offered by KIBSTrust within the period of using the Certificate or affixing a Qualified Electronic Signature or a Qualified Electronic Seal. The method by which the status of the Certificate can be checked is by consulting the most recent Certificates Revocation List from the Certificate Authority that issued the Certificate on which the Relying Party wishes to rely.

7.4. Relying Party shall consider any limitations stated within any Certificate issued by KIBSTrust and ensure that the transaction to be accepted complies with the relevant CP/CPS.

7.4.1. Qualified Certificates shall be used only to the extent that the use is in accordance with the applicable law. Qualified Certificates are not designed, intended or approved for use or resale as control equipment in hazardous circumstances or for use requiring safe performance such as operation of nuclear facilities, aircraft navigation systems or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

7.4.2. KIBSTrust ensures the availability of the Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99% overall availability per year, with a scheduled downtime not exceeding 0.4% per year.

7.4.3. Relying Party verifies the validity of the Certificate by checking its validity using information from the OCSP and CRL check services available through the links provided in the Certificate. The OCSP service is available over HTTP protocol and is publicly available at http://ocsp2.kibstrust.com/.

7.4.4. Relying Parties are expected to use the register of Qualified Trust Service Providers of the Ministry of Information Society and Administration in the Republic of North Macedonia to determine whether the electronic signature, seal or time stamp are eligible (https://trusteid.mioa.gov.mk/en/home/register-and-lists/).

8. Limited Warranty and Limitation of Liability

8.1. KIBSTrust is liable for service and its performance of provider of electronic identification, as set forth in its Practice and the present Terms and Conditions.

8.2. KIBSTrust is liable for the performance of its Trust Services, as stated in its CP/CPS for Qualified Electronic Signatures.

8.3. KIBS warrants that there are mandatory insurance contracts that cover all KIBSTrust Trust Services and services as provider of electronic identification to ensure compensation for damages caused by violation of KIBSTrust obligations.

8.4. KIBSTrust shall notify all Subscribers and Subjects of Electronic Identification before terminating the activity related to the electronic identification service and certification services, and shall maintain the documentation associated with the interrupted certification services and the necessary information in accordance with the process set out in CP / CPS.

8.5. KIBS is not liable for:

8.5.1. the secrecy of the Private Key access credentials (username, password, OTP) when located on a remote QSCD, for possible loss or damage to the mobile device used to generate OTP and authenticate the user.

8.5.2. the improper use of the Certificate by the Subject or any misuse of the Certificate or improper checks of the Certificate or for wrong decisions of the Subject or the Relying Party or any consequences due to error or omission by the Subject or error or omission in the validity checks.

8.5.3. forged electronic signature of a document, indicatively due to stolen or compromised user's Private Key.

8.5.4. non-fulfillment of its obligations, if such non-fulfillment is due to errors or security problems of the supervisory body, unavailability of the confidential data source like Central Population Register, register of Qualified Trust Services Providers and Electronic Identification Schemes of the Ministry of Information Society and Administration in the Republic of North Macedonia or any other private legal entity or public authority.

8.5.5. the operation of software or other applications provided by third parties not related to KIBSTrust.

8.5.6. non-fulfillment of obligations if such non-fulfillment is due to an event of force majeure.

8.6. As stated in the relevant CP/CPS, KIBS provides limited warranties and disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability and excludes all liability, except in the case of intentional misconduct or gross negligence, for any loss of profit, loss of data or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, licensing, execution, performance, non-performance or compromise of Certificates for Electronic Signatures, Electronic seals, Time Stamps or any other transactions or services offered or considered herein, even if KIBSTrust has been notified of the possibility of such damages. The overall liability of KIBS to all parties, including the Subject, shall in no case exceed the appropriate liability cap for such Qualified Certificate set forth below:

8.6.1. The combined aggregate liability of KIBS to any and all persons in connection with a particular Qualified Certificate is limited to an amount not exceeding five hundred (500) euros per Certificate and a total maximum claim of fifty thousand (50,000) euros for Qualified Service, regardless of the nature of liability and the type, amount or extent of damages suffered. The limitations of liability provided for in this paragraph shall be the same irrespective of the number of Certificates for Qualified Signatures / Seals, transactions or claims relating to such Certificate.

8.6.2. The limitations of liability provided herein shall apply to the maximum extent permitted under the valid law of the applicable jurisdiction.

8.7. Subjects and Relying Parties are notified of the possibility of theft or other form of compromise of a Private Key corresponding to a Public Key contained in a Qualified Certificate, which may or may not be disclosed, and of the possibility of using a stolen or compromised key to forge a Qualified Electronic Signature or a Qualified Electronic Stamp of a document.

8.8. KIBSTrust may terminate the validation process if it is established or suspected that inaccurate or false information has been provided by the Subject or if the Subject's authentication is not successful. Notwithstanding paragraph 8.5, KIBS shall not be liable in any way for the authenticity or reliability of the identification documents submitted by the Subject, nor for any damage that may be caused to the Subject or to third party persons.

9. Applicable Related Agreements, Policies and Practices

Relevant agreements, Policies and Practice Statements regarding the current Terms and Conditions:

9.1. KIBSTrust CP/CPS for Qualified Certificates for Electronic Signatures and Electronic Seals.

9.2. Certificate and OCSP Profiles for Qualified Electronic Signatures and Qualified Electronic Seals, and specifically:

- EU Qualified Certificate Policy issued to natural persons (OID 0.4.0.194112.1.0), QCP-n.
- EU Qualified Certificate Policy issued to natural persons where the Private Key and associated Certificate are located on QSCD (OID 0.4.0.194112.1.2), QCP-n-QSCD.

9.3. Privacy Policy (KIBSTrust).

9.4. Current versions of all above documents are publicly available in the KIBS repository https://www.kibstrust.com/repository .

10. Privacy and Confidentiality Policy

10.1. KIBS processes personal data according to the Privacy Policy (KIBSTrust) available in the repository at https://www.kibstrust.com/repository and pursuant to all legal regulations of the Republic of North Macedonia.

10.2. All information that became known during the provision of the Services and is not intended to be disclosed (e.g., information known to KIBSTrust because of the operation and provision of the Trust Services) is confidential. The Subject is entitled to receive information from KIBSTrust on which data about him are stored / processed in accordance with the law.

10.3. KIBSTrust shall protect confidential information and information intended for internal use from compromise and refrain from disclosing it to third parties by implementing various security controls.

10.4. In accordance with the relevant laws and regulations, KIBSTrust has the right to disclose information about the Subject or Subject of a third party entitled to obtain such information and provided that the disclosure is lawful, in accordance with the national and EU data protection regulations.

10.5. In addition, non-personalized KIBSTrust service statistical data are also considered public information. KIBS may publish non-personalized statistical data about its services.

11. Accessibility for Persons with Disabilities

11.1. The issuance of an Electronic Identification Means involves processes of performing online activities including remote identification.

11.2. The activities that are performed online can be carried out with persons with disabilities, if their workstations, smart mobile devices with specially created tools will make the requirements to be met by a person with disabilities understandable to him.

11.3. If online ordering is not possible, persons with disabilities can come to the KIBSTrust RA premises. Access to the KIBSTrust RA / LRA office is barrier free. Information on unimpeded access to LRA is clearly displayed on the website https://www.kibstrust.com . In addition, KIBSTrust offers a home help service at the request of a person with disabilities.

11.4. When persons with disabilities arrive in RA, the procedure for issuing an Electronic Identification Means can be carried out with the help of KIBS personnel. In any case, it is desirable for persons with disabilities to be accompanied by persons who understand the needs and have gained the trust of the person with disabilities in order to speed up the process of issuing an Electronic Identification Means.

11.5. The use of an Electronic Identification Means for persons with disabilities depends on how their workstations, smart devices, operating systems, and application software are tailored to their special needs.

12. Refund Policy

12.1. KIBSTrust strives to ensure the highest quality of its services. However, the following should be kept in mind:

12.1.1. The Subject may be charged for the Electronic Identification Service.

12.1.2. The Subject can file a complaint for the service received in case of invalid operation, inconsistency of the service description with the given description, purpose and use that are declared and published by KIBSTrust within five (5) days from the day of activation of the Certificate.

12.1.3. KIBSTrust will not accept any claims for improper use of the service or damages caused by fault or actions of the Subject.

12.1.4. The Subject has the right to withdraw from the online prepared procedure for creating an Electronic Identification Means before activating the service. If the Subject does not complete the procedure of issuing Electronic Identification Means, he will be automatically rejected by the system.

13. Applicable Law, Complaints and Dispute Resolution Mechanism

13.1. All disputes regarding the Trust Services provided in accordance with the present Terms and Conditions shall be governed in all respects and shall be construed in accordance with the laws of the Republic of North Macedonia.

13.2. To the extent permitted by law, before any dispute settlement mechanism can be used in relation to a particular dispute relating to any aspect of the Trust Services of KIBSTrust, the Subject or any other party to the dispute must notify KIBSTrust and all other parties involved in the dispute of any claims or complaints no later than thirty (30) calendar days after the discovery of the basis for the claim, unless otherwise provided by law. If the dispute is not resolved within sixty (60) days after the initial notification, the party may seek legal resolution. All parties agree that the courts of the Republic of North Macedonia shall have exclusive jurisdiction for hearing and resolving any dispute regarding the interpretation and application of these terms and the provision of KIBSTrust services.

13.3. The Subject or any other party may submit their claim or complaint to the following e-mail address: helpdesk@kibstrust.com .

13.4. All dispute requests should be sent to the information contact listed in these Terms and Conditions.

14. Audit and Conformity Assessment

14.1. KIBSTrust is a provider of Qualified Confidential Services and Electronic Identification Scheme. The mentioned status was granted by a supervisory body, after the submission of a conformity assessment report by an accredited conformity assessment body in accordance with paragraph 14.3 and 14.4.

14.2. The Trust Services and the Electronic Identification Scheme are registered in the Register of Trust Service Providers and Electronic Identification Schemes of the Ministry of Information Society and Administration in the Republic of North Macedonia. Prerequisite for such registration is compliance with the applicable regulations and standards in the country, at world and European level.

14.3. The Conformity Assessment Body is accredited in accordance with the Regulation (EC) no. 765/2008 as competent for assessing the conformity of the Qualified Trust Service Provider and the Qualified Trust Services it provides.

14.4. Accreditation scheme: ISO / IEC 17065 + ETSI EN 319 403 + eIDAS Art.3.18 scope of accreditation.

14.5. The conclusions of the audit or reports based on the results of the conformity assessment audit performed in accordance with the eIDAS Regulation, as well as the relevant laws and standards, are published in the KIBS repository at https://www.kibstrust.com/repository .

15. Contact Information

15.1. Qualified Trust Service Provider:

KIBS AD (KIBSTrust)
bul. "Kuzman Josifovski Pitu" 1,
+389 2 5513 444, +389 2 3297 444
https://www.kibstrust.com
helpdesk@kibstrust.com
1000 Skopje, Republic of North Macedonia
(Monday - Friday 8.30 - 16.00 Central European Time)

15.2. The applications on questions regarding the life cycle of the Electronic Identification Means are received from 08.30 to 16.00 (UTC +2) 8/5 in person in RA, or via email to oneid@kibstrust.com .

15.3. The information on the website and the contact data for the service web portal are available at https://www.oneid.mk, https://www.kibstrust.com.

16. Importance of the Terms and Conditions

16.1. These Terms and Conditions are set out in Macedonian and English versions. In case of any discrepancies between these versions, the Macedonian version shall prevail.

16.2. The provisions of the Practice shall apply to everything that is not contained in these Terms and Conditions or conflicts with the provisions of the Practice.

16.3. If any provision of these Terms and Conditions, or the application thereof, is for any reason and to any extend found invalid or unenforceable, the remaining provisions (as well as the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such a finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

17. Definitions and Acronyms

Term/Acronym	Definition
Certificate Authority (CA)	A part of KIBS company responsible for issuing and verifying Certificates and Certificate Revocation Lists with its electronic signature.
Certificate	Public Key, together with additional information, laid down in the Certificate profile rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Policy (CP)	Named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	Statements and practices which a Certification Authority employs in issuing, managing, revoking, and renewing or re-key Certificates.
Certificate Revocation List (CRL)	Signed list indicating a set of Certificates that have been revoked by the Certificate Authority.
eIDAS Regulation	Regulation (EY) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification Means and Trust Services for electronic transactions on the internal market and repealing Directive 1999/93/E3.
Identity verification/validation	Unique identification of a person by checking his/her alleged identity.
MK-eIDAS	Law on electronic documents, electronic identification, and trust services. (Official Gazette of Republic of North Macedonia no. 101/19....215/19).
KIBS	KIBS A.D. Skopje
OCSP	Online Certificate Status Protocol
OID	An identifier used to uniquely name an object.
PIN code	Activation code for the Qualified Certificates for Electronic Signatures and Electronic Seals.
Private key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is issued to create Electronic Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The kay of a key pair that may be publicly disclosed by the key holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Qualified Certificate	Qualified Certificate is a Certificate issued by a CA which is accredited and supervised by supervisory body appointed by the state and meets the requirements of the Law on Electronic Documents, Electronic Identification and Trust Services and eIDAS.
Qualified Electronic Signature	Advanced Electronic Signature that is created by Qualified Electronic Signature Device, and which is based on a Qualified Certificate for Electronic Signatures.
Qualified Electronic Seal	Advanced Electronic Seal that is created by a Qualified Electronic Seal Creation Device, and that is based on a Qualified Certificate for Electronic Seal.

Qualified Electronic Time Stamp	Data in electronic form which bind other data in electronic form to a particular time establishing evidence that the latter existed at that time, in such a way that the possibility of the data being changed is precluded. It is based on an accurate time source linked to UTC and is signed using an Advanced Electronic Signature or Advanced Electronic Seal of the Qualified Trust Service Provider.
Qualified Signature/Seal Creation Device (QSCD)	A Secure Signature/Seal Creation Device that meets the requirements laid down in Chapter II of the eIDAS Regulation. QSCD can be either local in the form of USB token or a smart card or remote in the form of a Hardware Security Module.
Qualified Trust Services	A Trust Service, as defined in eIDAS that meets the applicable requirements laid down in this Regulation.
Qualified Trust Service Provider	A Trust Service Provider who provides one or more Qualified Trust Services and is granted the qualification status by the supervisory body.
Relying Party	Natural or legal person that relies on the information contained within a Certificate or electronic identification means.
Subject	The Subject can be: а) natural person. б) natural person identified in association with a legal person. в) legal person (that can be an organization or a unit or a department identified in association with an organization).

END OF DOCUMENT