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-191

Šifra dokumenta

Praktična pravila izdavanja kvalifikovanih sertifikata

(CPS-Certificate Practice Statement)

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, 22. septembar 2025.

Sadržaj

1. Uvod 7
1.1. Pregled 7
1.2. Ime dokumenta i identifikacija 8
1.3. Učesnici u PKI sistemu ESS QCA 9
1.3.1. ESS QCA 9
1.3.2. Registraciona tela ESS QCA 10
1.3.3. Pretplatnici 11
1.3.3.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 12
1.3.3.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 12
1.3.4. Korisnici (OID 1.3.6.1.4.1.30496.1731.1.3.1) 12
1.3.5. Treće strane 13
1.3.6. Ostali učesnici 13
1.4. Korišćenje sertifikata 14
1.4.1. Prihvatljivo korišćenje sertifikata 14
1.4.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 14
1.4.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 14
1.4.2. Zabranjeno korišćenje sertifikata 14
1.5. Administracija CPS 14
1.5.1. Organizacija administriranja CPS 14
1.5.2. Kontakt podaci 14
1.5.3. Osoba koja određuje pogodnost CPS dokumenta 14
1.5.4. Procedura odobravanja CPS dokumenta 15
1.6. Definicije i skraćenice 15

2. Odgovornost za publikovanje i repozitorijume 15
2.1. Repozitorijum 15
2.2. Publikovanje informacija o sertifikatima 15
2.3. Vreme i frekvencija publikovanja 16
2.4. Kontrole pristupa repozitorijumima 16

3. Identifikacija i autentikacija korisnika 17
3.1. Imenovanje 17
3.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 17
3.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 18
3.2. Inicijalna provera identiteta 19
3.2.1. Identifikacija pretplatnika 19
3.2.2. Identifikacija fizičkog lica pripadnika entiteta pravnog lica (OID 1.3.6.1.4.1.30496.1731.1.3.1) 19
3.2.3. Identifikacija fizičkog lica koje nije pripadnik entiteta pravnog lica (OID 1.3.6.1.4.1.30496.1731.1.3.1) 20
3.3. Identifikacija i autentikacija u procesu reizdavanja sertifikata 20
3.3.1. Identifikacija pretplatnika 20
3.3.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 20
3.3.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 20
3.3.2. Identifikacija korisnika - fizičkih lica pripadnika entiteta pravnog lica -pretplatnika (OID 1.3.6.1.4.1.30496.1731.1.3.1) 21
3.3.3. Identifikacija korisnika - fizičkih lica (OID 1.3.6.1.4.1.30496.1731.1.3.1) 21
3.4. Identifikacija i autentikacija u procesu opoziva sertifikata 22
3.4.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 22
3.4.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 22

4. Operativni zahtevi u vezi životnog ciklusa sertifikata 23
4.1. Podnošenje zahteva za dobijanje sertifikata 23
4.1.1. Podnošenje zahteva za dobijanje sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 23
4.1.2. Podnošenje zahteva za dobijanje sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 24
4.2. Procesiranje zahteva za dobijanje sertifikata 26
4.2.1. Procesiranje zahteva za dobijanje sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 26
4.2.2. Procesiranje zahteva za dobijanje sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 26
4.3. Izdavanje sertifikata 27
4.4. Prihvatanje sertifikata 27
4.4.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 27
4.4.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 28
4.5. Korišćenje sertifikata i asimetričnog para ključeva 28
4.6. Obnavljanje sertifikata 28
4.7. Generisanje novog para ključeva i sertifikata 29
4.8. Modifikacije sertifikata 29
4.9. Suspenzija i opoziv sertifikata 29
4.9.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 31
4.9.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 31
4.10. Servisi provere statusa sertifikata 32
4.10.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1) 32
4.10.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2) 32
4.11. Prestanak korišćenja sertifikata 32
4.12. Čuvanje i rekonstrukcija privatnog ključa 32

5. Objekti, upravljanje i operativne kontrole 33
5.1. Fizičke bezbednosne kontrole 33
5.1.1. Lokacija i zgrada 33
5.1.2. Fizički pristup 33
5.1.3. Električno napajanje i klimatizacija 34
5.1.4. Izloženost poplavama 34
5.1.5. Prevencija i zaštita od požara 34
5.1.6. Medijumi za čuvanje podataka 34
5.1.7. Odlaganje otpada 34
5.1.8. Odlaganje rezervnih kopija 34
5.2. Proceduralne kontrole 34
5.2.1. Poverljive uloge 35
5.2.2. Broj osoba koje se zahtevaju po svakom zadatku 35
5.2.3. Identifikacija i autentikacija uloga od poverenja i ovlašćenja 36
5.2.4. Uloge koje zahtevaju razdvajanje odgovornosti 36
5.3. Kadrovske bezbednosne kontrole 36
5.3.1. Kvalifikacija i iskustvo 36
5.3.2. Procedura provere biografije 36
5.3.3. Zahtevi za obučenošću 36
5.3.4. Ponovna obuka 37
5.3.5. Rotacija poslova 37
5.3.6. Kaznene mere u odnosu na zaposlene 37
5.3.7. Kontrole nezavisnih ugovarača 37
5.3.8. Dokumentacija za inicijalnu obuku ii ponovnu obuku 37
5.4. Procedure bezbednosnih provera/auditing 37
5.4.1. Tipovi zabeleženih događaja 37
5.4.2. Učestalost pregleda evidentiranih događaja 38

5.4.3. Vreme čuvanja evidencije 38
5.4.4. Zaštita audit logova 38
5.4.5. Procedura backup-a audit logova 38
5.4.6. Sistem sakupljanja audit logova 38
5.4.7. Obaveštenje subjekta koji je prouzrokovao događaj 39
5.4.8. Ocena ranjivosti sistema 39
5.5. Arhiviranje zapisa 39
5.5.1. Tipovi arhiviranih zapisa 39
5.5.2. Period čuvanja arhive 39
5.5.3. Zaštita arhive 39
5.5.4. Procedura backup-a arhive 39
5.5.5. Zahtevi za vremenskim pečatom zapisa 40
5.5.6. Sistem sakupljanja zapisa 40
5.5.7. Procedura za dobijanje i verifikaciju informacija iz arhive 40
5.6. Izmena ključeva 40
5.7. Kompromitacija i oporavak u slučaju katastrofe 40
5.7.1. Procedura za postupanje u incidentnim i kompromitujućim situacijama 40
5.7.2. Računarski resursi, softver ili podaci koji su oštećeni 41
5.7.3. Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika 41
5.7.4. Mogućnost kontinuiteta poslovanja nakon katastrofe 41
5.8. Završetak rada CA ili RA 41

6. Tehničke bezbednosne kontrole 43
6.1. Generisanje i instalacija asimetričnog para ključeva 44
6.1.1. Generisanje asimetričnog para ključeva 44
6.1.2. Isporuka privatnog ključa 45
6.1.3. Dostava javnog ključa do izdavaoca sertifikata 45
6.1.4. Dostava javnog ključa izdavaoca sertifikata trećim stranama 45
6.1.5. Dužine ključeva 45
6.1.6. Generisanje kriptografskih parametara i provera kvaliteta 45
6.1.7. Namena ključa (Key Usage) 45
6.2. Zaštita privatnog ključa 45
6.2.1. Standardi i kontrole kriptografskog hardverskog modula 46
6.2.2. k od n distribucija odgovornosti kontrole privatnog ključa 47
6.2.3. Bezbedno čuvanje privatnog ključa 47
6.2.4. Backup privatnog ključa 47
6.2.5. Arhiviranje privatnog ključa 47
6.2.6. Transfer privatnog ključa na hardverski kriptografski modul 47
6.2.7. Čuvanje privatnog ključa na hardverskom kriptografskom modulu 47
6.2.8. Metoda aktivacije privatnog ključa 47
6.2.9. Metoda deaktivacije privatnog ključa 47
6.2.10. Metoda uništenja privatnog ključa 47
6.2.11. Rangiranje kriptografskih hardverskih modula 48
6.3. Drugi aspekti upravljanja parom ključeva 48
6.3.1. Arhiviranje javnih ključeva 48
6.3.2. Periodi validnosti sertifikata i privatnog ključa 48
6.4. Aktivacioni podaci 48
6.4.1. Generisanje i instalacija aktivacionih podataka 48
6.4.2. Zaštita podataka za aktiviranje 48
6.4.3. Drugi aspekti u vezi aktivacionih podataka 48
6.5. Bezbednosne kontrole računara 49

6.5.1. Specifični zahtevi za bezbednost računara....49
6.5.2. Rangiranje bezbednosti računara....49
6.6. Životni ciklus tehničkih bezbednosnih kontrola....50
6.7. Mrežne bezbednosne kontrole....50
6.8. Vremenski pečat....50

7. Profili sertifikata, CRL i OCSP....51
7.1. Profili sertifikata....51
7.1.1. *Root* CA telo....51
7.1.2. *Issuing* CA telo za izdavanje kvalifikovanih sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)....52
7.1.3. *Issuing* CA telo za izdavanje kvalifikovanih sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)....53
7.1.4. Kvalifikovani sertifikat za elektronski potpis za korisnike (OID 1.3.6.1.4.1.30496.1731.1.3.1)....54
7.1.5. Kvalifikovani sertifikat za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)....61
7.1.6. Sertifikat za timestamp servis....64
7.2. CRL profil....65
7.2.1. Profil *Root* CRL....65
7.2.2. Profil *Issuing* CRL sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)....65
7.2.3. Profil *Issuing* CRL liste sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)....66
7.3. OCSP profil....66
7.3.1. OCSP profil za kvalifikovane sertifikate za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)....66
7.3.2. OCSP profil za kvalifikovane sertifikate za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)....67

8. Audit usaglašenosti i druge provere....68

9. Drugi poslovni i pravni aspekti....69
9.1. Cene....69
9.1.1. Cene izdavanja ili obnove sertifikata....69
9.1.2. Cena pristupa sertifikatima....69
9.1.3. Cena pristupa informacijama o statusu sertifikata....69
9.1.4. Cene za druge servise....69
9.1.5. Politika povraćaja novca....69
9.2. Finansijska odgovornost....69
9.2.1. Pokrivanje osiguranja....69
9.2.2. Drugi fondovi....69
9.2.3. Osiguranje ili garancijsko pokrivanje za krajnje korisnike....69
9.3. Poverljivost poslovnih informacija....70
9.3.1. Opseg poverljivih informacija....70
9.3.2. Informacije koje nisu u opsegu poverljivih informacija....70
9.3.3. Odgovornost za zaštitu poverljivih informacija....70
9.4. Zaštita podataka o ličnosti....70
9.4.1. Plan privatnosti....70
9.4.2. Podaci o ličnosti koji se smatraju privatnim....71
9.4.3. Podaci o ličnosti koji se ne smatraju privatnim....71
9.4.4. Odgovornost za zaštitu podataka o ličnosti....71
9.4.5. Obaveštenje i saglasnost za korišćenje podataka o ličnosti....71
9.4.6. Otkrivanje informacija shodno pravnim i administrativnim procesima....71
9.4.7. Druge okolnosti za otkrivanje informacija....71
9.5. Prava intelektualnog vlasništva....71
9.6. Izjava o garanciji....71
9.7. Nepriznavanje garancije....71

9.8. Ograničenje odgovornosti 72
9.9. Odštete 72
9.10. Period važnosti i kraj validnosti CPS 72
9.10.1. Važnost 72
9.10.2. Kraj validnosti 72
9.10.3. Efekat završetka i ponovnog rada 72
9.11. Pojedinačna obaveštenja i komunikacija sa zainteresovanim stranama 72
9.12. Dopune 72
9.12.1. Procedure za dopunu 72
9.12.2. Mehanizam i period obaveštavanja 73
9.12.3. Uslovi promene OID-a 73
9.13. Postupak rešavanja sporova 73
9.14. Merodavno pravo 73
9.15. Saglasnost sa primenjivim zakonima 74
9.16. Razne odredbe 74
9.16.1. Ugovor sa korisnicima 74
9.16.2. Prenošenje prava 74
9.16.3. Izmena ili nevaženje odredbi ovih CPS 74
9.16.4. Primenjivost za advokatske naknade i odricanje od prava 74
9.16.5. Viša sila 74
9.17. Druge odredbe 74

10. Istorija dokumenta 75

1. Uvod

E-Smart Systems **DOO BEOGRAD – E-SMART SYSTEMS DOO BEOGRAD sertifikaciono telo** (u daljem tekstu: **ESS QCA**) donosi **Praktična pravila izdavanja kvalifikovanih sertifikata** koja se odnose na usluge od poverenja koje pruža **ESS QCA** u skladu sa Politikom izdavanja kvalifikovanih sertifikata (OID 1.3.6.1.4.1.30496.1731.1.3) 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** uključuju sledeće servise, i to:

- Registraciju pretplatnika/korisnika,
- Formiranje asimetričnog para ključeva za pretplatnike/korisnike,
- Formiranje kvalifikovanog sertifikata,
- Distribuciju privatnog ključa i kvalifikovanih sertifikata (QSCD) korisnicima na način u skladu sa Zakonom,
- Upravljanje procedurom opoziva i suspenzije kvalifikovanih sertifikata,
- Obezbeđivanje statusa opozvanosti 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 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**),
2) Praktična pravila izdavanja kvalifikovanih sertifikata (u daljem tekstu: **CPS**) - ovaj dokument i
3) Politika privatnosti i zaštite 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 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) *upravljanju razvojem, konfiguracijom i deployment-om 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 uslugu izdavanja kvalifikovanih sertifikata za elektronski pečat 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.

OID identifikacije korišćene u ovom dokumentu prate sledeću strukturu:

iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) e-smart systems d.o.o. (30496) ESS QCA (1731) tip dokumenta (a) verzija (b) tip usluge od poverenja (c)}

1.2. Ime dokumenta i identifikacija

Naziv dokumenta – Praktična pravila izdavanja kvalifikovanih sertifikata

Ovaj dokument ima jedinstvenu oznaku - OID 1.3.6.1.4.1.30496.1731.2.3 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) e-smart systems d.o.o. (30496) ESS QCA (1731) CPS (2) verzija (3) i pokriva praktična pravila u skladu sa politikama sledećih usluga od poverenja:

- Izdavanje kvalifikovanih za elektronski potpis OID {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) potpis (1)}
- Izdavanje kvalifikovanih za elektronski pečat OID {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) pečat (2)}

Politika izdavanja kvalifikovanih sertifikata koja odgovara ovom **CPS** je 1.3.6.1.4.1.30496.1731.1.3 i opisana je u dokumentu **CP** sa istim OID.

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 verziji **CP** koja odgovara ovom **CPS**.

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.

Identifikacioni podaci **ESS QCA CA** tela su:

Sertifikaciono telo	Jedinstveno ime (DN)
Root V3	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
Issuing CA telo V3 za izdavanje kvalifikovanih sertifikata za elektronski potpis	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
Issuing CA telo V3 za izdavanje kvalifikovanih sertifikata za elektronski pečat	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
Root	CN=ESS RQCA, O=E-Smart Systems d.o.o., C=RS
Issuing CA telo za izdavanje kvalifikovanih sertifikata za elektronski potpis	CN=ESS IQCA1, O=E-Smart Systems d.o.o., C=RS

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. **Politika izdavanja kvalifikovanih sertifikata (CP)** i **Praktična pravila izdavanja kvalifikovanih sertifikata (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 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** periodično 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 infrastrukturi 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, koje 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 (***Issuing CA***) koje je izdalo,
- **ESS IQCA**1 – Potčinjeno sertifikaciono telo (***Issuing CA***) od strane **ESS RQCA** koje potpisuje CRL do isteka kvalifikovanih sertifikata koje je izdalo.

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 site-a u cilju pružanja usluga od poverenja,
6) Obezbeđivanje sigurnih mehanizama koji uključuju mehanizam generisanja ključeva, zaštite ključeva, kao i procedure deljenih 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 fizičkog ili pravnog lica koje je podnelo zahtev za izdavanje sertifikata ukoliko **ESS QCA** nije u mogućnosti 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 zaštićenih lista opozvanih sertifikata (CRL), 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 namenjenih za kreiranje kvalifikovanog elektronskog potpisa, odnosno pečata po njihovom preuzimanju od strane korisnika odnosno pretplatnika.
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, pretplatnika 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 pretplatnike i korisnike **ESS QCA** se podnose **ESS QCA** telu ili udaljenim RA (Registration Authority), koja 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 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 fizička i pravna lica 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 u skladu sa **CP** i ovim **CPS**,
2) Izvršavanje svih aktivnosti na identifikaciji i proveri autentičnosti fizičkih i pravnih lica koja podnose zahteve za izdavanje kvalifikovanih sertifikata u skladu sa **ESS QCA** procedurama, **CP** i ovim **CPS**,
3) Slanje zahteva za izdavanje **ESS QCA** u elektronski potpisanoj poruci (zahtev za izdavanje kvalifikovanog sertifikata), u skladu sa **CP** i ovim **CPS**,
4) Upis sertifikata na QSCD uređaj, ukoliko je RA ovlašćen da raspolaže sa prethodno pripremljenim QSCD uređajima,
5) Štampa i uručenje PIN koverte korisniku,
6) Prijem, verifikacija i prosleđivanje **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, navode u atributima polja Subject. Atributi koji omogućavaju trećim stranama da mogu identifikovati pretplatnika ili korisnika kao pripadnika pretplatnika obuhvataju: O organizationIdentifier i (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) U poslovnom okruženju i procesima u kome se koriste kvalifikovani sertifikati obezbede internim bezbednosnim politikama i procedurama zaštitu integriteta, autentičnosti i ispravnosti kvalifikovanih sertifikata izdatih od strane **ESS QCA**,
5) Koriste **ESS QCA** kvalifikovane sertifikate samo za legalne i autorizovane svrhe u skladu sa **CP** i ovim **CPS**, kao i važećim zakonskim aktima,

6) Obaveste RA telo o bilo kojim promenama podataka koji su ranije dostavljeni,
7) Prekinu korišćenje kvalifikovanog sertifikata, ukoliko je bilo koja informacija u sertifikatu postala nevalidna,
8) Prekinu korišćenje kvalifikovanog sertifikata ukoliko sam sertifikat postane nevalidan,
9) Ni u kom slučaju ne koriste javni ključ koji odgovara privatnom ključu koji je sertifikovan od strane **ESS QCA**, u izdatom kvalifikovanom sertifikatu za potrebe izdavanja drugih sertifikata,
10) Koriste bezbedne uređaje i proizvode koji obezbeđuju odgovarajuću zaštitu u korišćenju privatnih ključeva sertifikata,
11) Spreče kompromitaciju, gubljenje, objavljivanje, modifikaciju ili bilo kakvo drugo neautorizovano korišćenje privatnog ključa kvalifikovanog sertifikata,
12) Prijave svaku moguću zloupotrebu privatnog ključa i u tom slučaju podnesu, bez odlaganja, zahtev za opoziv kvalifikovanog sertifikata,
13) Internim politikama i procedurama obezbede da lica delegirana za korišćenje kvalifikovanih sertifikata poseduju odgovarajuća znanja i, ako je neophodno, pohađaju odgovarajuće obuke za korišćenje kvalifikovanih sertifikata i usluga od poverenja.

1.3.3.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

U slučaju kvalifikovanog sertifikata za elektronski potpis, pretplatnička saglasnost daje pravo pretplatnicima da podnesu zahtev za izdavanje, opoziv ili suspenziju korisnikovih kvalifikovanih sertifikata.

1.3.3.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

U slučaju kvalifikovanog sertifikata za elektronski pečat, pretplatnik ima pravo na izdavanje, opoziv, suspenziju kvalifikovanih sertifikata i deblokadu PIN-a QSCD uređaja na osnovu potpisanog *Ugovora o izdavanju i korišćenju kvalifikovanih sertifikata* – **pretplatnički ugovor**.

1.3.4. Korisnici (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Korisnik je fizičko lice kome je izdat kvalifikovani sertifikat za elektronski potpis. Korisnici sa **ESS QCA** potpisuju *Ugovor o izdavanju i korišćenju kvalifikovanog sertifikata za elektronski potpis* – **korisnički ugovor**. Korisnički ugovor omogućava korisniku da podnese zahtev za opoziv, suspenziju, aktivaciju svog kvalifikovanog sertifikata ili deblokadu PIN-a QSCD uređaja.

Identifikacioni podaci korisnika se u izdatom kvalifikovanom sertifikatu navode u polju Subject.

Obaveze korisnika

Korisnici 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) Uzdržavaju se od narušavanja integriteta i činjenja neispravnim kvalifikovanog sertifikata izdatog od strane **ESS QCA**,
5) Koriste **ESS QCA** kvalifikovane sertifikate za elektronski potpis samo za legalne i autorizovane svrhe u skladu sa **CP** i ovim **CPS**, kao i važećim zakonskim aktima,
6) Obaveste RA telo o bilo kojim promenama podataka koji su ranije dostavljeni,

7) Prekinu korišćenje kvalifikovanog sertifikata za elektronski potpis, ukoliko je bilo koja informacija u sertifikatu postala nevalidna,
8) Prekinu korišćenje kvalifikovanog sertifikata za elektronski potpis ukoliko sam sertifikat postane nevalidan,
9) Ni u kom slučaju ne koriste javni ključ koji odgovara privatnom ključu koji je sertifikovan od strane **ESS QCA**, u izdatom kvalifikovanom sertifikatu za elektronski potpis, za potrebe izdavanja drugih sertifikata,
10) Koriste bezbedne uređaje i proizvode koji obezbeđuju odgovarajuću zaštitu u korišćenju privatnih ključeva sertifikata za elektronski potpis,
11) Spreče kompromitaciju, gubljenje, objavljivanje, modifikaciju ili bilo kakvo drugo neautorizovano korišćenje privatnog ključa kvalifikovanog sertifikata za elektronski potpis,
12) Prijave svaku moguću zloupotrebu privatnog ključa i u tom slučaju podnesu, bez odlaganja, zahtev za opoziv kvalifikovanog sertifikata za elektronski potpis,
13) Poseduju odgovarajuća znanja i, ako je neophodno, pohađaju odgovarajuće obuke za korišćenje kvalifikovanih sertifikata i usluga od poverenja.

1.3.5. Treće strane

Treće strane su entiteti, fizička (pojedinci) i/ili pravna lica (kompanije), koji prihvataju i verifikuju kvalifikovani elektronski potpis, odnosno pečat. Treće strane mogu da korisnika/pretplatnika identifikuju na osnovu atributa Subject u telu kvalifikovanog sertifikata u skladu sa Zakonom. **ESS QCA** garantuje pouzdanost i verodostojnost identifikacionih podataka korisnika/pretplatnika na validnim kvalifikovanim sertifikatima u roku trajanja.

Obaveze trećih strana

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

1) Upozna se sa **CP** i **CPS** u vezi navedenih uslova koji važe za treće strane,
2) Poštuje i sprovodi odredbe iz **CP** i ovih **CPS**,
3) 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,
4) 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,
5) Verifikuje kvalifikovani elektronski potpis, odnosno pečat,
6) Razumno se osloni i pouzda na **ESS QCA** izdati kvalifikovani sertifikat u skladu sa odgovarajućim okolnostima,
7) Poseduje odgovarajuća znanja o korišćenju kvalifikovanih sertifikata i drugih tehnologija vezanih za usluge od poverenja.

1.3.6. Ostali učesnici

ESS QCA se u pružanju usluge izdavanja kvalifikovanih sertifikata oslanja na usluge i proizvode eksternih isporučilaca (dobavljača). Izbor, vrednovanje, evaluacija i upravljanje eksternim isporučiocima obavlja se u skladu sa standardom ISO 20000, politikama, procedurama i *Planom menadžmenta servisom QCA* koje je donela i sertifikovala kompanija E-Smart Systems d.o.o.

1.4. Korišćenje sertifikata

1.4.1. Prihvatljivo korišćenje sertifikata

1.4.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

ESS QCA kvalifikovani sertifikati za elektronski potpis 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 site-ovima (ssl/tls autentikacija),
- elektronsko potpisivanje dokumenata i elektronske pošte.

1.4.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

ESS QCA kvalifikovani sertifikati za elektronski pečat 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 api (ssl/tls autentikacija),
- elektronsko pečatiranje dokumenata i elektronske pošte,
- validacija elektronskog računa/fakture,
- validacija elektronskog dokumenta privrednog subjekta.

1.4.2. Zabranjeno korišćenje sertifikata

Svaka druga upotreba kvalifikovanog sertifikata 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: mailto:qca@e-smartsys.com

1.5.3. Osoba koja određuje pogodnost CPS dokumenta

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

Definicije pojedinih izraza i termina, kao i skraćenice koje se u ovom dokumentu koriste, identične su onim navedenim i opisanim u **CP**.

2. Odgovornost za publikovanje i repozitorijume

2.1. Repozitorijum

ESS QCA publikuje sve informacije vezane za rad **ESS QCA** i izdate sertifikate na online repozitorijumima https://qca.e-smartsys.com i https://essqca.e-smartsys.com.

ESS QCA zadržava pravo da publikuje statusne informacije o sertifikatima i na repozitorijumu neke treće strane ukoliko je to pogodno.

2.2. Publikovanje informacija o sertifikatima

ESS QCA na online repozitorijumu objavljuje:

- sertifikate CA tela **ESS QCA**,
- CRL CA tela,
- OCSP servis za proveru statusa opoziva sertifikata,
- Web servis za proveru statusa sertifikata,
- Web servis za aktivaciju sertifikata,
- ova praktična pravila izdavanja kvalifikovanih sertifikata (**CPS**),
- politiku izdavanja kvalifikovanih sertifikata (**CP**),
- opšte uslove za pružanja usluga od poverenja,
- politiku privatnosti i zaštite podataka o ličnosti,
- politiku bezbednosti informacija,
- obrasce za pretplatnike/korisnike,
- korisnička uputstva, uslužne aplikacije i drajvere za QSCD nosioce kvalifikovanih sertifikata,
- 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.

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.

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.* Maksimalno dozvoljeno kašnjenje od izdavanja CRL do publikovanja je jedan sat.

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 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, OCSP i web servisi na online repozitorijumu su javno dostupni.

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 pretplatnika i korisnika. Proces identifikacije pretplatnika i korisnika **ESS QCA** je opisan u tački *4.1.* ovih **CPS**.

3.1. Imenovanje

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

ESS QCA pri obradi zahteva za izdavanje/opoziv/suspenziju kvalifikovanog sertifikata proverava verodostojnost svih dostavljenih podataka. Svi identifikacioni podaci koji se dostavljaju **ESS QCA** moraju biti verodostojni i proverljivi i moraju da jednoznačno predstavljaju pretplatnika, odnosno korisnika kvalifikovanog sertifikata.

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 kvalifikovane sertifikate korisnicima, kao ni kvalifikovane 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

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. Identifikacija fizičkog lica pripadnika entiteta pravnog lica (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Obavezni podaci koji se moraju dostaviti **ESS QCA** u vidu elektronskog zahteva, popunjenog korišćenjem aplikacije publikovane na https://essqca.e-smartsys.com/ čiji je prateći sadržaj i, od strane pretplatnika, popunjen i potpisan dokument saglasnosti za izdavanje kvalifikovanog sertifikata za elektronski potpis 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 fizičkog lica vrši se uz lično prisustvo u RA telu **ESS QCA**, upoređivanjem podataka sa zahteva i saglasnosti i podataka na identifikacionom dokumentu uključujući i proveru slike. Samo u slučaju da sve provere budu uspešne, zahtev se prihvata.

Na osnovu identifikacionih podataka, od strane RA operatera, formira se zahtev za izdavanje sertifikata, elektronski potpisuje i dostavlja u CA.

3.2.3. Identifikacija fizičkog lica koje nije pripadnik entiteta pravnog lica (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Identifikacija fizičkog lica koje nije pripadnik entiteta pravnog lica se vrši na osnovu elektronskog zahteva, popunjenog korišćenjem aplikacije publikovane na https://essqca.e-smartsys.com i priloženog identifikacionog dokumenta. Lično prisustvo fizičkog lica je obavezno u procesu identifikacije. Podaci koji se proveravaju obuhvataju:

- 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).

Na osnovu identifikacionih podataka, od strane RA operatera, formira se zahtev za izdavanje sertifikata, elektronski potpisuje i dostavlja u CA.

3.3. Identifikacija i autentikacija u procesu reizdavanja sertifikata

3.3.1. Identifikacija pretplatnika

3.3.1.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Po prijemu elektronskog zahteva za kvalifikovani sertifikat za fizičko lice pripadnika pravnog lica, RA operateri su dužni da pravno lice na koje se zahtev za reizdavanje odnosi provere u referentnim registrima ukoliko se isto ne nalazi u registrima APR. Naime, pravna lica koja postoje u registrima APR će biti automatski proverena korišćenjem elektronskih servisa APR, još u trenutku predavanja zahteva, pri čemu će biti ažurirani i podaci za pravno lice ukoliko je do promene istih došlo.

Kao prateća dokumentacija elektronskih zahteva u RA stižu potpisane elektronske saglasnosti i kartoni deponovanih potpisa.

3.3.1.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Pretplatnik podnosi elektronski zahtev za reizdavanje sertifikata za elektronski pečat, ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata.

Zahtev za reizdavanje kvalifikovanog sertifikata za elektronski pečat predaje se preko aplikacije publikovane na https://essqca.e-smartsys.com. Proces identifikacije vrši se kroz autentikaciju korišćenjem kvalifikovanog sertifikata za elektronski pečat, ukoliko je isti izdat od strane ESS QCA i za isti se traži reizdavanje.

Po prijemu elektronskog zahteva, RA operateri su dužni da pravno lice za koje je zahtev za reizdavanje primljen provere u referentnim registrima ukoliko se isto ne nalazi u registrima APR. Naime, pravna lica koja postoje u registrima APR će biti automatski proverena korišćenjem elektronskih servisa APR, još u trenutku predavanja zahteva, pri čemu će biti ažurirani i podaci za pravno lice ukoliko je do promene istih došlo.

Kao prateća dokumentacija elektronskih zahteva u RA stižu kartoni deponovanih potpisa i za kvalifikovane sertifikate za elektronski pečat čiji se privatni ključ nalazi na HSM uređaju i CSR, koje RA agenti proveravaju u smislu verodostojnosti i usaglašenosti sadržaja sa podacima unesenim u elektronskom zahtevu.

3.3.2. Identifikacija korisnika - fizičkih lica pripadnika entiteta pravnog lica - pretplatnika (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Zahtev za reizdavanje kvalifikovanog sertifikata za elektronski potpis za fizičko lice pripadnika pravnog lica se predaje elektronski korišćenjem aplikacije publikovane na https://essqca.e-smartsys.com/, ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata. Autentikacija korisnika na aplikaciju se vrši korišćenjem kvalifikovanog sertifikata za koji se zahteva reizdavanje.

U procesu autentikacije, iz subject polja sertifikata se izdvajaju podaci vezani za identifikaciju fizičkog lica, kao i pravnog lica kome pripada i ukoliko pravno pice postoji u registrima APR, automatski proverava ažurnost podataka pravnog lica i isti ažuriraju.

Od pratećih dokumenata fizičko lice prilaže:

- Skeniranu sliku identifikacionog dokumenta
- Elektronski generisanu saglasnost
- OP obrazac ukoliko je došlo do promena od poslednjeg izdavanja.

Kroz zahtev za reizdavanje moguće je zahtevati i promenu email adrese koja će biti upisana u sertifikat. Ostali podaci vezani za lice koji su deo Subject atributa (Ime, Prezime, da li se u sertifikat upisuje vlastiti identifikacioni broj - PNORS ili PNPAS) se ne mogu promeniti, kao ni identifikacioni brojevi pravnog lica (matični i poreski broj).

Sertifikat se dobija bez ponovne fizičke identifikacije korisnika i može biti isporučen na adresu sedišta pravnog lica.

Validnost elektronskog zahteva proverava RA operater **ESS QCA** na osnovu podataka iz zahteva, priloženih dokumenata, i podataka u RA bazi vezanih za JIK iz zahteva koji su ujedno upisani i u sertifikat.

Ukoliko su proveravani podaci identični, korisnik se smatra uspešno identifikovanim, a zahtev za reizdavanje sertifikata odobrenim. Razlika u broju identifikacionog dokumenta, ukoliko isti nije upisan u sertifikat korisnika, ne smatra se razlikom u podacima.

Ukoliko podaci ne odgovaraju u potpunosti, zahtev se odbija.

3.3.3. Identifikacija korisnika - fizičkih lica (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Zahtev za reizdavanje kvalifikovanog sertifikata za elektronski potpis za samostalno fizičko lice se predaje elektronski korišćenjem aplikacije publikovane na https://essqca.e-smartsys.com, ako je postojeći sertifikat validan, u periodu od 30 dana do isteka aktivnog sertifikata. Autentikacija korisnika na aplikaciju se vrši korišćenjem kvalifikovanog sertifikata za koji se zahteva reizdavanje.

U procesu autentikacije, iz subject polja sertifikata se izdvajaju podaci vezani za identifikaciju fizičkog lica.

Od pratećih dokumenata fizičko lice prilaže skeniranu sliku dokumenta identifikacije.

Kroz zahtev za reizdavanje moguće je zahtevati i promenu email adrese koja će biti upisana u sertifikat. Ostali podaci vezani za lice koji su deo Subject atributa (Ime, Prezime, da li se u sertifikat upisuje vlastiti identifikacioni broj - PNORS ili PNPAS) se ne mogu promeniti.

Sertifikat se preuzima lično u prostorijama RA tela.

Validnost elektronskog zahteva proverava RA operater **ESS QCA** na osnovu podataka iz zahteva, priloženog dokumenta, i podataka u RA bazi vezanih za JIK iz zahteva koji su ujedno upisani i u sertifikat.

Ukoliko su proveravani podaci identični, korisnik se smatra uspešno identifikovanim, a zahtev za reizdavanje sertifikata odobrenim. Razlika u broju identifikacionog dokumenta, ukoliko isti nije upisan u sertifikat korisnika, ne smatra se razlikom u podacima.

Ukoliko podaci ne odgovaraju u potpunosti, zahtev se odbija.

3.4. Identifikacija i autentikacija u procesu opoziva sertifikata

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. Obrađen zahtev za opoziv/suspenziju je vidljiv na CRL u roku od najviše 24 sata po prijemu zahteva.

3.4.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

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.

3.4.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Pretplatnik može da zahteva opoziv/suspenziju sertifikata za elektronski pečat. Zahtev za opoziv/suspenziju od strane pretplatnika se dostavlja elektronski 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

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

4.1.1. Podnošenje zahteva za dobijanje sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Zahtev podnosi fizičko lice koje može biti i pripadnik entiteta pravnog lica. Zahtev se podnosi elektronski korišćenjem aplikacije publikovane na https://essqca.e-smartsys.com/, u dva koraka:

1) Verifikacija e-mail adrese korisnika
2) Unos podataka i upload dokumenata zahteva za korisnike sa verifikovanim email adresama.

Kroz formu elektronskog zahteva korisnik dostavlja sledeće podatke:

1) ime fizičkog lica,
2) prezime fizičkog lica,
3) tip identifikacionog dokumenta fizičkog lica (identifikaciona dokumenta izdata od strane MUP RS ili pasoš za strane državljane),
4) broj identifikacionog dokumenta,
5) oznaka zemlje izdavaoca pasoša (ukoliko je identifikacioni dokument pasoš),
6) da li će se kvalifikovani sertifikat za elektronski potpis koristiti za rad na državnim portalima,
7) datum isteka pasoša i izabrana opcija korišćenja za rad sa državom,
8) broj mobilnog telefona fizičkog lica,
9) email adresa fizičkog lica,
10) šifra QSCD uređaja na kome će biti izdat kvalifikovani sertifikat za elektronski potpis (podatak iz cenovnika **ESS QCA**),
11) trajanje kvalifikovanog sertifikata u godinama,
12) za fizička lica pripadnike entiteta pravnog lica koja nisu pretplatnici evidentirani u sistemu ESS QCA potrebno je uneti i:
    a. matični broj pravnog lica pretplatnika
    b. PIB pretplatnika,
    c. naziv pravnog lica pretplatnika,
    d. poslovno ime pravnog lica pretplatnika,
    e. adresa sedišta pravnog lica pretplatnika,
    f. mesto sedišta pravnog lica pretplatnika,
    g. poslovni email pravnog lica pretplatnika,
    h. ime i prezime zakonskog zastupnika,
    i. ovlašćeno lice – lice ovlašćeno od strane pretplatnika za menjanje podataka na saglasnosti,
    j. ovlašćeni email - email adresa pretplatnika sa koje ovlašćeno lice može da šalje zahteve za izmenu podataka sa saglasnosti
13) za fizička lica pripadnike entiteta pravnog lica koja su pretplatnici evidentirani u sistemu ESS QCA potrebno je uneti i:

a. ovlašćeno lice – lice ovlašćeno od strane pretplatnika za menjanje podataka na saglasnosti,
b. ovlašćeni email - email adresa pretplatnika sa koje ovlašćeno lice može da šalje zahteve za izmenu podataka sa saglasnosti.

Uz navedene podatke korisnik prilaže i:

1) za fizička lica pripadnike entiteta pravnog lica koja nisu pretplatnici evidentirani u sistemu ESS QCA:
   a. OP obrazac
   b. overen elektronski dokument ugovora,
   c. overen elektronski dokument saglasnosti
2) za fizička lica pripadnike entiteta pravnog lica koja su pretplatnici evidentirani u sistemu ESS QCA potrebno je uneti i:
   a. OP obrazac, ukoliko je došlo do promena u odnosu na poslednji zahtev,
   b. overen elektronski dokument saglasnosti.

Sastavni deo ugovora koji overava korisnik čine i klauzule o prihvatanju **ESS QCA** CP/CPS, **ESS QCA** Opštih uslova za pružanje usluga od poverenja i **ESS QCA** Politike privatnosti i zaštite podataka o ličnosti.

Proces održavanja podataka o pretplatnicima realizuje se unutar RA tela prilikom svakog podnošenja elektronskog zahteva i obuhvata proveru i ažuriranje podataka na osnovu zapisa u nadležnim registrima: APR, NBS, Poreska uprava i priloženog dokumenta OP obrasca. Za pravna lica registrovana u APR, podaci iz tačke 12 se preuzimaju automatski korišćenjem servisa APR koji ESS QCA koristi u skladu sa Sporazumom o preuzimanju i korišćenju podataka.

Prijem saglasnosti za izdavanje kvalifikovanog sertifikata za elektronski potpis u RA stiže isključivo u elektronskom obliku.

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

Nakon evidencije uplate pretplatnika, RA telo šalje poruku fizičkom licu za koje je data saglasnost (koristeći podatke upisane u poljima email i mobilni telefon) da dođe 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,
- rok za obavljanje identifikacije,
- lokacije na kojima se mogu pročitati dokumenti **CP**, **CPS** i politike privatnosti i zaštite podataka o ličnosti.

U slučaju da samo fizičko lice podnosi zahtev za izdavanje kvalifikovanog sertifikata za elektronski potpis, RA sprovodi proces identifikacije i registracije na licu mesta po prijemu elektronskog zahteva.

4.1.2. Podnošenje zahteva za dobijanje sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

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

Prijem zahteva za izdavanje kvalifikovanog sertifikata za elektronski pečat u RA stiže isključivo u elektronskom obliku korišćenjem aplikacije publikovane na https://essqca.e-smartsys.com, u dva koraka:

1) Verifikacija e-mail adrese korisnika
2) Unos podataka i upload dokumenata zahteva za korisnike sa verifikovanim email adresama.

Kroz formu elektronskog zahteva za izdavanje kvalifikovanog sertifikata za elektronski pečat dostavljaju se sledeći podaci:

1) email za pečat – email koji će biti upisan u telo sertifikata
2) broj pečata – ukoliko se sertifikat izdaje na smart kartici može se zahtevati izdavanje više od jednog pečata

3) da li se upisuje mesto sedišta u polje Subject sertifikata,
4) organizaciona jedinica – ukoliko se zahteva upis iste u telo sertifikata
5) mobilni telefon – za komunikaciju u procesu izdavanja
6) šifra QSCD uređaja na kome će biti izdat kvalifikovani sertifikat za elektronski pečat (podatak iz cenovnika **ESS QCA**),
7) trajanje kvalifikovanog sertifikata u godinama
8) pravna lica koja nisu pretplatnici evidentirani u sistemu ESS QCA dostavljaju sledeće dodatne podatke:
    a. matični broj pravnog lica pretplatnika,
    b. PIB pretplatnika,
    c. naziv pravnog lica pretplatnika,
    d. poslovno ime pravnog lica pretplatnika,
    e. adresa sedišta pravnog lica pretplatnika,
    f. mesto sedišta pravnog lica pretplatnika,
    g. poslovni email pravnog lica pretplatnika,
    h. ovlašćeno lice za odobrenje izmene podataka,
    i. email lica ovlašćenog za odobrenje izmene podataka,
    j. ime i prezime, tip i broj dokumenta identifikacije lica koje će preuzeti pečate – ukoliko se pečati preuzimaju lično,
    k. poštanski broj i kontakt mobilni telefon – ukoliko se pečati preuzimaju kurirskom službom
9) pravna lica koja su već pretplatnici evidentirani u sistemu ESS QCA dostavljaju sledeće dodatne podatke:
    a. ovlašćeno lice za odobrenje izmene podataka,
    b. email lica ovlašćenog za odobrenje izmene podataka,
    c. ime i prezime, tip i broj dokumenta identifikacije lica koje će preuzeti pečate – ukoliko se pečati preuzimaju lično,
    d. poštanski broj i kontakt mobilni telefon – ukoliko se pečati preuzimaju kurirskom službom.

Uz navedene podatke korisnik prilaže i:

1) za elektronske pečate za koje se zahteva izdavanje na HSM uređaju:
    a. CSR sa javnim ključem para ključeva generisanog na HSM uređaju
2) za fizička lica pripadnike entiteta pravnog lica koja nisu pretplatnici evidentirani u sistemu ESS QCA:
    a. OP obrazac
    b. overen elektronski dokument ugovora
3) za fizička lica pripadnike entiteta pravnog lica koja su pretplatnici evidentirani u sistemu ESS QCA potrebno je uneti i:
    a. OP obrazac, ukoliko je došlo do promena u odnosu na poslednji zahtev.

Sastavni deo ugovora koji overava pretplatnik čine i klauzule o prihvatanju **ESS QCA** CP/CPS, **ESS QCA** Opštih uslova za pružanje usluga od poverenja i **ESS QCA** Politike privatnosti i zaštite podataka o ličnosti.

Nakon prijema elektronskog zahteva i provere validnosti podataka, RA operater sačinjava predračun i šalje ovlašćenom licu pretplatnika.

Sertifikati za elektronski pečat se izdaju na:

- QSCD uređajima koje obezbeđuje **ESS QCA** u skladu sa Zakonom,

- QSCD uređajima koje obezbeđuje sam pretplatnik, budući korisnik kvalifikovanog sertifikata za elektronski pečat (HSM korisnik) u skladu sa Zakonom. U ovom slučaju stručna lica **ESS QCA** će verifikovati usklađenost uređaja, nosioca privatnog ključa sa standardima i Zakonom pre izdavanja samog sertifikata.

Ceremonija formiranja CSR na QSCD uređaju mora biti nadgledana i kontrolisana od strane stručnog lica **ESS QCA**, i može se realizovati na lokaciji korisnika ili unutar CA zone bezbednosti **ESS QCA**. Proces ceremonije obuhvata:

- proveru i validaciju uređaja nosioca privatnog ključa
- generisanje CSR.

Upload CSR se vrši u procesu podnošenja elektronskog zahteva putem web aplikacije publikovane na https://essqca.e-smartsys.com.

Rezultat ceremonije predstavlja i zapisnik o procesu realizacije ceremonije kojim se potvrđuje da su sve gore navedene aktivnosti uspešno realizovane.

Proces održavanja podataka o pretplatnicima realizuje se unutar RA tela prilikom svakog podnošenja elektronskog zahteva i obuhvata proveru i ažuriranje podataka na osnovu zapisa u nadležnim registrima: APR, NBS, Poreska uprava i priloženog dokumenta OP obrasca. Za pravna lica registrovana u APR, podaci iz tačke 8 se preuzimaju automatski korišćenjem servisa APR koji ESS QCA koristi u skladu sa Sporazumom o preuzimanju i korišćenju podataka.

U slučaju da dođe do promene matičnih podataka pravnog lica, pre svega punog ili skraćenog naziva, odgovornost pretplatnika je da za sve kvalifikovane sertifikate za elektronski pečat u kojima su upisani nevažeći podaci zahteva povlačenje i reizdavanje sertifikata sa važećim podacima u skladu sa zakonom.

4.2. Procesiranje zahteva za dobijanje sertifikata

4.2.1. Procesiranje zahteva za dobijanje sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Fizičko lice se javlja RA operateru koji vrši identifikaciju u unapred utvrđenom terminu. Da bi se identifikacija smatrala uspešnom, potrebno je da fizičko lice poseduje identifikacioni dokument koji po broju i vrsti odgovara dokumentu navedenom u elektronskom zahtevu koji je u roku važenja.

Za uspešno identifikovano fizičko lice, u slučaju da se zahteva kvalifikovani sertifikat za elektronski potpis za rad za državom, unosi se i JMBG/EBS.

Uneti podaci se automatski struktuiraju u elektronski dokument zahteva za izdavanje kvalifikovanog sertifikata za elektronski potpis. RA operater stavlja svoj kvalifikovani elektronski potpis na elektronski dokument zahteva, nakon čega se zahtev zaštićenim kanalom automatski 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 QSCD uređaja.

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

Po isteku roka važenja zahteva za koje se nisu pojavila fizička lica da lično budu identifikovana, isti će biti automatski odbijeni.

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.

4.2.2. Procesiranje zahteva za dobijanje sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Nakon provere podataka iz elektronskog zahteva i potvrde izvršene uplate, RA operater odobrava podatke elektronskog zahteva koji uključuju i CSR i potvrđuje unos u sistem **ESS QCA**.

Informacioni sistem **ESS QCA** formira elektronski dokument zahteva, a RA operater stavlja svoj kvalifikovani elektronski potpis na ovaj elektronski dokument, nakon čega se zahtev zaštićenim kanalom automatski dostavlja u CA telo **ESS QCA**.

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 potpis RA operatera nad elektronskim dokumentom zahteva,
- odobrava ili odbija pojedinačni zahtev iz elektronskog dokumenta,
- formira CSR koja uključuje i javni ključ sa pripremljenog QSCD uređaja i vrši izdavanje kvalifikovanog sertifikata,
- **ESS QCA** sistem obaveštava pretplatnika/korisnika o tome da je izdat sertifikat i kako može da se aktivira. Sertifikat se po izdavanju suspenduje zbog zaštite u transportu, a pretplatnik/korisnik obaveštava o jednokratnom aktivacionom kodu kvalifikovanog sertifikata putem SMS poruke,
- CA operater upisuje na QSCD uređaj izdati kvalifikovani sertifikat ukoliko je u obradi zahteva radio sa pripremljenim QSCD uređajem. Ukoliko je RA operater dostavio zahtev sa javnim ključem, izdati kvalifikovani sertifikat se automatski dostavlja RA telu, gde se kasnije povezuje sa QSCD uređajem,
- 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 kojim pretplatnik/korisnik preko online repozitorijuma https://essqca.e-smartsys.com/aktivacija aktivira sertifikat nakon preuzimanja.
- PIN kod QSCD uređaja kojim se pristupa privatnom ključu.

4.4. Prihvatanje sertifikata

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

4.4.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Uručenje QSCD uređaja vrši se na jedan od sledećih načina:

- ličnim preuzimanjem - ako korisnik lično preuzima QSCD uređaj, u prostorijama **ESS QCA** ili ovlašćenog RA tela za rad sa pripremljenim QSCD uređajima, i koverta sa PIN/PUK mu se uručuje lično,

  kurirskom službom - ako se QSCD uređaj dostavlja kurirskom službom, što je moguće samo u slučaju reizdavanja ili promene podataka, kada je korisnik postojećeg pretplatnika već identifikovan a pri podnošenju zahteva je autentikovan korišćenjem postojećeg kvalifikovanog sertifikata za elektronski potpis, isti se šalje na adresu sedišta firme, a PIN/PUK šalju na mobilni telefon korisniku.

Prilikom preuzimanja QSCD uređaja korisnik potpisuje potvrdu o preuzimanju kvalifikovanog sertifikata. U slučaju ličnog preuzimanja kvalifikovanog sertifikata za elektronski potpis, potpisuje se i korisnički ugovor. Na ovaj način korisnik kvalifikovanog sertifikata i formalno prihvata preuzeti sertifikat i obaveze i uslove iz CP/CPS.

Korisnik preko online servisa https://essqca.e-smartsys.com/aktivacija aktivira sertifikat korišćenjem dva parametra:

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

4.4.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Uručenje QSCD uređaja vrši se na jedan od sledećih načina:

- ličnim preuzimanjem - ako ovlašćeno lice pretplatnika lično preuzima QSCD uređaj, u prostorijama **ESS QCA** ili ovlašćenog RA tela za rad sa pripremljenim QSCD uređajima, i koverta sa PIN/PUK mu se uručuje lično,
- kurirskom službom - sertifikat se šalje na adresu sedišta firme, a PIN/PUK šalju na registrovani mobilni telefon,
- elektronskim preuzimanjem – ako se sertifikat izdaje za par ključeva generisanih na QSCD uređaju pretplatnika (HSM korisnik). Nakon izdavanja sertifikata pretplatnik će dobiti link do strane na kojoj će moći da elektronski preuzme kvalifikovani sertifikat za elektronski pečat i potvrdi preuzimanje istog.

U prva dva slučaja pretplatnik prilikom preuzimanja QSCD uređaja potpisuje potvrdu o preuzimanju kvalifikovanog sertifikata..

U slučaju izdavanja kvalifikovanog sertifikata za elektronski pečat za HSM korisnika, nakon izdavanja istom se na verifikovanu e-mail adresu šalje poruka sa jednokratnim linkom do strane za potvrdu prijema i preuzimanje izdatog sertifikata.

Pretplatnik preko online servisa https://essqca.e-smartsys.com/aktivacija aktivira sertifikat korišćenjem dva parametra:

- jednokratnog aktivacionog koda (JAK) kvalifikovanog sertifikata koji je poslat direktno pretplatniku
- jedinstvenog identifikatora korisnika (JIK) poslatog mailom ili odštampanog na QSCD uređaju koji je uručen.

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 pretplatničkom/korisničkom ugovoru kao i u *Opštim uslovima za pružanje usluga od poverenja* i to:

- Odgovornosti pretplatnika kome je izdat kvalifikovani sertifikat za elektronski pečat, odnosno korisnika kvalifikovanog sertifikata za elektronski potpis – pretplatnik/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 pretplatničkog/korisničkog ugovora sa **ESS QCA**. U tom smislu, pretplatnik/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 provera validnost sertifikata u odnosu na period trajanja iz sertifikata i status na listi povučenih sertifikata (CRL) za suspendovane ili povučene sertifikate, kao i Javnu listu kvalifikovanih usluga od poverenja publikovanu na https://mit.gov.rs/extfile/sr/499/TSL-RS.xml.
- Obaveza registracionih tela, pretplatnika, korisnika i drugih učesnika je da informišu **ESS QCA** o svim promenama u informacijama koje su objavljene u kvalifikovanom sertifikatu 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 pretplatnika/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 pretplatnik/korisnik ne mora biti ponovno identifikovan, zahtev podnosi elektronski koristeći aplikaciju publikovanu na https://essqca.e-smartsys.com na koju se autentikuje 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 automatski obaveštava pretplatnika/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

Pretplatnici/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. U procesu izdavanja pretplatniku/korisniku će biti dodeljen i novi JIK.

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

4.8. Modifikacije sertifikata

Modifikacije postojećeg sertifikata nisu dozvoljene.

Ukoliko su potrebne modifikacije, radi se postupak promene podataka uz izdavanje novog sertifikata i automatski opoziv postojećeg.

Zahtev za izdavanje novog sertifikata sa promenjenim podacima podnosi se elektronski preko aplikacije publikovane na lokaciji https://essqca.e-smartsys.com. Pretplatnik/korisnik se na aplikaciju loguje važećim kvalifikovanim sertifikatom za koji se zahteva promena podataka.

4.9. Suspenzija i opoziv sertifikata

ESS QCA vrši opoziv izdatog kvalifikovanog sertifikata u slučaju:

- gubitka, krađe, promene podataka ili neke druge kompromitacije privatnog ključa sertifikata,
- kada se desila promena informacija koja su sadržane u sertifikatu datog lica,
- kada pretplatnik ukida pripadnost entitetu za korisnika,
- kada pretplatnik/korisnik zahteva opoziv sertifikata,
- kada su podaci za proveru kvalifikovanog elektronskog potpisa/pečata ugroženi na način koji utiče na bezbednost i pouzdanost sertifikata.

ESS QCA vrši suspenziju izdatog kvalifikovanog sertifikata u sledećim slučajevima:

- prilikom samog izdavanja kvalifikovanog sertifikata (opisano u poglavlju *4.4.*),
- prilikom izdavanja obnovljenog kvalifikovanog sertifikata (opisano u poglavlju *4.6.*),
- na zahtev pretplatnika/korisnika ili **ESS QCA** ukoliko postoji sumnja o kompromitaciji privatnog ključa,
- na zahtev pretplatnika kada privremeno ukida pripadnost entitetu za korisnika.

ESS QCA vrši opoziv sertifikata izdavajućeg tela u sledećim slučajevima:

- Pojave incidenta koji je kompromitovao privatni ključ CA tela tako da postoji osnovana sumnja da se može koristiti od neovlašćenih lica za izdavanje sertifikata u budućnosti

- Pojave incidenta koji je kompromitovao privatni ključ CA tela tako da je neovlašćeno izdat određeni broj sertifikata neusklađenih sa ESS QCA CP/CPS, a neovlašćeno izdati sertifikati se ne mogu pouzdano identifikovati i povući postojećim mehanizmima
- pojave incidenta koji je kompromitovao tehnički sistem CA tela do mere da više nije moguće koristiti privatni ključ izdavajućeg tela, pomoćne elemete sistema, uključujući i autentikacione tokene administratora, odnosno nije moguće izdavati liste povučenih sertiikata
- ESS QCA ne može iz drugih razloga uključujući i poslovne da održava proces izdavanja liste povučenih sertifikata.

Povlačenje sertifikata u prvom slučaju se vrši bez odlaganja i vanredno publikuje lista povučenih sertifikata root tela, a zatim obaveštava nadležno Ministarstvo. Procedura povlačenja obuhvata:

- povlačenje svih sertifikata koje je kompromitujuće CA telo izdalo,
- publikovanje liste povučenih sertifikata koja traje do datuma isteka sertifikata izdavajućeg tela
- povlačenje sertifikata izdavajućeg tela na root telu i publikovanje liste povučenih sertifikata root tela.

U drugom slučaju prvo se obaveštava nadležno Ministarstvo, a zatim izvodi povlačenje sertifikata po koracima iz prvog slučaja.

U preostala dva slučaja, prvo se obaveštava nadležno Ministarstvo, a zatim realizuje povlačenje sertifikata na root telu i vanredno publikuje lista povučenih sertifikata root tela.

Ukoliko je kompromitovano i root telo, odnosno mehanizmom liste povučenih sertifikata se ne može staviti van upotrebe kompromitovano izdavajuće telo, potrebno je obavestiti nadležno Ministarstvo kako bi isto bilo uklonjeno sa TSL.

ESS QCA sprovodi nadzor rada celog sistema i detektuje nepravilnosti. Detektovane nepravilnosti u slučaju kompromitacije jednog ili više kvalifikovanih sertifikata 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 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 za suspenziju 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 suspenzije.

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 pretplatnika ili korisnika.

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

ESS QCA ne reaktivira jednom opozvani sertifikat, odnosno isti ne može biti uklonjen sa liste povučenih sertifikata (CRL).

Korisniku čiji je sertifikat opozvan ili suspendovan automatski se šalje email sa porukom o promeni statusa sertifikata.

ESS QCA opozvani i suspendovane sertifikate publikuje u listi povučenih sertifikata (CRL) u skladu sa RFC 5280 i preko OCSP servisa.

4.9.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Proces opoziva kvalifikovanih sertifikata može inicirati:

1) Pretplatnik koji je inicirao izdavanje, kvalifikovanog sertifikata za elektronski potpis 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, 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.

4.9.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Proces opoziva kvalifikovanih sertifikata može inicirati:

1) Pretplatnik koji je inicirao izdavanje, kvalifikovanog sertifikata za elektronski pečat.

   Pretplatnik, pravno lice, ima pravo da podnese zahtev koji rezultuje opozivom kvalifikovanog sertifikata za elektronski pečat.

2) RA operater

   Ukoliko postoji greška u podacima upisanim u sertifikat, RA operater kreira zahtev za opoziv kvalifikovanog sertifikata, 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.

3) ESS QCA

   Ukoliko je ustanovljen rizik od kompromitacije privatnog ključa za jedan ili više izdatih kvalifikovanih sertifikata.

4.10. Servisi provere statusa sertifikata

Liste opozvanih sertifikata (CRL) *ESS IQCA1, ESS IQCA1 V3* i *ESS IQCA2 V3* se ažuriraju na svakih 24 sata, a *ESS RQCA* i *ESS RQCA V3* na svakih 6 meseci. Treće strane mogu koristiti jedan od dva raspoloživa online repozitorijuma https://qca.e-smartsys.com i https://essqca.e-smartsys.com za preuzimanje CRL, a za klijentske sertifikate i treći ldap://ldap.qca.e-smartsys.rs/.

Opozvani ili suspendovan kvalifikovani sertifikat je vidljiv na CRL 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. U slučaju opoziva *issuing CA* elektronskog sertifikata **ESS QCA** obaveštava korisnike direktno, a treće strane preko web site-a na lokaciji https://essqca.e-smartsys.com u roku od 24 sata od podnesenog zahteva za opoziv *issuing* CA elektronskog sertifikata **ESS QCA**.

Pretplatnici/korisnici trenutni status svog sertifikata mogu proveriti na site-u https://essqca.e-smartsys.com/status.

ESS QCA garantuje raspoloživost servisa publikacije CRL/OCSP 24x7 sa 99.99% dostupnosti na godišnjem nivou. Ukoliko dođe do prekida u raspoloživosti servisa, ESS QCA garantuje oporavak u periodu ne dužem od 30min.

Publikovana informacija o opozvanom/suspendovanom sertifikatu je istovremeno i jednoznačno dostupna i preko CRL publikacije i preko OCSP servisa.

4.10.1. Potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Podaci o statusu sertifikata dostupni su i preko OCSP servisa na lokacijama https://qca.e-smartsys.com/ocsp/ESSQCA1 i https://qca.e-smartsys.com/ocsp/ESSIQCA1V3.

4.10.2. Pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Podaci o statusu sertifikata dostupni su i preko OCSP servisa na lokaciji https://qca.e-smartsys.com/ocsp/ESSIQCA2V3.

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:

- Pretplatnik/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 se ne opozivaju.

4.12. Čuvanje i rekonstrukcija privatnog ključa

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

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 serije 27000, 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

Odgovarajuće fizičke kontrole zaštite primenjene su na sva identifikovana fizička dobra koja učestvuju u poslovnim procesima **ESS QCA**. Sistem fizičke kontrole **ESS QCA** je deo šireg sistema fizičke kontrole dobara E-Smart Systems d.o.o. u čijem okviru posluje **ESS QCA**.

5.1.1. Lokacija i zgrada

Matična lokacija **ESS QCA** nalazi se na lokaciji Kneza Višeslava 70.

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

- Zonu javnog pristupa – u kojoj se vrši provera lica i autorizacija za pristup ostalim zonama,
- Zonu boravka autorizovanih lica – u kojoj lica koja dolaze na ličnu identifikaciju čekaju na zakazani termin u **ESS QCA**,
- Zonu bezbednosti RA – u kojoj se obavlja lična identifikacija i obrada zahteva lica koje zahteva izdavanje i/ili opoziv sertifikata,
- Zonu bezbednosti CA – u kojoj se obrađuju zahtevi za izdavanje i/ili opoziv sertifikata, upravljanja ključevima na QSCD i personalizacija QSCD,
- Zonu visoke bezbednosti CA – u kojoj se upravlja ključevima CA tela, obezbeđuju funkcije izdavanja sertifikata i publikovanja CRL.

5.1.2. Fizički pristup

Sve opisane zone imaju primenjene kontrole fizičkog pristupa i to:

- Zona javnog pristupa – 24h FTO obezbeđenje, video nadzor
- Zona boravka autorizovanih lica – 24h FTO obezbeđenje, video nadzor
- Zona bezbednosti RA – 24h FTO, elektronska kontrola pristupa, video nadzor
- Zona bezbednosti CA – video nadzor, fizička barijera, elektronska kontrola pristupa
- Zonu visoke bezbednosti CA – video nadzor, fizička barijera, elektronska kontrola pristupa, 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, a sekundarno UPS uređajima. 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 zgradi. U okviru zgrade nalaze se protivpožarni aparati za odgovarajuću klasu požara. Aparati za gašenje požara nalaze se i u kavezima zona bezbednosti i visoke bezbednosti u cilju zaštite osoblja koje bi se tamo zateklo. Aparati za gašenje požara se redovno proveravaju i održavaju.

5.1.6. Medijumi za čuvanje podataka

Medijumi za čuvanje podataka **ESS QCA** dele se na interne i eksterne.

Interni medijumi su namenjeni čuvanju operativnih podataka i sastavni su deo serverskog hardvera u zoni visoke bezbednosti.

Eksterni medijumi su namenjeni čuvanju bekapa operativnih i arhivskih podataka. Upotreba i zaštita eksternih, pokretnih medijuma strogo je kontrolisana u mirovanju kao i u periodima operativnog rada.

Eksterni i interni medijumi koji su korišćeni u **ESS QCA** se nakon perioda korišćenja fizički uništavaju.

5.1.7. Odlaganje otpada

Iznošenje otpada se kontroliše. Papirni otpad se uništava u šrederima papira. Električni uređaji se posle uklanjanja iz procesa i iznošenja iz zona bezbednosti, fizički uništavaju.

5.1.8. Odlaganje rezervnih kopija

Backup medijumi se čuvaju na 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.

Posebna instanca Backup medija se čuva na DR lokaciji ZDC u Tehnološkom parku Vršac.

5.2. Proceduralne kontrole

Proceduralne ili administrativne kontrole oslanjaju se na ažuran i pouzdan proceduralni okvir koji obuhvata:

- Procedure registracije pretplatnika
- Kontrolu verodostojnosti podataka o pretplatniku
- Pripremu zahteva za izdavanje kvalifikovanog sertifikata
- Identifikaciju podnosioca zahteva
- Obradu zahteva

- Generisanje kvalifikovanog sertifikata
- Bezbedno dostavljanje i uručenje kvalifikovanog sertifikata
- Opoziv/suspenzija kvalifikovanog sertifikata
- Reizdavanje kvalifikovanog sertifikata
- Deblokada QSCD uređaja
- Upravljanje incidentima i bezbednosnim uređajima.

5.2.1. Poverljive uloge

Uloge od poverenja u **ESS QCA** realizuju resursi sa kvalifikacijama 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 **CP** i zahtevane Zakonom.

Poslovi uloga od poverenja obuhvataju:

- Upravljanje kompletnim sistemom bezbednosti **ESS QCA**,
- Administraciju i konfiguraciju serverskih i klijentskih resursa,
- Upravljanje promenama na sistemu **ESS QCA**,
- Upravljanje privatnim ključevima na HSM uređajima,
- Monitoring i kontrolu rada uloga od ovlašćenja i rada sistema u celini,
- Bezbednosno testiranje **ESS QCA**.

Uloge od ovlašćenja **ESS QCA** realizuju resursi sa sledećim kvalifikacijama:

- Tri zaposlena sa dugogodišnjim iskustvom u radu sa **PKI** tehnologijom i internom obukom iz domena bezbednosti, kriptografije i zakonske regulative iz oblasti elektronskog dokumenta, elektronskog potpisa, odnosno pečata 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, elektronskog potpisa, odnosno pečata za poslove RA operatera.

Poslovi uloga od ovlašćenja obuhvataju operativne poslove RA i CA operatera.

5.2.2. Broj osoba koje se zahtevaju po svakom zadatku

Za izvršenje operacija, 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 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, odnosno pečat.

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

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

5.2.3. Identifikacija i autentikacija uloga od poverenja i ovlašćenja

Uloge od poverenja i ovlašćenja koriste po pravilu dvostepenu 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 odgovornosti

U cilju zaštite procesa izdavanja kvalifikovanog sertifikata razdvajanjem uloga je obezbeđeno da proces ne može da se realizuje bez minimalno dva ili više lica, od kojih minimalno po jedno na strani RA, odnosno CA učestvuje u procesu.

Unutar RA i CA celina obezbeđeni su uslovi za simultani rad operatera i zamenu uloga na istom zahtevu u cilju kontrole i sprečavanja zloupotrebe prava.

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 sa minimalno tri odnosno jednom godinom radnog staža u preduzeću.

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 u skladu sa politikom bezbednosti, imaju ugovor o neotkrivanju poverljivih informacija (NDA) potpisan 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 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 obezbeđuje deljenje znanja vezanih za konfiguraciju i operacije sistema **ESS QCA** i obezbeđuje kontinuitet poslovanja u oblasti ljudskih resursa.

5.3.6. Kaznene mere u odnosu na zaposlene

U slučaju povrede radne dužnosti u **ESS QCA**, po pravilu i bez izuzetka primenjuje se mera dodatne obuke, treninga i provere znanja do postizanja neophodnog nivoa svesti učesnika u procesu.

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

Povrede radne dužnosti u **ESS QCA** povezane sa bezbednošću informacija sankcionisane su u skladu sa Politikom bezbednosti informacija Društva.

5.3.7. Kontrole nezavisnih ugovarača

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

5.3.8. Dokumentacija za inicijalnu obuku ii 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, analizira, obrađuje i nadzire događaje u tehničkom i poslovnom delu sistema koristeći centralizovano rešenje kojim upravlja uloga od poverenja – sistem evidentičar.

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 zaštićen kontrolom pristupa

- Događaji u fizičkom prostoru zona bezbednosti i visoke bezbednosti (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
  - Potpisani papirni dokumenti 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 sistema su tehničkim merama zaštićeni od promena. Ni jedna od uloga ESS QCA nema prava izmene audit logova. Manuelni pristup audit logovima u tranzitu i u skladištu tehnički je onemogućen.

Uvid u audit logove je obezbeđen za sve uloge, a publikovan je u vidu automatskog izveštaja koji se ne može trajno modifikovati. Automatsko publikovanje podataka iz audit logova se realizuje na dnevnom nivou.

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

Sistemski audit logovi se čuvaju u centralnoj bazi podataka u periodu od godinu dana. Nakon ovog perioda se čuvaju slike stanja sistema u periodu izdavanja kvalifikovanih sertifikata. Ove slike stanja se arhiviraju i čuvaju u periodu čuvanja sertifikata. Audit logovi vezani za izdavanje kvalifikovanih sertifikata se čuvaju u periodu propisanom Zakonom i dostupni su za direktan uvid tokom celokupnog životnog veka.

Opisani sistem se nalazi pod redovnom procedurom backup-a. Arhive podataka starijih od godinu dana se čuvaju na eksternim medijumima.

5.4.6. Sistem sakupljanja audit logova

Logovi svih računarski identifikovanih događaja u sistemu se sakupljaju u realnom vremenu i čuvaju u audit bazama RA i CA sistema, ili u centralnom rešenju za prikupljanje sistemskih logova. Sakupljaju se događaji sa svih nivoa arhitekture sistema od loga mrežnih uređaja preko logova centralnih računarskih resursa do logova klijentskih radnih stanica i aplikacija.

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 permanentnim bezbednosnim testiranjem koje se realizuje u skladu sa najboljim praksama PenTest i OWASP standarda testiranja.

U procesu evaluacije ranjivosti i testiranja bezbednosti koriste se automatizovani alati, usluge trećih strana sa adekvatnom kvalifikacijom i iskustvom i standardi i base line preporuke u skladu sa NIST 800-115.

5.5. Arhiviranje zapisa

Zapisi **ESS QCA** se čuvaju, štite, nadgledaju i izlučuju u skladu sa Zakonskom regulativom.

5.5.1. Tipovi arhiviranih zapisa

ESS QCA čuva na bezbedan način zapise o izdatim kvalifikovanim sertifikatima, 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 u periodu od 10 godina u odnosu na datum kada se događaj desio.

Zapisi za koje je period čuvanja istekao izlučuju se istovremeno iz elektronskih arhiva i papirne arhive.

Podaci o položaju informacija u papirnim arhivama se čuvaju u sistemu za automatsku obradu podataka, tako da se svaki zahtev i prateća dokumentacija u svakom trenutku životnog veka do izlučivanja mogu precizno locirati u papirnoj arhivi.

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**.

Papirna arhiva se nalazi u fizički obezbeđenom prostoru kome mogu pristupiti samo osobe od ovlašćenja RA operateri uz odobrenje osobe od poverenja – sistem evidentičara.

Administrator bezbednosti regularno u periodu ne dužem od 6 meseci nadgleda stanje **ESS QCA** papirne arhive.

5.5.4. Procedura backup-a arhive

ESS QCA sprovodi proceduru backup-a arhive na eksternu obezbeđenu lokaciju.

Backup-i arhiva se čuvaju i izlučuju u skladu sa periodom čuvanja podataka o kvalifikovanom sertifikatu na koji se odnose.

Backup-i arhiva se nakon isteka perioda čuvanja fizički uništavaju.

5.5.5. Zahtevi za vremenskim pečatom zapisa

Elektronski rekordi vezani za transakcije **ESS QCA** 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 **ESSElCollect** instaliranog na centralnoj lokaciji **ESS QCA**. Ovo rešenje obezbeđuje niz pregleda, statistika, report-a i notifikacija u cilju efikasnog korišćenja prikupljenih informacija.

5.5.7. Procedura 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. Procedura za dobijanje i verifikaciju informacija iz arhive obuhvata sledeće korake:

- Prijem zahteva za dobijanje podataka iz arhive
- Odobravanje zahteva za dobijanje podataka iz arhive
- Lociranje svih podataka vezanih za predmet arhiviranja
- Izdvajanje podataka iz arhive i formiranje bezbednih kopija za lice koje je podnelo zahtev
- Uručenje kopija arhivskih podataka licu koje je podnelo zahtev

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 Zakonom i internom **ESS QCA** regulativom. 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 https://essqca.e-smartsys.com/preuzimanje-i-instalacija-softvera kao i https://mit.gov.rs/extfile/sr/499/TSL-RS.xml koju održava nadležno Ministarstvo.

5.7. Kompromitacija i oporavak u slučaju katastrofe

5.7.1. Procedura za postupanje u incidentnim i kompromitujućim situacijama

Upravljanje incidentima unutar **ESS QCA** realizuje u skladu sa Procedurom za upravljanje incidentima prema sledećem poslovnom toku:

- Bezbednosni događaj se u najkraćem roku (odmah) prijavljuje timu za internu podršku,
- O događaju se formira dokumentovani zapis iza čega se automatski šalju notifikacije stručnim licima koja učestvuju u analizi i/ili daljem prikupljanju podataka o incidentu,
- Lica koja su učestvovala u analizi detaljno izveštavaju o incidentu što obuhvata prezentaciju svih prikupljenih podataka i moguće smernice za rešavanje. Izveštaji se unose u formi dokumentovanih zapisa na centralni portal Incidenata iza čega se šalju automatske notifikacije licima ovlašćenim za realizaciju hitnih promena u sistemu,
- Lica ovlašćena za realizaciju hitnih promena na sistemu, rešavaju incident prema planu i/ili realizuju kompenzaciju negativnih uticaja koje je izazvao,

- Administrator bezbednosti **ESS QCA** izveštava o posledicama incidenta i preduzetim merama za njihovu kontrolu i umanjenje,
- Rukovodilac sistema odlučuje o merama koje treba preduzeti u cilju predupređenja sličnih incidenata i formira zahteve za promenama na sistemu, kao i načinu publikovanja informacija o incidentu, uključujući identifikovane uzroke, ranjivosti i mere preduzete za rešavanje, kao i mesta prijave/publikovanja. Informacije o incidentima mogu biti publikovane na https://essqca.e-smartsys.com, o njima može biti informisano nadležno Ministarstvo ili nacionalni CERT (https://www.cert.rs).

5.7.2. Računarski resursi, softver ili podaci koji su oštećeni

ESS QCA razvija i testira BC/DR planove u slučaju pojave prepoznatih rizika otkaza delova sistema ili sistema u celini.

Za sistem **ESS QCA** određen je MAD i RTO sa minimalnim vrednostima od 2 sata, odnosno sat i 30 minuta respektivno.

BC planovi se primarno zasnivaju na obezbeđenim HA konfiguracijama HSM, mrežnih i računarskih resursa, toplim i hladnim rezervama svih komponenti računarskog sistema.

Osnovni BC scenario zamene oštećenog uređaja predstavlja njegov HA par.

U slučaju oštećenja podataka realizuju se procedure povratka poslednje ispravne verzije iz backup-a sačuvanih na eksternim zaštićeni medijumima ili namenskim backup repozitorijumima.

DR lokacija **ESS QCA** nalazi se u ZDC, Tehnološki park, Vršac.

5.7.3. Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika

U slučaju kompromitacije privatnog ključa korisnika vrši se opoziv kompromitovanog kvalifikovanog sertifikata i izdavanje novog sa novim parom ključeva.

U slučaju kompromitacije privatnog ključa CA tela vrši se opoziv svih izdatih sertifikata, zatim opoziv kompromitovanog sertifikata izdavajućeg tela, izdavanje novog sa novim parom ključeva i obeveštavanje nadležnog Ministarstva o promeni statusa sertifikata izdavajućeg tela.

5.7.4. Mogućnost kontinuiteta poslovanja nakon katastrofe

Plan oporavka od katastrofe baziran je na uspostavljanju kompromitovanih funkcija na centralnoj lokaciji **ESS QCA**.

DR plan je automatizovan u delu u kome se obezbeđuje kontinuitet izdavanja CRL u najraćem vremenskom periodu, a zatim i ostalih funkcija (opoziv, izdavanje) nakon stabilizacije rada sistema.

Za plan oporavka od katastrofe treniraju se nosioci uloga od poverenja i ovlašćenja. Plan oporavka se testira, 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:

1) Završetak rada RA tela;
2) Završetak rada CA tela (QCA) uz nastavak pružanja usluga suspenzije, opoziva i izdavanja CRL do isteka važenja svih aktivnih sertifikata;
3) Završetak rada CA tela (QCA) i prestanak pružanja usluga suspenzije i opoziva za izdate sertifikate.

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 uz nastavak pružanja usluga suspenzije, opoziva i izdavanja CRL do isteka važenja svih aktivnih 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 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 pružanja usluge suspenzije i opoziva 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 izdavajućih tela 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.
- Pristup operatera/administratora resursima **ESS QCA** autorizovan je za sledeće poslovne role:
    - osobe od poverenja (**ESS QCA** Administratori)
    - osobe od ovlašćenja (**ESS QCA** Operateri)
    - auditore (**ESS QCA** Audit).
- Pristup **ESS QCA** administratora se kontroliše pravilom dva čoveka,
- 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, a privatni podaci pretplatnika/korisnika kriptovani.
- Svi poslovni dokumenti koji se razmenjuju u procesima **ESS QCA** 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 sledeći način:
    - potpunom blokadom internet saobraćaja,
    - zabranom instalacije i korišćenja email klijenata na svim računarskim resursima
    - standardnim windows antimalware rešenjem u cilju detekcije i prevencije unosa malware-a preko eksternih medijuma
    - redovnim osvežavanjem antimalware baze u cilju pravovremene detekcije pretnji u procesima patch-ovanja windows operativnog sistema
    - redovnim patch-ovanjem operativnih sistema računarskih resursa **ESS QCA**.
- Kritični elementi **ESS QCA** su zaštićeni mehanizmima backup-a. 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. Proces se realizuje korišćenjem automatizovanih mehanizama CI/CD.
- **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 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. 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 public cloud-u. Ovim je obezbeđena 99.99% dostupnost servisa na godišnjem nivou 24 sata, 7 dana u nedelji. Publikovani servisi obuhvataju: CRL, OCSP i servise provere statusa sertifikata, odnosno servise aktiviranja sertifikata. Podaci o izdatim sertifikatima se nalaze u bazama na matičnoj lokaciji **ESS QCA** u **ESS DMZ** mreži i ne prenose se na public cloud. Prenos podataka između **ESS QCA** i **ESS DMZ** realizuje se periodično od strane servisa **ESS QCA** koji podatke predaju autorizovanim 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 i Procedurom ceremonije podizanja **ESS QCA**, u prisustvu Rukovodioca sistema i minimalno tri nosioca uloga od poverenja.
- 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 za izdavanje sertifikata.

Asimetrični par ključeva na QSCD uređajima koji će poslužiti kao osnova za izdavanje kvalifikovanih sertifikata 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. Inicijalizovane kartice se evidentiraju u sistemu **ESS QCA**.
- Ukoliko se par ključeva za potrebe izdavanja kvalifikovanog sertifikata za elektronski pečat generiše na QSCD uređaju pretplatnika (HSM) van prostorija **ESS QCA**, ovaj proces se realizuje prema prethodno propisanoj proceduri ceremonije i uz obavezno prisustvo odgovornog lica **ESS QCA**. Dužina RSA ključa u inicijalizovanom kontejneru je minimalno 4096 bita.
- Javni i privatni ključ ostaju na inicijalizovanom kontejneru. Javni ključ će biti eksportovan iz kontejnera u procesu izdavanja kvalifikovanog sertifikata, odnosno u procesu formiranja CSR, ukoliko se radi o QSCD uređaju u vlasništvu pretplatnika.
- U toku korišćenja aplikacije loguju se sve akcije operatera.

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

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.

Pretplatnik/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 zaštićen transakcijom i do završetka procesa formiranja sertifikata nepoznat operaterima koji u procesu učestvuju.

U slučaju izdavanja kvalifikovanog sertifikata za elektronski pečat na QSCD uređaju pretplatnika, u procesu personalizacije koristi se javni ključ sa QSCD uređaja i identifikacioni podaci korisnika na osnovu kojih se formira CSR. CSR se upload-uje korišćenjem web interfejsa i šalje u RA telo gde se proverava, odobrava i dalje standardnim kanalima šalje u CA telo na izdavanje.

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 svojim javno dostupnim repozitorijumima https://qca.e-smartsys.com, https://essqca.e-smartsys.com, ldap://ldap.qca.e-smartsys.rs.

6.1.5. Dužine ključeva

Dužine ključeva su implementirane prema zahtevima **CP**, poglavlje 6.3. Drugi aspekti 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, odnosno eIDAS sertifikovani.

ESS QCA će izvršiti izmenu kombinacija algoritama i dužina ključeva koje koristi u procesu izdavanja kvalifikovanih sertifikata 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 tela imaju namenu ključa za Certificate Signing, Off-line CRL Signing, CRL Signing.

OCSP ima namenu ključa za OCSP Signing.

Kvalifikovani sertifikat 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 izdavajućih 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 backup 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.

Asimetrični par ključeva OCSP servisa:

OCSP servisi se publikuju na public cloud-u, a sertifikati i privatni ključevi servisa se čuvaju u zaštićenim bazama podataka **ESS QCA** DMZ. U cilju zaštite kompromitacije ključeva ovih sertifikata primenjeno je sledeće:

- obavezna aktivacija ključa lozinkom prilikom formiranja response-a
- reizdavanje sertifikata u periodu ne dužem od 6 meseci.

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 Zoni visoke bezbednosti u koju je ulaz zaštićen kontrolom pristupa.
- PED ključevi su klasifikovani prema rolama čije se odgovornosti ne preklapaju.
- Pristup HSM uređaju se autorizuje korišćenjem PIN PED interfejsa i personalnih PED ključeva dodeljenih nosiocima uloga od poverenja.
- Pinovi za pristup PED ključevima poznati su samo vlasnicima PED ključeva.

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

- Javni ključ para asimetričnih ključeva generisan za korisnika ne napušta QSCD sve do otpočinjanja procesa personalizacije.
- U procesu personalizacije javni ključ se iščitava iz kontejnera i u zatvorenoj transakciji kojom upravlja CA operater, 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 operatera.

Zaštita para ključeva na QSCD uređaju pretplatnika regulisana je pretplatničkim ugovorom i obavezama preuzetim u toku ceremonije generisanja, a odnose se na:

- Zabranu korišćenja istog para ključeva za generisanje CSR za drugi sertifikat u roku trajanja kvalifikovanog sertifikata za elektronski pečat **ESS QCA**
- Zabranu reizdavanja sertifikata nad istim parom ključeva po isteku važenja kvalifikovanog sertifikata za elektronski pečat **ESS QCA**.

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 osobe od poverenja ovlašćene 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 realizuje se u toku procedure ceremonije podizanja i u procesu zanavljanja sertifikata izdavajućih CA tela.

Backup privatnog ključa kvalifikovanog sertifikata 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 se ne radi.

6.2.6. Transfer privatnog ključa na hardverski kriptografski modul

Privatni ključevi **ESS QCA** CA tela se generišu na namenskim HSM uređajima. Transfer privatnog ključa **ESS QCA** tela na druge hardverske kriptografske module nije podržan.

Privatni ključ kvalifikovanog sertifikata se generiše na QSCD uređaju. Transfer privatnog ključa na QSCD nije podržan.

6.2.7. Čuvanje privatnog ključa na hardverskom kriptografskom modulu

Na HSM uređajima čuvaju se privatni ključevi **ESS QCA** *Root* i *Issuing* CA tela.

6.2.8. Metoda aktivacije privatnog ključa

Osobe od poverenja su autorizovane da u skladu sa procedurom u kojoj je neophodno prisustvo 2 od 4, korišćenjem PED uređaja, aktiviraju privatni ključ *ESS RQCA, ESS RQCA V3, ESS IQCA1, ESS IQCA1 V3, ESS IQCA2 V3 CA* tela.

Za QSCD uređaje unošenje PIN-a omogućava korišćenje privatnog ključa.

6.2.9. Metoda deaktivacije privatnog ključa

Privatni ključevi sačuvani na HSM uređajima se automatski deaktiviraju u slučaju bilo kakve promene u radu sistema ili fizičke promene u okruženju u odnosu na trenutak kada su aktivirani.

Privatni ključevi QSCD uređaja se automatski deaktiviraju neposredno posle izvršene operacije potpisivanja.

6.2.10. Metoda uništenja privatnog ključa

Privatni ključevi CA tela koji se čuvaju na HSM uređajima se uništavaju po isteku sertifikata izdatih na javni ključ u skladu sa propisanom procedurom proizvođača uređaja. Privatni ključevi QSCD se ne uništavaju.

6.2.11. Rangiranje kriptografskih hardverskih modula

Nije primenljivo.

6.3. Drugi aspekti upravljanja parom ključeva

6.3.1. Arhiviranje javnih ključeva

ESS RQCA V3, ESS IQCA1 V3, ESS IQCA2 V3 arhiviraju javne ključeve zajedno sa pridruženim sertifikatima u elektronskoj arhivi ESS QCA, gde se isti trajno čuvaju.

Javni ključevi i kvalifikovani sertifikati arhiviraju se u **ESS QCA** i izlučuju po isteku 10 godina od datuma prestanka važenja sertifikata u skladu sa Zakonom.

6.3.2. Periodi validnosti sertifikata i privatnog ključa

Vreme validnosti *ESS QCA Root* CA elektronskog sertifikata je 20 (dvadeset) godina.

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

Vreme validnosti kvalifikovanog sertifikata 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 ili u procesu zanavljanja sertifikata CA tela.

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

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

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

6.4.2. Zaštita podataka za aktiviranje

Osobe od poverenja su dužne 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 PIN-a 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.

6.5. Bezbednosne kontrole računara

U skladu sa **CP** implementirani su odgovarajući baseline bezbednosnih kontrola prema klasifikaciji za pet različitih bezbednosnih zona.

Za opisane zone formirano je trinaest (13) bezbednosnih profila računarskih resursa na koje se mogu primeniti specifične bezbednosne konfiguracije. 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 operativnog sistema
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 zona 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 public 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 proveravaju backup-i sistema **ESS QCA**
12) QCA-BP-12 – Profil bezbednosti za resurse na kojima se čuvaju elektronske arhive i 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 sistema upravljanja bezbednošću informacija E-Smart Systems d.o.o. Beograd i detaljno su opisani u politikama, procedurama i uputstvima ovog sistema.

6.7. Mrežne bezbednosne kontrole

U skladu sa **CP** implementirane su odgovarajuće mrežne bezbednosne kontrole u skladu sa zahtevima Zakona, međunarodne regulative i standarda. Kontrole zaštite na mrežnom nivou deo su šireg sistema upravljanja bezbednošću informacija E-Smart Systems d.o.o. Beograd i detaljno su opisani u politikama, procedurama i uputstvima ovog sistema.

6.8. Vremenski pečat

Vremenski pečat je implementiran u skladu sa zahtevima **CP**.

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 izdavanje kvalifikovanih sertifikata za elektronski potpis,
- *Issuing* CA telo za izdavanje kvalifikovanih sertifikata za elektronski pečat,
- Kvalifikovani sertifikat za elektronski potpis,
- Kvalifikovani sertifikat za elektronski pečat,
- Sertifikat za OCSP servise.

7.1.1. *Root* CA telo

Polja Verzije1	Vrednost
Version	V3
Serial number	32 hex karaktera
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
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
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 20 godina
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
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	Policy Identifier=All issuance policies, All application policies
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

7.1.2. *Issuing* CA telo za izdavanje kvalifikovanih sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Polja Verzije1	Vrednost
Version	V3
Serial number	32 hex karaktera
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
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
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 10 godina
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
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=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	putanje do CRL *Root* CA na https://qca.e-smartsys.com/pki/ESS RQCA V3.crl https://qca.e-smartsys.rs/pki/ESS RQCA V3.crl ldap://ldap.qca.e-smartsys.rs/ESS RQCA V3?certificateRevocationList;binary
Authority Information Access	https putanje do fajla *Root* CA sertifikata na repozitorijumima https://qca.e-smartsys.com/pki/ESS RQCA V3.cer https://qca.e-smartsys.rs/pki/ESS RQCA V3.cer
Subject Alternative Name	Nema

7.1.3. *Issuing* CA telo za izdavanje kvalifikovanih sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Polja Verzije1	Vrednost
Version	V3
Serial number	32 hex karaktera
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
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
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 10 godina
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
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=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	putanje do CRL *Root* CA na https://qca.e-smartsys.com/pki/ESS RQCA V3.crl https://qca.e-smartsys.rs/pki/ESS RQCA V3.crl ldap://ldap.qca.e-smartsys.rs/ESS RQCA V3?certificateRevocationList;binary
Authority Information Access	https putanje do fajla *Root* CA sertifikata na repozitorijumima https://qca.e-smartsys.com/pki/ESS RQCA V3.cer https://qca.e-smartsys.rs/pki/ESS RQCA V3.cer
Subject Alternative Name	Nema

7.1.4. Kvalifikovani sertifikat za elektronski potpis za korisnike (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Kvalifikovani sertifikat za elektronski potpis za fizičko lice koje je pripadnik pravnog lica izdat na osnovu identifikacionog dokumenta izdatog od strane Republike Srbije

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)	32 hex karaktera
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 11 9 312 (7.3)	RSASSA-PSS
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha512
Issuer	ETSI EN 319 412-2 (4.2.3.1)	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
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|EBS},] 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 https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.pdf

Certificate Policies	Pravilnik (član 15.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.1731.1.3.1 Policy Qualifier Id=CPS Qualifier: https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.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)	putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA1 V3?certificateRevocationList;binary
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	https putanje do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA1V3

Kvalifikovani sertifikat za elektronski potpis za fizičko lice izdat na osnovu identifikacionog dokumenta izdatog od strane Republike Srbije

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)	32 hex karaktera
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	RSASSA-PSS
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha512
Issuer	ETSI EN 319 412-2 (4.2.3.1)	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
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|EBS},] 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: 1.3.6.1.4.1.30496.1731.1.3.1 Policy Qualifier Id=CPS Qualifier: https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.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

		https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.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)	putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA1 V3?certificateRevocationList;binary
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	https putanje do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA1V3
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-stranog državljanina 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)	32 hex karaktera
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	RSASSA-PSS
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha512
Issuer	ETSI EN 319 412-2 (4.2.3.1)	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
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}, 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}, [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: 1.3.6.1.4.1.30496.1731.1.3.1 Policy Qualifier Id=CPS Qualifier: https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.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 https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.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)	https putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA1 V3?certificateRevocationList;binary
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	https putanje do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA1V3
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 -stranog državljanina 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)	32 hex karaktera
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	RSASSA-PSS
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha512
Issuer	ETSI EN 319 412-2 (4.2.3.1)	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
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: 1.3.6.1.4.1.30496.1731.1.3.1 Policy Qualifier Id=CPS Qualifier: https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.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 https://qca.e-smartsys.com/doc_3/ESS_QCA_CPS.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)	putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA1 V3?certificateRevocationList;binary
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	https putanje do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA1V3
Subject Alternative Name	ETSI EN 319 412-2 (4.3.2) Pravilnik (član 14.)	RFC822 Name={email adresa}

7.1.5. Kvalifikovani sertifikat za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Kvalifikovani sertifikat za elektronski pečat izdat na pravno lice

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)	32 hex karaktera
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 11 9 312 (7.3)	RSASSA-PSS
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha512
Issuer	ETSI EN 319 412-2 (4.2.3.1)	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
Valid from		UTC datum i vreme
Valid to		UTC datum i vreme
Subject	ETSI EN 319 412-3 (4.2.4) Pravilnik (član 18.) C – stav 1, tačka 1 O – stav 1, tačka 2 CN – stav 1, tačka 3 Pravilnik (član 19.) 2.5.4.97 Pravilnik (član 19.) SERIALNUMBER (CA:RS)	CN={naziv pravnog lica}{redni broj} ESSQCA, O={naziv pravnog lica}, [L={sedište pravnog lica},]i 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
Public key	ETSI TS 119 312 RFC 5280 (4.1.2.7)	2048 bits
Polja Ekstenzije	**Zahtev**	**Vrednost**
Key Usage	ETSI EN 319 412-3 (4.3.1) Pravilnik (član 24.)	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage		Nema
Qualified Certificate Statements	Pravilnik (član 25.) 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) 0.4.0.1862.1.6.2 (eseal) 1.3.6.1.5.5.7.11.2 (QC Statement 2) 0.4.0.194121.1.2 https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.pdf
Certificate Policies	Pravilnik (član 24.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.1731.1.3.2 Policy Qualifier Id=CPS Qualifier: https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.pdf Policy Identifier: 0.4.0.194112.1.3

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)	putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA2 V3?certificateRevocationList;binary
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	https putanja do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA2V3

Kvalifikovani sertifikat za elektronski pečat koji je izdat za organizacionu jedinicu unutar pravnog lica

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)	32 hex karaktera
Signature algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 11 9 312 (7.3)	RSASSA-PSS
Signature hash algorithm	ETSI EN 319 412-2 (4.2.2), ETSI TS 119 312 (7.3)	sha512
Issuer	ETSI EN 319 412-2 (4.2.3.1)	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
Valid from		UTC datum i vreme
Valid to		UTC datum i vreme
Subject	ETSI EN 319 412-3 (4.2.4) Pravilnik (član 18.) C – stav 1, tačka 1 O – stav 1, tačka 2 CN – stav 1, tačka 3 Pravilnik (član 19.) 2.5.4.97 Pravilnik (član 19.) SERIALNUMBER (CA:RS)	CN={naziv pravnog lica} {naziv organizacione jedinice} {redni broj} ESSQCA, O={naziv pravnog lica}, OU={naziv organizacione jedinice}, [L={sedište pravnog lica},] 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
Public key	ETSI TS 119 312 RFC 5280 (4.1.2.7)	2048 bits

Polja Ekstenzije	Zahtev	Vrednost
Key Usage	ETSI EN 319 412-3 (4.3.1) Pravilnik (član 24.)	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage		Nema
Qualified Certificate Statements	Pravilnik (član 25.) 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) 0.4.0.1862.1.6.2 (eseal) 1.3.6.1.5.5.7.11.2 (QC Statement 2) 0.4.0.194121.1.2 https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.pdf
Certificate Policies	Pravilnik (član 24.) ETSI EN 319 412-2 (4.3.3)	Policy Identifier: 1.3.6.1.4.1.30496.1731.1.3.2 Policy Qualifier Id=CPS Qualifier: https://qca.e-smartsys.com/docs_3/ESS_QCA_CPS.pdf Policy Identifier: 0.4.0.194112.1.3
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)	putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA2 V3?certificateRevocationList;binary
Authority Information Access	ETSI EN 319 412-2 (4.4.1)	https putanja do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA2V3

7.1.6. Sertifikat za timestamp servis

Polja Verzije1	Vrednost
Version	V3
Serial number	32 hex karaktera
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
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
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 5 godina
Subject	CN= ESS QCA V3 TS, 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
Public key	4096 bits
Polja Ekstenzije	**Vrednost**
Key Usage (Critical)	Digital Signature (80)
Enhanced Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)
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	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a
CRL Distribution Points	putanje do CRL *Issuing* CA na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.crl https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.crl ldap://ldap.qca.e-smartsys.rs/ESS IQCA2 V3?certificateRevocationList;binary
Authority Information Access	https putanja do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.cer i OCSP servisa https://qca.e-smartsys.com/ocsp/ESSIQCA2V3
Subject Alternative Name	DNS Name=qca.e-smartsys.com

7.2. CRL profil

ESS QCA izdaje CRL verzije 2 u skladu sa RFC 5280 i zahtevima ETSI EN 411-1 6.3.10.

Opozvani sertifikati su upisani u CRL. Status opozvanog sertifikata može se dodatno proveriti na site-u https://essqca.e-smartsys.com/status.

7.2.1. Profil *Root* CRL

Polja	Vrednost
Version	V2
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
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
Effective date	UTC datum i vreme
Next update	UTC datum i vreme + 26 nedelja
Polja ekstenzije	**Vrednost**
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuje CRL listu
Revoked certificates	Serial number UTC datum i vreme opoziva razlog opoziva

7.2.2. Profil *Issuing* CRL sertifikata za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Polja	Vrednost
Version	V2
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
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
Effective date	UTC datum i vreme
Next update	UTC datum i vreme + 27 sati
Polja ekstenzije	**Vrednost**
CRL Number	Redni broj
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuje CRL listu
Next CRL Publish	UTC datum i vreme + 24 sata
Revoked certificates	Serial number UTC datum i vreme opoziva razlog opoziva

7.2.3. Profil *Issuing* CRL liste sertifikata za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Polja	Vrednost
Version	V2
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
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
Effective date	UTC datum i vreme
Next update	UTC datum i vreme + 27 sati
Polja ekstenzije	**Vrednost**
CRL Number	Redni broj
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuje CRL listu
Next CRL Publish	UTC datum i vreme + 24 sata
Revoked certificates	Serial number UTC datum i vreme opoziva Razlog opoziva

7.3. OCSP profil

Sertifikate za OCSP servise prema OCSP profilu izdaju izdavajuća **ESS QCA**.

7.3.1. OCSP profil za kvalifikovane sertifikate za elektronski potpis (OID 1.3.6.1.4.1.30496.1731.1.3.1)

Polja Verzije1	Vrednost
Version	V3
Serial number	32 hex karaktera
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
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
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 6 meseci
Subject	CN= ESS IQCA1 V3 OCSP, 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
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	https putanje do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA1 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA1 V3.cer
Subject Alternative Name	DNS Name=qcaapp.e-smartsys.com

7.3.2. OCSP profil za kvalifikovane sertifikate za elektronski pečat (OID 1.3.6.1.4.1.30496.1731.1.3.2)

Polja Verzije1	Vrednost
Version	V3
Serial number	32 hex karaktera
Signature algorithm	RSASSA-PSS
Signature hash algorithm	sha512
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
Valid from	UTC datum i vreme
Valid to	UTC datum i vreme + 6 meseci
Subject	CN= ESS IQCA2 V3 OCSP, 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
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	https putanje do fajla *Issuing* CA sertifikata na https://qca.e-smartsys.com/pki/ESS IQCA2 V3.cer https://qca.e-smartsys.rs/pki/ESS IQCA2 V3.cer
Subject Alternative Name	DNS Name=qcaapp.e-smartsys.com

8. Audit usaglašenosti i druge provere

ESS QCA obezbeđuje periodičnu proveru/audit usaglašenosti, uključujući ove **CPS** 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 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 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 usaglašenosti sa zahtevima Zakona i odgovarajućih podzakonskih akata.

9. Drugi poslovni i pravni aspekti

9.1. Cene

9.1.1. Cene izdavanja ili obnove sertifikata

ESS QCA naplaćuje izdavanje/obnovu kvalifikovanih sertifikata.

Objavljivanje važećih cena sertifikata i drugih usluga od poverenja vrši se putem site-a https://essqca.e-smartsys.com/cenovnik, 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 i OCSP).

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 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

9.3.1. Opseg poverljivih informacija

ESS QCA postupa poverljivo sa sledećim podacima:

- sa svim zahtevima za dobijanje kvalifikovanog sertifikata,
- 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. 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 **CP** 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 podataka o ličnosti sprovodi se na početku procesa izdavanja kada se pretplatnik/korisnik upoznaje sa uslovima navedenim u *Politici privatnosti i zaštite podataka o ličnosti* sa kojima se saglašava.

9.4.6. Otkrivanje informacija shodno pravnim i administrativnim procesima

ESS QCA ne objavljuje, niti se zahteva da objavljuje podatke o ličnosti bez autorizovanog 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 pretplatnika/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 site-ovima, 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. Ograničenje odgovornosti

Ograničenja odgovornosti su definisana u **CP** i *Opštim uslovima za pružanje usluga od poverenja*.

9.9. Odštete

Za štetu nastalu upotrebom kvalifikovanog sertifikata 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.

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 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 site-a https://essqca.e-smartsys.com i o tome se obaveštava nadležno Ministarstvo.

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

9.10.2. Kraj validnosti

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

9.10.3. Efekat završetka i ponovnog rada

Prilikom donošenja novog **CPS**, svi kvalifikovani sertifikati 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 site-u https://essqca.e-smartsys.com i navedeni u poglavlju *1.3.1* ovih **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 pretplatnika/korisnika putem email-a.

ESS QCA obaveštava nadležno Ministarstvo o svakom narušavanju bezbednosti ili gubitku integriteta usluge izdavanja kvalifikovanog 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

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 ovih **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 pretplatnika/korisnika jer ne utiču na njihovo buduće korišćenje usluge koju im **ESS QCA** obezbeđuje. Sve ispravke koje ne menjaju uslove izdavanja i/ili korišćenja kvalifikovanih sertifikata 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 online 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(u) na site-u https://essqca.e-smartsys.com/dokumentacija.

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 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 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 kvalifikovane sertifikate izdate od strane **ESS QCA** će biti procesuirane od strane odgovarajućeg suda u Srbiji.

9.15. Saglasnost sa primenjivim 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, odnosno pečat, 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 da uslovi pod kojima je Ugovor potpisan važe 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 ovih 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 pretplatniku/korisniku 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
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	22.07.2025.	Ispravke u tački 4.10.
3.3	22.09.2025.	Manje izmene dokumenta

Potpisi:

Mirna Kojić Veljović ESUFL001372703191
Digitally signed by Mirna Kojić Veljović ESUFL001372703191
Date: 2025.09.24 01:54:08 +02'00'

Srećko Atanasković ESUFL001806469784
Digitally signed by Srećko Atanasković ESUFL001806469784
Date: 2025.09.24 09:28:59 +02'00'