E-Smart Systems d.o.o. | **Adresa:** Kneza Višeslava 70a, 11030 Beograd, Srbija | **Sertifikaciono telo (ESS QCA)** | **Tel:** 011 3050280, **Fax:** 011 3050222
E-mail: qca@e-smartsys.com | **Matični broj:** 17247565, **PIB:** 101833141, **Šifra delatnosti:** 6201

L-QCA-190

Šifra dokumenta

Politika izdavanja kvalifikovanih sertifikata za elektronski potpis

(CP - Certificate Policy)

OID politike izdavanja (1.3.6.1.4.1.30496.509.1.1.2)
– verzija 2.6 –

Beograd, 15. januar 2021.

Sadržaj

1. Uvod

E-Smart Systems DOO BEOGRAD – E-SMART SYSTEMS DOO BEOGRAD sertifikaciono telo (u daljem tekstu: **ESS QCA**) donosi **Politiku izdavanja kvalifikovanih sertifikata za elektronski potpis** u skladu sa:

- Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima Republike Srbije uključujući, ali se ne ograničavajući na Uredbu o uslovima za pružanje kvalifikovanih usluga od poverenja, Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati i Pravilnik o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo (u daljem tekstu - **Zakon**),
- Zakonom referenciranom Uredbom EU br. 910/2014 Evropskog parlamenta i Saveta (u daljem tekstu – **eIDAS**):
- Standardima referenciranim Zakonom i/ili eIDAS-om uključujući, ali se ne ograničavajući na (u daljem tekstu - **Standardi**):
    - ETSI EN 319 401 „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“
    - ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“
    - ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates“
    - ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“
    - ETSI TS 119 412 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“
    - ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“
    - RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“
    - ISO/IEC 20000-1:2018
    - ISO/IEC 27001:2013, ISO/IEC 27002:2013
    - EN 419211:2014

1.1. Pregled

ESS QCA pružalac usluga od poverenja odgovoran je za izdavanje kvalifikovanih sertifikata za elektronski potpis, prema **šemi visokog nivoa pouzdanosti**, što obuhvata, ali se ne ograničava, na pružanje sledećih servisa:

- Registraciju korisnika,
- Formiranje asimetričnog para ključeva za korisnike,
- Formiranje kvalifikovanog sertifikata za elektronski potpis,
- Distribuciju privatnog ključa i kvalifikovanog sertifikata za elektronski potpis korisnicima na način u skladu sa Zakonom,
- Upravljanje procedurom opoziva i suspenzije kvalifikovanih sertifikata za elektronski potpis,
- Obezbeđivanje statusa opoziva kvalifikovanih sertifikata za elektronski potpis.

ESS QCA obezbeđuje **sredstvo za formiranje kvalifikovanog elektronskog potpisa** (**QSCD**) i pridruženi **PIN kod** (za aktivaciju privatnog ključa), **PUK kod** (za deblokadu PIN-a), kao i njihovu bezbednu distribuciju do korisnika. **ESS QCA** dodatno obezbeđuje jednokratni aktivacioni kod (JAK), podatak koji se koristi za aktivaciju kvalifikovanog sertifikata za elektronski potpis.

ESS QCA utvrđuje Opšte uslove za pružanje usluga od poverenja u skladu sa Zakonom koji zainteresovanim stranama obezbeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga. **Opšti uslovi** za pružanje usluga **ESS QCA** su formirani na osnovu sledećih dokumenata:

1. Politika izdavanja kvalifikovanih sertifikata za elektronski potpis (u daljem tekstu: **CP**) – ovaj dokument,
2. Praktična pravila izdavanja kvalifikovanih sertifikata za elektronski potpis (u daljem tekstu: **CPS**) i
3. Politika privatnosti i zaštita podataka o ličnosti.

CP i **CPS** su javni dokumenti. **CP** definiše predmet rada sertifikacionog tela u oblasti izdavanja i upravljanja kvalifikovanim sertifikatima za elektronski potpis, dok **CPS** definišu procese i način njihovog korišćenja u okviru pružanja svih usluga od poverenja.

ESS QCA utvrđuje i interna pravila rada sertifikacionog tela i zaštite sistema sertifikacije (u daljem tekstu: **Interna pravila**) u kojima su sadržani i detaljno opisani postupci i mere koji se primenjuju u **ESS QCA** u procesu pružanja usluga od poverenja. **Interna pravila** su interni dokumenti i predstavljaju poslovnu tajnu sertifikacionog tela.

ESS QCA je upisan u Registar pružalaca kvalifikovanih usluga od poverenja 07.05.2018. godine pod brojem 5, za uslugu izdavanja kvalifikovanih sertifikata za elektronski potpis i biće predmet periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona.

1.2. Ime dokumenta i identifikacija

Identifikacioni podaci **ESS QCA** su:

ESS QCA
E-Smart Systems d.o.o.
Kneza Višeslava 70a
11030 Beograd
Srbija

Sertifikaciono telo	Jedinstveno ime (DN)
Root	CN=ESS RQCA, O= E-Smart Systems d.o.o., C=RS
Issuing	CN=ESS IQCA1, O= E-Smart Systems d.o.o., C=RS

Ovaj dokument ima jedinstvenu oznaku - 1.3.6.1.4.1.30496.509.1.1.2
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) e-smart systems d.o.o. (30496) pki (509) ESS QCA (1) CP (1) verzija (2)}

U svakom izdatom kvalifikovanom sertifikatu za elektronski potpis od strane *ESS IQCA1* u kome u polju *Certificate Policy* stoji OID 1.3.6.1.4.1.30496.509.1.1.2 isti ukazuje da je sertifikat izdat po ovoj verziji politike izdavanja sertifikata.

1.3. Učesnici u PKI sistemu ESS QCA

U ovom poglavlju su date osnovne informacije o učesnicima u okviru PKI sistema **ESS QCA**.

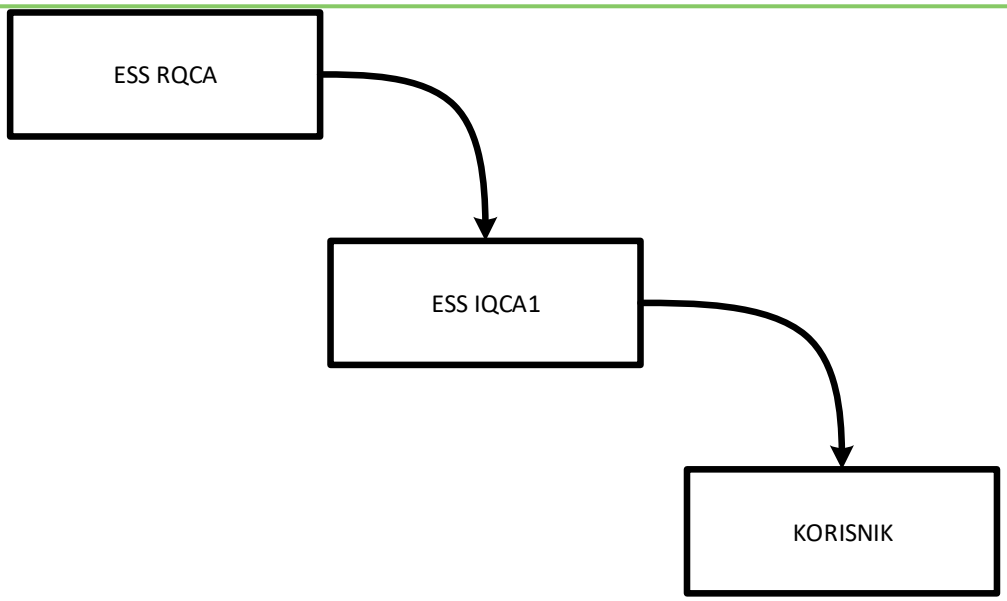
1.3.1. ESS QCA

ESS QCA je pružalac kvalifikovanih usluga od poverenja koji izdaje kvalifikovane sertifikate za elektronski potpis. **CP i CPS** predstavljaju odgovarajuću politiku i pravila koja se primenjuju pri izdavanju i upravljanju kvalifikovanim sertifikatima za elektronski potpis.

U cilju objavljivanja trećim stranama informacija koje se odnose na opozvane i suspendovane kvalifikovane sertifikate (status sertifikata), vrši se odgovarajuća publikacija liste opozvanih sertifikata (CRL – Certificate Revocation List). Provera statusa sertifikata je moguća direktnim uvidom u CRL i preko OCSP servisa. **ESS QCA** periodično objavljuje CRL listu u skladu sa uslovima definisanim u ovom dokumentu.

ESS QCA predstavlja hijerarhijsku strukturu **Infrastrukture Javnih Ključeva** (U daljem tekstu: **PKI**) za izdavanje kvalifikovanih sertifikata za elektronski potpis. U pomenutoj arhitekturi (Slika 1), postoji:

- **ESS RQCA** – centralno samopotpisano sertifikaciono telo (*Root CA*) koje izdaje sertifikate potčinjenim sertifikacionim telima (*Issuing* CA) i potpisuje svoju CRL listu.
- **ESS IQCA1** – potčinjeno sertifikaciono telo (***Issuing CA*)** od strane **ESS RQCA**, koje izdaje kvalifikovane sertifikate za elektronski potpis korisnicima, koje potpisuje svoju CRL listu.



Slika 1: Hijerarhijska struktura ESS QCA sistema

Sva navedena sertifikaciona tela se nalaze na centralnoj lokaciji ESS, u okviru sektora QCA.

1.3.2. Registraciona tela ESS QCA

Zahtevi za izdavanje sertifikata za korisnike **ESS QCA** se podnose **ESS QCA** telu ili na lokacijama udaljenih Registracionih tela, koje obavljaju ulogu Registracionih autoriteta (RA), tj. **ESS QCA** komunicira sa svojim korisnicima putem mreže Registracionih tela (centralno RA i mreža RA).

Registraciona tela su:

- **ESS QCA** na centralnoj lokaciji, kao **centralno RA telo**. Ovo RA telo nije ovlašćeno za rad sa pripremljenim QSCD uređajima.
- Organizacije sa kojima **ESS QCA** ima ugovor o poslovno tehničkoj saradnji, kao **udaljena RA tela**. RA telo može biti ovlašćeno za rad sa pripremljenim QSCD uređajima.

RA tela interaktivno komuniciraju sa pretplatnicima, podnosiocima zahteva, korisnicima i **ESS QCA** u cilju isporuke usluga od poverenja.

ESS QCA preuzima odgovornost za poštovanje ove CP i kada je uloga registracionog tela poverena drugim licima na osnovu ugovora o poslovno-tehničkoj saradnji. **ESS QCA** obezbeđuje mehanizam za ostvarivanje pune linije odgovornosti u procesu izdavanja i upravljanja izdatim kvalifikovanim sertifikatima.

1.3.3. Pretplatnici

ESS QCA kao pretplatnike prihvata pravna lica. Pretplatnik podnosi Saglasnost za izdavanje kvalifikovanog sertifikata za elektronski potpis i ima pravo podnošenja zahteva za opoziv ili suspenziju korisničkog sertifikata.

1.3.4. Korisnici

Korisnik je fizičko lice na čije ime glasi kvalifikovani sertifikat za elektronski potpis i koji je jedini ovlašćen da isti i koristi za generisanje kvalifikovanog elektronskog potpisa.

1.3.5. Treće strane

Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koji prihvataju i verifikuju kvalifikovani elektronski potpis.

Verifikacija kvalifikovanog elektronskog potpisa obuhvata:

- Proveru validnosti putanje sertifikacije korisnikovog kvalifikovanog sertifikata za elektronski potpis. U cilju provere validnosti kvalifikovanog sertifikata za elektronski potpis, treće strane moraju uvek da provere status opozvanosti datog sertifikata u okviru **ESS QCA**. Na raspolaganju su CRL liste (*ESS RQCA i ESS IQCA1*) i OCSP servis.
- Proveru potpisa elektronskog dokumenta na bazi javnog ključa koji se nalazi u korisnikovom kvalifikovanom sertifikatu za elektronski potpis.

1.3.6. Ostali učesnici

ESS QCA se u pružanju usluge izdavanja kvalifikovanih sertifikata za elektronski potpis oslanja na usluge i proizvode eksternih isporučilaca (dobavljača). Izbor, vrednovanje, evaluacija i upravljanje eksternim isporučiocima obavlja se po strogoj proceduri, a sam spisak svih eksternih isporučilaca za **ESS QCA** definisan je u Planu menadžmenta servisima.

1.4. Korišćenje sertifikata

1.4.1. Prihvatljivo korišćenje sertifikata

ESS QCA sertifikati se mogu koristiti za većinu transakcija elektronskog poslovanja i elektronske trgovine koje se baziraju na upotrebi kvalifikovanih sertifikata za elektronski potpis. U takve transakcije spadaju:

- pristup bezbednim web sajtovima (ssl autentikacija),
- elektronsko potpisivanje dokumenata i elektronske pošte,
- verifikacija elektronskog potpisa.

1.4.2. Zabranjeno korišćenje sertifikata

Svaka druga upotreba kvalifikovanog sertifikata za elektronski potpis koja nije propisana ovim dokumentom ili nije u saglasnosti sa odredbama Zakona i drugim dokumentima koji regulišu ovu oblast, smatra se nedozvoljenom.

1.5. Administracija CP

1.5.1. Organizacija administriranja CP

ESS QCA je odgovorno za propisnu administraciju ove CP, i to u smislu periodičnog pregleda i ažuriranja, kao i vanrednih promena odgovarajućih odredbi koje proističu iz eventualnih promena u zakonskoj regulativi ili tehničkim karakteristikama primenjenih kriptografskih algoritama i dužina ključeva.

1.5.2. Kontakt podaci

ESS QCA
E-Smart Systems d.o.o.
Kneza Višeslava 70a
11030 Beograd
Srbija
tel: 011/3050280
fax: 011/3050222
email: qca@e-smartsys.com

1.5.3. Osoba koja određuje pogodnost CP dokumenta

Osoba u ESS QCA odgovorna za ovu CP je:

Ana Marković
E-Smart Systems d.o.o.
Kneza Višeslava 70a
11030 Beograd
Srbija
tel: 011/3050212
fax: 011/3050222
email: ana.markovic@e-smartsys.com

1.5.4. Procedura odobravanja CP dokumenta

CP dokument se periodično pregleda. Ukoliko ima potrebe za izmenama, izmene se vrše od strane odgovornog lica za **ESS QCA** u kompaniji E-Smart Systems d.o.o. Dokument je odobren kada je potpisan od strane odgovorne osobe definisane u prethodnom poglavlju i Generalnog direktora kompanije E-Smart Systems d.o.o.

1.6. Definicije i skraćenice

U ovom dokumentu pojedini izrazi imaju sledeće značenje:

Aktivacioni podaci – podaci, koji nisu ključevi, koji su zahtevani u cilju rada kriptografskih modula i koji moraju biti zaštićeni (kao na primer PIN ili pristupna šifra).

Asimetrični kriptografski algoritmi – kriptografski algoritmi koji koriste različite ključeve za šifrovanje i dešifrovanje.

Asimetrični par ključeva (key pair) – privatni ključ i javni ključ, kao matematički par koji se koriste za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primer RSA algoritam.

Autentikacija – procedura provere deklarisanog identiteta pojedinca ili organizacije.

CA sertifikat – sertifikat za dato CA telo izdat (digitalno potpisan) od strane drugog CA (*Issuing* CA) ili samopotpisan (ukoliko se radi o *Root* CA).

Deljena tajna – deo kriptografske tajne koja je podeljena na unapred definisan broj delova koji su pridruženi različitim entitetima. To mogu biti fizički tokeni (na primer smart kartica) ili ljudi koji znaju pojedinačan podatak.

Digitalni potpis – tehnički postupak realizacije elektronskog potpisa gde se hash vrednost binarne reprezentacije elektronskog dokumenta šifruje asimetričnim kriptografskim algoritmom.

Elektronski dokument – dokument u elektronskom obliku koji može da se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom.

Elektronski potpis – skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

Hash algoritmi – jednosmerne ireverzibilne funkcije pomoću kojih se vrši transformacija informacije proizvoljne veličine u hash vrednost fiksne veličine (160, 224, 256, 374, 512 bitova (ili više)).

Identifikacija – proces deklarisanja identiteta pojedinca ili pravnog lica.

Kvalifikovani elektronski potpis – elektronski potpis koji se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa (QSCD – Qualified Signature Creation Device) i koji se proverava putem kvalifikovanog sertifikata za elektronski potpis potpisnika (javnog ključa). Ovaj potpis je pravno ekvivalentan svojeručnom potpisu prema Zakonu.

Kvalifikovani sertifikat za elektronski potpis – elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih sertifikata za elektronski potpis i sadrži podatke predviđene Zakonom.

Lista opozvanih sertifikata (CRL – Certificate Revocation List) – lista izdata i elektronski potpisana od strane CA koja uključuje serijske brojeve opozvanih sertifikata i vreme kada je opoziv izvršen. Takva lista se mora koristiti od strane trećih strana uvek kada treba proveriti validnost sertifikata i/ili verifikovati elektronski potpis.

Opoziv sertifikata – permanentno ukidanje validnosti datog sertifikata i njegovo smeštanje na CRL listu.

Podnosilac zahteva – fizičko lice koje je podnosilac zahteva za izdavanje kvalifikovanog sertifikata za elektronski potpis u vremenskom periodu do uručenja kada postaje korisnik.

Podnošenje zahteva za sertifikat – zahtev poslat od strane lica koje zahteva sertifikat (podnosilac zahteva) ka Sertifikacionom telu u cilju izdavanja kvalifikovanog sertifikata za elektronski potpis.

Potpisnik – lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica.

Praktična pravila za izdavanje kvalifikovanih sertifikata za elektronski potpis – javna praktična pravila i procedure koje sertifikaciono telo primenjuje u pružanju usluga od poverenja.

Registraciono telo (RA) – entitet koji je odgovoran za identifikaciju i autentikaciju pretplatnika, podnosioca zahteva i korisnika sertifikata. RA može vršiti i druge poslove delegirane od strane CA kako je definisano u ovom dokumentu.

Repozitorijum – baza podataka i/ili direktorijum na kome su publikovani osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje usluga od poverenja od strane datog CA.

Sertifikaciono telo – pravno lice koje izdaje kvalifikovane sertifikate za elektronski potpis u skladu sa odredbama Zakona.

Sredstva za formiranje kvalifikovanog elektronskog potpisa (QSCD) – sredstva za formiranje kvalifikovanog elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom.

Sredstva za proveru kvalifikovanog elektronskog potpisa – sredstva za proveru elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom.

Suspenzija kvalifikovanog sertifikata – privremeno ukidanje validnosti datog kvalifikovanog sertifikata i njegovo privremeno smeštanje na CRL listu.

Treća strana – primalac sertifikata koji proverava dati sertifikat i/ili proverava elektronski potpis dobijenog elektronskog dokumenta primenom javnog ključa potpisnika iz sertifikata. Takođe, treća strana proverava validnost sertifikata u istom procesu. Treća strana može biti i korisnik sertifikata izdatog od strane istog sertifikacionog tela, ali i ne mora.

Upravljanje kvalifikovanim sertifikatima – aktivnosti pridružene upravljanju sertifikatima uključuju generisanje, čuvanje, isporuku, objavljivanje, suspenziju i opoziv sertifikata.

Skraćenice koje se koriste u ovom dokumentu:

CA (Certification Authority) - sertifikaciono telo
CP (Certificate Policy) - Politika izdavanja kvalifikovanih sertifikata za elektronski potpis
CPS (Certification Practice Statement) - Praktična pravila izdavanja kvalifikovanih sertifikata za elektronski potpis
CRL (Certificate Revocation List) - lista opozvanih sertifikata
eIDAS (electronic IDentification, Authentication and trust Services) - Uredba EU br. 910/2014 Evropskog parlamenta i Saveta
ESS – E-Smart Systems d.o.o.
ESS QCA – E-Smart Systems DOO BEOGRAD – E-SMART SYSTEMS DOO BEOGRAD sertifikaciono telo
ETSI – European Telecommunications Standards Institute
JIK – Jedinstveni identifikator korisnika
OCSP - Online Certificate Status Protocol
OID (Object Identifier) - jedinstveni identifikator
PKI (Public Key Infrastructure) - infrastruktura javnih ključeva

Pravilnik – Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani sertifikati za elektronski potpis

QSCD (Qualified Signature Creation Device) - sredstvo za formiranje kvalifikovanog elektronskog potpisa

RA (Registration Authority) - registraciono telo

RFC – Request For Comments

Zakon - Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju

2. Odgovornosti za publikovanje i repozitorijume

2.1. Repozitorijum

ESS QCA publikuje informacije (sertifikate CA tela, CRL liste CA tela i OCSP) potrebne za proveru statusa kvalifikovanih sertifikata koje izdaje na on-line repozitorijumu https://qca.e-smartsys.com. **ESS QCA** zadržava pravo da publikuje statusne informacije o sertifikatima i na repozitorijumu neke treće strane ukoliko je to pogodno.

ESS QCA na pomenutom on-line repozitorijumu objavljuje sva dokumenta i informacije koje se odnose na izdavanje kvalifikovanih sertifikata:

- praktična pravila (CPS),
- ovu politiku izdavanja sertifikata (CP),
- opšte uslove za pružanja usluga od poverenja,
- politiku privatnosti i zaštite podataka o ličnosti,
- politiku bezbednosti informacija,
- obrasce za korisnike,
- korisnička uputstva,
- cenovnik,
- ostale informacije vezane za rad **ESS QCA**.

ESS QCA zadržava pravo da učini raspoloživim i publikuje informacije u vezi sopstvenih politika i procedura rada pored navedenog i putem bilo kog drugog pogodnog načina.

2.2. Publikovanje informacija o sertifikatima

ESS QCA publikuje informacije o sertifikatima **ESS QCA** (*Root* i *Issuing* CA) na prethodno pomenutom repozitorijumu.

Učesnici u uslugama od poverenja se obaveštavaju da će **ESS QCA** publikovati pojedine informacije koje su oni dostavili na javno pristupačnim direktorijumima uz pridružene statusne informacije o kvalifikovanim sertifikatima u formatu i sadržaju koji propisuje Zakon.

2.3. Vreme i frekvencija publikovanja

ESS QCA publikuje informacije o statusu opozvanosti izdatih elektronskih sertifikata (CRL liste), kao što je naznačeno i precizirano u CPS dokumentu. Maksimalno dozvoljeno kašnjenje od izdavanja CRL liste do publikovanja je jedan sat. Podaci o statusu sertifikata dostupni su i preko OCSP servisa na lokaciji https://qca.e-smartsys.com/ocsp/ESSQCA1. OCSP servis koristi isključivo podatke iz publikovane CRL liste tako da su u svakom trenutku podaci o statusu sertifikata publikovani preko CRL i OCSP identični.

ESS QCA publikuje sve ostale informacije i dokumente nakon izmena koje su usvojene i odobrene od strane **ESS QCA**.

2.4. Kontrole pristupa repozitorijumima

Dokumenta, informacije vezane za rad **ESS QCA**, CA sertifikati, kao i CRL liste na on-line repozitorijumu su javno dostupni.

ESS QCA može ograničiti ili zabraniti pristup određenim uslugama, kao što su publikovanje statusnih informacija o bazama podataka treće strane, određenim privatnim direktorijumima, itd.

3. Identifikacija i autentikacija korisnika

3.1. Dodela imena

Identifikacioni podaci pretplatnika i/ili korisnika koji se upisuju u kvalifikovani sertifikat za elektronski potpis struktuirani su po X.500 *distinguished name* formi i usklađeni sa zakonskom regulativom.

*Sertifikati pružaoca usluge od poverenja **ESS QCA***

Vrsta sertifikata	Naziv polja	Jedinstveno ime
Elektronski sertifikat pružaoca usluga od poverenja ESS QCA	Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
	Subject	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Elektronski sertifikat izdavajućeg tela ESS QCA	Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
	Subject	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS

Svi identifikacioni podaci koji se dostavljaju **ESS QCA** o pretplatniku i podnosiocu zahteva moraju biti verodostojni i proverljivi i moraju da jednoznačno predstavljaju korisnika kvalifikovanog sertifikata za elektronski potpis.

Sertifikat krajnjeg korisnika

Vrsta sertifikata	Naziv polja	Jedinstveno ime
Kvalifikovani elektronski sertifikat za elektronski potpis za fizičko lice pripadnika entiteta pravnog lica	Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
	Subject	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, O={naziv pravnog lica}, [SERIALNUMBER = PNORS-{JMBG}] ili [SERIALNUMBER = PAS{oznaka zemlje izdavaoca pasoša}-{broj pasoša}], SERIALNUMBER = CA:RS-{SN kartice}, 2.5.4.97 = MB:RS-{matični broj pravnog lica}, [2.5.4.97 = VATRS-{PIB pravnog lica}], C=RS
	Subject Alternative Name	RFC822 Name={email adresa}
Kvalifikovani elektronski sertifikat za elektronski potpis za fizičko lice	Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
	Subject	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, [SERIALNUMBER = PNORS-{JMBG}] ili [SERIALNUMBER = PAS{oznaka zemlje izdavaoca pasoša}-{broj pasoša}], SERIALNUMBER = CA:RS-{SN kartice}, C=RS

	Subject Alternative Name	RFC822 Name={email adresa}

ESS QCA ne izdaje anonimne sertifikate korisnicima, kao ni sertifikate zasnovane na pseudo podacima.

3.2. Inicijalna provera identiteta

3.2.1. Identifikacija pretplatnika i podnosioca zahteva (fizičkih lica pripadnika entiteta pravnog lica pretplatnika)

Pretplatnik je u obavezi da dostavi **ESS QCA** verodostojne podatke o svom pravnom licu i o fizičkom licu pripadniku entiteta pravnog lica koji je u svojstvu podnosioca zahteva. Podaci o podnosiocima zahteva se moraju dostaviti u okviru dokumenta Saglasnost za izdavanje kvalifikovanih elektronskih sertifikata.
Podaci o pretplatniku i podnosiocu zahteva se mogu dostaviti elektronski.
Procedure identifikacije pretplatnika i podnosioca zahteva (fizičkih lica pripadnika entiteta pravnog lica pretplatnika) su opisane u CPS dokumentu.
Identifikacija pretplatnika vrši se u skladu sa zakonskim propisima na osnovu dostavljenih podataka konsultovanjem ovlašćenih registara Republike Srbije.
Identifikacija podnosioca zahteva vrši se uz lično prisustvo podnosioca u procesu registracije na osnovu validnog identifikacionog dokumenta naznačenog od strane pretplatnika u dokumentu saglasnosti.
U slučaju da je podnosilac zahteva strani državljanin i da se u njegovo ime izdaje kvalifikovani sertifikat za elektronski potpis u svrhe rada se državom, identifikacioni dokument mora biti pasoš, lične karte drugih zemalja u ovom slučaju nisu prihvatljive kao identifikacioni dokument.

ESS QCA ne proverava verodostojnost email adrese pretplatnika i podnosioca zahteva. RA operater proverava ispravnost samog zapisa email adrese sa podnosiocem zahteva pri procesu identifikacije i registracije.

3.2.2. Identifikacija podnosioca zahteva (fizička lica)

Podnosilac zahteva je u obavezi da lično prisustvuje procesu identifikacije i registracije u okviru RA tela **ESS QCA**. Identifikacija na daljinu nije podržana u okviru operativnih procesa **ESS QCA**.
Podnosilac zahteva je u obavezi da obezbedi verodostojni identifikacioni dokument kao i podatke potrebne za formiranje kvalifikovanog elektronskog sertifikata.
Identifikaciju podnosilac zahteva izvršava RA Operater RA tela **ESS QCA** prema priloženom identifikacionom dokumentu.
U slučaju da je podnosilac zahteva strani državljanin i da se u njegovo ime izdaje kvalifikovani sertifikat za elektronski potpis u svrhe rada se državom, identifikacioni dokument mora biti pasoš , lične karte drugih zemalja u ovom slučaju nisu prihvatljive kao identifikacioni dokument.

ESS QCA ne proverava verodostojnost email adrese podnosioca zahteva kvalifikovanog elektronskog sertifikata. RA operater proverava ispravnost samog zapisa email adrese sa podnosiocem zahteva pri procesu identifikacije i registracije.

3.3. Identifikacija i autentikacija zahteva za reizdavanje kvalifikovanog sertifikata za elektronski potpis

3.3.1. Identifikacija pretplatnika i korisnika (fizičkih lica pripadnika entiteta pravnog lica pretplatnika)

Pretplatnik zahtev za reizdavanje sertifikata može da zatraži u ime korisnika slanjem novog dokumenta saglasnosti za datog korisnika, ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata.

Identitet pretplatnika i verodostojnost podataka garantuje pravni zastupnik svojim potpisom na saglasnosti. **ESS QCA** u ovom slučaju ne proverava ponovo identitet pretplatnika. Identitet korisnika proverava RA operater **ESS QCA** na osnovu:

- elektronskog potpisa korisnika na poslatom zahtevu za reizdavanje (zahtev mora biti potpisan sertifikatom koji treba da se reizda) ili
- identifikacionog dokumenta u procesu identifikacije kome je korisnik obavezan da lično prisustvuje, kao i pri inicijalnom izdavanju.

Korisnik u ovom slučaju ne može sam da podnese zahtev za reizdavanje sertifikata.

3.3.2. Identifikacija korisnika (fizička lica)

Korisnik zahtev za reizdavanje sertifikata može da zatraži ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata.

Identitet korisnika proverava RA operater **ESS QCA** na osnovu:

- elektronskog potpisa korisnika na poslatom zahtevu za reizdavanje (zahtev mora biti potpisan sertifikatom koji treba da se reizda) ili
- identifikacionog dokumenta u procesu identifikacije kome je korisnik obavezan da lično prisustvuje, kao i pri inicijalnom izdavanju.

3.4. Identifikacija i autentikacija zahteva za opoziv sertifikata

Korisnik može da zahteva od **ESS QCA** opoziv/suspenziju svog sertifikata. Zahtev za opoziv/suspenziju se dostavlja elektronski ili lično. Elektronski zahtev za opoziv/suspenziju mora da bude potpisan sertifikatom koji se opoziva/suspenduje. U slučaju da je sam uređaj izgubljen korisnik mora lično da podnese zahtev za opoziv/suspenziju u prostorijama RA tela, pri čemu je obavezna identifikacija korisnika na osnovu identifikacionog dokumenta.

Pretplatnik može da zahteva od **ESS QCA** opoziv/suspenziju sertifikata izdatog za ovlašćeno fizičko lice, za koje je prethodno dao saglasnost za izdavanje kvalifikovanog sertifikata za elektronski potpis. Zahtev za opoziv/suspenziju od strane pretplatnika se dostavlja elektronski uz navedene podatke o korisniku, jedinstvenom identifikatoru korisnika (JIK) sertifikata koji se opoziva/suspenduje i validnim potpisom ovlašćenog lica od strane pretplatnika.

Opoziv sertifikata može biti zahtevan i od strane **ESS QCA** zbog uočenih neregularnosti u radu.

Korisnik i pretplatnik se obaveštavaju nakon obrade zahteva za opoziv/suspenziju kvalifikovanog sertifikata za elektronski potpis. Obrađen zahtev za opoziv/suspenziju je vidljiv na CRL listi u roku od najviše 24 sata po prijemu zahteva.

4. Operativni zahtevi u vezi životnog ciklusa sertifikata

4.1. Podnošenje zahteva za dobijanje sertifikata

Podnosilac zahteva je fizičko lice koja može biti i pripadnik entiteta pravnog lica koje je budući korisnik kvalifikovanog elektronskog sertifikata.

U slučaju da je fizičko lice pripadnik entiteta pravnog lica, saglasnost za izdavanje kvalifikovanog sertifikata za elektronski potpis dostavlja pretplatnik čija je odgovornost da dostavi verodostojne i tačne informacije. RA operater sprovodi proces identifikacije i registracije pretplatnika u cilju sprovođenja postupka podnošenja zahteva za izdavanje kvalifikovanih sertifikata za elektronski potpis .

Proces održavanja podataka o pretplatnicima realizuje se unutar RA tela prilikom svakog podnošenja saglasnosti ili dostave novih podataka i obuhvata proveru i ažuriranje podataka.
Prijem saglasnosti za izdavanje kvalifikovanog sertifikata za elektronski potpis u RA može da stigne u elektronskom ili papirnom obliku, ali isključivo u formi popunjenog propisanog obrasca overenog potpisom registrovanog zastupnika.

U slučaju da je podnosioc zahteva samo fizičko lice, RA sprovodi proces identifikacije i registracije podnosioca zahteva na licu mesta u cilju izdavanja kvalifikovanog sertifikata za elektronski potpis. Podnosioc zahteva mora da priloži validan identifikacioni dokument i verodostojne i tačne podatke koji su potrebni za sačinjavanje zahteva.

Procedura obrade zahteva za izdavanje kvalifikovanog sertifikata je detaljno opisana u CPS dokumentu.

4.2. Procesiranje zahteva za dobijanje sertifikata

Procesuiranje zahteva za dobijanje sertifikata se obavlja u ovlašćenom RA telu **ESS QCA** od strane ovlašćenog RA operatera.

Ova procedura se detaljno opisuje u CPS dokumentu.

4.3. Izdavanje sertifikata

Nakon dostave validnog elektronskog dokumenta zahteva za izdavanje sertifikata, CA operater **ESS QCA** sprovodi proces izdavanja sertifikata.

Ovaj proces je detaljno opisan u CPS dokumentu.

4.4. Prihvatanje sertifikata

Uručenje QSCD uređaja vrši se na jedan od dva načina:

- ličnim preuzimanjem - ako korisnik lično preuzima QSCD uređaj, u prostorijama **ESS QCA** ili ovlašćenog RA tela za rad sa pripremljenim QSCD uređajima, i PIN koverta mu se uručuje lično
- kurirskom službom - ako se QSCD uređaj dostavlja kurirskom službom on se lično uručuje korisniku, a PIN koverta se šalje poštom.

U oba slučaja korisnik prilikom preuzimanja QSCD uređaja potpisuje korisnički ugovor i potvrdu o preuzimanju kvalifikovanog sertifikata za elektronski potpis.

Korisnik preko on-line servisa https://qca.e-smartsys.com aktivira sertifikat korišćenjem dva parametra:

- jednokratnog aktivacionog koda (JAK) kvalifikovanog sertifikata za elektronski potpis koji je poslat direktno korisniku i
- jedinstvenog identifikatora korisnika (JIK) odštampanog na QSCD uređaju koji je uručen.

Bilo koja primedba na prihvatanje izdatog sertifikata mora biti dostavljena **ESS QCA**, kao sertifikacionom telu – izdavaocu. Primedbe mogu biti dostavljene u RA telo koje ih prosleđuje **ESS QCA**.

4.5. Korišćenje sertifikata i asimetričnog para ključeva

U ovom poglavlju se definišu odgovornosti koje se odnose na korišćenje asimetričnog para ključeva i sertifikata, koje su detaljno opisane u korisničkom ugovoru, kao i u opštim pravilima poslovanja ESS QCA i to:

- Odgovornosti korisnika – korisnik se obavezuje da će koristiti privatni ključ i generisani sertifikat od strane **ESS QCA** u skladu sa definisanim načinom korišćenja ključa u samom sertifikatu (Key Usage ekstenzija). Korišćenje privatnog ključa i sertifikata predstavlja deo korisničkog ugovora sa **ESS QCA**. U tom smislu, korisnik može koristiti svoj privatni ključ samo nakon prihvatanja odgovarajućeg sertifikata.
- Odgovornost treće strane – treća strana je obavezna da prihvata izdate sertifikate od strane **ESS QCA** sa predviđenim načinom korišćenja sertifikata definisanim u samom sertifikatu. Treća strana je obavezna da propisno i uspešno primenjuje operaciju javnog ključa koji ekstrahuje iz izdatog sertifikata i odgovorna je da sprovodi proveru statusa opozvanosti datog sertifikata korišćenjem metoda koji je definisan u CP i CPS dokumentima **ESS QCA**.
- Obaveza registracionih tela, pretplatnika, korisnika i drugih učesnika je da informišu **ESS QCA** o svim promenama u informacijama koje su objavljene u kvalifikovanom sertifikatu za elektronski potpis u toku perioda važenja istog.

4.6. Obnavljanje sertifikata

ESS QCA ne obnavlja sertifikat nad istim parom ključeva, već reizdaje sertifikat za već registrovanog korisnika sa novim parom asimetričnih ključeva.

Reizdavanje sertifikata se može uraditi ako je postojeći sertifikat validan i u periodu od 30 dana do isteka aktivnog sertifikata. U tom slučaju korisnik ne mora biti ponovno identifikovan, ali je u obavezi da pošalje zahtev za reizdavanje sertifikata potpisan postojećim validnim sertifikatom.

Obnovljeni sertifikat se izdaje na novom QSCD uređaju, sa novim asimetričnim parom ključeva i novim PIN i PUK kodom. **ESS QCA** sistem obaveštava korisnika o tome da mu je sertifikat izdat i kako može da ga aktivira.

Aktiviranje sertifikata je isto kao u slučaju redovnog izdavanja.

4.7. Generisanje novog para ključeva i sertifikata korisnika

Korisnici kojima je sertifikat istekao ili opozvan, ukoliko žele da dobiju novi sertifikat, moraju da podnesu zahtev za izdavanje novog sertifikata. Procedura je ista kao i za inicijalno izdavanje sertifikata. Novi sertifikat se izdaje na novom QSCD uređaju, sa novim asimetričnim parom ključeva i novim PIN i PUK kodom.

S obzirom da je korisnik već registrovan u okviru **ESS QCA** i da poseduje jedinstveni identifikator korisnika (JIK), na zahtevu za izdavanje sertifikata se navodi da je već registrovan da bi se koristio isti JIK u novom sertifikatu.

Pravila prihvatanja sertifikata su ista kao što je opisano u poglavlju 4.4.

4.8. Modifikacije sertifikata korisnika

Modifikacije postojećeg sertifikata nisu dozvoljene. Ukoliko su potrebne modifikacije radi se postupak novog izdavanja sertifikata uz opoziv prethodnog.

4.9. Opoziv i suspenzija sertifikata

ESS QCA vrši opoziv izdatog kvalifikovanog sertifikata za elektronski potpis u slučaju:

- gubitka, krađe, modifikacije, objavljivanja ili neke druge kompromitacije privatnog ključa korisnika sertifikata,
- kada izvršenje odgovarajućih obaveza lica koja su navedena u ovoj CP kasni ili je sprečeno usled prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usled drugog uzroka koji izlazi van kontrole datog lica, i kao rezultat, informacije o drugom licu su materijalno ugrožene ili kompromitovane,
- kada se desila promena informacija koje su sadržane u sertifikatu datog lica,
- kada pretplatnik ukida pripadnost entitetu za korisnika,
- kada korisnik zahteva opoziv sertifikata,
- kada su podaci za proveru kvalifikovanog elektronskog potpisa ili ESS QCA ugroženi na način koji utiče na bezbednost i pouzdanost sertifikata.

ESS QCA vrši suspenziju izdatog kvalifikovanog sertifikata za elektronski potpis u sledećim slučajevima:

- prilikom samog izdavanja kvalifikovanog sertifikata za elektronski potpis (opisano u poglavlju 4.4),
- prilikom izdavanja obnovljenog kvalifikovanog sertifikata za elektronski potpis (opisano u poglavlju 4.6),
- na zahtev korisnika, potpisnika ili nadzora **ESS QCA** ukoliko imaju sumnju u kompromitaciju privatnog ključa,
- na zahtev pretplatnika kada privremeno ukida pripadnost entitetu za korisnika.

Proces opoziva kvalifikovanih sertifikata za elektronski potpis može inicirati :

1. pretplatnik koji je inicirao izdavanje kvalifikovanog sertifikata za pripadnika entiteta,

2. korisnik,
3. RA operater,
4. **ESS QCA** .

Ovaj proces je detaljno opisan u CPS dokumentu.

4.10. Servisi provere statusa sertifikata

Opozvani ili suspendovan kvalifikovani sertifikat za elektronski potpis je vidljiv na CRL listi u roku od najviše 24 sata od podnošenja zahteva za opoziv ili suspenziju. Opozvani ili suspendovani sertifikati koji su vremenski istekli nisu vidljivi na CRL listi. U slučaju opoziva *Issuing CA* elektronskog sertifikata ESS QCA obaveštava korisnike direktno, a treće strane preko on-line repozitorijuma https://qca.e-smartsys.com u roku od najviše 24 sata od podnesenog zahteva za opoziv ili suspenziju *Issuing CA* elektronskog sertifikata **ESS QCA**.

Lista opozvanih sertifikata (CRL) ESS IQCA1 se ažurira na svakih 24 sata, a CRL ESS RQCA na svakih 6 meseci. Treće strane moraju koristiti on-line repozitorijum https://qca.e-smartsys.com ESS QCA da preuzmu CRL listu. Podaci o statusu sertifikata dostupni su i preko OCSP servisa na lokaciji https://qca.e-smartsys.com/ocsp/ESSQCA1.

Korisnici trenutni status svog sertifikata mogu proveriti na repozitorijumu https://qca.e-smartsys.com?p=status.

4.11. Prestanak korišćenja sertifikata

Nakon prestanka korišćenja kvalifikovanog sertifikata izdatog od strane **ESS QCA**, dati sertifikat mora biti opozvan ukoliko je u tom trenutku i dalje aktivan.

Prestanak korišćenja sertifikata može biti iz sledećih razloga:

- Korisnik želi da prekine korišćenje **ESS QCA** usluga od poverenja.
- **ESS QCA** je prestalo sa pružanjem usluga od poverenja ili mu je rad zabranjen.

Vremenski istekli kvalifikovani sertifikati za elektronski potpis se ne opozivaju i trenutkom isteka nastupa prestanak korišćenja kvalifikovanog sertifikata za elektronski potpis.

Vremenski istekli opozvani kvalifikovani sertifikati za elektronski potpis se uklanjanju sa liste opozvanih kvalifikovanih sertifikata za elektronski potpis.

4.12. Čuvanje i rekonstrukcija privatnog ključa korisnika

Privatni ključ korisnika koji odgovara javnom ključu sadržanom u izdatom kvalifikovanom sertifikatu za elektronski potpis se ne čuva i nalazi se samo na QSCD uređaju korisnika.

5. Objekti, upravljanje i operativne kontrole

Poslovni procesi **ESS QCA** su uspostavljeni, realizovani, kontinualno unapređivani, proveravani od treće strane i sertifikovani, u skladu sa Zakonom, eIDAS-om i Standardima. Servis **ESS QCA** je kontinuirano:

- proveravan od strane nadležnog Ministarstva po ZEP i
- proveravan od treće strane i sertifikovan po standardima ISO 9001, ISO/IEC 27001 i ISO/IEC 20000.

U skladu sa zakonskim obavezama i zahtevima standarda, **ESS QCA** realizuje odgovarajuće aktivnosti procene, kvalifikacije/kvantifikacije i postupanja u vezi sa rizicima vezanim za servise koje pruža i informacije iz poslovnih procesa koji se u okviru servisa realizuju.

5.1. Fizičke bezbednosne kontrole

ESS QCA kompletan skup operacija realizuje sa lokacije Kneza Višeslava 70A, Beograd.

Elektronske servise koje **ESS QCA** obezbeđuje za korisnike izdatih kvalifikovanih sertifikata za elektronski potpis i pouzdajućim stranama mogu biti pruženi iz Azure cloud-a, internog data centra matične lokacije i Zelen Data centra Beogradski put BB, Vršac kao DR lokacije.

Usluge identifikacije i uručenja sertifikata **ESS QCA** može pružiti iz matične lokacije ili lokacije udaljenih RA tela.

Bezbednosno osetljive operacije izdavanja kvalifikovanih sertifikata i upravljanja parovima ključeva na korisničkim QSCD uređajima, kao i ključevima CA tela na HSM uređajima **ESS QCA** realizuje unutar *Zone bezbednosti* i *Zone visoke bezbednosti* iz prostorija **ESS QCA** na matičnoj lokaciji. Zone predstavljaju fizičke zaštićene perimetre sa primenjenim fizičkim, tehničkim i administrativnim kontrolama.

U slučaju da je za potrebe korisnika potrebno realizovati operacije identifikacije ili uručivanja sertifikata van matične lokacije **ESS QCA**, uključujući i lokacije RA tela, operateri koji u ovim operacijama učestvuju poštuju i primenjuju sva pravila bezbednosti i zaštite fizičkih uređaja i informacija koje se po pravilu primenjuju na matičnoj lokaciji.

ESS QCA primenjuje sledeće kontrole fizičke zaštite:

- Održava ažuran i detaljan popis svih dobara **ESS QCA**, uključujući fizička, logička, informaciona i ljudska.
- **ESS QCA** ima ustanovljen proces upravljanja životnim vekom dobara od uvođenja do isključenja iz sistema i izlučivanja, čišćenja, odnosno uništenja.
- Dobra su bezbedno klasifikovana i za svako dobro je određen vlasnik sa primarnom ulogom da se brine o očuvanju CIA triade poverene vrednosti.
- Prava pristupa dobrima definisana su korišćenjem RBAC modela (modela zasnovanog na poslovnim rolama).

- Za pristup posebno osetljivim dobrima i za izvođenje posebno osetljivih operacija koristi se pravilo dva čoveka (two-man rule), separacija uloga (separation of duties) i rotacija pozicija (job rotation).
- Pristup Zonama Bezbednosti i Visoke Bezbednosti je ograničen isključivo na period u kome postoji operativna potreba za pristup i isključivo za role osoba od poverenja, osoba od ovlašćenja i administratora bezbednosti. U zonama je zabranjeno zadržavanje, unošenje nepotrebnih stvari, neovlašćeno iznošenje. Za sakupljanje i uklanjanje otpada postoje posebno označeni kontejneri koji se prazne prema definisanim procedurama uvek uz prisustvo osoba od poverenja/ovlašćenja. Zone su pod 24 h video nadzorom. Zone u periodu van radnog vremena iz prostora van bezbednosnog perimetra nadgleda FTO ESS.
- Nosioci **ESS QCA** informacija su evidentirani i nadgledani. U slučaju kada se njihovo korišćenje prekida i isti iznose iz **ESS QCA** zona bezbednosti podaci na njima se bezbedno uništavaju, a samim uređajima menja klasifikacija.

5.2. Proceduralne kontrole

Dužnosti zaposlenih u **ESS QCA** koji izvršavaju operacije povezane sa upravljanjem ključevima *Root* i *Issuing* CA tela, kao i bilo koje druge operacije koje utiču na rad i konfiguraciju sistema, kao i nadgledanje logova, smatraju se dužnostima na poverljivim pozicijama. Poverljive dužnosti u **ESS QCA** su:

- Administrator bezbednosti,
- Sistem administrator,
- Sistem operater i
- Sistem evidentičar.

ESS QCA sprovodi proveru svih zaposlenih koji su kandidati za poverljive uloge zbog sticanja uvida u njihovu pouzdanost i kompetencije.

Dužnosti zaposlenih u **ESS QCA** koji izvršavaju operacije povezane sa upravljanjem ključevima na *QSCD* uređajima, kao i bilo koje druge operacije koje utiču na takve operacije, smatraju se dužnostima na ovlašćenim pozicijama. Ovlašćene dužnosti u **ESS QCA** su:

- RA operater i
- CA operater.

Zaposleni u **ESS QCA** može da ima samo jednu poverljivu dužnost i/ili jednu ovlašćenu dužnost. Dok obavlja poverljivu dužnost može da obavlja samo RA ovlašćenu dužnost, osim za svrhu ceremonije.

U skladu sa ISO 20000 uspostavljen je i realizuje se *proces upravljanja promenama*. Ovaj proces podrazumeva striktnu evidenciju i dokumentovanje, procenu relevantnosti/uticaja/pretnji svake promene i praćenje pripreme kroz testiranje i validaciju do finalnog spuštanja na produkciono okruženje.

Za potrebe upravljanja promenama uspostavljena su razdvojena razvojna i testna okruženja koja predstavljaju verne replike produkcije, a na kojima se testira i validizira svaka promena uključujući i

sistemske patch-eve. Tek nakon realizovane validacije na testnom okruženju i prihvaćene promene, može se dobiti odobrenje za spuštanje promene na produkciono okruženje.

U cilju evidencije, rezolucije i izveštavanja o bezbednosnim incidentima **ESS QCA** implementira proces upravljanja incidentima prema ustanovljenoj politici i proceduri u skladu sa ISO 27002 i ISO 20000. Evidencija, klasifikacija i kontrola procesa obrade incidenata i problema se realizuje od strane Administratora bezbednosti. Bezbednosni incidenti mogu biti prijavljeni od strane učesnika u procesu **ESS QCA** ili od strane monitoring sistema.

U slučaju pojave kritičnih bezbednosnih incidenata koji mogu da ugroze rad i pružanje servisa **ESS QCA** u skladu sa ovom politikom, **ESS QCA** će obavestiti korisnike, pouzdajuće strane i nadležno Ministarstvo u periodu ne dužem od 24h.

5.3. Kadrovske bezbednosne kontrole

ESS QCA izvršava neophodne aktivnosti u cilju provere zahtevane biografije, kvalifikacija, kao i neophodnog iskustva u cilju realizacije u okviru konteksta kompetencije specifičnog posla.

ESS QCA obezbeđuje obuku i proveru znanja i veština za svoje zaposlene na poverljivim i ovlašćenim dužnostima u cilju realizacije funkcija poslovanja CA i RA.

Zaštita pristupa **ESS QCA** sistemu od strane zaposlenih u **ESS QCA** obezbeđuje se primenom razdvajanja uloga (role separation), rotacijom uloga i primenom pravila „need to know“ i „least privileges“.

ESS QCA primenjuje odgovarajuće mere za kažnjavanje zaposlenih za neovlašćene aktivnosti, nemar ili nepažnju u obavljanju poverenih poslova.

5.4. Procedure bezbednosnih provera/auditing

ESS QCA vodi ažurnu, tačnu i zaštićenu elektronsku evidenciju (audit log) o svim događajima iz životnog veka QSCD uređaja i sertifikata koje izdaje, kao i o aktivnostima komunikacije sa korisnicima, rekonfiguracije sistema, pristupa sistemu, transakcija realizovanih u sistemu, događaja u okolnom fizičkom prostoru (video nadzor), a gde to nije moguće ručnu papirnu evidenciju sa datumom, vremenom i opisom događaja.

ESS QCA čuva audit logove u realnom vremenu. Audit logovi rada CA operatera, dnevnici događaja sistema i druga dokumentacija čuvaju se u obezbeđenom prostoru u bazama podataka obezbeđenim od prepisivanja.

Audit logovi čuvaju se deset godina, zaštićeni od neovlašćenog pristupa.

ESS QCA primenjuje procedure backup-a audit logova na isti način kao i u slučaju operativnih podataka.

Logovi **ESS QCA** sistema se on-line nadgledaju od strane elektronskih alata i periodično od strane autorizovanog osoblja – sistem evidentičara. Elektronsko i operatersko nadgledanje mogu da rezultuju podizanjem odgovarajućih bezbednosnih alarma. Bezbednosni alarmi predstavljaju ulaze procesa upravljanja bezbednosnim incidentima.

5.5. Arhiviranje zapisa

Zahtevi za čuvanjem zapisa se primenjuju na **ESS QCA** u celini kako na CA, tako i na RA funkcije sistema. Opšte politike čuvanja zapisa **ESS QCA** uključuju sledeće:

- tipove zapisa koji pokrivaju skup relevantnih zapisa iz poslovnog sistema **ESS QCA**,
- vremenske žigove zapisa – arhivirani zapisi **ESS QCA** imaju jasno naznačene odrednice vremena kada su kreirani i poslednji put modifikovani pre finalnog čuvanja u arhivi,
- period čuvanja – u skladu sa Zakonom,
- kontrole čuvanja u skladištu – u skladu sa ISO/IEC 27002 18.1.3 Zaštita zapisa i 18.1.4 Privatnost i zaštita podataka o ličnosti,
- izlučivanje po isteku vremena čuvanja - po isteku vremena čuvanja, arhivirani podaci se izlučuju iz sistema **ESS QCA**, odnosno bezbedno uništavaju korišćenjem automatizovanih elektronskih servisa i/ili procedura fizičkog uništenja. Nakon izlučivanja o njima ne ostaje trag u **ESS QCA** elektronskom i/ili fizičkom obliku,
- procedure u cilju dobijanja i verifikacije arhivskih informacija – na zahtev korisnika i/ili pouzdajućih strana **ESS QCA** može izdvojiti i dati na uvid arhivu čuvanih informacija iz poslovnih procesa. Pristup arhivi je obezbeđen iz prostorija matične lokacije **ESS QCA**.
- dokumentacija koja se u papirnoj formi dostavlja i stvara u RA telu se čuva u obezbeđenom prostoru. Sva dokumentacija koja je relevantna za proces izdavanja sertifikata se digitalizuje i kvalifikovano elektronski potpisuje od strane RA operatera.

5.6. Izmena ključeva

Period važenja sertifikata **ESS QCA** ograničen je na 30 godina za *Root* sertifikaciono telo, odnosno 10 godina za *Issuing* telo.

ESS QCA sprovodi zanavljanje sertifikata sertifikacionih tela u skladu sa Zakonom, eIDAS-om i Standardima. Sertifikati se zanavljaju uvek na novom paru RSA ključeva čija dužina odgovara preporukama/zahtevima Zakona, eIDAS-a i Standarda.

Sertifikat generisan za novi par ključeva se distribuira zainteresovanim stranama, telu koje održava registar pružalaca usluga od poverenja i javno objavljuje preko http publikacija **ESS QCA**.

5.7. Kompromitacija i oporavak u slučaju katastrofe

ESS QCA definiše pravila i procedure prema kojima se klasifikuju i rešavaju incidenti vezani za:

- Kompromitaciju ključeva **ESS QCA**
- Kompromitaciju procesa identifikacije korisnika
- Kompromitaciju procesa izdavanja sertifikata
- Kompromitaciju baze CA servisa
- Kompromitaciju informacija baze podataka **ESS QCA** CA tela
- Kompromitaciju informacija baze podataka **ESS QCA** RA tela
- Kompromitaciju informacija baze podataka zone za razmenu CA/RA tela.

Na mestima gde je primenjivo, za kritične resurse sistema primenjene su kontrole obezbeđenja visoke dostupnosti.

Za sve navedene resurse sistema obezbeđeni su odgovarajući BC/DR planovi zasnovani na odgovarajućoj backup strategiji. Backup strategija je obezbeđena za :

- Nosioce privatnih ključeva CA tela
- Baze podataka CA servisa
- Baze podataka RA tela, CA/RA zone i CA tela
- Baze podataka X.500 direktorijuma, kao i ostale elemente sistema, gde je backup potreban u cilju skraćivanja RTO (recovery time objective).

U skladu sa BC/DR planovima, a u slučaju pojave prirodne ili druge vrste fizičke katastrofe koja bi delimično ili u potpunosti učinila neuslovnom postojeću matičnu lokaciju **ESS QCA**, operacije **ESS QCA** se privremeno sele u Zelen Data Centar u Vršcu, gde se na hladnoj rezervi sistema nastavlja rad do završetka oporavka od katastrofe na matičnoj lokaciji. Na ovoj lokaciji se minimalno restauriraju funkcije generisanja lista povučenih sertifikata, a prema dinamici i planu oporavka na matičnoj lokaciji.

5.8. Završetak rada CA ili RA

Planovi završetka rada CA ili RA tela **ESS QCA** treba da umanje negativne uticaje koje rizik prekida rada nosi sa sobom, da obezbede kontinuitet poslovnih procesa korisnika i pouzdajućih strana.

Planovi završetka rada **ESS QCA** tretiraju sledeće rizike:

1. Neočekivani prekid servisa kreiranja elektronskog potpisa na listi povučenih sertifikata za korisnike kojima je **ESS QCA** izdao kvalifikovani sertifikat za elektronski potpis, a u roku važnosti sertifikata;
2. Nedostupnost podataka o statusu sertifikata (CRL liste) za treće strane koje treba da prihvate ili odbiju sertifikate korisnika kojima je **ESS QCA** izdao sertifikat;
3. Nemogućnost upravljanja životnim ciklusom već izdatih sertifikata od strane **ESS QCA**,
4. Nemogućnost uvida u dokumentaciju iz poslovanja u zakonskom roku od 10 godina nakon isteka (opoziva) izdatog sertifikata;
5. Neovlašćeno korišćenje sredstava za kreiranje elektronskog potpisa u procesu izdavanja sertifikata, a nakon gašenja operativne funkcije izdavanja **ESS QCA**;
6. Neovlašćeno korišćenje infrastrukture ili delova infrastrukture koja je nekada korišćena u poslovnim procesima **ESS QCA.**

U slučaju prestanka rada **ESS QCA** u celini sprovodi se procedura u skladu sa Zakonom, a minimum operativnog rada koji obuhvata izdavanje lista povučenih sertifikata i povlačenje sertifikata po zahtevu korisnika realizuje sa matične lokacije E-Smart Systems d.o.o. do isteka ili povlačenja poslednjeg sertifikata izdatog korisnicima.

6. Tehničke bezbednosne kontrole

Tehničke bezbednosne kontrole **ESS QCA** primenjene su u cilju tretiranja rizika i odgovora na pretnje iz okruženja za sledeća **ESS QCA** dobra i procese:

1. Asimetrične parove ključeva R*oot* i *Issuing* **ESS QCA** CA tela
2. Asimetrične parove ključeva sertifikata korisnika izdatih od strane **ESS QCA**
3. Softversko rešenje **ESS QCA**, izvorne kodove rešenja i proces razvoja softvera
4. QSCD uređaje nosioce asimetričnog para ključeva kvalifikovanih sertifikata
5. Proces nabavke QSCD uređaja od spoljnjeg dobavljača
6. Aktivacione podatke privatnih ključeva **ESS QCA** CA tela
7. Aktivacione podatke privatnih ključeva povezanih sa sertifikatima korisnika izdatih od strane **ESS QCA**
8. Internu računarsku infrastrukturu koja učestvuje u procesima CA i RA tela **ESS QCA**
9. Baze podataka **ESS QCA** uključujući CA, RA i CA/RA zone
10. Servise javnih publikacija podataka i servisa **ESS QCA**
11. X.500 direktorijume infrastrukture **ESS QCA**
12. Konfiguracije mrežnih uređaja koji povezuju **ESS QCA** sa internom infrastrukturom E-Smart Systems ili sa zaštićenom mrežom Ministarstva
13. Proces izdavanja kvalifikovanih sertifikata za elektronski potpis
14. Proces potpisivanja liste povučenih sertifikata **ESS QCA**
15. Proces povlačenja kvalifikovanih sertifikata za elektronski potpis
16. Proces inicijalizacije QSCD uređaja
17. Proces identifikacije i registracije korisnika
18. Proces uručenja i aktiviranja sertifikata
19. Proces deblokade aktivacionog koda QSCD uređaja
20. Bazu znanja iz procesa **ESS QCA**
21. Operativnu dokumentaciju i zapise iz procesa pružanja usluga od poverenja.

6.1. Generisanje i instalacija asimetričnog para ključeva

Asimetrični parovi ključeva *Root* i *Issuing* CA tela **ESS QCA**, kao i privatni ključevi na QSCD uređajima štite se u skladu sa Zakonom (Uredba za pružanje kvalifikovanih usluga od poverenja, član 30. Upravljanje sopstvenim asimetričnim ključevima) i standardom ISO/IEC 27002 10.1.2 Upravljanje ključevima.

6.2. Zaštita privatnog ključa

ESS QCA koristi odgovarajuće kriptografske uređaje u cilju realizacije zahteva zaštite ključeva CA u skladu sa Zakonom i Standardima.

Privatni ključ kvalifikovanog sertifikata za elektronski potpis generiše se na QSCD uređaju čime je obezbeđena zaštita privatnog ključa korisnika u skladu sa Zakonom i Standardima.

6.3. Drugi aspekti upravljanja parom ključeva

Privatni ključ *Root* CA **ESS QCA** se koristi za elektronsko potpisivanje samopotpisanog *Root* CA sertifikata, *Issuing* CA sertifikata i liste opozvanih sertifikata *Root* CA tela. Druge svrhe korišćenja privatnog ključa *Root* CA **ESS QCA** su zabranjene.

Kriptografski algoritmi koje koristi *Root* CA telo za formiranje elektronskog potpisa obuhvataju SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom RSA ključa od 4096 bita. Period validnosti sertifikata je 30 godina. Period validnosti izdatih sertifikata *Issuing* CA tela je do 10 godina. Javni ključ *Root* CA **ESS QCA** je objavljen na adresi https://qca.e-smartsys.com/repo/ESS%20RQCA.cer koju održava E-Smart Systems d.o.o. Beograd, kao i https://epotpis.mtt.gov.rs/TrustedList/TSL-RS.xml koju održava nadležno Ministarstvo.

Kriptografski algoritmi koje koristi *Issuing* CA telo za formiranje elektronskog potpisa obuhvataju SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom RSA ključa od 2048 bita. Period validnosti sertifikata *Issuing* CA tela je 10 godina. Period validnosti izdatih kvalifikovanih sertifikata je do 5 godina. Do sada su izdata četiri Issuing CA sertifikata koja odgovaraju određenim verzijama tehničkog sistema formiranim u periodu od 2013. do 2019. Sertifikati su objavljeni na adresama https://qca.e-smartsys.com/repo/ESS%20IQCA1.cer ,

https://qca.e-smartsys.com/repo/ESS%20IQCA1(1).cer ,

https://qca.e-smartsys.com/repo/ESS%20IQCA1(2).cer ,

https://qca.e-smartsys.com/repo/ESS%20IQCA1(3).cer .

Sertifikati su objavljeni i na adresi https://epotpis.mtt.gov.rs/TrustedList/TSL-RS.xml koju održava nadležno Ministarstvo.

Za kvalifikovane sertifikate za elektronski potpis **ESS QCA** koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom RSA ključa od 2048 bita. Izdati sertifikati se ne publikuju.

ESS QCA će izvršiti izmenu gore navedenih kombinacija algoritama i dužina ključeva po nalogu Nadležnog organa ukoliko se u kriptografskoj teoriji i praksi pokažu slabosti navedenih algoritama i svetska kriptografska javnost preporuči pouzdanije algoritme.

6.4. Aktivacioni podaci

Za potrebe aktivacije privatnog ključa koriste se sledeći aktivacioni podaci:

- Za privatne ključeve **ESS QCA** *Root* CA i *Issuing* CA koristi se deljena tajna čiji su nosioci osobe od poverenja, a koja je sačuvana na PED ključevima, pridruženim HSM uređaju u procesu ceremonije inicijalizacije. U procesu aktivacije PED ključevi se kao deljena tajna koriste po šemi 2 od 4.
- Za privatne ključeve kvalifikovanih sertifikata za elektronski potpis na QSCD uređajima koje izdaje *Issuing* CA kao aktivacioni podatak koristi se PIN. U procesu izdavanja ovaj podatak se randomizuje i štampa na zaštićenu kovertu koja se distribuira korisniku posebno u odnosu na kvalifikovani sertifikat. U slučaju blokade PIN-a, korisniku je na raspolaganju aplikacija QCA QSCD Manager za promenu/deblokadu PIN-a kojom može samostalno uz pomoć PUK koda

deblokirati PIN. Korisniku se PIN može deblokirati i od strane **ESS QCA**. U procesu deblokade u prostorijama ESS QCA PIN se reinicijalizuje na novu random vrednost i štampa na zaštićenoj koverti uz novi PUK kod, kao i prilikom inicijalnog izdavanja.

- Kao posebni nivo zaštite samog kvalifikovanog sertifikata koristi se proces aktivacije i aktivacioni kod sertifikata. S obzirom na to da se par ključeva i sam sertifikat izdaju bez direktnog prisustva korisnika, sertifikat se izdaje u statusu *suspendovan*. Korisnik u transakciji izdavanja sertifikata dobija *aktivacioni kod* za sertifikat. Aktivacioni kod se od strane korisnika preko web aplikacije publikovane na https://qca.e-smartsys.com/ unosi u sistem, čime korisnik potvrđuje da je primio sertifikat iza čega se sertifikat aktivira i na sledećoj CRL više ne nalazi na listi suspendovanih sertifikata.

6.5. Bezbednosne kontrole računara

Računarska infrastruktura poslovno/tehničkog sistema **ESS QCA** podeljena je na pet bezbednosnih perimetara:

- Zonu javnog pristupa u kojoj se realizuju operacije **ESS QCA RA** tela, komunikacija i razmena informacija sa korisnicima, kao i preuzimanje personalizovanih QSCD uređaja,
- Zonu bezbednosti u kojoj se realizuju operacije **ESS QCA CA** tela i produkuju kvalifikovani sertifikati za elektronski potpis uz operativno angažovanje CA operatera,
- Visoku zonu bezbednosti u kojoj rade serveri CA tela i pridružena serverska infrastruktura bez permanentnog ljudskog prisustva,
- Zonu razmene informacija kojima pristupaju servisi **ESS QCA RA** i **ESS QCA CA** dela sistema koju čine serverski resursi koji rade potpuno autonomno,
- Zonu publikacija javnih informacija **ESS QCA** koja se nalazi na Azure cloud-u.

Svaka od ovih infrastrukturnih zona prati odgovarajući baseline bezbednosnih kontrola koje odgovaraju pretnjama i ranjivostima kojima su računarski i informacioni resursi u odgovarajućoj zoni izloženi.

Kao okvir za primenu bezbednosnih baseline-a koriste se ISO 27002, NIST 800-37 r2 i CA/Browser Forum Baseline requirements.

6.6. Životni ciklus tehničkih bezbednosnih kontrola

Za potrebe razvoja, održavanja i unapređenja **ESS QCA**, primenjeni su procesi iz životnog veka sistema u skladu sa ISO/IEC/IEEE 15288 i ISO/IEC 20000. Ovi procesi obuhvataju:

- Upravljanje infrastrukturom
- Upravljanje ljudskim resursima
- Upravljanje kvalitetom
- Upravljanje znanjem
- Projektno planiranje
- Upravljanje rizicima
- Upravljanje konfiguracijom
- Upravljanje promenama

- Upravljanje informacijama
- Obezbeđenje kvaliteta (QA)
- Prikupljanje i analiza poslovnih i sistemskih zahteva
- Definisanje i izradu arhitekture
- Definisanje i izradu dizajna
- Analizu sistema
- Implementaciju i integraciju
- Verifikaciju
- Tranziciju u operacije
- Procese validacije
- Operativne procese
- Procese održavanja
- Procese uklanjanja iz operativnog okruženja.

ESS QCA je ISO 20000 sertifikovani servis koji se od treće strane kontinuirano proverava na godišnjem nivou.

6.7. Mrežne bezbednosne kontrole

Organizacija mreže **ESS QCA** prati već uspostavljenu segmentaciju poslovnog sistema. Mreža **ESS QCA** je podeljena na segmente:

- **ESS QCA RA** - interni mrežni segment unutar mreže ESS deo korporativnog Windows AD sa primenjenim odgovarajućim politikama bezbednosti,
- **ESS QCA CA** zona visoke bezbednosti – potpuno izolovan mrežni segment bez propuštenog ulaznog saobraćaja i sa strogo kontrolisanim izlaznim saobraćajem prema internoj mreži ESS,
- **ESS DMZ** zona razmene informacija – DMZ segment na internoj mreži ESS bez formiranih publikacija prema internetu. Prihvata podatke iz RA i CA servisa/aplikacija preko WCF https servisa na koje je obavezno logovanje sertifikatima,
- ESS Azure cloud – Azure SAAS web publikacija https://qca.e-smartsys.com web sajta preko koga su publikovani elementi PKI (CRL, CRT/CER), dokumentacija iz procesa **ESS QCA**, online uputstva za korisnike i servisi provere statusa i aktiviranja sertifikata. Automatski prenos sadržaja iz/u Azure App service vrši se preko hibridne konekcije prema resursu u ESS DMZ zoni razmene i preko ftps protokola iz zone razmene **ESS DMZ** prema Azure App servisu. Komunikacija i razmena podataka je potpuno automatizovana. Hibridna konekcija ne zahteva publikaciju resursa kome se pristupa već se zasniva na izlaznom https saobraćaju u ovom slučaju iz zone razmene **ESS DMZ** prema Azure App servisu. Na ovaj način povezivanje sa Azure cloud-om nije izazvalo otvaranje za ulazni saobraćaj zone razmene **ESS DMZ**,
- **ESS QCA** testno i razvojno okruženje – poseban segment ESS interne infrastrukture na kome se nalaze namenski podignuti resursi za testiranje rešenja,
- **ESS QCA** izvodi skeniranja ranjivosti interne infrastrukture u periodima od tri meseca,
- **ESS QCA** izvodi penetration testove na godišnjem nivou ili posle promena na mrežnoj infrastrukturi.

6.8. Vremenski pečat

Sve transakcije informacionog sistema **ESS QCA** imaju odgovarajući vremenski žig. Kao izvor referentnog vremena u skladu sa Zakonom koristi se NTP server Direkcije za mere i dragocene metale.

Za formiranje elektronskog potpisa u skladu sa XADES i PADES standardima koristi se interni time stamp server koji predstavlja implementaciju RFC 3161 sa primenjenim update-om RFC 5816.

7. Profili sertifikata, CRL lista i OCSP

Ovo poglavlje specificira formate sertifikata, CRL lista koje izdaje **ESS QCA** i OCSP-a.

7.1. Profili sertifikata

ESS QCA izdaje sledeće vrste sertifikata:

- *Root* CA telo,
- *Issuing* CA telo,
- Kvalifikovani sertifikat za elektronski potpis za korisnike.

Profili su detaljno opisani u CPS dokumentu.

7.2. Profil CRL liste

ESS QCA podržava izdavanje CRL lista koje su u saglasnosti sa sledećim uslovima:

- brojevi verzija su podržani za CRL liste,
- atributi i ekstenzije CRL liste su popunjene i njihova kritičnost je posebno naznačena.

ESS QCA izdaje CRL verzije 2 sa osnovnim poljima i ekstenzijama.

Opozvani sertifikati kojima je istekla vremenska validnost ne nalaze se u CRL listi.

Profili su detaljno opisani u CPS dokumentu.

7.3. OCSP profil

ESS QCA podržava izdavanje OCSP odgovora verzije 1 definisanim u IETF RFC 6960. Kao izvor informacija za vraćanje podataka o statusu sertifikata OCSP koristi isključivo publikovanu CRL listu, tako da su odgovori vezani za status sertifikata preko oba kanala provere u svakom trenutku identični.

Prilikom vraćanja podataka o validnosti sertifikata OCSP prati informacije CRL:

- Za sertifikat koji se nalazi na CRL, a izdavalac naveden u OCSP request-u odgovara **ESS QCA** izdavajućem telu, biće vraćen status "**revoked**"
- Za sertifikat koji se **ne** nalazi na CRL, a izdavalac naveden u OCSP request-u odgovara **ESS QCA** izdavajućem telu biće vraćen status "**good**"
- Za sertifikat za koji je u OCSP request-u naveden izdavalac koji ne odgovara **ESS QCA** izdavajućem telu biće vraćen status "**unknown**".

OCSP je javno dostupan servis, publikovan na javno dostupnoj internet lokaciji https://qca.e-smartsys.com/ocsp/ESSQCA1, autorizovan izdatim OCSP sertifikatom.

Sertifikat OCSP responder-a izdat je od strane ESS QCA izdavajućeg tela prema profilu definisanom u CPS sa uključenom ekstenzijom *id-kp-OCSPSigning* extended key usage atributa sertifikata, kao i ekstenzijom *id-pkix-ocsp-nocheck*.

Kao mera zaštite od kompromitacije ključeva i sertifikata OCSP respondera, ovaj sertifikat se izdaje sa periodom važenja ne dužim od 6 meseci. Za aktivaciju ključa OCSP respondera koristi se lozinka prilikom kreiranja svakog odgovora.

8. Audit usaglašenosti i druge provere

ESS QCA obezbeđuje periodičnu proveru/audit saglasnosti svojih politika, uključujući ovu CP što uključuje i periodičnu superviziju od strane nadležnog organa Republike Srbije. Rad **ESS QCA** je takođe u saglasnosti sa najvažnijim međunarodnim i evropskim standardima u ovoj oblasti, kao i sa eIDAS-om.

U domenu izdavanja kvalifikovanih sertifikata, **ESS QCA** radi u okviru ograničenja definisanih Zakonom, kao i odgovarajućim podzakonskim aktima.

ESS QCA prihvata pod određenim uslovima i proveru/auditing internih procedura i pravila rada koja nisu javno dostupna u cilju unapređenja svojih usluga. **ESS QCA** evaluira rezultate ovakvih provera pre nego što ih implementira.

ESS QCA sprovodi redovne godišnje interne audit-e usklađenosti poslovanja sa ovom CP, kao i sa CPS dokumentom. Interni audit sprovode odgovarajući zaposleni ESS sa datim zaduženjima. U slučaju neusaglašenosti rada sa politikom, **ESS QCA** obustavlja dalje izdavanje kvalifikovanih sertifikata za elektronski potpis dok se ne otkloni neusaglašenost.

ESS QCA je ISO 20000 sertifikovani servis koji se proverava od treće strane na godišnjem nivou.

ESS QCA je upisano u Registar pružalaca kvalifikovanih usluga od poverenja od strane nadležnog Ministarstva trgovine, turizma i telekomunikacija i predmet je periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona i odgovarajućim podzakonskim aktima.

9. Drugi poslovni i pravni aspekti

9.1. Cene

ESS QCA naplaćuje izdavanje/obnovu kvalifikovanih sertifikata za elektronski potpis.

Objavljivanje cena kvalifikovanih sertifikata i drugih usluga od poverenja se vrši putem on-line repozitorijuma https://qca.e-smartsys.com, partnera **ESS QCA** (treća lica) ili putem odgovarajućeg ugovora tamo gde je to primenljivo.

ESS QCA zadržava pravo da promeni uslove naplate kvalifikovanih sertifikata.

9.2. Finansijska odgovornost

ESS QCA obezbeđuje garancijski plan osiguranja za pokrivanje svih odgovornosti u skladu sa obavezama u Zakonu i podzakonskim aktima.

ESS QCA ne prihvata nikakvu drugu odgovornost koja izlazi iz pokrivanja definisanog pomenutim ograničenim garancijskim planom.

Korisnik je dužan da obešteti **ESS QCA** u odnosu na bilo koje aktivnosti ili propuste u odgovornosti, bilo koje gubitke ili štetu, kao i za bilo kakve troškove bilo koje vrste, uključujući razumne naknade advokata, koje bi **ESS QCA** mogao da ima kao rezultat:

- bilo kog lažnog ili pogrešno prezentovanog podatka dostavljenog od strane korisnika,
- bilo kog propusta korisnika da dostavi dokaz da je pogrešna prezentacija ili propust učinjen iz nemarnosti ili sa namerom da se prevari **ESS QCA**, ili bilo koje lice koje koristi dobijeni sertifikat,
- neobezbeđivanja odgovarajuće zaštite korisnikovog privatnog ključa, nekorišćenja bezbednog sistema kako je zahtevano, ili neizvršenja odgovarajućih preventivnih mera neophodnih da se spreči kompromitacija, gubitak, objavljivanje, modifikacija ili neautorizovano korišćenje korisnikovog privatnog ključa, ili napada na integritet *ESS RQCA* i *IQCA1* privatnih ključeva,
- kršenja bilo kojih zakona koji su primenljivi, uključujući one koji se odnose na zaštitu intelektualnih prava, bezbednost informacija, pristup računarskim sistemima, itd.

9.3. Poverljivost poslovnih informacija

Sertifikaciono telo **ESS QCA** postupa poverljivo sa sledećim podacima:

- sa svim zahtevima za dobijanje kvalifikovanog sertifikata za elektronski potpis,
- sa svim poverljivim podacima vezanim za finansijske obaveze,
- sa svim mogućim poverljivim podacima koji predstavljaju predmet međusobnih ugovora sa trećim licima i
- sa svim ostalim podacima koji su navedeni u internim pravilima rada **ESS QCA.**

ESS QCA javno objavljuje samo one poslovne podatke koji nisu poverljive prirode, a u skladu sa važećim zakonodavstvom.

9.4. Privatnost i zaštita podataka o ličnosti

ESS QCA se pridržava pravila privatnosti i zaštite podataka o ličnosti i pravila poverljivosti kako je propisano zakonom, kao i u CPS dokumentu, politici privatnosti i zaštite podataka o ličnosti.

Definicije poverljivih podataka navedene su u politici privatnosti i zaštite podataka o ličnosti.

ESS QCA ne objavljuje, niti se zahteva da objavljuje podatke o ličnosti bez autentikovanog i potvrđenog zahteva od strane:

- same strane za koju se takva informacija čuva,
- odgovarajućeg nadležnog organa.

ESS QCA zadržava pravo mogućnosti naplate procesiranja ovakvih zahteva.

Strane u komunikaciji koje zahtevaju i dobijaju poverljive informacije imaju dozvolu za to na osnovu pretpostavke da će oni te informacije koristiti za zahtevane svrhe, da će ih osigurati od kompromitacije i da će se uzdržavati od njihovog korišćenja i objavljivanja trećim stranama.

9.5. Prava intelektualnog vlasništva

ESS QCA poseduje i zadržava sva prava intelektualnog vlasništva pridružena njegovim bazama podataka, web sajtovima, kvalifikovanim sertifikatima za elektronski potpis koje izdaje, kao i bilo kojim drugim publikacijama koje na bilo koji način pripadaju ili potiču od strane **ESS QCA**, uključujući i ovaj dokument.

ESS QCA omogućava korisnicima, pretplatnicima i trećim stranama da koriste, kopiraju, distribuiraju i u svoje elektronske dokumente ugrađuju izdate sertifikate i CRL liste.

9.6. Izjava o garanciji

Nije primenljivo.

9.7. Nepriznavanje garancije

Nije primenljivo.

9.8. Ograničenja odgovornosti

Ni u kom slučaju ESS QCA ne prihvata odgovornost za štetu (direktnu ili indirektnu), gubitke, troškove i potraživanja koja proizilaze ili su nastali kao posledica korišćenja kvalifikovanog sertifikata, i to:

- korišćenje kvalifikovanih sertifikata za namene i na način koji nije izričito predviđen u CP i CPS,
- nepravilno ili pogrešno obezbeđenje lozinki ili privatnih ključeva korisnika kvalifikovanog sertifikata, otkrivanje poverljivih podataka ili ključeva trećim licima i neodgovorno postupanje korisnika kvalifikovanog sertifikata,
- zloupotrebu, odnosno upade u informacioni sistem korisnika kvalifikovanog sertifikata i na taj način dolaska do podataka o kvalifikovanim sertifikatima od strane neovlašćenih lica,
- nepostupanje ili loše postupanje sa podacima u okviru informacione infrastrukture korisnika kvalifikovanog sertifikata ili trećih lica,
- neproveravanje podataka, validnosti i statusa kvalifikovanih sertifikata u registru opozvanih kvalifikovanih sertifikata,

- neproveravanje vremena validnosti kvalifikovanih sertifikata,
- postupanje korisnika kvalifikovanog sertifikata ili trećeg lica suprotno informacijama i obaveštenjima koje objavljuje ESS QCA, CP, CPS i drugim propisima,
- omogućeno korišćenje, odnosno zloupotrebu kvalifikovanog sertifikata korisnika od strane neovlašćenih lica,
- sadržaj samih podataka koji se potpisuju korišćenjem kvalifikovanih sertifikata, već samo da je kod potpisa nad tim podacima korišćen kvalifikovani sertifikat izdat od strane ESS QCA,
- upotrebu i pouzdanost rada mašinske i programske opreme korisnika kvalifikovanog sertifikata.

9.9. Odštete

Za štetu nastalu upotrebom kvalifikovanog sertifikata za elektronski potpis i njemu pridruženog privatnog ključa usled nepoštovanja odredbi Ugovora, CP, CPS i važećeg zakonodavstva, odgovorna je stranka koja je istu prouzrokovala.

9.10. Period važnosti i kraj validnosti CP

Sertifikaciono telo **ESS QCA** zadržava pravo da izmeni CP i da nadogradi infrastrukturu bez prethodnog obaveštavanja vlasnika kvalifikovanog sertifikata za elektronski potpis.

U slučaju izmene uslova izdavanja i/ili korišćenja kvalifikovanih sertifikata za elektronski potpis izmenjena CP dobija novu verziju i novi OID. Svaki kvalifikovani sertifikat za elektronski potpis ima u sebi upisan OID CP po kojoj je izdat i uslovi korišćenja po toj verziji CP važe do vremenskog isteka kvalifikovanog sertifikata ili njegovog opoziva.

9.11. Pojedinačna obaveštenja i komunikacija sa zainteresovanim stranama

Kontakt podaci sertifikacionog tela objavljeni su na on-line repozitorijumu https://qca.e-smartsys.com i navedeni u poglavlju 1.5.2.

Obaveštavanje korisnika o promenama uslova poslovanja **ESS QCA** obavlja se isključivo putem site-a, a samo u specifičnim situacijama **ESS QCA** zadržava pravo obaveštavanja korisnika putem mail-a.

ESS QCA obaveštava nadležno Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge izdavanja kvalifikovanog sertifikata za elektronski potpis. U slučaju da se narušena bezbednost odnosi na zaštitu podataka o ličnosti, **ESS QCA** obaveštava i poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

9.12. Dopune

Dopune ili promene ovog CP dokumenta sertifikaciono telo može da objavi u obliku dopuna ili promena ovog CP.

Sve dopune koje ne menjaju uslove izdavanja i/ili korišćenja kvalifikovanih sertifikata za elektronski potpis ne utiču na menjanje identifikatora CP već samo na novu podverziju.

9.13. Postupak rešavanja sporova

Ukoliko dođe do spora između **ESS QCA** i pretplatnika ili korisnika kvalifikovanog sertifikata u vezi međusobnih prava i obaveza ili tumačenja ugovora ili nekog drugog dokumenta donetog od strane

ESS QCA, **ESS QCA** će nastojati da spor reši mirnim putem, sporazumno, a ukoliko do sporazuma ipak ne dođe, spor će rešavati nadležni sud u Beogradu.

9.14. Merodavno pravo

Za tumačenje i primenu ove CP merodavno je pravo Republike Srbije.

9.15. Saglasnost sa primenljivim zakonima

Ova CP je u potpunosti u skladu sa odgovarajućom zakonskom regulativom Republike Srbije, i to pre svega sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima. Sve pravne stvari koje se odnose na **ESS QCA** i/ili koje se odnose na sertifikate izdate od strane **ESS QCA** će biti procesuirane od strane odgovarajućeg suda u Srbiji.

ESS QCA posluje u skladu sa svim zakonima i podzakonskim aktima koji uređuju ovu oblast poslovanja, kao i eIDAS-om i odgovarajućim standardima kako je nabrojano u poglavlju 1. (Uvod) ovog dokumenta.

9.16. Ostale odredbe

Usluga izdavanja kvalifikovanog sertifikata za elektronski potpis kao i njegovo korišćenje regulisani su posebnim ugovorom između sertifikacionog tela **ESS QCA** i pravnog ili fizičkog lica, a u skladu sa Zakonom i drugim zakonskim propisima.

Korisnik kvalifikovanog sertifikata nema pravo da prava iz zaključenog ugovora sa **ESS QCA**, u celini ili delimično, prenese na treća lica.

9.17. Druge odredbe

Nema.

10.Istorija dokumenta

Verzija	Datum	Opis promena
0.1	01.11.2011.	Inicijalni dokument
0.2	10.08.2013.	Usklađivanje dokumenta sa software-skim rešenjem
1.0	22.10.2013.	Inicijalna verzija
1.1	25.11.2013.	Manje izmene dokumenta
1.2	14.01.2014.	Usklađivanje sa primedbama komisije
1.3	28.02.2014.	Usklađivanje sa primedbama komisije
1.4	13.03.2014.	Usklađivanje sa primedbama komisije
1.5	01.04.2014.	Gramatičke ispravke
1.6	03.06.2014.	Proširenje pretplatnika
1.7	21.01.2016.	Izmena osobe odgovorne za ovu CP
2.0	25.10.2018.	Usaglašavanje sa Zakonom
2.1	26.03.2019.	Manje izmene dokumenta
2.2	12.04.2019.	Manje izmene dokumenta
2.3	25.04.2019.	Usklađivanje sa nalazima provere
2.4	10.02.2020.	Izmene u poglavlju 5.8. u skladu sa novim Internim pravilom 10
2.5	21.08.2020.	Unapređenja podrške upravljanja rizicima i manje izmene dokumenta
2.6	15.01.2021.	Uvođenje novog tipa QSCD uređaja

11.Reference

- Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju („Službeni glasnik RS“ broj 94/17)
- Pravilnik o bližim uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati („Službeni glasnik RS“ broj 34/18 i 82/18)
- Pravilnik o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo („Službeni glasnik RS“ broj 34/18, 3/20 i 87/20)
- Uredba o uslovima za pružanje kvalifikovanih usluga od poverenja („Službeni glasnik RS“ broj 37/18)
- RFC 3647 – Request For Comments: 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 5280 – Request For Comments: 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- Praktična pravila izdavanja kvalifikovanih sertifikata za elektronski potpis Sertifikacionog tela E-Smart Systems d.o.o.
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014

12.Kompanije i organizacije

[1] E-Smart Systems d.o.o., http://www.e-smartsys.com
[2] IANA (Internet Assigned Numbers Authority), http://www.iana.org
[3] ETSI (European Telecommunications Standards Institute),
https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx

Potpisi:

Ana Marković
ESUPL000000000151-1203977715239

Digitally signed by Ana Marković
ESUPL00000000015 1-1203977715239
Date: 2021.01.14 12:49:37 +01'00'

Srećko Atanasković
ESUPL000000000027-2402962870013

Digitally signed by Srećko Atanasković
ESUPL000000000027-2 402962870013
Date: 2021.01.14 14:46:59 +01'00'