Pregled profila sertifikata PKSCA

Ver 1.1

Sadržaj

1 Struktura OID za dodeljivanje Certificate Policy OID brojeva

Struktura CP OID		
Naziv grupe	**Naziv grane OID-a**	**OID**
PKS PEN	Private enterprise number PKS	PKS-PEN
Organizaciona jedinica PKS-a za izdavanje sertifikata	OID grana dodeljena organizacionoj jedinici nadležnoj za izdavanje certifikata - PKSCA	OJCA = PKS-PEN.10
Certificate Policy	OID koji označava konkretan CP dokument davaoca elektronskih usluga od poverenja	CP = OJCA.y
Certificate Policy	OID koji označava verziju CP dokumenta davaoca elektronskih usluga od poverenja	CP = OJCA.y.a.b
Certificate Policy	OID koji označava CA telo koje je izdalo sertifikat ili servis za koji je izdat sertifikat	CP = OJCA.y.a.b.c
Certificate Policy	OID koji iznačava redni broj tipa sertifikata koji se izdaje ili OID koji označava verziju dokumenta davaoca elektronskih usluga od poverenja	CP = OJCA.y.a.b.c.N

2 Tipovi sertifikata, oblast primene sertifikata i način čuvanja privatnih ključeva

Grupe i tipovi sertifikata koje izdaje PKSCA		
Naziv grupe	**Naziv tipa sertifikata**	**PKSCA CP OID**
Sertifikat root CA tela	PKSCA Root CA sertifikat	PKSCA CP OID: nema
Sertifikat za podčinjena CA tela	PKSCA Class1, PKSCA Cloud CA i PKS TSA podčinjena tela sertifikati	PKSCA CP OID: nema
Sertifikati za OCSP servise	Sertifikat za PKSCA Class1 OCSP servis	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.1
	Sertifikat za PKSCA Cloud OCSP servis	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.1
	Sertifikat za PKSCA TSA OCSP servis	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.3.1
Sertifikati za elektronski potpis	Sertifikat za autentikaciju i enkripciju na smart kartici	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.2
	Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizička lica i ovlašćena lica u okviru pravnog lica na smart kartici	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.3
	Kvalifikovani sertifikat za kvalifikovani elektronski potpis za nerezidenta na smart kartici	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.4
	Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizička lica	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.2
	Kvalifikovani sertifikat za kvalifikovani elektronski potpis za ovlašćena lica u okviru pravnog lica u Cloud-u	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.3
	Kvalifikovani sertifikat za kvalifikovani elektronski potpis za nerezidenta u Cloud-u	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.4
	Kvalifikovani sertifikat za kvalifikovani elektronski potpis za nerezidenta u okkviru pravnog lica u Cloud-u	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.5
	Sertifikat za SIC	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.7
Sertifikati za elektronski pečat	Kvalifikovani sertifikat za kvalifikovani elektronski pečat za Time Stamp Unit	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.3.2
	Kvalifikovani sertifikat za kvalifikovani elektronski pečat za Signature Verification Authority Unit	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.5
	Kvalifikovani sertifikat za kvalifikovani elektronski pečat za pravna lica u Cloud-u	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.6

Područje primene, sredstvo zaštite privatnog ključa sertifikata, tip sertifkata i tip nosioca sertifikata koje izdaje NetSeT Root CA telo			
Naziv tipa sertifikata	**Područje primene sertifikata**	**Sredstvo zaštite privatnog ključa**	**Tip sertifkata i tip nosioca sertifikata**
Sertifikat za PKSCA Root CA	Self-sigend root CA sertifikat. Koristi se za izradu potpisa prilikom izdavanja sertifikata za podređeni CA i odgovarajući OCSP servis i za potpisivanje izdate CRL liste.	Odgovarajući token na HSM-u u PKSCA	Sertifikat sa pripadajućim parom ključeva na HSM-u
Sertifikat za PKSCA Class1 CA podređeno CA telo	Izdaje se podčinjenom PKSCA Class1 CA telu. Koristi se za izradu potpisa prilikom izdavanja sertifikata krajnjim korisnicima, odgovarajućim servisima i za potpisivanje CRL liste koju izdaje podređeno CA telo.	Odgovarajući token na HSM-u u PKSCA	Sertifikat sa pripadajućim parom ključeva na HSM-u
Sertifikat za PKSCA Cloud CA podređeno CA telo	Izdaje se podčinjenom PKSCA Cloud CA telu. Koristi se za izradu potpisa prilikom izdavanja sertifikata za potpis u oblaku i za potpisivanje CRL liste koju izdaje podređeno CA telo.	Odgovarajući token na HSM-u u PKSCA	Sertifikat sa pripadajućim parom ključeva na HSM-u
Sertifikat za PKSCA TSA CA podređeno CA telo	Izdaje se podčinjenom PKSCA TSA CA telu. Koristi se za izradu potpisa prilikom izdavanja sertifikata za Time Stamp servis i za potpisivanje CRL liste koju izdaje podređeno CA telo.	Odgovarajući token na HSM-u u PKSCA	Sertifikat sa pripadajućim parom ključeva na HSM-u
Sertifikat za PKSCA Class1 CA OCSP servis	Izdaje se OCSP servisu za potpis OCSP odgovora za status sertifikata koje izdaje PKSCA Class1 CA, osim za sam sertifikat OCSP servisa.	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa i ZMK ključa sa odgovarajućeg tokena HSM u PKSCA	Sertifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem
Sertifikat za PKSCA Cloud CA OCSP servis	Izdaje se OCSP servisu za potpis OCSP odgovora za status sertifikata koje izdaje PKSCA Cloud CA, osim za sam sertifikat OCSP servisa.	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa i ZMK ključa sa odgovarajućeg tokena HSM u PKSCA	Sertifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem
Sertifikat za PKSCA TSA CA OCSP servis	Izdaje se OCSP servisu za potpis OCSP odgovora za status sertifikata koje izdaje PKSCA TSA CA, osim za sam sertifikat OCSP servisa.	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa i ZMK ključa sa odgovarajućeg tokena HSM u PKSCA	Sertifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem
Kvalifikovani sertifikat za Time Stamp Unit pečat	Izdaje se TSA servisu za potrebe obezbeđivanja vremenskog žiga	Odgovarajući token na HSM-u u PKSCA	Sertifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem
Kvalifikovani sertifikat za Validation Unit pečat	Izdaje se VA servisu za potrebe pečaćenja izveštaja o validaciji elektronskog potpisa/pečata	Odgovarajući token na HSM-u u PKSCA	Sertifikat sa pripadajućim parom ključeva na HSM-u
Sertifikat za autentikaciju i enkripciju	Izdaje se kao drugi sertifikat krajnjim korisnicima na SSCD uređaju (smart kartici)	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa i ZMK ključa sa odgovarajućeg tokena HSM u PKSCA	Sertifikat sa pripadajućim parom ključeva u KMS aplikaciji zaštićen HSM uređajem
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizička lica i ovlašćena lica pravnog lica na smart karticama	Izdaje se krajnjim korisnicima – fizičkim licima za potpis na SSCD uređaju (smart kartici)	Ključ je pod zaštitom SSCD uređaja (smart kartice)	Sertifikat sa pripadajućim parom ključeva pod zaštitom SSCD uređaja (smart kartice)
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za nerezidente na smart karticama	Izdaje se krajnjim korisnicima – nerezidentima za potpis na SSCD uređaju (smart kartici)	Ključ je pod zaštitom SSCD uređaja (smart kartice)	Sertifikat sa pripadajućim parom ključeva pod zaštitom SSCD uređaja (smart kartice)

Područje primene, sredstvo zaštite privatnog ključa sertifikata, tip sertifkata i tip nosioca sertifikata koje izdaje NetSeT Root CA telo			
Naziv tipa sertifikata	**Područje primene sertifikata**	**Sredstvo zaštite privatnog ključa**	**Tip sertifkata i tip nosioca sertifikata**
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizička lica i ovlašćena lica u okviru pravnih lica u cloud-u	Izdaje se krajnjim korisnicima za potpis u oblaku. Izdaje ga PKSCA Cloud CA.	Ključ je pod zaštitom SAM-a i u skladu sa EN 419 241-2: 2019	Sertifikat sa odgovarajućim parom ključeva u SAM-u zaštićen HSM uređajem sertifikovanim po EN 419221-5
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za nerezidenta u cloud-u	Izdaje se krajnjim korisnicima za potpis u oblaku. Izdaje ga PKSCA Cloud CA.	Ključ je pod zaštitom SAM-a i u skladu sa EN 419 241-2: 2019	Sertifikat sa odgovarajućim parom ključeva u SAM-u zaštićen HSM uređajem sertifikovanim po EN 419221-5
Kvalifikovani sertifikat za kvalifikovani elektronski pečat za korisnike u cloud-u	Izdaje se krajnjim korisnicima za potpis u oblaku. Izdaje ga PKSCA Cloud CA.	Ključ je pod zaštitom SAM-a i u skladu sa EN 419 241-2: 2019	Sertifikat sa odgovarajućim parom ključeva u SAM-u zaštićen HSM uređajem sertifikovanim po EN 419221-5

3 Profili sertifikata

3.1 Profil sertifikata za root CA telo: PKSCA Root CA

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
SerialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifri)
SignatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
SignatureValue		Self-signed digital signature
Issuer	commonName	PKS CA Root
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja sertifikata
	notAfter	Vreme izdavanja sertifikata + 20 godina
Subject	commonName	PKS CA Root CA
	organizationName	Privredna komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
SubjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	4096 bit RSA public key

Ekstenzije		
Polje	**Kritično**	**Vrednost**
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280

3.2 Profil sertifikata za podređeno CA telo: PKSCA Class1 CA

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA Root
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 20 godina
Subject	commonName	PKS CA Class1
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA

	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	3072-bit RSA public key

Ekstenzije

Polje	Kritično	Vrednost	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLen=0	
certificatePolicies	NE	policyIdentifier	anyPolicy: 2.5.29.32.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: http://v3.pksca.rs/docs
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation:
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCARoot.crt
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs./crl/PKSCARoot.crl URI: http://crl.pksca.rs/v3/PKSCARoot.crl

3.3 Profil sertifikata za podređeno CA telo: PKSCA Cloud CA

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA Root CA
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 20 godina
Subject	commonName	PKS CA Cloud
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	3072-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Vrednost**	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLen=0	
certificatePolicies	NE	policyIdentifier	anyPolicy: 2.5.29.32.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: http://v3.pksca.rs/docs
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation:
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCARoot.crt
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs./crl/PKSCARoot.crl URI: http://crl.pksca.rs/v3/PKSCARoot.crl

3.4 Profil sertifikata za podređeno CA telo: PKSCA TSA

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA Root
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 20 godina
Subject	commonName	PKS CA TSA
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	3072-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Vrednost**	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLen=0	
certificatePolicies	NE	policyIdentifier	anyPolicy: 2.5.29.32.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: http://v3.pksca.rs/docs
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash as per RFC 5280	
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation:
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCARoot.crt
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs./crl/PKSCARoot.crl URI: http://crl.pksca.rs/v3/PKSCARoot.crl

3.5 Profil sertifikata za OCSP servis za PKSCA Class1 CA telo: PKSCA Class1 OCSP Servis

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA Class1
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	commonName	OCSP Server
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	digitalSignature nonRepudiation	Uključen digitalSignature bit, Non-Repudiation
extKeyUsage	DA	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.1 cPSuri: http://v3.pksca.rs/docs
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCAClass1.crl URI: http://crl.pksca.rs/v3/PKSCAClass1.crl
AuthorityKeyIdentifier SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
		keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/ocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCAClass1.crt

3.6 Profil sertifikata za OCSP servis za PKSCA Cloud CA telo: PKSCA Cloud OCSP Servis

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA Cloud
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	commonName	OCSP Cloud Server
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	digitalSignature nonRepudiation	Uključen digitalSignature bit, Non-Repudiation
extKeyUsage	DA	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.1 cPSuri: http://v3.pksca.rs/docs
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
		keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation:http://v3.pksca.rs/certs/PKSCACloud.crt

3.7 Profil sertifikata za OCSP servis za PKSCA TSA telo: PKSCA TSA OCSP Servis

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA TSA
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	commonName	PKS CA TSA OCSP Servis
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	digitalSignature nonRepudiation	Uključen digitalSignature bit, Non-Repudiation
extKeyUsage	DA	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.3.1 cPSuri: http://v3.pksca.rs/docs
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCATSA.crl URI: http://crl.pksca.rs/v3/PKSCATSA.crl
AuthorityKeyIdentifier SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
		keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/tsaocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCATSA.crt

3.8 Profil sertifikata za Time Stamp Unit: PKS TSA servis

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA TSA
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Privatekey Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 1 godina
	Common Name (CN=)	PKS QTSA Servis i broj servisa (rastući pozitivan ceo broj počevši od 1)
	Organizational Unit	PKS CA
	organizationName (O=)	Privredna Komora Srbije
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation Digital Signature	Uključen nonRepudiation bit, Digital Signature
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.3.2 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-legal-qscd, OID: 0.4.0.194112.1.3
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-eseal (0.4.0.1862.1.6.2)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCATSA.crl URI: http://crl.pksca.rs/v3/PKSCATSA.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/tsaocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCATSA.crt

3.9 Profil sertifikata za Verification Authority Unit: PKS QSVA Servis

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName	PKS CA Class 1
	organizationName	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	Serial Number (serialNumber=)	Jedinstveni serijski broj u okviru PKSCA: „PKS SVU „ i rastući pozitivan ceo broj počevši od 1
	Common Name (CN=)	PKS QSVA Servis
	Organizational Unit	PKS CA
	organizationName (O=)	Privredna Komora Srbije
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.5 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-legal-qscd, OID: 0.4.0.194112.1.3
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-eseal (0.4.0.1862.1.6.2)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCAClass1.crl URI: http://crl.pksca.rs/v3/PKSCAClass1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/ocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCAClass1.crt

3.10 Profil sertifikata za autentikaciju i enkripciju

Sertifikat za autentikaciju i enkripciju se izdaje uz kvalifikovane sertifikate za elektronski potpis fizičkim licima, fizičkim licima u okviru pravnog lica i nerezidentima. Iz tog razloga su pojedini atributi ovog sertifikata identični atributima sertifikata uz koji se izdaje.

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Class1
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godine
Subject	Serial Number (serialNumber=)	[1] "PNORS" i JMBG [2] "CA:RS-" i interni broj iz baze PKSCA
	Common Name (CN=)	Kao u sertifikatu uz koji se izdaje
	organizationalIdentifier:	Kao u sertifikatu uz koji se izdaje
	OrganizationName (O=)	Kao u sertifikatu uz koji se izdaje
	OrganizationUnit (OU=)	Kao u sertifikatu uz koji se izdaje
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	NE	Key Encipherment, Digital Signature	Uključen key Encipherment, Digital Signature
extKeyUsage	NE	Client Authentication, Microsoft Smartcard Login	Ukljucen Client Auth, Microsoft Smart Card Logon
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.2 cPSuri: http://v3.pksca.rs/docs
CRLDistributionPoints	NE	DistributionPoint	[1] URI: URI: http://v3.pksca.rs/crl/PKSCAClass1.crl URI: http://crl.pksca.rs/v3/PKSCAClass1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/ocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCAClass1.crt

3.11 Profil sertifikata za elektronski potpis za fizička lica i ovlašćena lica u okviru pravnog lica na smart karticama

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Class1
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godine
Subject	serialNumber (serialNumber=)	[1] "PNORS" i JMBG [2] "CA:RS-" i interni broj iz baze PKSCA
	commonName (CN=)	Ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	givenName	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname (SN=)	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	Za ovlašćena lica u okviru pravnog lica: [1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Za ovlašćena lica u okviru pravnog lica: Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Za fizička lica: Mesto prebivališta korisnika Za ovlašćena lica u okviru pravnog lica: Sedište pravnog lica
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.3 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-natural, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: URI: http://v3.pksca.rs/crl/PKSCAClass1.crl URI: http://crl.pksca.rs/v3/PKSCAClass1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/ocsp

Access		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCAClass1.crt

3.12 Profil sertifikata za elektronski potpis za nerezidenta na smart karticama

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Class1
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godine
Subject	serialNumber (serialNumber=)	[1] "PAS" i dvoslovčana ISO oznaka države koja je izdala putnu ispravu i broj putne isprave [2] "CA:RS-" i interni broj iz baze PKSCA
	commonName (CN=)	Ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	givenName	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname (SN=)	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	[1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Sedište pravnog lica
	countryName	Dvoslovčana ISO oznaka države koja je izdala putnu ispravu
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.1.4 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-natural, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCAClass1.crl URI: http://crl.pksca.rs/v3/PKSCAClass1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/ocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCAClass1.crt

Dodatne ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
PassportNumber	NE	OID 1.3.6.1.0.1	Broj putne isprave
PassportIssuer	NE	OID 1.3.6.1.0.2	Oznaka zemlje koja je izdala putnu ispravu
PassportDate	NE	OID 1.3.6.1.0.3	Datum do koga važi putna isprava

3.13 Profil sertifikata za elektronski potpis fizičkog lica

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Cloud CA
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	serialNumber (serialNumber=)	[1] "PNORS" i JMBG [2] "CA:RS-" i interni broj iz baze PKSCA
	commonName (CN=)	Ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	givenName	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname (SN=)	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	Za ovlašćena lica u okviru pravnog lica: [1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Za ovlašćena lica u okviru pravnog lica: Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Za fizička lica: Mesto prebivališta korisnika Za ovlašćena lica u okviru pravnog lica: Sedište pravnog lica
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.2 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-natural-qscd, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCACloud.crt

3.14 Profil sertifikata za elektronski potpis ovlašćenog lica u okviru pravnog lica u cloud-u

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Cloud CA
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	serialNumber (serialNumber=)	[1] "PNORS" i JMBG [2] "CA:RS-" i interni broj iz baze PKSCA
	commonName (CN=)	Ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	givenName	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname (SN=)	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	Za ovlašćena lica u okviru pravnog lica: [1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Za ovlašćena lica u okviru pravnog lica: Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Za fizička lica: Mesto prebivališta korisnika Za ovlašćena lica u okviru pravnog lica: Sedište pravnog lica
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.3 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-natural-qscd, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None

Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCACloud.crt

3.15 Profil sertifikata za nerezidenta u cloud-u

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Cloud CA
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	serialNumber (serialNumber=)	[1] "PAS" i dvoslovčana ISO oznaka države koja je izdala putnu ispravu i broj putne isprave [2] "CA:RS-" i interni broj iz baze PKSCA
	commonName (CN=)	Ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	givenName	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname (SN=)	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	[1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Sedište pravnog lica
	countryName	Dvoslovčana ISO oznaka države koja je izdala putnu ispravu
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.4 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-natural-qscd, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCACloud.crt

Dodatne ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
PassportNumber	NE	OID 1.3.6.1.0.1	Broj putne isprave
PassportIssuer	NE	OID 1.3.6.1.0.2	Oznaka zemlje koja je izdala putnu ispravu
PassportDate	NE	OID 1.3.6.1.0.3	Datum do koga važi putna isprava

3.16 Profil sertifikata za nerezidenta u okviru pravnog lica u cloud-u

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Cloud CA
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	serialNumber (serialNumber=)	[1] "PAS" i dvoslovčana ISO oznaka države koja je izdala putnu ispravu i broj putne isprave [2] "CA:RS-" i interni broj iz baze PKSCA
	commonName (CN=)	Ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	givenName	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname (SN=)	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	[1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Sedište pravnog lica
	countryName	Dvoslovčana ISO oznaka države koja je izdala putnu ispravu
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation, Digital Signature
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.5 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-natural-qscd, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx

		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCACloud.crt

Dodatne ekstenzije

Polje	Kritično	Atribut	Vrednost
PassportNumber	NE	OID 1.3.6.1.0.1	Broj putne isprave
PassportIssuer	NE	OID 1.3.6.1.0.2	Oznaka zemlje koja je izdala putnu ispravu
PassportDate	NE	OID 1.3.6.1.0.3	Datum do koga važi putna isprava

3.17 Profil sertifikata za elektronski pečat u cloud-u

Osnovna polja			
Polje	**Atribut**		**Vrednost**
Version	Version		X.509 V3
serialNumber	CertificateSerialNumber		9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier		SHA256withRSA
signatureValue			Potpis izdavaca certifikata
Issuer	commonName (CN)		PKSCA Cloud CA
	organizationName (O)		Privredna Komora Srbije
	Organizational Unit		PKS CA
	countryName (C)		RS
Validity	notBefore		Vreme izdavanja certifikata
	notAfter		Vreme izdavanja certifikata + 5 godina
Subject	serialNumber (serialNumber=)		Jedinstveni serijski broj u okviru PKSCA sistema
	commonName (CN=)		Naziv korisnika kako je navedeno u identifikadionoj ispravi
	organizationalIdentifier		[1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)		Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)		Sedište pravnog lica
	countryName		RS
subjectPublic KeyInfo	AlgorithmIdentifier		RSA
	subjectPublicKey		2048-bit RSA public key
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation, Digital Signature	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.6 cPSuri: http://v3.pksca.rs/docs
		policyIdentifier	eIDAS OID: qcp-legal-qscd, OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		esi4-qcStatement-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		esi4-qcStatement-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) [1] URI: http://v3.pksca.rs/docs/PKI_DISCLOSURE_STATEMENT_PKSCA.docx
		esi4-qcStatement-6	QCstatement QcType (0.4.0.1862.1.6) id-etsi-qct-eseal (0.4.0.1862.1.6.2)
CRLDistributionPoints	NE	DistributionPoint	[1 URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCACloud.crt

3.18 Profil sertifikata za SIC

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	9 okteta, serijski broj je uvek pozitivana vrednost (18 hexadecimalnih cifara)
signatureAlgorithm	AlgorithmIdentifier	SHA256withRSA
signatureValue		Potpis izdavaca certifikata
Issuer	commonName (CN)	PKS CA Cloud CA
	organizationName (O)	Privredna Komora Srbije
	Organizational Unit	PKS CA
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja certifikata
	notAfter	Vreme izdavanja certifikata + 5 godina
Subject	serialNumber (serialNumber=)	Jedinstveni serijski broj u okviru PKSCA sistema
	commonName (CN=)	Naziv korisnika kako je navedeno u identifikadionoj ispravi
	Given Name	Ime fizičkog lica kako je navedeno u identifikacionoj ispravi
	Surname	Prezime fizičkog lica kako je navedeno u identifikacionoj ispravi
	organizationalIdentifier	[1] "VATRS-" i PIB (poreski identifikacioni broj pravnog lica) [2] "MB:RS-" i MB (matični broj pravnog lica)
	OrganizationName (O=)	Puni ili skraćeni registrovani naziv pravnog lica
	localityName (L=)	Sedište pravnog lica
	countryName	RS
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	NE	Digital Signature, Key Encipherment	
Extended Key Usage	NE	Client Authentication	
certificatePolicies	NE	policyIdentifier	PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.3.1.0.2.7 cPSuri: http://v3.pksca.rs/docs
CRLDistributionPoints	NE	DistributionPoint	[1 URI: http://v3.pksca.rs/crl/PKSCACloud.crl URI: http://crl.pksca.rs/v3/PKSCACloud.crl
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://v3.pksca.rs/cloudocsp
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://v3.pksca.rs/certs/PKSCACloud.crt