LTAB OCTA

Certificate Profile

2018.10.22
Version 01

OID: 1.3.6.1.4.1.52826.1.2.1

DOCUMENT SUMMARY

The document describes certificate profile, i.e. the meaning of the content and the structure of the user certificates of LTAB OCTA.

DOCUMENT IDENTIFICATION

The object identifier (OID) of this document is: 1.3.6.1.4.1.52826.1.2.1

DESCRIPTION OF THE IDENTIFIER:

1.3.6.1.4.1.52826.x.y.z

1.3.6.1.4.1.51321 – the identifier of the organization - Latvijas Transportlidzeklu Apdrosinataju birojs;

x – product identifier -.1 – LTAB OCTA;

y – document identifier, .1 – terms & conditions, .2 – certificate profile;

z – document version number.

CONTENT

1. DEFINITIONS

eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identifcation and trust services for electronic transactions in the internal market and repealing **Directive 1999/93/EC**

Electronic Signature - Electronic data used by the Subscriber to sign the document by adding this data to the electronic document or by logically associating it with **the document**.

Advanced Electronic Signature - Electronic Signature which meets the requirements provided in Article **26 of eIDAS**.

Authentication - Electronic process which enables electronic identifcation of the legal or **natural person.**

Authentication Certifcate - Electronic proof, certifcate which is has the intended use of **Authentication and ciphering**.

Certifcate - Public Key, together with additional information, laid down in the Certifcate Profle, rendered unforgeable via encipherment using the **Private Key of the Certifcate Authority which issued it.**

Certifcate Authority - **State JSC "Latvija Radio and Television Centre", Reg. No. 40003011203**, which ensure issuing, verifcation and revocation of the **certifcates for the use within LTAB OCTA application.**

Identity Provider - An organization who is providing electronic authentication means and is responsible for identifcation of the person, creation of the electronic identity of the person, and approval of the electronic identity of the **person to the Registration Authority, i.e. credit institution**.

LTAB OCTA - A mobile application provided and maintained by If which contains one pair of Certifcates consisting of the Authentication Certifcate and the Electronic Signature Certifcate and their corresponding Private Keys **which are intended for insurance-related use**.

Electronic Signature Certifcate - Certifcate which links electronic signature validation data to a natural **person and confrms at least the name of that person**.

OCSP - **The Online Certifcate Status Protocol**

LTAB – Biedrība "Latvijas Transportlīdzekļu apdrošinātāju birojs" registered with No. **40008084453** in the Commercial Registry of Latvia of Latvia.

2. DOCUMENT VERSIONS

DATE - 2018.10.22.	VERSION - 01	AMENDMENTS – Initial version

3. REFERENCES

[1] ETSI EN 319 412-1 v1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures;

[2] ETSI EN 319 412-2 v2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

[3] LTAB OCTA Terms and Conditions (LTAB OCTA Lietošanas noteikumi), published at: https://www.ltab.lv/par-mums/ltab-octa-lietosanas-dokumentacija/

[4] ISO 3166 Codes, published: http://www.iso.org/iso/country_codes;

[5] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[6] RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;

[7] RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revoca- tion List (CRL) Profile;

[8] 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 transac- tions in the internal market and repealing Directive 1999/93/EC.

4. TECHNICAL PROFILE OF THE CERTIFICATE

Natural person certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280, ETSI EN 319 412-2 (2016-02).

4.1. CERTIFICATE BODY

FIELD	OID	MANDATORY	VALUE	CHANGEABLE	DESCRIPTION
VERSION		yes	V3	no	Certificate format version
SERIAL NUMBER		yes		no	Unique serial number of the certificate
SIGNATURE ALGORITHM	1.2.840.113549.1.1.11	yes	Sha256WithRSAEncryptior	no	Signature algorithm in accordance to RFC 52808 [4]
ISSUER DISTINGUISHED NAME					
Common name (CN)	2.5.4.3	yes	eParaksts ICA 2017 NQC	no	Certificate authority name
Organisation Identifier	2.5.4.97	yes	NTRLV-40003011203	no	Identification of the issuer organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Organization (O)	2.5.4.10	yes	VAS Latvijas Valsts radio un televīzijas centrs	no	Issuer organization name
Country (C)	2.5.4.6	yes	LV	no	Country code: LV – Latvia (2 character ISO 3166 country code)
VALID FROM		yes	(date)	no	First date of certificate validity.
VALID TO		yes	(date)	no	The last date of certificate validity. Generally, date of issuance + 1095 days (3 years).
SUBJECT DISTINGUISHED NAME					
SerialNumber (S)	2.5.4.5	yes		yes	Certificate holder's personal code as specified in clause 5.1.3 of ETSI EN 319 412-1.
GivenName (G)	2.5.4.42	yes		yes	Person given names in UTF8 format according to RFC 5280.
SurName (SN)	2.5.4.4	yes		yes	Person surnames in UTF8 format according to RFC 5280.
OrganizationalUnit Name (OU)	2.5.4.11	yes	LTAB OCTA	yes	The name of the product the issued certificate has to be used for.
Organizational UnitName (OU)	2.5.4.11	yes	GUID	yes	GUID value of the person authentication response provided by the identity provider during user enrollment, formatted in 8-4-4-4-12 pattern. Ensures the proof of identity verification linked to the response of the identity provider.
CommonName (CN)	2.5.4.3	yes		yes	Comma-separated first name, surname, personal identity code of the person.
Country (C)	2.5.4.6	yes	LV	yes	Country of origin in accordance with ISO 3166.
SUBJECT PUBLIC KEY		yes	RSA 2048 bits	no	The public key of the Certificate holder.

4.2. CERTIFICATE EXTENSIONS

EXTENSION	OID	VALUES AND LIMITATIONS	CRITICAL	MANDATORY
CERTIFICATE POLICIES	2.5.29.32	For **authentication** certificate: Certificate Policy: 1.3.6.1.4.1.32061.2.4.1 CPSUri: https://www.eparaksts.lv/repository userNotice: Sertifikātu ir izsniegusi VAS Latvijas Valsts radio un televīzijas centrs (Reģ. Nr. Latvijas Uzņēmumu reģistrā 40003011203) lietošanai LTAB OCTA lietotnē, ko nodrošina Biedrība "Latvijas Transportlīdzekļu apdrošinātāju birojs" (Reģ. Nr. 40008084453, OID: 1.3.6.1.4.1.52826). 1.3.6.1.4.1.52826.1.2.1 CPSUri: https://www.ltab.lv/par-mums/ltab-octa-lietosanas-dokumentacija/ userNotice: LTAB OCTA lietošanas noteikumi For eIDAS advanced **electronic signature** certificate: 1.3.6.1.4.1.32061.2.4.1 CPSUri: https://www.eparaksts.lv/repository userNotice: Sertifikātu ir izsniegusi VAS Latvijas Valsts radio un televīzijas centrs (Reģ. Nr. Latvijas Uzņēmumu reģistrā 40003011203) lietošanai LTAB OCTA lietotnē, ko nodrošina Biedrība "Latvijas Transportlīdzekļu apdrošinātāju birojs" (Reģ. Nr. 40008084453, OID: 1.3.6.1.4.1.52826). 1.3.6.1.4.1.52826.1.2.1 CPSUri: https://www.ltab.lv/par-mums/ltab-octa-lietosanas-dokumentacija/ userNotice: LTAB OCTA lietošanas noteikumi	no	yes
KEY USAGE	2.5.29.15	For **authentication** certificate: DigitalSignature, KeyEncipherment, dataEncipherment. For eIDAS advanced **electronic signature** certificate: nonRepudiation.	yes	yes
EXTENDED KEY USAGE	2.5.29.37	id-kp-clientAuth to be used for authentication certificate ONLY, 1.3.6.1.5.5.7.3.2 szOID_KP_DOCUMENT_SIGNING, to be used for eIDAS advanced electronic signature certificate only, 1.3.6.1.4.1.311.10.3.12	no	yes
AUTHORITY KEYIDENTIFIER	2.5.29.35	Hash of the public key used to sign the certificate	no	yes
SUBJECTKEY IDENTIFIER	2.5.29.14	Hash of the public key used to sign the certificate	no	yes
CRL DISTRIBUTION POINTS	2.5.29.31	CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.eparaksts.lv/crl/ eParaksts_NQC_ICA_2017_x.crl	no	yes
AUTHORITY INFORMATION ACCESS	1.3.6.1.5.5.7.1.1 .	[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_NQC_ICA_2017.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol	no	yes

(1.3.6.1.5.5.7.48.1)
Alternative Name: URL=http://ocsp.eparaksts.lv

"LTAB" Auth certificate profile

Tiek izmantoti Produkcijas nosaukumi un linki

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 NQC CA 1 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 O = LTAB OU = LTAB OCTA OU = GUID value of the person authentication response provided by the identity provider, formatted in 8-4-4-4-12 pattern 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=1.3.6.1.4.1.32061.2.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.eparaksts.lv/repository [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Sertifikātu ir izsniegusi VAS Latvijas Valsts radio un televīzijas centrs (Reģ. Nr. Latvijas Uzņēmumu reģistrā 40003011203) lietošanai LTAB OCTA lietotnē, ko nodrošina ko nodrošina Biedrība

		“Latvijas Transportlīdzekļu apdrošinātāju birojs” (Reģ. Nr. 40008084453, OID: 1.3.6.1.4.1.52826). [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.52826.1.2.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.ltab.lv/par-mums/ltab-octa-lietosanas-dokumentacija/ [2,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=LTAB OCTA lietošanas noteikumi
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_NQC_ICA_1.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_NQC_ICA_2017_x.crl
Extended Key Usage	No	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	