Title:	**Technical profile of certificates, OCSP responses and CRLs**
Label:	**[ZE PROFILE]**
Category:	**Certificate Profiles**
Version:	**1.2**
Status:	**Final**
Effective date:	**20/05/2026**
Organisation:	**Zetes Estonia OÜ**
Classification	**PUBLIC**

Table of Contents

1 DOCUMENT HISTORY

Version	Date	Comments
1.0	01/10/2025	First publication
1.1	23/04/2026	Lay-out improvements, Changes to subscriber Givenname and CommonName fields
1.2	20/05/2026	Changes to subscriber valid to description

2 OVERVIEW

This document includes the technical profiles of:

- Root CA certificate
- Intermediate CA certificate
- Subscriber certificates
  - Authentication
  - Qualified electronic signature (QES)
- OCSP responder certificate of the intermediate CA
- OCSP response body
- CRLs

2.1 Terminology

2.1.1 Definitions

Term	Definition
certificate	Public key, together with additional information, laid down in the Certificate Profiles, rendered unforgeable via encipherment using the private key of the Certification Authority which issued the certificate.
certificate owner	The Subscriber to whom the Subscriber certificate has been issued to.
Certificate Profiles	This document, which determines the information contained within a certificate, CRL and OCSP response.
Certificate Revocation List	A list of invalid intermediate certificates or Subscriber certificates during their validity period, i.e. until they expire.
Certification Authority	A service provider who provides certification services including all the procedures related to the lifecycle of the keys, certificates and related services. In the context of Certificate Profiles, the service provider is Zetes Estonia OÜ.
CRL service	A service for publishing Certificate Revocation Lists.
intermediate CA/certificate	Certification Authority whose certificate is issued by the root CA. Intermediate CA issues the Subscriber certificates.
OCSP responder service	A certificate status service on the basis of OCSP.
private key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic messages, records or files that were encrypted with the corresponding public key.

public key	The key of a key pair that may be publicly disclosed by the holder of the corresponding private key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding private key and/or to encrypt messages, records and files so that they can be decrypted only with the holder's corresponding private key.
root CA/certificate	Highest level Certification Authority, which is identified by the root certificate. The root CA issues certificate for the intermediate CA.
Subscriber	A natural person to whom the Subscriber certificates are issued to as a public service, provided that the person has a statutory right to them and has requested them.
Subscriber certificates	A uniform term for a certificate that enables digital authentication and a certificate that enables creation of qualified electronic signatures.

2.1.2 Abbreviations

Term	Definition
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
eIDAS Regulation	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.
eID CP	Certificate Policy of ID-1 format identity documents of the Republic of Estonia
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
QSCD	Qualified Signature Creation Device
root CP	Certificate Policy of the root Certification Authority of the Republic of Estonia
UTF-8	Unicode Transformation Format-8

3 TECHNICAL PROFILE OF THE CERTIFICATES

3.1 Technical profile of the root certificate

3.1.1 The root certificate shall be compliant with clause 7.1 of root CP [9].

3.1.2 Root certificate body

Field	OID	Mandatory	Value	Description
Version	*Not applicable*	yes	V3	X.509 version 3 shall be used.
Serial Number	*Not applicable*	yes	[serial number]	Shall be unique and random.
Signature Algorithm	1.2.840.10045.4.3.3	yes	ECDSA-SHA-384	NIST P-384 (secp384r1)
Issuer DN				
Common Name (CN)	2.5.4.3	yes	Production Environment: EEGovCA2025 Test Services: Test EEGovCA2025	• Format of the value: EEGovCAYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one root CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. EEGovCA2025_02).
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	
Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].
Valid from	*Not applicable*	yes	Date and time of certificate issuance	UTC time shall be used.

Valid to	*Not applicable*	yes	Date of certificate issuance + 15y	UTC time shall be used.
Subject DN				Shall have the same values as the Issuer DN.
Common Name (CN)	2.5.4.3	yes	Production Environment: EEGovCA2025 Test Services: Test EEGovCA2025	• Format of the value: EEGovCAYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one root CA issued in a single year an enumeration (suffix) in the form of '_XX'will be added (e.g. EEGovCA2025_02).
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	
Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].
Subject Public Key	*Not applicable*	yes	ECDSA_P384	NIST P-384 (secp384r1)
Signature	*Not applicable*	yes	[signature value]	Shall include the signature of the root CA.

3.1.3 Root certificate extensions

Extension	OID	Mandatory	Value	Criticality
Basic Constraints	2.5.29.19	yes	Subject Type=CA Path Length Constraint=1	Critical
Key Usage	2.5.29.15	yes	Certificate signing CRL signing Off-line CRL Signing	Critical

Certificate Policies	2.5.29.32	yes	Production Environment: https://repository.eidpki.ee Test Services: https://repository-test.eidpki.ee policy OID's Anypolicy: 2.5.29.32.0	Non-critical
Authority Key Identifier	2.5.29.35	yes	SHA-1 hash of the public key	Non-critical
Subject Key Identifier	2.5.29.14	yes	SHA-1 hash of the public key	Non-critical

3.2 Technical profile of the intermediate certificate

3.2.1 The intermediate certificate shall be compliant with clause 7.1 of root CP [9].

3.2.2 Intermediate certificate body

Field	OID	Mandatory	Value	Description
Version	*Not applicable*	yes	V3	X.509 version 3 shall be used.
Serial Number	*Not applicable*	yes	[serial number]	Shall be unique and random.
Signature Algorithm	1.2.840.10045.4.3.3	yes	ECDSA-SHA-384	NIST P-384 (secp384r1)
Issuer DN				

Common Name (CN)	2.5.4.3	yes	Production Environment: EEGovCA2025 Test Services: Test EEGovCA2025	• Format of the value: EEGovCAYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one root CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. EEGovCA2025_02).
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	
Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].
Valid from	*Not applicable*	yes	Date and time of certificate issuance	UTC time shall be used.
Valid to	*Not applicable*	yes	Date of certificate issuance + 15y	• UTC time shall be used. • Validity may be few days less than for the root certificate.
Subject DN				
Common Name (CN)	2.5.4.3	yes	Production Environment: ESTEID2025 Test Services: Test ESTEID2025	• Format of the value: ESTEIDYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. ESTEID2025_02).
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	
Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].

Subject Public Key	*Not applicable*	yes	ECDSA_P384	NIST P-384 (secp384r1)
Signature	*Not applicable*	yes	[signature value]	Shall include the signature of the root CA.

3.2.3 Intermediate certificate extensions

Extension	OID	Mandatory	Value	Criticality	Description
Basic Constraints	2.5.29.19	yes	Subject Type=CA Path Length Constraint=0	Critical	
Key Usage	2.5.29.15	yes	Certificate signing CRL signing Off-line CRL Signing	Critical	
Certificate Policies	2.5.29.32	yes	Production Environment: https://repository.eidpki.ee Test Services: https://repository-test.eidpki.ee policy OID's Anypolicy 2.5.29.32.0	Non-critical	
CRL Distribution Points	2.5.29.31	yes	Production Environment: http://crl.eidpki.ee/EEGovCA2025.crl Test Services: http://crl-test.eidpki.ee/testEEGovCA2025.crl	Non-critical	• Format of the value: EEGovCAYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. EEGovCA2025_02).
Authority Key Identifier	2.5.29.35	yes	SHA-1 hash of the public key	Non-critical	
Subject Key Identifier	2.5.29.14	yes	SHA-1 hash of the public key	Non-critical	

Authority Information Access	1.3.6.1.5.5.7.1.1	yes	[calssuers]	Non-critical	
calssuers	1.3.6.1.5.5.7.48.2	yes	Production Environment: http://crt.eidpki.ee/EEGovCA2025.crt Test Services: http://crt-test.eidpki.ee/testEEGovCA2025.crt	Non-critical	• Format of the value: EEGovCAYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. EEGovCA2025_02).

3.3 Technical profile of the Subscriber certificates

3.3.1 The Subscriber certificates shall be compliant with clause 7.1 of eID CP [10].

3.3.2 Subscriber certificate body

Field	OID	Mandatory	Value	Description
Version	*Not applicable*	yes	V3	X.509 version 3 shall be used.
Serial Number	*Not applicable*	yes	[serial number]	Shall be unique and random.
Signature Algorithm	1.2.840.10045.4.3.3	yes	ECDSA-SHA-384	NIST P-384 (secp384r1)
Issuer DN				
Common Name (CN)	2.5.4.3	yes	Production Environment: ESTEID2025	• Format of the value: ESTEIDYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. ESTEID2025_02).

			Test Services: Test ESTEID2025	
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	
Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].
Valid from	*Not applicable*	yes	Date and time of certificate issuance	UTC time shall be used.
Valid to	*Not applicable*	yes	Expiration date of the Document + time	• UTC time shall be used. • The 'Valid to' date of a Subscriber certificate shall be equal to the expiration date of the corresponding Document for which the certificate is issued, for certificates expiring during summer time the expiry time will be set to 20:59:59 UTC, for certificates expiring during winter time the expiry time will be set to 21:59:59 UTC.
Subject DN				
Serial Number	2.5.4.5	yes	PNOEE-[personal identification code]	• Refer to clause 5.1.3 of ETSI EN 319 412-1 [1]. • Refer to clause 3.1.1 and 4.1.2 of the eID CP [10]. • Example*: PNOEE-38001085718*
Given Name (G)	2.5.4.42	no	[given name(s)]	• UTF-8 encoding shall be used. • Length of the given name is set in IDA [3]. Given Name length may not meet the requirements of IETF RFC 5280 [4]. • Refer to clause 3.1.1 and 4.1.2 of the eID CP [10]. • Example*: JAAK-KRISTJAN*
Surname (SN)	2.5.4.4	yes	[surname(s)]	• UTF-8 encoding shall be used. • Length of the surname is set in IDA [3] and IETF RFC 5280 [4]. • Refer to clause 3.1.1 and 4.1.2 of the eID CP [10]. • Example*: JÕEORG*

Common Name (CN)	2.5.4.3	yes	If Given Name is present: [surname(s)],[given name(s)],[personal identification code] If Given Name is not present: [surname(s)],[personal identification code]	• Shall be comma-separated list of ○ Surname(s) ○ Givenname(s) (if present) ○ Personal identification code • CN length may not meet the requirements of IETF RFC 5280 [4]. • Refer to clause 3.1.1 and 4.1.2 of the eID CP [10]. • Examples: ○ *JÕEORG,JAAK-KRISTJAN,38001085718* ○ *JÕEORG,38001085718*
Country (C)	2.5.4.6	yes	EE	• Alpha-2 country code according to ISO 3166 [2]. • Refer to clause 3.1.1 of the eID CP [10].
Subject Public Key	*Not applicable*	yes	ECDSA_P384	NIST P-384 (secp384r1)
Signature	*Not applicable*	yes	[signature value]	Shall include the signature of the intermediate CA.

3.3.3 Subscriber certificate Extensions

Extension	OID	Mandatory	Value	Criticality	Description
Basic Constraints	2.5.29.19	yes	Subject Type=End Entity Path Length Constraint=None	Non-critical	
Certificate Policies	2.5.29.32	yes	Production Environment: https://repository.eidpki.ee Test Services: https://repository-test.eidpki.ee policy OID's: Different value for the different, certificate types, refer to clause 2.3.5	Non-critical	

Subject Alternative Name	2.5.29.17	yes	Email address of the certificate owner (rfc822Name according to IETF RFC 5280 [4]).	Non-critical	Shall be present only in the Subscriber certificate for authentication.
Key Usage	2.5.29.15	yes	Refer to clause 2.3.4	Critical	
Extended Key Usage	2.5.29.37	yes	Refer to clause 2.3.4	Non-critical	
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	yes	Refer to clause 2.3.4	Non-critical	
Authority Key Identifier	2.5.29.35	yes	SHA-1 hash of the public key	Non-critical	
Subject Key Identifier	2.5.29.14	yes	SHA-1 hash of the public key	Non-critical	
cRLDistributionPoints	2.5.29.31	yes	Production Environment: http://crl.eidpki.ee/ESTEID2025.crl Test Services: http://crl-test.eidpki.ee/testESTEID2025.crl	Non-critical	• Format of the value: ESTEIDYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year the enumeration (suffix) in the form of '_XX' will be added (e.g. ESTEID2025_02).
Authority Information Access	1.3.6.1.5.5.7.1.1	yes	[ocsp,caIssuers]	Non-critical	
ocsp	1.3.6.1.5.5.7.48.1	yes	Production Environment: http://ocsp.eidpki.ee Test Services: http://ocsp-test.eidpki.ee	*Not applicable*	
caIssuers	1.3.6.1.5.5.7.48.2	yes	Production Environment: http://crt.eidpki.ee/ESTEID2025.crt Test Services: http://crt-test.eidpki.ee/testESTEID2025.crt	*Not applicable*	

3.3.4 Extensions of specific Subscriber certificate

Extension	Subscriber certificate for authentication (AUTH)	Subscriber certificate for QES (SIGN)
Key Usage	Digital Signature Key Agreement	Non-Repudiation
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	*Not applicable*
Qualified Certificate Statement		
id-etsi-qcs-QcCompliance	*Not applicable*	• Shall include a QCStatement claiming that the certificate is a EU qualified certificate. • Refer to clause 4.2.1 of ETSI EN 319 412-5 [5].
id-etsi-qcsQcSSCD	*Not applicable*	• Shall include a QCStatement claiming the private key related to the certified public key resides in a QSCD. • Refer to clause 4.2.2 of ETSI EN 319 412-5 [5].
id-etsi-qcsQcType	*Not applicable*	• Shall include a QcType 1 for certificate for electronic signatures as defined in Regulation (EU) No 910/2014 [6]. • Shall be used according to clause 4.2.3 of ETSI EN 319 412-5 [5].
id-etsi-qcsQcPDS	Production Environment: https://repository.eidpki.ee Test Services: https://repository-test.eidpki.ee	Production Environment: https://repository.eidpki.ee Test Services: https://repository-test.eidpki.ee

3.3.5 Policy OID's for Subscriber certificate

Type	Policy OID's
AUTH Identity card of Estonian citizens	1.3.6.1.4.1.51361.2.1.1 * 0.4.0.2042.1.2
SIGN Identity card of Estonian citizens	1.3.6.1.4.1.51361.2.1.1 * 0.4.0.194112.1.2
AUTH Identity card of European union citizens	1.3.6.1.4.1.51361.2.1.2 * 0.4.0.2042.1.2
SIGN Identity card of European union citizens	1.3.6.1.4.1.51361.2.1.2 * 0.4.0.194112.1.2
AUTH Residence permit card for long-term residents	1.3.6.1.4.1.51361.2.1.3 * 0.4.0.2042.1.2
SIGN Residence permit card for long-term residents	1.3.6.1.4.1.51361.2.1.3 * 0.4.0.194112.1.2
AUTH Residence permit card for temporary residents and the right of stay in the Republic of Estonia	1.3.6.1.4.1.51361.2.1.4 * 0.4.0.2042.1.2
SIGN Residence permit card for temporary residents and the right of stay in the Republic of Estonia	1.3.6.1.4.1.51361.2.1.4 * 0.4.0.194112.1.2
AUTH Residence permit card for family members of EU and UK citizens and the right of residence of UK citizens	1.3.6.1.4.1.51361.2.1.5 * 0.4.0.2042.1.2
SIGN Residence permit card for family members of EU and UK citizens and the right of residence of UK citizens	1.3.6.1.4.1.51361.2.1.5 * 0.4.0.194112.1.2

AUTH Digital identity card of e-residents	1.3.6.1.4.1.51361.2.1.6 * 0.4.0.2042.1.2
SIGN Digital identity card of e-residents	1.3.6.1.4.1.51361.2.1.6 * 0.4.0.194112.1.2
AUTH Diplomatic identity card	1.3.6.1.4.1.51455.2.1.1 * 0.4.0.2042.1.2
SIGN Diplomatic identity card	1.3.6.1.4.1.51455.2.1.1 * 0.4.0.194112.1.2

* According to the general practice, the propriotary OIDs for UAT and test certificates will be prefixed with "2.999." to differentiate them from the production OID's. The ETSI OIDs will not be prefixed.
eg. "AUTH Identity card of Estonian citizens" in UAT/Test will have the following OIDs:

- *2.999.1.3.6.1.4.1.51361.2.1.1*
- *0.4.0.2042.1.2*

3.4 Technical profile of the OCSP responder certificate issued by the intermediate CA

3.4.1 OCSP responder certificate extensions

Extension	OID	Values and limitations	Criticality	Mandatory
Key Usage	2.5.29.15	Digital signature	Critical	yes
Extended Key Usage	2.5.29.37	OCSP Signing	Critical	yes
ocspNoCheck	1.3.6.1.5.5.7.48.1.5	null	Non-critical	yes

4 CRL PROFILES

4.1 CRL profile of the root CA

4.1.1 The CRL shall be compliant with clause 7.2 of root CP [9].

4.1.2 CRL body

Field	OID	Mandatory	Value	Description
Version	*Not applicable*	yes	V2	X.509 version 2 shall be used.
Signature Algorithm	*Not applicable*	yes	ECDSA-SHA-384	NIST P-384 (secp384r1)
Issuer DN				
Common Name (CN)	2.5.4.3	yes	Production Environment EEGovCA2025 Test Services Test EEGovCA2025	• Format of the value: EEGovCAYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one root CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. EEGovCA2025_02).
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	
Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].
This Update	*Not applicable*	yes	[date and time]	UTC time shall be used.
Next Update	*Not applicable*	yes	[date and time]	• UTC time shall be used. • Refer to clause 4.9.7 of the Root CP [9].
Revoked Certificates				Shall include a list of revoked certificates.

Serial Number	*Not applicable*	yes	[serial number]	Shall include a serial number of the revoked certificates.
Revocation Date	*Not applicable*	yes	[date and time]	UTC time shall be used.
Reason Code	2.5.29.21	yes	[CRL reason code]	Shall include the reason code of the certificate revocation.
Signature	*Not applicable*	yes	[signature value]	Shall include the signature of the root CA.

4.1.3 CRL Extensions

Extension	OID	Value	Criticality	Mandatory
CRL Number	2.5.29.20	CRL sequence number shall increase in succession.	non-critical	yes
Authority Key Identifier	2.5.29.35	Shall match the field *Subject Key Identifier* of the root certificate.	non-critical	yes

4.2 CRL profile of the intermediate CA

4.2.1 The CRL shall be compliant with clause 7.2 of eID CP [10].

4.2.2 CRL body

Field	OID	Mandatory	Value	Description
Version	*Not applicable*	yes	V2	X.509 version 2 shall be used.
Signature Algorithm	*Not applicable*	yes	ECDSA-SHA-384	NIST P-384 (secp384r1)
Issuer DN				
Common Name (CN)	2.5.4.3	yes	Production Environment: ESTEID2025 Test Services: Test ESTEID2025	• Format of the value: ESTEIDYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. ESTEID2025_02).
Organisation Identifier	2.5.4.97	yes	NTREE-17066049	

Organisation (O)	2.5.4.10	yes	Zetes Estonia OÜ	
Country (C)	2.5.4.6	yes	EE	Alpha-2 country code according to ISO 3166 [2].
This Update	*Not applicable*	yes	[date and time]	UTC time shall be used.
Next Update	*Not applicable*	yes	[date and time]	• UTC time shall be used. • Refer to clause 4.9.7 of the eID CP [10]. • The field value shall be defined according to clause 6.3.9 (requirement CSS6.3.9-06) of ETSI EN 319 411-1 [7].
Revoked Certificates				Shall include a list of suspended and revoked certificates.
Serial Number	*Not applicable*	yes	[serial number]	Shall include a serial number of the invalid certificates.
Revocation Date	*Not applicable*	yes	[date and time]	• UTC time shall be used. • Shall include the date and time when the invalidation of the certificate was processed.
Reason Code	2.5.29.21	yes	[CRL reason code]	Shall include the reason code of the certificate invalidation.
Signature	*Not applicable*	yes	[signature value]	Shall include the signature of the intermediate CA.

4.2.3 CRL Extensions

Extension	OID	Values and limitations	Criticality	Mandatory
CRL Number	2.5.29.20	CRL sequence number shall increase in succession.	non-critical	yes
Authority Key Identifier	2.5.29.35	Shall match the field *Subject Key Identifier* of the intermediate certificate.	non-critical	yes

5 OCSP RESPONSE PROFILES

5.1 OCSP response profile of the intermediate CA

5.1.1 The OCSP response profile shall be compliant with clause 7.3 of the eID CP [10].

5.1.2 OCSP response body

Field	Mandatory	Values	Description
Response Status	yes	0 for successful or error code	OCSP response status 0 shall be applicable for successful response or error code.
Response Bytes	no	[response bytes]	Shall be dependent on the Response Status.
Response Type	yes	id-pkix-ocsp-basic	Type of the response.
Basic OCSP Response			
tbs Response Data			
Version	yes	1	
Responder ID	yes	Production Environment: CN= ESTEID2025 OCSP Responder 2.5.4.97= NTREE-17066049 O= Zetes Estonia OÜ C= EE Test Environment: CN= Test ESTEID2025 OCSP Responder 2.5.4.97= NTREE-17066049 O= Zetes Estonia OÜ C= EE	• Shall include Subject DN of the OCSP responder certificate. • Format of the CN value: ESTEIDYYYY where YYYY shall be the year of issuance of the CA. • In case there is more than one intermediate CA issued in a single year an enumeration (suffix) in the form of '_XX' will be added (e.g. ESTEID2025_02).
Produced at	yes	[date and time]	GeneralizedTime shall be used.
Responses			
Cert ID	yes	[ASN.1 CertID structure]	Hash Algorithm: sha256 Issuer Name Hash: Hash of issuer's DN Issuer Key Hash: Hash of issuer's public key

			Serial Number: CertificateSerialNumber of the certificate for which the status is being requested
Cert Status	yes	[CertStatus]	The following certificate statuses are allowed: • good – certificate is issued and has not been revoked or suspended; • revoked – certificate is revoked, suspended or not issued by the intermediate CA; • unknown – the issuer of certificate is unrecognised by the OCSP responder service.
Revocation Time	no	[date and time]	GeneralizedTime shall be used.
Revocation Reason	no	[RevocationReason]	Code for revocation reason shall be in accordance with IETF RFC 6960 [8].
This Update	yes	[date and time]	• GeneralizedTime shall be used. • Shall match the date and time of the field *Produced at*.
Archive *Cutoff*	no	[date and time]	Shall match the date and time of the field *Valid from* of the intermediate certificate.
Extended Revoked Definition	no	NULL	
Nonce	no	[Octet String]	Value shall be copied from OCSP request, if included.
Signature Algorithm	yes	ECDSA-SHA-256	
Signature	yes		Shall include the signature of the OCSP responder.
Certificate	yes		OCSP certificate corresponding to the private key used to sign the OCSP response.

REFERENCES

[1] ETSI EN 319 412-1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. Published: https://www.etsi.org;

[2] ISO 3166 – Codes for the representation of names of countries and their subdivisions;

[3] IDA – Identity Documents Act, RT I 1999, 25, 365. Published: https://www.riigiteataja.ee/en/eli/ee/521062017003/consolide/current;

[4] IETF RFC 5280 – Request for Comments 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Published: https://www.ietf.org/rfc/rfc5280.txt;

[5] ETSI EN 319 412-5 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. Published: https://www.etsi.org/;

[6] 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.transactions in the internal market and repealing Directive 1999/93/EC. Published https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

[7] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. Published: https://www.etsi.org/;

[8] IETF RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP https://www.ietf.org/rfc/rfc6960.txt;

[9] Root CP – Certificate Policy of the root Certification Authority of the Republic of Estonia. Published: www.id.ee;

[10] eID CP – Certificate Policy of ID-1 format identity documents of the Republic of Estonia. Published: www.id.ee.