Slovenská národná certifikačná autorita

Profily
používaných a vydávaných certifikátov SNCA

Vypracoval: Marek Žáčik, Štefan Szilva
Dátum: 12.07.2023
Verzia: 1.2

Obsah

1. Profily vydávaných certifikátov

1.1. Profil vydávajúcej CA – SNCA4

Basic Fields	Critical	Attribute	Value
Version			V3(0x2)
Serial number			automatically assigned number
Signature algorithm			sha512WithRSAEncryption
Issuer			C=SK, OU=SNCA 2.5.4.97=NTRSK-42156424, O=Narodna agentura pre sietove a elektronicke sluzby, CN=SNCA4
Validity		notBefore	validity period begin date (UTC time)
		notAfter	validity period end date (UTC time)
Subject			C=SK OU=SNCA 2.5.4.97=NTRSK-42156424 O=Narodna agentura pre sietove a elektronicke sluzby CN=SNCA4
Public key			public key value and signature algorithm (rsaEncryption, 4096bit)
Extensions			
Subject Key Identifier	No		the 160 bit hash value of issuer public key
Certificate policies	No		Policy: 1.3.158.42156424.0.1.1 CPS: https://snca.gov.sk/cps/cps_snca.pdf
Key Usage	Yes		Certificate Signing, CRL Signing (06)
Basic Constraints	Yes		CA:TRUE pathlen:0

1.2. Kvalifikované certifikáty (KC) pre kvalifikované elektronické pečate (KEPe)

Použité profily vydavateľa:

- KC pre KEPe Gemalto
- KC pre KEPe ProID+Q
- KC pre KEPe HSM
- KC pre KEPe v QSCD

Spoločné atribúty:

Basic Fields	Critical	Attribute	Value
Version			V3(2)
Serial number			automatically assigned number
Signature algorithm			sha256WithRSAEncryption
Issuer			C=SK OU=SNCA/organizationIdentifier=NTRSK-42156424 O=Narodna agentura pre sietove a elektronicke sluzby CN=SNCA4
Validity		notBefore	validity period begin date (UTC time)
		notAfter	validity period end date (UTC time)
Subject		commonName	CN=Common name
		organizationName	O=OrganizationName
		organizationUnit	OU=Organization Unit name
		organizationIdentifier	OrganizationIdentifier=NTRSK-Legal person number (IČO)
		locality	L=locality/city
		countryName	C=SK
Public key			public key value and signature algorithm (rsaEncryption 3072 bit - Monet or 4096bit - Gemalto)
Extensions			
Authority Information Access	No	OCSP	URI:http://snca4-ocsp.snca.gov.sk/ocsp/snca4
		CA Issuers	URI:http://cdp.snca.gov.sk/snca4/cert/snca4.der DirName:/serialNumber=TLISK-132
Subject Key Identifier	No	keyIdentifier	the 160 bit hash value of public key
Authority Key Identifier	No	keyIdentifier	the 160 bit hash value of issuing CA public key
Basic Constrains	Yes		CA: false
Certificate Policies	No	policyIdentifier	1.3.158.36061701.0.0.0.1.2.2
		policyIdentifier	1.3.158.42156424.0.1.1
		CPS	https://snca.gov.sk/cps/cps_snca.pdf
	No	Full Name	URI:http://cdp1.snca.gov.sk/snca4/crl/snca4.crl

CRL Distribution Points		Full Name	URI:http://cdp2.snca.gov.sk/snca4/crl/snca4.crl
Key Usage	Yes		Digital Signature, Non-Repudiation
Qualified Certificate Statement	No	EU Qualified Certificate statement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		QC Type	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

1.3. Mandátne kvalifikované certifikáty pre kvalifikovaný elektronický podpis

Vydávané profily:

- MKC pre KEP pre MV SR
- MKC pre KEP pre OVM Gemalto
- MKC pre KEP pre OVM ProID+Q

Spoločné atribúty:

Basic Fields	Critical	Attribute	Value
Version			V3(2)
Serial number			automatically assigned number
Signature algorithm			sha256WithRSAEncryption
Issuer			C=SK OU=SNCA/organizationIdentifier=NTRSK-42156424 O=Narodna agentura pre sietove a elektronicke sluzby CN=SNCA4
Validity		notBefore	validity period begin date (UTC time)
		notAfter	validity period end date (UTC time)
Subject		countryName	C=SK
		givenName	G= Name (Meno)
		surname	SN=Surname (Priezvisko)
		serialNumber	SERIALNUMBER=Natural person semantics identifier – 3 characters representing identifier type, followed by country code „SK-“, followed by identification number (e.g.passport number, Identity card number or personal identification number)
		title	T=Title contains mandate (Názov mandátu)
		organizationName	O=text “MANDANT“ followed by OrganizationName (Názov organizácie)
		organizationIdentifier	OrganizationIdentifier =MANDANT NTRSK-Legal person ID Number (IČO)
		locality	L=locality/city
		commonName	CN= Name of the subject followed by text OPRÁVNENIE, number and name of the mandate
Public key			public key value and signature algorithm (rsaEncryption 3072 bit - Monet or 4096bit - Gemalto)
Extensions			
Authority Information Access	No	OCSP	URI:http://snca4-ocsp.snca.gov.sk/ocsp/snca4
		CA Issuers	URI:http://cdp.snca.gov.sk/snca4/cert/snca4.der DirName:/serialNumber=TLISK-132

Subject Key Identifier	No	keyIdentifier	the 160 bit hash value of public key
Authority Key Identifier	No	keyIdentifier	the 160 bit hash value of issuing CA public key keyid:
Basic Constrains	Yes	CA	False
Certificate Policies	No	Policy	policyIdentifier: 1.3.158.36061701.0.0.0.1.2.2
		Policy	policyIdentifier: 1.3.158.42156424.0.1.1 CPS: https://snca.gov.sk/cps/cps_snca.pdf User Notice: Explicit Text: Kvalifikovaný mandátny certifikát podľa zákona č. 272/2016 Z. z. EN: Qualified certificate of mandant pursuant to Act No. 272/2016 Coll.
		Policy	policyIdentifier: mandate OID - 1.3.158.36061701.1.1.xyz (xyz stands for mandate ID) User Notice: Mandate description User Notice: Mandate description 2
CRL Distribution Points	No	Full Name	URI:http://cdp1.snca.gov.sk/snca4/crl/snca4.crl
		Full Name	URI:http://cdp2.snca.gov.sk/snca4/crl/snca4.crl
Key Usage	Yes		Digital Signature, Non-Repudiation
Qualified Certificate Statement	No	EU Qualified Certificate statement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		QC Type	id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-qct-eSign (0.4.0.1862.1.6.1)

1.4. Kvalifikované zamestnanecké certifikáty pre kvalifikovaný elektronický podpis

Ide o certifikáty, ktoré nespĺňajú požiadavky § 8 zákona č. 272/2016 Z. z.

Vydávané profily:

- KC pre KEP za organizáciu

Spoločné atribúty:

Basic Fields	Critical	Attribute	Value
Version			V3(2)
Serial number			automatically assigned number
Signature algorithm			sha256WithRSAEncryption
Issuer			C=SK OU=SNCA/organizationIdentifier=NTRSK-42156424 O=Narodna agentura pre sietove a elektronicke sluzby CN=SNCA4
Validity		notBefore	validity period begin date (UTC time)
		notAfter	validity period end date (UTC time)
Subject		countryName	C=SK
		givenName	G= Name (Meno)
		surname	SN=Surname (Priezvisko)
		serialNumber	SERIALNUMBER=Natural person semantics identifier – 3 characters representing identifier type, followed by country code „SK-“, followed by identification number (e.g.passport number, Identity card number or personal identification number)
		title	T=Title (pracovná pozícia alebo činnosť v organizácii na základe predloženého dokladu)
		organizationName	O=OrganizationName (Názov organizácie)
		organizationIdentifier	OrganizationIdentifier = NTRSK-Legal person ID Number (IČO)
		locality	L=locality/city
		commonName	CN= Name of the subject (titul, meno, priezvisko)
Public key			public key value and signature algorithm (rsaEncryption 3072 bit - Monet or 4096bit - Gemalto)
Extensions			
Authority Information Access	No	OCSP	URI:http://snca4-ocsp.snca.gov.sk/ocsp/snca4
		CA Issuers	URI:http://cdp.snca.gov.sk/snca4/cert/snca4.der DirName:/serialNumber=TLISK-132

Subject Key Identifier	No	keyIdentifier	the 160 bit hash value of public key
Authority Key Identifier	No	keyIdentifier	the 160 bit hash value of issuing CA public key keyid:
Basic Constrains	Yes	CA	False
Certificate Policies	No	Policy	policyIdentifier: 1.3.158.36061701.0.0.0.1.2.2
		Policy	policyIdentifier: 1.3.158.42156424.0.1.1 CPS: https://snca.gov.sk/cps/cps_snca.pdf
CRL Distribution Points	No	Full Name	URI:http://cdp1.snca.gov.sk/snca4/crl/snca4.crl
		Full Name	URI:http://cdp2.snca.gov.sk/snca4/crl/snca4.crl
Key Usage	Yes		Digital Signature, Non-Repudiation
Qualified Certificate Statement	No	EU Qualified Certificate statement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		SSCD statement	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
		QC Type	id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qcs-qct-eSign (0.4.0.1862.1.6.1)

1.5. Kvalifikované certifikáty pre autentifikáciu webových sídiel

Basic Fields	Critical	Attribute	Value
Version			V3(2)
Serial number			automatically assigned number
Signature algorithm			sha256WithRSAEncryption
Issuer			C=SK OU=SNCA/organizationIdentifier=NTRSK-42156424 O=Narodna agentura pre sietove a elektronicke sluzby CN=SNCA4
Validity		notBefore	validity period begin date (UTC time)
		notAfter	validity period end date (UTC time)
Subject		commonName	CN= Fully-qualified domain name / FQDN (webové sídlo držiteľa certifikátu)
		organizationName	O=OrganizationName
		organizationUnitName	OU=Organization Unit name
		organizationIdentifier	OrganizationIdentifier=NTRSK-Legal person number (IČO)
		locality	L=locality/city
		countryName	C=SK
Public key			public key value and signature algorithm (rsaEncryption 3072bit)
Extensions			
Authority Information Access	No	OCSP	URI:http://snca4-ocsp.snca.gov.sk/ocsp/snca4
		CA Issuers	URI:http://cdp.snca.gov.sk/snca4/cert/snca4.der DirName:/serialNumber=TLISK-132
Subject Key Identifier	No	keyIdentifier	the 160 bit hash value of public key
Authority Key Identifier	No	keyIdentifier	the 160 bit hash value of issuing CA public key
Basic Constrains	Yes		CA: false
Certificate Policies	No	policyIdentifier	1.3.158.36061701.0.0.0.1.2.2
		policyIdentifier	1.3.158.42156424.0.1.1
		CPS	https://snca.gov.sk/cps/cps_snca.pdf
CRL Distribution Points	No	Full Name	URI:http://cdp1.snca.gov.sk/snca4/crl/snca4.crl
		Full Name	URI:http://cdp2.snca.gov.sk/snca4/crl/snca4.crl
Key Usage	Yes		Digital Signature, Non-Repudiation
Extended Key Usage	No		Server authentication

Qualified Certificate Statement	No	EU Qualified Certificate statement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
		QC Type	id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qct-web (0.4.0.1862.1.6.3)
Subject Alternative Name	No	DNS	DNS: URL