Trusted Services Provider KIBS

Terms and Conditions

For Use of Qualified Trust Services

(Qualified Certificates for Electronic Signatures, Electronic Seals, and timestamps)

Last modified: 01.04.2021, 0903-108/3 (view archived versions)

Version History

Version	Date	Author	Purpose of changes
1.0	01.04.2021	Policy Management Authority	Initial document

1. General Terms

Present General Terms and Conditions describe main policies and practices followed by KIBS and provided in following documents:

- Certification Practice & Certificate Practice Statement for Electronic Signatures and Electronic seals;
- PKI Disclosure Statement (PDS) for Qualified Electronic Signatures and Qualified Electronic Seals
- Time Stamping Authority Certification Practice & Certificate Practice Statement
- Time Stamping Authority Disclosure Statement.

1.1. The Terms and Conditions governs Subscribers use of the Qualified Certificates for Electronic Signatures, Seals and Time Stamping Services and constitute a legally binding contract between Subscriber and KIBS.

1.2. The Subscriber must be familiar with and accept the Terms and Conditions.

1.3. KIBS reserves the right, at its sole discretion, to amend the Terms and Conditions at any time and without notice, should KIBS have a justified need for such amendments. The current version and previous versions are published on https://www.kibstrust.com/repository.

1.4. The Subscriber can apply for:

1.4.1. Qualified Certificate for Qualified Electronic Signature (issued on a QSCD) to a natural person.
1.4.2. Qualified Certificate for Advance Electronic Signature (without a QSCD) to a natural person.
1.4.3. Qualified Certificate for Qualified Electronic Signature (issued on a QSCD) to a natural person associated with a legal person.
1.4.4. Qualified Certificate for Advance Electronic Signature (without a QSCD) to a natural person associated with a legal person.
1.4.5. Qualified Certificate for Qualified Electronic Seal (issued on a QSCD) issued to a legal person.
1.4.6. Qualified Certificate for Advanced Electronic Seal (without a QSCD) issued to a legal person.
1.4.7. Qualified Service for issuing Qualified timestamps.

1.5. Identity verification & Application for the issuance of a Certificate

1.5.1. Before the issuance of a Qualified Certificate, the Subscriber's identity is verified by KIBS using one of the following methods:

- by the physical presence of Subscriber, who submits the acceptable official identification documents (Art.24 par.1a of the eIDAS Regulation and art.11 of MK-eIDAS); or
- remotely, by means of a Qualified Certificate for electronic signature or electronic seal (art.24 par.1c of the eIDAS Regulation and art.11 of MK-eIDAS) ; or
- by equivalent to physical presence Remote ID verification using liveness method (art.24 par.1d of the eIDAS Regulation and art.31 of MK-eIDAS); or

1.5.2. Subscriber / Subject shall sign and submit to KIBS's RA/LRA the respective Purchase Order and Agreement form, as well as proof of identity and other required documents, as specified in the Purchase Order. Acceptable identification documents are: National ID Card for resident of Republic of North Macedonia, temporary ID Card for foreign citizen with temporary residence in Republic of North Macedonia, foreign citizens ID Card for citizens from countries that Government of Republic of North Macedonia accept as legal travel document and passport for all citizens. KIBS may assign part or the whole identity verification process to a third party.

1.6. The Subscriber of Qualified Time Stamping Services can be a natural person or natural person associated with legal person, or a legal person, by entering in a relevant contract with KIBS.

1.7. For Subscribers, whose identity is verified through the Remote ID verification method, the terms and conditions specified in paragraph 5.4 shall apply additionally. Remote ID verification shall be available and feasible, only when the circumstances during the identity verification process are satisfactory enough to provide accurate proof of the Subscriber's ID.

1.8. KIBS may refuse the issuance of the Certificate at its sole discretion if identity validation using any of the methods specified in paragraph 1.5 is not successful.

1.9. The Subscriber must complete the certificate issuance process within 30 days from the date of submission of the Purchase Order for the issuance of a Qualified Certificate.

1.10. Subscriber shall be legally eligible to apply for a Qualified Trust Service.

1.11. Subscriber agrees to use a Qualified Signature Creation Device (QSCD), which will be provided by KIBS. QSCD can either be local or remote. The Subscriber is solely responsible for the proper use of the QSCD.

1.12. Subscriber may require the non-publication of the certificate to KIBS's Public directory of issued certificates.

1.13. Subscriber is responsible for the payment of any fees for the offered trust service, as well as any compensation arising from the improper use of the Certificate.

1.14. KIBS as QTSP ensures that respect principle of equality and protection against discrimination in the exercise of human rights and freedoms[1].

1.15. .

1.16. KIBS has the right to amend the present Terms and Conditions at any time when there is a justified need for such amendments, i.e. when it is mandated by regulatory requirements. The amended Terms and Conditions along with the enforcement date are published 30 days before enforcement. Current and all previous versions are published on: https://www.kibstrust.com/repository.

2. Certificate Acceptance for Electronic Signature or Seal, Certificate Types

2.1. Upon submitting Purchase Order and Agreement form for a Certificate, the Subscriber confirms that he/she is familiar with and accepts the Terms and Conditions.

The following conduct constitutes Certificate acceptance for Qualified Electronic Signature and Qualified Electronic Seal:

- Generation the Certificate constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the Certificate or its content within 24 hours from downloading it, constitutes Certificate acceptance.

2.2. If the Certificate re-keying is performed the Subscriber confirms that he/she has read and agrees to the Terms and Conditions.

2.3. Certificate Type, Usage and Certification Procedure.

Certificate Type	Usage	Certification Policy Applied and Published
Qualified Electronic Signatures compliant with MK-eIDAS and eIDAS.	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.	KIBS CP/CPS for Qualified Certificates for Electronic Signatures and Qualified Electronic Seals, published on: https://www.kibstrust.com/repository ETSI EN 319 411-2 Policy: QCP-n-qscd
Qualified Electronic Seals compliant with MK-eIDAS and eIDAS.	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.	KIBS CP/CPS for Qualified Certificate for Electronic Signatures and Qualified Electronic Seals, published on: https://www.kibstrust.com/repository ETSI EN 319 411-2 Policy: QCP-l-qscd

Qualified Certificates are either Long-lived or Short-lived. A Long-lived Certificate is valid for 1 to 3 years and Short-lived Certificate is valid from 1 to 72 hours and can be used for one transaction.

[1] Preventing and protection from Discrimination law

3. Prohibitions of use

3.1. The Subscriber's Certificates shall not be used outside of the limits and contexts specified in KIBS CP/CPS for Qualified Certificates for Electronic Signatures and Seals or for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of KIBS. Indicatively, the use of Certificates is prohibited for any of the following purposes:

3.1.1. Unlawful activity (including cyber-attacks and attempt to infringe the Certificate).
3.1.2. Issuance of new Certificates and information regarding Certificate validity.
3.1.3. Enabling other parties to use the Subscriber's Private Key.
3.1.4. Enabling the Certificate issued for electronic signing to be used in an automated way.
3.1.5. Using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

3.2. The Time Stamping Services shall be used within the limits and contexts specified in the TSA Certificate Policy & Certification Practice Statement. Any unlawful use outside those limits is prohibited.

4. Reliance Limits

4.1. Reliance Limits for Qualified Certificates for Electronic Signatures and Seals

4.1.1. The information in the Certificates is correct. There are no errors or material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
4.1.2. Certificates become valid as of the date specified in the Certificate. The validity of the Certificate expires on the date of expiry indicated in the Certificate or on the date and time the Certificate is revoked.
4.1.3. Audit logs are retained on-site for no less than two (2) months. Physical or digital archive records regarding Certificate applications, registration information and revocation are retained for at least ten (10) years after the expiry of the relevant Certificate.

4.2. Reliance Limits for Time Stamps

4.2.1. Time Stamps become valid as of the date specified in them. The validity of the Time Stamp expires on the date of expiry indicated in the Time Stamp or if the Time Stamp Unit (TSU) Certificate is revoked. KIBS TSA ensures that the Time Stamp Unit's private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place when a Time Stamp Unit's key usage period expires, and that Time Stamp Unit's private keys or any part, including any copies are destroyed such that the private key cannot be retrieved. The Time Stamp Token (TST) generation system shall reject any attempt to issue a TST if the signing private key is expired or if the signing private key usage period is expired.
4.2.2. KIBS has in place technical procedures to ensure that Time Stamp Tokens are issued securely and include the correct time. The KIBS Time Stamping Authority ensures that its time is synchronized with UTC within the declared accuracy with multiple independent time sources. The TSTs are issued with an accuracy of ± one (1) second. KIBS implements security controls preventing unauthorized operation, aimed at calibration of TSA time. KIBS monitors that synchronization is maintained when a leap second occurs.
4.2.3. Local NTP servers with GPS time sources and rubidium atomic clock are used for NTP reference. Monitoring of clock synchronization is done by comparing the time sources. Information about loss of clock synchronization will be made available in public media.
4.2.4. Time-Stamping Certificates are valid for six (6) years. Logs and records for Timestamping are retained for ten (10) years after the expiration of the Time Stamping Unit Certificate.

5. Subscriber's Rights and Obligations - Indemnity

5.1. The Subscriber has the right to submit an application for issuing a Certificate or request a Time Stamp, accepting the present Terms and Conditions and adhere to the requirements provided in KIBS's CP/CPS for

Qualified Certificates for Electronic Signatures and Electronic Seals and Time Stamping Authority CP & CPS respectively.

5.2. The Subscriber and/or Subject of Qualified Electronic Signatures or Seals shall:

5.2.1. Be solely responsible for the maintenance of their Private Key.
5.2.2. Be solely and fully responsible for any consequences of using their certificates both during and after the validity of the certificate.
5.2.3. Be solely liable for any damage caused due to failure or undue performance of their obligations specified in the present Terms and Conditions and/or the laws of Republic of North Macedonia.
5.2.4. Be aware that Electronic Signatures or Electronic Seals given based on expired or revoked Certificates are invalid.
5.2.5. Submit accurate, true, and complete information in relation to the issuance of the Certificate.
5.2.6. Submit the necessary identification documents to KIBS as specified in the Purchase Order and Agreement form for certificate issuance, as well as follow the steps that KIBS indicates for completing the registration process.
5.2.7. Not continue with the certificate issuance procedure if the Subscriber is not legally eligible to do so.
5.2.8. Ensure that Subscriber´s Private Key is used under his/her control and exercise reasonable care to avoid unauthorized use of it.
5.2.9. Be responsible for the secrecy of the Private Keys when residing on a Local QSCD, as well as the authentication credentials accessing private keys (username, password, OTP) when residing on a Remote QSCD.
5.2.10. Be responsible for the proper use of the mobile device on which the application for the generation of the OTP has been installed to generate and use the Qualified Certificate residing on a Remote QSCD. If the Subscriber loses or destroys or is unable to use the Qualified certificate for any other reason outside KIBS's control, the Subscriber should contact KIBS directly to request revocation of his/her Certificate.
5.2.11. Use his/her Private Key and Certificate in accordance with present Terms and Conditions, including applicable agreements set out in Section 9, and the laws of Republic of North Macedonia.
5.2.12. Notify KIBS of the correct information during a reasonable time, in case of a change in his/her personal details, or of the legal person's details and/or of the legal person's representative or of any other inaccuracy of the certificate content;
5.2.13. Immediately inform KIBS of a possibility of unauthorized use of his/her Private Key or if his/her Private Key has been lost, stolen, potentially compromised or if control over his/her Private Key has been lost due to a compromise of authentication credentials (e.g. PIN, PUK, username, password, OTP) or other reasons and immediately revoke his/her Certificate.
5.2.14. Report any change of information submitted during certificate request or change in submitted accompanying documents.
5.2.15. Immediately request revocation of the certificate if previously established relations with the person subject of certification terminated or ceased to exist.
5.2.16. Be responsible of placing the timestamp when signing with their Qualified Certificate.
5.2.17. Not continue using the private key if the certificate has been revoked or the CA has been compromised.

5.3. The Subscriber of Time Stamping Service shall:

5.3.1. use timestamping service in compliance with KIBS Time Stamp Authority CP/CPS and this Terms and Conditions.
5.3.2. create timestamp request only with KIBS approved software or method.
5.3.3. inform end-users of timestamps about the applicable rules. Subscribers shall protect the secrecy of credentials necessary to access the timestamp issuance system by not communicating or disclosing them to third parties.
5.3.4. Verify the signatures created by the KIBS TSA on the TST (Verification whether the TSA signature on the TST is valid and Verification of the TSA certificate).
5.3.5. Use secure cryptographic functions for time-stamping requests.
5.3.6. Be aware that expired Time Stamps are invalid.

5.4. The following terms shall additionally apply to the Subscriber whose identity is verified using the Remote ID verification method:

5.4.1. The Subscriber shall follow the instructions exactly as per KIBS's given documentation or authorized employee who is conducting the validation process.

5.4.2. The Subscriber shall present the identification document(s) in good condition to the extent that their originality can be verified.

5.4.3. At the beginning of the remote recognition and before the initiation of the verification process, the Subscriber must provide their explicit consent regarding the use, recording and storage of the remote ID verification process, taking snapshots of the Subscriber's face, liveliness sequences, identification document and, possibly, other necessary material.

5.4.4. If any third person other than Subscriber/Subject appears in the remote ID verification process, the session shall be terminated, any data recorded will be erased and the process will be repeated provided that no third persons appear.

5.4.5. KIBS's remote authentication system or authorized employee will discontinue the Remote ID verification process immediately:

- when the identification document is not appropriate or causes doubt as to its authenticity and reliability; or
- when the Subscriber behaves inappropriately towards KIBS's automatic process of remote authentication or towards authorized employee, or there are indications that the Subscriber is under duress, psychological or mental disorder or substance abuse; in these cases, the process cannot be repeated and the Subscriber must choose one of the other identity verification methods specified in par. 1.5.

5.4.6. The Subscriber shall submit to KIBS a consent, in which they will state their personal information in detail and their intention to proceed with the issuance of a qualified certificate.

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

5.5.1. Falsehood or misrepresentation of fact by the Subscriber on the Purchase Order and Agreement form for the issuance of a Certificate.

5.5.2. Failure by the Subscriber to disclose a material fact on the Purchase Order and Agreement form, if the misrepresentation or omission was made negligently or with intent to deceive any party.

5.5.3. The Subscriber's failure to protect the Subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key;

5.5.4. The Subscriber's use of a name that infringes the Intellectual Property rights of a third party.

6. KIBS's Rights

Without prejudice to Section 8, KIBS shall provide the services in accordance with the CP/CPS for Qualified Electronic Signatures and Electronic Seals, KIBS Time Stamping Authority CP/CPS, as well as the relevant legislation.

7. Certificate Status Checking Obligations of Relying Parties

7.1. A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in the relevant CP/CPS. A Relying Part acknowledges that he/she has access to sufficient information to ensure that he/she can make an informed decision as to the extent to which he/she will chose to rely on the information in a Qualified Certificate. A RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A QUALIFIED CERTIFICATE.

7.2. A Relying Party acknowledges and agrees that his/her use of KIBS Repository and his/her reliance on any Qualified Certificate shall be governed by KIBS applicable CP/CPS that can have changes from time to time. The applicable CP/CPS is published on the Internet in the Repository at https://www.kibstrust.com/repository and is available via Email by sending a request to: helpdesk@kibstrust.com. Current version and previous version to the applicable CP/CPS are also posted in KIBS Repository at https://www.kibstrust.com/repository.

7.3. If not enough evidence is enclosed to the Certificate of Electronic Signature or Electronic Seal with regard to the validity of the Certificate a Relying Party verifies the validity or revocation of the Qualified Certificate using current revocation status information on the basis of certificate validation services offered by KIBS created with a private key corresponding to a public key contained in a Qualified Certificate on the basis of certificate validation services offered by KIBS at the time of using the Certificate or affixing a Qualified Electronic Signature or Qualified Electronic Seal. A method by which the Certificate status can be checked is by consulting the most recent Certificate Revocation List from the Certification Authority that issued the Certificate on which he/she wishes to rely.

7.4. A Relying Party should take into account all limitations stated within any Certificate issued by KIBS and makes sure that the transaction to be accepted corresponds to the relevant CP/CPS .

7.4.1. Qualified Certificates shall be used only to the extent use is consistent with applicable law. Qualified certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation 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. Time stamps shall be used only to the extent that use is consistent with applicable law. Any limitations on usage of time stamps indicated by the KIBS Time Stamping Authority CP/CPS should be considered. Subscribers and Relying Parties shall verify the signatures created by the KIBS TSA on the TST. If the verification takes place after the end of the validity period of the Certificate, they should follow the guidance denoted in Annex D of ETSI EN 319 421.

7.5. KIBS ensures the availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0,4% annually.

7.6. A Relying Party verifies the validity of the Certificate by checking Certificate's validity against OCSP and CRL references located in the Certificate. OCSP Service is accessible over HTTP protocol and publicly available on http://ocsp2.kibstrust.com/.

7.7. Relying parties are expected to use a register at Trusted List of Qualified Trust Service Providers of Ministry of Information Society and Administration in Republic of North Macedonia to establish whether an Electronic Signature, Seal or Time Stamp is qualified.

8. Limited Warranty and Disclaimer/Limitation of Liability

8.1. KIBS is liable for the performance of its Trust Services as specified in its CP/CPS for the Use of Qualified Certificates Electronic Signatures and Seals and KIBS Time Stamping Authority CP/CPS.

8.2. KIBS ensures that it has compulsory insurance contracts covering all KIBS trust services to ensure compensation for damages caused by KIBS's breach of obligations.

8.3. KIBS informs all Subscribers and Subjects before KIBS terminates service of Certificates and maintains the documentation related to the terminated service of Certificates and information needed according to the process set out in the CP/CPS.

8.4. KIBS is not liable for:

8.4.1. the secrecy of the Private Keys of Subscriber and Subject when residing on a local QSCD, or for possible loss or damage of the local QSCD.

8.4.2. the secrecy of the credentials accessing private keys (username, password, OTP) when residing on a remote QSCD, for possible loss or damage of the mobile device used for the OTP generation.

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

8.4.4. forged electronic signature or electronic seal on a document, indicatively due to a stolen or compromised Private key or QSCD or otherwise.

8.4.5. the loss, improper storage, or improper use of time stamp tools.

8.4.6. the non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, register at Trusted List of Qualified Trust Service Providers of Ministry of Information Society and Administration in Republic of North Macedonia, or any other public authority.
8.4.7. the operation of software or other applications provided by third parties not related to KIBS.
8.4.8. the failure to perform if such failure is occasioned by force majeure.

8.5. As stated in the respective 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 case of willful misconduct or gross negligence, for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, performance, nonperformance, or compromise of certificates for electronic signatures, electronic seals, time stamps or any other transactions or services offered or contemplated herein, even if KIBS has been advised of the possibility of such damages. In no event will the aggregate liability of KIBS to all parties (including you) exceed the applicable liability cap for such qualified certificate set forth, below:

8.5.1. the combined aggregate liability of KIBS to any and all persons concerning a specific qualified certificate shall be limited to an amount not exceeding five hundred (500) euro per certificate and a total maximum of claims of fifty thousand (50.000) euro, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The liability limitations provided in this paragraph shall be the same irrespective of the number of certificates for Qualified Signatures/Seals, transactions, or claims related to such certificate.
8.5.2. the combined aggregate liability of KIBS to any and all persons concerning Time Stamp Services shall be limited to an amount not exceeding that of the respective contract (prepaid or postpaid) for the time stamping service, which will be calculated on a pro rata basis, and a total maximum of claims of fifty thousand (50.000,00) euros, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The liability limitations provided in this paragraph shall be the same irrespective to the number of Time Stamps or claims related to such Time Stamp.

The limitations on liability provided herein shall apply to the maximum extent allowed under the applicable law of the applicable jurisdiction.

8.6. Subscribers, Subjects and Relying Parties are hereby 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 detected, and of the possibility of use of a stolen or compromised key to forge a qualified electronic signature or qualified electronic seal on a document.

8.7. KIBS may discontinue the validation process if any information provided by the Subscriber is found or suspected to be inaccurate or false or if identity verification of the Subscriber is not successful. Without prejudice to paragraph 8.5, KIBS is not in any way liable for the authenticity or reliability of the identification documents submitted by the Subscriber nor for any damage that may be caused therefrom to the Subscriber or other persons.

8.8. Subscriber/Subject is hereby notified that, depending on the Subscriber/Subject's decision, KIBS may use the following identifiers within the Certificate:

- National trade register identification number.
- Unique Identifier.

One of the above identifiers shall be visible in Subscriber/Subject's electronic signature. KIBS is not liable for any use thereof by third parties concerning the Subscriber/Subject's identity verification or identification or other uses thereof.

9. Applicable Agreements, Policies, CP, CPS

Relevant agreements, policies and practice statements related to the present Terms and Conditions:

9.1. KIBS 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:

- Policy for EU qualified certificates issued to natural persons (OID 0.4.0.194112.1.0), QCP-n
- Policy for EU qualified certificates issued to legal persons for qualified certificate issued to a legal person (OID 0.4.0.194112.1.1), QCP-l.
- Policy for EU qualified certificate issued to natural person where the private key and the related certificate reside on a QSCD (OID 0.4.0.194112.1.2), QCP-n-QSCD.
- Policy for EU qualified certificate issued to legal person where the private key and the related certificate reside on a QSCD (OID 0.4.0.194112.1.3), QCP-l-QSCD.

9.3. KIBS Time Stamping Authority CP/CPS.

9.4. KIBS Privacy Policy.

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

10. Privacy Policy and Confidentiality

10.1. KIBS processes personal data according to the Privacy Statement, provided in the KIBS's repository at https://www.kibstrust.com/repository and all legal acts of Republic of North Macedonia and European Union.

10.2. All information that has become known while providing services and that is not intended for disclosure (e.g. information that had been known to KIBS because of operating and providing Trust Services) is confidential. The Subscriber has the right to obtain information from KIBS about him/her pursuant to the law.

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

10.4. KIBS has the right to disclose information about the Subscriber or Subject to a third party who pursuant to relevant laws and legal acts is entitled to receive such information and provided that such disclosure is lawful according to national and EU data protection legislation.

10.5. Additionally, non-personalized statistical data about KIBS services is also considered public information. KIBS may publish non-personalized statistical data about its services.

11. Accessibility for persons with disabilities

Issuing Qualified Certificates for Electronic Signatures and Electronic Seals includes processes of placing online Purchase Order and Agreement form, face-to-face identification in front of RA/LRA representative or remote identification.

Submitting PO online is available for persons with disabilities if their workstations and used operating systems and application software is adjusted to their needs.

If fulfilling online PO is not possible, persons with disabilities can show up in premises of RA/LRA of KIBS. Reaching RA/LRA office of KIBS is with barrier free entrance. Information which LRA's and authorized third party entities can be visited with barrier free entrance is clearly shown on web site https://www.kibstrust.com. Additionally, KIBS offers on demand assistance service at home for preparation of PO and face-to-face recognition by KIBS officers or officers of authorized third-party entities.

Also, PO can be prepared for persons with disabilities that reach RA, LRA or authorized third party entity offices from officers employed by KIBS, by LRA or by authorized third party entities. In this case person with disability, it is good to be accompanied by persons that understand needs and have trust from disability person to speed up process of issuing certificate.

Usage of issued qualified certificates for persons with disabilities is dependable on how their workstations, operating systems and application software is adjusted to dear needs.

12. Refund Policy

KIBS makes efforts to secure the highest level of quality of its services. Nevertheless:

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

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

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

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

12.4. KIBS handles refund case-by-case. In rare cases KIBS may refund Subscriber. The exercise of this right shall be made in writing by Subscriber to KIBS by sending an e-mail to helpdesk@kibstrust.com.

13. Applicable law, complaints, and dispute resolution

13.1. Any disputes related to the trust services provided under these terms shall be governed in all respects by and construed in accordance with the laws of the Republic of North Macedonia excluding its conflict of laws rules, and European Union.

13.2. To the extent permitted by law, before any dispute resolution mechanism may be invoked with respect to a dispute involving any aspect of KIBS Trust Services, the Subscriber or other party must notify KIBS, and any other party to the dispute of any claim or complaint not later than thirty (30) calendar days after the detection of the basis of the claim, unless otherwise provided by law. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may seek legal resolution. All parties agree that the courts of the Republic of North Macedonia, shall have exclusive jurisdiction and venue for hearing and resolving any dispute regarding the interpretation and execution of these terms and the provision of KIBS services.

13.3. The Subscriber or other party can submit their claim or complaint on the following email: helpdesk@kibstrust.com.

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

14. KIBS and Repository Licenses, Trust Marks, and Audit

14.1. KIBS is a Qualified Trust Service Provider and is granted the qualified status by a supervisory body, following the submission of a conformity assessment report by an accredited Conformity Assessment Body.

14.2. KIBS Trusted Services for Qualified Electronic Signatures and Qualified Electronic Seals are register at register at Trusted List of Qualified Trust Service Providers of Ministry of Information Society and Administration in Republic of North Macedonia. The prerequisite requirement of this registration follows applicable regulations and standards.

14.3. The Conformity Assessment Body is accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out conformity assessment of the Qualified Trust Service Provider and 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. Audit conclusions or certificates, which are based on audit results of the conformity assessment conducted pursuant to the eIDAS Regulation, corresponding legislation and standards are published on KIBS repository at https://www.kibstrust.com/repository.

15. Contact Information

15.1. Qualified Trust Service Provider

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

15.2. The applications for revoking Certificates are accepted from 08.30 to 16.00 (UTC+1) 8/5 in-person in RA, or via email revoke@kibstrust.com.

15.3. Website Information and contact details of the self-service web portal is available on https://www.kibstrust.com.

16. Validity of Terms and Conditions

16.1. The present Terms and Conditions exist in English and Macedonian versions. In case of any discrepancies between these versions, the Macedonian version will prevail.

16.2. If any provision of these Terms and Conditions, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such 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 company KIBS 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 indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that have been revoked by the certificate issuer.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in ITU-R Recommendation TF.460-5
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Identity verification / validation	Unique identification of a person by checking his/her alleged identity.
Local Registration Authority (LRA)	An entity that performs the identification and validation of Subscribers and Subjects and the initial examination of their respective documents for the issuance, re-keying and revocation of Certificates.
Long-lived Certificate	A Qualified Certificate which is valid for 1 to 3 years.
MK-eIDAS	Law for electronic documents, electronic identification, and trusted services. (Official gazette of Republic of North Macedonia 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 for 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 used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the 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 has been accredited and supervised by supervisory body in the Country and meets the requirements of Law for electronic documents, electronic identification and trusted services and eIDAS.
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation 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 binds 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 a 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 qualified status by the supervisory body.
Registration Authority (RA)	An entity that performs identity verification and validation of Subscribers for issuing Certificates initiates, or passes along revocation requests for Certificates, and approves applications for re-keying certificates on behalf of the CA.
Relying Party	Natural or legal person that relies on the information contained within a Certificate.
Remote ID verification	The method/process by which the Subscriber is identified through a video conference and is equivalent to identity verification through physical presence.
Short-lived Certificate	A Qualified Certificate which is valid from 1 to 72 hours and can be used for one transaction.
Subject	The subject can be: a) a natural person. b) a natural person identified in association with a legal person. c) a legal person (that can be an Organization or a unit or a department identified in association with an Organization);
Subscriber	Natural or legal person subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
Terms and Conditions for Use of Qualified Trust Services (Terms and Conditions)	Present document that sets forth the Terms and Conditions under which a natural or legal person acts as a Subscriber and/or as a Subject or as a Relying Party and KIBS provides the corresponding Trust Services.
Time Stamping Authority (TSA)	The Authority of the Time Stamping Services which issues Time Stamp Tokens.
Time Stamp Token (TST)	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time Stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single Time Stamp Token signing key active at a time.
Trusted List	List containing information about qualified trust service providers in the EU, as well as information on the qualified trust services provided by them.

END OF DOCUMENT