OCE-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-191

Šifra dokumenta

Praktična pravila izdavanja kvalifikovanih sertifikata za elektronski potpis

(CPS - Certification Practice Statement)

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 **Praktična pravila za izdavanje kvalifikovanih sertifikata za elektronski potpis** koja se odnose na usluge od poverenja koje pruža **ESS QCA** u skladu sa Politikom izdavanja kvalifikovanih sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.509.1.1.2) i u politici definisanim Zakonom, EU regulativom i Standardima.

1.1. Pregled

ESS QCA je odgovorno za pružanje usluga od poverenja, koje **za uslugu izdavanja kvalifikovanih sertifikata za elektronski potpis** uključuju sledeće servise, i to:

- Registraciju korisnika,
- Formiranje asimetričnog para ključeva za korisnike,
- Formiranje kvalifikovanog sertifikata za elektronski potpis,
- Distribuciju privatnog ključa i kvalifikovanih sertifikata za elektronski potpis (QSCD) korisnicima na način u skladu sa Zakonom,
- Upravljanje procedurom opoziva i suspenzije kvalifikovanih sertifikata za elektronski potpis,
- Obezbeđivanje statusa opozvanosti 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**) i
2. Praktična pravila za izdavanje kvalifikovanih sertifikata za elektronski potpis (u daljem tekstu: **CPS**) - ovaj dokument.

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 interna dokumenta i predstavljaju poslovnu tajnu sertifikacionog tela. Interna pravila sadrže detalje o:

1. *sistemu za upravljanje dobrima i fizičku zaštitu ESS QCA;*
2. *sistemu za mrežno povezivanje, logičku kontrolu pristupa, zaštitu informacija u skladištu i transportu ESS QCA;*
3. *sistemu za upravljanje ključevima u ESS QCA;*
4. *sistemu distribuirane odgovornosti u ESS QCA;*
5. *sistemu obezbeđenja kontinuiteta poslovanja i oporavka od katastrofe u ESS QCA;*
6. *proceduri ceremonije podizanja ESS QCA;*
7. *operativnim procedurama rada i upravljanju incidentima ESS QCA;*
8. *procedurama backup-a, arhiviranja i izlučivanja u ESS QCA;*
9. *procedurama nadzora ESS QCA;*
10. *planu završetka rada ESS QCA,*
11. *razvoju i deployment-u softverskog rešenja ESS QCA i*
12. *oceni ranjivosti i testiranju bezbednosti ESS QCA.*

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 predmet je periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima Republike Srbije.

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 - 1.3.6.1.4.1.30496.509.1.2.2
{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) CPS (2) verzija (2)}

Politika izdavanja kvalifikovanih sertifikata za elektronski potpis koja odgovara ovom CPS je 1.3.6.1.4.1.30496.509.1.1.2. i opisana je u dokumentu CP sa istim OID.

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 verziji CP koja odgovara ovom CPS.

1.3. Učesnici u PKI sistemu ESS QCA

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

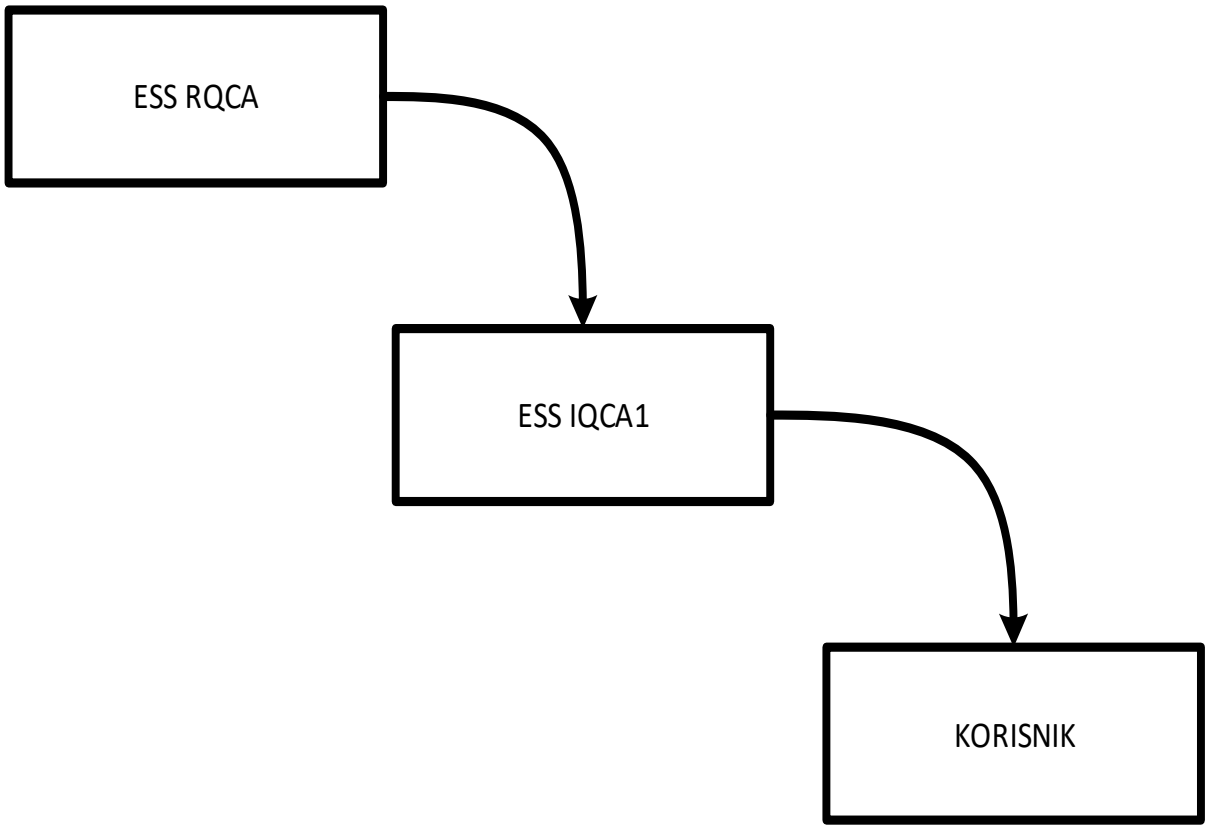
1.3.1. ESS QCA

ESS QCA je pružalac kvalifikovanih usluga od poverenja koji izdaje kvalifikovane sertifikate za elektronski potpis. **Politika izdavanja kvalifikovanih sertifikata za elektronski potpis (CP)** i **Praktična pravila izdavanja kvalifikovanih sertifikata za elektronski potpis (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 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.

Obaveze ESS QCA

ESS QCA garantuje da će sprovoditi sve procedure definisane ovim CPS. **ESS QCA** se obavezuje na:

1) Potpunu usaglašenost sa zvanično objavljenim CP i CPS,
2) Redovno ažuriranje dokumenata CP i CPS i javno publikovanje,
3) Objavljivanje kontakt detalja sertifikacionog autoriteta,
4) Obezbeđivanje usluga od poverenja u skladu sa Zakonom i podzakonskim aktima,
5) Obezbeđivanje infrastrukture i usluga od poverenja, uključujući uspostavljanje i održavanje **ESS QCA** repozitorijuma i odgovarajućeg web sajta u cilju pružanja usluga od poverenja,
6) Obezbeđivanje sigurnih mehanizama koji uključuju mehanizam generisanja ključeva, zaštite ključeva, kao i procedure deljenja tajni u skladu sa svojom PKI infrastrukturom,
7) Obezbeđivanje obaveštavanja u slučaju kompromitacije sopstvenog privatnog ključa,
8) Bezbedno generisanje ključeva na QSCD uređajima za korisnike,
9) Izdavanje kvalifikovanih sertifikata u skladu sa Zakonom, CP i ovim CPS,
10) Obaveštavanje korisnika da su kvalifikovani sertifikati generisani za njih, kao i o načinu preuzimanja kvalifikovanih sertifikata,
11) Obaveštavanje podnosioca zahteva ukoliko **ESS QCA** nije sposobno da izvrši validaciju njihove aplikacije za dobijanje kvalifikovanih sertifikata u skladu sa CP i ovim CPS,
12) Izdavanje kvalifikovanih sertifikata u skladu sa CP i ovim CPS nakon prijema validnog zahteva od strane RA koje radi u okviru **ESS QCA** mreže,
13) Opoziv kvalifikovanih sertifikata koji su izdati u skladu sa CP i ovim CPS nakon prijema validnog zahteva za opoziv sertifikata od strane autorizovanog lica koje može da zahteva opoziv,
14) Obezbeđivanje podrške korisnicima i trećim stranama kao što je opisano u CP i ovim CPS,
15) Objavljivanje ažurne, tačne i bezbednim merama zaštićene liste opozvanih sertifikata (CRL liste), u skladu sa CP i ovim CPS koja je dostupna svim zainteresovanim stranama,
16) Obezbeđivanje vidljivog podatka u registru opozvanih sertifikata o tačnom datumu i vremenu (sat i minut) opoziva sertifikata,
17) Dostavljanje kopije CP i ovih CPS, kao i ostalih primenljivih dokumenata po zahtevu neke od strana.

ESS QCA potvrđuje da, osim gore navedenih, nema drugih obaveza po ovom CPS dokumentu.

Odgovornosti ESS QCA

ESS QCA je odgovorno za izvršavanje gore navedenih obaveza u obimu koji određuje zakonska regulativa Republike Srbije.

1) **ESS QCA** nije odgovorno za zaštitu privatnih ključeva korisnika namenjenih za kreiranje kvalifikovanog elektronskog potpisa po njihovom preuzimanju od strane korisnika.
2) **ESS QCA** nije odgovorno za neodgovarajuću proveru validnosti kvalifikovanih sertifikata od strane koja se pouzdaje u sertifikat izdat od strane **ESS QCA**.

3) **ESS QCA** nije odgovorno za moguću zloupotrebu kvalifikovanih sertifikata koja je nastala usled neispunjavanja obaveza korisnika ili treće strane koja se pouzdaje u kvalifikovani sertifikat izdat od strane **ESS QCA**.
4) **ESS QCA** nije odgovorno za neizvršavanje svojih obaveza koje su posledica vanredne situacije ili više sile.

1.3.2. Registraciona tela ESS QCA

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

Registraciona tela mogu biti:

- **ESS QCA** na centralnoj lokaciji, kao **centralno RA**. 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 podnosiocima zahteva, pretplatnicima i korisnicima **ESS QCA** u cilju isporuke usluga od poverenja. U tom smislu, registraciona tela **ESS QCA**:

- Prihvataju, analiziraju, potvrđuju ili odbijaju registraciju odgovarajućih zahteva za sertifikatima,
- Registruju podnosioce zahteva za korišćenje **ESS QCA** usluga od poverenja,
- Sprovode sve korake u proceduri identifikacije pravnog ili fizičkog lica u skladu sa Zakonom, kao i proveru tačnosti podataka u Zahtevu za izdavanje/promenu statusa kvalifikovanog sertifikata,
- Koriste službene i overene dokumente u cilju provere identiteta korisnika,
- Nakon potvrde aplikacije korisnika, obaveštavaju **ESS QCA** u cilju izdavanja kvalifikovanog sertifikata,
- Iniciraju proces opoziva ili suspenzije sertifikata od strane **ESS QCA**.

Registraciona tela **ESS QCA (RA)** deluju lokalno u okviru njihovog sopstvenog konteksta geografskog ili poslovnog partnerstva koje je potvrđeno i autorizovano od strane **ESS QCA**. **ESS QCA** registraciona tela deluju u skladu sa praksom, procedurama i osnovnim dokumentima rada **ESS QCA**. Ne postoji ograničenje u smislu broja registracionih tela koja mogu biti pridružena **ESS QCA PKI** infrastrukturi.

ESS QCA obezbeđuje registracionim telima u svojoj infrastrukturi neophodnu tehnologiju i *know-how*, kao i odgovarajući trening, u cilju postizanja visokog nivoa obučenosti u skladu sa **ESS QCA** funkcionalnim zahtevima.

RA obaveze

1. Prijem aplikacija za izdavanje kvalifikovanog sertifikata za elektronski potpis u skladu sa CP i ovim CPS,
2. Izvršavanje svih aktivnosti na identifikaciji i proveri autentičnosti podnosioca zahteva u skladu sa opisom **ESS QCA** procedura, CP i ovim CPS,
3. Dostavljanje zahteva podnosioca do **ESS QCA** u elektronski potpisanoj poruci (zahtev za izdavanje kvalifikovanog sertifikata), u skladu sa CP i ovim CPS,
4. Ukoliko je RA ovlašćen da raspolaže sa prethodno pripremljenim QSCD uređajima, obaveza je upisa sertifikata na QSCD uređaj i štampa PIN koverte, kao i njihovo uručenje korisniku,
5. Zapisivanje svih aktivnosti u dnevniku događaja,
6. Prijem, verifikacija i prosleđivanje ka **ESS QCA** svih zahteva za opoziv i suspenziju **ESS QCA** izdatih kvalifikovanih sertifikata u skladu sa **ESS QCA** procedurama, CP i ovim CPS.

ESS QCA preuzima odgovornost za poštovanje ove CP čak 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.

Identifikacioni podaci pretplatnika se, u izdatom kvalifikovanom sertifikatu za elektronski potpis, navode u atributima polja Subject. Ovi atributi omogućavaju trećim stranama da mogu identifikovati korisnika kao pripadnika pretplatnika. U ovom slučaju, pretplatnička saglasnost i saglasnost sa Opštim uslovima za pružanje usluga od poverenja omogućavaju pretplatnicima da podnesu zahtev za izdavanje, opoziv ili suspenziju korisnikovih kvalifikovanih sertifikata za elektronski potpis u kojima je pretplatnikov identifikacioni podatak u atributima polja Subject, konkretno Subject:O i atributima organizationIdentifier (oid: 2.5.4.97) sa vrednostima MB:RS-<matični broj firme> (obavezan) i VATRS-<PIB> (opcionalni).

Obaveze pretplatnika

Pretplatnici usluga od poverenja **ESS QCA** su u obavezi da:

1) Poštuju CP i CPS publikovane od strane **ESS QCA**,
2) Pruže tačne i pouzdane podatke u komunikaciji sa RA telima **ESS QCA**,
3) Upoznaju se, razumeju i saglase se sa svim stavovima i uslovima u CP i ovim CPS, kao i drugim dokumentima koji su objavljeni na **ESS QCA** repozitorijumu,
4) Obaveste RA telo o bilo kojim promenama podataka koji su ranije dostavljeni.

1.3.4. Korisnici

Korisnik je fizičko lice kome je izdat kvalifikovani sertifikat za elektronski potpis. Korisnici sa **ESS QCA** potpisuju U*govor za usluge izdavanja i upravljanja kvalifikovanim sertifikatom za elektronski potpis* koje pruža **ESS QCA** – **korisnički ugovor**. Korisnički ugovor omogućava korisniku da podnese zahtev za

opoziv, suspenziju, aktivaciju svog kvalifikovanog sertifikata za elektronski potpis ili deblokadu PIN-a QSCD uređaja.

Identifikacioni podaci korisnika se u izdatom kvalifikovanom sertifikatu za elektronski potpis navode u polju *Subject.*

Obaveze korisnika

Korisnici usluga od poverenja **ESS QCA** su u obavezi da:

1) Poseduju odgovarajuća znanja i, ako je neophodno, pohađaju odgovarajuće obuke za korišćenje kvalifikovanih sertifikata za elektronski potpis i usluga od poverenja,
2) Poštuju CP i CPS publikovane od strane **ESS QCA**,
3) Pruže tačne i pouzdane podatke u komunikaciji sa RA telima **ESS QCA**,
4) Upoznaju se, razumeju i saglase se sa svim stavovima i uslovima u CP i ovim CPS, kao i drugim dokumentima koji su objavljeni na **ESS QCA** repozitorijumu,
5) Uzdržavaju se od narušavanja integriteta i činjenja neispravnim kvalifikovanog sertifikata izdatog od strane **ESS QCA**,
6) Koriste **ESS QCA** kvalifikovane sertifikata samo za legalne i autorizovane svrhe u skladu sa CP i ovim CPS, kao i važećim zakonskim aktima,
7) Obaveste RA telo o bilo kojim promenama podataka koji su ranije dostavljeni,
8) Prekinu korišćenje kvalifikovanog sertifikata za elektronski potpis ukoliko je bilo koja informacija u sertifikatu postala nevalidna,
9) Prekinu korišćenje kvalifikovanog sertifikata za elektronski potpis ukoliko sam sertifikat postane nevalidan,
10) Uzdrže se od korišćenja javnog ključa koji odgovara privatnom ključu koji je sertifikovan od strane **ESS QCA**, u izdatom kvalifikovanom sertifikatu, pod istim imenom za potrebe izdavanja drugih sertifikata,
11) Koriste bezbedne uređaje i proizvode koji obezbeđuju odgovarajuću zaštitu privatnih ključeva,
12) Spreče kompromitaciju, gubljenje, objavljivanje, modifikaciju ili bilo kakvo drugo neautorizovano korišćenje svog privatnog ključa,
13) Prijave svaku moguću zloupotrebu svog privatnog ključa i u tom slučaju podnesu, bez odlaganja, zahtev za opoziv kvalifikovanog sertifikata.

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. Treće strane mogu da korisnika identifikuju kao pripadnika pretplatnika na osnovu atributa *organizationName* u telu kvalifikovanog sertifikata za elektronski potpis. **ESS QCA** obezbeđuje pouzdanost i verodostojnost identifikacionih podataka korisnika i pretplatnika ukoliko je urađena verifikacija kvalifikovanog sertifikata za elektronski potpis.

Verifikacija kvalifikovanog elektronskog potpisa obuhvata:

1. 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.

2. Proveru potpisa elektronskog dokumenta na bazi javnog ključa koji se nalazi u korisnikovom kvalifikovanom sertifikatu za elektronski potpis.

Obaveze trećih strana

Strana koja se oslanja na **ESS QCA** izdati kvalifikovani sertifikat obavezna je da:

1) Poseduje odgovarajuća znanja o korišćenju kvalifikovanih sertifikata za elektronski potpis i drugih tehnologija vezanih za usluge od poverenja,
2) Upozna se sa **CP** i **CPS** u vezi navedenih uslova koji važe za treće strane,
3) Poštuje i sprovodi odredbe iz **CP** i ovih **CPS,**
4) Verifikuje **ESS QCA** izdati kvalifikovani sertifikat:
    a. Proverom da je lanac sertifikata od *Root CA* sertifikata kompletan,
    b. Proverom opozvanosti sertifikata u lancu,
    c. Proverom da su svi sertifikati u lancu validni u vremenskom trenutku provere sertifikata,
5) Proveri kompletnost podataka u kvalifikovanom sertifikatu izdatom od strane **ESS QCA**, kao i da proveri da li dati sertifikat služi odgovarajućoj oblasti primene koja je navedena u sertifikatu,
6) Verifikuje kvalifikovani elektronski potpis,
7) Razumno se osloni i pouzda na **ESS QCA** izdati kvalifikovani sertifikat u skladu sa odgovarajućim okolnostima.

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 kompanije E-Smart Systems d.o.o. 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 CPS

1.5.1. Organizacija administriranja CPS

ESS QCA je odgovorno za propisnu administraciju ovih CPS, 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 CPS dokumenta

Osoba u **ESS QCA** odgovorna za ovu CPS 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 CPS dokumenta

CPS 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

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 Zakon.

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.

Podnošenje zahteva za izdavanje kvalifikovanog sertifikata za elektronski potpis – zahtev poslat od strane lica koje zahteva kvalifikovani sertifikat (podnosilac zahteva) ka ESS QCA u cilju izdavanja kvalifikovanog sertifikata za elektronski potpis.

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

Politika izdavanja kvalifikovanih sertifikata za elektronski potpis – imenovan skup pravila koji indicira primenljivost sertifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbednosnim zahtevima.

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

Praktična pravila izdavanja 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 sertifikata – privremeno ukidanje validnosti datog 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 kvalifikovanim sertifikatima uključuju generisanje, čuvanje, isporuku, objavljivanje, suspenziju i opoziv kvalifikovanog 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
JAK – Jednokratni aktivacioni kod
JIK – Jedinstveni identifikator korisnika
JMBG – Jedinstveni matični broj građana
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:

- ova praktična pravila izdavanja kvalifikovanih sertifikata za elektronski potpis (CPS),
- politiku izdavanja kvalifikovanih sertifikata za elektronski potpis (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 na bilo koji drugi pogodan način.

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.

Iz razloga njihove osetljivosti i poslovne tajne, **ESS QCA** neće publikovati interna pravila rada koja se odnose na izvesne podkomponente i elemente koji uključuju bezbednosne kontrole, procedure koje se odnose na upravljanje ključevima, distribuiranu odgovornost, bezbednost registracionog tela, postupke u vanrednim situacijama i sve ostale bezbednosno osetljive procedure.

2.3. Vreme i frekvencija publikovanja

ESS QCA publikuje informacije o statusu opozvanosti izdatih kvalifikovanih sertifikata (CRL liste), kao što je naznačeno i precizirano u ovom dokumentu. Maksimalno dozvoljeno kašnjenje od izdavanja CRL liste do publikovanja je jedan sat. 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.

ESS QCA ima implementirane logičke i fizičke kontrole pristupa u cilju sprečavanja neautorizovanog dodavanja, promene ili brisanja podataka.

3. Identifikacija i autentikacija korisnika

Obaveza ESS QCA je da obezbedi identifikaciju i autentikaciju podnosioca zahteva i korisnika. Proces identifikacije podnosioca zahteva i korisnika **ESS QCA** je opisan *u Internom pravilu 7 Operativne procedure rada i upravljanje incidentima ESS QCA*.

3.1. Nazivi

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

*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

ESS QCA pri obradi zahteva za izdavanje/opoziv/suspenziju kvalifikovanog sertifikata za elektronski potpis proverava verodostojnost svih dostavljenih podataka o pretplatniku i podnosiocu zahteva za izdavanje kvalifikovanog sertifikata za elektronski potpis. 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	Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS

elektronski sertifikat za elektronski potpis za fizičko lice	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 kvalifikovane sertifikate korisnicima, kao ni kvalifikovane sertifikate zasnovane na pseudo podacima.

3.2. Inicijalna provera identiteta

3.2.1. Identifikacija pretplatnika

Obavezni podaci koji se moraju dostaviti **ESS QCA** pri identifikaciji pretplatnika su:

- Naziv,
- matični broj,
- PIB,
- email adresa.

ESS QCA verodostojnost dostavljenih podataka o pretplatniku proverava na osnovu zapisa u registrima APR-a, Poreske uprave i NBS-a, kao i na osnovu OP obrasca:

- Naziv i matični broj pretplatnika se proveravaju u registru APR-a.
- PIB i ostali dostavljeni podaci se proveravaju upoređivanjem podataka u registrima APR-a, NBS-a i Poreske uprave.
- Verodostojnost potpisa ovlašćenog lica na saglasnosti za izdavanje kvalifikovanog elektronskog sertifikata se proverava na osnovu OP obrasca ili drugog priloženog ovlašćenja koje sadrži deponovan potpis.

3.2.2. Identifikacije podnosioca zahteva (fizička lica pripadnici entiteta pravnog lica)

Obavezni podaci koji se moraju dostaviti **ESS QCA** o podnosiocu zahteva u vidu saglasnosti za izdavanje kvalifikovanog sertifikata za elektronski potpis popunjenu od strane pretplatnika su:

- ime i prezime,
- email adresa,
- mobilni telefon,
- vrsta i broj identifikacionog dokumenta,
- datum isteka važenja i zemlja izdavanja dokumenta* (u slučaju kada se pasoš koristi kao identifikacioni dokument).

Identifikacija podnosioca zahteva vrši se uz lično prisustvo podnosioca zahteva u RA telu **ESS QCA**, upoređivanjem podataka sa saglasnosti i podataka na identifikacionom dokumentu uključujući i proveru slike korisnika. Samo u slučaju da sve provere budu uspešne, zahtev se prihvata.

Identifikovani podaci pretplatnika i podnosioca zahteva se struktuiraju u X.500 *distinguished name* formu, elektronski potpisuju od strane RA operatera kao potvrda identifikacije i dostavljaju u CA.

3.2.3. Identifikacija podnosioca zahteva (fizička lica)

Identifikacija podnosioca zahteva koji je fizičko lice se vrši na osnovu priloženog identifikacionog dokumenta od strane podnosioca. Stoga je lično prisustvo podnosioca zahteva obavezno u procesu identifikacije i registracije.

Identifikovani podaci podnosioca zahteva se struktuiraju u X.500 *distinguished name* formu, elektronski potpisuju od strane RA operatera kao potvrda identifikacije i dostavljaju u CA.

Proces registracije korisnika završava se prihvatanjem sertifikata i potpisivanjem Korisničkog ugovora.

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 fizičkih 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 opoziv/suspenziju svog sertifikata. Zahtev 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 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 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

Sve operativne procedure **ESS QCA** opisane su *u Internom pravilu 7 Operativne procedure rada i upravljanje incidentima ESS QCA*.

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 koji obuhvata:

- popunjavanje pretplatničkog ugovora,
- popunjavanje forme saglasnosti,
- dostavljanje neophodne dokumentacije,
- potvrdu o uplati.

Potrebni podaci forme saglasnosti za kvalifikovane sertifikate su:

1. ime (podatak podnosioca zahteva),
2. prezime (podatak podnosioca zahteva),
3. tip identifikacionog dokumenta (lična karta za građane Republike Srbije, privremena lična karta ili pasoš za strane državljane) (podatak podnosioca zahteva),
4. broj identifikacionog dokumenta (podatak podnosioca zahteva),
5. oznaka zemlje izdavaoca pasoša (ukoliko je identifikacioni dokument pasoš) (podatak podnosioca zahteva),
6. datum isteka pasoša ukoliko je podnosilac zahteva strani državljanin (podatak podnosioca zahteva),
7. broj mobilnog telefona (podatak podnosioca zahteva),
8. email adresa (podatak podnosioca zahteva),
9. šifra QSCD uređaja na kome će biti izdat kvalifikovani sertifikat za elektronski potpis (podatak iz cenovnika **ESS QCA**),
10. trajanje kvalifikovanog sertifikata u godinama,
11. da li će se kvalifikovani sertifikat za elektronski potpis koristiti za rad sa državom,
12. naziv pravnog lica (podatak pretplatnika),
13. matični broj pravnog lica (podatak pretplatnika),
14. PIB (podatak pretplatnika),
15. email adresa pravnog lica (podatak pretplatnika),
16. ovlašćeno lice – lice ovlašćeno od strane pretplatnika za menjanje podataka na saglasnosti (podatak pretplatnika),

17. ovlašćeni email - email adresa sa koje ovlašćeno lice može da šalje zahteve za izmenu podataka o podnosiocima zahteva sa saglasnosti (podatak pretplatnika).

Proces održavanja podataka o pretplatnicima realizuje se unutar RA tela prilikom svakog podnošenja saglasnosti ili dostave novih podataka i obuhvata proveru i ažuriranje podataka: zanavljanje dokumenata pravosnažne potvrde nadležnog organa o registraciji (Izvoda iz APR) i obrasca „Overenih potpisa lica ovlašćenih za zastupanje“.
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.

Nakon provere validnosti podataka, RA operater sačinjava predračun i šalje kontakt licu pretplatnika.

Nakon evidencije uplate pretplatnika, RA telo šalje poruke podnosiocima zahteva sa saglasnosti (koristeći podatke upisane u poljima email i mobilni telefon) da dođu na lokaciju RA tela u cilju lične identifikacije.

U pozivu za dolazak koji se šalje email-om priloženi su:

- elementi saglasnosti za izdavanje kvalifikovanog sertifikata za elektronski potpis koji su definisani od strane pretplatnika,
- rok za obavljanje identifikacije,
- lokacije na kojima se mogu pročitati dokumenti CP, CPS i politike privatnosti i zaštite podataka o ličnosti.

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

- broj mobilnog telefona (podatak podnosioca zahteva),
- email adresa (podatak podnosioca zahteva),
- šifra QSCD uređaja na kome će biti izdat kvalifikovani sertifikat za elektronski potpis (podatak iz cenovnika **ESS QCA**),
- trajanje kvalifikovanog sertifikata u godinama,
- da li će se kvalifikovani sertifikat za elektronski potpis koristiti za rad sa državom,
- poštanska adresa (podatak podnosioca zahteva).

4.2. Procesiranje zahteva za dobijanje sertifikata

Podnosilac zahteva se javlja RA operateru koji vrši identifikaciju lica u unapred utvrđenom terminu. Da bi se identifikacija smatrala uspešnom, potrebno je da podnosilac zahteva poseduje identifikacioni dokument koji po broju i vrsti odgovara dokumentu navedenom u saglasnosti koja je u roku važenja, ako ista postoji, tj. ako je podnosilac zahteva fizičko lice pripadnik entiteta pretplatnika.

Za uspešno identifikovanog podnosioca zahteva, u slučaju da se zahteva kvalifikovani sertifikat za elektronski potpis za rad za državom, se unosi JMBG.

RA operater skenira, anonimizira i prilaže u informacioni sistem identifikacioni dokument.

RA operater struktuira podatke iz aplikacije u elektronski dokument zahteva za izdavanje kvalifikovanog sertifikata za elektronski potpis. RA operater stavlja svoj kvalifikovani elektronski potpis na elektronski dokument zahteva i zaštićenim kanalom ga dostavlja u CA telo **ESS QCA**.

U slučaju da je RA operater ovlašćen da raspolaže sa prethodno pripremljenim QSCD uređajima, u elektronski dokument zahteva uključuje i javni ključ sa jednog takvog QSCD uređaja. Kada se uspešno obrade svi koraci taj QSCD uređaj će biti uručen korisniku.

RA operater ima pravo da odbije zahtev i u tom slučaju mora da navede razlog odbijanja.

Po isteku roka važenja saglasnosti pretplatnika, na svim stavkama za koje se nisu pojavili podnosioci zahteva da lično budu identifikovani, biće automatski postavljen status odbijen.

Generisanje asimetričnog para ključeva na QSCD uređaju (pripremljen QSCD uređaj) se vrši samo u zaštićenim prostorijama CA tela **ESS QCA**. Ukoliko je RA telo ovlašćeno od strane **ESS QCA** da radi sa pripremljenim QSCD uređajem, pripremljen QSCD uređaj mu se dostavlja na bezbedan način.

4.3. Izdavanje sertifikata

Nakon dostave validnog elektronskog dokumenta zahteva za izdavanje sertifikata, CA operater **ESS QCA** sprovodi proces izdavanja odgovarajućeg sertifikata u sledećim koracima:

- verifikuje se kvalifikovani elektronski potpisa RA operatera nad elektronskim dokumentom zahteva,
- odobrava ili odbija pojedinačni zahtev iz elektronskog dokumenta,
- u elektronski dokument zahteva uključuje se javni ključ sa pripremljenog QSCD uređaja i vrši izdavanje kvalifikovanog sertifikata za elektronski potpis za odobrene zahteve u kojim nije postojao javni ključ,
- **ESS QCA** sistem obaveštava korisnika o tome da mu je sertifikat izdat i kako može da ga aktivira. Sertifikat se po izdavanju suspenduje zbog zaštite u transportu, a korisnik obaveštava o jednokratnom aktivacionom kodu kvalifikovanog sertifikata za elektronski potpis putem SMS poruke,
- CA operater upisuje na QSCD uređaj izdati kvalifikovani sertifikat za elektronski potpis ukoliko je u obradi zahteva radio sa pripremljenim QSCD uređajem. Ukoliko je RA operater dostavio zahtev sa javnim ključem dostavlja mu se izdati kvalifikovani sertifikat za elektronski potpis koji on upisuje na QSCD uređaj,
- RA telo se obaveštava o statusu obrade prosleđenog zahteva,
- u RA telu, RA operater štampa PIN kovertu.

Prilikom korišćenja sertifikata postoje dva aktivaciona koda:

- Jednokratni aktivacioni kod (JAK) kvalifikovanog sertifikata za elektronski potpis kojim korisnik preko on-line repozitorijuma https://qca.e-smartsys.com aktivira sertifikat nakon preuzimanja.
- PIN kod QSCD uređaja kojim se pristupa privatnom ključu.

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 kvalifikovani sertifikat nad istim parom ključeva, već reizdaje kvalifikovani sertifikat za već registrovanog korisnika sa novim parom asimetričnih ključeva.

Reizdavanje kvalifikovanog sertifikata se može uraditi ako je postojeći kvalifikovani 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 kvalifikovani 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 kvalifikovani 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 kvalifikovani sertifikat istekao ili opozvan, ukoliko žele da dobiju novi kvalifikovani sertifikat, moraju da podnesu zahtev za izdavanje novog kvalifikovanog sertifikata. Procedura je ista kao i za inicijalno izdavanje kvalifikovanog sertifikata. Novi kvalifikovani 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 kvalifikovanog sertifikata se navodi da je već registrovan da bi se koristio isti JIK u novom kvalifikovanom 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 postojećeg.

4.9. Suspenzija i opoziv sertifikata

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

- gubitka, krađe, modifikacije podataka, objavljivanja ili neke druge kompromitacije privatnog ključa korisnika sertifikata,
- kada izvršenje odgovarajućih obaveza lica koja su navedena u 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 koja 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 ili **ESS QCA** ukoliko postoji sumnja o kompromitaciji 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 korisnika koji je pripadnik entiteta pravnog lica
   Pretplatnik, pravno lice, ima pravo da podnese zahtev koji rezultuje opozivom sertifikata korisnika, pripadnika entiteta pravnog lica.
2. Korisnik
   Prema Zakonu (član 44.) korisnik je dužan da odmah zatraži opoziv svog sertifikata u slučaju gubitka, oštećenja uređaja ili promene podataka za formiranje elektronskog potpisa. Korisnik overeni zahtev u papirnoj ili elektronskoj formi podnosi u RA telo. RA verifikuje identitet strane koja je zahtevala opoziv na osnovu informacija koje su sadržane u identifikacionim podacima koje je korisnik dostavio RA telu. RA operater je dužan da pristigli zahtev obradi i prosledi u CA u toku istog radnog dana. Ukoliko podaci iz zahteva nisu verodostojni, zahtev se odbija i o tome obaveštava korisnik i **ESS QCA**. CA Operater je dužan da u toku istog radnog dana obradi zahtev za opoziv i obavesti korisnika o opozivu.
3. RA operater
   Ukoliko postoji greška u podacima upisanim u sertifikat, RA operater kreira zahtev za opoziv kvalifikovanog sertifikata za elektronski potpis, elektronski potpisuje zahtev i šalje ga u CA telo **ESS QCA**. CA Operater je dužan da proveri verodostojnost zahteva. CA Operater je dužan da u toku istog radnog dana obradi zahtev za opoziv i obavesti korisnika i podnosioca zahteva o opozivu. U slučaju nevalidnog zahteva obaveštava nadzor **ESS QCA** o nepravilnosti rada.
4. **ESS QCA**
   Ukoliko je ustanovljen rizik od kompromitacije privatnog ključa za jedan ili više izdatih kvalifikovanih sertifikata za elektronski potpis.
   ESS QCA sprovodi istrage na sve detektovane i prijavljene nepravilnosti u radu celog sistema. Za sve potvrđene nepravilnosti podnosi zahtev CA operaterima za opoziv jednog ili više kvalifikovanih sertifikata za elektronski potpis. CA Operater je dužan da u toku istog radnog dana obradi podneti zahtev za opoziv i obavesti korisnika i pretplatnika o opozivu.

ESS QCA sprovodi nadzor rada celog sistema i detektuje nepravilnosti. Detektovane nepravilnosti u slučaju kompromitacije jednog ili više kvalifikovanih sertifikata za elektronski potpis povlače zahtev za opoziv istih.

ESS QCA sprovodi istragu na svaku prijavljenu nepravilnost. Prijavu nepravilnosti mogu uraditi ovlašćena lica **ESS QCA**, pretplatnici, korisnici ili treće strane. Prijavljena nepravilnost u slučaju

kompromitacije jednog ili više kvalifikovanih sertifikata za elektronski potpis povlači zahtev za opoziv istih.

U slučaju da je potrebno više od 24 sata da se potvrdi sumnja u kompromitaciju privatnog ključa, podnosi se zahtev za suspenziju sertifikata RA telu isti radni dan kada je ustanovljena sumnja. Na zahtevu se navodi vreme trajanja suspenzije. Operater RA tela je dužan da izvrši identifikaciju podnosioca zahteva i obradi zahtev istog radnog dana kada je zahtev primljen. Potvrdno obrađen zahtev se istog radnog dana podnosi u CA telo. CA operater validira i obrađuje zahtev istog dana.

Za vreme trajanja suspenzije podnosilac zahteva je dužan da ispita sumnju i ako je potvrđena sumnja podnese zahtev za opoziv. Ukoliko se u toku trajanja suspenzije ne podnese zahtev za opoziv, to znači da su sumnje neopravdane i kvalifikovani sertifikat se vraća u validno stanje po isteku roka susupenzije.

Suspenzija sertifikata traje onoliko dugo koliko traju i uslovi zbog kojih je suspenzija i zahtevana, a maksimalno trideset (30) dana. U slučaju da uslovi zahtevaju da suspenzija traje duže od 30 dana, mora se koristiti procedura opoziva. Izuzetak predstavlja suspenzija prilikom izdavanja sertifikata, kada sertifikat ostaje suspendovan do trenutka kada se aktivira ili opozove na eksplicitni zahtev korisnika ili pretplatnika.

CA operater opozivom i suspenzijom elektronskog sertifikata menja njegov status u bazi CA tela koja se koristi prilikom generisanja CRL liste.

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

Prestanak korišćenja kvalifikovanih sertifikata može biti iz sledećih razloga:

- Korisnik želi da prekine korišćenje usluga od poverenja **ESS QCA**.
- **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

U predviđenom vremenskom periodu, a najmanje jednom godišnje **ESS QCA** preispituje *Plan upravljanja rizikom* što obuhvata:

- analizu i procenu rizika poslovanja,
- evaluaciju efektivnosti primenjenih kontrola bezbednosti,
- izbor i primenu kontrola bezbednosti,
- odlučivanje o preostalom riziku,
- preispitivanje i unapređenje metodologije upravljanja rizikom.

Na osnovu identifikovanih rizika, a u cilju umanjenja njihovog negativnog uticaja na poslovanje izabrane su i primenjene kontrola bezbednosti u skladu sa Zakonom i standardima ISO/IEC 27002, NIST 800-37 r2 i CA/Browser Forum Baseline requirements, network security and code signing.

Ovo poglavlje opisuje primenjene metodologije, procese i kontrole bezbednosti kojima se tretiraju bezbednosni rizici iz poslovanja **ESS QCA**.

5.1. Fizičke bezbednosne kontrole

ESS QCA implemetira fizičke bezbednosne kontrole u skladu i na način opisan u *Internom pravilu 1 Sistem za upravljanje dobrima i fizičku zaštitu ESS QCA.*

Fizičke kontrole zaštite rezultat su implementacije procesa upravljanja dobrima (asset management), upravljanja konfiguracijom, upravljanja promenama i upravljanja rizicima.

Sve fizičke kontrole su u elektronskom registru vrednosti **ESS QCA** zavedene i klasifikovane kao kontrole bezbednosti, jasno fizički označene i prikazane na arhitekturi, a njihova primena opisana u *Internom pravilu 1 – Sistem za upravljanje dobrima i fizičku kontrolu pristupa.*

5.1.1. Lokacija i zgrada

Matična lokacija **ESS QCA** nalazi se u skladu sa politikom na lokaciji Kneza Višeslava 70.

Prema klasifikaciji prostora u E-Smart Systems d.o.o., **ESS QCA** koristi sledeće oblasti:

- Oblast dozvoljenu za javni pristup – u svrhu prijema stranaka koje dolaze na ličnu identifikaciju,
- Oblast dozvoljenu za pristup autorizovanim licima – u svrhu prijema stranaka koje dolaze na ličnu identifikaciju u periodu dok čekaju na zakazani termin u **ESS QCA**,
- Bezbednosni perimetar RA – u svrhu lične identifikacije i obrade zahteva lica koje aplicira za kvalifikovani sertifikat,
- Bezbednosni perimetar CA – u svrhu obrade zahteva za izdavanjem i/ili opozivom sertifikata, upravljanja ključevima na QSCD i upisa sertifikata na QSCD,
- Visoko bezbedni perimetar CA – u svrhu upravljanja ključevima CA tela, obezbeđenja funkcije izdavanja sertifikata i publikovanja CRL lista.

5.1.2. Fizički pristup

Svi opisani perimetri imaju primenjene kontrole fizičkog pristupa i to:

- Oblast dozvoljena za javni pristup– 24h FTO obezbeđenje, video nadzor
- Oblast dozvoljena za pristup autorizovanim licima – 24h FTO obezbeđenje, video nadzor
- Bezbednosni perimetar RA – 24h FTO, elektronske brave, video nadzor
- Bezbednosni perimetar CA – video nadzor, fizička barijera, elektronske brave
- Visoko bezbedni perimetar CA – video nadzor, fizička barijera, elektronska brava, obavezno prisustvo dve osobe od poverenja prilikom ulaska.

5.1.3. Električno napajanje i klimatizacija

Napajanje električnih uređaja **ESS QCA** primarno je obezbeđeno iz javne električne mreže. U slučaju nestanka struje u javnoj mreži, nakon 10 sekundi po nestajanju, funkciju neprekidnog napajanja preuzima centralni motorni agregat. Sva oprema **ESS QCA** u obe zone nalazi se na UPS jedinicama koje služe da premoste vreme od nestanka neprekidnog mrežnog napajanja do uključenja alternativnog izvora (agregat).

U prostorima u kojima se obavljaju poslovne funkcije **ESS QCA** su instalirani, operativni i redovno se održavaju uređaji za klimatizaciju.

5.1.4. Izloženost poplavama

Poplave shodno položaju poslovnog prostora **ESS QCA** ne predstavljaju rizik sa verovatnoćom koja nalaže tretiranje.

5.1.5. Prevencija i zaštita od požara

Prostorije **ESS QCA** obezbeđene su detektorima dima koji su povezani na centralni sistem detekcije požara u kompletnoj zgradi. U okviru zgrade nalazi se protivpožarni aparat za odgovarajuću klasu požara. Aparat za gašenje požara nalazi se i u kavezu zone visoke bezbednosti u cilju zaštite osoblja koje bi se zateklo u zoni. Aparati za gašenje požara se redovno proveravaju i održavaju.

5.1.6. Medijumi za čuvanje podataka

Medijumi za čuvanje podataka **ESS QCA** su strogo kontrolisani. Namena i način rukovanja medijumima je opisan u *Internom pravilu 1 Sistem za upravljanje dobrima i fizičku zaštitu ESS QCA*.

5.1.7. Odlaganje smeća

Iznošenje smeća se kontroliše. Papirni otpad se uništava na mašini. Električni uređaji se pre odlaganja fizički uništavaju.

5.1.8. Odlaganje rezervnih kopija

Backup medijumi se čuvaju na odvojenoj lokaciji koja je fizički obezbeđena i zaštićena od požara i poplava. Rezervne kopije obuhvataju sve elemente sistema potrebne za njegov oporavak uključujući rezervne kopije računara, HSM modula, konfiguracije mrežnih uređaja. Formiranje i odlaganje rezervnih kopija je detaljno opisano u *Internom pravilu 8 Procedura backup-a, arhiviranja i izlučivanja ESS QCA.*

5.2. Proceduralne kontrole

Proceduralne ili administrativne kontrole obezbeđuju ažuran i pouzdan proceduralni okvir koji za zaposlene u **ESS QCA** obezbeđuje solidnu osnovu za obavljanje poverenih operativnih zaduženja. Ovaj okvir je opisan *u Internom pravilu 7 Operativne procedure rada i upravljanje incidentima ESS QCA*. Kontrole podele odgovornosti realizuju se prema pravilima opisanim u *Internom pravilu 4 Sistem distribuirane odgovornosti ESS QCA.*

5.2.1. Poverljive uloge

Za potrebe obavljanja uloga od poverenja u **ESS QCA** su obezbeđeni resursi u skladu sa Zakonom i to:

- Dva zaposlena sa visokom stručnom spremom i dugogodišnjim iskustvom (5 + godina) iz domena bezbednosti sa sertifikatom CISSP i
- Dva zaposlena sa visokom stručnom spremom i dugogodišnjim iskustvom (5 + godina) iz domena bezbednosti i sertifikatom CompTIA Security +.

Ovi resursi u skladu sa pravilima rotacije uloga obavljaju jednu od 4 uloge definisane u Politici izdavanja sertifikata i zahtevane Zakonom.
Detaljan opis poslova, zaduženja i odgovornosti za uloge od poverenja dat je u *Internom pravilu 4 Sistem distribuirane odgovornosti u ESS QCA.*

Za potrebe obavljanja uloga od ovlašćenja **ESS QCA** obezbeđuje sledeće resurse:

- Tri zaposlena sa dugogodišnjim iskustvom u radu sa PKI tehnologijom i internom obukom iz domena bezbednosti, kriptografije i zakonske regulative iz oblasti elektronskog dokumenta i elektronskog potpisa za poslove CA operatera
- Tri zaposlena sa iskustvom u prodaji i kontaktu sa korisnicima vezano za PKI tehnologije i internom obukom iz domena bezbednosti, kriptografije i zakonske regulative iz oblasti elektronskog dokumenta i elektronskog potpisa za poslove RA operatera.

Detaljan opis poslova, zaduženja i odgovornosti za uloge od ovlašćenja (CA i RA operateri) dat je u *Internom pravilu 4 Sistem distribuirane odgovornosti u ESS QCA.*

5.2.2. Broj osoba koje se zahtevaju po svakom zadatku

Za operacije, za koje se zahteva dualna kontrola, potrebno je da najmanje dva od ukupno četiri zaposlena **ESS QCA** na poverljivim dužnostima učestvuju u procesu autentikacije/autorizacije unoseći delove podeljenih tajni (shared secrets) u cilju omogućavanja izvršenja istih. U operativnom radu sa korisnicima **ESS QCA** ovlašćene dužnosti RA i CA operatera dele sve tekuće operacije, bez preklapanja, uz odgovarajuću autentikaciju / autorizaciju.

Operacije na kojima se zahteva dualna kontrola su:

- kreiranje, aktiviranje korišćenja, backup-ovanje ili uništenje asimetričnog privatnog ključa *Root i Issuing* CA tela,
- konfiguracija/rekonfiguracija **ESS QCA** okruženja,
- opoziv kvalifikovanog sertifikata za elektronski potpis.

Operacije koje se dele između uloga CA i RA operatera su:

- izdavanje kvalifikovanog sertifikata za elektronski potpis na QSCD uređaju,
- opoziv ili suspenzija kvalifikovanog sertifikata za elektronski potpis.

Tehnički i bezbednosni detalji primene principa separacije rola su opisani u *Internom pravilu 4 Sistem distribuirane odgovornosti u ESS QCA.*

5.2.3. Identifikacija i autentikacija za svaku ulogu

Uloge od poverenja i ovlašćenja koriste po pravilu dvofaktorsku autentikaciju na računarske sisteme **ESS QCA**. Na mestima gde ovakva vrsta autentikacije nije primenjiva koristi se dualni pristup odnosno lozinka koja predstavlja deljenu tajnu između minimalno dva operatera.

Za posebno kritične operacije gde je na transakcijama **ESS QCA** važno da ostane zabeležen i elektronski potpis operatera, uloge od ovlašćenja se autentikuju korišćenjem kvalifikovanih sertifikata za elektronski potpis.

5.2.4. Uloge koje zahtevaju razdvajanje dužnosti

Razdvajanje dužnosti primenjeno u poslovnim procesima **ESS QCA** opisano je *u Internom pravilu 4 Sistem distribuirane odgovornosti u ESS QCA.*

5.3. Kadrovske bezbednosne kontrole

5.3.1. Kvalifikacija i iskustvo

ESS QCA regrutuje zaposlene za uloge od poverenja i ovlašćenja između zaposlenih u E-Smart Systems d.o.o. Beograd koji su na poverljivim dužnostima u preduzeću, a van **ESS QCA** proveli minimum jednu godinu.

Prilikom izbora kandidata vodi se računa o neophodnim uslovima vezanim za obrazovanje, sertifikaciju, znanja i veštine koje zaposleni poseduje. Zaposleni koji su kandidati za zaposlenje u **ESS QCA** moraju u prethodnom radu pokazati visok nivo svesti vezan za primenu principa bezbednosti u radnim praksama, marljivost i brižljivost vezano za radne procese i rezultate rada.

Zaposleni po pravilu imaju potpisan ugovor o neotkrivanju poverljivih informacija (NDA) koji su potpisali prilikom zapošljavanja u E-Smart Systems d.o.o.

5.3.2. Procedura provere biografije

ESS QCA sprovodi sledeće provere biografije kandidata:

- proveru postojanja kriminalne osude za ozbiljne zločine,
- proveru postojanja pogrešne prezentacije informacija od strane kandidata,
- proveru postojanje odgovarajućih referenci.

ESS QCA realizuje relevantne provere eventualnih zaposlenih na bazi statusnih izveštaja koji su izdati od strane kompetentnih autoriteta, izjava trećih strana ili izjava samih potencijalnih zaposlenih.

5.3.3. Zahtevi za obučenošću

Pre početka rada u **ESS QCA** izabrani kandidat se dodatno obučava za rad u **ESS QCA** prema CP i CPS, kao i detaljnije prema internim pravilima.

Poseban deo obuke predstavlja upoznavanje sa relevantnom zakonskom regulativom, eIDAS i standardima iz oblasti koji zaposlenima treba da obezbede solidan nivo razumevanja posla koji obavljaju.

Pre početka rada u **ESS QCA** kandidati prolaze proveru znanja po ustanovljenom okviru tema koje se proveravaju.

5.3.4. Ponovna obuka

Rad CA/RA operatera se periodično proverava od strane zaposlenih na poverljivim dužnostima sa pauzom provere ne dužom od 3 meseca. U slučaju da zaposleni nije napredovao sprovodi se obnavljanje i ponavljanje obuke.

Za poslove koji se retko obavljaju ili u slučaju promene procedure ili uputstava za rad realizuje se doobuka zaposlenih u cilju osvežavanja i aktualizacije znanja i veština vezano za učestvovanje u procesima **ESS QCA**.

5.3.5. Rotacija poslova

ESS QCA primenjuje rotaciju zaposlenih na poverljivim dužnostima svake 3 godine. Rotacija zaposlenih povlači izmenu podeljenih znanja zaposlenih i rekonfiguraciju **ESS QCA** sistema tako da ne utiču na kontinuitet poslovanja.

5.3.6. Kaznene mere u odnosu na zaposlene

ESS QCA primenjuje kaznene mere u vidu materijalnih penala i suspenzija iz operativnog rada u slučaju povreda radne dužnosti u **ESS QCA**. O kaznenim merama se vode zapisi, i o istima odlučuje u procesu preispitivanja rukovodstva.

5.3.7. Kontrole nezavisnih ugovarača

Na nezavisne ugovarače se primenjuju iste kontrole zaštite privatnosti i poverljivosti informacija kao i na zaposlene u **ESS QCA**.

5.3.8. Dokumentacija za inicijalnu obuku i ponovnu obuku

ESS QCA čini dostupnom dokumentaciju zaposlenima na poverljivim i ovlašćenim dužnostima koja se odnosi na inicijalnu obuku, doobuku i pomoć u operativnom radu.

5.4. Procedure bezbednosnih provera/auditing

ESS QCA evidentira i nadzire događaje u sistemu u skladu *sa Internim pravilom 9 Procedura nadzora ESS QCA.*

5.4.1. Tipovi zabeleženih događaja

Događaji u radu **ESS QCA** mogu se podeliti prema mestu na kome nastaju na:

- Događaje koji se javljaju unutar računarskih sistema i koji se mogu automatski elektronski evidentirati. U ove događaje spadaju:

- Događaji vezani za transakcije unutar SQL baza podataka uključujući RA, CA bazu
- Događaji u operativnim sistemima računara koji čine informacioni sistem **ESS QCA**
- Događaji na mrežnim uređajima koji upravljaju pravilima komunikacije infrastrukture **ESS QCA**

- Događaje koji se javljaju izvan računarskih sistema, ali se beleže u računarskim sistemima automatski. U ove događaje spadaju:
  - Događaji vezani za fizički pristup prostoru kontrolisan access kontrolom
  - Događaji u fizičkom prostoru nadziranih zona (video nadzor)
- Događaje koji se javljaju izvan računarskih sistema i koje je potrebno naknadno manuelno evidentirati u računarskom sistemu najčešće od strane ovlašćenih operatera:
  - Saglasnosti
  - Zahtevi korisnika
  - Identifikacija korisnika
  - Evidencija unosa QSCD i pratećeg materijala u Zonu bezbednosti
- Događaje koji se javljaju izvan računarskog dela sistema i čiji originalni zapisi postoje na medijumima (najčešće papir) koji se ne mogu direktno sačuvati u elektronskom delu sistema
  - Potpisivanje papirnih formulara u procesu preuzimanja sertifikata.

5.4.2. Učestalost pregleda evidentiranih događaja

Svi sistemski evidentirani događaji se čuvaju i pregledaju jedanput mesečno prema rasporedu formiranom na godišnjem nivou. Zapisi o obavljenom nadzoru se beleže na **ESS QCA** portalu.

Rad RA i CA operatera se periodično proverava od strane sistem evidentičara na tromesečnom nivou prema rasporedu formiranom na godišnjem nivou. Zapisi o obavljenom nadzoru se beleže na **ESS QCA** portalu.

5.4.3. Vreme čuvanja evidencije

Audit logovi se arhiviraju prema postavljenim ograničenjima za veličinu, a čuvaju se najmanje 10 godina.

5.4.4. Zaštita Audit logova

Audit logovi se mogu videti samo od strane autorizovanog osoblja – sistem evidentičara. Dokumentacija dostavljena u RA telo se čuva u obezbeđenom prostoru u RA telu. Deo primljene papirne dokumentacije se digitalizuje i kvalifikovano elektronski potpisuje od strane RA operatera.

5.4.5. Procedura backup-a audit logova

Backup audit logova se obavlja na način, alatima i prema procedurama opisanim u *Internom pravilu 8 Procedura backup-a, arhiviranja i izlučivanja ESS QCA.*

5.4.6. Sistem sakupljanja audit logova

Logovi svih računarski identifikovanih događaja u sistemu se sakupljaju u realnom vremenu. U slučaju događaja koji se dešavaju izvan računarskih sistema logovi se prikupljaju prema *Internom pravilu 7 Operativne procedure rada i upravljanje incidentima ESS QCA*, u periodu ne dužem od 6 sati.

5.4.7. Obaveštenje subjekta koji je prouzrokovao događaj

Subjekat koji je prouzrokovao određeni događaj se ne obaveštava o samoj audit aktivnosti. U slučaju alarma ili incidentnog događaja, obaveštava se administrator bezbednosti **ESS QCA**. Administrator bezbednosti **ESS QCA** odlučuje o daljem toku obrade incidenta, klasifikacije, rezolucije i zaključenja.

5.4.8. Ocena ranjivosti sistema

Ocena ranjivosti sistema i testiranje kontrola bezbednosti vrši se u skladu sa *Internim pravilom 12 Ocena ranjivosti i testiranje bezbednosti ESS QCA.*

5.5. Arhiviranje zapisa

Zapisi **ESS QCA** se čuvaju, štite, nadgledaju i izlučuju u skladu sa *Internim pravilom 8 Procedura backup-a, arhiviranja i izlučivanja ESS QCA.*

5.5.1. Tipovi arhiviranih zapisa

ESS QCA čuva na bezbedan način zapise o izdatim kvalifikovanim sertifikatima za elektronski potpis, audit podatke sistema, izvorne kodove i konfiguracije **ESS QCA** sistema, kao i operativnu procesnu dokumentaciju. Svi zapisi su evidentirani, klasifikovani i povereni na staranje odgovarajućim osobama od poverenja.

5.5.2. Period čuvanja arhive

ESS QCA čuva na bezbedan način sve zapise iz procesa upravljanja životnim vekom **ESS QCA** kvalifikovanih sertifikata za elektronski potpis u periodu od 10 godina u odnosu na datum kada se događaj desio. Zapisi za koje je period čuvanja istekao izlučuju se u skladu *sa Internim pravilom 8 Procedura backup-a, arhiviranja i izlučivanja ESS QCA.*

5.5.3. Zaštita arhive

Nad arhiviranim podacima **ESS QCA** realizuje istovetne kontrole zaštite pristupa i tajnosti kao i nad operativnim podacima. Podaci se čuvaju u bazama zaštićenim od prepisivanja. Prava pristupa podacima iz arhiva RA sistema ima Administrator bezbednosti **ESS QCA** ili delegirani zaposleni udaljenog RA tela odgovoran za bezbednost i sistem evidentičar **ESS QCA**. Prava pristupa podacima iz arhiva **ESS QCA** ima sistem evidentičar **ESS QCA**. Detalji implementacije opisani su u *Internom pravilu 2 Sistem za mrežno povezivanje, logičku kontrolu pristupa, zaštitu informacija u skladištu i transportu ESS QCA.*

5.5.4. Procedura backup-a arhive

ESS QCA sprovodi proceduru backup-a arhive u skladu *sa Internim pravilom 8 Procedura backup-a, arhiviranja i izlučivanja ESS QCA.*

5.5.5. Zahtevi za vremenskim pečatom zapisa

Zapisi koji su elektronski imaju u sebi datum i vreme sa računara na kojem su napravljeni, a vreme na računaru se sinhroniše sa autoritativnim izvorom vremena definisanim Zakonom.

5.5.6. Sistem sakupljanja zapisa

Zapisi se sakupljaju korišćenjem softverskog rešenja **ESS QCA**, detaljno opisanom u *Internom pravilu 7 Operativne procedure rada i upravljanje incidentima ESS QCA.*

5.5.7. Procedure za dobijanje i verifikaciju informacija iz arhive

ESS QCA zapisi u elektronskoj ili papirnoj formi mogu biti predmet pregleda/nadzora od drugih ili trećih strana. Procedure za dobijanje i verifikaciju informacija iz arhive opisane su u *Internom pravilu 8 Procedura backup-a, arhiviranja i izlučivanja u ESS QCA*. Upit za dobijanje i verifikaciju informacija iz arhive u **ESS QCA** dolazi u slobodnoj formi od strane korisnika ili pouzdajućih strana. O opravdanosti zahteva i formi informacija koje se daju na uvid odlučuje **ESS QCA** Administrator bezbednosti.

5.6. Izmena ključeva

U slučaju isteka ili opoziva sertifikata sertifikacionog tela, vrši se zanavljanje sertifikata i ključeva sertifikacionog tela, u skladu sa *Internim pravilom 3 Sistem za upravljanje ključevima ESS QCA*. U oba slučaja, vrši se generisanje novog para ključeva sertifikacionog tela i distribucija sertifikata CA svim korisnicima i zainteresovanim stranama, kao i u slučaju prvog generisanog sertifikata CA. Sertifikati sertifikacionih tela su publikovani na lokaciji qca.e-smartsys.com - preuzimanje.

5.7. Kompromitacija i oporavak u slučaju katastrofe

5.7.1. Procedure za postupanje u incidentnim i kompromitujućim situacijama

U *Internom pravilu 7 Operativne procedure rada i upravljanje incidentima ESS QCA*, opisan je proces upravljanja incidentima, uključujući klasifikaciju incidenata i izveštavanje u skladu sa Zakonom.

5.7.2. Računarski resursi, softver ili podaci koji su oštećeni

U internom pravilu 5 Sistem obezbeđenja kontinuiteta poslovanja i oporavka od katastrofe ESS QCA opisani su BC/DR planovi u slučaju pojave prepoznatih rizika otkaza delova sistema **ESS QCA**. Za sistem **ESS QCA** određen je MAD i RTO sa minimalnim vrednostima od 2 sata, odnosno sat i 30 minuta respektivno.

5.7.3. Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika

U slučaju kompromitacije privatnog ključa korisnika vrši se opoziv kompromitovanog kvalifikovanog sertifikata za elektronski potpis i izdavanje novog sa novim parom ključeva. Procedura zanavljanja privatnog ključa izdavajućeg tela opisana je u *Internom pravilu 3 Sistem za upravljanje ključevima ESS QCA*.

5.7.4. Mogućnosti kontinuiteta poslovanja nakon katastrofe

Planovi kontinuiteta poslovanja i oporavka od katastrofe opisni su *u Internom pravilu 5 Sistem obezbeđenja kontinuiteta poslovanja i oporavka od katastrofe ESS QCA*. Za planove kontinuiteta poslovanja i oporavka od katastrofe treniraju se nosioci uloga od poverenja i ovlašćenja. Planovi kontinuiteta poslovanja se testiraju, a rezultati testiranja čuvaju na internom portalu **ESS QCA**.

5.8. Završetak rada CA ili RA

U cilju tretiranja rizika koje završetak rada CA ili RA tela **ESS QCA** nosi sa sobom, **ESS QCA** je razvio tri opcije plana završetka rada detaljno opisane *u Internom pravilu 10 Plan završetka rada ESS QCA*:

1. Završetak rada RA tela;
2. Završetak rada CA tela (**ESS QCA**) uz nastavak pružanja usluga održavanja korisnicima sertifikata do datuma isteka svih izdatih sertifikata;

3. Završetak rada CA tela (**ESS QCA**) uz prestanak pružanja svih usluga uključujući i usluge održavanja aktivnih sertifikata.

Prve dve opcije potpuno minimizuju rizik na strani korisnika, dok treća opcija ovaj rizik svodi na minimalnu meru u cilju prevencije najznačajnijeg neželjenog rizika – kompromitacije identiteta vlasnika sertifikata.

U slučaju završetka rada RA tela E-Smart Systems d.o.o. je dužan da obezbedi sukcesora koji može biti drugo već postojeće RA telo u okviru **ESS QCA**, novo RA telo **ESS QCA** ili osnovno RA telo koje se nalazi u samom **ESS QCA** na lokaciji E-Smart Systems d.o.o. U ovom slučaju, sertifikati izdati od RA tela koje se gasi nastavljaju da se održavaju od strane **ESS QCA** (CRL) i RA tela sukcesora (suspenzija/povlačenje/deblokada PIN-a). U ovom slučaju dobra i bezbednost korisnika ostaju sačuvani u potpunosti.

U slučaju završetka rada CA tela uz nastavak pružanja usluga održavanja korisnicima sertifikata do datuma isteka svih izdatih sertifikata, gase se sva RA tela prema scenariju za završetak rada RA tela, a sukcesor postaje RA telo na centralnoj lokaciji **ESS QCA**.

Centralno RA telo od publikovanog dana gašenja nastavlja da prima i obrađuje zahteve iz životnog veka izdatih sertifikata, a CA telo nastavlja da izdaje CRL liste za izdate sertifikate do datuma njihovog isteka. RA telo na centralnoj lokaciji nastavlja da vrši aktivnosti arhiviranja i izlučivanja do isteka perioda čuvanja poslednjeg izdatog sertifikata sa najdužim rokom trajanja. I u ovom slučaju dobra i bezbednost korisnika ostaju sačuvani u potpunosti.

U slučaju završetka rada CA tela (**ESS QCA**) pri čemu E-Smart Systems d.o.o. nije u mogućnosti da obezbedi kontinuitet usluge održavanja za izdate sertifikate, kao ni obavezu čuvanja podataka iz procesa registracije i izdavanja sa pratećim arhiviranjem i izlučivanjem, ili uslugu publikacije podataka o statusu sertifikata, operacije **ESS QCA** tela se gase po skraćenom postupku. U ovom slučaju se povlače svi izdati sertifikati, uključujući i sertifikate izdavajućim telima i podaci o tome publikuju na lokacijama koje su upisane u sertifikatima, ali će biti ukinute po isteku perioda gašenja o čemu će biti obaveštene sve zainteresovane strane uključujući, ali se ne ograničavajući na: korisnike izdatih sertifikata, pouzdajuće strane, nadležno ministarstvo ili odgovarajućeg predstavnika državne uprave. U ovom slučaju korisnici gube vrednost izdatog sertifikata, ali se obezbeđuje očuvanje bezbednosti identiteta sa kojim je sertifikat, kojim **ESS QCA** više ne može da upravlja, povezan.

Interes **ESS QCA** i šire poslovnog sistema E-Smart Systems d.o.o. je da procese završetka rada ograniči na prve dve opcije plana.

6. Tehničke bezbednosne kontrole

ESS QCA primenjuje sledeće tehničke kontrole zaštite:

- Pristup mreži **ESS QCA** je potpuno zatvoren za ulazni saobraćaj.
- Firewall uređaji su konfigurisani tako da propuštaju samo izlazni saobraćaj i to do tačno definisanih tačaka publikacija u internoj mreži ESS.
- Informacije dolaze u **ESS QCA** zonu isključivo koristeći mehanizme povlačenja. **ESS QCA** zona nema publikovane tačke pristupa.
- **ESS QCA** poznaje tri nivoa pristupa:
    - Pristup za osobe od poverenja (**ESS QCA** Administratori)
    - Pristup za osobe od ovlašćenja (**ESS QCA** Operateri)
    - Pristup za auditore (**ESS QCA** Audit).
- Pristup **ESS QCA** administratora se kontroliše pravilom dva čoveka i periodično ukida.
- Pristupa fizičkom prostoru, logovanje na računare i izvršavanje promena na konfiguracijama/podacima se kontroliše i loguje.
- Baze podataka **ESS QCA** su zaštićene restriktivnim pravima pristupa. Svi poslovni podaci su zaštićeni elektronskim potpisom. Pristup operatera **ESS QCA** aplikacijama je obezbeđen isključivo korišćenjem kvalifikovanih sertifikata.
- Mreža i računarski uređaji su zaštićeni u skladu sa CA/Browser Forum NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS.
- Sistem **ESS QCA** se štiti od pojave malicioznog i neautorizovanog softvera na tri načina:
    - potpunom blokadom internet saobraćaja,
    - zabranom instalacije i korišćenja email klijenata na svim računarskim resursima
    - lokalnim antimalware rešenjem u cilju detekcije i prevencije unosa malware-a preko eksternih medijuma
    - regularnim osvežavanjem antimalware baze u cilju pravovremene detekcije pretnji.
- Kritični elementi **ESS QCA** su zaštićeni mehanizmima backup-a. Backup medije su kriptovane. BU medije se formiraju i čuvaju prema planu za BC/DR koji se periodično testira.
- Zaštita integriteta podataka o vremenu realizacije svih operacija, uključujući i vreme izdavanja, opoziva sertifikata realizovana je u skladu sa Zakonom koristeći autoritativne izvore vremena Direkcije za mere i dragocene metale.
- Skeniranje sistema na poznate ranjivosti vrši se prema rasporedu, a najmanje jednom godišnje ili pri pojavi pretnji za koje se oceni da mogu da ugroze rad **ESS QCA** i bez obzira na rad izolovan od pristupa spoljnim mrežama
- Instalacije softvera u **ESS QCA** realizuju se isključivo u procesu release menadžmenta. Ovaj proces obuhvata planiranje, evaluaciju i validaciju novih verzija softvera/hardvera i kontroliše konfiguracione verzije sistema za sve komponente konfiguracione baze.
- **ESS QCA** je vlasnik i potpuno kontroliše izvršne kodove svih delova operativnog **softvera ESS QCA** rešenja. Namenski razvijeni softverski alati za kontrolu procesa **ESS QCA** implementiraju zahteve bezbednosti koji se odnose, ali ne ograničavaju na korišćenje odgovarajućih kriptografskih algoritama, verzija i struktura elektronski potpisanih i poruka i dokumenata,

odgovarajućih mehanizama kontrole pristupa i odgovarajućih pravila obrade i zaštite podataka.

- Za potrebe kontrole razvoja i testiranja, koriste se razvojna i testna okruženja, sistemi za kontrolu verzija izvornog i izvršnih kodova, kao i sistem za kontrolu instalacije izvršnih kodova na klijentske stanice. Sve komponente klijentskog softvera **ESS QCA** rešenja su elektronski potpisane odgovarajućim code signing sertifikatima izdatim od strane enterprise PKI infrastrukture ESS.
- Javne publikacije **ESS QCA** se nalaze na Azure cloud-u. Ovim je obezbeđana 99.99% dostupnost servisa publikovanja CRL lista i servisa provere statusa sertifikata, odnosno servisa aktiviranja sertifikata. Podaci o izdatim sertifikatima se nalaze u bazama na matičnoj lokaciji **ESS QCA** u ESS DMZ mreži i ne prenose se na Azure cloud. Prenos podataka između **ESS QCA** i ESS DMZ realizuje se periodično od strane servisa **ESS QCA** koji podatke predaju autorizovani servisima ESS DMZ.

6.1. Generisanje i instalacija asimetričnog para ključeva

6.1.1. Generisanje asimetričnog para ključeva

Asimetrični parovi ključeva *Root* i *Issuing* CA tela **ESS QCA** se generišu i koriste uz primenu sledećih tehničkih bezbednosnih kontrola:

- Generisanje asimetričnog para ključeva CA tela **ESS QCA** realizuje se prema propisanoj ceremoniji definisanoj *Internim pravilom 6 Procedura ceremonije podizanja ESS QCA*, u prisustvu Administratora bezbednosti i minimalno dva administratora bezbednosti.
- Ključevi se generišu na hardveru HSM uređaja koji obezbeđuje zaštitu od krađe, zloupotrebe i zaštitu od eksporta.
- Ključevima se od strane drugih aplikacija i Windows operativnog sistema pristupa korišćenjem CNG key storage provider-a koji obezbeđuje dodatnu autorizaciju windows naloga na korišćenje particija sa privatnim ključem. Novi sloj zaštite pristupa u korišćenju obezbeđuje da aktiviranoj particiji može prići samo jedan autorizovani windows nalog pod kojim se izvršava servis autorizovan za izdavanje sertifikata.

Asimetrični par ključeva na QSCD uređajima koji će poslužiti kao osnova za izdavanje kvalifikovanih sertifikata za elektronski potpis se generiše uz primenu sledećih tehničkih bezbednosnih kontrola:

- QSCD uređaji zadovoljavaju zahteve propisane Zakonom, eIDAS i standardima.
- Par ključeva se generiše na QSCD uređaju u posebnom procesu inicijalizacije smart kartice kojim upravlja CA operater, osoba od ovlašćenja. U ovom procesu operater koristi alate na koje se autentikuje korišćenjem kvalifikovanog sertifikata. Dužina RSA ključa u inicijalizovanom kontejneru je 2048 bita.
- Javni i privatni ključ ostaju na inicijalizovanom kontejneru. Javni ključ će biti eksportovan iz kontejnera u procesu izdavanja kvalifikovanog sertifikata.
- Alati loguju sve akcije operatera i objekte kartica koje su u procesu bile inicijalizovane.

Inicijalizovane kartice imaju randomizovane aktivacione PIN-ove i profile koji se mogu koristiti za sertifikate tačno određenog **ESS QCA RA** tela.

6.1.2. Isporuka privatnog ključa korisniku

Pripremljen QSCD uređaj se čuva u **ESS QCA** zoni bezbednosti. U slučaju da je RA ovlašćen za rad sa QSCD, uređaji se na bezbedan način dostavljaju u RA gde ih RA čuva u obezbeđenoj prostoriji. Privatni ključ se ne koristi u komunikaciji RA i **ESS QCA**. Korisnik preuzimanjem QSCD uređaja preuzima i privatni ključ. QSCD uređaj se korisniku uručuje ili lično od strane CA operatera ili bezbednim kanalom poštanske dostave uz potvrdu o prijemu i osiguranje lične dostave.

6.1.3. Dostava javnog ključa do izdavaoca sertifikata

Javni ključ se, kao i privatni, generiše u procesu inicijalizacije QSCD i ostaje sačuvan na QSCD uređaju u zoni bezbednosti do ulaska u proces personalizacije. Tek u transakciji personalizacije QSCD javni ključ se čita sa QSCD, ali ostaje enkapsuliran transakcijom i do završetka procesa formiranja sertifikata nepoznat operaterima koji u procesu učestvuju.

CA Operater koristi javni ključ sačuvan na QSCD uređaju i sa identifikacionim podacima dobijenim od RA u procesu formiranja PKCS10 zahteva prema servisima CA.

Ukoliko je RA ovlašćen za rad sa QSCD uređajima, u procesu RA se koristi javni ključ sa QSCD uređaja i identifikacioni podaci korisnika za formiranje PKCS10 zahteva. PKCS10 zahtev se envelopira u XML dokument koji se elektronski potpisuje i šalje u CA telo. CA operater validira XML zahtev i ekstrahuje PKCS10 zahtev.

PKCS10 zahtev prolazi validaciju samog **ESS QCA** sistema u odnosu na pripremljeni QSCD uređaj kojom se proverava da li je tačno određeni CA ili RA operater ovlašćen za rad sa QSCD formirao zahtev za izdavanje.

Tek nakon ove provere PKCS10 zahtev se upućuje u CA na izdavanje sertifikata.

6.1.4. Dostava javnog ključa izdavaoca sertifikata trećim stranama

ESS QCA dostavlja svoje javne ključeve *Root* i *Issuing* CA tela u obliku X.509 v3 elektronskih sertifikata na svom javno dostupnom repozitorijumu https://qca.e-smartsys.com.

6.1.5. Dužine ključeva

Dužine ključeva su implementirane prema zahtevima CP, poglavlje 6.3. Drugi zahtevi upravljanja parom ključeva.

6.1.6. Generisanje kriptografskih parametara i provera kvaliteta

Kvalitet kriptografskih parametara asimetričnog para ključeva obezbeđuje hardverski generator slučajnih brojeva na HSM ili QSCD uređajima koji su FIPS 140-2 level 3 sertifikovani.

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.

6.1.7. Namena ključa (Key Usage)

Root CA telo ima namenu ključa za Certificate Signing, Off-line CRL Signing, CRL Signing.

Issuing CA telo ima namenu ključa za Certificate Signing, Off-line CRL Signing, CRL Signing.

Kvalifikovani sertifikat za elektronski potpis ima namenu ključa za Digital Signature, Non-Repudiation.

6.2. Zaštita privatnog ključa

Asimetrični par ključeva *Root* i *Issuing* CA tela **ESS QCA** se štiti primenom sledećih tehničkih bezbednosnih kontrola:

- Trajanje ključa je ograničeno trajanjem sertifikata za koji je izdat. Zahtev za sertifikat izdavajućeg tela se uvek formira na novo generisanom paru asimetričnih ključeva na HSM.
- Privatni ključevi smešteni na HSM se backup-uju na backup HSM istih tehničkih karakteristika sa identično primenjenim politikama bezbednosti. Privatni ključevi se backup-uju poštujući odgovarajuću proceduru backup-a propisanu od strane proizvođača za koju je primarno nadležna rola Administratora bezbednosti. Nakon backup-a, backup-ovani sadržaj ključeva se proverava, a HSM uređaj čuva u sefu na matičnoj lokaciji **ESS QCA**.
- Sistem za izdavanje loguje sve aktivnosti CA operatera.
- Inicijalizovane kartice ne napuštaju zonu bezbednosti do njihove personalizacije. O stanju inicijalizovanih kartica, kao i kartica koje su u toku procesa inicijalizacije/personalizacije proglašene neusaglašenim proizvodom, prema njihovim serijskim brojevima vodi se elektronska evidencija koja se proverava u periodu ne dužem od 3 meseca.

6.2.1. Standardi i kontrole kriptografskog hardverskog modula

- Ključevi se izdaju na FIPS 140-2 level 3 sertifikovanim HSM uređajima sa pridruženim PIN PED-ovima i PED ključevima za zaštitu kontrole pristupa i aktivacije poverljivog sadržaja HSM.
- HSM uređaji i CA serveri koji koriste privatne ključeve smeštene na HSM uređajima nalaze se u Zonu visoke bezbednosti u koju je ulaz kontrolisan access kontrolom baziranom na MIFARE tokenima kao elementima autentikacije.
- PED ključevi su klasifikovani prema rolama čije se odgovornosti ne preklapaju.
- Pristup HSM uređaju od strane administratora bezbednosti ili oficira bezbednosti se autorizuje korišćenjem PIN PED interfejsa i personalnih PED ključeva u zavisnosti od role koja je određenom PED ključu pridružena
- Pinovi za pristup PED ključevima pomoću kojih se autorizuju administrator bezbednosti i oficir bezbednosti i aktivira particija privatnog ključa HSM-a izdavajućeg tela predstavljaju deljene tajne. Aktivacioni parametar tokena je poznat samo staraocu PED ključa.

Asimetrični par ključeva na QSCD uređajima koji će poslužiti kao osnova za izdavanje kvalifikovanih sertifikata za elektronski potpis se štiti primenom sledećih tehničkih bezbednosnih kontrola:

- Javni ključ para asimetričnih ključeva generisan za korisnika ne napušta sigurni nosilac sve do otpočinjanja procesa personalizacije.
- U procesu personalizacije javni ključ se iščitava iz kontejnera i u zatvorenoj transakciji kojom upravlja CA operater, se formira zahtev, obrađuje, odobrava izdavanje sertifikata, preuzima i validizira izdati sertifikat i upisuje na QSCD uređaj. Transakcija se može nastaviti od mesta na kome je prekinuta ukoliko dođe do neočekivanog prekida u radu infrastrukture sve dok je QSCD uređaj funkcionalno ispravan i prisutan.
- Transakcija se može izvršiti isključivo od strane CA.

- Ključevima se od strane drugih aplikacija i Windows operativnog sistema pristupa korišćenjem CNG key storage provider-a koji obezbeđuje dodatnu autorizaciju windows naloga za korišćenje particija sa privatnim ključem. Novi sloj zaštite pristupa obezbeđuje da aktiviranoj particiji može prići samo jedan autorizovani windows nalog pod kojim se izvršava servis autorizovan za izdavanje sertifikata.

6.2.2. k od n distribucija odgovornosti kontrole privatnog ključa

Za obavljanje bilo koje operacije vezane za privatne ključeve sačuvane na HSM potrebna je autorizacija dva od četiri administratora ovlašćena za rad sa HSM privatnim ključevima koji će aktivirati ključ i na taj način obezbediti CA servisu da ključ koristi u procesima izdavanja kvalifikovanih sertifikata i publikovanja lista povučenih sertifikata.

6.2.3. Bezbedno čuvanje privatnog ključa

- HSM uređaji se automatski zaključavaju i deaktiviraju particije privatnih ključeva u slučaju prekida veze sa računarom sa kojim su bili povezani u procesu aktivacije ključa.
- Sve operacije na ključevima se loguju u internom logu HSM uređaja.

6.2.4. Backup privatnog ključa

- Procedura backup-a privatnog ključa **ESS QCA** CA tela opisana je u *Internom pravilu 3 Sistem za upravljanje ključevima ESS QCA.*
- Backup privatnog ključa kvalifikovanog sertifikata za elektronski potpis se ne radi.

6.2.5. Arhiviranje privatnog ključa

- Po isteku sertifikata privatnog ključa **ESS QCA** CA tela, odnosno prestanku operativnog korišćenja privatnog ključa, isti se bezbedno uništava.
- Arhiviranje privatnog ključa kvalifikovanog sertifikata za elektronski potpis se ne radi.

6.2.6. Transfer privatnog ključa na hardverski kriptografski modul

- Privatni ključevi **ESS QCA** CA tela se generišu na HSM uređajima, te ne postoji potreba za njihovim transferom na iste.
- Privatni ključ kvalifikovanog sertifikata za elektronski potpis se generiše na QSCD uređaju i nema mogućnost exporta.

6.2.7. Čuvanje privatnog ključa na hardverskom kriptografskom modulu

- Sopstveni privatni ključ **ESS QCA** *Root* i *Issuing* CA tela čuva se na HSM uređaju.
- Privatni ključ kvalifikovanog sertifikata za elektronski potpis čuva se na QSCD.

6.2.8. Metoda aktivacije privatnog ključa

- Nosioci deljenih tajni (staraoci) *ESS RQCA* i *ESS IQCA1* imaju zadatak da aktiviraju i deaktiviraju privatni ključ odgovarajućeg CA.
- Za QSCD uređaje unošenje PIN-a omogućava korišćenje privatnog ključa.

6.2.9. Metoda deaktivacije privatnog ključa

Nosioci deljenih tajni onemogućavaju korišćenje privatnog ključa preko HSM uređaja, odnosno njegovu deaktivaciju.

6.2.10. Metoda uništenja privatnog ključa

- Privatni ključ **ESS QCA** se ne obnavlja.
- Privatni ključ **ESS QCA** se bezbedno uništava na kraju svog životnog ciklusa, odnosno isteka sertifikata uz koji je bio vezan. Procedura uništenja je opisana u *Internom pravilu 3 Sistem za upravljanje ključevima ESS QCA.*

6.2.11. Rangiranje kriptografskih hardverskih modula

Nije primenljivo.

6.3. Drugi aspekti upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

ESS RQCA i *ESS IQCA1* arhiviraju svoje sopstvene javne ključeve prema zahtevima CP.

6.3.2. Periodi validnosti sertifikata i privatnog ključa

Vreme validnosti *ESS QCA Root* CA elektronskog sertifikata je 30 (trideset) godina.

Vreme validnosti *ESS QCA Issuing* CA elektronskog sertifikata je 10 (deset) godina

Vreme validnosti kvalifikovanog sertifikata za elektronski potpis je 1 (jedna), 2 (dve), 3 (tri), 4 (četiri) ili 5 (pet) godina.

6.4. Aktivacioni podaci

Aktivacioni podaci privatnih ključeva sertifikata **ESS QCA** implementiraju se u skladu sa CP.

6.4.1. Generisanje i instalacija aktivacionih podataka

Aktivacioni podaci privatnog ključa za *Root* i *Issuing* CA telo se kreiraju prilikom ceremonije podizanja CA tela kako je opisano u *Internom pravilu 6 Procedura ceremonije podizanja ESS QCA.*

Kvalifikovani sertifikat za elektronski potpis se inicijalno po izdavanju proglašava suspendovanim. **ESS QCA** generiše jednokratni kod za aktiviranje suspendovanog kvalifikovanog sertifikata za elektronski potpis i dostavlja ga putem SMS-a krajnjem korisniku. U poglavlju 4.4. ovog CPS je opisano kako korisnik aktivira sertifikat.

U CA, ili u ovlašćenom RA za rad sa QSCD uređajima, se, kao poslednji korak pred uručenje kvalifikovanog sertifikata za elektronski potpis, PIN i PUK kod QSCD uređaja podešavaju na slučajno generisanu vrednost i štampaju na PIN koverti.

Vlasnik kvalifikovanog sertifikata za elektronski potpis može promeniti PIN kod nakon preuzimanja QSCD ili u bilo kom drugom trenutku u periodu trajanja sertifikata.

6.4.2. Zaštita podataka za aktiviranje

Nosioci tajni/znanja su dužni da čuvaju lozinke koje se koriste za aktiviranje ključeva.

Korisnici QSCD uređaja su dužni da čuvaju PIN i PUK za pristup privatnom ključu na QSCD uređaju.

6.4.3. Drugi aspekti u vezi aktivacionih podataka

ESS QCA omogućava svojim korisnicima da urade deblokiranje aktivacionog podatka QSCD uređaja. U tu svrhu, korisniku je na raspolaganju aplikacija QCA QSCD Manager putem koje može samostalno deblokirati PIN i to uz pomoć PUK koda koji je, takođe, dobio uz uređaj u PIN koverti. Ukoliko posle dva pokušaja korisnik nije uspeo da deblokira PIN kod, korisnik mora potražiti pomoć u prostorijama **ESS QCA**.

U slučaju da se deblokada radi u prostorijama **ESS QCA** od korisnika se zahteva:

- lično prisustvo i ponovna identifikacija od strane RA operatera
- fizička dostava QSCD uređaja čiji je aktivacioni podatak (PIN kod) blokiran ili ga je korisnik zaboravio
- podnošenje zahteva za deblokadu.

Proces deblokade PIN-a je opisan u *Internom pravilu 7 Operativne procedure rada i upravljanje incidentima u ESS QCA.*

6.5. Bezbednosne kontrole računara

U skladu sa CP implementirani su odgovarajući baseline bezbednosnih kontrola prema klasifikaciji za pet različitih bezbednosnih perimetara. Definicije baseline-a date su u *Internom pravilu 2 Sistem za mrežno povezivanje, logičku kontrolu pristupa, zaštitu informacija u skladištu i transportu ESS QCA.*

Za opisane perimetre formirano je trinaest (13) bezbednosnih profila računarskih resursa na koje se može primeniti specifičan bezbednosni baseline. Prilikom formiranja ovih profila polazi se od toga da računari koji pripadaju istom profilu moraju imati slične ili iste zahteve za bezbednošću koji obezbeđuju primenu istih automatizovanih procedura održavanja, monitoringa, backup-a i oporavka od katastrofe.

6.5.1. Specifični zahtevi za bezbednost računara

Zahtevi za bezbednost računara, odnosno tačke po kojima je baseline specificiran obuhvataju:

1. Mod rada – permanentno uključen, povremeno uključen
2. Mreža i firewall – da li je mrežno povezan i na koji način je mrežni saobraćaj ograničen
3. Aktivni servisi i aktivirani windows features
4. Dozvoljeni instalirani softver
5. File share-ing
6. Pristup resursu od strane operatera (po kojim protokolima)
7. Korisnički nalozi i prava
8. Operativne funkcije koje resurs samostalno obavlja ili koje se na njemu mogu obaviti od strane operatera
9. Pravila za update operativnog sistema
10. Pravila za update hardware firmware-a
11. Način na koji se realizuje backup
12. Način na koji se realizuje oporavak
13. Periferali i zaštita periferala
14. Zabranjene operacije

15. Način realizacije audit-a.

6.5.2. Rangiranje bezbednosti računara

Bezbednost računara prema bezbednosnim profilima formiranim unutar politikom definisanih perimetara rangirana je na sledeći način (od najvišeg prema najnižem nivou bezbednosti)

1. QCA-BP-1 – Profil najvišeg nivoa bezbednosti koja sadrži isključivo resurse Root CA tela ESS QCA
2. QCA-BP-2 – Profil visoke bezbednosti koja sadrži izdavajuća CA tela ESS QCA
3. QCA-BP-3 – Profil visoke bezbednosti koja sadrži domen kontrolere ESS QCA
4. QCA-BP-4 – Profil visoke bezbednosti koja sadrži ostale serverske resurse ESS QCA infrastrukture
5. QCA-BP-5 – Profil visoke bezbednosti koja sadrži klijentske resurse ESS QCA CA
6. QCA-BP-6 – Profil srednje visoke bezbednosti koja sadrži serverske resurse ESS QCA RA
7. QCA-BP-7 – Profil srednje visoke bezbednosti koja sadrži serverske resurse protočne zone ESS QCA
8. QCA-BP-8 – Profil srednje visoke bezbednosti koja sadrži resurse javne zone na QCA Azure cloud
9. QCA-BP-9 – Profil bezbednosti koja sadrži klijentske resurse ESS QCA RA
10. QCA-BP-10 – Profil bezbednosti za resurse na kojima se radi audit i monitoring ESS QCA (CA/RA)
11. QCA-BP-11 – Profil bezbednosti za resurse na kojima se validiziraju backup-i sistema ESS QCA
12. QCA-BP-12 – Profil bezbednosti za resurse na kojima se čuvaju backup-i sistema ESS QCA
13. QCA-BP-13 – Profil bezbednosti za resurse koji se koriste za razvoj i testiranje

6.6. Životni ciklus tehničkih bezbednosnih kontrola

U skladu sa CP implementirani su odgovarajući procesi životnog ciklusa tehničkih kontrola bezbednosti. Ovi procesi su deo šireg integrisanog sistema menadžmenta E-Smart Systems d.o.o. Beograd i detaljno su opisani u Poslovniku integrisanog sistema menadžmenta i Planu menadžmenta servisima. Specifična pravila i organizacija upravljanja procesom razvoja softvera, release i change management-a opisani su u *Internom pravilu 11 Razvoj i deployment softverskog rešenja ESS QCA.*

6.7. Mrežne bezbednosne kontrole

U skladu sa CP implementirane su odgovarajuće mrežne bezbednosne kontrole. Detaljna konfiguracija mreže i primenjenih kontrola na mrežnom nivou data je u *Internom pravilu 2 Sistem za mrežno povezivanje, logičku kontrolu pristupa, zaštitu informacija u skladištu i transportu ESS QCA.*

6.8. Vremenski pečat

Vremenski pečat je implementiran u skladu sa zahtevima CP.

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
- Sertifikat za OCSP servis.

7.1.1. *Root* CA telo

Polja Verzije1	Vrednost
Version	V3
Serial number	20 hex karaktera bez vodećih nula
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 30 godina
Subject	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Public key	4096 bits
Polja Ekstenzije	**Vrednost**
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints (Critical)	Subject Type=CA Path Length Constraint=1
Enhanced Key Usage	Nema
Application Policies	Nema
Certificate Policies	Nema
Qualified Certificate Statements	Nema
Subject Key Identifier	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	Nema
CRL Distribution Points	Nema
Authority Information Access	Nema
Subject Alternative Name	Nema
Polja Atributa	**Vrednost**
Thumbprint algorithm	Sha1
Thumbprint	40 hex karaktera

7.1.2. *Issuing* CA telo

Polja Verzije1	Vrednost
Version	V3
Serial number	20 hex karaktera bez vodećih nula
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 10 godina
Subject	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Public key	2048 bits
Polja Ekstenzije	**Vrednost**
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints (Critical)	Subject Type=CA Path Length Constraint=0
Enhanced Key Usage	Nema
Application Policies	Nema
Certificate Policies	Policy Identifier=All issuance policies
Qualified Certificate Statements	Nema
Subject Key Identifier	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
CRL Distribution Points	http putanja do CRL liste *Root* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	http putanja do fajla *Root* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Subject Alternative Name	Nema
Polja Atributa	**Vrednost**
Thumbprint algorithm	sha1
Thumbprint	40 hex karaktera

7.1.3. Kvalifikovani sertifikat za elektronski potpis za korisnike

Kvalifikovani sertifikat za elektronski potpis za fizičko lice koje je pripadnik pravnog lica izdat na osnovu lične karte

Polja sertifikata verzije 1	Zahtev	Vrednost
Version	ETSI EN 319 412-2 (4.2.1)	V3
Serial number	Pravilnik (član 7. stav 5), IETF RFC 5280 (4.1.2.2)	20 hex karaktera bez vodećih nula
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 11 9 312 (7.3)	sha256RSA
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha256
Issuer	ETSI EN 319 412-2 (4.2.3.1)	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Valid from		UTC datum i vreme
Valid to		UTC datum i vreme
Subject	ETSI EN 319 412-2 (4.2.4) Pravilnik (član 7.) C – stav 1, tačka 1 G, SN – stav 1, tačka 2; stav 3 CN – stav 1, tačka 3; stav 2; stav 3 SERIALNUMBER – stav 1 tačka 4, stav 4; stav 5 Pravilnik (član 8.) SERIALNUMBER Pravilnik (član 11.) SERIALNUMBER (CA:RS)	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, O={naziv pravnog lica}, [SERIALNUMBER = PNORS-{JMBG}], 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
Public key	ETSI TS 119 312 RFC 5280 (4.1.2.7)	2048 bits
Polja Ekstenzije	**Zahtev**	**Vrednost**
Key Usage	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage		Nema
Qualified Certificate Statements	Pravilnik (član 16.) RFC3739 (3.2.6) ETSI EN 319 412-5 (4.2.1) ETSI EN 319 412-5 (4.2.2) ETSI EN 319 412-5 (4.2.3) ETSI EN 319 412-1 (5.1.1)	0.4.0.1862.1.1 (European Qualified Certificate) 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate) 0.4.0.1862.1.6 (QcType) 0.4.0.1862.1.6.1 (esign) 1.3.6.1.5.5.7.11.2 (QC Statement 2) 0.4.0.194121.1.1 http://qca.e-smartsys.com/docs_2/ESS_QCA_CPS_KES.pdf
Certificate Policies	Pravilnik (član 15.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.509.1.1.2 Policy Qualifier Id=CPS Qualifier: http://qca.e-

		smartsys.com/docs_2/ESS_QCA_CPS_KES.pdf Policy Identifier: 0.4.0.194112.1.2
Subject Key Identifier		40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	ETSI EN 319 412-2 (4.3.1)	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
Subject Alternative Name	ETSI EN 319 412-2 (4.3.5)	RFC822 Name={email adresa}
CRL Distribution Points	ETSI EN 319 412-2 (4.3.11)	http putanja do CRL liste *Issuing* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	http putanja do fajla *Issuing* CA sertifikata na http://qca.e-smartsys.com repozitorijumu

Kvalifikovani sertifikat za elektronski potpis za fizičko lice izdat na osnovu lične karte

Polja sertifikata verzije 1	Zahtev	Vrednost
Version	ETSI EN 319 412-2 (4.2.1)	V3
Serial number	Pravilnik (član 7. stav 5), IETF RFC 5280 (4.1.2.2)	20 hex karaktera bez vodećih nula
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha256RSA
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha256
Issuer	ETSI EN 319 412-2 (4.2.3.1)	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Valid from		UTC datum i vreme
Valid to		UTC datum i vreme
Subject	ETSI EN 319 412-2 (4.2.4) Pravilnik (član 7.) C – stav 1, tačka 1 G, SN – stav 1, tačka 2; stav 3 CN – stav 1, tačka 3; stav 2; stav 3 SERIALNUMBER – stav 1 tačka 4, stav 4; stav 5 Pravilnik (član 8.) SERIALNUMBER Pravilnik (član 11.) SERIALNUMBER (CA:RS)	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, [SERIALNUMBER = PNORS-{JMBG}], SERIALNUMBER = CA:RS-{SN kartice}, C=RS
Public key	ETSI TS 119 312 RFC 5280 (4.1.2.7)	2048 bits
Polja Ekstenzije	**Zahtev**	**Vrednost**
Key Usage	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage		Nema
Certificate Policies	Pravilnik (član 15.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.509.1.1.2 Policy Qualifier Id=CPS

		Qualifier: http://qca.e-smartsys.com/docs_2/ESS_QCA_CPS_KES.pdf Policy Identifier: 0.4.0.194112.1.2
Qualified Certificate Statements		0.4.0.1862.1.1 (European Qualified Certificate) 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate) 0.4.0.1862.1.6 (QcType) 0.4.0.1862.1.6.1 (esign) 1.3.6.1.5.5.7.11.2 (QC Statement 2) 0.4.0.194121.1.1 http://qca.e-smartsys.com/docs_2/ESS_QCA_CPS_KES.pdf
Subject Key Identifier	ETSI EN 319 412-2 (4.3.1)	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	ETSI EN 319 412-2 (4.3.5)	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
CRL Distribution Points	ETSI EN 319 412-2 (4.3.11)	http putanja do CRL liste *Issuing* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	http putanja do fajla *Issuing* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Subject Alternative Name	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	RFC822 Name={email adresa}

Kvalifikovani sertifikat za elektronski potpis za fizičko lice koje je pripadnik pravnog lica izdat na osnovu pasoša

Polja sertifikata verzije 1	Zahtev	Vrednost
Version	ETSI EN 319 412-2 (4.2.1)	V3
Serial number	Pravilnik (član 7. stav 5), IETF RFC 5280 (4.1.2.2)	20 hex karaktera bez vodećih nula
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha 256RSA
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha256
Issuer	ETSI EN 319 412-2 (4.2.3.1)	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Valid from		UTC datum i vreme
Valid to		UTC datum i vreme
Subject	ETSI EN 319 412-2 (4.2.4) Pravilnik (član 7.) C – stav 1, tačka 1 G, SN – stav 1, tačka 2; stav 3 CN – stav 1, tačka 3; stav 2; stav 3 SERIALNUMBER – stav 1 tačka 4, stav 4; stav 5 Pravilnik (član 9.) SERIALNUMBER	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, O={naziv pravnog lica}, [SERIALNUMBER = PAS{oznaka zemlje izdavaoca pasoša}-{broj pasoša}], SERIALNUMBER = CA:RS-{SN kartice}, 2.5.4.97 = MB:RS-{matični broj pravnog lica},

	Pravilnik (član 11.) SERIALNUMBER (CA:RS)	[2.5.4.97 = VATRS-{PIB pravnog lica}], C=RS
Public key	ETSI TS 119 312 RFC 5280 (4.1.2.7)	2048 bits
Polja Ekstenzije	Zahtev	Vrednost
Key Usage	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage		Nema
Certificate Policies	Pravilnik (član 15.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.509.1.1.2 Policy Qualifier Id=CPS Qualifier: http://qca.e-smartsys.com/docs_2/ESS_QCA_CPS_KES.pdf Policy Identifier: 0.4.0.194112.1.2
Qualified Certificate Statements		0.4.0.1862.1.1 (European Qualified Certificate) 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate) 0.4.0.1862.1.6 (QcType) 0.4.0.1862.1.6.1 (esign) 1.3.6.1.5.5.7.11.2 (QC Statement 2) 0.4.0.194121.1.1 http://qca.e-smartsys.com/doc_2/ESS_QCA_CPS_KES.pdf
Subject Key Identifier	ETSI EN 319 412-2 (4.3.1)	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	ETSI EN 319 412-2 (4.3.5)	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
CRL Distribution Points	ETSI EN 319 412-2 (4.3.11)	http putanja do CRL liste *Issuing* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	http putanja do fajla *Issuing* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Subject Alternative Name	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	RFC822 Name={email adresa}

Kvalifikovani sertifikat za elektronski potpis za fizičko lice izdat na osnovu pasoša

Polja sertifikata verzije 1	Zahtev	Vrednost
Version	ETSI EN 319 412-2 (4.2.1)	V3
Serial number	Pravilnik (član 7. stav 5), IETF RFC 5280 (4.1.2.2)	20 hex karaktera bez vodećih nula
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha256RSA
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha256
Issuer	ETSI EN 319 412-2 (4.2.3.1)	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C

		= RS
Valid from		UTC datum i vreme
Valid to		UTC datum i vreme
Subject	ETSI EN 319 412-2 (4.2.4) Pravilnik (član 7.) C – stav 1, tačka 1 G, SN – stav 1, tačka 2; stav 3 CN – stav 1, tačka 3; stav 2; stav 3 SERIALNUMBER – stav 1 tačka 4, stav 4; stav 5 Pravilnik (član 9.) SERIALNUMBER Pravilnik (član 11.) SERIALNUMBER (CA:RS)	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, [SERIALNUMBER = PAS{oznaka zemlje izdavaoca pasoša}-{broj pasoša}], SERIALNUMBER = CA:RS-{SN kartice}, C=RS
Public key	ETSI TS 119 312 RFC 5280 (4.1.2.7)	2048 bits
Polja Ekstenzije	Zahtev	Vrednost
Key Usage	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage		Nema
Certificate Policies	Pravilnik (član 15.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.509.1.1.2 Policy Qualifier Id=CPS Qualifier: http://qca.e-smartsys.com/docs_2/ESS_QCA_CPS_KES.pdf Policy Identifier: 0.4.0.194112.1.2
Qualified Certificate Statements		0.4.0.1862.1.1 (European Qualified Certificate) 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate) 0.4.0.1862.1.6 (QcType) 0.4.0.1862.1.6.1 (esign) 1.3.6.1.5.5.7.11.2 (QC Statement 2) 0.4.0.194121.1.1 http://qca.e-smartsys.com/doc_2/ESS_QCA_CPS_KES.pdf
Subject Key Identifier	ETSI EN 319 412-2 (4.3.1)	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	ETSI EN 319 412-2 (4.3.5)	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
CRL Distribution Points	ETSI EN 319 412-2 (4.3.11)	http putanja do CRL liste *Issuing* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	http putanja do fajla *Issuing* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Subject Alternative Name	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	RFC822 Name={email adresa}

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, ali se nalaze u registru opozvanih sertifikata.

7.2.1. Profil *Root* CRL liste

Polja	Vrednost
Version	V2
Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Effective date	UTC datum i vreme
Next update	UTC datum i vreme + 26 nedelja
CA Version	Vmajor.minor
CRL Number	Redni broj
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuuje CRL listu
Revoked certificates	Serial number UTC datum i vreme opoziva razlog opoziva

7.2.2. Profil *Issuing* CRL liste

Polja	Vrednost
Version	V2
Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Effective date	UTC datum i vreme
Next update	UTC datum i vreme + 24 sata
CA Version	Vmajor.minor
CRL Number	Redni broj
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuuje CRL listu
Revoked certificates	Serial number UTC datum i vreme opoziva razlog opoziva

7.3. OCSP profil

OCSP profil sertifikata definisan je za izdavajuće ESS QCA telo koje izdaje ove sertifikate za potrebe generisanja OCSP odgovora na OCSP request-e. OCSP servisi se publikuju na javnim lokacijama van Zone visoke bezbednosti ESS QCA tako da je u cilju zaštite kompromitacije ključeva ovih sertifikata primenjeno sledeće:

- obavezna aktivacija ključa lozinkom prilikom svakog izdavanja
- reizdavanje sertifikata u periodu ne dužem od 6 meseci.

OCSP lokacija za proveru statusa sertifikata za ESS QCA izdavajuće telo nalazi se na lokaciji https://qca.e-smartsys.com/ocsp/ESSQCA1. Pozicija OCSP responder-a nije upisana u izdate sertifikate, ali se može koristiti preko eksterne konfiguracije za potrebe formiranja elektronskog potpisa.

Polja Verzije1	Vrednost
Version	V3
Serial number	20 hex karaktera bez vodećih nula
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN= ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 6 meseci
Subject	CN= ESS IQCA1 OCSP , O = E-Smart Systems d.o.o., C = RS
Public key	4096 bits
Polja Ekstenzije	**Vrednost**
Key Usage (Critical)	Digital Signature (80)
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	05 00
Subject Key Identifier	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
Authority Information Access	http putanja do fajla *Root* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Polja Atributa	**Vrednost**
Thumbprint algorithm	sha1
Thumbprint	40 hex karaktera

8. Audit usaglašenosti i druge provere

ESS QCA obezbeđuje periodičnu proveru/audit saglasnosti, uključujući ove CPS 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 ovim CPS dokumentom. Interni audit sprovode odgovarajući zaposleni ESS sa datim zaduženjima. U slučaju neusaglašenosti rada sa pravilima izdavanja, **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 biće predmet periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona i odgovarajućim podzakonskim aktima.

9. Drugi poslovni i pravni aspekti

9.1. Cene

9.1.1. Cene izdavanja ili obnove sertifikata

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

Objavljivanje važećih cena sertifikata i drugih usluga od poverenja vrši se 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 prava da menja uslove naplate kvalifikovanih sertifikata.

9.1.2. Cena pristupa sertifikatima

ESS QCA ne pruža uslugu udaljenog korišćenja sertifikata.

9.1.3. Cena pristupa informacijama o statusu sertifikata

ESS QCA ne naplaćuje pristup informacijama o statusu sertifikata, kao ni registru opozvanih sertifikata (CRL).

9.1.4. Cene za druge servise

ESS QCA besplatno pruža servis deblokade PIN-a i podrške u radu sa kvalifikovanim sertifikatima.

9.1.5. Politika povraćaja novca

Nije primenljivo.

9.2. Finansijska odgovornost

ESS QCA snosi finansijsku odgovornost za obavljanje svoje delatnosti u skladu sa zakonskim propisima.

9.2.1. Pokrivanje osiguranja

ESS QCA je dužno da obezbedi najniži iznos osiguranja od odgovornosti za moguću štetu nastalu vršenjem usluga izdavanja kvalifikovanih sertifikata u skladu sa važećim propisima, tako da:

- Osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 20.000 € u dinarskoj protivvrednosti, podrazumevajući pritom kao štetni događaj pojedinačnu štetu nastalu upotrebom jednog kvalifikovanog sertifikata u jednom aktu u pravnom prometu;
- Ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti sertifikacionog tela, kumulativno na godišnjem nivou, po svim štetnim događajima, ne može biti niža od 1.000.000 € u dinarskoj protivvrednosti.

9.2.2. Drugi fondovi

Nije primenljivo.

9.2.3. Osiguranje ili garancijsko pokrivanje za krajnje korisnike

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

9.3.1. Opseg poverljivih informacija

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 poverljivim podacima koji predstavljaju predmet međusobnih ugovora sa trećim licima i
- sa svim ostalim podacima koji su navedeni u internim pravilima rada **ESS QCA.**

9.3.2. Informacije koje nisu u opsegu poverljivih informacija

Poverljivim podacima se ne smatraju:

- Registar opozvanih sertifikata, kao i podaci koje oni sadrže,
- CP,
- CPS – ovaj dokument,
- Podaci i dokumenta koja se nalaze na zvaničnom site-u **ESS QCA**.

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

9.3.3. Odgovornost za zaštitu poverljivih informacija

Ovlašćena lica **ESS QCA** i pretplatnici u obavezi su da:

- Čuvaju tajnost podataka primenom mera koje se koriste za zaštitu poverljivih informacija i koriste ih samo za potrebe zbog kojih su bili prikupljeni,
- Ne otkrivaju poverljive informacije bez prethodnog odobrenja koje daje pretplatnik ili nadležni organ, u pisanoj formi.

9.4. Privatnost i zaštita podataka o ličnosti

9.4.1. Plan privatnosti

ESS QCA se pridržava pravila privatnosti i zaštite podataka o ličnosti i pravila poverljivosti kako je propisano u CPS dokumentu, *Politici privatnosti i zaštite podataka o ličnosti* i u skladu sa zakonom.

9.4.2. Podaci o ličnosti koji se smatraju privatnim

Definicije privatnih podataka navedene su u *Politici privatnosti i zaštite podataka o ličnosti*.

9.4.3. Podaci o ličnosti koji se ne smatraju privatnim

Definicije podataka koji se ne smatraju privatnim navedene su u *Politici privatnosti i zaštite podataka o ličnosti*.

9.4.4. Odgovornost za zaštitu podataka o ličnosti

ESS QCA je odgovorno za zaštitu podataka o ličnosti prikupljenih u okviru zahteva za svoje usluge, a prema *Politici privatnosti i zaštite podataka o ličnosti* i odgovarajućem zakonu.

9.4.5. Obaveštenje i saglasnost za korišćenje podataka o ličnosti

Obaveštenje o uslovima za zaštitu privatnosti, kao i o korišćenju i obradi korisnikovih podataka o ličnosti sprovodi se na početku procesa izdavanja kada se korisnik upoznaje sa uslovima navedenim u *Politici privatnosti i zaštite podataka o ličnosti* i sa kojima se saglašava, što potvrđuje potpisivanjem *Saglasnosti sa politikom privatnosti i zaštite podataka o ličnosti*.

9.4.6. Otkrivanje informacija shodno pravnim i administrativnim procesima

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 i čuva,
- odgovarajućeg državnog organa.

9.4.7. Druge okolnosti za otkrivanje informacija

ESS QCA će otkriti podatke o ličnosti zaštićene zakonom uz prethodnu saglasnost korisnika ili na zahtev nadležnog organa i u drugim slučajevima predviđenim zakonom.

ESS QCA zadržava pravo mogućnosti naplate procesiranja ovakvih zahteva.

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 CPS

ESS QCA zadržava pravo da izmeni CP i ovaj CPS dokument 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 politike po kojoj je izdat i uslovi korišćenja po toj verziji politike važe do vremenskog isteka kvalifikovanog sertifikata ili njegovog opoziva.

9.10.1. Važnost

CPS sa novim **OID** - om i označenim datumom početka važenja prethodno se, osam (8) dana pre zvaničnog datuma početka važenja, objavljuje preko on-line repozitorijuma https://qca.e-smartsys.com i o tome se obaveštava nadležno Ministarstvo.

CPS sa promenjenom podverzijom važi od datuma objavljivanja na gore pomenutom on-line repozitorijumu **ESS QCA**.

9.10.2. Kraj validnosti

Kraj validnosti CPS dokumenta nije određen, niti je povezan sa periodom validnosti kvalifikovanih sertifikata za elektronski potpis izdatih na osnovu određenog CPS.

9.10.3. Efekat završetka i ponovnog rada

Prilikom donošenja novog CPS, svi kvalifikovani sertifikati za elektronski potpis izdati nakon tog datuma procesiraju se prema novom CPS.

9.11. Pojedinačna obaveštenja i komunikacija sa zainteresovanim stranama

Kontakt podaci ESS QCA objavljeni su na on-line repozitorijumu https://qca.e-smartsys.com i navedeni u poglavlju 1.3.1. ovog CPS.

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 email-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

9.12.1. Procedure za dopunu

Promene ili dopune ovog CPS dokumenta **ESS QCA** je u obavezi da sprovodi kako bi CPS dokument uvek bio ažuran i aktuelan. Potreba za promenom/dopunom ovog CPS dokumenta nastaje usled promena na ESS QCA sistemu. Te promene mogu biti rezultat unapređenja sistema ili uvođenja novih rešenja/usluga, zatim otklanjanja evidentiranih neusaglašenosti na **ESS QCA**, ali i promena koje su izazvane promenama u Zakonu, a koje imaju uticaja na samo **ESS QCA** rešenje.

Zavisno od tipa promene, odgovorna osoba za administraciju CP i ovog CPS (definisana u poglavlju 1.5.3. ovog dokumenta), donosi odluku o načinu administriranja ovih promena. Nekada su promene takve da ne zahtevaju obaveštavanje postojećih korisnika jer ne utiču na njihovo dotadašnje i buduće korišćenje usluge koju im **ESS QCA** obezbeđuje. Sve ispravke koje ne menjaju uslove izdavanja i/ili korišćenja kvalifikovanih sertifikata za elektronski potpis ne utiču na menjanje OID CP, pa samim tim ni na OID CPS, već samo na novu podverziju.

Međutim, ukoliko je promena suštinska, ona dovodi do promene OID broja CP kada je neophodno obavestiti nadležni organ, a potom objaviti CP, ovaj CPS i, po potrebi, ažurirana druga javna dokumenta preko on-line repozitorijuma.

Svaka promena je dokumentovana označavanjem nove verzije, datuma odobravanja i opisom uzroka promene verzije u tabeli – Istorija dokumenta.

9.12.2. Mehanizam i period obaveštavanja

O izmenama i dopunama CPS i ostalih dokumenata vezanih za CPS, **ESS QCA** obaveštava, pre svega, svoje zaposlene uključene u rad samog sertifikacionog tela. Ukoliko je potrebno, organizuje se obuka o promenama nastalim u CPS dokumentu i **ESS QCA** sistemu.

Dokument(a) se objavljuje na on-line repozitorijumu https://qca.e-smartsys.com

U specifičnim situacijama, **ESS QCA** zadržava pravo da postojeće korisnike obavesti o novonastalim uslovima i putem email-a.

Objavljivanje i važnost novog CPS i drugih dokumenata koji su pod uticajem promene, definisana je u poglavlju 9.10.1. ovog dokumenta.

9.12.3. Uslovi promene OID-a

ESS QCA zadržava pravo promene OID-a.

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 politike važe do vremenskog isteka sertifikata ili njegovog opoziva.

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

ESS QCA posluje 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 kao 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.

9.15. Saglasnost sa primenljivim zakonima

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 i u poglavlju 1. (Uvod) u CP.

Nadzor usklađenosti operativnog rada **ESS QCA** sa važećim zakonodavstvom i propisima sprovodi nadležna inspekcijska služba.

9.16. Razne odredbe

9.16.1. Ugovor sa korisnicima

Usluga izdavanja kvalifikovanog sertifikata za elektronski potpis, kao i njegovo korišćenje regulisano je posebnim Ugovorom između **ESS QCA** i pravnog ili fizičkog lica, a u skladu sa Zakonom i drugim zakonskim propisima.

Korisnicima se mora obezbediti važenje uslova pod kojima je Ugovor potpisan do prestanka važenja kvalifikovanog sertifikata koji je bio predmet Ugovora. U slučaju kada to nije moguće, korisnicima se nudi aneks ugovora čiji uslovi moraju biti isti ili bolji za korisnika.

9.16.2. Prenošenje prava

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

9.16.3. Izmena ili nevaženje odredbi ove CPS

Ako je bilo koja od odredbi ovih CPS nevažeća ili postane nevažeća, to ne utiče na druge odredbe CPS ili sam Ugovor. Nevažeća odredba se zamenjuje važećom koja mora biti što je moguće bliže svrsi koju je nevažeća odredba imala.

9.16.4. Primenjivost za advokatske naknade i odricanje od prava

Nije primenljivo.

9.16.5. Viša sila

ESS QCA odriče se odgovornosti za bilo koju štetu učinjenu korisniku, pretplatniku ili trećem licu prilikom pružanja usluge izdavanja i korišćenja kvalifikovanog sertifikata ukoliko je do štete došlo usled razloga koji su izvan kontrole **ESS QCA**, odnosno više sile.

Ukoliko **ESS QCA** zbog više sile ne može u potpunosti ili delimično da ispuni obaveze preuzete iz ugovornog odnosa, o tome će obavestiti sve zainteresovane strane, u pisanoj formi, odmah, a najkasnije u roku od dva radna dana o slučaju nastanka više sile, uključujući i procenu trajanja i moguće posledice više sile.

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 CPS
2.0	25.10.2018.	Usaglašavanje sa Zakonom
2.1	26.03.2019.	Manje izmene dokumenta
2.2	12.04.2019.	Usaglašavanje sa promenama vezanim za operativne postupke rada RA
2.3	25.04.2019.	Usaglašavanje sa primedbama proveravača
2.4	10.02.2020.	Izmene u poglavlju 5.8. u skladu sa novim Internim pravilom 10
2.5	21.08.2020.	Unapređenje 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 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
- Politika izdavanja kvalifikovanog 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., https://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
ESUPL000000000151-12039777152 39

Digitally signed by Ana Marković
ESUPL000000000151-12039777152 39
Date: 2021.01.14 12:50:29 +01'00'

Srećko Atanasković
ESUPL000000000027-2402962870013

Digitally signed by Srećko Atanasković
ESUPL000000000027-2402962870013
Date: 2021.01.14 13:12:41 +01'00'