PKI disclosure statement

Version 1.0

Komerční banka, a.s., Na Příkopě 33, 114 07 Praha 1

Table of Contents

1 INTRODUCTION 4
2 CONTACT INFORMATION 5
3 CERTIFICATE TYPES AND VERIFICATION PROCEDURES 6
3.1 KB client certificates 6
3.2 Qualified certificates for electronic seal 6
4 LIMITATIONS OF USE 7
5 OBLIGATIONS OF CERTIFICATE SUBSCRIBERS 8
6 OBLIGATIONS OF THE RELYING PARTIES 9
7 LIMITATION OF WARRANTY AND LIABILITY 10
8 AGREEMENTS AND CERTIFICATE POLICIES 11
9 PERSONAL DATA PROTECTION 12
10 REFUND AND CLAIMS POLICY 13
11 LEGAL ENVIRONMENT 14
12 CERTIFICATIONS, AUDITS AND INSPECTIONS 15

Version overview

Version	Date	Description	Approved
1.0	May 29th, 2023	First published version	Tomáš Prjacha, Manager PKI  Digitálně podepsal(a) Tomáš Prjacha dne 29.05.2023 10:16:12

Abbreviation overview

Abbreviation	Full meaning
eIDAS	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
KB	Komerční banka, a.s.
KB QCA	Komerční banka Qualified CA/RSA
Terms and conditions	General terms and conditions
PKI	Private Key Infrastructure
TSP	Trust Services Provider

1 INTRODUCTION

This document provides a basic overview related to operation of certification and related qualified trust services of Komerční banka, a.s. and summarizes important information regarding the types of certificates issued, rights and obligations of the parties involved and complaint procedures, including contact details.

The document is structured according to annex A of ETSI EN 319 411-1 regulation.

2 CONTACT INFORMATION

The provider of certification and related qualified trust services (referred to as „TSP“) is Komerční banka, a.s., which operates the Public Key Infrastructure (referred to as "PKI") for this purpose. The operator of these services is Komerční banka, a.s. (referred to as "KB").

Contact and identification information:

Komerční banka, a.s.

IČ 45317054, DIČ CZ699001182

Na Příkopě 33, Praha 1, 114 07

Tel: 800 521 521

e-mail: info_ca@kb.cz

Certification policies, certificates and any other documents related to the operation of PKI KB are published on the website https://www.kb.cz/pki.

3 CERTIFICATE TYPES AND VERIFICATION PROCEDURES

Komerční banka Qualified CA/RSA (referred to „KB QCA“) issues:

- **Qualified certificates for electronic signature.**

  These certificates are issued:

  - To KB clients who have signed an Electronic Signature Agreement (referred to as the Agreement).

- **Qualified certificates for electronic seal.**

  These certificates are issued to legal entities.

The certificates are issues based on REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (referred to as „eIDAS“).

Certificate policies for all types of certificates issued are available at https://www.kb.cz/pki

3.1 KB CLIENT CERTIFICATES

Before the certificate is issued, the identity of the client must be verified at a KB branch. The client must sign an Electronic Signature Agreement (referred to as the "Agreement") with KB. After signing the Agreement, the client will have access to the MůjProfil web portal, where he/she can manage the certificates.

Certificates are issued to clients in smart cards issued by KB. Before submitting an application, the client must install software on his/her computer: an application wizard for working with certificates.

The client applies for a certificate using the MůjProfil web portal. The first step is to log in to the portal. Next step is to start the process of issuing the certificate. The application wizard guides the client through the process of issuing the certificate to the smart card. The client must authorize this by entering the PIN of the card.

The certificate renewal is done in the same way as the certificate issuance - via the MůjProfil portal and the smart card.

The client can use the issued certificate to create advanced electronic signatures.

3.2 QUALIFIED CERTIFICATES FOR ELECTRONIC SEAL

Prior to issuing a certificate, the identity of the applicant must be verified, as well as the identity of the legal entity for which the certificate is requested, and the applicant's power of attorney that declares agreement the subscriber is allowed to represent the legal person and is entitled to request certificates for that legal person or its members the legal entity in the matter of issuing a qualified certificate.

The identity of the applicant and other requirements are verified at the registration office of KB.

The applicant must appear at the registration office with the relevant documents. They must also deliver an electronic application for a certificate.

The applicant prepares the application in advance, using the technical means of the device that stores the cryptographic keys of the certificate. In case the keys are generated in a qualified electronic seal creation device, an authorized representative of the TSP must be present during the generation process.

If the applicant has fulfilled all the requirements, then based on the application the certificate shall be issued to the applicant. The applicant must sign a contract to confirm certificate ownership transfer.

The subject may use the issued certificate to create advanced electronic seals.

If the key pair related to the certificate has been generated in a qualified electronic seal creation device, then the subject may use the certificate to create qualified electronic seals.

4 LIMITATIONS OF USE

All certificates issued by KB may only be used in accordance with the applicable CR/EU legislation (a detailed description of the related legislation is provided in the chapter "Legal Environment"), the Agreement, the General Terms and Conditions (referred to as "Terms and Conditions") and the relevant certification policies of the issuing KB QCA.

KB processes information and personal data in accordance with Act 297/2016 on trust services for electronic transactions.

Further information related to personal data processing is published at https://www.kb.cz/cs/ochrana-osobnich-udaju.

5 OBLIGATIONS OF CERTIFICATE SUBSCRIBERS

The certificate subscriber is obliged to:

- become familiar with the Agreement, Terms and Conditions, Certificate Policy and related documentation and ensure compliance,
- treat the private key for which the certificate has been issued in accordance with the Agreement and the relevant certification policy with due care so that it cannot be compromised or used in an unauthorized manner (loss of exclusive possession of the private key).
- provide KB with true, accurate and complete information relating to the certificate being issued/issued without unnecessary delay and inform KB of any changes to the information listed in the certificate,
- immediately inform KB of any suspected misuse of the private key, and request that the certificate be revoked.

Additional obligations of the subscribers may be specified in the Agreement and the relevant certificate policy.

6 OBLIGATIONS OF THE RELYING PARTIES

A relying party is an entity that relies on qualified certificates issued by KB or more precisely the KB QCA for its activities. The relying party is obliged in particular to:

- Obtain and install KB PKI certificates from a secure source (https://www.kb.cz/pki) and verify the “fingerprint“ of these certificates,
- Before using the certificate, verify its validity, as well as the validity of CA certificates, against the current Certificate Revocation List (CRL) or using the Online Certificate Status Protocol (OCSP) service
- Use certificates in accordance with applicable legislation and the relevant certificate policy
- Other obligations of relying parties may be specified in the relevant certificate policy.

7 LIMITATION OF WARRANTY AND LIABILITY

KB commits to comply with all obligations implied by certificate policies and relevant legislation.

The specific limitations of warranties and responsibilities are part of the relevant certificate policy.

8 AGREEMENTS AND CERTIFICATE POLICIES

The relationship between the Client and TSP is, in addition to the relevant provisions of mandatory legislation, governed by the Agreement.

The relationship between the relying party and KB is governed by the relevant provisions of the applicable certification policies; it is not contractually regulated.

All public information, including Certificate Policies, is available on the website https://www.kb.cz/pki in the Qualified Certificates section.

9 PERSONAL DATA PROTECTION

Personal data is considered to be the information defined in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (referred to as “GDPR”)

TSP shall ensure the protection of personal data of persons to whom it gains access when providing certification services, in accordance with the requirements of the relevant legal standards. The principles for the processing of personal data are included in the certificate policies of trust services.

The responsibility for the protection of personal data processed in certification services systems lies with KB, as TSP, all its employees and contractors.

The processing of personal data is carried out to the extent necessary according to the GDPR and Act 297/2016 on trust services for electronic transactions.

10 REFUND AND CLAIMS POLICY

KB shall not be liable for damages resulting from the use of a certificate if the conditions of its use as stated in the certificate policy, the certification practice statement and related documents have not been complied with.

KB shall not be liable for any damage resulting from the use of the certificate in the period between receiving the revocation request and the actual revocation if it has taken all the steps required by the certificate policy and the certification practice statement.

KB shall be liable to the certificate subscriber for damages incurred in accordance with applicable law. KB shall be liable for damage caused by a breach of the certification service provider's obligations defined in the certificate policy and related documents.

Other possible damages are based on the provisions of the relevant laws and their amount may be decided by the court.

Complaints are handled in accordance with the KB Complaints code.

11 LEGAL ENVIRONMENT

KB's activities in qualified certification services are governed by the relevant provisions of the Czech legal system, namely:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)
- Act No 297/2016 Coll. on trust services for electronic transactions
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)
- Act No. 110/2019 Coll. on the processing of personal data

12 CERTIFICATIONS, AUDITS AND INSPECTIONS

KB is a qualified trust service provider for issuing:

- Qualified certificates for electronic signatures
- Qualified certificates for electronic seals
- Qualified electronic time stamps

The provision of KB's qualified trust services is regularly audited and controlled in accordance with applicable legislation.