Crna Gora

Ministarstvo unutrašnjih poslova

TrustME - Pregled profila certifikata

Verzija. 1.2

Podgorica, mart 2020. godine.

Sadržaj

Struktura OID brojeva za dodjeljivanje Certificate Policy OID brojeva

Struktura CP OID		
NAZIV GRUPE	**NAZIV GRANE OID-a**	**OID**
MUP-PEN	Private enterprise number MUP ME	MUP-PEN
Organizaciona jedinica MUP za izdavanje certifikata	OID grana dodijeljena organizacionoj jedinici nadležnoj za izdavanje certifikata	OJCA = MUP-PEN.1
Certificate Policies	OID grana namijenjena za dodjeljivanje polisa certifikata	CPs = OJCA.1
Certificate Authority	OID grana koja označava konkretno CA tijelo	CAs = CPs.x
Certificate Policy	OID koji označava konkretnu CP	CP = CAs.y

Tipovi certifikata, oblast primjene certifikata i način čuvanja privatnih ključeva

Tipovi certifikata koje izdaje MNE eID Root CA		
NAZIV GRUPE	**NAZIV TIPA CERTIFIKATA**	**MNE eID CERTIFICATE POLICY OID**
Certifikat root CA tela	MNE eID root CA certifikat	
Certifikat za podčinjena CA tela	MNE eID podređeni CA certifikat	anyPolicy: 2.5.29.32.0
Certifikati za servise	Certifikat za OCSP servis root CA tela	1.3.6.1.4.1.54748.1.1.1.1

Tipova certifikata koje izdaje MNE eID CA 1		
NAZIV GRUPE	**NAZIV TIPA CERTIFIKATA**	**MNE eID CERTIFICATE POLICY OID**
Kvalifikovani certifikati za fizička lica	Kvalifikovani certifikat za kvalifikovani elektronski potpis (QCP-n-qscd)	1.3.6.1.4.1.54748.1.1.2.2
	Certifikat za elektronsku identifikaciju (NCP+)	1.3.6.1.4.1.54748.1.1.2.3
Certifikati za servise	Certifikat za OCSP servis podčinjenog CA tela	1.3.6.1.4.1.54748.1.1.2.1

Područje primjene i sredstvo zaštite privatnog ključa certifikata koje izdaju MNE eID PKI CA tela		
NAZIV CERTIFIKATA	**PODRUČJE PRIMJENE CERTIFIKATA**	**SREDSTVO ZAŠTITE PRIVATNOG KLJUČA**
MNE eID root CA certifikat	Self-sigend root CA certifikat. Koristi se za izradu potpisa prilikom izdavanja certifikata za subordinirani CA i odgovarajući OCSP servis i za potpisivanje izdate CRL liste.	Odgovarajući token na HSM modulu u MUP ME
MNE eID CA1 podčinjeno tijelo certifikat	Izdaje se podređenom MNE eID CA1. Koristi se za izradu potpisa prilikom izdavanja certifikata fizičkim licima, odgovarajućem OCSP servisu i za potpisivanje CRL liste koju izdaje podređeni CA.	Odgovarajući token na HSM modulu u MUP ME
Certifikat za OCSP servis root CA tela	Izdaje se OCSP servisu za potpis OCSP odgovora za status certifikata koje izdaje MUP Root CA, osim za sam certifikat OCSP servisa.	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa sa odgovarajućeg tokena HSM modula u MUP ME

Kvalifikovani certifikat za kvalifikovani elektronski potpis (QCP-n-qscd)	Izdaje se fizičkim licima – građanima. Koristi se za izradu kvalifikovanog elektronskog potpisa koji je definisan u Zakonu o elektronskoj identifikaciji i elektronskom potpisu član 11 i u skladu sa eIDAS regulativom.	QSCD uređaj (lična karta)
Certifikat za elektronsku identifikaciju (NCP+)	Izdaje se fizičkim licima – građanima. Koristi se za jaku autentifikaciju na bazi nekvalifikovanog certifikata u skladu sa eIDAS regulativom.	QSCD uređaj (lična karta)
Certifikat za OCSP servis podčinjenog CA tela	Izdaje se OCSP servisu za potpis OCSP odgovora za status certifikata koje izdaje MUP Subordinirani CA, osim za sam certifikat OCSP servisa.	Ključ je pod zaštitom KMS modula, upotrebom KEK ključa sa odgovarajućeg tokena HSM modula u MUP ME

Profil certifikata za root CA tijelo: **MNE eID 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	MNE eID Root CA
	organizationName	Ministarstvo unutrašnjih poslova
	organizationalIdentifier	VATME-02016010
	countryName	ME
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 30 godina i 3 mjeseca
Subject	commonName	MNE eID Root CA
	organizationName	Ministarstvo unutrašnjih poslova
	organizationalIdentifier	VATME-02016010
	countryName	ME
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	3072-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

Profil certifikata za OCSP servis za root CA tijelo: **MNE eID Root CA OCSP Servis**

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			Potpis izdavaca certifikata
Issuer	commonName (CN)		MNE eID Root CA
	organizationName (O)		Ministarstvo unutrašnjih poslova
	orgazinationalIdentifier		VATME-02016010
	countryName (C)		ME
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 3 mjeseca
Subject	commonName (CN)		MNE eID Root CA OCSP Servis
	organizationName (O)		Ministarstvo unutrašnjih poslova
	organizationalIdentifier		VATME-02016010
	countryName (C)		ME
subjectPublic KeyInfo	AlgorithmIdentifier		RSA
	subjectPublicKey		2048-bit RSA javni kljuc
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	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	MNE eID PKI CP OID: 1.3.6.1.4.1.54748.1.1.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: https://ca.elk.gov.me/cpcps/
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.elk.gov.me/crl/MNEeIDRootCA.crl URI: ldap://ldap.elk.gov.me/CN=MNE eID Root CA,O=Ministarstvo unutrašnjih poslova,2.5.4.97=VATME-02016010,C=ME?certificateRevocationList;binary
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://ocsp.elk.gov.me/MNEeIDRootCAOCSP
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: ldap://ldap.elk.gov.me/CN=MNE eID Root CA,O=Ministarstvo unutrašnjih poslova,organizationIdentifier=VATME-02016010,C=ME?cACertificate;binary
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.elk.gov.me/cacert/MNEeIDRootCA.cer

Profil CRL liste koju izdaje MNE eID Root CA tijelo

Osnovna polja			
Polje	**Atribut**		**Vrednost**
Version	Version		X.509 V2
signatureAlgorithm	AlgorithmIdentifier		SHA256withRSA
signatureValue			Potpis izdavaca CRL liste
Issuer	commonName (CN)		MNE eID Root CA
	organizationName (O)		Ministarstvo unutrašnjih poslova
	organizationalIdentifier		VATME-02016010
	countryName (C)		ME
	thisUpdate		Vrijeme izdavanja CRL liste
	nextUpdate		Vrijeme izdavanja CRL liste + 6 mjeseci
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**

CRLNumber	NE	CRL Number	Monotono rastuci pozitivan broj, početna vrednost 1
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
ReasonCode	NE	reasonCode	Kod razloga opoziva certifikata

Profil certifikata za podređeno CA tijelo: **MNE eID CA1**

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		Potpis izdavaca certifikata	
Issuer	commonName	MNE eID Root CA	
	organizationName	Ministarstvo unutrašnjih poslova	
	organizationalIdentifier	VATME-02016010	
	countryName	ME	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 20 godina + 3 mjeseca	
Subject	commonName	MNE eID CA1	
	organizationName	Ministarstvo unutrašnjih poslova	
	organizationalIdentifier	VATME-02016010	
	countryName	ME	
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: https://ca.elk.gov.me/cpcps/
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: http://ocsp.elk.gov.me/MNEeIDRootCAOCSP
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: ldap://ldap.elk.gov.me/CN=MNE eID Root CA,O=Ministarstvo unutrašnjih poslova,organizationIdentifier=VATME-02016010,C=ME?cACertificate;binary
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.elk.gov.me/cacert/MNEeIDRootCA.cer
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.elk.gov.me/crl/MNEeIDRootCA.crl URI: ldap://ldap.elk.gov.me/CN=MNE eID Root CA,O=Ministarstvo unutrašnjih poslova, 2.5.4.97=VATME-02016010,C=ME?certificateRevocationList;binary

Profil certifikata za elektronsku identifikaciju

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			Potpis izdavaca certifikata
Issuer	commonName (CN)		MNE eID CA1
	organizationName (O)		Ministarstvo unutrašnjih poslova
	organizationalIdentifer		VATME-02016010
	countryName (C)		ME
Validity	notBefore		Punoljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata Maloljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata
	notAfter		Punoljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata + 10 godina (važenje lične karte) Maloljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata + 10 godina (važenje lične karte)
Subject	serialNumber		Osmocifreni jedinstveni identifikator korisnika definisan clanom 4. Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog certifikata za elektronski potpis sa prefiksom „**PNOME–**“
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u dokumentu kojim se dokazuje identitet i namjena certifikata: CN=Ime Prezime IDENTITET
	givenName (G)		Ime(na) potpisnika kako je navedeno u dokumentu kojim se dokazuje identitet
	surname (SN)		Prezime(na) potpisnika kako je navedeno u dokumentu kojim se dokazuje identitet
	countryName (C)		ME
subjectPublic KeyInfo	AlgorithmIdentifier		RSA
	subjectPublicKey		2048-bit RSA public key
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	MNE eID PKI CP OID: 1.3.6.1.4.1.54748.1.1.2.3
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://ca.elk.gov.me/cpcps/
		policyIdentifier	eIDAS OID: ncpplus (2), OID: 0.4.0.2042.1.2
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://ca.elk.gov.me/crl/MNEeIDCA1.crl URI:ldap://ldap.elk.gov.me/CN=MNE eID CA1, O=Ministarstvo unutrašnjih poslova, 2.5.4.97=VATME-02016010,C=ME?certificateRevocationList;binary
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 Path Length Constraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.elk.gov.me/MNEeIDCA1OCSP
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: ldap://ldap.elk.gov.me/CN=MNE

			eID CA1,O=Ministarstvo unutrašnjih poslova,organizationIdentifier=VATME-02016010,C=ME?cACertificate;binary
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.elk.gov.me/cacert/MNEeIDCA1.cer

Profil certifikata za kvalifikovani elektronski potpis

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		Potpis izdavaca certifikata
Issuer	commonName (CN)	MNE eID CA1
	organizationName (O)	Ministarstvo unutrašnjih poslova
	organizationalIdentifier	VATME-02016010
	countryName (C)	ME
Validity	notBefore	Punoljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata Maloljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme sticanja punoljetstva
	notAfter	Punoljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata + 10 godina (važenje lične karte) Maloljetno fizičko lice u vrijeme izdavanja lične karte: Vrijeme izdavanja certifikata + 10 godina (važenje lične karte) Napomena: certifikat će važiti manje od 10 godina, da datuma važenja lične karte
Subject	serialNumber	Osmocifreni jedinstveni identifikator korisnika definisan članom 4. Uredbe o načinu određivanja identifikacionog broja potpisnika kvalifikovanog certifikata za elektronski potpis sa prefiksom „**PNOME–**“
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u dokumentu kojim se dokazuje identitet i namjena certifikata: CN=Ime Prezime POTPIS
	givenName (G)	Ime(na) potpisnika kako je navedeno u dokumentu kojim se dokazuje identitet
	surname (SN)	Prezime(na) potpisnika kako je navedeno u dokumentu kojim se dokazuje identitet
	countryName (C)	ME
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	2048-bit RSA public key

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	MNE eID PKI CP OID: 1.3.6.1.4.1.54748.1.1.2.2

		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://ca.elk.gov.me/cpcps/
		policyIdentifier	eIDAS OID: qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://ca.elk.gov.me/pds/PDS-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://ca.elk.gov.me/crl/MNEeIDCA1.crl URI:ldap://ldap.elk.gov.me/CN=MNE eID CA1, O=Ministarstvo unutrašnjih poslova, 2.5.4.97=VATME-02016010,C=ME?certificateRevocationList;binary
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://ocsp.elk.gov.me/MNEeIDCA1OCSP
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: ldap://ldap.elk.gov.me/CN=MNE eID CA1,O=Ministarstvo unutrašnjih poslova,organizationIdentifier=VATME-02016010,C=ME?cACertificate;binary
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.elk.gov.me/cacert/MNEeIDCA1.cer

Profil certifikata za **MNE eID CA1** OCSP servis

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			Potpis izdavaca certifikata
Issuer	commonName (CN)		MNE eID CA1
	organizationName (O)		Ministarstvo unutrašnjih poslova
	OrganizationalIdentifier		VATME-02016010
	countryName (C)		ME
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 3 mjeseca
Subject	commonName (CN)		MNE eID CA1 OCSP Servis
	organizationName (O)		Ministarstvo unutrašnjih poslova
	organizationIdentifier		VATME-02016010
	countryName (C)		ME
subjectPublic KeyInfo	AlgorithmIdentifier		RSA
	subjectPublicKey		2048-bit RSA javni kljuc
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	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	MNE eID PKI CP OID: 1.3.6.1.4.1.54748.1.1.2.1

		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1} cPSuri: https://ca.elk.gov.me/cpcps/
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://ca.elk.gov.me/crl/MNEeIDCA1.crl URI:ldap://ldap.elk.gov.me/CN=MNE eID CA1, O=Ministarstvo unutrašnjih poslova, 2.5.4.97=VATME-02016010, C=ME?certificateRevocationList;binary
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://ocsp.elk.gov.me/MNEeIDCA1OCSP
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: ldap://ldap.elk.gov.me/CN=MNE eID CA1,O=Ministarstvo unutrašnjih poslova,organizationIdentifier=VATME-02016010,C=ME?cACertificate;binary
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://ca.elk.gov.me/cacert/MNEeIDCA1.cer

Profil CRL liste koju izdaje MNE eID CA1 podređeno CA tijelo

Osnovna polja			
Polje	**Atribut**		**Vrednost**
Version	Version		X.509 V2
signatureAlgorithm	AlgorithmIdentifier		SHA256withRSA
signatureValue			Potpis izdavaca CRL liste
Issuer	commonName (CN)		MNE eID CA1
	organizationName (O)		Ministarstvo unutrašnjih poslova
	OrganizationalIdentifier		VATME-02016010
	countryName (C)		ME
	thisUpdate		Vrijeme izdavanja CRL liste
	nextUpdate		Vrijeme izdavanja CRL liste + 24hr
Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrijednost**
CRLNumber	NE	CRL Number	Monotono rastuci pozitivan broj, početna vrednost 1
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash as per RFC 5280
ReasonCode	NE	reasonCode	Kod razloga opoziva certifikata