Trusted Services Provider KIBS

Terms and Conditions

For Use of Qualified Certificates
for Electronic Signatures and Electronic Seals

Last modified: 06.07.2020, 1201-288/1 (view archived versions)

Version History

Version	Date	Author	Purpose of changes
1.0	06.07.2019	Marin Piperkoski	Initial document

Definitions and Acronyms

Term/Acronym	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
CA	Certificate Authority: A part of KIBS structure responsible for issuing and verifying electronic 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.
CP	Certificate Policy. KIBS as Qualified Trust Service Provider is under hierarchy of globally trusted certificate provider DigiCert. This global trust is also transferred to the certificates issued by KIBS.
CPS	KIBS Certification Practice Statement
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
MK-eIDAS	Law for electronic documents, electronic identification, and trusted services.
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.
QSCD	A Qualified Signature Creation Device that meets the requirements laid down in eIDAS Regulation.
Relying Party	Natural or legal person that relies on the information contained within a Certificate.
Authorized third party	Legal entity that under special conditions is authorized by the TSP KIBS to perform marketing activities and sale of TSP KIBS's services.
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.
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 Certificates	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.

1. General Terms

Present General Terms and Conditions describe main policies and practices followed by KIBS and provided in CP, CPS and KIBS Disclosure Statement for Qualified Electronic Signatures and Qualified Electronic Seals.

1.1. The Terms and Conditions govern Subscribers' use of the Certificates 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 has the right to change the Terms and Conditions at any time should KIBS have a justified need for such changes. Every time a Subscriber use certificate he/she is bound by the Terms and Conditions in effect published on the website https://www.kibstrust.com/repository. KIBS kindly reminds Subscribers to visit this website from time to time and review it.

1.4. The Subscriber can apply for:

1.4.1. Qualified Electronic Signatures only personally, except in case the Subscriber is a legal person and the Subject is a natural person associated with the legal person.

1.4.2. Qualified Electronic Seals though the natural person representing the legal person to whom the Qualified Certificate for the Qualified Electronic Seal is provided.

KIBS as TSP ensures that respect principle of equality and protection against discrimination in the exercise of human rights and freedoms[2].

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

2.1. Upon applying 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

[2] Preventing and protection from Discrimination law

- 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 Certification Practice Statement for Qualified 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 Certification Practice Statement for Qualified Electronic Signatures and Qualified Electronic Seals, published on: https://www.kibstrust.com/repository ETSI EN 319 411-2 Policy: QCP-l-qscd

3. Prohibitions of use

3.1. The use of the Subscriber´s 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).

4. Reliance Limits

4.1. Certificates become valid as of the date specified in the Certificate.

4.2. 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.

4.3. Audit logs are retained on-site for no less than two (2) months. Physical or digital archive records regarding Certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are retained for at least ten (10) years after the expiry of the relevant Certificate.

5. Subscriber's Rights and Obligations

5.1. The Subscriber has the right to apply for issuing a Certificate.

5.2. The Subscriber is obligated to:

5.2.1. Accept the Terms and Conditions.
5.2.2. Adhere to the requirements provided by KIBS.
5.2.3. Submit accurate, true, and complete information in relation to the issuance of the Certificate.
5.2.4. Not to continue with the Certificate issuance procedure, if the Subscriber is not legally eligible to do so, and/or is not an adult.
5.2.5. Ensure that the credentials under which he/she gets access to the Private Key is used under his/her control and exercise reasonable care to avoid unauthorized use of it.

5.2.6. Use his/her Private Key and Certificate in accordance with Terms and Conditions, including applicable agreements set out in Section 9, and the laws of the Republic of North Macedonia and the European Union.

5.2.7. Notify KIBS of the correct details during a reasonable time, in case of a change in his/her personal details or of the legal person's details and of the identity of the natural person representing it or of any inaccuracy or to the Certificate content;

5.2.8. 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 activation data (e.g. username, password, OTP code, PIN code) or other reasons and immediately revoke his/her Certificate.

5.2.9. Not to continue using the private key if the Certificate has been revoked or is aware that the CA has been compromised.

6. KIBS Rights and Obligations

KIBS is obligated to:

6.1. Supply certification service in accordance with the applicable agreements set out in Section 9 and the relevant legislation.

6.2. Keep account of the certificates issued by it and of their validity.

6.3. Provide security with its internal security procedures.

6.4. Provide the possibility to check the validity of certificates 24 hours a day.

6.5. Ensure that the certification keys are protected by hardware security modules (i.e. HSM):

6.6. Provide the subscriber certification keys used in the supply of the certification service are activated on the basis of subscriber sole control.

6.7. Publish the Certificates it issues at its website, at: https://e-shop.kibstrust.com/raforms/VerbaSearchCert.aspx, in order for a third party to be able to search it, provided that the Subscriber has granted his/her consent for this purpose.

6.8. Keep records related to the Certificate applications submitted, the relative Certification Authority's event logs, as well as the Certificates, safely for ten (10) years, after the revocation or expiration day of the Certificate.

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 CPS and the CP. 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 CPS that can have changes from time to time. The applicable 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 CPS are also posted in KIBS Repository at https://www.kibstrust.com/repository.

7.3. If not enough evidence is enclosed to the Certificate or Electronic Signature with regard to the validity of the Certificate a Relying Party verifies the validity, suspension or revocation of the Qualified Certificate using current revocation status information prior to relying on a Signature or Seal 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. 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.

7.4. A Relying Party follows the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CPS and CP. Generally: 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.

7.5. 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. KIBS offers OCSP service for checking Certificate status. Service is accessible over HTTP protocol and publicly available on http://ocsp1.kibstrust.com.

7.7. A Relying Party verifies the validity of the Certificate by checking Certificates validity against OCSP.

The URL of the OCSP service is included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile.

8. Limited Warranty and Disclaimer/Limitation of Liability

8.1. The Subscriber and Subject is solely responsible for the maintenance of his/her Private Key and credentials that allows access to it.

8.2. The Subscriber and Subject is solely and fully responsible for any consequences of using their Certificates both during and after the validity of the Certificates.

8.3. The Subscriber and Subject is solely liable for any damage caused due to failure or undue performance of their obligations specified in the Terms and Conditions and/or the laws in Republic of North Macedonia and European Union.

8.4. The Subscriber and Subject is aware that electronic signatures given based on expired or revoked Certificates are invalid.

8.5. KIBS ensures that:

1. The certification service is provided in accordance with CPS, CP and the relevant legislation in Republic of North Macedonia of European Union.
2. The CA certification keys are protected by hardware security modules (HSM).
3. The Subscriber certification Keys on a Remote QSCD are protected by hardware security modules (HSM) and are under sole control of KIBS.
4. The certification keys used to provide the certification service are activated on the basis of shared control.
5. It has compulsory insurance contracts covering all KIBS trust services to ensure compensation for damages caused by KIBS breach of obligations.
6. It 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 CPS.

8.6. KIBS is not liable for:

- The secrecy of the Private Keys of the Subscriber or Subject when reside on a Local QSCD, for possible loss or damage of the local QSCD.
- 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.
- Any misuse of the Certificates or inadequate checks of the Certificates or for the wrong decisions of a Relying Party or any consequences due to error or omission in Certificate validation checks.

- The non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, the data protection supervision authority, Trusted List or any other public authority.
- The failure to perform if such failure is occasioned by force majeure.

8.7. As stated in the 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 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 unavailability of certificates, electronic signatures, electronic seals, 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:

- the combined aggregate liability of KIBS to any and all persons concerning a specific qualified certificate shall be limited to an amount not exceeding thirty thousand (30.000,00) denars per certificate and a total maximum of claims of six million (6.000.000,00) denars, 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 certificates for Qualified Signatures/Seals, transactions, or claims related to such certificate.

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

8.8. 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 to a document.

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

9. Applicable Agreements, Policies, CP, CPS

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

9.1. DigiCert Certificate Policy.
9.2. KIBS Certification Practice Statement for Qualified Certificates for Electronic Signatures and Electronic Seals.
9.3. Certificate and OCSP Profiles for Qualified Electronic Signatures and Qualified Electronic Seals, and specifically:

- Policy for Class 2 Certificate: (2.16.840.1.114412.5.2)
- Policy for qualified certificate issued to a natural person (0.4.0.194112.1.0)
- Policy for qualified certificate issued to a legal person (0.4.0.194112.1.1)
- 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 certificate issued to a legal person where the private key and the related certificate reside on a QSCD (0.4.0.194112.1.3)

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 follows the Privacy Policy, provided in the KIBS repository https://www.kibstrust.com/repository and all legal acts of Republic of North Macedonia and European Union, when handling personal information and logging information.

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 online of Purchase Order and face-to-face identification in front of RA/LRA representative or online.

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. 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.

12.2. 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 for Qualified Certificate for electronic signature or seal in/to RA/LRA

of Trusted service provider, the purchase order 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.

12.3. 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. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

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 Trusted List of Qualified Trust Service Providers of Ministry of Information Society and Administration. The prerequisite requirement of this registration is in compliance with 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. 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
helpdesk@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 24/7 via email or 8/5 in-person in RA.

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

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.

END OF DOCUMENT