PKI Disclosure Statement (PDS)

Verba Sign, Verba Seal, Momentum

Version: 2.1

Date: 15.01.2025

111.08

KIBS AD Skopje

http://www.kibstrust.com/

Intellectual Property Rights

Version History

Version	Date	Author	Changes
2.1	15.01.2025	Lile Gagovska	Changes in chapters 4, 8 and 14
2.0	09.09.2022	Marin Piperkoski	Merging TSA disclosure statement with PKI disclosure statement. Change of document encoding from 4-111.01-02 to 111.08. Rearranging titles and some content.
1.0	08.05.2012	Marin Piperkoski	Initial document connected with KIBS Root CA G2

Table of Contents

1. Overview

This document aims to provide the Subscriber and Relying Parties of Qualified Certificates and Trusted Services with a quick recap concerning the information available in KIBStrust Certificate Policy & Certificate Practice Statement (KIBSTrust CP/CPS) for Use of Qualified Certificates and the Terms and Conditions for use of Qualified Trusted Services.

This document does not substitute or replace the Terms and Conditions nor the KIBSTrust CP/CPS, just summarizes the key points for the benefit of Subscribers and Relying Parties. All documents are available at: https://www.kibstrust.com/repository.

2. Contact information

All inquiries and comments concerning the contents of stated documents can be directed to:

KIBS AD Skopje (KIBSTrust)
Bul. "Kuzman Josifovski Pitu" 1, 5-th floor,
1000 Skopje, Republic of North Macedonia
+389 2 5513 444, +389 2 3297 444
https://www.kibstrust.com
pma@kibstrust.com
(Mon-Fri 8.30 - 16.00 Central European Time).

3. Important information

- Subscriber shall be aware of and accept KIBSTrust's applicable Terms and conditions.
- Subscriber must complete the certificate issuance process within one month from the date of submission of the certificate application.
- Subscriber shall be legally eligible or duly authorized to submit the certificate application.
- Subscriber agrees to use the Qualified Signature Creation Device (QSCD) which will be provided by KIBSTrust. The QSCD can either be local or remote. Subscriber is solely responsible for the proper use of the QSCD.
- Subscriber may require the non-publication of the certificate to KIBSTrust's Public Directory.
- 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.
- KIBSTrust is not liable for the operation of software or other applications provided by third parties outside KIBSTrust's control.

4. Certificates types, Identity proofing procedures and Use

KIBSTrust will issue all below types of certificates, on both: local QSCD as well as remote QSCD, and without a QSCD.

- Qualified certificate for qualified electronic signature issued to a natural person with use of local or remote QSCD.
- Qualified certificate for advanced electronic signature for natural person, without the use of a QSCD.
- Qualified Certificate for qualified electronic seal issued to a legal person, with use of local or remote QSCD.
- Qualified certificate for advanced electronic seal issued to a legal person, without the use of a QSCD.
- Qualified time stamping.

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

The Subscriber's identity is verified by 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 Law on Electronic Documents, Electronic Identification, and Trust Services); 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 Law on Electronic Documents, Electronic Identification, and Trust Services) ; or

- by equivalent to physical presence Remote ID verification using liveness method (art.24 par.1d of the eIDAS Regulation and art.31 of Law on Electronic Documents, Electronic Identification, and Trust Services).

Validation procedures comply with the latest version of KIBSTrust's "RA Manual for Qualified certificates for electronic signature and electronic seal (103.01)" and are printed in certificate Purchase Order and Agreement form.

Certificates shall be used as prescribed by the KIBSTrust CP/CPS and Terms and Conditions only. Any different usage is forbidden.

5. Revocation

A Subscriber requesting revocation or a successor who wishes to request revocation in case of a deceased Subscriber (natural person) provided that is legally eligible, shall send a request to KIBSTrust by e-mail at revoke@kibstrust.com or communicate by telephone at +389 2 3297444 or alternatively via KIBSTrust's Self Service Web Portal or submit revocation form in person in RA/LRA. KIBS will initiate revocation of the certificate in timely manner.

6. Subscriber's obligations

The certificate subscriber has the obligations set forth in the KIBSTrust CP/CPS and the Terms and Conditions. But not only, following obligations have to be respected:

- In the process of certificate request and identification to provide the CA with trustworthy evidence to prove his/her identity and the identity of the organization with which he/she is associated with.
- Examine issued certificate and verify that the identification information contained in the certificate is accurate.
- To be the only person that use a private key corresponding to the public key in the certificate.
- Make sure that the certificate at the time of its use has not expired and has not been revoked.
- Use the certificate only in the ways and for the purposes provided for in the KIBSTrust CP/CPS.
- Subscriber shall protect and ensure the safety of the local QSCD or the authentication credentials in case of the remote QSCD.
- Not leave the local QSCD or the authentication credentials in case of the remote QSCD exposed and place it in a secure location.
- Treat the local QSCD or the authentication credentials in case of the remote QSCD as any object containing private data.
- In the event of confirmed compromise of own private key, to contact KIBSTrust immediately.
- Report any change of information submitted during certificate request or change in submitted acompanying documents.
- Immediately request revocation of the certificate if previously established relations with the person subject of certification terminated or ceased to exist.

7. Relying parties' obligations

Relying Parties shall check the status of certificates on which they wish to rely. A way of checking the certificate's status is by consulting the most recent Certificate Revocation List (CRL) from KIBSTrust CA that issued the certificate.
Alternatively, Relying Parties may check the Certificate status using the KIBSTrust's online repository or OCSP responder. KIBSTrust provides Relying parties with information on how to find the appropriate CRL, repository or OCSP responder to check whether certificates have been revoked.

8. Certificate status checking obligations of Relying parties

Relying Parties shall check the status of Certificates on which they wish to rely. A way of checking the status is by consulting the most recent CRL from the Certification Authority that issued the Certificate on which the Relying Party wishes to rely.

Alternatively, Relying Parties may meet this requirement by checking Certificate status using the KIBS web-based repository (https://e-shop.kibstrust.com/raforms/VerbaSearchCert.aspx) or by using OCSP publicly accessible at

http://ocsp2.kibstrust.com and http://ocsp3.kibstrust.com.The URL of the OCSP service is also included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile.

KIBS is obligated to publish the certificates it issues at its website: https://e-shop.kibstrust.com/raforms/VerbaSearchCert.aspx, in order for a third party to be able to search it. Subscriber must give consent for publishing data from certificate.

9. Reliance Limits

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.

10. Applicable Agreements, CP/CPS

Relevant agreements, policies, and practice statements for use of Certificates are:

- Certificate Policy & Certification Practice Statement for Qualified Certificates for Electronic Signatures and Electronic Seals (KIBSTrust CP/CPS).
- Qualified Time Stamping Authority Certificate Policy & Certification Practice Statement (QTSA CP/CPS)
- Terms and Conditions for Use of Qualified Trust Services.
- Professional Liability Insurance of the Trusted Services Provider.
- Privacy policy.

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

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

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

The Subscriber, within the period of five (5) 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, access problems or 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.

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

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 within thirty (30) days from his/her purchase order for Qualified Certificate for electronic signature, electronic seal or timestamping 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, electronic seal, or electronic timestamping, KIBS will not refund payment, but will bind payment to a new procedure for purchasing a Certificate during the ongoing fiscal year. Transferring payment to another fiscal year is not allowed.

Claims for refunding qualified certificates for electronic signature, electronic seal an electronic timestamping KIBSTrust handles 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. Privacy Policy

KIBSTrust processes personal data in accordance with the applicable data protection legislation in force. For further details, please refer to KIBS Privacy Policy at https://www.kibstrust.com/repository.

14. Repository Licenses, Trust Marks, and Audit

KIBS through its brand KIBSTrust is Trusted Services provider for Qualified and non-Qualified trusted services registered at **Register of trust service providers and electronic identification schemes** published by Ministry of Digital Transformation (MDT) on https://trusteid.mdt.gov.mk/en/home/register-and-lists/.

The prerequisite requirement of this registration follows applicable regulations and standards. 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 on regular, yearly basis. Audit conclusions or certificates, which are based on audit results of the conformity assessment conducted pursuant to the eIDAS Regulation and accreditation scheme: ISO/IEC 17065 + ETSI EN 319 403 + eIDAS Art.3.18 Scope of accreditation.

15. Limited warranty and Disclaimer, Limitation of liability

For warranty and liability limitations, please refer to the Terms and Conditions published under the Repository of KIBSTrust website at: https://www.kibstrust.com/repository.

16. Applicable Law, Complaints, Dispute Resolution

Any disputes related to the Trust Services provided by KIBSTrust shall be governed by the laws of the Republic of North Macedonia. The Subscriber must notify Trusted service provider KIBSTrust 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 Subscriber may seek legal resolution. Competent court in Skopje shall have exclusive jurisdiction and venue for hearing and resolving any dispute.

This document is prepared in Macedonian and other languages. In case of conflict between the original document in Macedonian and its other language translationc, the document in Macedonian language shall prevail.

END OF DOCUMENT