Terms and Conditions
for Use of Qualified Trust Services

Verba Sign, Verba Seal, Momentum

Version: 2.0

Date: 09.09.2022

111.07

KIBS AD Skopje

http://www.kibstrust.com/

Trademark notice and document Information

KIBS and KIBSTrust are registered trademarks 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 AD Skopje, but operates under the brand name KIBSTrust, hence the terms "Trusted Service Provider" and "Qualified Trusted Service Provider" are identified with "KIBSTrust".

KIBS AD Skopje as legal entity trough out this document will be represented abbreviated as KIBS.

This document has been developed by KIBSTrust and contains the conditions, according to which KIBSTrust is acting as Qualified Trusted Services Provider (QTSP) and Qualified Time Stamping Services Provider (QTSSP).

Intellectual Property Rights

Requests for any other permission to reproduce this publication (as well as requests for copies) must be addressed to KIBSTrust (KIBS) 1, Kuzman Josifovski Pitu, 1000, Skopje, Republic of North Macedonia; Attn: Policy Management Authority. Tel: +389 2 3297 412, e-mail: pma@kibstrust.com.

Version History

Version	Date	Changes
2.0	09.09.2022	Document “Terms and Conditions for use of Qualified Trusted Services” is updated with service for issuing qualified time stamps. Change of document encoding from 4-111.01-01 to 111.07. Rearranging titles and some content.
1.0	08.05.2012	Initial document connected with KIBS Root CA G2

Table of Contents

1. General Terms

THESE TERMS AND CONDITIONS AFFECT YOUR LEGAL RIGHTS. PLEASE READ THEM CAREFULLY. BY ACCEPTING THESE TERMS AND CONDITIONS, YOU AGREE TO FOLLOW AND BE BOUND BY THEM.

1.1. The present Terms and Conditions for Qualified Trust Services (hereafter "Terms and Conditions") govern the use of the Qualified Certificates for Electronic Signatures, Seals and Time Stamps by Subscriber (hereafter "Subscriber") and constitute a legally binding contract between Subscriber and KIBS as Qualified Trusted Service Provider (hereinafter KIBSTrust).

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

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

1.4. KIBSTrust may refuse the issuance of the Certificate at its sole discretion if Subscriber's identity verification is not successful.

1.5. The Subscriber must complete the certificate issuance process within 30 days from the date of submission of the Purchase Order prepared as Agreement form (hereinafter Purchase Order) for the issuance of a Qualified Certificate.

1.6. Subscriber shall be legally eligible or duly authorized for the issuance of a Qualified Certificate or for any trust service in general.

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

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

1.9. 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 or the trust service.

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

1.11. The Certificate may in no case be transferred to another person.

2. Trust Services

The Subscriber can apply for the following Trusted services offered by KIBSTrust:

2.1. Qualified Certificate for Qualified Electronic Signature issued to a natural person, with the use of a QSCD.

2.2. Qualified Certificate for Advanced Electronic Signature issued to a natural person, without the use of a QSCD.

2.3. Qualified Certificate for Qualified Electronic Signature issued to a natural person associated with a legal person, with the use of QSCD.

2.4. Qualified Certificate for Advance Electronic Signature issued to a natural person associated with a legal person, without the use of a QSCD.

2.5. Qualified Certificate for Qualified Electronic Seal issued to a legal person, with the use of a QSCD.

2.6. Qualified Certificate for Advanced Electronic Seal issued to a legal person, without the use of a QSCD.

2.7. Qualified Service for issuing Qualified timestamps.

Qualified Certificates are Long-term certificates. A Long-term certificate is valid from 1 to 3 years.

[1] Law on the Prevention and Protection from Discrimination

3. Reliance Limits

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

3.1.1. 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.

3.1.2. 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.

3.1.3. 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. Identity Proofing & Certificate Application

4.1. Before the issuance of a Qualified Certificate, the Subscriber's identity is verified by KIBSTrust 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).

4.2. Subscriber / Subject shall sign and submit to KIBSTrust's RA/LRA the respective Purchase Order, 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 the 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 the Government of the Republic of North Macedonia accept as a legal travel document and passport for all citizens. KIBSTrust may assign part of or the whole identity verification process to a third party.

5. Electronic Time Stamps

5.1. Subscriber of Qualified Time-Stamping Services can be a natural person or legal person, by entering into a relevant agreement with KIBSTrust.

5.2. Subscriber shall be responsible for placing the Time Stamp when signing with his Qualified Certificate.

5.3. Reliance Limits for Time Stamps:

5.3.1. Time Stamps become valid as of the date specified in them. Expired Time Stamps are invalid. 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. KIBSTrust Time Stamping Authority (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.

5.3.2. KIBSTrust has in place technical procedures to ensure that Time Stamp Tokens are issued securely and include the correct time. The KIBSTrust QTSA 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. KIBSTrust implements security controls preventing unauthorized

operation, aimed at calibration of QTSA time. KIBSTrust monitors that synchronization is maintained when a leap second occurs.

5.3.3. 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.

5.3.4. Time-Stamping Certificates are valid for ten (10) years. Logs and records for Timestamping are retained for ten (10) years after the expiration of the TSU Certificate.

5.3.5. Subscriber of Time-Stamping Services shall:

- use secure cryptographic functions for time-stamping requests.
- verify that:
  - the Time-Stamping Unit (TSU) Certificate belongs to KIBSTrust
  - the TSU Certificate has not been revoked
  - it is marked as qualified
  - the issuing QTSA Certificate has not been revoked.

5.3.6. Relying Parties of Time-Stamping Services shall verify that:

- the Time-Stamping Unit (TSU) Certificate belongs to KIBSTrust
- the TSU Certificate has not been revoked
- it is marked as qualified
- the issuing QTSA Certificate has not been revoked.

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

6.1. Upon submitting Purchase Order 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 120 hours (5 days) from certificate generation, constitutes Certificate acceptance.

6.2. Certificate Type and applicable policy:

Certificate Type	Certification Policy Applied and Published
Qualified Electronic Signatures compliant with MK-eIDAS and eIDAS.	KIBSTrust 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.	KIBSTrust 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; QCP-l-qscd
Qualified Timestamping	KIBSTrust Qualified Time Stamping Authority Certificate Policy & Certification Practice Statement, published on: https://www.kibstrust.com/repository ETSI EN 319 421, ETSI EN 319 422 Policies

7. Acceptable use

7.1. A qualified electronic signature has equivalent legal effect of a handwritten signature and is linked to the signatory so that the latter cannot deny in the future that he was the one who signed.

7.2. A qualified electronic seal is used to ensure the origin and integrity of the data to which it is linked.

7.3. Certificates shall not be used outside the limits and contexts specified in KIBSTrust CP/CPSs or for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of KIBSTrust.

7.4. Time-Stamping Services shall be used within the limits and contexts specified in the KIBSTrust QTSA CP/CPS. Any unlawful use outside those limits is prohibited.

8. KIBSTrust's obligations

8.1. Without prejudice to Section 12, KIBSTrust shall provide the services in accordance with the CP/CPS for Qualified Electronic Signatures and Electronic Seals, KIBSTrust Qualified Time Stamping Authority CP/CPS, as well as the relevant legislation.

9. Subscriber's Obligations

9.1. 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 KIBSTrust's CP/CPS for Qualified Certificates for Electronic Signatures and Electronic Seals and Time Stamping Authority CP & CPS respectively.

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

9.2.1. Be solely responsible for the maintenance of their Private Key.

9.2.2. Be solely and fully responsible for any consequences of using their certificates both during and after the validity of the certificate.

9.2.3. 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.

9.2.4. Be aware that Electronic Signatures or Electronic Seals given based on expired or revoked Certificates are invalid.

9.2.5. Submit accurate, true, and complete information in relation to the issuance of the Certificate.

9.2.6. Submit the necessary identification documents to KIBSTrust as specified in the Purchase Order and Agreement form for certificate issuance, as well as follow the steps that KIBSTrust indicates for completing the registration process.

9.2.7. Not continue with the certificate issuance procedure if the Subscriber is not legally eligible to do so.

9.2.8. Ensure that Subscriber´s Private Key is used under his/her control and exercise reasonable care to avoid unauthorized use of it.

9.2.9. Be responsible for the secrecy of the Private Keys when residing on a local QSCD, as well as the authentication credentials (username, password, OTP) accessing private keys when residing on a remote QSCD.

9.2.10. 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.

9.2.11. Use his/her Private Key and Certificate in accordance with present Terms and Conditions, including applicable agreements set out in Section 13, and the laws of Republic of North Macedonia.

9.2.12. Notify KIBSTrust 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;

9.2.13. Immediately inform KIBSTrust 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.

9.2.14. Report any change of information submitted during certificate request or change in submitted accompanying documents.

9.2.15. Immediately request revocation of the certificate if previously established relations with the person subject of certification terminated or ceased to exist.

9.2.16. Be responsible of placing the timestamp when signing with their Qualified Certificate.

9.2.17. Not continue using the private key if the certificate has been revoked or the CA has been compromised.

9.3. The Subscriber of Qualified Time Stamping Service shall:

9.3.1. use timestamping service in compliance with KIBSTrust Time Stamp Authority CP/CPS and these Terms and Conditions.

9.3.2. create timestamp requests only according to international standards supported by KIBSTrust, approved software or methods.

9.3.3. 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.

9.3.4. Verify the signatures created by the KIBSTrust QTSA on the TST (Verification whether the QTSA signature on the TST is valid and Verification of the QTSA certificate).

9.3.5. Use secure cryptographic functions for time-stamping requests.

9.3.6. Be aware that expired Time Stamps are invalid.

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

9.4.1. The Subscriber shall follow the instructions exactly as per the instructions presented by the mobile application made available for download by KIBSTrust or a partner company or the authorized employee of KIBSTrust who conducts the validation process.

9.4.2. Subscriber should present identification document(s) in good condition to the extent that its authenticity can be verified.

9.4.3. At the beginning of the remote recognition and before the initiation of the verification process, the Subscriber must provide his consent regarding the use, recording and storage of the remote identity recognition process and collected data.

9.4.4. If a third party other than the Subscriber / Subject appears in the process of remote identity verification, the process will not end successfully, and all recorded data will remain as an audit trail and the process can be repeated.

9.4.5. KIBSTrust'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 KIBSTrust's automatic process of remote authentication or towards authorized employee. In these cases, the process can be repeated and the Subscriber must choose one of the other identity verification methods specified in section 4.

10. Relying Parties Obligations

10.1. Any Relying Party studies the risks and liabilities related to the acceptance of a Certificate. 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 will chose to rely on the information in a Certificate. A Relying Party is responsible for deciding whether to rely on the information in a Certificate.

10.2. A Relying Party acknowledges and agrees that his use of KIBSTrust's Repository and his reliance on any Certificate shall be governed by KIBSTrust's Certification Practice Statement, as applicable at any time.

10.3. If not enough evidence is referenced in the Certificate regarding its the validity, a Relying Party shall verify the validity, suspension or revocation of the Certificate using current revocation status information based on the most recent Certificate Revocation List of the KIBSTrust Certification Authority.

10.4. Any limitations on usage of time stamps indicated by the KIBSTrust Time Stamping Authority CP / CPS should be considered.

10.5. A Relying Party shall verify the validity of any Certificate issued by KIBSTrust by checking OCSP and CRL references located in the Certificate.

10.6. A Relying Party is expected to use a Trusted List to establish whether an Electronic Signature, Seal or Time Stamp is qualified.

11. Certificate Revocation

11.1. Subscriber may request the revocation of a Certificate at any time by contacting KIBSTrust as provided in paragraph 19.2. KIBSTrust also has the right to revoke a Certificate only in the cases listed below. The revoked Certificate is published in the Certificate Revocation List (CRL).

11.2. A Certificate me by revoked by KIBSTrust in the following cases:

- KIBSTrust believes or strongly suspects that the Certificate has been compromised,
- KIBSTrust has reason to believe that the Subscriber has breached a material obligation under the present Terms and Conditions,
- KIBSTrust has reason to believe that the Certificate was issued in a manner not in accordance with its applicable procedures or issued to a person other than the one named in the Application or a that an unauthorized person has requested the issuance of the Certificate;
- KIBSTrust has reason to believe that a material fact in the Certificate Application is inaccurate or false, or becomes aware of changes which impact the validity of the certificate,
- Subscriber loses his legal eligibility, passes away, is declared absent; or is under liquidation or other similar procedure,
- Subscriber loses ability to use the local or remote QSCD,
- Subscriber requests revocation of the Certificate of a natural person associated with a legal person.
- A final court judgment requires the revocation,
- The private key of the CA has been compromised. In this case KIBSTrust will make a relevant announcement
- The Supervisory Body requests the revocation,
- Subscriber has not submitted payment, when due,
- Continuing the use of a certificate is harmful to KIBSTrust.

12. Warranties - Limitations of Liability - Indemnity

12.1. KIBSTrust ensures the availability of its Trust 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.

12.2. KIBSTrust is liable for the performance of its trust services as specified in its applicable Certification Practice Statements.

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

12.4. KIBSTrust informs all Subscribers, Subjects, the supervisory body and other parties with which it maintains relevant agreements and which may be affected, before it terminates any trust service and maintains documentation related to the terminated service, as well as the information necessary according to legal requirements.

12.5. KIBSTrust is not liable for:

12.5.1. 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,

12.5.2. 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,

12.5.3. the improper or incorrect 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,

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

12.5.5. the operation of software or other applications provided by third parties not related to KIBS.

12.5.6. the inauthenticity of identification documents or for any damage caused to the subscriber or other persons for this reason, provided that the procedure set out in the KIBSTrust identity verification policy has been carried out with all necessary checks during the verification of the authenticity of the document,

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

12.5.8. 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.

12.5.9. the failure to perform if such failure is occasioned by force majeure.

12.6. Limitations of liability

As stated in the respective CP/CPS-es, KIBStrust 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 KIBSTrust has been advised of the possibility of such damages.

12.6.1. In no event will the aggregate liability of KIBSTrust to all parties exceed the applicable liability cap for such qualified certificate set forth, below:

12.6.2. the combined aggregate liability of KIBSTrust 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 (50.000,00) euro, expressed in Denars according to the average exchange rate of the Denar against the Euro published by the National Bank of the Republic of North Macedonia on date payment, 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.

12.6.3. the combined aggregate liability of KIBSTrust 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, expressed in Denars according to the average exchange rate of the Denar against the Euro published by the National Bank of the Republic of North Macedonia on date payment, 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.

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

12.7. Indemnity

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

- inaccuracies or misrepresentations of information on the Certificate Purchase Order; or Subscriber's failure to disclose important information which will affect the Certificate's content, if such false representation or omission made with intent to deceive any party,
- Subscriber's failure to protect his private key, to use a trustworthy system, or to otherwise take the preventive measures necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of his private key,
- the Subscriber's use of a name that infringes the Intellectual Property rights of any third party.

13. Applicable Agreements, Policies, CP/CPS

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

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

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

- Policy for Qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (0.4.0.194112.1.2)
- Policy for Qualified certificates issued to natural persons (OID 0.4.0.194112.1.0), QCP-n
- Policy for Qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (0.4.0.194112.1.3)
- Policy for Qualified certificate issued to a legal person where the private key and the related certificate do not reside on a QSCD (0.4.0.194112.1.1)
- Normalized Certificate Policy (OID 0.4.0.2042.1.1)
- Normalized Certificate Policy requiring a secure cryptographic device (OID 0.4.0.2042.1.2)

13.3. KIBSTrust Time Stamping Authority CP/CPS.

13.4. KIBSTrust Privacy Policy.

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

14. Privacy Policy and Confidentiality

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

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

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

14.4. KIBSTrust 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.

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

15. Accessibility for persons with disabilities

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

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

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

Also, a PO can be prepared for persons with disabilities that reach RA, LRA or authorized third-party entity offices from officers employed by KIBSTrust, by LRA or by authorized third party entities. In this case person with disability should be accompanied by someone to assist them in the process of issuing the certificate.

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

16. Refund Policy

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

16.1. In case the sale of the Certificate is effected via the internet 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

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

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

16.4. The Subscriber has the right to withdraw from the online prepared Purchase Order 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, KIBSTrust will not refund payment, but will bind payment to a new procedure for purchasing a Certificate during the ongoing fiscal year.

16.5. KIBSTrust 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 KIBSTrust by sending an e-mail to helpdesk@kibstrust.com.

17. Applicable law, complaints, and dispute resolution

17.1. Any disputes related to the trust services provided under these Terms and Conditions 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.

17.2. To the extent permitted by law, before any dispute resolution mechanism may be invoked with respect to a dispute involving any aspect of KIBSTrust Trust Services, the Subscriber or other party must notify KIBSTrust, 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) calendar 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.

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

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

18. Licenses, Trust list and Audit

18.1. KIBSTrust is a Qualified Trust Service Provider and is granted the qualified status by a supervisory body, Ministry of Information Society and Administration in Republic of North Macedonia (MIOa) and it is listed in Register of trust service providers and electronic identification schemes (on https://trusteid.mioa.gov.mk/en/home/register-and-lists/) , following the submission of a conformity assessment report by an accredited Conformity Assessment Body.

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

18.3. 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.

19. Contact Information

19.1. Qualified Trust Service Provider

KIBS AD Skopje (KIBSTrust)
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)

19.2. 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.

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

20. Validity of Terms and Conditions

20.1. The present Terms and Conditions is prepared in Macedonian and other languages. In case of conflict between the original document in Macedonian language and its other language translations, the document in Macedonian language shall prevail.

20.2. 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.

21. 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.
KIBS	KIBS A.D. Skopje
KIBSTrust	The Trust Service Provider is organizationally part of KIBS AD Skopje, but operates under the brand name KIBSTrust, hence the terms "Trusted Service Provider" and "Qualified Trusted Service Provider" are identified with "KIBSTrust".
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-term 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)
NTP	Network Time Protocol, an internet protocol used to synchronize with computer clock time sources in a network
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 and MK-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.
Subject	The subject can be: a) a natural person. b) a natural person identified in association with a legal person.
Subscriber	Natural or legal person subscribing for any Trust Service with a Trust Service Provider and 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.
Trust Services	The Subscriber can apply for the following Trusted services offered by KIBSTrust: - Qualified Certificate for Qualified Electronic Signature issued to a natural person, with the use of a QSCD. - Qualified Certificate for Advanced Electronic Signature issued to a natural person, without the use of a QSCD. - Qualified Certificate for Qualified Electronic Signature issued to a natural person associated with a legal person, with the use of a QSCD. - Qualified Certificate for Advanced Electronic Signature issued to a natural person associated with a legal person, without the use of a QSCD. - Qualified Certificate for Qualified Electronic Seal issued to a legal person, with the use of a QSCD. - Qualified Certificate for Advanced Electronic Seal issued to a legal person, without the use of a QSCD. - Qualified Service for issuing Qualified timestamps.

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