DESCRIPTION of Trust and electronic identification service provider issued certificate profiles

ANNEX: 1. Usage of keys and extended usage of keys
2. Issued certificate profiles

Public

References:

1. Trust service provision regulations
2. [eIDAS Regulation] Regulation (EU) No.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.
3. [RFC 5280] IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.
4. [RFC 3739] IETF RFC 3739 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
5. [RFC 3161] IETF RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
6. [RFC 6960] IETF RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
7. [ETSI EN 319 412-1] European Standard EN 319 412-1 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures”.
8. [ETSI EN 319 412-2] European Standard EN 319 412-2 “Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons”
9. [ETSI EN 319 412-3] European Standard EN 319 412-3 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons”
10. [ETSI EN 319 412-5] European Standard EN 319 412-5 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements”
11. [ETSI EN 319 422] European Standard EN 319 422 “Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles”
12. [ETSI TS 119 312] Technical specification TS 119 312 V1.1.1 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”

13. [ITU-T X.509] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"
14. [ITU-T X.520] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".
15. [ISO 3166] Codes for the representation of names of countries and their subdivisions

HISTORY OF CHANGES:

Revised variant No.	**Date of entry into force**	**Summary of changes**
01.0	01.07.2017.	Initial version
01.1	01.07.2017	Annex 2 added
02.0	01.08.2017	Added “eParaksts” service related certificate profiles and OCSP responder certificate profile. Added paragraph 5.3.2.10.
03.0	01.05.2018	The document is linked to the Law on Electronic Identification of Physical Persons. Changes have been made to the definitions and the title of the document.
04.0	01.09.2019	Updated CRL profile, Updated Annex 1 table with new key functionality (encryption), added Annex 2 and Annex 3 with descriptions of new eID card certificates.

CONTENT

1. Porpose of the document

1.1. *Description of Trust and electronic identification service provider issued certificate profiles are designed for the purpose to inform Subscribers of the Service provider regarding issued certificate profiles, meaning of certificate fields and minimal requirements.*

1.2. *Description of Trust and electronic identification service provider issued certificate profiles are binding on Subscribers and Relying parties.*

1.3. *Description of Trust and electronic identification service provider issued certificate profiles is prepared in Latvian language. This document May be translated and available in other languages. In case of document translation inconsistences, document version in Latvian language prevails.*

2. Definitions and abbreviations

CA	Certificate Authority
CRL	Certificate revocation list
eIDAS	Regulation (EU) No.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.
ETSI	European Telecommunications Standards Institute
Laws and regulations effective in the Republic of Latvia	Include all laws and regulations effective in the Republic of Latvia. Reference to the laws and regulations effective in the Republic of Latvia shall include also international agreements and legal acts of the European Union binding to the Republic of Latvia. If the relevant law issue is governed by the legal acts of the European Union, which are directly applicable in Latvia, the Latvian law shall be applied to the extent the legal acts of the European Union permit for that.
LVRTC	State Joint Stock Company "Latvia State Radio and Television Centre" registration Nr. 40003011203, Address - Ērgļu iela 7, Rīga, Latvija, LV-1012
OCSP	Online Certificate Status Protocol
PDS	PKI disclosure statement
Relying party	A natural or legal person, who relies on the electronic identification or trust service
Service provider	LVRTC, acting as Trust and electronic identification service provider
SSL	Secure Sockets Layer
Subscriber	A natural or legal person who has concluded an agreement

	with Service provider on one or more trust and electronic identification service or other Service provider provided service or to which Service provider services are provided on the basis of regulatory enactments, without concluding an agreement with the Subscriber. Includes certificate holders (Subjects) – Signatories, Creators of seals, Time stamp requestors, users of authentication certificate.
TSP	Trust service provider

3. Introduction

3.1. LVRTC operate as a Trust and electronic identification service provider. Trust and electronic identification services provided by the Service provider are related to different types of certificates.

3.2. Certificate profiles issued by Service provider are defined in Annex 2.

4. Types of certificates related to this document

4.1. Certificates related to a natural person

4.1.1. authentication;

4.1.2. signature;

4.2. Certificates related to a legal person

4.2.1. electronic stamp;

4.2.2. authentication;

4.2.3. Service provider’s time stamping;

4.2.4. Service provider’s Online Certificate Status Protocol (hereinafter - OCSP)

4.3. Service provider published CRL profiles.

5. Certificate data

5.1. Data on the certificate issuer

Field - “Issuer”			
Name of the value	Abbreviation	Explanation/ content	CA type
Common Name	CN	eParaksts Root CA	Root CA
		LV eID ICA 2017	Issuing CA
		eParaksts ICA 2017	Issuing CA
Organization	O	VAS *Latvijas Valsts radio un televīzijas centrs*	All CA
Country	C	LV	All CA
Organization Identifier	2.5.4.97	NTRLV-40003011203	All CA

5.2. Data on the certificate holder

5.2.1. **For a natural person**

Field - “Subject”				
Value	Abbreviation	OID	Explanation	Condition
Common Name	CN	2.5.4.3	Name and Surname combination	Mandatory
Given Name	G	2.5.4.42	Name of a natural person	Mandatory
surName	SN	2.5.4.4	Surname of a natural person	Mandatory
Organizational Unit	OU	2.5.4.11	Structural Unit	Optional
Organization	O	2.5.4.10	Organization	Optional
Country	C	2.5.4.6	Country code in accordance with [ISO 3166]	Mandatory
e-mail	E	1.2.840.113549.1.9.1	e-mail address	Optional
Serial Number	SERIALNUMBER	2.5.4.5	See Paragraph 5.2.1.1	Mandatory
Locality	L	2.5.4.7	City	Optional
State	S	2.5.4.8	Region	Optional

5.2.1.1. id-etsi-qcs-SemanticsId-Natural semantics shall be used for Identity number in the certificate of a natural person, in accordance with the requirements defined by Paragraph 5.1.3 of the standard [ETSI EN 319 412-1]

5.2.2. **For a legal person**

Field - “Subject”				
Name of the value	Abbreviation	OID	Explanation	Condition
Common Name	CN	2.5.4.3	See Paragraph 5.2.2.1	Mandatory
Organizational Unit	OU	2.5.4.11	Organizational Unit	Optional
Organization	O	2.5.4.10	Name of the organization	Mandatory
Country	C	2.5.4.6	Country code of the organization in accordance with [ISO 3166]	Mandatory
e-mail	E	1.2.840.113549.1.9.1	e-mail address	Optional
Organization Identifier		2.5.4.97	See Paragraph 5.2.2.2	Mandatory
Locality	L	2.5.4.7	City	Optional
State	S	2.5.4.8	Region	Optional

5.2.2.1. Content of the certificate name field depends from the type of certificate:

5.2.2.1.1. Electronic stamp certificates - the field shall contain a value, which the certificate Subscriber is using in order to represent him. Value may not be equal with the value of the field “Organization”;

5.2.2.1.2. OCSP certificate - OCSP service identifier, according to which it is possible to clearly identify the Issuing authority, regarding the certificates issued by which the particular OCSP service shall be responsible;

5.2.2.1.3. Time stamping certificate - Time stamping service identifier, according to which it is possible to clearly identify the time stamping authority issuing the time stamp.

5.2.2.2. id-etsi-qcs-SemanticsId-Legal semantics shall be used for Organization identifier in the certificate of a legal person, in accordance with the requirements defined by Paragraph 5.1.4 of the standard [ETSI EN 319 412-1].

5.3. Data included in other certificates

5.3.1. Service provider issued certificate profiles shall contain the following fields of X.509 version 1

5.3.1.1. Version

X.509 V1 field	**Mandatory**	**Content**

X.509 V1 field	Mandatory	Content
Version	Yes	*V3*

5.3.1.2. Serial number

X.509 V1 field	Mandatory	Content
Serial Number	Yes	Unique certificate number, which is automatically granted by the certifying authority (CA)

5.3.1.3. Signature and control sum algorithm

X.509 V1 fields	Mandatory	Content
Signature Algorithm	Yes	SHA256RSA, SHA384RSA or SHA512RSA
Signature Hash Algorithm	Yes	*SHA256, SHA384 or SHA512*

5.3.1.4. Period of Validity of the Certificate

X.509 V1 fields	Mandatory	Content
Valid from	Yes	Date and time of the issue of certificate
Valid to	Yes	Date and time of the period of validity of certificate

5.3.1.5. Public key

X.509 V1 field	Mandatory	Content
Public Key	Yes	RSA (2048) or RSA (4096), Additional field contains public key.

5.3.2. Service provider issued certificate profiles may contain the following extensions:

5.3.2.1. Certificate Holder and Certifying Authority (CA) key identifiers

X.509 V3 extensions	Crucial	Content
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier

5.3.2.2. Certificate policies

X.509 V3 extension	Crucial	Content
Certificate Policies	No	*The field shall contain OID value of the particular policy*
		May contain "*Notice Text*"
		Contains URI http://www.eparaksts.lv/repository

		where the policy and regulations of the particular product is placed

5.3.2.3. Publishing sites of the list of cancelled certificates

X.509 V3 extension	Crucial	Content
CRL Distribution Points	No	*Contains the site, where a list of cancelled certificates is available*

5.3.2.4. Online Certificate verification service site

X.509 V3 extension	Crucial	Content
Authority Info Access	No	*Contains:* *1. Site address, where CA certificate is published;* *2. Site, where OCSP service is available;* *3. Other (if used) sites related to publication of certificates*

5.3.2.5. Enhanced key usage

X.509 V3 extensions	Crucial	Content
Enhanced Key Usage	No	Contains key usage extensions appropriate for the use of certificate **(see Annex 1)**

5.3.2.6. Qualified certificate statement

X.509 V3 extensions	Crucial	Contents
Qualified Certificate Statement	No	*Field content for subscribers certificates is created in accordance with the requirements defined in the standard [ETSI EN 319 412-5]* *Field content for Time stamping certificate is created in accordance with the requirements defined in the standard [ETSI EN 319 422]*

5.3.2.7. Key usage purpose

X.509 V3 extensions	Crucial	Content
Key Usage	Yes	Contains key usages appropriate for the use of certificate **(see Annex 1)**

5.3.2.8. Certificate holder alternative names

X.509 V3 extensions	Crucial	Content

Subject Alternative Name	No	Authentication certificates may contain e-mail address of the holder.

5.3.2.9. Basic constraints for Subscribers certificates

Unless otherwise specified in the certificate profile.

X.509 V3 extensions	**Crucial**	**Content**
Basic Constraints	Yes	*Subject Type=End Entity* *Path Length Constraint=None*

5.3.2.10. OCSP responder additional extension

X.509 V3 extensions	**Crucial**	**Content**
OCSP No Revocation Checking	No	*05 00 (Windows OS)*

5.3.3. Certificate profiles issued by Service provider contain the following details:

Properties	**Content**
Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

6. CRL profile

6.1. CRL profile issued by Service provider shall contain the following data:

CRL standard	**Content**
Version	*V2*
Issuer	*Issuer of the list of cancelled certificates (see Paragraph 5.1)*
Effective Date	Date and time of entry into force
Next Update	Date and time of next update
Signature Algorithm	*SHA256RSA, SHA384RSA or SHA512RSA*
Signature Hash Algorithm	*SHA256, SHA384 or SHA512*
CRL extensions	
Authority Key Identifier	Certifying Authority (CA) key identifier
CRL Number	Unique CRL number, which is granted by the certifying authority (CA)

Issuing Distribution Point	CRL publishing site

7. Final provisions

7.1. Amendments in Description of Trust and electronic identification service provider issued certificate profiles will be made if there will be changes in Laws and regulations effective in the Republic of Latvia or improving LVRTC business processes.

7.2. Responsible for amendment management in this document is eParaksta division of LVRTC.

7.3. This Description of Trust and electronic identification service provider issued certificate profiles comes in to the force with approval of LVRTC board.

Annex 1

For description of trust and electronic identification service provider issued certificate profiles

Usage of keys and extended usage of keys

Key usage type	Certificate type					
	CA certificate	OCSP certificate	Time stamping	eStamp	Signature	Authentication
Key Usage						
CRL Signing	X					
Off-line CRL Signing	X					
Certificate Signing	X					
Digital Signature		X	X			X
Non-Repudiation		X	X	X	X	
Enhanced Key Usage						
Secure Email				X	X	
Document Signing				X	X	
Client Authentication						X
OCSP Signing		X				
Time Stamping			X			
Smart Card Logon						X
Key Encipherment (a0) for RSA Key Agreement (88) for ECC						X

"eID karte" Signature certificate profile 2019 with RSA keys

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	*[1]Certificate Policy:* *Policy Identifier=0.4.0.194112.1.2* *[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *https://www.eparaksts.lv/repository* *[2]Certificate Policy:* *Policy Identifier=1.3.6.1.4.1.32061.2.1.2.2* *[2,1]Policy Qualifier Info:* *Policy Qualifier Id=User Notice* *Qualifier:* *Notice Text=Šis sertifikāts ir iekļauts Latvijas Republikas izsniegta personu apliecinošā dokumentā. Sertifikātu izdevis VAS Latvijas Valsts radio un televīzijas centrs (reģ.Nr. 40003011203), nodrošinot atbilstību Elektronisko dokumentu likumam un Eiropas Parlamenta un Padomes regulai Nr. 910/2014* [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:

		https://www.eparaksts.lv/repository
Authority Information Access	No	*[1] Authority Info Access* *Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)* *Alternative Name:* *URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt* *[2]Authority Info Access* *Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)* *Alternative Name: URL=http://ocsp.eparaksts.lv*
CRL Distribution Points	No	*[1]CRL Distribution Point* *Distribution Point Name:* *Full Name:* *URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl*
Extended Key Usage	No	*id-kp-emailProtection(1.3.6.1.5.5.7.3.4)* *szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)*
Qualified Certificate Statement	No	*id-etsi-qcs-QcCompliance* *id-etsi-qcs-QcSSCD* *id-etsi-qcs-QcType - id-etsi-qct-esign* *id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Natural* *id-etsi-qcs-QcPDS* *en: https://www.eparaksts.lv/en/pds* *lv: https://www.eparaksts.lv/lv/pds*
Basic Constraints	Yes	Signatory Type=End Entity Path Length Constraint=None
Key Usage	Yes	*nonRepudiation*

Properties

Thumbprint Algorithm	Digest algorithm of the certificate
Thumbprint	*Digest value of the certificate*

"eID karte" Authentication certificate profile 2019 with RSA keys

X.509 V1	***Content***	
Version	V3	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.2.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Šis sertifikāts ir iekļauts Latvijas Republikas izsniegtā personu apliecinošā dokumentā [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:

		URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv
CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	No	id-kp-clientAuth
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	Digital Signature Key Encipherment (a0)
Properties		
Thumbprint Algorithm	*Digest algorithm of the certificate*	
Thumbprint	Digest value of the certificate	

Annex 4

For description of trust and electronic identification service provider issued certificate profiles

"eID karte" Signature certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	*[1]Certificate Policy:* *Policy Identifier=0.4.0.194112.1.2* *[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *https://www.eparaksts.lv/repository* *[2]Certificate Policy:* *Policy Identifier=1.3.6.1.4.1.32061.2.1.2.1* *[2,1]Policy Qualifier Info:* *Policy Qualifier Id=User Notice* *Qualifier:* *Notice Text=Šis sertifikāts ir iekļauts Latvijas Republikas izsniegta personu apliecinošā dokumentā. Sertifikātu izdevis VAS Latvijas Valsts radio un televīzijas centrs (reģ.Nr. 40003011203), nodrošinot atbilstību Elektronisko dokumentu likumam un Eiropas Parlamenta*

		un Padomes regulai Nr. 910/2014 [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	*[1] Authority Info Access* *Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)* *Alternative Name:* *URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt* *[2]Authority Info Access* *Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)* *Alternative Name: URL=http://ocsp.eparaksts.lv*
CRL Distribution Points	No	*[1]CRL Distribution Point* *Distribution Point Name:* *Full Name:* *URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl*
Extended Key Usage	No	*id-kp-emailProtection(1.3.6.1.5.5.7.3.4)* *szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)*
Qualified Certificate Statement	No	*id-etsi-qcs-QcCompliance* *id-etsi-qcs-QcSSCD* *id-etsi-qcs-QcType - id-etsi-qct-esign* *id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Natural* *id-etsi-qcs-QcPDS* *en: https://www.eparaksts.lv/en/pds* *lv: https://www.eparaksts.lv/lv/pds*
Basic Constraints	No	Signatory Type=End Entity Path Length Constraint=None
Key Usage	Yes	*nonRepudiation*

Properties

Thumbprint Algorithm	Digest algorithm of the certificate
Thumbprint	*Digest value of the certificate*

"eID karte" Authentication certificate profile

X.509 V1	***Content***	
Version	V3	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.2.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Šis sertifikāts ir iekļauts Latvijas Republikas izsniegtā personu apliecinošā dokumentā [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

Access		Alternative Name: URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv
CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	No	id-kp-clientAuth
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature
Properties		
Thumbprint Algorithm	*Digest algorithm of the certificate*	
Thumbprint	Digest value of the certificate	

"eParaksts karte" Authentication certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.4.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-clientAuth
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature
	Properties	
Thumbprint Algorithm	*Digest algorithm of the certificate*	
Thumbprint	Digest value of the certificate	

"eParaksts karte" Signature certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.4.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-emailProtection(1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)
Qualified Certificate Statement	No	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcType - id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Natural id-etsi-qcs-QcPDS en: https://www.eparaksts.lv/en/pds lv: https://www.eparaksts.lv/lv/pds
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	nonRepudiation

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

"eParaksts karte+" Authentication certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.5.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Subject Alternative Name	No	RFC822 Name=email Other Name: Principal Name=email
Extended Key Usage	No	Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

"eParaksts karte+" Signature certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.5.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)
Subject Alternative name	No	RFC822 Name=email@
Qualified Certificate Statement	No	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcType - id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Natural id-etsi-qcs-QcPDS en: https://www.eparaksts.lv/en/pds lv: https://www.eparaksts.lv/lv/pds
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	nonRepudiation
	Properties	
Thumbprint Algorithm	*Digest algorithm of the certificate*	
Thumbprint	Digest value of the certificate	

"eZīmogs" seal certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = the field shall contain a value, which the holder is using in order to represent him. Value may not be equal with the value of the field “Organization” O = Name of the organization 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.2.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)
Qualified Certificate Statement	No	id-etsi-qcs-QcCompliance id-etsi-qcs-QcType - id-etsi-qct-eZīmogs id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Legal id-etsi-qcs-QcPDS en: https://www.eparaksts.lv/en/pds lv: https://www.eparaksts.lv/lv/pds
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	nonRepudiation

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

"eZīmogs+" seal certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = the field shall contain a value, which the holder is using in order to represent him. Value may not be equal with the value of the field “Organization” O = Name of the organization 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.2.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)
Qualified Certificate Statement	No	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcType - id-etsi-qct-eZīmogs id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Legal id-etsi-qcs-QcPDS en: https://www.eparaksts.lv/en/pds lv: https://www.eparaksts.lv/lv/pds
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	nonRepudiation

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

Legal person Authentication certificate profile under eZīmogs policy (NCP)

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = the field shall contain a value, which the holder is using in order to represent him. Value may not be equal with the value of the field “Organization” O = Name of the organization 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.2.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-clientAuth
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

Legal person Authentication certificate profile under eZīmogs policy (NCP+)

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	5 years from Date and time of the issue of certificate	
Subject	CN = the field shall contain a value, which the holder is using in order to represent him. Value may not be equal with the value of the field “Organization” O = Name of the organization 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.2.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	id-kp-clientAuth
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

"eParaksts" Authentication certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	3 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.3.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv

CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	No	id-kp-clientAuth
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature

Properties

Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate

"eParaksts" Signature certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	3 years from Date and time of the issue of certificate	
Subject	CN = Given Name + Surname G = Given Name SN = Surname SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.32061.2.1.3.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv
CRL Distribution	No	[1]CRL Distribution Point

Points		Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	No	id-kp-emailProtection(1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)
Qualified Certificate Statement	No	id-etsi-qcs-QcCompliance id-etsi-qcs-QcType - id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 - id-etsi-qcs-SemanticsId-Natural id-etsi-qcs-QcPDS en: https://www.eparaksts.lv/en/pds lv: https://www.eparaksts.lv/lv/pds
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	nonRepudiation
		Properties
Thumbprint Algorithm	*Digest algorithm of the certificate*	
Thumbprint	Digest value of the certificate	

Issuing CA OCSP responder certificate profile

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unique certificate number, which is automatically granted by the certifying authority (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 or eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Date and time of the issue of certificate	
Valid To	1 month from Date and time of the issue of certificate	
Subject	CN = O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Public Key	RSA (2048 biti) Additional field contains public key	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	No	Certificate holder key identifier
Authority Key Identifier	No	Certifying Authority (CA) key identifier
OCSP no Revocation Checking	No	
Authority Information Access	No	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.eparaksts.lv/cert/LV_eID_ICA_2017.crt or URL=http://www.eparaksts.lv/cert/eParaksts_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv
CRL Distribution Points	No	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl or URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	No	OCSP Signing
Basic Constraints	Yes	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Yes	digitalSignature

	nonRepudiation
	Properties
Thumbprint Algorithm	*Digest algorithm of the certificate*
Thumbprint	Digest value of the certificate