RELYING PARTY AGREEMENT

For Qualified Certificates

A Relying Party is an individual or entity that acts in reliance of a certificate issued.

Before validating Qualified Certificate or otherwise accessing or using the database of the Certificate Authority KIBS AD Skopje (hereinafter: Issuer), or relying on the information about issued and revoked certificates, read carefully this Relying Party Agreement (hereinafter: Agreement) and Issuers Certificate Practice Statement (hereinafter: CPS). The CPS, which can be updated and amended, is incorporated in this Agreement by reference. The applicable CPS is published on the website of the Issuer:

https://www.kibstrust.mk/repository/cps

Qualified Certificate will be issued in accordance with the requirements set by the Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999 on a Community framework for Electronic Signatures (hereinafter: Directive) and the Law on Data in Electronic Form and Electronic Signature of the Republic of Macedonia.

The Issuer is registered in the Certificate Issuers' Registry of Republic of Macedonia with decision number 02-20725/1 since 22.06.2006.

The following table indicates how you know what the object identifier (hereafter: OID) and certificate policy (DL1 or DL2) corresponding to the Qualified Certificate you are requesting for, is. These policies are described in the document "VeriSign Trust Network European Directive Certificate Policies (hereafter: EDP)", which is being published at KIBS repository at https://www.kibstrust.mk/repository/cps. Each of these certificate policies corresponds to specific requirements of the EU Directive and to respective specific requirements of the ETSI 101 456 standard (Policy Requirements for CAs issuing Qualified Certificates).

OID	EU Directive Article	ETSI Standard Terminology	EDP Terminology
(0.4.0.1456.1.2)	Article 5.2	QCP public	DL1
(0.4.0.1456.1.1)	Article 5.1	QCP public + SSCD	DL2

Table 1: Object identifier and certificate policy

Contract subject

Article 1

This Agreement regulates the conditions under which Relying Party submits a query for a Qualified Certificate, asks for verification of a digital signature created with a private key corresponding to a public key contained in a Qualified Certificate, or when otherwise use or rely upon any information's or services provided in KIBS's Repository (https://www.kibstrust.mk/repository/rpa) or website relating to a Digital Certificate.

Article 2

Accepting this Agreement you hereby acknowledge that you have access to sufficient information in order to make an informed decision as to the extent to which you will chose to rely on the information contained in a Qualified Certificate and that you are solely responsible for deciding whether or not to rely on such information.

You demonstrate knowledge and acceptance of the terms of the Agreement by submitting a query to search for, or verify the revocation status of a Qualified Certificate, or by otherwise using or relying upon any information or services provided by the Issuer. With any of previous actions you are bound to the terms of this Agreement, as though you had signed it by hand.

Rights and obligations of the Issuer

Article 3

Issuer has obligation to:

1. Maintain an accurate directory of issued certificates.
2. Maintain an accurate Certificate Revocation List (hereinafter: CRL).
3. Provide limited guarantees for the Relying Parties concerned to rely on Qualified Certificates for verifying the digital signature, and that:
    - Providing Qualified Certificate to contain all the necessary information according to the CPS.

- Subscriber's Qualified Certificate has public key which corresponds to its private key generated just before Qualified Certificate was issued.
- Upon revocation of a Subscriber's Certificate, the Issuer publishes notice of such revocation in the CRL, pursuant to the provisions of the CPS.

4. Records related to the Qualified Certificate application form and the relative Certification Authority's event logs will be kept securely for at least five (5) years after the expiration or revocation day of the Qualified Certificate.

Rights and obligations of the Relying Party

Article 4

Relying party

1. Shall verify the validity or revocation of the Qualified Certificate using current revocation status information prior to relying on a digital signature created with a private key corresponding to a public key contained in a Qualified Certificate. A method by which you may check Certificate status is by consulting the most recent Certificate Revocation List issued by Issuer.
2. Shall take into account the specific limitations on the usage of the certificate indicated to the relying party in the applicable CPS. Generally:
    - Qualified Certificates shall be used only to the extent their use is consistent with applicable law.
    - Subscribers of DL2 Certificates, in their own responsibility, solely create digital signatures only in connection with the use of an SSCD.
    - Issuer's 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.
3. Shall take any other precautions prescribed in this Agreement.

Disclaimer

Article 5

Issuer cannot be held liable for:

- damages caused by theft or other form of compromise of a private key corresponding to a public key contained in a digital certificate, which may or may not be detected, and of the possibility of use of a stolen or compromised key to forge a digital signature to a document.
- any damages, or for any loss of profits, loss of data, arising from or in connection with the use, of qualified certificates and digital signatures.

Or liability is limited, in a way that:

- In no event will the aggregate liability of Issuer to all parties exceed the applicable liability cap stipulated in Issuer's CPS.

Entry into force

Article 6

This Agreement becomes effective when a Relying Party submits a query for a Qualified Certificate, or asks for the verification of a digital signature created with a private key corresponding to a public key contained in a Qualified Certificate, or when otherwise uses or relies upon any information or services provided by the Issuer.

Force Majeure

Article 7

"Force Majeure" refers to any event, including, but not limited to, wars or natural disasters, that is unforeseeable, the occurrence and effect of which is unavoidable and insurmountable. The Issuer that failed to perform this Agreement in full or in part, due to the occurrence of Force Majeure, should be exempted from all or some of its responsibilities hereunder. Specifically the Issuer shall not be liable for any delay, default or failure in performance under this Agreement to the extent said failures or delays are proximately caused by conditions beyond the Issuer's (reasonable) control and occurring without its fault or negligence, including, without limitation, natural disasters (earthquakes, fires, floods) social events (strikes, wars, riots or other major upheaval) acts of public authority and distortions in the functioning of the system.

Competent law

Article 8

For all that is not governed by this Agreement, shall apply the provisions of the CPS.

Final provisions

Article 9

In the event that a clause or provision of this Agreement is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the Agreement shall remain valid.

Article 10

The Relying party agrees that for any disputes related to the services provided under this Agreement, shall first notify the Issuer for the purpose of seeking dispute resolution. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may seek legal resolution on court. Competent court is court in Skopje.

Issuer
Goran Anastasovski
Signature: