PKI Disclosure Statements

Version 7.0

Document contents

Records of revisions and changes

Version	Date of revision	Change reason and description	Author	pproved by
1.0	15.12.2015	First version	Security officer	CIO
2.0	15.5.2017	Addition of performed audits	Security officer	CIO
3.0	15.4.2018	Addition of performed audits	Security officer	CIO
4.0	15.5.2020	Addition of performed audits	Security officer	CIO
5.0	15.4.2021	Addition of performed audits	Security officer	CIO
6.0	15.5.2023	Addition of performed audits	Security officer	CIO
7.0	15.4.2024	Addition of performed audits, using the Bank identity	Security officer	CIO

1. Introduction

1.1. Document purpose

This document provides a basic overview of the hierarchy of certification authorities eIdentity QCA and eIdentity VCA, the rights and duties of holders of certificates issued by eIdentity Qualified CA, eIdentity Public CA and parties relying on them.

This document has an informative character, is not intended to replace certification policies and is not part of any contract on provision of certification services entered into between the customer and the eIdentity a. s.

1.2. History of performed audits and system checks

Date	Type of audit/check	Auditor's/Inspector's statement
April 2024	Audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by EZÚ	Conformity
March 2024	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by URS	Conformity
April 2023	Re-certification audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by EZÚ	Conformity
March 2021	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by URS	Conformity
April 2020	Re-certification audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by EZÚ	
March 2018	Re-certification audit for certification in relation to ISO 9001 and ISO 27001, conducted by URS.	Conforms
April 2017	Certification audit confirming that the provided by qualified trust services are in conformity with regulation eIDAS and the relevant technical standards, conducted by EZÚ	Conformity

2. Contact information

2.1. Certification service provider

The ACAeID certification service provider is:
eIdentity a.s.
Vinohradská 184
130 00 Prague 3
IČ: 27112489

2.2. Contact workplaces

- Entering into agreements with eIdentity a. s. customers is ensured by sales and contact locations of eIdentity a. s. and External registration authority. Contact information is available on the website of eIdentity a. s. – https://www.eidentity.cz and http://www.ie.cz

Issuing and invalidation of certificates are ensured by branch of eIdentity a. s. and External registration authority.

Invalidation of certificates outside of working hours of branch is ensured by the following website:

www.eidentity.cz

2.3. Communication with clients

General inquiries can be sent to email: info@ eidentity.cz.
Technical questions can be sent to email: info@ eidentity.cz.

You can also use the eIdentity a.s. Customer Line: 222 866 150 (the line is only in the Czech language and is charged to standard rate).

2.4. Publication of information

This report for users, certification policies and other public information can be found on the website of eIdentity a.s.:

- https://www.eidentity.cz
- http://www.ie.cz

3. Types of signatures and verification procedures

3.1. Types of issued certificates

3.1.1. ACAeID QCA

The ACAeID has set up a two-level hierarchy of certification authorities named ACAeID CA. The root of this hierarchy is the certification authority ACAeID RCA, which issued the certificate for certification authority ACAeID QCA.

ACAeID QCA issues certificates to end users, and it applies two basic registration models depending on the end user. The first registration model is focused on legal person and natural person performing business activities and the second model is focused on natural person not performing business activities.

ACAeID QCA issues these types of certificates:

- Qualified certificates for electronic signature
- Qualified certificates for electronic seals

Certificates for public keys issued within the ACAeID QCA hierarchy satisfy the X.509 v3 standard.

Validity of certificates is 90-day.

3.2. Verification of the applicant when issuing the initial certificate

During the process of issuing the initial certificate, the identity of the applicant for the certificate is always verified through his personal documents and in the case of a certificate for a legal or entrepreneurial natural person also the link of the applicant for the certificate to this person.

The applicant for the certificate must be physically present during the process of issuing the certificate or must use electronic bank identity for issuing BankID certificate.

A detailed description of the registration procedures can be found in the relevant certification policies.

3.3. Verification of the applicant when issuing the subsequent certificate

During the process of issuing the subsequent certificate, the identity of the applicant for the subsequent certificate is verified by checking the electronic signature on the application for the subsequent certificate.

A detailed description of the registration procedures can be found in the relevant certification policies.

4. Restrictions on use

4.1.1. Qualified certificates for electronic signature

Qualified certificates for electronic signatures issued by ACAeID QCA may be used only for verifying an electronic signature in accordance with valid legislation.

The corresponding private key to the certificate issued by the qualified electronic signature can be stored on a qualified device for creating electronic signatures, but this is not required.

Qualified certificates for electronic signature issued by ACAeID QCA are not intended for communication or transactions in areas with increased risk of harm to health or damage to property, such as chemical operations, aviation, nuclear facilities, etc. or in connection with national security and defence.

4.1.2. Qualified certificates for electronic seal

Qualified certificates for electronic seal issued by ACAeID QCA may be used only for verifying an electronic signature in accordance with valid legislation.

The corresponding private key to the certificate issued by the qualified electronic seals can be stored on a qualified device for creating electronic seals, but this is not required.

Qualified certificates for electronic seal issued by ACAeID QCA are not intended for communication or transactions in areas with increased risk of harm to health or damage to property, such as chemical operations, aviation, nuclear facilities, etc. or in connection with national security and defence.

5. Obligations of customers and their representatives

A customer of the certification authority ACAeID is a legal person or natural person who is in a contractual relationship with the eIdentity a.s.. The customer must in particular

- provide truthful and complete information when entering into an agreement on provision of certification services,
- immediately inform the provider of certification services about changes to information contained in the contract or certificate.

An applicant for a certificate is natural person who based on having been entrusted to do so by a customer applies for issuance of a certificate and manages the issued certificate. (If the customer is natural person not performing business activities, then the customer is the applicant.) The applicant must in particular

- become familiar with the certification policy under which the certificate is to be issued,
- provide truthful and complete information to the certification service provider,
- promptly inform the certification service provider of any changes in details contained in the contract on provision of certification services or in the issued certificate,
- handle the private key corresponding to the public key in the certificate issued based on the selected certification policy with proper care, to ensure that it is not used by anyone unauthorised and that the private key is used only for the purposes specified in the certification policy, according to which the certificate has been issued,
- to notify the certification service provider immediately of any circumstances that will lead to invalidation of the certificate, particularly if there is suspicion that the private key has been misused, and to request that the certificate be invalidated.
- in the case if the private key will be stored on a qualified device for creating electronic signatures or electronic seals:
  - have to generate and use private key under their exclusive control
  - the private key is used only for creating electronic signatures or seals, and in accordance with applicable law.

6. Basic obligations of relying parties and other users

Relying parties and other users must in particular

- obtain certificates from certification authorities ACAeID QCA and ACAeID RCA from safe sources and verify the prints („fingerprints“) of these certificates,
- before using a certificate issued by ACAeID QCA verify the validity of the certificate of ACAeID QCA, ACAeID RCA and subsequently also the validity of the issued final certificate,
- sufficiently consider particularly based on knowledge of the particular certification policy whether a certificate issued by ACAeID QCA based on the respective policy is suitable for the purpose for which it is planned to be used.

.

7. Limitations on warranty and liability

The eIdentity a.s. agrees to fulfil all obligations imposed by the certification policies, based no which it shall issue certificates, and mandatory provisions of applicable legislation.

The eIdentity a.s. is providing the warranties specified above for the entire duration of the validity of the agreement on provision of certification services entered into with the customer.

The warranties specified above are exclusive warranties of the eIdentity a.s. , and the eIdentity a.s. does not provide any other warranties.

The eIdentity a.s. shall not be liable for defects in provided services resulting from improper or unauthorised use of the services provided during fulfilment of the agreement on provision of certification services by the holder, particularly for operation in a manner that conflicts with the conditions specified in the certification policy, as well as for defects resulting from force majeure circumstances, including temporary outages of telecommunications lines, etc. the eIdentity a.s also shall not be liable for damages stemming from use of a qualified certificate for an electronic signature or certificate for an electronic seal after the request for its invalidation has been submitted, as long as the eIdentity a.s fulfils the defined deadline for publication of the invalidated qualified certificate for electronic signature or the certificate for the electronic seal in the list of invalidated certificates (CRL).

8. Agreements and certification policy

The relationship between the customer and the eIdentity a.s as the provider of certification services is (except for the relevant provisions of mandatory legal regulations) governed by the contract, which includes, among other parts

- the General Commercial Terms for Certification Services,
- valid certification policies and
- currently valid price list.

The relationship between the relying party and the eIdentity a.s as the provider of certification services is governed by relevant provisions of valid certification policies.

The relationship between the eIdentity a.s and relying parties is not governed by the contract.

All of the documents referred to are available on the eIdentity a.s website or at the certification authority's business locations.

9. Personal data protection

The eIdentity a.s agrees to protect the personal data of persons to which it gains access while providing the certification services. The basic principles for personal data protection are outlined in the certification policies, the General Commercial Terms of the certification services and in the current implementing certification directive and are based on relevant provisions of Act No. 110/2019 Coll., the Personal Data Processing, as amended.

The applicant for the certificate hereby grants permission for the eIdentity a.s to process personal data to the extent necessary for issuance and/or invalidation of a certificate with the required data.

10. Compensation and complaint policy

If the services are not delivered in the defined quality (for example, if a certificate is issued with wrong contents), the customer shall be entitled to be refunded the price for the particular service or to be provided with new service free of charge.

More detailed information about complaint handling can be found on the eIdentity a.s website - https://www.eidentity.cz and http://www.ie.cz.

11. Governing law

The activities of eIdentity a.s are governed by relevant provisions of Czech law, particularly

- Act No. 297/2016 Sb. 227/2000 Coll., on trust services for electronic transactions,
- Regulation of the European Parliament and of the Council (EU) No. 910/2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS),
- Act No. 110/2019 Coll., the Personal DataProcessing, as amended.

.

.

12. Accreditation and conformity assessment

The eIdentity a.s as a provider of ACAeID certification services became an accredited provider of certification services based on accreditation issued by the Ministry of Informatics of the Czech Republic.

The information system ACAeID received certification of conformity with ISO 9001 (QMS, Quality Management System) and ISO 27001 (ISMS, Information Security Management System).

The eIdentity a.s became a qualified provider of trust services in accordance with eIDAS for issuing of qualified certificate for electronic signature and electronic seal

The activities of the eIdentity a.s certification authority are subject to performance of checks. Conformity assessment with applicable laws and regulations and technical standards is performed by auditor independent of the eIdentity a.s. The intervals for performance of checks are specified in the certification policies.