Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu
PROFILU APRAKSTS

PIELIKUMĀ:

1. Atslēgu un paplašinātie atslēgu lietojumi
2.-18.Izsniegto sertifikātu profili

SAGATAVOJA: ePakalpojumu daļa

NOSŪTĪTS: Publisks

SAISTĪTIE DOKUMENTI:

1. [eIDAS regula] 2014.gada 23.jūlija Eiropas Parlamenta un Padomes (ES) regula Nr. 910/2014 "par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK"
2. [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".
3. [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"
4. [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"
5. [ETSI EN 319 412-5] European Standard EN 319 412-5 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements"
6. [ETSI EN 319 422] European Standard EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"
7. [RFC 3161] IETF RFC 3161 - Internet X.509 Public Key InfrastructureTime-Stamp Protocol (TSP)
8. [RFC 3739] IETF RFC 3739 - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
9. [RFC 5280] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
10. [ISO 3166] Codes for the representation of names of countries and their subdivisions
11. [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"

12. [ITU-T X.520] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".
13. [ETSI TS 119 312] Technical specification TS 119 312 V1.1.1 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”
14. Uzticamības pakalpojumu sniegšanas noteikumi

IZMAIŅU VĒSTURE:

Pārskatītā varianta nr.	**Spēkā stāšanās datums**	**Izmaiņu kopsavilkums**
01.0	01.07.2017.	Sākotnējā versija
01.1	01.07.2017	Pievienots 2. pielikums
02.0	01.08.2017	Pievienoti “eParaksts” pakalpojuma saistīto sertifikātu un OCSP sertifikāta profili. Pievienots 5.3.2.10. punkts
03.0	01.05.2018	Dokuments sasaistīts ar Fizisko personu elektroniskās identifikācijas likumu. Veiktas izmaiņas definīcijās un dokumenta nosaukumā.
04.0	01.09.2019	Aktualizēts CRL profils, Papildināta 1.pielikuma tabula ar jaunu atslēgas pielietojumu (šifrēšana), papildināts 2. un 3.pielikums ar jauno eID karšu sertifikātu aprakstiem.
05.0	16.09.2019	Papildināts 1. un 3. pielikums saistībā ar šifrēšanas funkcionalitāti.
06.0	30.06.2020	Papildināts 15. un 16. pielikums saistībā ar kvalificēta paraksta sertifikāta izsniegšanu. Pievienots 17. un 18. pielikums saistībā ar kvalificēta paraksta sertifikāta izsniegšanu.

SATURS

1. Mērķis un auditorija

1.1. “Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksta” mērķis ir iepazīstināt Uzticamības un elektroniskās identifikācijas pakalpojumu Abonentus un Atkarīgās puses ar Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profiliem, to lauku nozīmēm un minimālajām prasībām.

1.2. “Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts” ir saistošs valsts akciju sabiedrības “Latvijas Valsts radio un televīzijas centra” sniegto uzticamības un elektroniskās identifikācijas pakalpojumu Abonentiem un Atkarīgajām pusēm.

1.3. “Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts” ir sagatavots latviešu valodā. Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts var tikt tulkots un var būt pieejams arī citās valodās. Tulkojumu nesakritību gadījumā versija latviešu valodā vienmēr ir vadoša.

2. Termini un saīsinājumi

Saīsinājums, termins	Skaidrojums
Abonents	Fiziska vai juridiska persona, kas ir noslēgusi līgumu ar Pakalpojuma sniedzēju par vienu vai vairākiem uzticamības un elektroniskās identifikācijas vai citu Pakalpojuma sniedzēja sniegto pakalpojumu saņemšanu vai kurai tiek sniegti Pakalpojuma sniedzēja pakalpojumi pamatojoties uz normatīvo aktu, nenoslēdzot līgumu ar Abonentu. Iekļauj sevī sertifikātu turētājus (subjektus) - Parakstītāju, Zīmoga radītāju, Laika zīmogu pieprasītāju un Autentifikācijas sertifikātu lietotāju.
Atkarīgās puses	Fiziska vai juridiska persona, kas paļaujas uz elektronisku identifikāciju vai uzticamības pakalpojumu
CA	Sertifikātu izsniegšanas institūcija
CRL	Atsaukto sertifikātu saraksts
eIDAS	Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regula (ES) Nr. 910/2014 "Par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK"
ETSI	Eiropas Telekomunikāciju standartu institūts
LVRTC	Valsts akciju sabiedrība “Latvijas Valsts radio un televīzijas centrs”,

Saīsinājums, termins	Skaidrojums
	vienotais reģistrācijas Nr. 40003011203, Ērgļu iela 14, Rīga, Latvija, LV-1012
OCSP	Tiešsaistes sertifikātu statusa pārbaudes serviss
Pakalpojumu sniedzējs	LVRTC, kas darbojās kā Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzējs
PDS	Publiskās atslēgas infrastruktūras atklāšanas noteikumi
SSL	Protokols drošas un privātas saziņas nodrošināšanai internetā

3. Vispārīgi

3.1. LVRTC darbojas kā Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzējs. LVRTC sniegtie uzticamības un elektroniskās identifikācijas pakalpojumi ir saistīti ar dažāda veida sertifikātiem.

3.2. Pakalpojuma sniedzēju sniegto pakalpojumu sertifikātu profili ir definēti no 2.līdz 16.pielikumam.

4. Ar šo aprakstu saistītie sertifikātu tipi

4.1. Ar fizisku personu saistīti sertifikāti:

4.1.1. autentifikācijas,

4.1.2. parakstīšanas.

4.2. Ar juridisku personu saistīti sertifikāti:

4.2.1. elektroniskā zīmoga,

4.2.2. autentifikācijas,

4.2.3. Pakalpojumu sniedzēja laika zīmogošanas,

4.2.4. Pakalpojumu sniedzēja OCSP.

4.3. Pakalpojumu sniedzēja atsaukto sertifikātu saraksta profils.

5. Sertifikātu dati

5.1. Dati par sertifikātu izsniedzēju

Lauks – "Issuer"			
Vērtības nosaukums	Saīsinājums	Skaidrojums/saturs	CA veids
Common Name	CN	eParaksts Root CA	Saknes CA
		LV eID ICA 2017	Izsniegšanas CA
		eParaksts ICA 2017	Izsniegšanas CA
Organization	O	VAS "Latvijas Valsts radio un televīzijas centrs"	Visām CA
Country	C	LV	Visām CA
Organization Identifier	2.5.4.97	NTRLV-40003011203	Visām CA

5.2. Dati par sertifikātu turētāju

5.2.1. **Fiziskai personai**

Lauks – "Subject"				
Vērtības nosaukums	Saīsinājums	OID	Skaidrojums	Nosacījums
Common Name	CN	2.5.4.3	Vārda un Uzvārda salikums	Obligāts
Given Name	G	2.5.4.42	Fiziskas personas vārds	Obligāts
surName	SN	2.5.4.4	Fiziskas personas uzvārds	Obligāts
Organizational Unit	OU	2.5.4.11	Struktūrvienība	Izvēles
Organization	O	2.5.4.10	Organizācija	Izvēles
Country	C	2.5.4.6	Valsts kods atbilstoši [ISO 3166]	Obligāts
e-mail	E	1.2.840.113549.1.9.1	e-pasta adrese	Izvēles
Serial Number	SERIALNUMBER	2.5.4.5	Sk. 5.2.1.1. punktu	Obligāts
Locality	L	2.5.4.7	Pilsēta	Izvēles
State	S	2.5.4.8	Reģions	Izvēles

5.2.1.1. Fiziskas personas sertifikātā Identifikācijas numuram ir jāizmanto id-etsi-qcs-SemanticsId-Natural semantika atbilstoši [ETSI EN 319 412-1] standarta 5.1.3.punktā definētajām prasībām.

5.2.2. **Juridiskai personai**

Lauks – "Subject"				
Vērtības nosaukums	Saīsinājums	OID	Skaidrojums	Nosacījums
Common Name	CN	2.5.4.3	Sk. 5.2.2.1. punktu	Obligāts
Organizational Unit	OU	2.5.4.11	Struktūrvienība	Izvēles
Organization	O	2.5.4.10	Organizācijas nosaukums	Obligāts
Country	C	2.5.4.6	Organizācijas valsts kods atbilstoši [ISO 3166]	Obligāts
e-mail	E	1.2.840.113549.1.9.1	e-pasta adrese	Izvēles
Organization Identifier		2.5.4.97	Sk. 5.2.2.2. punktu	Obligāts
Locality	L	2.5.4.7	Pilsēta	Izvēles
State	S	2.5.4.8	Reģions	Izvēles

5.2.2.1. Sertifikāta nosaukuma lauka saturs ir atkarīgs no sertifikātu veida:

5.2.2.1.1. elektroniskā zīmoga sertifikāti – laukam ir jāsatur vērtība, ko sertifikāta Abonents izmanto lai reprezentētu sevi. Vērtība var nesakrist ar lauka "Organizācija" vērtību,

5.2.2.1.2. OCSP sertifikātam – OCSP servisa identifikators, pēc kura var viennozīmīgi identificēt Izsniegšanas institūciju par kuras izsniegtajiem sertifikātiem atbild minētais OCSP serviss,

5.2.2.1.3. laika zīmogošanas sertifikātam – laika zīmogošanas servisa identifikators, pēc kura var viennozīmīgi identificēt laika zīmogu izsniegušo laika zīmogošanas institūciju,

5.2.2.2. juridiskas personas sertifikātā organizācijas identifikatoram ir jāizmanto id-etsi-qcs-SemanticsId-Legal semantika atbilstoši [ETSI EN 319 412-1] standarta 5.1.4.punktā definētajām prasībām.

5.3. Citi sertifikātos iekļautie dati

5.3.1. Pakalpojuma sniedzēja sertifikātu profili satur sekojošus X.509 versijas 1 laukus

5.3.1.1. Versija

X.509 V1 lauks	**Obligāts**	**Saturs**
Version	Jā	*V3*

5.3.1.2. Sērijas numurs

X.509 V1 lauks	Obligāts	Saturs
Serial Number	Jā	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (CA)

5.3.1.3. Paraksta un kontrolsummas algoritms

X.509 V1 lauki	Obligāts	Saturs
Signature Algorithm	Jā	SHA256RSA, SHA384RSA vai SHA512RSA
Signature Hash Algoritm	Jā	*SHA256,* SHA384 *vai SHA512*

5.3.1.4. Sertifikāta derīguma termiņš

X.509 V1 lauki	Obligāts	Saturs
Valid from	Jā	Sertifikāta izsniegšanas datums un laiks
Valid to	Jā	Sertifikāta derīguma termiņa datums un laiks

5.3.1.5. Publiskā atslēga

X.509 V1 lauks	**Obligāts**	**Saturs**
Public Key	Jā	RSA (2048) vai RSA (4096), Papildus lauks satur publisko atslēgu.

5.3.2. Pakalpojuma sniedzēja izsniegto sertifikātu profili var saturēt sekojošus paplašinājumus:

5.3.2.1. Sertifikāta turētāja un sertifikāta izsniedzēja (CA) atslēgu identifikatori

X.509 V3 paplašinājumi	Kritisks	Saturs
Subject Key Identifier	Nav	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nav	Sertifikāta izsniedzēja (CA) atslēgas identifikators

5.3.2.2. Sertifikātu politikas

X.509 V3 paplašinājums	Kritisks	Saturs
Certificate Policies	Nav	*Laukam jāsatur konkrētā produkta politikas OID vērtība*
		Var saturēt "Notice Text"
		Satur URI http://www.eparaksts.lv/repository *kur izvietota konkrētā produkta politika un noteikumi*

5.3.2.3. Atsaukto sertifikātu saraksta publicēšanas vietnes

X.509 V3 paplašinājums	Kritisks	Saturs
CRL Distribution Points	nav	*Satur vietni, kur pieejams atsaukto sertifikātu saraksts*

5.3.2.4. Tiešsaistes sertifikātu pārbaudes servisa vietne

X.509 V3 paplašinājums	Kritisks	Saturs
Authority Info Access	nav	*Satur:* *1. Vietnes adresi kurā publicēts CA sertifikāts;* *2. Vietni kur pieejams OCSP serviss;* *3. Citas (ja izmantotas) ar sertifikātu publicēšanu saistītas vietnes*

5.3.2.5. Paplašinātā atslēgu lietošana

X.509 V3 paplašinājumi	Kritisks	Saturs
Enhanced Key Usage	nav	Satur sertifikāta pielietojumam atbilstošus atslēgu lietošanas paplašinājumus **(sk. 1.pielikumu)**

5.3.2.6. Kvalificēta sertifikāta paziņojums

X.509 V3 paplašinājumi	Kritisks	Saturs
Qualified Certificate Statement	nē	*Abonentu sertifikātiem lauka saturs tiek veidots atbilstoši [ETSI EN 319 412-5] standartā definētajām prasībām* *Laika zīmogošanas sertifikātam lauka saturs tiek veidots atbilstoši [ETSI EN 319 422] standartā definētajām prasībām*

5.3.2.7. Atslēgu lietošanas mērķis

X.509 V3 paplašinājumi	Kritisks	Saturs
Key Usage	jā	Satur sertifikāta pielietojumam atbilstošus atslēgu lietojumus **(sk. 1.pielikumu)**

5.3.2.8. Sertifikātu turētāja alternatīvie vārdi

X.509 V3 paplašinājumi	Kritisks	Saturs
Subject Alternative Name	nē	Autentifikācijas sertifikātos var saturēt turētāja e-pasta adresi.

5.3.2.9. Pamata ierobežojumi Abonentu sertifikātiem

Ja sertifikāta profilā nav norādīts savādāk.

X.509 V3 paplašinājumi	**Kritisks**	**Saturs**
Basic Constraints	jā	*Subject Type=End Entity* *Path Length Constraint=None*

5.3.2.10. OCSP sertifikāta papildus paplašinājums

X.509 V3 paplašinājumi	**Kritisks**	**Saturs**
OCSP No Revocation Checking	Nē	*05 00 (Windows OS)*

5.3.3. Pakalpojumu sniedzēja izsniegto sertifikātu profili satur sekojošus rekvizītus:

Īpašības	**Saturs**
Thumbprint Algorithm	*Sertifikāta īssavilkuma algoritms*
Thumbprint	Sertifikāta īssavilkuma vērtība

6. CRL profils

6.1. Pakalpojuma sniedzēja izsniegto atsaukto sertifikātu saraksta profili satur šādus datus:

***CRL* standarts**	**Saturs**
Version	*V2*
Issuer	*Atsaukto sertifikātu saraksta izsniedzējs (sk.5.1.punktu)*
Effective Date	Spēkā stāšanās datums un laiks
Next Update	Nākamā papildinājuma datums un laiks
Signature Algorithm	*SHA256RSA, SHA384RSA vai SHA512RSA*
Signature Hash Algorithm	*SHA256, SHA384 vai SHA512*
***CRL* paplašinājumi**	
Authority Key Identifier	Sertifikāta izsniedzēja (CA) atslēgas identifikators
CRL Number	Unikāls CRL numurs, ko piešķir sertifikātu izsniedzošā institūcija (CA)
Issuing Distribution Point	CRL publikācijas vietne

7. Noslēguma noteikumi

7.1. “Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstā” tiek veikti grozījumi, mainoties saistošajiem normatīvajiem aktiem, kā arī pilnveidojot LVRTC biznesa procesus.

7.2. “Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksta” izmaiņu vadību nodrošina eParaksta daļa.

7.3. Šis “Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu apraksts” stājas spēkā ar tā apstiprināšanu LVRTC Valdes sēdē Valdes lēmumā noteiktajā kārtībā.

1.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

Atslēgu un paplašinātie atslēgu lietojumi

Atslēgu lietojuma veids	Sertifikāta veids					
	CA sertifikāts	OCSP sertifikāts	Laika zīmogošanas	eZīmoga	Parakstīšanas	Autentifikācijas
Key Usage						
CRL Signing	X					
Off-line CRL Signing	X					
Certificate Signing	X					
Digital Signature		X	X			X
Non-Repudiation		X	X	X	X	
Key Encipherment (a0) priekš RSA Key Agreement (88) priekš ECC						X
Enhanced Key Usage						
Secure Email				X	X	X
Document Signing				X	X	
Client Authentication						X
OCSP Signing		X				
Time Stamping			X			
Smart Card Logon						X

2.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

“eID karte” elektroniskā paraksta sertifikāta profils 2019 RSA atslēgām

Attiecas uz sertifikātiem, kas izsniegti pēc 2019.gada rudens (jaunā parauga eID karšu ražošanas uzsākšana)

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 Paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	*[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	Nē	*[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	Nē	*[1]CRL Distribution Point* *Distribution Point Name:* *Full Name:* *URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl*
Extended Key Usage	Nē	*Document Signing (1.3.6.1.4.1.311.10.3.12)* *Secure Email (1.3.6.1.5.5.7.3.4)*
Qualified Certificate Statement	Nē	*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	Jā	Signatory Type=End Entity Path Length Constraint=None
Key Usage	Jā	*nonRepudiation*

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

3.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

“eID karte” autentifikācijas sertifikāta profils 2019 RSA atslēgām

Attiecas uz sertifikātiem, kas izsniegti pēc 2019.gada rudens (jaunā parauga eID karšu ražošanas uzsākšana)

X.509 V1 lauks	***Saturs***	
Version	V3	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	Nē	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	Digital Signature Key Encipherment (a0)
Īpašības		
Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms	
Thumbprint	Sertifikāta īssavilkuma vērtība	

4.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

“eID karte” elektroniskā paraksta sertifikāta profils

Attiecas uz sertifikātiem, kas izsniegti līdz 2019.gada rudenim (jaunā parauga eID karšu ražošanas uzsākšana)

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 Paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	*[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	Nē	*[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	Nē	*[1]CRL Distribution Point* *Distribution Point Name:* *Full Name:* *URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl*
Extended Key Usage	Nē	*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	Nē	*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	Nē	Signatory Type=End Entity Path Length Constraint=None
Key Usage	Jā	*nonRepudiation*

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

5.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

“eID karte” autentifikācijas sertifikāta profils

Attiecas uz sertifikātiem, kas izsniegti līdz 2019.gada rudenim (jaunā parauga eID karšu ražošanas uzsākšana)

X.509 V1 lauks	***Saturs***	
Version	V3	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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 Access	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	Nē	id-kp-clientAuth
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature
Īpašības		
Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms	
Thumbprint	Sertifikāta īssavilkuma vērtība	

6.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts karte" autentifikācijas sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	id-kp-clientAuth
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

7.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts karte" elektroniskā paraksta sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	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	Nē	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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	nonRepudiation

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

8.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts karte+" autentifikācijas sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Subject Alternative Name	Nē	RFC822 Name=email Other Name: Principal Name=email
Extended Key Usage	Nē	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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

9.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts karte+" elektroniskā paraksta sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	5 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	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	Nē	RFC822 Name=email@
Qualified Certificate Statement	Nē	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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	nonRepudiation
Īpašības		
Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms	
Thumbprint	Sertifikāta īssavilkuma vērtība	

10.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eZīmogs" elektroniskā zīmoga sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	2 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = laukam ir jāsatur vērtība, ko turētājs izmanto lai reprezentētu sevi. Vērtība var nesakrist ar lauka "Organizācija" vērtību O = Organizācijas nosaukums 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	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	Nē	id-etsi-qcs-QcCompliance id-etsi-qcs-QcType - id-etsi-qct-eseal 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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	nonRepudiation

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

11.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eZīmogs+" elektroniskā zīmoga sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	2 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = laukam ir jāsatur vērtība, ko turētājs izmanto lai reprezentētu sevi. Vērtība var nesakrist ar lauka "Organizācija" vērtību O = Organizācijas nosaukums 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	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	Nē	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcType - id-etsi-qct-eseal 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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	nonRepudiation

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

12.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

Juridiskas personas autentifikācijas sertifikāta profils izdots zem eZīmoga politikas (NCP)

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	2 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = laukam ir jāsatur vērtība, ko turētājs izmanto lai reprezentētu sevi. Vērtība var nesakrist ar lauka "Organizācija" vērtību O = Organizācijas nosaukums 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	id-kp-clientAuth
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

13.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

Juridiskas personas autentifikācijas sertifikāta profils izdots zem eZīmoga politikas (NCP+)

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	2 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = laukam ir jāsatur vērtība, ko turētājs izmanto lai reprezentētu sevi. Vērtība var nesakrist ar lauka "Organizācija" vērtību O = Organizācijas nosaukums 2.5.4.97 = NTRLV=1234556789 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	id-kp-clientAuth
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature
Īpašības		
Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms	
Thumbprint	Sertifikāta īssavilkuma vērtība	

14.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts" autentifikācijas sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	3 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	Nē	id-kp-clientAuth
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature
	Īpašības	
Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms	
Thumbprint	Sertifikāta īssavilkuma vērtība	

15.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts" autentifikācijas sertifikāta profils no 2020.gada

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	3 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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=1.3.6.1.4.1.32061.2.1.3.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	Nē	id-kp-clientAuth
Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

16.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts" elektroniskā paraksta sertifikāta profils

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	3 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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	Nē	[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	Nē	[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	Nē	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	Nē	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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	nonRepudiation

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

17.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

"eParaksts" elektroniskā paraksta sertifikāta profils no 2020.gada

X.509 V1 lauks	***Saturs***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (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	Sertifikāta izsniegšanas datums un laiks	
Valid To	3 gadi no sertifikāta izsniegšanas datuma un laika	
Subject	CN = Vārds + Uzvārds G = Vārds SN = Uzvārds SERIALNUMBER = PNOLV-123456-12345 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 paplašinājums	**Kritisks**	**Saturs**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
Certificate Policies	Nē	[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=1.3.6.1.4.1.32061.2.1.3.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository
Authority Information Access	Nē	[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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl
Extended Key Usage	Nē	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	Nē	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	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	nonRepudiation

Īpašības

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība

18.pielikums

Uzticamības un elektroniskās identifikācijas pakalpojumu sniedzēja izsniegto sertifikātu profilu aprakstam

Sertifikātu izsniegšanas CA OCSP sertifikāta profils

X.509 V1	***Content***	
Version	*V3*	
Serial number	Unikāls sertifikāta numurs, ko automātiski piešķir sertifikātu izsniedzošā institūcija (CA)	
Signature Algorithm	SHA256RSA	
Issuer	CN = LV eID ICA 2017 vai eParaksts ICA 2017 O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Valid From	Sertifikāta izsniegšanas datums un laiks	
Valid To	1 mēnesis no sertifikāta izsniegšanas datuma un laika	
Subject	CN = O = VAS Latvijas Valsts radio un televīzijas centrs 2.5.4.97 = NTRLV-40003011203 C = LV	
Public Key	RSA (2048 biti) Papildus lauks satur publisko atslēgu	
X.509 V3 Extensions	**Critical**	**Content**
Subject Key Identifier	Nē	Sertifikāta turētāja atslēgas identifikators
Authority Key Identifier	Nē	Sertifikāta izsniedzēja (CA) atslēgas identifikators
OCSP no Revocation Checking	Nē	
Authority Information Access	Nē	[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 vai 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	Nē	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.eparaksts.lv/crl/LV_eID_ICA_2017_N.crl vai URL=http://www.eparaksts.lv/crl/eParaksts_ICA_2017_N.crl
Extended Key Usage	Nē	OCSP Signing

Basic Constraints	Jā	*Signatory Type=End Entity* *Path Length Constraint=None*
Key Usage	Jā	digitalSignature nonRepudiation

Properties

Thumbprint Algorithm	Sertifikāta īssavilkuma algoritms
Thumbprint	Sertifikāta īssavilkuma vērtība