IF MOBILE

Certificate Profile

2018.02.15
Version 01

OID: 1.3.6.1.4.1.51321.2.1.2.1

Relax, we'll help you.

DOCUMENT SUMMARY

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

DOCUMENT IDENTIFICATION

The object identifier (OID) of this document is: 1.3.6.1.4.1.51321.2.1.2.1

DESCRIPTION OF THE IDENTIFIER:

1.3.6.1.4.1.51321.x.y.z.q

1.3.6.1.4.1.51321 – the identifier of the organization - If P&C Insurance AS;

x – country identifier, possible values - .1 – Estonia, .2 – Latvia, .3 – Lithuania;

y – product identifier, possible values - .1 – If Mobile;

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

q – document version number.

CONTENT

1. DEFINITIONS

TERM	DEFINITION
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
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 identification of the legal or natural person.
Authentication Certificate	Electronic proof, certificate which is has the intended use of Authentication and ciphering.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile, rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	State JSC "Latvija Radio and Television Centre", Reg. No. 40003011203, which ensure issuing, verification and revocation of the certificates for the use within If Mobile application.
Identity Provider	An organization who is providing electronic authentication means and is responsible for identification 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.
If Mobile	A mobile application provided and maintained by If which contains one pair of Certificates consisting of the Authentication Certificate and the Electronic Signature Certificate and their corresponding Private Keys which are intended for insurance-related use.
Electronic Signature Certificate	Certificate which links electronic signature validation data to a natural person and confirms at least the name of that person.
OCSP	The Online Certificate Status Protocol
If	If P&C Insurance AS registered with No. 10100168 in the National Trade Registry of Estonia and its affiliates in Latvia and Lithuania: If P&C Insurance AS Latvijas filiāle, unified registration number Nr.40103201449 in the Commercial Registry of Latvia, and "If P&C Insurance AS" filialas, registration number 4302279548 in the National Trade Registry of Lithuania.

2. DOCUMENT VERSIONS

VERSION HISTORY		
DATE	**VERSION**	**AMENDMENTS**
2018.02.15	01	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] If Mobile Terms and Conditions (If Mobile Lietošanas noteikumi), published at https://www.if.lv/if-mobile#dokumenti

[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 Revocation 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 transactions 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	sha256WithRSAEncryption	no	Signature algorithm in accordance to RFC 52808 [4]
ISSUER DISTINGUISHED NAME					
Common name (CN)	2.5.4.3	yes	eParaksts NQC ICA 2017	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.
Organisation (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	If Mobile	yes	The name of the product the issued certificate has to be used for.
Organizational UnitName (OU)	2.5.4.11	yes	SHA256 base64 value	yes	SHA256 hash value of the person authentication response provided by the identity provider during user enrollment encoded in base64. Ensures the proof of identity verification linked to the response of the identity provider.
Organizational UnitName (OU)	2.5.4.11	yes	base64 value	yes	The unique identifier of the instance of the user identity, base64 format.

FIELD	OID	MANDATORY	VALUE	CHANGEABLE	DESCRIPTION
Common Name (CN)	2.5.4.3	yes		yes	Comma-separated first names, surnames, personal identity code and mobile phone number of the person.
telephone Number	2.5.4.20	yes		yes	Mobile phone number of the person.
Country (C)	2.5.4.6	yes		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 If Mobile lietotnē, ko nodrošina If P&C Insurance AS (Reģ. Nr. Igaunijas Uzņēmumu reģistrā 10100168, OID: 1.3.6.1.4.1.51321). 1.3.6.1.4.1.51321.2.1.2.1 CPSUri: https://www.if.lv/if-mobile#dokumenti userNotice: If Mobile 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 If Mobile lietotnē, ko nodrošina If P&C Insurance AS (Reģ. Nr. Igaunijas Uzņēmumu reģistrā 10100168, OID: 1.3.6.1.4.1.51321). 1.3.6.1.4.1.51321.2.1.2.1 CPSUri: https://www.if.lv/if-mobile#dokumenti userNotice: If Mobile 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

EXTENSION	OID	VALUES AND LIMITATIONS	CRITICAL	MANDATORY
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 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 ceritificate	no	yes
SUBJECTKEY IDENTIFIER	2.5.29.14	Hash of the public key used to sign the ceritificate	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 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eparaksts.lv	no	yes