

<b>Title:</b>	Zetes Estonia OÜ - Subscriber Terms and Conditions for Certificates issued by Zetes Estonia OÜ for ID-1 format identity documents of the Republic of Estonia
<b>Label:</b>	[ZE TC-ID1-SUB]
<b>Document OID:</b>	[1.3.6.1.4.1.47718.3.14].01
<b>Category:</b>	Subscriber Terms & Conditions
<b>Version:</b>	1.3
<b>Status:</b>	Approved
<b>Effective Date</b>	20/10/2025
<b>Organisation:</b>	Zetes Estonia OÜ
<b>Classification</b>	PUBLIC
<b>Copyright:</b>	<p>© 2025 Zetes Estonia OÜ - All rights reserved.</p> <p>No part of this document or any of its contents may be reproduced, copied, modified or adapted, without the prior written consent of the author, unless otherwise indicated for stand-alone materials.</p> <p>Commercial use and distribution of the contents of this document is not allowed without express and prior written consent of the author.</p>

# Table of Content

- 1 ABOUT YOUR CERTIFICATE AND YOUR ID1 DOCUMENT ..... 3**
  - 1.1 What is my personal “ID1 Document”? ..... 3**
  - 1.2 What are Certificates, a Document Holder, a Subject and a Subscriber? ..... 3**
  - 1.3 What is the relationship between the Document and the Certificates? ..... 3**
  - 1.4 What is the role of Zetes Estonia OÜ? ..... 3**
  - 1.5 About the Subscriber Terms & Conditions..... 4**
  - 1.6 About the PKI Disclosure Statement ..... 4**
- 2 SUBSCRIBER TERMS AND CONDITIONS ..... 5**
  - 2.1 General Terms and Conditions ..... 5**
  - 2.2 Applicable Legislation ..... 5**
    - 2.2.1 Estonian Legislation ..... 5
    - 2.2.2 EU Legislation ..... 6
  - 2.3 Certificate Acceptance ..... 6**
    - 2.3.1 Certificate Acceptance as part of the normal Document Acceptance procedure ..... 6
    - 2.3.2 Certificate Acceptance as part of a special re-key campaign for existing Documents..... 6
    - 2.3.3 Certificate revocation for a new Document ..... 7
  - 2.4 Certificate Revocation ..... 7**
  - 2.5 Certificate Usage ..... 7**
    - 2.5.1 Allowed Key and Certification Usage ..... 7
    - 2.5.2 Forbidden Key and Certificate Usage..... 8
  - 2.6 Subscriber Fees for Certificates ..... 8**
  - 2.7 Refund Policy ..... 8**
  - 2.8 Reliance Limits ..... 8**
  - 2.9 Other Subscriber Rights and Obligations ..... 9**
  - 2.10 Other ZE Rights and Obligations ..... 9**
  - 2.11 Certificate Status Checking Obligations for Subscribers and Relying Parties..... 10**
  - 2.12 Certificate Status Services ..... 10**
  - 2.13 Limited Warranty and Disclaimer ..... 11**
  - 2.14 Force Majeure ..... 11**
  - 2.15 Applicable Law ..... 11**
  - 2.16 Contact information ..... 11**
  - 2.17 Complaints and Dispute Resolution ..... 11**
  - 2.18 Applicable Agreements, Practice Statements, Certification Policies ..... 12**
  - 2.19 Privacy of personal information ..... 12**
    - 2.19.1 Privacy plan..... 12
    - 2.19.2 Information treated as private ..... 13
    - 2.19.3 Information not deemed private ..... 13
    - 2.19.4 Notice and consent to use private information ..... 13
    - 2.19.5 Retention period..... 13
    - 2.19.6 Disclosure pursuant to judicial or administrative process ..... 13
    - 2.19.7 Other information disclosure circumstances ..... 13
- 3 LIST OF DOCUMENTS THAT CONTAIN CERTIFICATES ..... 14**

## Document History

Version	Changes
1.3	No content change compared to 1.2. This version is the first version for production purposes and with an effective date for the public issuance of Certificates. Approved by the PMA and labelled "PUBLIC" for publication.
1.2	For internal use only, no public effect, for pre-production context only. Internal review version. Changes after additional review cycle. Updated the e-mail address for contacts. Mentioned the limit of 1 cert serial number per OCSP request.
1.1	For internal use only, no public effect, for pre-production context only. Internal review version. First review after the audit of 06/2025.. Added chapter 2.19.5 with information about data retention periods.
1.0	For internal use only, no public effect, for pre-production context only. Internal review version. Approved version for initial audit.

# 1 ABOUT YOUR CERTIFICATE AND YOUR ID1 DOCUMENT

## 1.1 What is my personal “Document”?

ID-1 format identity documents (hereinafter referred to as Documents) refer to your personal identity card (e.g. an ID card, a residence permit card, a digital identity card for e-residents or a diplomatic identity card) issued by the Republic of Estonia.

The Document contains a security chip that you can use in computer applications such as most web browsers, DigiDoc, Adobe Reader and others. The chip can be used with a browser to log in to online services like eesti.ee, bank web sites, etc. as well as to encrypt and/or to sign electronic documents. With DigiDoc you can sign and encrypt various file formats.

## 1.2 What are Certificates, a Document Holder, a Subject and a Subscriber?

The Document Holder is the person (you) who has received a Document from the Republic of Estonia.

Certificates are digital expression of identity that link the Document Holder’s unique identity with the cryptographic keys that the chip in the Document uses when authenticating, encrypting or signing on behalf of the Document Holder.

Because Document Holder receives these Certificates on chip in their Document, the Document Holder is deemed to subscribe to the Certificate issuance and lifecycle management services. For this reason, the Document Holder is usually referred to as the Subject and Subscriber in the context of the Certificates whereas the term Document Holder is used in the context of the Documents.

The term **Subject** refers to the person to whom a Certificate is issued and who has the usage rights for the Certificate. The Subject is the natural person whose identity is encoded in the Subject name fields in the Certificate.

The term **Subscriber** refers to the person who subscribes to the Trust Service associated with the Certificate.

A Certificate links the Subject’s identity (name, personal identification code ...) to a unique cryptographic key that was generated in the chip of a Document issued by the Police and Border Guard Board (PBGB) or the Ministry of Foreign Affairs (MFA). Both government agencies play a crucial role in the validation of the Subject’s identity and in the decision to issue a Document, with Certificates, to the Subject. The issuance and lifecycle management of Documents is managed entirely by these government agencies and their contractors.

## 1.3 What is the relationship between the Document and the Certificates?

The lifecycle of Documents and Certificates are closely related.

- A Certificate has the same expiration date as the Document it belongs to.
- If a Document Holder needs a new Document, for whatever reason, new Certificates are generated for the new Document.
- If a Document Holder dies, the Certificates will be revoked to prevent abuse.
- If the identity data of Document Holder changes, the current Certificates will be revoked and the person will receive a new Document with new Certificates that express the person’s new identity data.

## 1.4 What is the role of Zetes Estonia OÜ?

Although the issuance of the Documents is done by the PBGB and by the MFA, your personal Certificates on these Documents are created by a private company Zetes Estonia OÜ (ZE) who has the role of a Qualified Trust Services Provider (QTSP), registered as QTSP by the Information System Authority (RIA) in its role as the Supervisory Body of the Republic of Estonia. It is the QTSP’s responsibility to create the Certificates and manage the lifecycle status of the Certificates (either suspended, active or revoked).

ZE as QTSP operates under the laws of the Republic of Estonia and under the laws of the European Union, most notably the eIDAS Regulation for Trust Service Providers. A list of applicable laws is provided at the end of this document. ZE is contracted by PBGB to issue Certificates for the Documents.

Because the Certificates are made exclusively for use with Documents issued by the Republic of Estonia, the QTSP adheres to the Certificate Policies of PBGB.

ZE as QTSP provides public services that you can use:

- CRL and OCSP to check Certificate status information for your own Certificates and others Certificates,
- a web page to request revocation of Certificates,
- an LDAP directory service to find Certificates of others.

## 1.5 About the Subscriber Terms & Conditions

The document you are reading now constitutes the **Subscriber Terms & Conditions** [ZE TC-ID1-SUB]. It is made available to Subscribers in the context of Certificates issued by ZE for Documents issued by the Republic of Estonia.

## 1.6 About the PKI Disclosure Statement

The Subscriber is encouraged to read the **PKI Disclosure Statement** [ZE PDS-ID1]. It contains a simplified summary of the Certification Practice Statement, which is an elaborate public document that describes in full detail the practices that are applied by the QTSP and other parties for the issuance of the Certificates as part of the issuance of the Documents and also provides more detailed information regarding the rights and obligations of Subscribers and Relying Parties.

## 2 SUBSCRIBER TERMS AND CONDITIONS

The relevant version of this document is the most recent version that is available online at <https://www.id.ee/termsandconditions> at the date you have applied for a Document. A printed version of this document may be available at the service points but is only provided as courtesy for convenience. In no way does the printed courtesy copy supplant, overrule or otherwise negate the version online.

### 2.1 General Terms and Conditions

The Subscriber accepts that ZE must adhere to Estonian legislation, specifically but not limited to what is listed in chapter 2.2.

The Subscriber accepts that the Certificates are an integral part of the Documents issued by the Republic of Estonia and accepts the rules and terms and conditions pertaining to the Document that holds the Certificates.

The Subscriber accepts that any and all aspects relating to the procedures for identity verification, application for a Document containing the Certificates and the issuance of said Document and Certificates are governed by the procedures and processes of the Document issuers, either PBGB or MFA depending on the type of Document.

The Subscriber accepts that the usage of the Certificates is governed by the conditions of use that are specified in the present document and in the Certificate Practice Statement [ZE CPS-ID1-EID-CA] of ZE.

ZE has the right to amend the terms and conditions for ensuring the legality, security, continuity, quality and integrity of the services.

### 2.2 Applicable Legislation

#### 2.2.1 Estonian Legislation

[EST DIPLCARD REG]	Procedure, form, technical specifications and list of data to be entered on the diplomatic identity card and the procedure for registration of non-residents exempt from income tax Published: <a href="https://www.riigiteataja.ee/akt/101022022008?leiaKehtiv">https://www.riigiteataja.ee/akt/101022022008?leiaKehtiv</a>
[EST EIDTSET ACT]	Electronic Identification and Trust Services for Electronic Transactions Act, RT I, 25.10.2016, 1 Published: <a href="https://www.riigiteataja.ee/en/eli/527102016001/consolide/current">https://www.riigiteataja.ee/en/eli/527102016001/consolide/current</a>
[EST EMERGENCY ACT]	Emergency Act, RT I, 03.03.2017, 1. Published: <a href="https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide/current">https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide/current</a>
[EST FEES ACT]	State Fees Act. Published: <a href="https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current">https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current</a>
[EST ID ACT]	Identity Documents Act, RT I 1999, 25, 365 Published: <a href="https://www.riigiteataja.ee/en/eli/ee/521062017003/consolide/current">https://www.riigiteataja.ee/en/eli/ee/521062017003/consolide/current</a>
[EST PDP ACT]	Personal Data Protection Act RT I, 04.01.2019, 11 Published: <a href="https://www.riigiteataja.ee/en/eli/523012019001/consolide">https://www.riigiteataja.ee/en/eli/523012019001/consolide</a>
[EST PROCIDVERIF REG]	Procedure for identification and verification of the identity of the applicant for a Document Published: <a href="https://www.riigiteataja.ee/akt/126082022002?leiaKehtiv">https://www.riigiteataja.ee/akt/126082022002?leiaKehtiv</a>
[EST LISTDOCID ACT]	List of Documents and Data to be Submitted When Applying for the Issuance of an Identity Card, Residence Permit Card, Digital Identity Card, Estonian Citizen's Passport, Seafarer's Service Book, Foreign National Passport, Temporary Travel Document, Refugee Travel Document, or Seafarer's Certificate, the Procedure for Issuance, and the Issuance Deadlines. Published: <a href="https://www.riigiteataja.ee/akt/126082022012?leiaKehtiv">https://www.riigiteataja.ee/akt/126082022012?leiaKehtiv</a>

## 2.2.2 EU Legislation

- [EU 910/2014 EIDAS]** Regulation (EU) 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 – as amended by Regulation (EU) 2024/1183. Published: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018>
- [EU 679/2016 GDPR]** Regulation (EU) 679/2016 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 (General Data Protection Regulation). Published: <http://data.europa.eu/eli/reg/2016/679/oj>
- [EU 1502/2015]** Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of 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. Published: [http://data.europa.eu/eli/reg\\_impl/2015/1502/oj](http://data.europa.eu/eli/reg_impl/2015/1502/oj)

## 2.3 Certificate Acceptance

### 2.3.1 Certificate Acceptance as part of the normal Document Acceptance procedure

The Certificate Acceptance process is an integral part of the Document Acceptance process.

The Subscriber is deemed to have agreed to the creation of the Certificates when the Subscriber has explicitly applied for the Document that will hold the Certificates.

Certificates are created in suspended state and are switched to active state as part of the Document and Certificate Acceptance procedure.

The Subscriber is requested to verify that the names and personal identification code on the Document are correct before accepting the Document and the Certificates.

The Subscriber confirms acceptance and correctness of the Certificates content by signing the acceptance clause on the Document carrier or otherwise expressing acceptance and by taking possession of the Document that holds the Certificates.

### 2.3.2 Certificate Acceptance as part of a special re-key campaign for existing Documents

The Certificate Acceptance process is an integral part of the re-key process. A re-key is an exceptional procedure to replace the keys and Certificates on existing Documents.

Certificates that are issued for existing Documents as part of a re-key campaign, will have the same Subscriber information as the original Certificates and are issued in active state.

The Subscriber is instructed to verify that the names and personal identification code on the Document are correct before initiating the re-key process and accepting the new Certificates.

If the re-key process is done via the web portal of the Card Manufacturer, the Subscriber confirms acceptance and correctness of the Certificate content and acceptance of the Subscriber Terms & Conditions [ZE TC-ID1-SUB] by

- ticking the acceptance box
- inserting their Document in the smart card reader during the re-key process.

If the re-key process is done via a service point, the Subscriber confirms acceptance and correctness of the Certificate content and acceptance of the Subscriber Terms & Conditions [ZE TC-ID1-SUB] by

- signing the application form and

- either inserting their Document in the smart card reader during the re-key process or handing their Document to the operator in the service point.

### 2.3.3 Certificate revocation for a new Document

The Subscriber can request immediate revocation of the Certificates when receiving the Document.

## 2.4 Certificate Revocation

With exception for the digital identity card for e-residents, revocation of the Certificates does not affect the validity of the Document. In the case of a digital identity card for e-residents, revocation of the Certificates also terminates the validity of the Document.

After revocation of the Certificates, the Document cannot be used anymore for online authentication, for encryption nor for signature.

Certificate revocation is irreversible.

The Subscriber accepts that revocation of the Certificates may render decryption of previously encrypted data difficult or impossible.

The Subscriber accepts not to use revoked Certificates for any purpose other than decryption of previously encrypted data.

Certificate revocation does not give right to a refund or any other form of compensation or discount.

The Subscriber can request revocation of the Certificates at any time.

The Subscriber can request revocation

- via the Certificate Revocation Portal at this URL:<https://revocation.eidpki.ee>. The Subscriber must be able to authenticate successfully with one of the following authentication means: the Document, Smart-ID, Mobile-ID or a one-time password. ZE is not responsible for the Subscriber's inability or self-induced failure to authenticate or the Subscriber's inability or unwillingness to use any of the accepted authentication means.
- at the PBGB service point, or in-case of the diplomatic identity card, at the MFA service point.

ZE has a legitimate right to revoke the Subscriber's Certificate if compelled to do so under contractual obligation with PBGB or MFA, on instruction of PBGB or MFA, if compelled to do so by law and specifically by [EU 910/2014 EIDAS] or if compelled to do so according to Certification Practice Statement [ZE CPS-ID1-EID-CA].

The Subscriber accepts that to receive new Certificates after revocation, requires application for a new Document.

The Subscriber will receive a notification via their official Estonian e-mail address (your\_personal\_identification\_code@eesti.ee) when Certificates have been revoked.

Subscriber can have all mails to this address forwarded automatically to another personal e-mail account.

The Subscriber has no rights to refunds, damages or other compensations because of legitimate revocation of the Certificates.

## 2.5 Certificate Usage

### 2.5.1 Allowed Key and Certification Usage

The Subscriber shall use the private key and the Certificates lawfully and in accordance with the Subscriber Terms and Conditions [ZE TC-ID1-SUB].

It is forbidden to use Certificates for any other purpose than the following:

- The Certificate for authentication and encryption is intended for authentication and for encryption.
- The Certificate for signature is intended for the creation of qualified electronic signatures.

When using the signature key to sign documents or transactions, the Subscribers are recommended to use a signature solution that embeds the status of the Certificate in the signature data structure and are recommended to apply a qualified time stamp.

The Subscribers are recommended to use signature functionality of the DigiDoc software.

### 2.5.2 Forbidden Key and Certificate Usage

It is forbidden to use expired Certificates or revoked Certificates for any purpose other than decrypting encrypted data (files, messages, transactions, ...).

It is forbidden to delegate or relinquish control over the use of the Document and its Certificates to another person or to an automated system.

It is forbidden to use the Certificate for signature in an automated way.

It is forbidden to use the Certificate for signature for any other purpose than creating a signature.

It is forbidden to use the Certificate for signing documents which can bring about unwanted consequences or for signing documents for testing purposes.

It is forbidden to use the Certificates for any purpose that is not explicitly allowed, a.o. but not limited to any unlawful activity (including cyber-attacks and attempt to infringe the Certificate(s) or the Document), the issuance of other certificates, etc.

It is forbidden to use the Certificate for authentication and encryption to create an electronic signature.

It is forbidden to use the Certificate for authentication and encryption to encrypt data that is associated with unlawful activities.

### 2.5.3 Obligations to use the Trusted List to validate the Certificate and electronic signature made with the Certificate

The Subscriber must use means that validate that the Certificate is issued by a QTSP that is listed in the trusted list of the Republic of Estonia or in the EU trusted list.

The following URLs are provided purely for convenience and may change without notice:

Trusted List of the Republic of Estonia <https://sr.riik.ee/en/trusted-list/>

Trusted List of the European Union: <https://eid.ec.europa.eu/efda/trust-services/browse/eidas/tls>

## 2.6 Subscriber Fees for Certificates

The fee for the Certificates is included in the fee for the Document, in accordance with the [EST FEES ACT] and for diplomatic identity cards in agreement between the MFA and the PBGB.

## 2.7 Refund Policy

There are no refunds for Certificates from ZE to Subscribers.

Any entitlement to a refund, if any, follows from the Subscriber's rights as enacted in the [EST FEES ACT] and pertains to the refund policy for the Document that contains the Certificates.

Requests for refunds must be directed to the Document issuer, either PBGB or MFA, depending on the type of Document.

## 2.8 Reliance Limits

Certificates have a validity period that is stated in the Certificate itself (not before/not after).

The Certificate validity period is aligned with the validity period of the Document to which the Certificate is associated.

Certificates have a status that can be one of the following: active, suspended or revoked.

The validity period and the Certificate status together determine whether a Certificate should be considered valid.

## 2.9 Other Subscriber Rights and Obligations

The Subscriber is advised to set a self-defined non-obvious PIN code to replace the original PIN code.

The Subscriber has the right to request revocation of the Certificates at any time.

The Subscriber has the right to request revocation of the Certificates without giving a reason provided that the Document and the security codes (PIN and PUK) are still under the control of Subscriber (i.e. not lost, not stolen, not compromised, not damaged, ...).

The Subscriber must protect the Document and the associated security codes against loss, theft, disclosure, or compromise.

The Subscriber must present true and complete information to PBGB or MFA for all aspects and procedures relating to the Document and the Certificates.

The Subscriber must notify PBGB or MFA within one month of any changes pertaining to the Subject's personal details and official status such as but not limited to nationality, residence status, diplomatic status, etc. in accordance with the Estonian legislation.

The Subscriber must notify PBGB or MFA without delay of loss, theft, damage or destruction of the Document and submit a request for revocation of the Certificates.

The Subscriber must notify PBGB or MFA of any suspicion of loss of control or actual loss of control over the Document and its Certificates such as but not limited to compromise of the secrecy of the security codes and submit a request for revocation of the Certificates.

The Subscriber must stop using the Certificates if a direct or public notification is given that the Certificates may not be used anymore.

The Subscriber is recommended to physically destroy the contact chip through perforation or cutting when the Document expires or was replaced by a new one, unless required by law to return the document to PBGB or MFA.

Warning: the destruction of the contact chip will make it impossible to decrypt previously encrypted files.

The Subscriber must not use keys of expired or revoked Certificates for any purpose other than decrypting encrypted data (files, messages, transactions, ...).

The Subscriber is responsible for making sure all their encrypted data is decrypted as soon as possible and before the Document's Certificates expire or are revoked or before the Document is returned to PBGB or MFA or otherwise disposed of.

## 2.10 Other ZE Rights and Obligations

ZE has the right to take any action it is obligated to take under Estonian legislation or EU legislation or under contractual obligation to PBGB.

ZE has the right to terminate the Certificate Status Services when all Certificates have either expired or have been revoked. Eventually the Certificate Status Services will terminate.

ZE has the right to publish the authentication and encryption Certificate in a publicly accessible online repository (LDAP).

ZE has the obligation to provide the following 24/7 services to Subscribers and Relying Parties:

- Certificate Status Service (CRL and OCSP)
- Certificate Repository Service (LDAP)
- Certificate Revocation Portal for Subscribers
- Documentation and CA certificate Repository Service

ZE has the obligation to perform all the duties of a QTSP under Estonian law and EU legislation.

ZE has the obligation to perform all the duties as specified in its contract with PBGB.

## 2.11 Certificate Status Checking Obligations for Subscribers and Relying Parties

*Note: For readability reasons, in this chapter the Subscriber and the Relying Party will be commonly referred to as Relying Party.*

A Relying Party must make sure to be fully aware and informed of its risks and liabilities related to reliance on and acceptance of a Certificate.

The Relying Party must reject any and all reliance on the Certificate if the Certificate was suspended, revoked or expired at the time of using the Certificate.

When a Relying Party uses a Certificates for its intended purpose, the systems and software used must be able to successfully validate the Certificate status using at least one of two Certificate Status Services (called CRL and OCSP) indicated in the Certificate or must be able to validate properly dated and verifiable Certificate status information that is embedded within or associated with the file or transaction.

The Relying Party must validate a Certificate using at least one of the Certificate Status Services.

The Relying Party will trust a Certificate only if it has not been suspended in the relevant period and has not been revoked before the relevant period.

The Relying Party may not rely on a Certificate if the Certificate status cannot be established or cannot be properly related to the date and time at which the Certificate was used.

The Relying Party will rely on Certificates only for the purpose as set forth in the present document, in the [ZE CPS-ID1-EID-CA] and in [PBGB CP-ID1-EID-CA] and in the key usage information encoded in the Certificate itself.

The Relying Party is entirely responsible for determining relevance and interpretation of the date and time with regards to the validation of Certificate status and how this applies to the interpretation of the Certificate status for a specific moment in time.

The Relying Party is entirely responsible for the interpretation of the relevance and consequences of the date and time associated with a signature in conjunction with the Certificate status at the date and time of the creation of the signature and at the date and time of each validation of the signature.

The Relying Party is entirely responsible for the interpretation of the relevance and consequences of the date and time associated with a signature in conjunction with the Certificate expiration date and time versus the date and time of the creation of the signature and at the date and time of each validation of the signature.

## 2.12 Certificate Status Services

Subscribers and Relying Parties can use two standard Certificate Status Services (CRL and OCSP) free of charge.

### CRL

For maximum interoperability with 3rd party software

- the CRL adheres to the RFC 5280 standard
- the Certificate to be checked contains the URI for the CRL
- the CRL is signed by the CA itself
- the QTSP does not use another trusted authority to sign the CRL
- the CRL files can be downloaded via HTTP and HTTPS

The Relying Party is solely responsible for taking into account the periodicity of the CRL for deciding whether this is fit for purpose.

### OCSP

For maximum interoperability with 3rd party software

- the OCSP format adheres to the RFC 6960 standard.
- the Certificate to be checked contains the URI for the OCSP service

- the OCSPs support the use of a nonce in requestExtension
- OCSP requests must include only 1 (one) certificate serial number

Relying Parties who wish to use local caching of OCSP responses for faster processing and for reducing their network traffic cannot use nonces in the OCSP request.

#### **Retention period for Certificate Status Information after expiration for qualified Certificates**

Certificate Status information in the Certificate Status Services shall be updated at least until all Certificates that were issued have either expired or have been revoked.

#### **Termination of the Certificate Status Services**

Subscribers and Relying Parties are advised to use systems and software that includes the Certificate status information at the time of usage within the file or transaction especially if the file or transaction has a long term character and may require validation in the future.

### **2.13 Limited Warranty and Disclaimer**

ZE explicitly declines all liability towards Relying Parties and Subscribers in all cases where

- a Certificate was used improperly,
- a Certificate was used for any purpose other than the Certificate's intended use,
- the validity of the Certificate was not properly checked at the relevant time,
- an authentication Certificate was used in a private setting between private parties, which is beyond authentication that is required under national law or by administrative practice to access a service provided by a public sector body,
- the concepts or principles on which the security and trust were based become moot due to a disruptive scientific or technological development.

The QTSP limits and excludes its liability, including towards Subscribers and all Relying Parties. The exclusions and limitations are iterated amongst other in chapters 9.7 and 9.8 of [ZE CPS-ID1-EID-CA].

### **2.14 Force Majeure**

ZE as the QTSP accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as Acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters. See also chapter 9.8 about excluded liability in [ZE CPS-ID1-EID-CA].

### **2.15 Applicable Law**

ZE activities as QTSP registered in the Republic of Estonia is governed by the jurisdictions of the European Union and of the Republic of Estonia.

### **2.16 Contact information**

ZE can be contacted for topics relating to Certificates for Documents via these channels:

E-mail: info\_eidpki AT ee.zetes.com

Web site: <https://repository.eidpki.ee>

### **2.17 Complaints and Dispute Resolution**

Complaints regarding the Document processes (fees, application process, delivery or handover process, re-key process, etc.) must be addressed to the Document issuers.

Complaints regarding the DigiDoc software must be addressed to the Information System Authority (RIA) at <https://www.ria.ee>.

Complaints regarding the content of the Certificates or the public services provided by ZE such as Certificate Status Services (CRL and OCSP), LDAP Directory Services and the Certificate Revocation Portal must be addressed to ZE. Complaints to ZE must be submitted via e-mail (see chapter 2.17).

All disputes will be resolved according to Estonian legislation.

Any arbitration shall, unless agreed otherwise between the parties, take place in the Republic of Estonia.

## 2.18 Applicable Agreements, Practice Statements, Certification Policies

The documents listed below are published on the following web sites:

- English and Estonian: <https://repository.eidpki.ee>
- English: <https://www.id.ee/en/rubriik/certificates/>
- Estonian: <https://www.id.ee/rubriik/sertifikaadid/>

List of documents:

<b>[ZE CPS-ID1-ROOT-CA]</b>	Zetes Estonia OÜ - Certificate Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia
<b>[ZE CPS-ID1-EID-CA]</b>	Zetes Estonia OÜ - Certificate Practice Statement for the Intermediate CA for ID-1 documents of the Republic of Estonia
<b>[ZE PDS-ID1]</b>	Zetes Estonia OÜ – PKI Disclosure Statement for Subscriber Certificates for ID-1 documents of the Republic of Estonia
<b>[ZE PROFILES]</b>	Zetes Estonia OÜ Technical profile of Certificates, OCSP responses and CRLs
<b>[ZE TSPS-ID1]</b>	Zetes Estonia OÜ - Trust Services Practice Statement for the CA-hierarchy for ID-1 Documents of the Republic of Estonia
<b>[ZE TC-ID1-SUB]</b>	Zetes Estonia OÜ- Terms and Conditions and PKI Disclosure Statement for Subscriber Certificates for ID-1 Documents of the Republic of Estonia.
<b>[ZE TC-ID1]</b>	Zetes Estonia OÜ- Terms and Conditions the OCSP, CRL and LDAP services for Certificates for ID-1 Documents of the Republic of Estonia.
<b>[PBGB CP-ID1-EID-CA]</b>	Police and Border Guard Board – Certificate Policy for the ID-1 format identity documents of the Republic of Estonia, <a href="https://www.id.ee">https://www.id.ee</a>
<b>[PBGB CP-ID1-ROOT-CA]</b>	Police and Border Guard Board – Certificate Policy of for the root Certification Authority of the Republic of Estonia, <a href="https://www.id.ee">https://www.id.ee</a>

## 2.19 Privacy of personal information

### 2.19.1 Privacy plan

The QTSP does not release nor is it required to release any confidential information without an authenticated and justified request.

The QTSP shall:

- where it processes personal data do so in line with the [EU 679/2016 GDPR] and the [EST EIDTSET ACT].
- treat all personal data as confidential, unless the Subscriber determines otherwise;
- take adequate technical and organisational measures ensuring the security of the processing of personal data in line with the [EU 679/2016 GDPR] and the [EST EIDTSET ACT];

The QTSP warrants that:

- the technical and organisational measures offer an appropriate level of protection in proportion to the risks involved against the accidental or unauthorised destruction, loss, alteration or access to personal data or any other form of unauthorised processing of personal data;
- its personnel shall only have access to personal data insofar the access is necessary for performing their duties;
- its personnel charged with the processing of personal data have been duly informed of the applicable obligations under the [EST PDP ACT] and their obligations under this clause.

### 2.19.2 Information treated as private

Personal data encoded in the Certificate is deemed private information whilst being processed by the QTSP, the RAs and their contractors in the RA role and the Card Manufacturer. However, the Certificates are intended for public exposure either as part of a signature data structure, as part of an authentication data structure or by virtue of being published in the public LDAP directory for encryption purposes.

OCSP usage information such as the requester's IP address and date & time of the OCSP request is deemed private information but is retained under Estonian Law for future forensic investigation by authorized law enforcement agencies.

### 2.19.3 Information not deemed private

Certificates published in the LDAP service is not deemed private.

Certificate Status information published via the CRL service and the OCSP service is not deemed private.

### 2.19.4 Notice and consent to use private information

During the Certificate Application process the Subscriber is presented the Subscriber Terms and Conditions [ZE TC-ID1-SUB] as notice and the Subscriber expresses consent regarding the use of their private information, in accordance with the [EST ID ACT] and the [EST EIDTSET ACT]. The Subscriber can request revocation of the Subscriber Certificates at any time.

### 2.19.5 Retention period

ZE retains audit logs and copies of Subscriber Certificates for 5 years from the expiry date of the Certificate.

PBGB and MFA retains information supporting the issuance and life-cycle management of the Subscriber Certificates for a period of at least 10 years after the Certificate ceased to be valid.

The record retention for Certificate related evidences are retained for the required duration as set in [EST EUTS ACT] and the requirements of [EU 910/2014 EIDAS].

PBGB electronic records are retained based on the database regulations which exceed eIDAS requirements and are laid down in the [EST ITDAK REG], [EST ABISDB REG] and [EST ARCHIVES ACT]. Electronic records held by the contractors of the RA are held by the contractors and are then transferred to PBGB.

MFA paper records are archived by the MFA. The record retention for Certificate related evidences are retained for the required duration as set in [EST EUTS ACT] and the requirements of [EU 910/2014 EIDAS].

MFA electronic records are retained based on the database regulations which exceed eIDAS requirements and are laid down in the [EST VEISDB REG]

PBGB ensures that information supporting the issuance and post-issuance update of the Documents and Certificates is retained for a period of at least 10 years after the Certificate ceased to be valid.

### 2.19.6 Disclosure pursuant to judicial or administrative process

Information may be disclosed in the course of a judicial or administrative proceeding.

### 2.19.7 Other information disclosure circumstances

The QTSP is under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order.

### 3 LIST OF DOCUMENTS THAT CONTAIN CERTIFICATES

The following table lists all Documents that contain Certificates and the Certificate Policy [PBGB CP-ID1-EID-CA] that applies for each.

Certificate Policy OID	Issuer	Document Type	Usage
1.3.6.1.4.1.51361.2.1.1 0.4.0.2042.1.2	PBGB	Identity card of Estonian citizens	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.1 0.4.0.194112.1.2	PBGB	Identity card of Estonian citizens	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.2 0.4.0.2042.1.2	PBGB	Identity card of European Union citizens	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.2 0.4.0.194112.1.2	PBGB	Identity card of European Union citizens	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.3 0.4.0.2042.1.2	PBGB	Residence permit card for long-term residents	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.3 0.4.0.194112.1.2	PBGB	Residence permit card for long-term residents	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.4 0.4.0.2042.1.2	PBGB	Residence permit card for temporary residents	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.4 0.4.0.194112.1.2	PBGB	Residence permit card for temporary residents	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.5 0.4.0.2042.1.2	PBGB	Residence permit card for family members of EU and UK citizens	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.5 0.4.0.194112.1.2	PBGB	Residence permit card for family members of EU and UK citizens	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.6 0.4.0.2042.1.2	PBGB	Digital identity card of e-residents	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.6 0.4.0.194112.1.2	PBGB	Digital identity card of e-residents	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51455.2.1.1 0.4.0.2042.1.2	MFA	Diplomatic identity card	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51455.2.1.1 0.4.0.194112.1.2	MFA	Diplomatic identity card	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures

----- Last page of this document -----