Praktična Pravila Sertifikacije za izdavanje i upravljanje kvalifikovanim elektronskim sertifikatima

(CPS - Certificate Practice Statement)

OID Dokumenta (1.3.6.1.4.1.30496.509.1.2.1)

– verzija 1.8–

Beograd, april 2019.

Sadržaj

1. Uvod

E-Smart Systems d.o.o. Sertifikaciono telo (u daljem tekstu: **ESS QCA**) donosi Praktična Pravila koja se odnosi na izdavanje i upravljanje kvalifikovanim elektronskim sertifikatima od strane **ESS QCA** u skladu sa Zakonom o elektronskom potpisu i odgovarajućim podzakonskim aktima Republike Srbije (u daljem tekstu - **Zakon**).

ESS QCA izdaje kvalifikovane elektronske sertifikate korisnika u skladu sa dokumentima

- ETSI TS 101 862 V1.3.2 (2004-06) „Qualified Certificate Profile",
- RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile",
- RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" i
- ETSI TS 102 280 V1.1.1 (2004-03) „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons"

i sa obaveznim sadržajem definisanim u članu 17. Zakona o elektronskom potpisu.

1.1. Pregled

ESS QCA je odgovorno za pružanje kompletnih usluga sertifikacije, koje uključuju sledeće servise, i to:

- Registraciju korisnika,
- Formiranje asimetričnog para ključeva za korisnike,
- Formiranje kvalifikovanog elektronskog sertifikata,
- Distribuciju privatnog ključa i kvalifikovanih elektronskih sertifikata (SSCD) korisnicima na način u skladu sa Zakonom,
- Upravljanje procedurom opoziva i suspenzije kvalifikovanih elektronskih sertifikata
- Obezbeđivanje statusa opozvanosti kvalifikovanih elektronskih sertifikata.

ESS QCA obezbeđuje **sredstvo za formiranje kvalifikovanog elektronskog potpisa** (**SSCD**) i pridruženi PIN kod (za aktivaciju sredstva), kao i njihovu bezbednu distribuciju do korisnika. ESS QCA dodatno obezbeđuje jednokratni aktivacioni kod (JAK), podatak (za aktivaciju kvalifikovanog elektronskog sertifikata).

ESS QCA utvrđuje Opšta pravila pružanja usluge sertifikacije u skladu sa Zakonom koja korisnicima obezbeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga. **Opšta pravila ESS QCA** su ugrađena u dokumentima:

1. Politika Sertifikacije za pravna lica – (u daljem tekstu: **Politika Sertifikacije**) i
2. Praktična Pravila Sertifikacije (u daljem tekstu: **Praktična pravila**) ovaj dokument.

Politika sertifikacije i **Praktična pravila** su javni dokumenti. **Politika sertifikacije** definiše predmet rada sertifikacionog tela, dok **Praktična pravila** definišu procese i način njihovog korišćenja pri formiranju i upravljanju kvalifikovanim elektronskim sertifikatima. Opšta pravila funkcionisanja **ESS QCA** su u skladu sa dokumentima:

- RFC 3647 „Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework" i
- ETSI TS 101 456 v1.4.3 (2007-05) „Policy Requirements for Certification Authorities Issuing Qualified Certificates".

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 prilikom izdavanja i rukovanja elektronskim sertifikatima i kvalifikovanim elektronskim sertifikatima. **Interna** pravila su privatni dokument i predstavljaju poslovnu tajnu sertifikacionog tela. Interna pravila sadrže detalje o:

1. sistemu fizičke kontrole pristupa;
2. sistemu logičke kontrole pristupa;
3. sistemu za upravljanje ključevima;
4. sistemu distribuirane odgovornosti;
5. postupcima i radnjama u vanrednim situacijama.

ESS QCA je akreditovano od strane Nadležnog organa za poslove akreditacije i supervizije, prema Zakonu o elektronskom potpisu u Republici Srbiji (Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija) i biće predmet periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona o elektronskom potpisu i odgovarajućim podzakonskim aktima.

1.2. Ime dokumenta i identifikacija

Identifikacioni podaci ESS QCA su:

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

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

Ovaj dokument ima jedinstvenu oznaku - 1.3.6.1.4.1.30496.509.1.2.1
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) e-smart systems d.o.o. (30496) pki (509) ESS QCA (1) CPS (2) verzija (1)}

U svakom izdatom kvalifikovanom elektronskom sertifikatu od strane ESS IQCA1 u polju Certificate Policy stoji OID 1.3.6.1.4.1.30496.509.1.1.1 koji ukazuje da je sertifikat izdat po ovoj verziji politike sertifikacije za pravna lica. U polju Certificate Policy stoji i putanja do ove CPS.

1.3. Učesnici u PKI sistemu ESS QCA

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

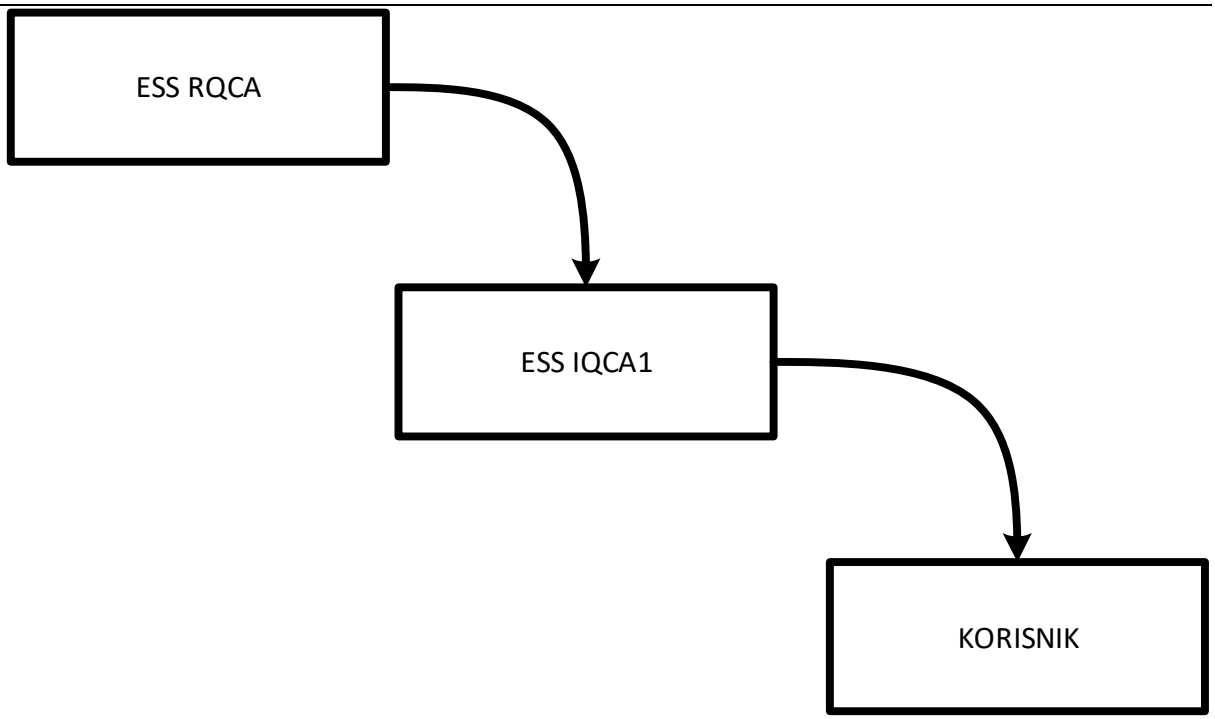
1.3.1. ESS QCA

ESS QCA je Sertifikaciono telo koja izdaje kvalifikovane elektronske sertifikate. **Politika sertifikacije (CP)** i **Praktična pravila (CPS)**, predstavljaju odgovarajuću politiku i pravila koja se primenjuju pri izdavanju i upravljanju kvalifikovanih elektronskih sertifikata.

U cilju objavljivanja trećim stranama informacija koje se odnose na opozvane i suspendovane sertifikate, vrši se odgovarajuća publikacija liste opozvanih sertifikata (CRL – Certificate Revocation List). ESS QCA periodično objavljuje takvu listu u skladu sa uslovima definisanim u ovom dokumentu.

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

- **ESS RQCA** – centralno samopotpisano sertifikaciono telo (***Root CA***) koje izdaje sertifikate podčinjenim Issuing sertifikacionim telima (***Issuing* CA**) i potpisuje svoju CRL listu.
- **ESS IQCA1** – podčinjeno sertifikaciono telo (***Issuing CA*)** od strane **ESS RQCA**, koje izdaje kvalifikovane elektronske sertifikate korisnicima, koje potpisuje svoju CRL listu.



Slika 1: Hijerarhijska struktura ESS QCA sistema

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

Obaveze ESS QCA

ESS QCA garantuje da će sprovodit sve procedure definisane ovom CPS. ESS QCA se obavezuje na:

1) Potpunu usaglašenost sa zvanično objavljenim CP i CPS
2) Regularno ažuriranje dokumenata CP i CPS i javno publikovanje
3) Objavljivanje kontakt detalja sertifikacionog autoriteta
4) Obezbeđivanje usluga sertifikacije u skladu sa Zakonom, Pravilnikom i ostalim podzakonskim aktima
5) Obezbeđivanje infrastrukture i sertifikacionih usluga, uključujući uspostavu i održavanje ESS QCA repozitorijuma i odgovarajućeg web sajta u cilju pružanja sertifikacionih usluga
6) Obezbeđivanje sigurnih mehanizama koji uključuju mehanizam generisanja ključeva, zaštite ključeva, kao i procedure deljenja tajni u skladu sa svojom sopstvenom PKI infrastrukturom
7) Obezbeđivanje obaveštavanja u slučaju kompromitacije sopstvenog privatnog ključa
8) Bezbedno generisanje ključeva na SSCD uređajima za korisnike
9) Izdavanje elektronskih sertifikata u skladu sa CP i ovim CPS, kao i ispunjavanje sopstvenih preuzetih obaveza
10) Obaveštavanje korisnika da su sertifikati generisani za njih, kao i o načinu kako korisnici mogu da preuzmu sertifikate

11) Obaveštavanje aplikanta ukoliko ESS QCA nije sposobno da izvrši validaciju korisničke aplikacije za dobijanje sertifikata u skladu sa CP i ovim CPS
12) Nakon prijema validnog zahteva od strane RA koje radi u okviru ESS QCA mreže izdaje sertifikat u skladu sa CP i ovim CPS
13) Opoziv 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) Regularno i periodično objavljivanje liste opozvanih sertifikata, CRL liste, u skladu sa CP i ovim CPS koja je uvek dostupna svim zainteresovanim stranama
16) Obaveštavanje trećih strana o statusu sertifikata putem publikovanja CRL lista na ESS QCA online repozitorijumu
17) Dostavljanja kopije CP i ovih CPS, kao i ostalih primenjlivih dokumenata po zahtevu neke od strana

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

Odgovornosti ESS QCA

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

1) ESS QCA nije odgovorno za zaštitu privatnih ključeva korisnika namenjenih za kreiranje kvalifikovanog elektronskog potpisa po njihovom preuzimanju od strane korisnika.
2) ESS QCA nije odgovorno za neodgovarajuću proveru validnosti sertifikata od strane koja se pouzdaje u sertifikat izdat od strane ESS QCA
3) ESS QCA nije odgovorno za moguću zloupotrebu sertifikata koja je nastala usled neispunjavanja obaveza korisnika ili treće strane koja se pouzdaje u 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 izdavanjem sertifikata za korisnike **ESS QCA** se podnose na adresi središta ESS QCA tela ili na lokacijama udaljenih RA (Registration Authority), koje obavljaju ulogu Registracionih autoriteta tj. ESS QCA komunicira sa svojim korisnicima putem mreže registracionih tela (centralno RA i mreža RA).

Registraciona tela mogu biti:

- ESS QCA na centralnoj lokaciji, kao **centralno RA**. Ovo RA telo nije ovlašćeno za rad sa pripremljenim SSCD 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 SSCD uređajima.

RA tela interaktivno komuniciraju sa pretplatnicima, aplikantima, korisnicima i ESS QCA u cilju isporuke sertifikacionih usluga. U tom smislu, registraciona tela ESS QCA:

- Prihvataju, analiziraju, potvrđuju ili odbijaju registraciju odgovarajućih zahteva za sertifikatima (aplikacije za sertifikate).
- Registruju pretplatnike i korisnike za korišćenje ESS QCA sertifikacionih usluga.
- Sprovode sve korake u proceduri identifikacije pretplatnika i korisnika u skladu sa Zakonom i Opštim pravilima rada ESS QCA.
- Koriste službene i overene dokumente u cilju provere korisničke aplikacije.
- Nakon potvrde aplikacije korisnika, obaveštavaju ESS QCA u cilju izdavanja 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 na broj 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 funckionalnim zahtevima.

RA obaveze

1) Prijem aplikacija za izdavanje kvalifikovanog elektronskog sertifikata u skladu sa CP i CPS.
2) Izvršavanje svih aktivnosti na verifikaciji i proveri autentičnosti aplikanata u skladu sa opisom ESS QCA procedura, CP i ovim CPS
3) Dostavljanje zahteva aplikanata do ESS QCA u elektronski potpisanoj poruci (zahtev za izdavanjem sertifikata), u skladu sa CP i CPS
4) Ukoliko je RA ovlašćen da raspolaže sa prethodno pripremljenim SSCD uređajima obaveza je upisa sertifikata na SSCD uređaj i štampa PIN koverte, kao i njihovo uručenje korisniku u skladu sa opštim pravilima
5) Zapisivanje svih aktivnosti u žurnalu događaja
6) Prijem, verifikaciju i prosleđivanje ka ESS QCA svih zahteva za opozivom i suspenzijom ESS QCA izdatih sertifikata u skladu sa ESS QCA procedurama, CP i CPS

ESS QCA preuzima odgovornost za poštovanje ove politike sertifikacije čak i kada je uloga registracionog tela poverena drugim licima na osnovu ugovora o poslovno tehničkoj saradnji. ESS QCA obebeđuje mehanizam da ostvari punu liniju odgovornosti u procesu izdavanja i upravljanja izdatim sertifikatima.

1.3.3. Pretplatnici

Pretplatnici su entiteti koji sa ESS QCA potpisuju ugovor za usluge izdavanja i upravljanja kvalifikovanim elektronskim sertifikatom koju pruža ESS QCA – pretplatnički ugovor. Saglasnost za idavanje kvalifikovanog elektronskog sertifikata podnosti pretplatnik koji reguliše i naknadu za izdavanje kvalifikovanog elektronskog sertifikata.

ESS QCA kao pretplatnike prihvata:

- Pravno lice,
- Preduzetnike,
- Državni organ,
- Organ teritorijalne autonomije,
- Organ lokalne samouprave.

Identifikacioni podaci pretplatnika se u izdatom kvalifikovanom elektronskom sertifikatu navode u atributu *organizationName*. Ovaj atribut omogućava trećim stranama da mogu identifikovati korisnika kao pripadnika entiteta pretplatnika.

Pretplatnički ugovor omogućava pretplatnicima da podnesu zahtev za opozivom ili suspenzijom korisnikovih kvalifikovanih elektronskih sertifikat u kojima je pretplatnikov identifikacioni podatak u atributu *organizationName*.

Obaveze pretplatnika

Pretplatnici sertifikacionih usluga ESS QCA su odgovorni za:

1) Poštovanje Politike sertifikacije (CP) i Praktičnih pravila rada (CPS) publikovanih od strane ESS QCA,
2) Obezbeđivanje tačnih informacija u njihovoj komunikaciji sa RA telima ESS QCA,
3) Upoznavanje, razumevanje i saglasnost sa svim stavovima i uslovima u CP i ovoj CPS, kao i drugim dokumentima koji su objavljeni na ESS QCA repozitorijumu,
4) Obaveštavanje RA tela o bilo kojim promenama informacija koje su ranije dostavljene,

1.3.4. Korisnici

Korisnik je fizičko lice, pripadnik entiteta pretplatnika, kome je izdat kvalifikovani elektronski sertifikat na osnovu zahteva za izdavanjem koji je podneo pretplatnik. Korisnici sa ESS QCA potpisuju ugovor za usluge izdavanja i upravljanja kvalifikovanim elektronskim sertifikatom koju pruža ESS QCA – korisnički ugovor.

Korisnički ugovor omogućava korisniku da podnese zahtev za opozivom, suspenzijom, aktivacijom svog kvalifikovanog elektronskog sertifikata ili deblokadom *PINa SSCD* uređaja.

Identifikacioni podaci korisnika se u izdatom kvalifikovanom elektronskom sertifikatu navode u atributu *commonName*.

Obaveze korisnika

Korisnici sertifikacionih usluga ESS QCA su odgovorni za:

1) Posedovanje odgovarajućih znanja i, ako je neophodno, pohađanje odgovarajuće obuke za korišćenje elektronskih sertifikata i sertifikacionih usluga,
2) Poštovanje Politike sertifikacije (CP) i Praktičnih pravila rada (CPS) publikovanih od strane ESS QCA,

3) Obezbeđivanje tačnih informacija u njihovoj komunikaciji sa RA telima ESS QCA,
4) Upoznavanje, razumevanje i saglasnost sa svim stavovima i uslovima u CP i ovoj CPS, kao i drugim dokumentima koji su objavljeni na ESS QCA repozitorijumu,
5) Uzdržavanje od narušavanja integriteta i proizvođenja neispravnim, sertifikata izdatog od strane ESS QCA,
6) Korišćenje ESS QCA sertifikata samo za legalne i autorizovane svrhe u skladu sa CP i CPS, kao i važećim zakonskim aktima,
7) Obaveštavanje RA tela o bilo kojim promenama informacija koje su ranije dostavljene,
8) Prekid korišćenja kvalifikovanog elektronskog sertifikata ukoliko je bilo koja informacija u sertifikatu postala nevalidna,
9) Prekid korišćenja kvalifikovanog elektronskog sertifikata ukoliko sam sertifikat postane nevalidan,
10) Uzdržanje od korišćenja svog privatnog ključa koji odgovara javnom ključu koji je sertifikovan od strane ESS QCA, u izdatom sertifikatu, pod istim imenom za potrebe izdavanja drugih sertifikata,
11) Sprečavanje kompromitacije, gubljenja, objavljivanja, modifikacije ili bilo kog drugog neautorizovanog korišćenja svog privatnog ključa,
12) Zahtevanje opoziva sertifikata u slučaju događaja koji materijalno utiče na integritet izdatog sertifikata od strane ESS QCA,
13) Prijavljivanje svake moguće zloupotrebe svog privatnog ključa i zahtevanje da se sertifikat opozove u tom slučaju.

1.3.5. Treće strane

Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koji prihvataju i verifikuju kvalifikovani elektronski potpis. Treće strane mogu da korisnika identifikuju kao pripadnika pretplatnika na osnovu atributa *organizationName* u telu kvalifikovanog elektronskog sertifikata. ESS QCA obezbeđuje pouzdanost u verodostojnost identifikacionih podataka korisnika i pretplatnika ukoliko je urađena verifikacija kvalifikovanog elektronskog sertifikata.

Verifikacija kvalifikovanog elektronskog potpisa obuhvata:

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

Obaveze trećih strana

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

1) Poseduje odgovarajuća znanja o korišćenju elektronskih sertifikata i drugih tehnologija vezanih za usluge sertifikacije
2) Upozna se sa Politikom sertifikacije (CP) i ovim Praktičnim pravilima rada (CPS) u vezi navedenih uslova koji važe za treće strane

3) Poštuje i sprovodi odredbe iz CP i ovih CPS
4) Verifikuje ESS QCA izdati sertifikat
    a. Proverom da je kompletan lanac sertifikata od *Root CA* sertifikata
    b. Proverom opozvanosti sertifikata u lancu
    c. Proverom da su svi sertifikati u lancu validni u vremenskom trenutku provere sertifikata
5) Proveri kompletnost podataka u sertifikatu izdatom od strane ESS QCA, kao i da proveri da li dati sertifikat služi odgovarajućoj oblasti primene koja je navedena u sertifikatu
6) Verifikuje kvalifikovani elektronski potpis
7) Razumno osloni i pouzda na ESS QCA izdati sertifikat u skladu sa odgovarajućim okolnostima

1.3.6. Ostali učesnici

To su proizvođači SSCD i HSM uređaja.

1.4. Korišćenje sertifikata

1.4.1. Prihvatljivo korišćenje sertifikata

U skladu sa Zakonom kvalifikovani elektronski sertifikat se koristi za verifikaciju kvalifikovanog elektronsog potpisa.

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

- Transakcije elektronskog poslovanja pravnih lica – kompanija,
- Elektronski ugovori,
- Pristup bezbednim web sajtovima (SSL autentikacija) i drugim on-line sadržajima,
- Elektronsko potpisivanje dokumenata,

1.4.2. Zabranjeno korišćenje sertifikata

Svaka druga upotreba kvalifikovanog elektronskog sertifikata koja nije propisana ovim dokumentom ili nije u saglasnosti sa odredbama Zakona o elektronskom potpisu i drugim dokumentima koji regulišu ovu oblast smatra se nedozvoljenom.

1.5. Administracija Praktičnih pravila sertifikacije

1.5.1. Organizacija administriranja Praktičnih pravila sertifikacije

ESS QCA je odgovorno za propisnu administraciju ove 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 osoba

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

1.5.3. Osoba koja određuje pogodnost CPS dokumenta

Osoba u ESS QCA, odgovorna za ovu CPS je:

Nenad Stanković
E-Smart Systems d.o.o.
Kneza Višeslava 70a
11030 Beograd
Srbija
tel: 011/3050236
fax: 011/3050222
email: nenad.stankovic@e-smartsys.com

1.5.4. Procedura odobravanja CPS dokumenta

Dokument se redovno periodično pregleda i vrše se izmene od strane odgovornog za ESS QCA sistem u kompaniji E-Smart Systems.

1.6. Definicije i skraćenice

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

Aplikacija za sertifikat – Zahtev poslat od strane lica koje zahteva sertifikat (aplikant) ka Sertifikacionom telu u cilju izdavanja elektronskog sertifikata.

Aplikant – fizičko lice koje je podnosilac zahteva za izdavanjem kvalifikovanog elektronskog sertifikata u vremenskom periodu do uručenja kada postaje korisnik.

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

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

Autentikacija – procedura provere deklarisanog identiteta pojedinca ili organizacije.

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

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

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

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

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

Elektronski sertifikat – elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.

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

Identifikacija – proces deklarisanja identiteta pojedinca ili pravnog lica.

Kvalifikovani elektronski potpis – Elektronski potpis koji se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa (SSCD – Secure Signature Creation Device) i koji se proverava putem

kvalifikovanog elektronskog sertifikata potpisnika (javnog ključa). Ovaj potpis je pravno ekvivalentan svojeručnom potpisu po Zakonu o elektronskom potpisu.

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

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

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

Politika sertifikacije – Imenovan skup pravila koji indicira primenljivost sertifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbednosnim zahtevima.

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

Praktična pravila – Javna Praktična pravila i procedure koje sertifikaciono telo primenjuje u proceduri izdavanja sertifikata.

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

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

Sertifikaciono telo – pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama Zakona o elektronskom potpisu.

Sredstva za formiranje kvalifikovanog elektronskog potpisa (SSCD) – sredstva za formiranje kvalifikovanog elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom o elektronskom potpisu.

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

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

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

Upravljanje sertifikatima – Aktivnosti pridružene upravljanju sertifikatima uključuju generisanje čuvanje, isporuku, objavljivanje i opoziv sertifikata.Skraćenice koje se koriste u ovom dokumentu:

CA (Certification Authority) - Sertifikaciono telo
CP (Certificate Policy) - Politika Sertifikacije
CPS (Certificate Practise Statement) - Praktična pravila
CRL (Certificate Revocation List) - Lista opozvanih sertifikata
ESS – E-Smart Systems
ETSI – European Telecommunication Standardization Institute
OID (Object Identifier) - jedistveni identifikator
PKI (Public Key Infrastructure) - Infrastruktura javnih ključeva
QCA – E-Smart Systems d.o.o. Sertifikaciono telo
RA (Registration Authority) - Registraciono telo
RFC – Request For Comments
SSCD (Secure Signature Creation Devices) - Sredstva za formiranje kvalifikovanog elektronskog potpisa

2. Odgovornosti za publikovanje i repozitorijume

2.1. Repozitorijum

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

ESS QCA na pomenutom on-line repozitorijumu objavljuje dokumenata o praktičnim pravilima i procedurama rada, uključujući CP kao i ovu CPS. ESS QCA zadržava pravo da učini raspoloživim i publikuje informacije u vezi sopstvenih politika i procedura rada pored navedenog i putem bilo kog drugog pogodnog načina.

2.2. Publikovanje informacija o sertifikatima

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

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

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

2.3. Vreme i frekvencija publikovanja

ESS QCA publikuje informacije o statusu opozvanosti izdatih elektronskih sertifikata (CRL liste), kao što je naznačeno i precizirano u ovom dokumentu.

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

2.4. Kontrole pristupa repozitorijumima

ESS QCA održava raspoloživim pristup do svog javnog repozitorijuma trećim stranama sa svrhom:

- Dobavljanja CA sertifikata ESS IQCA1 i ESS RQCA
- CRL liste ESS IQCA1 i ESS RQCA

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

3. Identifikacija i autentikacija korisnika

U ovom poglavlju su navedeni uslovi koje je neophodno ispuniti prilikom podnošenja zahteva za izdavanjem/opozivom/suspenzijom kvalifikovanog elektronskog sertifikata.

Uslovi se odnose na:

- Identifikaciju pretplatnika,
- Identifikaciju aplikanta, pripadnika entiteta pretplatnika,
- Identifikaciju korisnika

3.1. Nazivi

Identifikaconi podaci pretplatnika i aplikanta, pripadnika entiteta pretplatnika koji se ugrađuju u kvalifikovani elektronski sertifikat struktuirani su po X.500 *distinguished name* formi.

ESS QCA izdaje kvalifikovane elektronske sertifikate aplikantima. Pretplatnik dostavlja dokumentovane aplikacije koje sadrže nazive koji se mogu verifikovati (naziv i matični broj pretplatnika; ime, prezime i opcioni JMBG aplikanta). Ukoliko se na zahtevu navede da će se sertifikat koristiti za komunikaciju sa državom, onda se navodi JMBG u samom zahtevu i JMBG će se naći u izdatom kvalifikovanom elektronskom sertifikatu. U suprotnom JMBG se ne navodi u zahtevu i neće se naći u izdatom kvalifikovanom elektronskom sertifikatu.

Ograničenje za naziv pretplatnika u telu sertifikata je 45 karaktera i ni ne sme sadržati znak zareza (,). Pogodno je koristiti skraćeni naziv pravnog lica kao što je npr. naveden u APR obrascu.

ESS QCA ne izdaje anonimne sertifikate korisnicima.

U domenu ESS QCA imena pridružena korisnicima sertifikata su jedinstvena.

ESS QCA ne prihvata “trademark” oznake, loga ili druge grafičke ili tekstualne materijale koji su zaštićeni od kopiranja, a razmatrani su za uključenje u sertifikate.

3.2. Inicijalna provera identiteta

- Identifikacija pretplatnika. Od dostavljenih podataka proverava se naziv (skraćeni naziv u APR ako postoji) i matični broj. Konsultuju se baza podataka treće strane koje jednoznačno identifikuju pravno lice. Ne proveravuju su dostavljeni kontaktni podaci adresa, telefon i *e-mail*. Sa identifikovanim pretplatnikom se potpisuje ugovor o pružanju usluge izdavanja i upravljanja kvalifikovanim elektronskim sertifikatima od strane ESS QCA– pretplatnčki ugovor.
- Identifikovani pretplatnik dostavlja za svoje pripadnike aplikante – saglasnost za izdavanje kvalifikovanog elektronskog sertifikata.
- Aplikanti, pripadnici entiteta pretplatnika se uz lično prisustvo u registracionom telu i validnim identifikacionim dokumentom (lična karta ili pasoš) identifikuju. Proveravaju se identifikovani podaci sa podacima u dostavljenom ovlašćenju.

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

3.3. Identifikacija i autentikacija zahteva za obnavljanje ključeva

Ovo poglavlje nije primenljivo.

3.4. Identifikacija i autentikacija zahteva za opoziv sertifikata

Pretplatnik može da zahteva opoziv/suspenziju kvalifikovanih elektronskih sertifikata u kojima su njegovi identifikacioni podaci tako što će prijaviti promene u podatku kvalifikovanog elektronskog sertifikata. Zahtev, potpisan zakonskim zastupnikom pravnog lica, se dostavlja poštom ili elektronski (sa kvalifikovanim elektronskim potpisom) u RA telo.

Korisnik može da zahteva opoziv/suspenziju svog sertifikata. Zahtev se dostavlja elektronski (sa kvalifikovanim elektronskim potpisom) ili lično uz obaveznu identifikaciju korisnika identifikacionim dokumentom u RA telo.

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

Korisnik i pretplatnik se obaveštavaju nakon obrade zahteva za opoziv kvalifikovanog elektronskog sertfikata. Obrađen zahtev za opozivom/suspenzijom je vidljiv na CRL listi u roku od 24 sata po prijemu zahteva.

4. Operativni zahtevi u vezi životnog ciklusa sertifikata

Za ESS QCA, registraciona tela, pretplatnike, korisnike, ili druge učesnike postoji stalna obaveza da informišu ESS QCA o svim promenama u informacijama koje su objavljene u sertifikatu za čitav period važenja takvog sertifikata. Određene druge obaveze se takođe mogu dodatno uspostaviti.

4.1. Aplikacija za dobijanje sertifikata

Aplikanti su fizička lica pripadnici entiteta pretplatnika. Saglasnost za izdavanje kvalifikovanog elektronskog sertifikata dostavlja pretplatnik.

RA sprovodi proces identifikacije, autentikacije i registracije pretplatnika radi zaključenja pretplatničkog ugovora u cilju sprovođenja postupka podnošenja aplikacije za izdavanje kvalifikovanih elektronskih sertifikata koji zahteva:

- Popunjavanje forme saglasnosti,
- Dostavljanje neophodne dokumentacije,
- Potvrdu o uplati i
- Prihvatanje pretplatničkog ugovora.

Potrebni podaci forme saglasnosti za kvalifikovane elektronske sertifikate su:

1) Ime (podatak aplikanta)
2) Prezime (podatak aplikanta)
3) JMBG (ukoliko je sertifikat namenjen za rad sa Državnim organima) (podatak aplikanta)
4) Naziv organizacje (podatak pretplatnika)
5) Matični broj (podatak pretplatnika)
6) Poštanska adresa (podatak aplikanta)
7) Broj mobilnog telefona (podatak aplikanta)
8) E-mail adresa korisnika (podatak aplikanta)

Proces održavanja podataka o pretplatnicima realizuje se unutar RA tela i obuhvata kontinualnu proveru i ažuriranje podataka: zanavljanja dokumenata pravosnažne potvrde nadležnog organa o registraciji (Izvoda iz APR, …) i obrasca „Overenih potpisa lica ovlašćenih za zastupanje“.

Prijem saglasnosti za izdavanje kvalifikovanog elektronskog sertifikata u RA može da stigne u elektronskom ili papirnom obliku, ali isključivo u formi popunjenog propisanog obrasca overenog potpisom registrovanog zastupnika.

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

Nakon evidencije uplate RA operater šalje poruke aplikantima sa liste (koristeći podatke upisane u poljima e-mail i mobilni telefon) da dođu na lokaciju RA tela u cilju lične identifikacije.

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

- Elementi saglasnosti za izdavanje kvalifikovanog elektronskog sertifikata koji su definisani od strane pretplatnika (datum slanja, broj pod kojim je zaveden u poslovnom sistemu pravnog lica, zastupnik koji je poslao zahtevi i sl.),
- Rok za obavljanje identifikacije,
- Lokacije na kojima se mogu pročitati dokumenti Politike Sertifikacije i Praktičnih Pravila,
- Molba da sa sobom ponese ovaj poziv, s obzirom da je na taj način verifikovana ispravnost unete e-mail adrese.

4.2. Procesiranje aplikacije za dobijanje sertifikata

Aplikant pripadnik entiteta pretplatnika se javlja RA operateru koji vrši identifikaciju lica. Da bi se identifikacija smatrala uspešnom potrebno je da:

- Aplikant poseduje identifikacioni dokument koji po broju i vrsti odgovara dokumentu navedenom u saglasnosti
- Da podaci iz dokumenta zahteva (ime i prezime) odgovaraju podacima iz prezentiranog identifikacionog dokumenta
- Da se aplikant pojavio u roku važenja zahteva
- Da aplikant ima kod sebe e-mail poruke (na uvid)

Za uspešno identifikovanog aplikanta se unosi JMBG ukoliko se zahteva elektronski sertifikat za rad za državom, skeniraju i prilažu u informacioni sistem svi prezentovani dokumenti.

Po isteku roka važenja kompletnog zahteva, sve stavke zahteva za koje se nisu pojavili aplikanti da lično budu identifikovana biće automatski postavljen status Odbijen.

Ukoliko odbija zahtev RA operater mora da navede razlog odbijanja.

RA operater Struktuira podatke iz aplikacije u elektronski dokument. Samo ukoliko je RA operater ovlašćen da raspolaže sa prethodno pripremljenim SSCD uređajima, u elektronski dokument uključuje i asimetrični javni ključ sa jednog takvog SSCD uređaja. Kada se uspešno obrade svi koraci taj SSCD uređaj će biti uručen korisniku. RA operater stavlja kvalifikovani elektronski potpis na elektronski dokument i zaštićenim kanalom ga dostavlja u ESS QCA.

RA operater vrši obezbeđenje dokumentacije aplikacije koja je dostavljena (papirna i elektronska) od otuđenja i uništenja. Skenirane dokumente elektronski potpisuje koristeći privatni ključ svog kvalifikovanog elektronskog sertifikata.

Generisanje asimetričnog privatnog i javnog ključa na SSCD uređaju (pripremljen SSCD uređaj) se vrši samo u zaštićenim prostorijama ESS QCA. Ukoliko je RA telo ovlašćeno od strane ESS QCA da podnosi zahteve sa asimetričnim javnim ključem, pripremljen SSCD uređaj mu se dostavlja na bezbedan način.

Tehnički i bezbednosni detalji su opisani u internim pravilima rada.

4.3. Izdavanje sertifikata

Nakon dostave validnog elektronskog dokumenta za izdavanjem sertifikata, CA operater ESS QCA sprovodi proces izdavanja odgovarajućeg sertifikata koji se sastoji od:

- Verifikacije kvalifikovanog elektronskog potpisa RA operatera nad elektronskim dokumentom,
- Odobrenje ili odbijanje pojedinačnih zahteva iz elektronskog dokumenta,
- CA operater u elektronski dokument zahteva uključuje i asimetrični javni ključ sa pripremljenog SSCD uređaja i vrši izdavanje kvalifikovanog elektronskog sertifikata za odobrene zahteve iz elektronskog dokumenta u kojem nije postojao javni ključ,
- ESS QCA sistem obaveštava korisnika o tome da mu je sertifikat izdat i kako može da ga aktivira. Sertifikat se po izdavanju suspenduje zbog zaštite transporta, a korisnik obaveštava o jednokratnom aktivacionom kodu kvalifikovanog elektronskog sertifikata,
- CA operater upisuje na SSCD uređaj izdati kvalifikovani elektronski sertifikat ukoliko je u obradi zahteva radio sa pripremljenim SSCD uređajem. Ukoliko je RA dostavio zahtev sa javnim ključem dostavlja mu se izdati kvalifikovani elektronski sertifikat koji upisuje na SSCD uređaj.
- Obaveštavanje RA o statusu obrade prosleđenog zahteva.
- U RA se štampa aktivacioni kod SSCD uređaja na kovertu za PIN kod.

Postoje dva aktivaciona koda:

- Aktivacioni kod SSCD uređaja (PIN), kojim se pristupa asimetričnom privatnom ključu i
- Jednokratni aktivacioni kod (JAK) kvalifikovanog elektronskog sertifikata kojim korisnik preko on-line repozitorijumu http://qca.e-smartsys.com aktivira sertifikat nakon preuzimanja.

Tehnički i bezbednosni detalji su opisani u internim pravilima rada.

4.4. Prihvatanje sertifikata

Uručenje SSCD uređaja vrši se na jedan od dva načina:

- Kurirskom službom. Ako se SSCD uređaj dostavlja kurirskom službom on se lično uručuje korisniku, a koverta sa PIN kodom se šalje poštom.
- Lično preuzimanje. Ako korisnik lično preuzima SSCD uređaj, u prostorijama ESS QCA ili ovlašćenog RA tela za rad sa pripremljenim SSCD uređajima, i koverta sa PIN kodom mu se uručuje lično.

U oba slučaja korisnik prilikom preuzimanja SSCD uređaja potpisuje korisnički ugovor.

Samo za sertifikate za koje je izvršeno uručenje može se uraditi aktiviranje, tj. prekid suspenzije. Izdati sertifikat od strane ESS QCA se smatra prihvaćenim od strane korisnika ukoliko se ispunjen jedan od uslova:

- korisnik preko on-line repozitorijuma http://qca.e-smartsys.com aktivira sertifikat korišćenjem dva parametra:

  - jednokratni aktivacioni kod kvalifikovanog elektronskog sertifikata poslat direktni potpisniku
  - jedinstveni identifikator korisnika odštampan na SSCD uređaju koji je uručen
- Trideset (30) dana nakon izdavanja sertifikata ukoliko korisnik ne javi da postoje bilo kakvi problemi u izdatom sertifikatu. Ukoliko SSCD uređaj nije bio uručen u roku od 30 dana izdati elektronski sertifikat se opoziva po automatizmu.

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

RA operater obaveštava pretplatnika o status zahteva nakon obrade svih pojedinačnih stavki saglasnosti koji je podneo.

4.5. Korišćenje sertifikata i asimetričnog para ključa

U ovom poglavlju se definišu odgovornosti koje se odnose na korišćenje asimetričnog para ključeva i sertifikata, i to:

- Odgovornosti korisnika – korisnik se obavezuje da će koristiti privatni ključ i izgenerisani 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 korisnikovog ugovora sa CA. U tom smislu, korisnik može koristiti svoj privatni ključ samo nakon prihvatanja odgovarajućeg sertifikata. Takođe, korisnik mora prestati da koristi svoj privatni ključ nakon isticanja perioda validnosti ili opoziva izdatog sertifikata.
- Odgovornost treće strane – treća strana je obavezna da prihvata izdate sertifikate ESS sa predviđenim načinom korišćenja sertifikata definisanim u samom sertifikatu. Treća strana je obavezna da propisno i uspešno primenjuje operaciju javnog ključa koji ekstrahuje iz izdatog sertifikata i odgovorna je da sprovodi proveru statusa opozvanosti datog sertifikata korišćenjem metoda koji je definisan u CP i CPS dokumentima ESS QCA.

4.6. Obnavljanje sertifikata

Obnavljanje sertifikata se može uraditi samo ako je postojeći sertifikat validan i u periodu od 30 dana pre isteka aktivnog sertifikata.

Zakonom je predviđeno da se korisnik sertifikata lično identifikuje kao mera provere da su podaci koji se nalaze u sertifikatu i dalje validni. Zbog toga se primenjuje ista procedura kao i za inicijalno izdavanje sertifikata. Na zahtevu za idavanje sertifikata se navodi da je već registrovan da bi se koristio isti jedinstveni identifikator korisnika (JIK) u novom sertifikatu.

Obnovljeni sertfikat se izdaje na novom SSCD uređaju, sa novim asimetričnim parom ključeva i novim PIN kodom. ESS QCA sistem obaveštava korisnika o tome da mu je sertifikat izdat i kako može da ga aktivira. Aktiviranje sertifikata je isto kao kod redovnog izdavanja.

4.7. Generisanje novog para ključeva i sertifikata korisnika

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

Korisnik je već registrovan u okviru ESS QCA i poseduje jedinstveni identifikator korisnika (JIK). Na zahtevu za idavanje sertifikata se navodi da je već registrovan da bi se koristio isti JIK u novom sertifikatu.

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

4.8. Modifikacije sertifikata korisnika

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

4.9. Suspenzija i opoziv sertifikata

ESS QCA vrši opoziv izdatog elektronskog sertifikata u slučaju:

- Gubitka, krađe, modifikacije, objavljivanja ili neke druge kompromitacije privatnog ključa korisnika sertifikata,
- Da izvršenje odgovarajućih obaveza lica koja su navedena u ovoj CP kasni ili je sprečeno usled prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usled drugog uzroka koji izlazi van kontrole datog lica, i kao rezultat, informacije o drugom licu su materijalno ugrožene ili kompromitovane,
- Da se desila promena informacija koja su sadržane u sertifikatu datog lica,
- Na zahtev pretplatnika kada ukida pripadnost entitetu za korisnika.
- Na zahtev korisnika

ESS QCA vrši suspenziju izdatog elektronskog sertifikata u slučaju:

- Odmah nakon izdavanja kvalifikovanog elektronskog sertifikata isti se suspenduje (opisano u poglavlju 4.4),
- Odmah nakon izdavanja obnovljenog kvalifikovanog elektronskog sertifikata isti se suspenduje (opisano u poglavlju 4.6),
- Na zahtev korisnika, potpisnika ili nadzora ESS QCA ukoliko imaju sumnju u kompromitaciju privatnog ključa,
- Na zahtev pretplatnika kada privremeno ukida pripadnost entitetu za korisnika.

Proces opoziva kvalifikovanih elektronskih sertifikata može se inicirati iz sledećih izvora:

1. Overenim zahtevom pretplatnika koje je iniciralo izdavanje kvalifikovanog sertifikata za pripadnika entiteta,
2. RA operater u slučaju da sertifikat nije isporučen korisniku,

3. ESS QCA ukoliko je ustanovljen rizik od kompromitacije privatnog ključa za jedan ili više izdatih kvalifikovanih elektronskih sertifikata.

U prvom slučaju, po zakonu o elektronskom potpisu član 26. , korisnik je dužan da odmah zatraži opoziv svog sertifikata u svim slučajevima gubitka, oštećenja sredstva ili promena 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 informacionih elemenata koji su sadržani u identifikacionim podacima koje je korisnik dostavio do RA. RA operater je dužan da obradi i prosledi u CA u toku istog radnog dana u kojem je stigao zahtev. Ukoliko podaci iz zahteva nisu verodostojni, zahtev se odbija i o tome obaveštava kontakt lice korisnika i nadzor ESS QCA. CA Operater je dužan da u toku istog radnog dana obradi zahtev za opozivom i obavesti korisnika o opozivu.

U trećem slučaju, RA operater koji nije dobio potvrdu preuzimanja SSCD uređaja od strane aplikanta, na poslednji radni dan pre tridesetog dan od dana izdavanja elektronskog sertifikata, kreira zahtev za opozivom za ne uručeni elektronski sertifikat. Elektronski potpisuje zahtev i šalje ga u ESS QCA. CA Operater je dužan da proveri verodostojnost zahteva. CA Operater je dužan da u toku istog radnog dana obradi zahtev za opozivom i obavesti korisnika i podnosioca zahteva o opozivu. U slučaju nevalidnog zahteva obaveštava nadzor ESS QCA o nepravilnosti rada.

U četvrtom slučaju, ESS QCA sprovodi istrage na sve detektovane i prijavljene nepravilnosti u radu celog sistema. Na sve potvrđene nevalidnosti podnosi zahtev CA operaterima za opoziv jednog ili više elektronskih sertifikata. CA Operater je dužan da u toku istog radnog dana obradi podneti zahtev za opozivom i obavesti korisnika i pretplatnika o opozivu.

ESS QCA sprovodi nadzor rada celog sistema i izlaz su detektovane nepravilnosti. Detektovane nepravilnosti u slučaju kompromitacije jednog ili više elektronskih sertifikata povlače zahtev za opozivom istih.

ESS QCA sprovodi istragu na svaku prijavljenu nepravilnost. Prijavu nepravilnosti mogu uraditi službenici ESS QCA, službenici RA, pretplatnici, korisnici, ili treće strane. Prijavljena nepravilnost u slučaju kompromitacije jednog ili više elektronskih sertifikata povlače zahtev za opozivom istih.

U slučaju da je potrebno više od 24 sata da se potvrdi sumnja u kompromitciju prvatnog ključa, podnosi se zahtev za suspenzijom sertifikata u RA telo 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 isti radni dan po prijemu zahteva. Potvrdno obrađen zahtev isti radni dan podnosi u CA telo. CA operater validira i obrađuje zahtev isti radni dan.

Za vreme trajanja suspenzije podnosilac zahteva je dužan da ispita sumnju i ako je potvrdna sumnja podnese zahtev za opozivom. Ukoliko se u toku trajanja suspenzije ne podnese zahtev za opozivom, to znači da su sumnje neopravdane i elektronski sertifikat se vraća u stanje validnog.

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 treba da je duža od 30 dana, mora se koristi procedura opoziva.

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

4.10. Servisi provere statusa sertifikata

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

Lista opozvanih sertifikata (CRL) ESS IQCA1 se ažurira na svakih 24 sata, a CRL ESS RQCA na svakih 6 meseci. Treće strane moraju koristiti on-line repozitorijuma http://qca.e-smartsys.com ESS QCA da preuzmu CRL listu.

Tehnički i bezbednosni detalji su opisani u internim pravilima rada.

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 sertifikat.

Prestanak korišćenja sertifikata može biti iz sledećih razloga:

- Korisnik želi da prekine korišćenje sertifikacionih servisa ESS QCA.
- ESS QCA je prestalo sa pružanjem usluga sertifikacije.

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

Vremenski istekli opozvani kvalifikovani elektronski sertifikati se uklanjanju sa liste opozvanih elektronskih sertifikata.

4.12. Čuvanje i rekonstrukcija privatnog ključa korisnika

Asimetrični privatni ključ korisnika koji odgovara javnom ključu sadržanom u izdatom kvalifikovanom elektronskom sertifikatu se ne čuva i nalazi se samo na SSCD uređaju korisnika.

5. Upravne, operativne i fizičke bezbednosne kontrole

Ovo poglavlje opisuje sve bezbednosne kontrole koje koristi ESS QCA za obavljanje funkcija kreiranja para ključeva, provere zahteva, izdavanje sertifikata, opoziv sertifikata, provere/auditinga i arhiviranja.

ESS QCA planira i izvodi sve bezbednosne mere u skladu sa standardom ISO/IEC 27001.

5.1. Fizičke bezbednosne kontrole

ESS QCA zahteva i implemetira fizičke bezbednosne kontrole na svim lokacijama na kojima se obavlja bilo koji deo rada.

Detaljan opis primenjenih kontrola opisan je u internim pravilima vezanim za fizičke bezbednosne kontrole.

5.1.1. Lokacija i zgrada

Oprema ESS QCA nalazi se u posebnim prostorijama koje odgovaraju potrebama izvršenja operacija visoke bezbednosti.

5.1.2. Fizički pristup

Fizički pristup je ograničen implementacijom odgovarajućih mehanizama kontrole pristupa u i iz zone bezbednosti, kao i u i iz zone visoke bezbednosti.

- zone bezbednosti (zona rada sa bezbednosnim parametrima SSCD),
- zone visoke bezbednosti (zona generisanja kvalifikovanog elektronskog sertifikata).

U zoni bezbednosti SSCD uređaji se klasifikuju na Neinicijalizovane (fabrički SSCD), Inicijalizovane (pripremljen SSCD), Personalizovane (obrađen SSCD) i Škart (sa greškom). Tehnički i bezbednosni detalji rada sa SSCD uređajima je opisan u internim pravilima.

5.1.3. Električno napajanje i klimatizacija

Napajanje i ventilacija se izvršavaju sa redundansom.

5.1.4. Izloženost poplavama

Prostorije ESS QCA su zaštićene od poplava.

5.1.5. Prevencija i zaštita od požara

Prevencija i zaštita od požara su implementirane.

5.1.6. Medijumi za čuvanje podataka

Medijumi se čuvaju u fizički obezbeđenom prostroru.

5.1.7. Odlaganje smeća

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

5.1.8. Odlaganje rezervnih kopija

Backup medijumi čuvaju se na odvojenoj lokaciji koja je fizički obezbeđena i zaštićena od požara i poplava. Detaljano opisano u internim pravilima.

5.2. Proceduralne kontrole

ESS QCA sprovodi kadrovsku i upravnu praksu koja obezbeđuje razumnu sigurnost u poverljivost i kompetenciju zaposlenih u domenu tehnologija koje se odnose na elektronski potpis i PKI sisteme.

5.2.1. Poverljive uloge

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

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

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

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

- RA operater i
- CA operater.

5.2.2. Broj osoba koje se zahtevaju po svakom zadatku

Tamo gde se zahteva dualna kontrola, potrebno je da najmanje dva od ukupno četiri zaposlena ESS QCA na poverljivim dužnostima iskažu njihova podeljena znanja u cilju omogućavanja izvršenja tekućih operacija. U operativnom radu sa korisnicima ESS QCA potrebno je da se koriste obe ovlašćene dužnosti iskazivanjem njihovih znanja u cilju omogućavanja izvršenja tekućih operacija. Svaka poverljiva ili ovlašćena dužnost definiše odgovarajuće zahteve u pogledu identifikacije i autentikacije.

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.
- Izdavanje kvalifikovanog elektronskog sertifikata na SSCD uređaju,
- Opoziv kvalifikovanog elektronskog sertifikata,
- Štampa PIN koverte.

Tehnički i bezbednosni detalji su opisani u internim pravilima rada.

5.2.3. Identifikacija i autentikacija za svaku ulogu

Svaka poverljiva ili ovlašćena dužnost definiše odgovarajuće zahteve u pogledu identifikacije i autentikacije. Detaljnije opisano u internim pravilima.

5.2.4. Uloge koje zahtevaju razdvajanje dužnosti

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

5.3. Kadrovske bezbednosne kontrole

5.3.1. Kvalifikacija i iskustvo

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

- Da ne postoje kriminalne osude za ozbiljne zločine,
- Da ne postoje pogrešne prezentacije informacija od strane kandidata,
- Da postoje odgovarajuće reference.

ESS QCA zahteva da su zaposleni članovi E-Smart Systems d.o.o. na poverljivim dužnostima minimum jednu godinu zaposleni i da imaju potpisan ugovor o neotkrivanju poverljivh informacija (NDA). ESS QCA zahteva da zaposleni na osetljivim dužnostima imaju potpisan ugovor o neotkrivanju poverljivh informacija (NDA).

5.3.2. Procedura provere biografije

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

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

5.3.4. Ponovna obuka

Periodično ažuriranje obuke i doobuka zaposlenih radi se u cilju uspostave kontinuiteta i ažurnosti znanja zaposlenih, kao i odgovarajućih procedura.

5.3.5. Rotacija poslova

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

5.3.6. Kaznene mere u odnosu na zaposlene

ESS QCA ima odgovarajuće mere za kažnjavanje zaposlenih za neovlašćene aktivnosti, neovlašćeno korišćenje autoriteta, kao i neovlašćeno korišćenje sistema u cilju sprovođenja sankcija za određeno neposlovno i rizično ponašanje, koje može biti različito u zavisnosti od različitih okolnosti.

5.3.7. Kontrole nezavisnih ugovarača

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

5.3.8. Dokumentacija za inicijalnu obuku i ponovnu obuku

ESS QCA čini dostupnom dokumentaciju zaposlenima na poverljivim i ovlašćenim dužnostima koja se odnosi na inicijalnu obuku, doobuku ili za druge svrhe.

5.4. Procedure bezbednosnih provera/auditing

ESS QCA vodi ažurnu, tačnu i bezbednu evidenciju izdatih sertifikata koja nije javno dostupna i čiji integritet je potvrđen elektronskim potpisom.

Vodi se evidencija o svim događajima u radu ESS QCA elektronski (audit log) a gde to nije moguće ručno sa datumom, vremenom i opisom događaja.

5.4.1. Tipovi zabeleženih događaja

ESS QCA zapisuje događaje koji uključuju ali nisu ograničeni na operacije vezane za životni ciklus sertifikata, pokušaje pristupa sistemu, kao i zahteve dostavljene sistemu.

Celokupna razmena informacija između RA tela i ESS QCA su elektronski dokumenti sa kvalifikovanim elektronskim potpisom RA operatera odnosno CA operatera zavisno od smera komunikacije.

5.4.2. Učestalost pregleda evidentiranih događaja

Svi evidentirani događaji se čuvaju i pregledaju jedanput mesečno. Rad RA operatera se periodično proverava od strane zaposlenih na poverljivim dužnostima sa pauzom provere ne dužom od 6 meseci. Rad CA operatera se periodično proverava od strane zaposlenih na poverljivim dužnostima sa pauzom provere ne dužom od 3 meseca

5.4.3. Vreme čuvanja evidencije

Audit logovi se arhiviraju minimalno jedanput u 3 meseca a čuvaju se najmanje 10 godina.

5.4.4. Zaštita Audit log

Audit logovi se mogu videti samo od strane autorizovanog osoblja – sistem evidentičari. Dokumentacija dostavljena u RA telo se čuva u obezbeđenom prostoru. Dostavljena dokumentacija čuva se u RA telu. Sva dokumentacija se digitalizuje i kvalifikovano elektronski potpisuje od strane RA operatera. Audit logovi rada RA operatera sa sistemom i elektronski dokumenti sa kvalifikovanim elektronskim potpisom nalaze se na obezbeđenom računaru za tu namenu. Celokupna evidencija rada CA operatera, audit dnevici i druga dokumentacija čuva se u zoni visoke bezbednosti.

5.4.5. Procedura backup-a audit logova

ESS QCA implementira procedure backup-a audit logova.

5.4.6. Sistem sakupljanja audit logova

Logovi se skupljaju u realnom vremenu.

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.

5.4.8. Ocena ranjivosti sistema

U okviru redovnih analiza rizika po ISO 27001 za E-Smart Systems vrši se i anliza rizika ESS QCA sistema.

5.5. Arhiviranje zapisa

Zahtevi za čuvanjem zapisa se primenjuju kako na ESS QCA tako i na RA.

Detaljni opis procedure se nalazi u internim pravilima rada.

5.5.1. Tipovi arhiviranih zapisa

ESS QCA čuva na bezbedan način zapise o izdatim elektronskim sertifikatima, audit podacima, informacijama o aplikacijama za dobijanjem sertifikata, kao i dokumentaciju o samim aplikacijama za izdavanje sertifikata.

5.5.2. Period čuvanja arhive

ESS QCA čuva na bezbedan način pomenute zapise o ESS QCA kvalifikovanim elektronskim sertifikatima za period koji je naznačen u Zakonu o elektronskom potpisu i odgovarajućim podzakonskim aktima.

5.5.3. Zaštita arhive

ESS QCA sprovodi odgovarajuću proceduru zaštite medije backup-a arhive u obezbeđenom prostoru.

5.5.4. Procedura back-up-a arhive

ESS QCA sprovodi odgovarajuću proceduru backup-a arhive.

5.5.5. Zahtevi za vremesnkim pečatom zapisa

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

5.5.6. Sistem sakupljanja zapisa

Sprovodi se odgovarajući sistem skupljanja zapisa koji se arhiviraju.

5.5.7. Procedure za dobijanje i verifikaciju informacija iz arhive

ESS QCA čuva zapise u elektronskoj ili papirnoj formi. ESS QCA može zahtevati od svojih RA, korisnika ili njihovih agenata da dostave odgovarajuća dokumenta u cilju provere ispunjenosti ovog zahteva. Ovi zapisi mogu biti čuvani u elektronskoj, papirnoj i u bilo kojoj drugoj formi za koju ESS QCA smatra da je odgovarajuća.

5.6. Izmena ključeva

ESS QCA poseduje proceduru, detaljno opisanu u internim pravilima, koja se sprovodi u slučaju isteka sertifikata sertifikacionog tela ili opoziva sertifikata sertifikacionog tela u skladu sa uslovima definisanim u ovim CPS. U oba slučaja, vrši se generisanje novog para ključeva seritifikacionog tela i distribucija sertifikata CA svim korisnicima i zainteresovanim stranama, kao i u slučaju prvog generisanog sertifikata CA.

5.7. Kompromitacija i oporavak u slučaju katastrofe

5.7.1. Procedure za postupanje u incidentnim i kompromitujućim situacijama

U internim pravilima rada, ESS QCA dokumentuje procedure koje treba izvršiti pri rešavanju incidenata, kao i izveštavanja u vezi sa eventualnom kompromitacijom ključeva CA.

5.7.2. Računarski resursi, softver ili podaci koji su oštećeni

ESS QCA takođe dokumentuje u internim pravilima procedure oporavka koje se koriste ukoliko su računarski resursi, softver, i/ili podaci neispravni ili se sumnja da su neispravni.

5.7.3. Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika

Vrši se opoziv kompromitovanog kvalifikovanog elektronskog sertifikata i izdavanje novog sa novim parom ključeva.

5.7.4. Mogućnosti kontinuiteta poslovanja nakon katastrofe

Plan kontinuiteta poslovanja se implementira da osigura nastavak poslovanja nakon prirodne ili druge katastrofe i opisan je u internim pravilima ESS QCA.

5.8. Završetak rada CA ili RA

Pre nego što prekine svoje aktivnosti pružanja sertifikacionih usluga, ESS QCA:

- Obezbeđuje svojim korisnicima koji imaju validne sertifikate obaveštenje o nameri da prestane sa pružanjem sertifikacione usluge, tj. da prestane da izvršava aktivnosti u svojstvu CA.
- Opoziva sve sertifikate koji su još uvek validni (tj. one koji nisu opozvani ili im je istekao rok važnosti) nakon obaveštenja a bez zahteva za saglasnošću korisnika.
- Blagovremeno obaveštava o opozivu sertifikata sve korisnike na koje se to odnosi.
- Čini razumne mere u cilju zaštite zapisa koje čuva u skladu sa ovom CPS.
- Ukoliko je to moguće, obezbeđuje odgovarajuće mere obezbeđenja sukcesije u smislu ponovnog izdavanja sertifikata od strane drugog CA koje je sukcesor.

U slučaju prekida rada određenog udaljenog RA tela, ESS QCA:

- Prenosi kompletnu dokumentaciju, papirnu i elektronsku, nastalu radom RA u centralno RA telo u okviru ESS QCA,
- ESS QCA vrši nadzor svih zapisa rada RA operatera, i sertifikate za koje postoji neregularnost u radu RA tela opoziva,

- Ukida ovlašćenja svim RA operaterima za ovlašćenu dužnost u ESS QCA sistemu,
- Ažurira javno dostupan spisak RA tela ESS QCA sistema na repozitorijumu http://qca.e-smartsys.com.

6. Tehničke bezbednosne kontrole

Ovo poglavlje definiše tehničke bezbednosne mere koje primenjuje ESS QCA u cilju zaštite kriptografskih ključeva i aktivacionih podataka (kao na primer PIN-ovi, lozinke, itd.). Bezbednosno upravljanje ključevima je kritično u cilju osiguranja da su svi ključevi i aktivacioni podaci zaštićeni i da se koriste isključivo od strane autorizovanih zaposlenih.

Takođe, definisane su i druge tehničke bezbednosne kontrole koje se koriste od strane CA da se bezbedno izvršavaju funkcije generisanja ključeva, autentikacije korisnika, registracije korisnika, izdavanja sertifikata, opoziva sertifikata, provere/auditinga i arhiviranja. Tehničke kontrole uključuju životni ciklus bezbednosnih kontrola kao i operativne bezbednosne kontrole.

U ovom poglavlju se takođe definišu tehničke bezbednosne kontrole nad repozitorijumima, registracionim telima, korisnicima i drugim učesnicima.

6.1. Generisanje i instalacija asimetričnog para ključeva

6.1.1. Generisanje asimetričnog para ključeva

ESS QCA bezbedno generiše i štiti svoje sopstvene privatne ključeve korišćenjem bezbednih i pouzdanih sistema i primenjujući preventivne mere u cilju sprečavanja kompromitacije.

Za CA tela asimetrični par ključeva se generiše na HSM uređaju i privatni ključ nikada ne napušta uređaj u otvorenom obliku i na nezaštićenom medijumu.

Za kvalifikovan elektronski sertifikat asimetrični par ključeva se generiše na SSCD uređaju i privatni ključ nikada ne napušta uređaj. Generisanje obavlja CA operater u zoni bezbednosti. SSCD uređaji se uvode u sistem tako što im se izmene bezbednosni parametri i njihovi identifikatori se dodele CA operaterima ili ovlašćenim RA operaterima. Samo ovako pripremljeni SSCD uređaj (sa generisanim asimetričnim parom ključeva) prolaze proveru prilikom procesa izdavanja kvalifikovanog elektronskog sertifikata

6.1.2. Isporuka privatnog ključa korisniku

Pripremljen SSCD uređaj se čuva u ESS QCA zoni bezbednosti. U slučaju da je RA ovlašćen za rad sa SSCD uređaji se u obezbeđenim uslovima dostavljaju u RA gde ih RA čuva u obezbeđenoj prostoriji. Privatni ključ se ne koristi u komunikaciji RA i ESS QCA. Korisnik preuzimanjem SSCD uređaja preuzima i privatni ključ.

6.1.3. Dostava javnog ključa do izdavaoca sertifikata

CA Operater koristi javni ključ sa SSCD uređaja i sa identifikacionim podacima dobijenim od RA formira PKCS10 zahtev. Ukoliko je RA ovlašćen za rad sa SSCD uređajima onda RA operater koristi javni ključ sa

SSCD uređaja i sa identifikacionim podacima formira PKCS10 zahtev. Takav PKCS10 zahtev zapakuje u XML dokument koji potpisuje i šalje u CA telo. CA operater validira XML zahtev i dolazi do PKCS10 zahteva.

Ovakav PKCS10 zahtev prolazi validaciju samog ESS QCA sistema da je korišćen samo pripremljen SSCD uređaj i to baš od CA ili RA operatera koji je bio ovlašćen za rad sa SSCD.

6.1.4. Dostava javnog ključa izdavaoca sertifikata trećim stranama

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

6.1.5. Dužine ključeva

Za potrebe svog *Root* CA privatnog ključa i odgovarajuće potpisivanje, ESS RQCA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma. Dužina RSA ključa je 4096 bita. Period validnosti root sertifikata je 30 godina. Period validnosti izdatih sertifikata *Issuing* CA je do 10 godina.

Za svoj *Issuing* CA privatni ključ i odgovarajući algoritam za elektronsko potpisivanje, ESS IQCA1 koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma. Dužina RSA ključa je 2048 bita. Period validnosti sertifikata izdavajućeg tela je 10 godina. Period validnosti izdatih kvalifikovanih elektronskih sertifikata je do 5 godina.

Za kvalifikovane elektronske sertifikate koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma. Dužina RSA ključa je 2048 bita. Period validnosti sertifikata izdavajućeg tela je do 5 godina.

6.1.6. Generisanje kriptografskih parametara i provera kvaliteta

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

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

6.1.7. Namena ključa (Key Usage)

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

Izdavajuće CA telo ima namenu ključa za Certificate Signing, CRL Signing.

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

6.2. Zaštita privatnog ključa

ESS QCA koristi odgovarajuće kriptografske uređaje u cilju realizacije zadataka upravljanja ključevima CA. Pomenuti kriptografski uređaji su poznati pod imenom Hardverski bezbednosni moduli (HSM - Hardware Security Modules).

Privatni ključ kvalifikovanog elektronskog sertifikata generiše se na SSCD uređaju (smart kartica)

6.2.1. Standardi i kontrole kriptografskog hardverskog modula

Generisanje privatnog ključa ESS RQCA i ESS IQCA1 se dešava u okviru bezbednog kriptografskog uređaja koji zadovoljava odgovarajuće zahteve u skladu sa međunarodnim standardom FIPS 140-2 level3.

HSM uređaji ne smeju da napuštaju ESS QCA prostorije izuzev retkih prilika unapred definisanih premeštanja i preseljenja. ESS QCA čuva zapise u vezi svih tih premeštanja ili preseljenja. HSM uređaji se pre izlaska iz prostorija ESS QCA prvo backup-uju na bezbedne medije za tu namenu, obriše im se sadržaj i ako je u pitanju preseljenje nikada ne putuju zajedno sa backup medijom.

SSCD uređaj je u skladu sa međunarodnim standardom, FIPS 140-2 level3.

6.2.2. k od n distribucija odgovornosti kontrole privatnog ključa

Generisanje privatnog ključa ESS RQCA i ESS IQCA1 zahteva pod uslovima definisanim u okviru dva od četiri kontrole od strane više zaposlenih sa poverljivim dužnostima preko mehanizama koje obezbeđuje HSM uređaj. Autorizacija procedure generisanja ključeva se mora izvršiti od strane više od jednog člana upravne strukture ESS QCA.

Kod upotrebe sopstvenog privatnog ključa ESS QCA koristi minimalno dva nosioca USB tokena od četiri i kod *Root* CA tela i kod *Issuing* CA tela.

6.2.3. Bezbedno čuvanje privatnog ključa

Hardverski i softverski mehanizmi koji štite privatne ključeve CA su dokumentovani u internim pravilima rada. Uređaji poseduju sertifikat po FIPS 140-2 level3 standardu.

SSCD uređaji poseduju sertifikat po FIPS 140-2 level3 standardu.

6.2.4. Back-up privatnog ključa

Prilikom backup HSM uređaja privatni ključ se čuva u šifrovanom obliku i na, od strane proizvođača HSM uređaja, fizički za tu namenu zaštićenom medijumu. Prilikom uništenja privatnog ključa na HSM uređaju uništava se i na svim backup kopijama.

Detaljna procedura backup-a opisana je u posebnim internim pravilima.

Backup privatnog ključa kvalifikovanog elektronskog sertifikata se ne radi.

6.2.5. Arhiviranje privatnog ključa

Arhiviranje privatnog ključa kvalifikovanog elektronskog sertifikata se ne radi.

6.2.6. Transfer privatnog ključa na hardverski kriptografski modul

Opisano u posebnim internim pravilima za sopstveni privatni ključ ESS QCA.

Privatni ključ kvalifikovanog elektronskog sertifikata se generiše na smart kartici i nema mogućnost exporta.

6.2.7. Čuvanje privatnog ključa na hardverskom kriptografskom modulu

Sopstveni privatni ključ ESS QCA *Root* i *Issuing* Ca tela čuva se na HSM uređaju.

Privatni ključ kvalifikovanog elektronskog sertifikata čuva se na SSCD.

6.2.8. Metoda aktivacije privatnog ključa

Nosioci deljenih tajni (staraoci) ESS RQCA i ESS IQCA1 imaju zadatak da aktiviraju i deaktiviraju privatni ključ odgovarajućeg CA. Privatni ključ je tada aktivan u definisanom režimu rada.

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

6.2.9. Metoda deaktivacije privatnog ključa

Nosioci deljenih tajni onemogućavaju korišćenje privatnog ključa preko HSM uređaja.

6.2.10. Metoda uništenja privatnog ključa

Privatni ključ ESS QCA se ne obnavlja. Privatni ključ ESS QCA će biti uništen na kraju svog životnog ciklusa preko HSM uređaja. Uništenje je opisano u internim pravilima.

6.2.11. Rangiranje kriptografskih hardverskih modula

Nije primenljivo

6.3. Drugi aspekti upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

ESS RQCA i ESS IQCA1 arhivira svoj sopstveni javni ključ.

6.3.2. Periodi validnosti sertifikata i privatnog ključa

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

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

Vreme Validnosti kvalifikovanog elektronskog sertifikata je 3 (tri) ili 5 (pet) godina.

6.4. Aktivacioni podaci

ESS QCA kreiranje i procesiranje aktivacionih podataka pridružene privatnim ključevima CA, kao i svim drugim privatnim ključevima u datom PKI sistemu (Izdavajući CA, RA, korisnici) opisuje u ovom poglavlju a detaljnije u internim pravilima.

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.

Svaki izdati kvalifikovani elektronski sertifikat se proglašava suspendovanim nakon izdavanja. ESS QCA generiše jednokratni kod za aktiviranje suspendovanog kvalifikovanog elektronskog sertifikata i dostavlja ga putem SMS-a krajnjem korisniku. U poglavlju 4.4 je opisano kako korisnik aktivira sertifikat.

U CA, ili u ovlašćenom RA za rad sa SSCD uređajima, se prilikom instalacije kvalifikovanog elektronskog sertifikata, PIN kod SSCD uređaja podešava na slučajno generisanu vrednost i štampa na koverti za PIN kod.

Vlasnik kvalifikovanog elektronskog sertifikata može promeniti PIN kod nakon preuzimanja ili u bilo kom drugom periodu trajanja i korišćenja sertifikata.

6.4.2. Zaštita podataka za aktiviranje

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

Korisnici SSCD uređaja su dužni da čuvaju PIN za pristup privatnom ključu na SSCD uređaju.

6.4.3. Drugi aspekti u vezi aktivacionih podataka

ESS QCA omogućva svojim korisnicima da urade deblokiranje aktivacionog podatka SSCD uređaja. Od korisnika se zahteva:

- Lično prisustvo kod RA operatera
- Da donese SSCD uređaj čiji je aktivacioni podatak (PIN kod) blokiran ili ga je korisnik zaboravio
- Da podnese zahtev za deblokadom

RA operater će na SSCD uređaju izvršiti deblokadu PIN koda na neku slučajnu vrednost i odštampati kovertu sa PIN kodom. SSCD uređaj i koverta se uručuju korisniku.

6.5. Bezbednosne kontrole računara

ESS QCA implementira bezbednosne kotrole nad računarima koji se koriste u okviru datog PKI sistema.

6.5.1. Specifični zahtevi za bezbednost računara

Računari koji se koriste za ESS QCA čuvaju se u posebno zaštićenim prostorijama

6.5.2. Rangiranje bezbednosti računara

Nije primenljivo

6.6. Životni ciklus tehničkih bezbednosnih kontrola

ESS QCA realizuje kontrole periodičnog razvoja sistema i upravljanja bezbednošću sistema preko implementiranog ISO 27001 standarda.

6.7. Mrežne bezbednosne kontrole

ESS QCA održava i primenjuje visok nivo sistema mrežne bezbednosti, uključujući primenu firewall uređaja i intrusion detection/prevention sistema.

6.8. Vremenski pečat

Vremenski žig se koristi samo za interni operativni rad ESS QCA. RA i CA operateri u razmeni informacija koriste kvalifikovani elektronski potpis.

7. Profili sertifikata i CRL lista

Ovo poglavlje specificira formate sertifikata i CRL lista koje izdaje ESS QCA.

7.1. Profili sertifikata

ESS QCA izdaje sledeće vrste sertifikata:

- *Root* CA telo,
- *Issuing* CA telo,
- Kvalifikovani elektronski sertifikat korisnike,

7.1.1. *Root* CA telo

Polja Verzije1	Vrednost
Version	V3
Serial Number	20 hex karaktera bez vodećih nula
Signature Algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Valid From	UTC datum i vreme
Valid To	UTC datum i vreme + 30godina
Subject	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Public Key	4096bit
Polja Ekstenzije	**Vrednost**
Key Usage (Critical)	Certificate Signing, CRL Signing (06)
Basic Constraints (Critical)	Subject Type=CA Path Length Constraint=1
Enhanced Key usage	Nema
Application Policies	Nema
Certificate Policies	Nema
Qualified Certificate Statements	Nema
Subject Key Identifier	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	Nema
CRL Distribution Points	Nema

Authority Information Access	Nema
Subject Alternate Name	Nema
Polja Atributa	Vrednost
Thumbprint algorithm	Sha1
Thumbprint	40 hex karaktera
Frendly Name	E-Smart Systems Root QCA

7.1.2. *Issuing* CA telo

Polja Verzije1	Vrednost
Version	V3
Serial Number	20 hex karaktera bez vodećih nula
Signature Algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Valid From	UTC datum i vreme
Valid To	UTC datum i vreme + 10godina
Subject	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Public Key	2048bit
Polja Ekstenzije	**Vrednost**
Key Usage (Critical)	Certificate Signing, CRL Signing (06)
Basic Constraints (Critical)	Subject Type=CA Path Length Constraint=0
Enhanced Key usage	nema
Application Policies	Nema
Certificate Policies	Policy Identifier=All issuance policies
Qualified Certificate Statements	Nema
Subject Key Identifier	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a

CRL Distribution Points	http putanja do CRL liste *Root* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	http putanja do fajla *Root* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Subject Alternate Name	Nema
Polja Atributa	Vrednost
Thumbprint algorithm	sha1
Thumbprint	40 hex karaktera
Frendly Name	E-Smart Systems Issuing 1 QCA

7.1.3. Kvalifikovani elektronski sertifikat za korisnike

Polja Verzije1	Vrednost
Version	V3
Serial Number	20 hex karaktera bez vodećih nula
Signature Algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
Valid From	UTC datum i vreme
Valid To	UTC datum i vreme + (1,2,3,4 ili 5) godina
Subject	CN={ime} {prezime} {JIK}[-{JMBG}], O={ime_organizacije}-{matični_broj}, SERIALNUMBER={SN SSCD}, C=RS
Public Key	2048bit
Polja Ekstenzije	**Vrednost**
Key Usage	Digital Signature, Non-Repudiation (c0)
Enhanced Key usage	Nema
Application Policies	Nema
Certificate Policies	1.3.6.1.4.1.30496.509.1.1.1 (http://qca.e-smartsys.com/repo/ESS_QCA_CPS.pdf)
Qualified Certificate Statements	0.4.0.1862.1.1 (European Qualified Certificate) 0.4.0.1862.1.4 (QC SSCD Statement)
Subject Key Identifier	40 hex karaktera Hash vrednost PublicKey – koristi se za konstrukciju putanje sertifikata
Authority Key Identifier	KeyID=40 hex karaktera Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a

CRL Distribution Points	http putanja do CRL liste *Issuing* CA na http://qca.e-smartsys.com repozitorijumu
Authority Information Access	http putanja do fajla *Issuing* CA sertifikata na http://qca.e-smartsys.com repozitorijumu
Subject Alternate Name	Nema
Polja Atributa	Vrednost
Thumbprint algorithm	sha1
Thumbprint	40 hex karaktera
Frendly Name	Nema

7.2. Profil CRL liste

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

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

ESS QCA izdaje CRL verzije 2 sa osnovnim poljima i ekstenzijama

Opozvani sertifikati kojima je istekala validnost ne nalaze se u CRL listi ali se nalaze u registru opozvanih sertifikata.

7.2.1. Profil *Root* CRL liste

Polja	Vrednost
Version	v2
Issuer	CN=ESS RQCA, O = E-Smart Systems d.o.o., C = RS
Signature Algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
This Update	UTC datum i vreme
Next Update	UTC datum i vreme + 26nedelja
CA Version	Vmajor.minor
CRL Number	Redni broj
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuuje CRL listu
Revocated Certificate	Serial Number UTC datum i vreme opoziva razlog opoziva

7.2.2. Profil *Issuing* CRL liste

Polja	Vrednost
Version	v2
Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS

Signature Algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN=ESS IQCA1, O = E-Smart Systems d.o.o., C = RS
This Update	UTC datum i vreme
Next Update	UTC datum i vreme + 24sata
CA Version	Vmajor.minor
CRL Number	Redni broj
Authority Key Identifier	KeyID=hash javnog ključa CA tela koje potpisuuje CRL listu
Revocated Certificate	Serial Number UTC datum i vreme opoziva razlog opoziva

7.3. OCSP profil

OCSP servis se ne koristi.

8. Provera saglasnosti sa Politikom sertifikacije

ESS CA prihvata periodičnu poveru/audit saglasnosti svojih politika, uključujući ovu CPS što uključuje i periodičnu superviziju od strane Nadležnog organa Republike Srbije. Rad ESS QCA je takođe u saglasnosti sa najvažnijim međunarodnim i Evropskim standardima u ovoj oblasti, kao i sa Evropskom direktivom 1999/93/EC o elektronskim potpisima.

U domenu izdavanja kvalifikovanih elektronskih serifikata, ESS QCA radi u okviru ograničenja definisanim u okviru Zakona o elektronskom potpisu Republike Srbije, kao i odgovarajućim podzakonskim aktima.

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

ESS QCA sprovodi redovne interne audit-e usklađenosti poslovanja sa CP, kao i sa ovim CPS dokumentom. Interni audit sprovode odgovarajući zaposleni ESS sa datim zaduženjima. U slučaju neusaglašenosti rada sa politikom ESS QCA obustavlja dalje izdavanje elektronskih sertifiakta, osim probnih, dok se ne otkloni neusaglašenost.

ESS QCA je akreditovano od strane Nadležnog organa za poslove akreditacije i supervizije, prema Zakonu o elektronskom potpisu u Republici Srbiji (Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija) i

biće predmet periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona o elektronskom potpisu i odgovarajućim podzakonskim aktima.

9. Drugi poslovni i pravni aspekti

9.1. Cene

9.1.1. Cene izdavanja ili obnove sertifikata

ESS QCA naplaćuje izdavanje kvalifikovanih elektronskih sertifikata.

Objavljivanje cena sertifikata i drugih sertifikacionih usluga se vrši putem web sajta ESS QCA, partnera ESS QCA (treća lica) ili putem odgovarajućeg ugovora tamo gde je to primenljivo.

ESS QCA zadržava prava da menja uslove naplaćivanja sertifikata.

9.1.2. Cena pristupa sertifikatima

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.1.3. Cena pristupa informacijama o statusu sertifikata

Pristup registru opozvanih sertifikata (CRL) je besplatan .

9.1.4. Cene za druge servise

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.1.5. Politika povraćaja novca

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.2. Finansijska odgovornost

9.2.1. Pokrivanje osiguranja

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

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

Sertifikaciono telo ESS QCA poseduje odgovarajuće osiguranje za bilo koju štetu koju mogu da pretrpe treća lica, a za koju je odgovorno sertifikaciono telo. Detaljne informacije objavljene su na web stranicama.

9.2.2. Druga dobra

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.2.3. Osiguranje ili garancijsko pokrivanje za krajnje korisnike

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

- Bilo kog lažnog ili pogrešno prezentovanog podatka dostavljenog od strane korisnika ili njihovih agenata.
- Bilo kog propusta korisnika da dostavi materijalnu činjenicu da je pogrešna prezentacija ili propust učinjen iz nemarnosti ili sa namerom da se prevari ESS QCA, ili bilo koje lice koje prima i odnosi se prema dobijenom sertifikatu.
- Neobezbeđivanja odgovarajuće zaštite korisnikovog privatnog ključa, nekorišćenja bezbednog sistema kako je zahtevano, ili neizvršenja odgovarajućih preventivnih mera neophodnih da se spreči kompromitacija, gubitak, objavljivanje, modifikacija ili neautorizovano korišćenje korisnikovog privatnog ključa, ili napada na integritet ESS RQCA i IQCA1 privatnog ključa.
- Kršenja bilo kojih zakona koji su primenljivi, uključujući one koji se odnose na zaštitu intelektualnih prava, viruse, pristup računarskim sistemima, itd.

9.3. Poverljivost poslovnih informacija

9.3.1. Opseg poverljivih informacija

Sertifikaciono telo ESS QCA postupa poverljivo sa sledećim podacima:

- Sa svim zahtevima za dobijanje kvalifikovanog elektronskog sertifikata ili drugih usluga
- Sve moguće poverljive podatke vezane za finansijske obaveze,
- Sve moguće poverljive podatke koji predstavljaju predmet međusobnih ugovora sa trećim licima i
- Sve ostale podatke koji su navedeni u internim pravilima rada sertifikacionog tela ESS QCA.

U toku obrade svih mogućih poverljivih podataka o vlasnicima sertifikata i trećim licima, koji su nužno potrebni za usluge upravljanja kvalifikovanim elektronskim sertifikatima, sertifikaciono telo ESS QCA postupa u skladu sa važećim zakonodavstvom.

9.3.2. Informacije koje nisu u opsegu poverljivih informacija

Sertifikaciono telo 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

Sertifikaciono telo ESS QCA ne preuzima nikakve odgovornosti za sadržaj podataka koje vlasnik kvalifikovanog elektronskog sertifikata elektronski potpisuje. Takođe, sertifikaciono telo ne preuzima nikakve odgovornosti za pitanja da li su vlasnik ili treće lice poštovali sve važeće propise, sve odredbe politike sertifikacije i drugih pravila sertifikacionog tela ESS QCA, odnosno vodili računa o svim objavljenim uputstvima.

Sertifikaciono telo ESS QCA ne preuzima nikakve odgovornosti za posledice do kojih dolazi ukoliko vlasnik kvalifikovanog elektronskog sertifikata nije postupao u skladu sa sigurnosnim zahtevima iz poglavlja 5 ovog CPS dokumenta.

9.4. Privatnost i zaštita personalnih informacija

9.4.1. Plan privatnosti

ESS QCA se pridržava pravila zaštite privatnosti personalnih podataka i pravila poverljivosti kako je propisano u CPS dokumentu, kao i u odgovarajućim zakonskim dokumentima.

9.4.2. Informacije koje se tretiraju kao privatne

Lični podaci koji se čuvaju su svi lični podaci koje sertifikaciono telo ESS QCA prikupi u okviru zahteva za svoje usluge ili u odgovarajućim registrima za dokazivanje identiteta vlasnika.

9.4.3. Informacije koje se ne smatraju privatnim

ESS QCA sertifikaciono telo ne smatra privatnim isključivo one informacije korisnika za koje je sam korisnik dao saglasnost da se mogu publikovati.

ESS QCA u procesu registracije pretplatnika i pripadnika entiteta prikuplja identifikacione podatke. Identifikacioni podaci pretplatnika kao što su skraćeni naziv i matični broj naći će se na kvalifikovanom elektronskom sertifikatu u polju *organizationName*. Identifikacioni podaci pripadnika entiteta kao što su Ime i Prezime naći će se na kvalifikovanom elektronskom sertifikatu u polju *commonName*, ukoliko je na zahtevu stajalo da će se sertifikat koristi i za komunikaciju sa državom u okviru *commonName* naći će se i JMBG korisnika.

9.4.4. Odgovornost za zaštitu privatnih informacija

ESS QCA je odgovorno za zaštitu privatnosti korisnikovih informacija prikupljenih u okviru zahteva za svoje usluge ili u odgovarajućim registrima za dokazivanje identiteta vlasnika.

9.4.5. Obaveštenje i saglasnost za korišćenje privatnih informacija

ESS QCA sertifikaciono telo definiše uslove u vezi objavljivanja privatnih informacija za koje dati korisnik treba da da saglasnost i ti su uslovi objavljeni u ugovoru koji se potpisuje sa korisnikom.

Vlasnik ovlašćuje sertifikaciono telo ESS QCA za korišćenje ličnih podataka koji se nalaze na zahtevu za dobijanje kvalifikovanih elektronskih sertifikata, u skladu sa zakonom o zaštiti ličnih podataka.

9.4.6. Otkrivanje informacija shodno pravnim i administrativnim procesima

ESS QCA ne objavljuje, niti se zahteva da objavljuje, bilo koju poverljivu informaciju bez autentikovanog i potvrđenog zahteva od strane:

- Same strane za koju se takva infromacija i čuva,
- Odgovarajućeg suda.

ESS QCA može naplatiti odgovarajuću administrativnu cenu za procesiranje ovakvih objavljivanja.

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

9.4.7. Druge okolnosti za otkrivanje informacija

ESS QCA i njegovi partneri mogu učiniti raspoloživom specifičnu politiku privatnosti u cilju zaštite personalnih podataka aplikanta koji zahteva izdavanje sertifikata od strane ESS QCA ili njegovog partnera putem njihovih web sajtova i/ili CP ili CPS dokumenata.

9.5. Prava intelektualnog vlasništva

ESS QCA poseduje i zadržava sva prava intelektualnog vlasništva pridružena njegovim bazama podataka, web sajtovima, kvalifikovanim elektronskim sertifikatima koje izdaje, kao i bilo kojim drugim publikacijama koje na bilo koji način pripadaju ili potiču od strane ESS QCA, uključujući i ovu CP.

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

9.6. Izjava o garanciji

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.7. Nepriznavanje garancije

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.8. Ograničenja odgovornosti

ESS QCA ne prihvata bilo kakvu drugu odgovornost osim one koja je eksplicitno definisana u ovom dokumentu.

Ni u kom slučaju (izuzev zloupotrebe ili namere) ESS QCA nije odgovorno za:

- korišćenje kvalifikovanih elektronskih sertifikata za namene i na način koji nije izričito predviđen u politici sertifikacije i CPS dokumentu,
- nepravilnog ili pogrešnog obezbeđenja lozinki ili privatnih ključeva vlasnika kvalifikovanog elektronskog sertifikata, otkrivanje poverljivih podataka ili ključeva trećim licima i neodgovornog postupanja vlasnika kvalifikovanog elektronskog sertifikata,
- zloupotrebe odnosno upada u informacioni sistem vlasnika kvalifikovanog elektronskog sertifikata i na taj način dolaska do podataka o kvalifikovanim elektronskim sertifikatima od strane neovlašćenih lica,
- nepostupanja ili lošeg postupanja sa podacima u okviru informacione infrastrukture vlasnika kvalifikovanog elektronskog sertifikata ili trećih lica,
- neproveravanja podataka i validnosti (statusa povučenosti) kvalifikovanih elektronskih sertifikata u registru opozvanih kvalifikovanih elektronskih sertifikata,
- neproveravanja vremena validnosti kvalifikovanih elektronskih sertifikata,
- postupanja vlasnika kvalifikovanog elektronskog sertifikata ili trećeg lica suprotno informacijama i obaveštenjima koje objavljuje sertifikaciono telo ESS QCA, politikom sertifikacije, CPS dokumentom i drugim propisima,

- omogućenog korišćenja odnosno zloupotrebe vlasnikovog kvalifikovanog elektronskog sertifikata od strane neovlašćenih lica,
- sadržaj samih podataka koji se potpisuju korišćenjem kvalifikovanih elektronskih sertifikata, već samo da je kod potpisa nad tim podacima korišćenjem kvalifikovani elektronski sertifikata ESS QCA,
- upotrebe i pouzdanosti rada mašinske i programske opreme vlasnika kvalifikovanog elektronskog sertifikata.

9.9. Odštete

Za štetu nastalu upotrebom kvalifikovanog elektronskog sertifikata i njemu pridruženog privatnog ključa usled nepoštovanja odredbi ugovora, politike sertifikacije, praktičnih pravila rada i važećeg zakonodavstva, odgovorna je stranka koja je istu prouzrokovala.

9.10. Period važnosti i kraj validnosti Praktičnih Pravila Sertifikacije

Sertifikaciono telo ESS QCA zadržava pravo da izmeni politiku sertifikacije i ovaj CPS dokument i da nadogradi infrastrukturu bez prethodnog obaveštavanja vlasnika kvalifikovanog elektronskog sertifikata.

Važeći sertifikati tako ostaju važeći do isteka njihove validnosti i za njih još uvek važi onaj CPS dokument koji je važio u vreme njihovog izdavanja. Za sve sertifikate izdate nakon početka validnosti novog CPS dokumenta, važi taj novi.

Ovaj CPS dokument stupa na snagu onoga dana kada je odobren i objavljen od strane sertifikacionog tela ESS QCA.

9.10.1. Važnost

Nova verzija (odnosno promene) CPS dokumenta sertifikacionog tela ESS QCA prethodno se, osam (8) dana pre zvaničnog datuma validnosti, objavljuje na web stranici sertifikacionog tela ESS QCA sa novim identifikacionim brojem (CPS OID) i označenim datumom početka validnosti.

9.10.2. Kraj validnosti

Kraj validnosti CPS dokumenta nije određen niti je povezan sa periodom validnosti kvalifikovanih elektronskih sertifikata izdatih na osnovu ovog CPS.

9.10.3. Efekat završetka i ponovnog rada

Prilikom objavljivanja novog CPS, svi kvalifikovani elektronski sertifikati izdati nakon tog datuma procesiraju se prema novom CPS dokumentu.

9.11. Pojedinačna obaveštenja i komunikacija sa učesnicima

Kontaktni podaci sertifikacionog tela objavljeni su na web stranicama istog i navedeni u poglavlju 1.3.1.

9.12. Ispravke

9.12.1. Procedure za ispravku

Promene ili dopune ovog CPS dokumenta sertifikaciono telo može da objavi u obliku promena ili dopuna ovog CPS ako se ne radi o suštinskim promenama operativnog rada sertifikacionog tela.

Amandmani se usvajaju i prihvataju istim postupkom kao i sama praktična pravila rada.

9.12.2. Mehanizam i period obaveštavanja

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.12.3. Uslovi promene objektnog identifikatora (OID)

Ovo poglavlje nije primenljivo u okviru ove CPS.

9.13. Procedure rešavanja sporova

ESS QCA se referiše na arbitražu u cilju rešavanja svih sporova koji se odnose na ovu CPS. Ako se spor ne reši u okviru deset (10) dana nakon inicijalnog obaveštenja shodno pravilima CPS, strane u sporu dostavljaju spor na arbitražu. Arbitraža se sastoji od 3 arbitra, svaka strana predlaže po jednog, dok trećeg predlažu zajedno obe strane u sporu. Mesto za arbitražu je Beograd, Srbija, a arbitri određuju sve troškove arbitraže.

Za sve sporove koji se odnose na tehnologiju, kao i sporove koji se odnose na sam CPS dokument, strane u sporu prihvataju arbitražno telo koje će biti izabrano od strane vlade Srbije.

9.14. Zakon koji se poštuje

Ova CPS je u potpunosti u skladu sa odgovarajućom zakonskom regulativom države Srbije, i to pre svega sa Zakonom o elektronskom potpisu i odgovarajućim podzakosnkim aktima. Sve pravne stvari koje se odnose na ESS QCA i/ili koji se odnose na sertifikate izdate od strane ESS QCA će biti procesuirane od strane odgovarajućeg suda u Srbiji.

9.15. Saglasnost sa primenljivim zakonima

Ovo poglavlje nije primenljivo u okviru ove CP.

9.16. Razne odredbe

Ovo poglavlje nije primenljivo u okviru ove CP.

9.17. Druge odredbe

Ovo poglavlje nije primenljivo u okviru ove CP.

10. Istorija dokumenta

Verzija.	Datum	Opis promena
0.1	1.11.2011	Inicijalni dokument
0.2	10.8.2013	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	1.4.2014	Gramatičke ispravke
1.6	3.6.2014	Proširenje pretplatnika
1.7	21.01.2016	Izmena osobe odgovorne za ovu CPS
1.8	1.4.2019	Manje izmene dokumenta

11. Reference

- Zakon o elektronskom potpisu, Sl. Glasnik Republike Srbije, br. 135/2004
- Pravilnik o bližim uslovima za izdavanje elektronskih sertifikata, Sl. Glasnik Republike Srbije, br. 26/2008,
- Pravilink o tehničko-tehnološkim postupcima z aformiranje kvalifikovanog elektronskog potpisa i kriterijuma koje treba da ispune sredstva za formiranje elektronskog potpisa, Sl. Glasnik Republike Srbije, br. 26/2008, 13/2010
- RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- RFC 5280 – Request For Comments 5280, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile
- Politika Sertifikacije Sertifikacionog tela E-Smart Systems d.o.o.

12. Kompanije i organizacije

[1] E-Smart Systems d.o.o., http://www.e-smartsys.com

[2] IANA (Internet Assigned Numbers Authority), http://www.iana.org