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

L-QCA-190

Šifra dokumenta

Politika izdavanja kvalifikovanih sertifikata

(CP-Certificate Policy)

OID politike izdavanja (1.3.6.1.4.1.30496.1731.1.3) za usluge od poverenja:

OID politike za uslugu od poverenja – izdavanje kvalifikovanih sertifikata za elektronski potpis (1.3.6.1.4.1.30496.1731.1.3.1)

OID politike za uslugu od poverenja – izdavanje kvalifikovanih sertifikata za elektronski pečat (1.3.6.1.4.1.30496.1731.1.3.2)

Beograd, 20. maj 2026.

1. Uvod **4**
1.1. Pregled 5
1.2. Ime dokumenta i identifikacija 5
1.3. Učesnici u PKI sistemu ESS QCA 6
1.3.1. ESS QCA 6
1.3.2. Registraciona tela ESS QCA 6
1.3.3. Pretplatnici 7
1.3.4. Korisnici 7
1.3.5. Treće strane 7
1.3.6. Ostali učesnici 7
1.4. Korišćenje sertifikata 7
1.4.1. Prihvatljivo korišćenje sertifikata 7
1.4.2. Zabranjeno korišćenje sertifikata 7
1.5. Administracija CP 7
1.5.1. Organizacija administriranja CP 7
1.5.2. Kontakt podaci 7
1.5.3. Osoba koja određuje pogodnost CP dokumenta 8
1.5.4. Procedura odobravanja CP dokumenta 8
1.6. Definicije i skraćenice 8

2. Odgovornost za publikovanje i repozitorijume **12**
2.1. Repozitorijum 12
2.2. Publikovanje informacija o sertifikatima 12
2.3. Vreme i frekvencija publikovanja 12
2.4. Kontrole pristupa repozitorijumima 12

3. Identifikacija i autentikacija korisnika **13**
3.1. Imenovanje 13
3.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 13
3.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 14
3.2. Inicijalna provera identiteta 14
3.2.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 15
3.2.2. Pečat na QSCD HSM (OID 1.3.6.1.4.1.30496.1731.1.3.2) 15
3.3. Identifikacija i autentikacija u procesu reizdavanja sertifikata 15
3.3.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 15
3.3.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 15
3.4. Identifikacija i autentikacija u procesu opoziva sertifikata 15
3.4.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 15
3.4.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 16

4. Operativni zahtevi u vezi životnog ciklusa sertifikata **17**
4.1. Podnošenje zahteva za dobijanje sertifikata 17
4.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 17
4.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 17
4.2. Procesiranje zahteva za dobijanje sertifikata 17
4.3. Izdavanja sertifikata 17
4.4. Prihvatanje sertifikata 18
4.5. Korišćenje sertifikata i asimetričnog para ključeva 18
4.6. Obnavljanje sertifikata 18
4.7. Generisanje novog para ključeva i sertifikata 18
4.8. Modifikacija sertifikata 18
4.9. Opoziv i suspenzija sertifikata 18

4.10. Servisi provere statusa sertifikata 18
4.11. Prestanak korišćenja sertifikata 18
4.12. Čuvanje i rekonstrukcija privatnog ključa 18

5. Objekti, upravljanje i operativne kontrole 19
5.1. Fizičke bezbednosne kontrole 19
5.2. Proceduralne kontrole 20
5.3. Kadrovske bezbednosne kontrole 20
5.4. Procedure bezbednosnih provera/auditing 21
5.5. Arhiviranje zapisa 21
5.6. Izmena ključeva 21
5.7. Kompromitacija i oporavak u slučaju katastrofe 22
5.8. Završetak rada CA ili RA 22

6. Tehničke bezbednosne kontrole 24
6.1. Generisanje i instalacija asimetričnog para ključeva 24
6.2. Zaštita privatnog ključa 24
6.3. Drugi aspekti upravljanja parom ključeva 25
6.4. Aktivacioni podaci 25
6.5. Bezbednosne kontrole računara 25
6.6. Životni ciklus tehničkih bezbednosnih kontrola 26
6.7. Mrežne bezbednosne kontrole 26
6.8. Vremenski pečat 27

7. Profili sertifikata, CRL i OCSP 28
7.1. Profili sertifikata 28
7.2. CRL profil 28
7.3. OCSP profil 28

8. Audit usaglašenosti i druge provere 30

9. Drugi poslovni i pravni aspekti 31
9.1. Cene 31
9.2. Finansijska odgovornost 31
9.3. Poverljivost poslovnih informacija 31
9.4. Privatnost i zaštita podataka o ličnosti 31
9.5. Prava intelektualnog vlasništva 32
9.6. Izjava o garanciji 32
9.7. Nepriznavanje garancije 32
9.8. Ograničenja odgovornosti 32
9.9. Odštete 33
9.10. Period važnosti i kraj validnosti CP 33
9.11. Pojedinačna obaveštenja i komunikacija sa zainteresovanim stranama 33
9.12. Dopune 33
9.13. Postupak rešavanja sporova 33
9.14. Merodavno pravo 33
9.15. Saglasnost sa primenljivim zakonima 33
9.16. Ostale odredbe 34
9.17. Druge odredbe 34

10. Istorija dokumenta 35

1. Uvod

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

- Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima Republike Srbije uključujući, ali se ne ograničavajući na Uredbu o uslovima za pružanje kvalifikovanih usluga od poverenja, Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati i Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovano sredstvo za kreiranje elektronskog potpisa, odnosno pečata i uslovima koje mora da ispunjava imenovano telo (u daljem tekstu - Zakon),
- Zakonom referenciranom Uredbom EU br. 910/2014 Evropskog parlamenta i Saveta (u daljem tekstu – eIDAS),
- Standardima referenciranim Zakonom i/ili eIDAS-om uključujući, ali se ne ograničavajući na (u daljem tekstu - Standardi):
    - ETSI EN 319 401 „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“
    - ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“
    - ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates“
    - ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“
    - ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“
    - ETSI EN 319 412-3 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons“
    - ETSI EN 319 412-5 „Certificate profiles; Part 5: QCStatements“
    - RFC 822 „Standard for the format of ARPA Internet Text Messages“
    - RFC 3161 „Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)“
    - RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“
    - RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“
    - RFC 5186 „Internet Group Management Protocol Version 3 (IGMPv3) /Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction“
    - RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”
    - RFC 5816 „ESSCertIDv2 Update for RFC 3161“
    - RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP“
    - ISO/IEC 20000-1:2018 – Service management system - Requirements
    - ISO/IEC 27001:2013 - Information security management systems — Requirements

- ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls

1.1. Pregled

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

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

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

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 od poverenja* su formirani na osnovu sledećih dokumenata:

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

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

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

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

1.2. Ime dokumenta i identifikacija

Naziv dokumenta – Politika izdavanja kvalifikovanih sertifikata

Ovaj dokument ima jedinstvenu oznaku - OID 1.3.6.1.4.1.30496.1731.1.3 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) e-smart systems d.o.o. (30496) ESS QCA (1731) CP (1) verzija (3)}

U svakom kvalifikovanom sertifikatu za elektronski potpis izdatom od strane ESS IQCA1 V3 u kome u polju Certificate Policy stoji OID 1.3.6.1.4.1.30496.1731.1.3.1 isti ukazuje da je sertifikat izdat po ovoj verziji politike izdavanja sertifikata.

U svakom kvalifikovanom sertifikatu za elektronski pečat izdatom od strane ESS IQCA2 V3 u kome u polju Certificate Policy stoji OID 1.3.6.1.4.1.30496.1731.1.3.2 isti ukazuje da je sertifikat izdat po ovoj verziji politike izdavanja sertifikata.

Struktura OID identifikacije opisana je u 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. **CP** i **CPS** predstavljaju odgovarajuću politiku i pravila koja se primenjuju pri izdavanju i upravljanju kvalifikovanim sertifikatima.

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

ESS QCA predstavlja hijerarhijsku strukturu Infrastrukture Javnih Ključeva (U daljem tekstu: PKI) za izdavanje kvalifikovanih sertifikata. U pomenutoj arhitekturi postoji:

- ESS RQCA V3 – centralno samopotpisano sertifikaciono telo (*Root* CA) koje izdaje sertifikate potčinjenim sertifikacionim telima (*Issuing* CA) i potpisuje svoju CRL,
- ESS IQCA1 V3 – potčinjeno sertifikaciono telo (*Issuing* CA) od strane ESS RQCA V3, koje izdaje kvalifikovane sertifikate za elektronski potpis korisnicima i potpisuje svoju CRL,
- ESS IQCA2 V3 – potčinjeno sertifikaciono telo (*Issuing* CA) od strane ESS RQCA V3, koje izdaje kvalifikovane sertifikate za elektronski pečat i potpisuje svoju CRL,
- ESS RQCA - centralno samopotpisano sertifikaciono telo (*Root* CA) koje potpisuje svoju CRL do isteka sertifikata potčinjenih sertifikacionih tela (I*ssuing* CA) koje je izdalo,
- ESS IQCA1 - potčinjeno sertifikaciono telo (*Issuing* CA) od strane ESS RQCA, koje potpisuje CRL do isteka kvalifikovanih sertifikata za elektronski potpis koje je izdalo.

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

1.3.2. Registraciona tela ESS QCA

Zahtevi za izdavanje sertifikata za pretplatnike i korisnike **ESS QCA** se podnose **ESS QCA** telu ili udaljenim Registracionim telima, koja obavljaju ulogu Registracionih autoriteta (RA), tj. **ESS QCA** komunicira sa svojim korisnicima putem mreže registracionih tela (centralno RA i mreža RA).

Registraciona tela su:

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

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

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

1.3.3. Pretplatnici

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

1.3.4. Korisnici

Korisnik je fizičko lice na čije ime glasi kvalifikovani sertifikat za elektronski potpis i koji je jedini ovlašćen da isti i koristi za generisanje kvalifikovanog elektronskog potpisa. U slučaju kvalifikovanog sertifikata za elektronski pečat, korisnik sertifikata je pravno lice.

1.3.5. Treće strane

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

1.3.6. Ostali učesnici

ESS QCA se u pružanju usluge izdavanja kvalifikovanih sertifikata oslanja na usluge i proizvode eksternih isporučilaca (dobavljača).

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. U takve transakcije spadaju:

- pristup bezbednim web sajtovima (ssl/tls autentikacija),
- elektronsko potpisivanje, odnosno pečatiranje dokumenata i elektronske pošte.

1.4.2. Zabranjeno korišćenje sertifikata

Svaka druga upotreba kvalifikovanog sertifikata koja nije u saglasnosti sa odredbama Zakona i drugim dokumentima koji regulišu ovu oblast, smatra se nedozvoljenom.

1.5. Administracija CP

1.5.1. Organizacija administriranja CP

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

1.5.2. Kontakt podaci

ESS QCA
E-Smart Systems d.o.o.
Kneza Višeslava 70a
11030 Beograd
Srbija
tel: 011/3050280

fax: 011/3050222
email: qca@e-smartsys.com

1.5.3. Osoba koja određuje pogodnost CP dokumenta

Osoba u **ESS QCA** odgovorna za ovu **CP** je:

Mirna Kojić Veljović
E-Smart Systems d.o.o.
Kneza Višeslava 70a
11030 Beograd
Srbija
tel: 011/3050270
fax: 011/3050222
email: mirna.kojic.veljovic@e-smartsys.com

1.5.4. Procedura odobravanja CP dokumenta

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

1.6. Definicije i skraćenice

U ovom dokumentu pojedini izrazi imaju sledeće značenje:

Aktivacioni podaci – podaci koji su zahtevani u cilju izvršavanja funkcija 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 par koji se koristi 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 – elektronski dokument je skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video materijala, u elektronskom obliku;

Elektronski pečat - skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (pečatiranim) podacima u elektronskom obliku tako da se elektronskim pečatom potvrđuje integritet tih podataka i identitet pečatioca;

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

Fizičko lice u svojstvu registrovanog subjekta - fizičko lice koje je registrovano za obavljanje određene delatnosti u skladu sa zakonom;

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;

Identifikacioni dokument - dokument koji omogućava pouzdano utvrđivanje identiteta građana. U kontekstu pružanja usluga od poverenja to su dokumenta definisana u tački 3a *Uredbe o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za pojedine nivoe pouzdanosti.*

Kvalifikovani elektronski pečat - napredni elektronski pečat koji se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog pečata (QSCD – Qualified Signature Creation Device) i koji se zasniva na kvalifikovanom sertifikatu za elektronski pečat;

Kvalifikovani elektronski potpis – napredni elektronski potpis koji se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa (QSCD – Qualified Signature Creation Device) i koji se zasniva na kvalifikovanom sertifikatu za elektronski potpis. Ovaj potpis je pravno ekvivalentan svojeručnom potpisu prema Zakonu;

Kvalifikovani sertifikat za elektronski pečat - sertifikat za elektronski pečat koji izdaje kvalifikovani pružalac usluga od poverenja i ispunjava uslove predviđene Zakonom;

Kvalifikovani sertifikat za elektronski potpis – sertifikat za elektronski potpis koji izdaje kvalifikovani pružalac usluga od poverenja 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, odnosno pečat;

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

Podnošenje zahteva za sertifikat – zahtev poslat od strane lica koje zahteva sertifikat ka Sertifikacionom telu u cilju izdavanja kvalifikovanog sertifikata;

Politika izdavanja kvalifikovanih sertifikata – 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 – 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 u skladu sa odredbama Zakona;

Sredstvo za kreiranje kvalifikovanog elektronskog potpisa, odnosno pečata – tehničko sredstvo koje se koristi za kreiranje elektronskog potpisa, odnosno pečata uz korišćenje podataka za kreiranje elektronskog potpisa, odnosno pečata;

Sredstvo za proveru kvalifikovanog elektronskog potpisa, odnosno pečata – sredstvo za proveru elektronskog potpisa, odnosno pečata koje ispunjava dodatne uslove utvrđene Zakonom;

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

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

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

Skraćenice koje se koriste u ovom dokumentu:

CA (Certification Authority) - sertifikaciono telo

CP (Certificate Policy) - Politika izdavanja kvalifikovanih sertifikata

CPS (Certification Practice Statement) - Praktična pravila izdavanja kvalifikovanih sertifikata

CRL (Certificate Revocation List) - lista opozvanih sertifikata

CSR (Certificate Signing Request) - zahtev za potpisivanje sertifikata

EBS –(Evidencijski broj stranca) - jedinstveni indikator za strance sa odobrenim boravkom u Republici Srbiji

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 sertifikaciono telo (ESS QCA)

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 elektronski sertifikati

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

RA (Registration Authority) - registraciono telo

RFC – Request For Comments

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

2. Odgovornost za publikovanje i repozitorijume

2.1. Repozitorijum

ESS QCA publikuje informacije (sertifikate CA tela, CRL CA tela i OCSP) potrebne za proveru statusa kvalifikovanih sertifikata koje izdaje na site-u https://essqca.e-smartsys.com.

2.2. Publikovanje informacija o sertifikatima

ESS QCA publikuje informacije o sertifikatima na prethodno pomenutom repozitorijumu.

Detaljan skup publikovanih informacija dat je u **CPS**.

ESS QCA na javnom repozitorijumu ne publikuje poverljive informacije iz poslovanja kao ni lične podatke korisnika sertifikata.

2.3. Vreme i frekvencija publikovanja

ESS QCA publikuje informacije o statusu opozvanosti izdatih kvalifikovanih sertifikata (CRL), kao što je naznačeno i precizirano u dokumentu *Opšti uslovi za pružanje usluga od poverenja*.

Podaci o statusu kvalifikovanih sertifikata dostupni su i preko OCSP servisa na lokacijama https://qca.e-smartsys.com/ocsp/ESSQCA1 i https://qca.e-smartsys.com/ocsp/ESSQCA1V3 (sertifikati za elektronski potpis) i https://qca.e-smartsys.com/ocsp/ESSQCA2V3 (sertifikati za elektronski pečat). OCSP servisi koriste isključivo podatke iz publikovanih CRL tako da su u svakom trenutku podaci o statusu sertifikata publikovani preko CRL i OCSP identični.

ESS QCA publikuje sve ostale informacije i dokumenta 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 na online repozitorijumu su javno dostupni.

3. Identifikacija i autentikacija korisnika

3.1. Imenovanje

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

Svi identifikacioni podaci koji se dostavljaju **ESS QCA** moraju biti verodostojni i proverljivi i moraju da jednoznačno predstavljaju pretplatnika, odnosno korisnika kvalifikovanog sertifikata.

Sertifikati izdavajućih tela koji se reizdaju za isto jedinstveno ime (Subject) na tačkama publikacija (AIA putanje) dobijaju sufiks ***(n)***, gde n označava redni broj zanavljanja sertifikata.

Na CRL i OCSP URL sertifikata izdavajućih tela se primenjuje isto pravilo imenovanja.

3.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

*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 V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
	Subject	CN=ESS RQCA V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
Elektronski sertifikat izdavajućeg tela ESS QCA kvalifikovanih sertifikata za elektronski potpis	Issuer	CN=ESS RQCA V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
	Subject	CN=ESS IQCA1 V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
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 kvalifikovanih sertifikata za elektronski potpis	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

Kvalifikovani sertifikat za elektronski potpis

Vrsta sertifikata	Naziv polja	Jedinstveno ime
Kvalifikovani sertifikat za elektronski potpis za fizičko lice pripadnika entiteta pravnog lica	Issuer	CN=ESS IQCA1 V3, OU= ESS QCA, O= E-Smart Systems d.o.o., 2.5.4.97 = MB:RS-17247565, 2.5.4.97 = VATRS-101833141, C=RS
	Subject	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, O={naziv pravnog lica}, [SERIALNUMBER = PNORS-{JMBG},] ili [SERIALNUMBER = PNORS-{EBS},] 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 sertifikat za elektronski potpis za fizičko lice	Issuer	CN=ESS IQCA1 V3, OU= ESS QCA, O= E-Smart Systems d.o.o., 2.5.4.97 = MB:RS-17247565, 2.5.4.97 = VATRS-101833141, C=RS
	Subject	CN={ime} {prezime} {JIK}, G={ime} , SN={prezime}, [SERIALNUMBER = PNORS-{JMBG},] ili [SERIALNUMBER = PNORS-{EBS},] ili [SERIALNUMBER = PAS{oznaka zemlje izdavaoca pasoša}-{broj pasoša},] SERIALNUMBER = CA:RS-{SN kartice}, C=RS
	Subject Alternative Name	RFC822 Name={email adresa}

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

3.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

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 V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
	Subject	CN=ESS RQCA V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
Elektronski sertifikat izdavajućeg tela ESS QCA kvalifikovanih sertifikata za elektronski pečat	Issuer	CN=ESS RQCA V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS
	Subject	CN=ESS IQCA2 V3, OU=ESS QCA, O=E-Smart Systems d.o.o., 2.5.4.97=MB:RS-17247565, 2.5.4.97=VATRS-101833141, C=RS

Kvalifikovani sertifikat za elektronski pečat

Vrsta sertifikata	Naziv polja	Jedinstveno ime
Kvalifikovani sertifikat za elektronski pečat	Issuer	CN=ESS IQCA2 V3, OU= ESS QCA, O= E-Smart Systems d.o.o., 2.5.4.97 = MB:RS-17247565, 2.5.4.97 = VATRS-101833141, C=RS
	Subject	CN={naziv pravnog lica}[{naziv organizacione jedinice}] {Redni broj} ESSQCA, O={naziv pravnog lica}, [OU={naziv organizacione jedinice},] [L={sedište},] SERIALNUMBER = CA:RS-{JIK}.{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}

3.2. Inicijalna provera identiteta

Pretplatnik je u obavezi da dostavi **ESS QCA** verodostojne podatke o svom pravnom licu.

Identifikacija pretplatnika vrši se u skladu sa zakonskim propisima na osnovu dostavljenih podataka konsultovanjem ovlašćenih registara Republike Srbije. Procedura identifikacije pretplatnika detaljno je opisana u **CPS** dokumentu.

3.2.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Identifikaciju fizičkog lica koje je pripadnik entiteta pravnog lica vrši RA Operater RA tela **ESS QCA** uz lično prisustvo i upoređivanjem podataka sa saglasnosti i podataka na priloženom identifikacionom dokumentu, uključujući i proveru slike.

Identifikacija fizičkog lica koje nije pripadnik entiteta pravnog lica vrši se na osnovu priloženog identifikacionog dokumenta. Lično prisustvo fizičkog lica je obavezno u procesu identifikacije i registracije.

Procedura identifikacije korisnika detaljno je opisana u **CPS** dokumentu.

3.2.2. Pečat na QSCD HSM (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Identifikacija pretplatnika (pravnog lica) u procesu inicijalnog izdavanja kvalifikovanog sertifikata za elektronski pečat na QSCD HSM uređaju u vlasništvu pretplatnika realizuje se elektronskim putem kroz aplikaciju ESS QCA. Pretplatnik podnosi PKCS#10 zahtev generisan u okviru ceremonije na sopstvenom HSM uređaju, zajedno sa zapisom iz ceremonije generisanja ključeva u kome su evidentirani: identifikacija HSM uređaja, učesnici ceremonije, datum i lokacija, kao i potvrda da su sve aktivnosti realizovane u skladu sa propisanom procedurom. Provera valjanosti zapisa iz ceremonije i adekvatnosti HSM uređaja u odnosu na listu nadležnog Ministarstva sprovodi se od strane ovlašćenog validacionog operatera ESS QCA. Procedura je detaljno opisana u CPS dokumentu i Internim pravilima.

3.3. Identifikacija i autentikacija u procesu reizdavanja sertifikata

3.3.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Korisnik podnosi elektronski zahtev za reizdavanje sertifikata za elektronski potpis, ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata, koristeći aplikaciju na lokaciji https://essqca.e-smartsys.com. Na aplikaciju se loguje kvalifikovanim sertifikatom za elektronski potpis za koji se zahteva reizdavanje. Identifikacija korisnika se vrši kroz aplikaciju i servise autentikacije i sertifikat izdaje bez dodatne lične provere korisnika.

3.3.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Pretplatnik podnosi elektronski zahtev za reizdavanje sertifikata za elektronski pečat izdat na smart kartici ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata, koristeći aplikaciju na lokaciji https://essqca.e-smartsys.com. Na aplikaciju se loguje kvalifikovanim sertifikatom za elektronski pečat za koji se zahteva reizdavanje. Identifikacija pravnog lica se vrši kroz aplikaciju i servise autentikacije.

S obzirom da proces provere pravnog lica u postupku podnošenja elektronskog zahteva uključuje direktni proveru i ažuriranje podataka pozivom elektronskih servisa APR-a, dodatna provera podataka od strane RA operatera potrebna je samo za pravna lica koja APR ne vodi u svojim registrima. RA operateri **ESS QCA** su dužni da svaki elektronski zahtev za reizdavanje obrade po proceduri koja uključuje provere izvršenih plaćanja i proveru kompletnosti/validnosti priložene elektronske dokumentacije.

3.4. Identifikacija i autentikacija u procesu opoziva sertifikata

3.4.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

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 putem email-a uz navedene podatke o korisniku, jedinstvenom identifikatoru korisnika (JIK) sertifikata koji se opoziva/suspenduje i validnim potpisom ovlašćenog lica od strane pretplatnika.

Korisnik može da zahteva opoziv/suspenziju svog sertifikata. Zahtev se dostavlja elektronski putem email-a 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.

3.4.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Pretplatnik može da zahteva opoziv/suspenziju kvalifikovanog sertifikata za elektronski pečat. Zahtev za opoziv/suspenziju od strane pretplatnika se dostavlja elektronski putem email-a uz navedene podatke o jedinstvenom identifikatoru korisnika (JIK) sertifikata koji se opoziva/suspenduje i validnim potpisom ovlašćenog lica od strane pretplatnika.

4. Operativni zahtevi u vezi životnog ciklusa sertifikata

4.1. Podnošenje zahteva za dobijanje sertifikata

4.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Zahtev za izdavanje kvalifikovanog sertifikata za elektronski potpis može podneti fizičko lice koje može biti i pripadnik entiteta pravnog lica.

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

Proces održavanja podataka o pretplatnicima realizuje se unutar RA tela prilikom svakog podnošenja saglasnosti ili dostave novih podataka i obuhvata ažuriranje i sinhronizaciju podataka sa nadležnim registrima.

Proces podnošenja zahteva za izdavanje kvalifikovanog sertifikata za elektronski potpis započinje se preko aplikacije publikovane na lokaciji https://essqca.e-smartsys.com/. U prvom koraku se verifikuje email korisnika/pretplatnika korišćenjem OTP koda i za verifikovane mail-ove proces se nastavlja preko aplikacije publikovane na istoj lokaciji.

Sva fizička lica bez obzira na to da li su pripadnici pravnih lica ili nezavisni, zahteve za kvalifikovanim sertifikatima za elektronski potpis podnose isključivo u elektronskom obliku.

4.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Zahtev za dobijanje sertifikata za elektronski pečat podnosi pravno lice ili fizičko lice u svojstvu registrovanog subjekta (preduzetnik) koje je budući korisnik kvalifikovanog sertifikata za elektronski pečat isključivo u elektronskom obliku.

Proces podnošenja zahteva za izdavanje kvalifikovanog sertifikata za elektronski pečat započinje se preko aplikacije publikovane na lokaciji https://essqca.e-smartsys.com/.

Procedura prijema i obrade zahteva za izdavanje kvalifikovanih sertifikata detaljno je opisana u **CPS** dokumentu.

Ukoliko se zahteva izdavanje kvalifikovanog sertifikata za elektronski pečat na QSCD HSM uređaju u vlasništvu pretplatnika, pretplatnik prilaže PKCS#10 zahtev formiran u okviru ceremonije generisanja para ključeva na sopstvenom HSM uređaju, zajedno sa elektronskim zapisom iz te ceremonije. Pre nego što zahtev postane dostupan za dalju obradu, podleže elektronskoj validaciji od strane operatera ESS QCA ovlašćenog za validaciju PKCS#10 zahteva. Operater pregleda PKCS#10 i zapis iz ceremonije, potvrđuje adekvatnost HSM uređaja u odnosu na listu nadležnog Ministarstva i prilaže potpisani zapis iz ceremonije. Tek nakon uspešno sprovedene validacije, zahtev se prosleđuje na dalju obradu.

4.2. Procesiranje zahteva za dobijanje sertifikata

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

Ova procedura je detaljno opisana u **CPS** dokumentu.

4.3. Izdavanja sertifikata

Nakon dostave validnog elektronskog dokumenta zahteva za izdavanje sertifikata elektronski potpisanog od strane RA operatera, CA operater **ESS QCA** sprovodi proces izdavanja sertifikata.

Ovaj proces je detaljno opisan u **CPS** dokumentu.

4.4. Prihvatanje sertifikata

Nakon završenog procesa izdavanja kvalifikovanog sertifikata, isti se uručuje pretplatniku/korisniku u RA telu koje je generisalo zahtev za izdavanje ili poštom.

Ovaj proces je detaljno opisan u **CPS** dokumentu.

4.5. Korišćenje sertifikata i asimetričnog para ključeva

Odgovornosti koje se odnose na korišćenje asimetričnog para ključeva i sertifikata detaljno su opisane u pretplatničkom/korisničkom ugovoru, u *Opštim uslovima za pružanje usluga od poverenja* i **CPS** dokumentu.

4.6. Obnavljanje sertifikata

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

Ovaj proces je detaljno opisan u **CPS** dokumentu.

4.7. Generisanje novog para ključeva i sertifikata

Procedura za generisanje novog para ključeva i sertifikata je ista kao i za inicijalno izdavanje i detaljno je opisana u **CPS** dokumentu.

4.8. Modifikacija sertifikata

Modifikacije postojećeg sertifikata nisu dozvoljene. Ukoliko su potrebne modifikacije, radi se postupak novog izdavanja sertifikata uz opoziv postojećeg. Zahtev za izdavanje novog sertifikata sa promenjenim podacima podnosi se elektronski preko aplikacije publikovane na lokaciji https://essqca.e-smartsys.com/. Korisnik se na aplikaciju loguje važećim kvalifikovanim sertifikatom za koji se zahteva promena podataka.

4.9. Opoziv i suspenzija sertifikata

Uslovi pod kojima se vrši opoziv/suspenzija sertifikata kao i sam proces detaljno su opisani u **CPS** dokumentu.

4.10. Servisi provere statusa sertifikata

Detalji o publikovanim servisima za proveru statusa sertifikata dati su u **CPS** dokumentu.

4.11. Prestanak korišćenja sertifikata

Uslovi pod kojima prestaje korišćenje sertifikata detaljno su opisani u **CPS** dokumentu.

4.12. Čuvanje i rekonstrukcija privatnog ključa

Privatni ključ pretplatnika/korisnika kvalifikovanog sertifikata izdatog od **ESS QCA** nalazi se samo na QSCD uređaju i ne može se eksportovati.

5. Objekti, upravljanje i operativne kontrole

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

- proveravan od strane nadležnog Ministarstva po ZEP-u,
- proveravan od treće strane i sertifikovan po standardima ISO 9001, ISO/IEC 27001 i ISO/IEC 20000-1 i
- proveravan u kontekstu E-Smart Systems d.o.o. Beograd po Zakonu o privatnom obezbeđenju.

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

5.1. Fizičke bezbednosne kontrole

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

Elektronski servisi, koje **ESS QCA** obezbeđuje za korisnike izdatih kvalifikovanih sertifikata i pouzdajuće strane, mogu biti pruženi iz public cloud-a, internog data centra matične lokacije i Zelen Data centra Beogradski put BB, Vršac.

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

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

Za potrebe HSM korisnika, ceremonija generisanja para ključeva na QSCD HSM uređaju u vlasništvu pretplatnika i formiranje pripadajućeg PKCS#10 zahteva (CSR) realizuju se na lokaciji pretplatnika u skladu sa propisanom procedurom ceremonije. Ceremonija se dokumentuje elektronskim zapisom koji potpisuje pretplatnik. Verifikacija usaglašenosti HSM uređaja sa listom nadležnog Ministarstva i provera kompletnosti i validnosti zapisa iz ceremonije sprovode se elektronski, od strane operatera ESS QCA ovlašćenog za validaciju PKCS#10 zahteva, čime se obezbeđuje puna sledljivost i kontrola procesa bez obaveze fizičkog prisustva odgovornog lica ESS QCA na lokaciji pretplatnika.

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

ESS QCA primenjuje sledeće kontrole fizičke zaštite:

- Održava ažuran i detaljan popis svih dobara **ESS QCA**, uključujući fizička, logička, informaciona i ljudska.
- **ESS QCA** ima ustanovljen proces upravljanja životnim vekom dobara od uvođenja do isključenja iz sistema i izlučivanja, čišćenja, odnosno uništenja.
- Dobra su bezbedno klasifikovana i za svako dobro je određen vlasnik sa primarnom ulogom da se brine o očuvanju CIA triade poverene vrednosti.
- Prava pristupa dobrima definisana su korišćenjem RBAC modela (modela zasnovanog na poslovnim rolama).
- Za pristup posebno osetljivim dobrima i za izvođenje posebno osetljivih operacija koristi se pravilo dva čoveka (two-man rule), separacija uloga (separation of duties) i rotacija pozicija (job rotation).
- Pristup zonama bezbednosti i visoke bezbednosti je ograničen isključivo za role osoba od poverenja, osoba od ovlašćenja i administratora bezbednosti. U zonama je zabranjeno zadržavanje, unošenje nepotrebnih stvari, neovlašćeno iznošenje. Za sakupljanje i uklanjanje otpada postoje posebno označeni kontejneri koji

se prazne prema definisanim procedurama uvek uz prisustvo osoba od poverenja/ovlašćenja. Zone su pod 24 h video nadzorom. Zone u periodu van radnog vremena nadgleda FTO ESS.

- Nosioci **ESS QCA** informacija su evidentirani i nadgledani. U slučaju kada se njihovo korišćenje prekida i isti iznose iz **ESS QCA** zona bezbednosti podaci na njima se bezbedno uništavaju, a samim uređajima menja klasifikacija.

5.2. Proceduralne kontrole

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

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

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

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

- RA operater i
- CA operater.

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

U skladu sa ISO/IEC 20000-1 uspostavljen je i realizuje se proces upravljanja promenama. Ovaj proces podrazumeva striktnu evidenciju i dokumentovanje, procenu relevantnosti/uticaja/pretnji svake promene i praćenje pripreme kroz testiranje i validaciju do finalnog spuštanja na produkciono okruženje.

Za potrebe upravljanja promenama uspostavljena su razdvojena razvojna i testna okruženja koja predstavljaju verne replike produkcije, a na kojima se testira i validizira svaka promena uključujući i sistemske patch-eve. Tek nakon realizovane validacije na testnom okruženju i prihvaćene promene, može se dobiti odobrenje za spuštanje promene na produkciono okruženje.

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

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

5.3. Kadrovske bezbednosne kontrole

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

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

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

ESS QCA primenjuje odgovarajuće disciplinske mere u slučaju da se ustanovi da je nosilac uloge od poverenja ili ovlašćenja izvršio neovlašćene aktivnosti, ili poverene poslove izvršavao sa nemarom ili nepažnjom.

5.4. Procedure bezbednosnih provera/auditing

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

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

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

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

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

5.5. Arhiviranje zapisa

Proces arhiviranja zapisa u **ESS QCA** uključuje sledeće:

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

5.6. Izmena ključeva

Period važenja sertifikata **ESS QCA** ograničen je na 20 godina za *Root* sertifikaciono telo, odnosno 10 godina za *Issuing* telo.

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

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

5.7. Kompromitacija i oporavak u slučaju katastrofe

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

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

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

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

- Nosioce privatnih ključeva CA tela (HSM)
- Baze podataka CA servisa, konfiguracija i log aktivnosti aplikacija CA tela
- Baze podataka RA tela, CA/RA zone i CA tela
- Baze podataka X.500 direktorijuma, kao i ostale elemente sistema, gde je backup potreban u cilju skraćivanja RTO (recovery time objective)
- Mrežnu konfiguraciju CA i CARA zone
- Internu DNS konfiguraciju, konfiguraciju public cloud servisa i web aplikacija
- Source kodove i izvršne verzije CA, CARA i RA softvera
- U skladu sa BC/DR planovima, a u slučaju pojave prirodne ili druge vrste fizičke katastrofe koja bi delimično ili u potpunosti učinila neuslovnom postojeću matičnu lokaciju **ESS QCA**, operacije **ESS QCA** se privremeno sele u Zelen Data Centar u Vršcu, gde se na hladnoj rezervi sistema nastavlja rad do završetka oporavka od katastrofe na matičnoj lokaciji. Na ovoj lokaciji se minimalno restauriraju funkcije generisanja lista povučenih sertifikata, a prema dinamici i planu oporavka na matičnoj lokaciji.

5.8. Završetak rada CA ili RA

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

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

1) Neočekivani prekid servisa kreiranja elektronskog potpisa na listi povučenih sertifikata za kvalifikovane sertifikate u roku važnosti koje je izdao **ESS QCA**,
2) Nedostupnost podataka o statusu sertifikata (CRL) za treće strane koje treba da prihvate ili odbiju sertifikate koje je izdao **ESS QCA**,
3) Nemogućnost upravljanja životnim ciklusom već izdatih sertifikata od strane **ESS QCA**,
4) Nemogućnost uvida u dokumentaciju iz poslovanja u zakonskom roku od 10 godina nakon isteka (opoziva) izdatog sertifikata,
5) Neovlašćeno korišćenje sredstava za kreiranje elektronskog potpisa, odnosno pečata u procesu izdavanja sertifikata, a nakon gašenja operativne funkcije izdavanja **ESS QCA**,

6) Neovlašćeno korišćenje infrastrukture ili delova infrastrukture koja je nekada korišćena u poslovnim procesima **ESS QCA**.

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

6. Tehničke bezbednosne kontrole

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

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

6.1. Generisanje i instalacija asimetričnog para ključeva

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

6.2. Zaštita privatnog ključa

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

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

6.3. Drugi aspekti upravljanja parom ključeva

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

Kriptografski algoritmi koje koristi *Root* CA tela za formiranje elektronskog potpisa obuhvataju SHA-512/RSASSA-PSS kombinaciju hash i asimetričnog algoritma sa dužinom RSA ključa od 4096 bita. Period validnosti sertifikata je 20 godina. Period validnosti izdatih sertifikata *Issuing* CA tela je do 10 godina. Javni ključevi *Root* CA tela **ESS QCA** su objavljeni na site-u https://essqca.e-smartsys.com/preuzimanje koji održava E-Smart Systems d.o.o. Beograd, kao i https://mit.gov.rs/extfile/sr/499/TSL-RS.xml koju održava nadležno Ministarstvo.

Kriptografski algoritmi koje koriste *Issuing* CA tela za formiranje elektronskog potpisa obuhvataju SHA-512/RSASSA-PSS kombinaciju hash i asimetričnog algoritma sa dužinom RSA ključa od 4096 bita. Period validnosti sertifikata *Issuing* CA tela je 10 godina. Period validnosti izdatih kvalifikovanih sertifikata je do 5 godina. Sertifikati su objavljeni na site-u https://essqca.e-smartsys.com/preuzimanje koji održava E-Smart Systems d.o.o. Beograd, kao i https://mit.gov.rs/extfile/sr/499/TSL-RS.xml koju održava nadležno Ministarstvo.

Za kvalifikovane sertifikate **ESS QCA** koristi SHA-512/RSASSA-PSS kombinaciju hash i asimetričnog algoritma sa dužinom RSA ključa od 4096 bita. Izdati sertifikati pretplatnika/korisnika se ne publikuju.

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

6.4. Aktivacioni podaci

Za potrebe aktivacije privatnog ključa koriste se sledeći aktivacioni podaci:

- Za privatne ključeve **ESS QCA** *Root* CA i *Issuing* CA koristi se deljena tajna čiji su nosioci osobe od poverenja, a koja je sačuvana na PED ključevima ili namenski personalizovanim SSCD uređajima, pridruženim HSM uređaju odnosno aplikaciji za upravljanje radom CA tela u procesu ceremonije inicijalizacije. U procesu aktivacije PED ključevi ili sscd uređaji se kao deljena tajna koriste po šemi 2 od 4.
- Za privatne ključeve kvalifikovanih sertifikata na QSCD uređajima koje izdaje *Issuing* CA kao aktivacioni podatak koristi se PIN. U procesu izdavanja ovaj podatak se randomizuje i štampa na zaštićenu kovertu koja se uručuje korisniku posebno u odnosu na kvalifikovani sertifikat ili šalje putem SMS poruke ukoliko se sertifikat isporučuje poštom. U slučaju blokade PIN-a, korisniku je na raspolaganju aplikacija QCA QSCD Manager za promenu/deblokadu PIN-a kojom može samostalno uz pomoć PUK koda deblokirati PIN. Korisniku se PIN može deblokirati i od strane **ESS QCA**. U procesu deblokade u prostorijama **ESS QCA** PIN se reinicijalizuje na novu random vrednost i štampa na zaštićenoj koverti uz novi PUK kod, kao i prilikom inicijalnog izdavanja.
- Kao poseban nivo zaštite samog kvalifikovanog sertifikata koristi se proces aktivacije i aktivacioni kod sertifikata. S obzirom na to da se par ključeva i sam sertifikat izdaju bez direktnog prisustva pretplatnika/korisnika, sertifikat se izdaje u statusu suspendovan. Pretplatnik/korisnik u transakciji izdavanja sertifikata dobija aktivacioni kod za sertifikat. Aktivacioni kod se od strane pretplatnika/korisnika preko web aplikacije publikovane na https://essqca.e-smartsys.com/aktivacija unosi u sistem, čime pretplatnik/korisnik potvrđuje da je primio sertifikat iza čega se sertifikat aktivira i na sledećoj CRL više se ne nalazi na listi suspendovanih sertifikata.

6.5. Bezbednosne kontrole računara

Računarska infrastruktura poslovno-tehničkog sistema **ESS QCA** podeljena je na pet bezbednosnih zona:

- Zonu javnog pristupa u kojoj se realizuju operacije **ESS QCA RA** tela, komunikacija i razmena informacija sa pretplatnicima/korisnicima, kao i preuzimanje personalizovanih QSCD uređaja,

- Zonu bezbednosti u kojoj se realizuju operacije **ESS QCA CA** tela i izdaju kvalifikovani sertifikati uz operativno angažovanje CA operatera,
- Visoku zonu bezbednosti u kojoj rade serveri CA tela i pridružena serverska infrastruktura bez permanentnog ljudskog prisustva,
- Zonu razmene informacija kojima pristupaju servisi **ESS QCA RA** i **ESS QCA CA** dela sistema koju čine serverski resursi koji rade potpuno autonomno,
- Zonu publikacija javnih informacija **ESS QCA** koja se nalazi na public cloud-u.

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

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

6.6. Životni ciklus tehničkih bezbednosnih kontrola

Za potrebe razvoja, održavanja i unapređenja **ESS QCA**, primenjeni su procesi iz životnog veka sistema u skladu sa ISO/IEC/IEEE 15288, ISO/IEC 27000 i ISO/IEC 20000.

ESS QCA je u okviru ISO 27001 sertifikacije E-Smart Systems d.o.o. Beograd i kao takav se kontinuirano proverava na godišnjem nivou od treće strane, a dva puta godišnje u okviru internih provera.

6.7. Mrežne bezbednosne kontrole

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

- **ESS QCA RA** - interni mrežni segment sa kontrolisanim ulaznim i izlaznim saobraćajem prema internoj mreži ESS, deo korporativnog Windows AD sa primenjenim odgovarajućim politikama bezbednosti,
- **ESS QCA CA** zona visoke bezbednosti – potpuno izolovan mrežni segment bez propuštenog ulaznog saobraćaja i sa strogo kontrolisanim izlaznim saobraćajem prema internoj mreži ESS,
- **ESS DMZ** zona razmene informacija – DMZ segment na internoj mreži ESS sa kontrolisanim ulaznim saobraćajem iz interne mreže ESS i kontrolisanim https i ldap internet publikacijama. Prihvata podatke iz RA i CA servisa/aplikacija preko WCF https endpoint-a na koje je obavezno logovanje sertifikatima,
- **Public cloud** – Servisi i javna dokumentacija ESS QCA publikovana je preko Azure SAAS web publikacije https://qca.e-smartsys.com i Site Ground WP web sajtova https://essqca.e-smartsys.com . Na ovaj način su publikovani elementi PKI (CRL, CRT/CER), OCSP servisi, dokumentacija iz procesa **ESS QCA**, online uputstva za pretplatnike/korisnike i servisi provere statusa i aktiviranja sertifikata i druge servisne informacije za pretplatnike/korisnike. Automatski prenos sadržaja iz/u public cloud okruženja vrši se preko hibridne konekcije prema resursu u **ESS DMZ** zoni razmene i preko ftps protokola iz zone razmene **ESS DMZ** prema cloud repozitorijumima. Komunikacija i razmena podataka je potpuno automatizovana. Hibridna konekcija ne zahteva publikaciju resursa kome se pristupa već se zasniva na izlaznom https saobraćaju, u ovom slučaju iz zone razmene **ESS DMZ** prema public cloud servisima.
- **ESS QCA** testno i razvojno okruženje – poseban segment ESS interne infrastrukture sa kontrolisanim ulaznim i izlaznim saobraćajem na kome se nalaze namenski podignuti resursi za testiranje, verifikaciju i validaciju rešenja.

ESS QCA izvodi skeniranja ranjivosti interne infrastrukture u periodima od šest meseca.

ESS QCA izvodi penetration testove na godišnjem nivou ili posle promena na mrežnoj infrastrukturi.

6.8. Vremenski pečat

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

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

7. Profili sertifikata, CRL i OCSP

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

7.1. Profili sertifikata

ESS QCA izdaje sledeće vrste sertifikata:

- *Root* CA telo,
- *Issuing* CA telo za elektronski potpis,
- *Issuing* CA telo za elektronski pečat,
- Kvalifikovani sertifikat za elektronski potpis,
- Kvalifikovani sertifikat za elektronski pečat,
- Sertifikate za OCSP servise.

Profili su detaljno opisani u **CPS** dokumentu.

7.2. CRL profil

ESS QCA podržava izdavanje CRL u saglasnosti sa RFC 3280 i sledećim uslovima:

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

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

Opozvani sertifikati se nalaze u CRL.

Profili su detaljno opisani u **CPS** dokumentu.

7.3. OCSP profil

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

Prilikom vraćanja podataka o validnosti sertifikata OCSP prati informacije CRL:

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

OCSP su javno dostupni servisi, publikovani na javno dostupnim internet lokacijama https://qca.e-smartsys.com/ocsp/ESSQCA1, https://qca.e-smartsys.com/ocsp/ESSQCA1V3 i https://qca.e-smartsys.com/ocsp/ESSQCA2V3, autorizovani od strane **ESS QCA** izdatim OCSP sertifikatima.

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

Kao mera zaštite od kompromitacije ključeva i sertifikata OCSP respondera, ovi sertifikati se izdaju sa periodom važenja ne dužim od 6 meseci. Za aktivaciju ključa OCSP respondera koristi se lozinka prilikom kreiranja svakog odgovora, lozinke se čuvaju zaštićene u bazi podataka.

8. Audit usaglašenosti i druge provere

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

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

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

ESS QCA sprovodi redovne godišnje interne audit-e usklađenosti poslovanja sa ovom **CP**, kao i sa **CPS** dokumentom. Interni audit sprovode odgovarajući zaposleni ESS sa datim zaduženjima. U slučaju neusaglašenosti rada sa politikom, **ESS QCA** obustavlja dalje izdavanje kvalifikovanih sertifikata 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 i predmet je periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona i odgovarajućim podzakonskim aktima.

9. Drugi poslovni i pravni aspekti

9.1. Cene

ESS QCA naplaćuje izdavanje/obnovu kvalifikovanih sertifikata.

Objavljivanje cena kvalifikovanih sertifikata i drugih usluga od poverenja se vrši putem site-a https://essqca.e-smartsys.com/cenovnik, partnera **ESS QCA** (treća lica), putem odgovarajućeg ugovora tamo gde je to primenljivo kao i u procesu podnošenja elektronskog zahteva.

ESS QCA zadržava pravo da promeni uslove naplate kvalifikovanih sertifikata.

9.2. Finansijska odgovornost

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

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

Pretplatnik/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 pretplatnika/korisnika,
- bilo kog propusta pretplatnika/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, modifikacija ili neautorizovano korišćenje korisnikovog privatnog ključa, ili napada na integritet privatnih ključeva **ESS QCA** *Root* i *Issuing* CA tela,
- kršenja bilo kojih zakona koji su primenljivi, uključujući one koji se odnose na zaštitu intelektualnih prava, bezbednost informacija, pristup računarskim sistemima, itd.

9.3. Poverljivost poslovnih informacija

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

- sa svim zahtevima za dobijanje kvalifikovanog sertifikata, a posebno sa privatnim podacima koje uključuju,
- sa svim poverljivim podacima vezanim za finansijske obaveze,
- sa svim mogućim poverljivim podacima koji predstavljaju predmet međusobnih ugovora sa trećim licima i
- sa svim ostalim podacima koji su navedeni u Internim pravilima rada **ESS QCA**.

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

9.4. Privatnost i zaštita podataka o ličnosti

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

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

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

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

ESS QCA zadržava pravo mogućnosti naplate procesiranja ovakvih zahteva.

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

9.5. Prava intelektualnog vlasništva

ESS QCA poseduje i zadržava sva prava intelektualnog vlasništva pridružena bazama podataka, web sajtovima, kvalifikovanim sertifikatima 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 pretplatnicima, korisnicima i trećim stranama da koriste, kopiraju, distribuiraju i u svoje elektronske dokumente ugrađuju izdate sertifikate i CRL.

9.6. Izjava o garanciji

ESS QCA daje garanciju na proizvode i usluge koje pruža, a informacije o garantnom roku i procesu reklamacije objavljuje kao sastavni deo publikovanih cenovnika.

9.7. Nepriznavanje garancije

ESS QCA garancije na isporučene proizvode i pružene usluge priznaje u skladu sa objavljenim politikama koje su sastavni deo publikovanih cenovnika.

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 za:

- namene i na način koji nije izričito predviđen u **CP** i **CPS**,
- nepravilno ili pogrešno obezbeđenje PIN-a, PUK-a ili privatnog ključa kvalifikovanog sertifikata, otkrivanje poverljivih podataka trećim licima i neodgovorno postupanje pretplatnika/korisnika kvalifikovanog sertifikata,
- zloupotrebu, odnosno upade u informacioni sistem pretplatnika/korisnika kvalifikovanog sertifikata i na taj način dolaska do podataka o kvalifikovanom sertifikatu od strane neovlašćenih lica,
- nepostupanje ili nedozvoljeno postupanje sa podacima u okviru informacione infrastrukture pretplatnika/korisnika kvalifikovanog sertifikata ili trećih lica,
- neproveravanje podataka, validnosti i statusa kvalifikovanih sertifikata u registru opozvanih kvalifikovanih sertifikata,
- neproveravanje vremena validnosti kvalifikovanih sertifikata,
- postupanje pretplatnika/korisnika kvalifikovanog sertifikata ili trećeg lica suprotno informacijama i obaveštenjima koje objavljuje **ESS QCA**, a publikovane su u **CP**, **CPS** i drugim propisima,
- omogućeno korišćenje, odnosno zloupotrebu kvalifikovanog sertifikata pretplatnika/korisnika od strane neovlašćenih lica,
- sadržaj samih podataka koji se potpisuju korišćenjem kvalifikovanih sertifikata

- upotrebu i pouzdanost rada računarske i programske opreme pretplatnika/korisnika kvalifikovanog sertifikata.

9.9. Odštete

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

9.10. Period važnosti i kraj validnosti CP

Sertifikaciono telo **ESS QCA** zadržava pravo da izmeni **CP** i da nadogradi infrastrukturu bez prethodnog obaveštavanja pretplatnika/korisnika kvalifikovanog sertifikata.

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

9.11. Pojedinačna obaveštenja i komunikacija sa zainteresovanim stranama

Kontakt podaci sertifikacionog tela objavljeni su na site-u https://essqca.e-smartsys.com i navedeni u poglavlju *1.5.2*.

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

ESS QCA obaveštava nadležno Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge izdavanja kvalifikovanih sertifikata.

ESS QCA obaveštava nadležno Ministarstvo u skladu sa Zakonom o broju izdatih sertifikata od početka pružanja usluge do 31. decembra kalendarske godine i podatke o broju važećih sertifikata na dan 31. decembar kalendarske godine.

9.12. Dopune

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

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

9.13. Postupak rešavanja sporova

Ukoliko dođe do spora između **ESS QCA** i pretplatnika ili korisnika kvalifikovanog sertifikata u vezi međusobnih prava i obaveza ili tumačenja ugovora ili nekog drugog dokumenta donetog od strane **ESS QCA**, **ESS QCA** će nastojati da spor reši mirnim putem, sporazumno, a ukoliko do sporazuma ipak ne dođe, spor će rešavati nadležni sud u Beogradu.

9.14. Merodavno pravo

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

9.15. Saglasnost sa primenljivim zakonima

Ova **CP** je u potpunosti u skladu sa odgovarajućom zakonskom regulativom Republike Srbije, i to pre svega sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom

poslovanju i odgovarajućim podzakonskim aktima. Sve pravne stvari koje se odnose na **ESS QCA** i/ili koje se odnose na sertifikate izdate od strane **ESS QCA** će biti procesuirane od strane odgovarajućeg suda u Srbiji.

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

9.16. Ostale odredbe

Usluga izdavanja kvalifikovanih sertifikata kao i njihovo korišćenje regulisani su posebnim ugovorom između sertifikacionog tela **ESS QCA** i pretplatnika/korisnika, a u skladu sa Zakonom i drugim zakonskim propisima.

Pretplatnik/korisnik kvalifikovanih sertifikata nema pravo da prava iz zaključenog ugovora sa **ESS QCA**, u celini ili delimično, prenese na treća lica.

9.17. Druge odredbe

Nema.

10. Istorija dokumenta

Verzija	Datum	Opis promena
0.1	01.11.2011.	Inicijalni dokument
0.2	10.08.2013.	Usklađivanje dokumenta sa software-skim rešenjem
1.0	22.10.2013.	Inicijalna verzija
1.1	25.11.2013.	Manje izmene dokumenta
1.2	14.01.2014.	Usklađivanje sa primedbama komisije
1.3	28.02.2014.	Usklađivanje sa primedbama komisije
1.4	13.03.2014.	Usklađivanje sa primedbama komisije
1.5	01.04.2014.	Gramatičke ispravke
1.6	03.06.2014.	Proširenje pretplatnika
1.7	21.01.2016.	Izmena osobe odgovorne za ovu CP
2.0	25.10.2018.	Usaglašavanje sa Zakonom
2.1	26.03.2019.	Manje izmene dokumenta
2.2	12.04.2019.	Manje izmene dokumenta
2.3	25.04.2019.	Usklađivanje sa nalazima provere
2.4	10.02.2020.	Izmene u poglavlju 5.8. u skladu sa novim Internim pravilom 10
2.5	21.08.2020.	Unapređenja podrške upravljanja rizicima i manje izmene dokumenta
2.6	15.01.2021.	Uvođenje novog tipa QSCD uređaja
2.7	30.05.2023.	Uvođenje elektronskog podnošenja zahteva
3.0	29.03.2024.	Uvođenje novog izdavajućeg tela za izdavanje kvalifikovanog sertifikata za elektronski potpis i uvođenje usluge izdavanja kvalifikovanih sertifikata za elektronski pečat
3.1	16.12.2024.	Uvođenje izdavanja kvalifikovanog sertifikata za elektronski potpis na osnovu EBS
3.2	22.09.2025.	Manje izmene dokumenta
3.3	31.12.2025.	Promenjena dužina RSA ključa za kvalifikovane sertifikate na 4096 bita
3.4	26.03.2026.	Manje izmene dokumenta
3.5	20.05.2026.	Formalizacija validacije zahteva za KEP na QSCD HSM uređajima

Potpisi:

Mirna Kojić Veljović ESUFL001880349261

Digitally signed by Mirna Kojić Veljović ESUFL001880349261
Date: 2026.05.20 13:51:14 +02'00'