

U skladu sa eIDAS-om i uslugom kvalifikovanog elektronskog čuvanja

Politika kvalifikovanog elektronskog čuvanja dokumenata

Verzija 1.4

Sadržaj

1 Uvod 6

1.1 Pregled 6

1.2 Naziv i identifikacija dokumenta 6

1.2.1 Efekat 7

Obim usluge 7

Vremenski okvir 7

Obim učesnika 7

Geografski obim 7

1.3 PKI Učesnici 8

1.3.1 Sertifikaciono telo 8

1.3.2 Pretplatnici 8

1.3.3 Oslanjajuće strane 8

1.4 Administracija politike 9

1.4.1 Organizacija koja vrši administraciju dokumenta 9

1.4.2 Kontakt osoba 9

1.4.3 Osoba ili organizacija odgovorna za prikladnost dokumenta Praktična pravila za kvalifikovano elektronsko čuvanja dokumenata 9

1.4.4 Procedure odobravanja praktičnih pravila 9

1.5 Definicije i akronimi 10

1.5.1 Definicije 10

1.5.2 Akronimi 18

2 Objavljivanje i obaveze 19

2.1 Repozitorijumi 19

2.2 Vreme ili učestalost objavljivanja 19

2.2.1 Učestalost objavljivanja Opštih uslova 19

3 Elektronski servis za čuvanje 21

3.1 Zaključivanje Ugovora o uslugama 22

3.2 Učitavanje objekta za očuvanje 22

3.3 Obezbeđivanje materijala za validaciju/Dostupnost dokaza o čuvanju – preuzimanje dokaza o čuvanju 23

3.4 Izdavanje potvrde 23

3.5 Raskid ugovora o usluzi 24

4 Tehničke mere bezbednosti 25
4.1 Sigurnosne garancije 25
4.2 Mere predostrožnosti za računarsku bezbednost 26
4.3 Tehničke mere predostrožnosti vezane za životni ciklus 26
4.4 Redovna sertifikacija 26
4.5 Ponovno šifrovanje arhive 26
4.6 Kontinuirano praćenje tehnologije 27
4.7 Prihvatanje sertifikata i vremenskog žiga Pružalaca usluga 27
4.8 Dostupnost određenih elemenata usluge elektronskog čuvanja 27
5 Objekti, upravljanje i operativne kontrole 28
5.1 Fizičke kontrole 28
5.1.1 Lokacija i izgradnja 28
5.1.2 Fizičku pristup 29
5.1.3 Napajanje i klimatizacija 30
5.1.4 Izloženost vodi 30
5.1.5 Prevencija i zaštita od požara 30
5.1.6 Skladištenje medija 30
5.1.7 Odlaganje otpada 31
5.1.8 Bekap van lokacije 31
5.2 Proceduralne kontrole 31
5.2.1 Uloge od poverenja 32
5.2.2 Broj potrebnih osoba po zadatku 32
5.2.3 Identifikacija i autentifikacija za svaku ulogu 33
5.2.4 Uloge koje zahtevaju razdvajanje dužnosti 33
5.3 Kontrola zaposlenih 34
5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje 34
5.3.2 Procedure provere zaposlenih 34
5.3.3 Zahtevi za obuku 35
5.3.4 Učestalost i uslovi prekvalifikacije 35
5.3.5 Učestalost i redosled rotacije poslova 36
5.3.6 Sankcije za nedozvoljene radnje 36
5.3.7 Zahtevi nezavisnog izvođača 37
5.3.8 Dokumentacija dostavljena osoblju 37

5.4 Procedure evidentiranja revizije 37
5.4.1 Vrste evidentiranih događaja 37
5.4.2 Učestalost obrade log fajlova 41
5.4.3 Period zadržavanja log fajlova 41
5.4.4 Zaštita logova 41
5.4.5 Procedure za pravljenje rezervnih kopija log fajlova 42
5.4.6 Sistem prikupljanja revizije (interni naspram eksternog) 42
5.4.7 Obaveštenje subjektu koji izaziva događaj 42
5.4.8 Procene ugroženosti 42
5.5 Arhivski zapisi 43
5.5.1 Vrste arhiviranih zapisa 43
5.5.2 Period čuvanja arhive 43
5.5.3 Zaštita arhive 43
5.5.4 Procedure arhiviranja rezervnih kopija 44
5.5.5 Zahtevi za označavanje zapisa vremenskim žigom 44
5.5.6 Sistem prikupljanja arhiva (interni ili eksterni) 44
5.5.7 Procedure za dobijanje i verifikaciju informacija arhive 45
5.6 Oporavak od kompromitovanja i katastrofe 45
5.6.1 Procedure za rukovanje incidentima i kompromitovanjem informacija 45
5.6.2 Oštećenje računarskih resursa, softvera i/ili podataka 45
5.6.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe 46
5.7 Prestanak usluge čuvanja 47
6 Tehničke kontrole bezbednosti 48
6.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula 48
6.1.1 Standardi i kontrole kriptografskog modula 48
6.1.2 Privatni ključ (N od M) Kontrola više osoba 49
6.1.3 Deponovanje privatnog ključa 49
6.1.4 Rezervna kopija privatnog ključa 49
6.1.5 Arhiviranje privatnog ključa 49
6.1.6 Prenos privatnog ključa u ili iz kriptografskog modula 49
6.1.7 Skladištenje privatnog ključa na kriptografskom modulu 50
6.1.8 Način aktiviranja privatnog ključa 50
6.1.9 Metoda deaktiviranja privatnog ključa 50

6.1.10 Metoda uništavanja privatnog ključa 50
6.1.11 Ocena kriptografskog modula 50
6.2 Podaci o aktivaciji 51
6.2.1 Aktivacija generisarnih podataka i instalacija 51
6.2.2 Zaštita podataka aktivacije 51
6.2.3 Drugi aspekti aktivacije podataka. 51
6.3 Kontrole računarske bezbednosti 51
6.3.1 Specifični tehnički zahtevi za bezbednost računara 51
6.3.2 Ocena računarske bezbednosti 52
6.4 Tehničke kontrole životnog ciklusa 52
6.4.1 Kontrole razvoja sistema 52
6.4.2 Kontrole upravljanja sigurnošću 53
6.4.3 Životni ciklus sigurnosnih kontrola 53
6.5 Bezbedonosne kontrole mrežnog okruženja 54
6.6 Stavljanje vremenskog žiga 55
7 Revizija usklađenosti i druge procene 56
7.1 Učestalost ili okolnosti procene 57
7.2 Identitet/Kvalifikacije procenjivača 57
7.3 Odnos procenjivača prema procenjenom entitetu 57
7.4 Teme obuhvaćene ocenjivanjem 57
7.5 Radnje preduzete kao rezultat nedostatka 58
7.6 Saopštavanje rezultata 58
REFERENCE 59

1 Uvod

Ovaj dokument sadrži Politiku kvalifikovanog elektronskog čuvanja dokumenata koju je definisao i kojom upravlja Inception d.o.o Beograd (u daljem tekstu: Inception ili Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata) u vezi sa kvalifikovanom uslugom od poverenja.

Politika kvalifikovanog elektronskog čuvanja dokumenata je u skladu sa zahtevima propisanim eIDAS Uredbom[1], usluga koja se pruža u skladu sa ovim propisima je kvalifikovana za izdavanje:

- Elektronskih potpisa
- Elekronskih pečata

1.1 Pregled

Politika kvalifikovanog elektronskog čuvanja dokumenata je skup pravila koja specificiraju upotrebljivost kvalifikovane usluge čuvanja za zajednicu i/ili klasu aplikacija sa zajedničkim bezbednosnim zahtevima.

Politika kvalifikovanog elektronskog čuvanja dokumenata postavlja osnovne zahteve za Pružaoca usluga u vezi sa kvalifikovanim čuvanjem koje treba uspostaviti.

Politika kvalifikovanog elektronskog čuvanja dokumenata je jedan od nekoliko dokumenata koje izdaje Pružalac usluga od poverenja koji zajednički regulišu uslove usluga koje pruža Pružalac usluga. Ostali važni dokumenti uključuju Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata i druge ugovore sa klijentima i partnerima.

1.2 Naziv i identifikacija dokumenta

Izdavač	Inception d.o.o
Naziv dokumenta	U skladu sa eIDAS-om i kvalifikovanom uslugom elektronskog čuvanja dokumenata
OID	Politika
Verzija dokumenta	1.3.6.1.4.1.57738.40.1.1.4.0
Datum stupanja na snagu	1.4

1.2.1 Efekat

Praktična pravila i Politika kvalifikovanog elektronskog čuvanja dokumenata zasnovana na ovim politikama treba revidirati najmanje jednom godišnje i obezbediti njihovu dopunu potencijalno izmenjenim zahtevima i preduslovima.

Obim usluge

Politika kvalifikovanog elektronskog čuvanja dokumenata definiše specifične zahteve za usluge opisane u ovom dokumentu.

Vremenski okvir

Trenutna verzija dokumenta važi od datuma stupanja na snagu navedenog u odeljku 1.2 ovog dokumenta do povlačenja. Efekat automatski prestaje sa prestankom pružanja usluge ili izdavanjem novije verzije dokumenta Praktična pravila.

Obim učesnika

Efekat Politike kvalifikovanog elektronskog čuvanja dokumenata se proteže na svakog od pomenutih učesnika.

Pružalac usluge čuvanja pruža usluge prvenstveno građanima Republike Srbije i organizacijama registrovanim u Republici Srbiji, ali ne isključuje građane ili organizacije iz drugih zemalja sve dok prihvataju sistem pravila kojih se pridržava Pružalac usluge čuvanja i kontrole neophodne kako bi se pružene usluge mogle obavljati bezbedno i u skladu sa zakonom Republike Srbije.

Geografski obim

Trenutna Politika kvalifikovanog elektronskog čuvanja dokumenata zasnovana je na zahtevima Evropske unije, ali takođe uključuje i zahteve specifične za Srbiju za usluge koje posluju po zakonu Srbije u Republici Srbiji.

Pružalac usluge čuvanja može proširiti geografski obim usluge, u ovom slučaju neće koristiti manje stroge zahteve od onih koji se primenjuju u Politici kvalifikovanog elektronskog čuvanja. Kod usluga koje se pružaju stranim klijentima, detaljni uslovi koji se razlikuju od Politike čuvanja mogu se regulisati posebnim ugovorom o uslugama.

Usluga koja se pruža u skladu sa ovom Politikom kvalifikovanog elektronskog čuvanja

dokumenata dostupna je širom sveta. Valjanost dokumenata, materijal za dugoročnu validaciju i pripadajuće izdate izjave arhiviraju se prema sadašnjoj Politici.

Politika kvalifikovanog elektronskog čuvanja dokumenata je nezavisna od geografske lokacije sa koje su poslati u arhivu i odakle se isčitavaju.

Usluga koja se pruža u skladu sa ovom Politikom može se koristiti samo na način opisan u ovoj Politici kvalifikovanog elektronskog čuvanja dokumenata i u Praktičnim pravilima.

1.3 PKI Učesnici

1.3.1 Sertifikaciono telo

Inception d.o.o (Pružalac usluga) je Pružalac usluga od poverenja, u okviru kojeg se Usluge od poverenja bave očuvanjem valjanosti elektronskih potpisa, elektronskih pečata, vremenskih žigova i njihovih autorskih sertifikata, opciono uključujući i očuvanje potpisanih i zapečaćenih elektronskih dokumenata.

1.3.2 Pretplatnici

Pretplatnici definišu obim korisnika koji koriste uslugu i pokrivaju naknade koje se odnose na korišćenje ovih usluga.

1.3.3 Oslanjajuće strane

Pouzdana strana nije nužno u ugovornom odnosu sa Pružaocem usluge kvalifikovanog elektronskog čuvanja dokumenata.

1.4 Administracija politike

1.4.1 Organizacija koja vrši administraciju dokumenta

Podatke organizacije koja sprovodi Politiku kvalifikovanog elektronskog čuvanja dokumenata možete pronaći ovde:

Naziv organizacije	Inception d.o.o Beograd
Adresa organizacije	Admirala Vukovića 57, Beograd, Srbija
Telefon	+381 11 2920 355
Broj faksa	+381 11 2920 355
Email adresa	office@inception.rs

1.4.2 Kontakt osoba

Pitanja u vezi sa Politikom kvalifikovanog elektronskog čuvanja dokumenata mogu se direktno postaviti sledećoj osobi:

Kontakt osoba	Jovan Vistać
Naziv organizacije	Inception d.o.o
Adresa organizacije	Admirala Vukovića 57, Belgrade, Serbia
Telefon	+381 11 2920 355
Broj faksa	+381 11 2920 355
Email adresa	office@inception.rs

1.4.3 Osoba ili organizacija odgovorna za prikladnost dokumenta Praktična pravila za kvalifikovano elektronsko čuvanja dokumenata

Pružalac koji je izdao Praktična pravila odgovoran je za njenu usklađenost sa Politikom kvalifikovanog elektronskog čuvanja dokumenata koja je navedena u njoj i za pružanje usluge u skladu sa propisima.

1.4.4 Procedure odobravanja praktičnih pravila

Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata će opisati proceduru prihvatanja Praktičnih pravila čuvanja koja objavljuje njenu usklađenost sa ovom Politikom kvalifikovanog elektronskog čuvanja dokumenata u navedenom dokumentu.u navedenom dokumentu.

1.5 Definicije i akronimi

1.5.1 Definicije

Data Centar	Objekat dizajniran za postavljanje i rad računarskih sistema i povezanih komponenti. Ove komponente obično uključuju telekomunikacione sisteme i komunikacione veze, redundantno napajanje, skladištenje podataka, klimatizaciju, zaštitu od požara i sigurnosne sisteme.
Dokaz o čuvanju	Dokazi koje su proizvedeni putem servisa za čuvanje mogu se koristiti da se pokaže da je ispunjen jedan ili više ciljeva čuvanja za dati objekat čuvanja.
Produžavanje trajanja dokaza o čuvanju	Dodavanje podataka postojećem dokazu o čuvanju radi produženja perioda važenja tog dokaza.
Cilj očuvanja	Jedan od narednih ciljeva postignutih tokom vremenskog okvira čuvanja: produženje statusa validnosti elektronskih potpisa ili pečata na duži period, pružanje dokaza o postojanju podataka tokom dugih vremenskih perioda, ili dopunjavajući eksterno obezbeđene dokaze o čuvanju.
Način čuvanja	Jedinstveni identifikovani skup detalja implementacije koji se odnosi na model za skladištenje i čuvanje i jedan ili više ciljeva čuvanja koji specificiraju kako se dokazi o čuvanju generišu i validiraju.

Šema čuvanja	Generički skup procedura i pravila koji se odnose na model za skladištenje i čuvanje i jedan ili više ciljeva čuvanja koji opisuje kako se stvaraju i potvrđuju dokazi o čuvanju.
Usluga čuvanja	Usluga od poverenja koja može da produži status važenja elektronskog potpisa ili pečata na duži vremenski period i/ili da pruži dokaze o postojanju podataka tokom dužeg vremenskog perioda.
Pružalac usluge čuvanja	Pružalac usluga od poverenja koji pruža uslugu čuvanja
Usluga od poverenja	"Označava elektronsku uslugu koja se obično pruža uz naknadu koja se sastoji od: - kreiranje, verifikacija i validacija elektronskih potpisa, elektronskih pečata ili elektronskih vremenskih žigova, elektronskih usluga registrovane dostave i sertifikata koji se odnose na te usluge, ili - kreiranje, verifikaciju i validaciju sertifikata za autentifikaciju veb stranice; ili - očuvanje elektronskih potpisa, pečata ili sertifikata koji se odnose na te usluge; " (eIDAS [1] 3. član 16. tačka)
Jedinica za posredničku sertifikaciju	Jedinica za sertifikaciju čiji sertifikat je izdat od strane druge Jedinice za sertifikaciju.
Pružalac usluga od poverenja	" Fizičko ili pravno lice koje pruža jednu ili više usluga od poverenja bilo kao

kvalifikovani ili kao nekvalifikovani pružalac usluga od poverenja." (eIDAS [1] 3. član 19. tačka)	
E-dosije	Elektronska datoteka (e-dosije) je kontejner formata elektronskog potpisa, vrsta e-dokumenta. E-dosije može da sadrži dokumente, ili povezane podatke (metapodatke), potpise, kontrapotpise i vremenske žigove.
E-dokument	E-dokument je takav dokument koji sadrži najmanje jedan elektronski potpis ili pečat u skladu sa eIDAS Uredbom. U zavisnosti od vrste e-dokumenta može sadržati dalje elektronske dokumente i odgovarajuće podatke (metapodatke), potpise, kontrapotpise i vremenske žigove.
Elektronski dokument	"Označava svaki sadržaj sačuvan u elektronskom obliku, posebno tekst ili zvučni, vizuelni ili audiovizuelni snimak " (eIDAS [1] 3. član 35. tačka)
Pretplatnik	Osoba ili organizacija koja potpisuje ugovor o usluzi sa pružaocem usluga očuvanja da bi koristila neke od njegovih usluga.
Elektronski vremenski žig	"Označava podatke u elektronskom obliku koji druge podatke u elektronskom obliku vezuju za određeno vreme čime se utvrđuje dokaz da su poslednji podaci postojali u to vreme." (eIDAS [1] 3. član 33. tačka)

Izvozno-uvozni paket	Informacija (elektronski potpisan dokument, dokaz o čuvanju, metapodaci, itd.) koja se izdaje od strane Pružaoca usluge za čuvanje i omogućava da ih uveze drugi Pružalac usluge za čuvanje radi postizanja ciljeva čuvanja.
Suspenzija	Privremena pauza važenja sertifikata pre kraja perioda važenja navedenog na sertifikatu. Suspenzija sertifikata nije konačna; validnost suspendovanog sertifikata se može vratiti.
Izvorni sertifikat	Takođe poznat kao sertifikat najvišeg nivoa. Samopotpisani sertifikat, koji izdaje posebna jedinica za sertifikaciju za sebe, koji je potpisan sopstvenim privatnim ključem, tako da može biti verifikovan sopstvenim javnim ključem – naznačeno na sertifikatu.
HSM: hardverski sigurnosni modul	Bezbedonosni uređaj zasnovan na hardveru koji generiše, čuva i štiti kriptografske ključeve i obezbeđuje bezbedno okruženje za implementaciju kriptografskih funkcija.
Sertifikaciono telo za izdavanje sertifikata	Pružalac usluga od poverenja, koji identifikuje podnosioca zahteva u okviru usluge sertifikacije, izdaje sertifikate, vodi evidenciju, prima izmene podataka u vezi sa sertifikatom i objavljuje propise koji pripadaju sertifikatu i informacije o trenutnom stanju (posebno o eventualnom opozivu) sertifikata.

Jedinica sertifikacije	Jedinica sistema pružaoca usluge čuvanja koja potpisuje sertifikate. Uvek samo jedan podatak za kreiranje sertifikata (ključ za potpisivanje, podaci za kreiranje potpisa) pripada jedinici za sertifikaciju.
Dugoročno	Vremenski period tokom kojeg tehnološke promene mogu predstavljati problem u verifikaciji validnosti elektronskog potpisa.
Kompromitovanost	Kriptografski ključ se smatra kompromitovanim, kada se može pretpostaviti da mu neovlašćena osoba ima pristup.
Nadzorni organ Pružaoca usluge od poverenja	Ministarstvo trgovine, turizma i telekomunikacija Republike Srbije, nadzorni organ koji prati rad Pružalaca usluga od poverenja.
Kvalifikovana usluga od poverenja	"Usluga od poverenja koja ispunjava primenljive zahteve propisane eIDAS uredbom." (eIDAS [1] član 3. tačka 17.
Dugoročno čuvanje	Produženje statusa važenja elektronskog potpisa ili pečata na duži vremenski period i/ili produženje pružanja dokaza o postojanju podataka u dužem vremenskom periodu,

uprkos zastarelosti kriptografska tehnologija kao što su kripto algoritmi, veličine ključeva ili heš funkcije,	kompromisi ključa ili gubitak mogućnosti da se proveri status validnosti sertifikata javnog ključa.
Upravljanje ključem	Proizvodnja kriptografskih ključeva, njihova dostava korisnicima ili njihova algoritamska implementacija, kao i registracija, skladištenje, arhiviranje, opoziv i ukidanje ključeva koji su usko povezani sa korišćenim bezbednosnim metodom.
Kvalifikovani Pružalac usluge od poverenja	" Pružalac usluga od poverenja koji pruža jednu ili više kvalifikovanih usluga od poverenja i kome je nadzorni organ dodelio kvalifikovani status." (eIDAS [1] član 3. tačka 20.)
Privatni ključ	U infrastrukturi javnog ključa, element asimetričnog kriptografskog para ključeva koji pripada vlasniku para ključeva koji subjekt treba da čuva u strogoj tajnosti. Prilikom izdavanja sertifikata, Izdavalac koristi privatne ključeve jedinice za sertifikaciju za postavljanje elektronskog potpisa ili pečata na sertifikat kako bi ga zaštitio.
Javni ključ	U infrastrukturi javnog ključa, element asimetričnog kriptografskog para ključeva koji pripada vlasniku para ključeva, koji treba da bude javno objavljen. Otkrivanje je obično u obliku sertifikata, koji povezuje ime aktera sa njegovim javnim ključem. Autentičnost

sertifikata se može proveriti javnim ključem jedinice za sertifikaciju.	
Infrastruktura javnog ključa, PKI	Infrastruktura zasnovana na asimetričnoj kriptografiji, uključujući kriptografske algoritme, ključeve, sertifikate, srodne standarde i zakone, osnovni institucionalni sistem, razne provajdere i uređaje.
Nešifrovani e-dosije	E-dosije, koji uključuje nešifrovane datoteke i elektronske potpise ili elektronske pečate na njima. U nešifrovanom e-dosijeu fajlovi i potpisi koji su pečatirani i potpisani i pečati su uključeni nešifrovani.
Organizacija	Pravno lice.
Politika usluge od poverenja	Skup pravila u kojima Pružalac usluga od poverenja, strana koja se oslanja ili druga osoba zahteva uslove za korišćenje usluge poverenja za zajednicu proverenih strana i/ili klasu aplikacija sa zajedničkim bezbednosnim zahtevima.
Vanredna operativna situacija	Vanredna situacija koja uzrokuje smetnje u radu Pružaoca usluge čuvanja, kada nastavak normalnog rada Pružaoca usluga čuvanja nije moguć ni privremeno ni trajno.
Praktična pravila Usluga od poverenja	Izjava pružaoca usluga od poverenja detaljnih procedura ili drugih operativnih zahteva koji se koriste u vezi sa pružanjem određenih usluga poverenja.

Ugovor o usluzi	Ugovor između pružaoca usluga od poverenja i klijenta usluga poverenja, koji obuhvata uslove za pružanje usluge poverenja i za korišćenje usluga.
Klijent	Pretplatnik i korisnici usluga kojima Pretplatnik daje korisnička prava.
Šifrrovan e-dosije	Ovaj e-dosije je XML datoteka koja sadrži još jedan (nešifrovani ili šifrovani) e-dosije (takođe) – šifrovan prema S/MIME specifikaciji.
Sertifikat Sertifikat elektronskog potpisa, sertifikat elektronskog pečata i sertifikat o	autentifikaciji veb lokacije, i sve one elektronske verifikacije koje je u okviru usluge poverenja izdao pružalac usluga, što uključuje podatke o verifikaciji u vezi sa sertifikatom i informacije u vezi sa korišćenjem sertifikata, i koji je kao elektronski dokument pouzdano zaštićen od raspoloživih tehnologija falsifikovanja u trenutku izdavanja i tokom roka važenja.
Repozitorijum sertifikata	Repozitorijum podataka koji sadrži različite sertifikate. Sertifikaciono telo ima Repozitorijum sertifikata u kome se obelodanjuju izdati sertifikati, ali sistem koji sadrži sertifikate dostupne aplikaciji na računaru Oslanjajuće strane se takođe naziva Repozitorijum sertifikata.
Opoziv	Prestanak važenja sertifikata pre iste ka roka važenja navedenog na sertifikatu. Opoziv sertifikata je trajan, opozvani sertifikat se više ne može vratiti.

Zapisi o statusu opoziva	Interna evidencija suspendovanih i opozvanih sertifikata koja uključuje činjenicu suspenzije ili opoziva i vreme suspenzije ili opoziva dato u sekundama koju vodi Sertifikaciono telo.

1.5.2 Akronimi

eIDAS	Elektronska identifikacija, autentifikacija i potpis
LDAP	Lightweight Directory Access Protocol
MTT	Ministarstvo trgovine, turizma i telekomunikacija Republike Srbije
OCSP	Online protokol statusa sertifikata
OID	Identifikator dokumenta
PKI	Infrastruktura javnog ključa
TSP	Pružalac usluga od poverenja

2 Objavljivanje i obaveze

2.1 Repozitorijumi

Pružalac usluga čuvanja će objaviti ugovorne uslove i politike elektronskim putem na svojoj veb stranici.

Radna verzija novih dokumenata koji se uvode biće objavljena na internet stranici 30 dana pre stupanja na snagu.

Dokumenti koji su na snazi biće dostupni na sajtu kao dodatak svim prethodnim verzijama svih dokumenata.

Stvarna verzija politika i ugovornih uslova biće čitljiva u korisničkom odeljku Pružaoca usluge čuvanja.

Nakon zaključenja ugovora, Pružalac usluga čuvanja će učiniti pojedinačni Ugovor o usluzi, Opšte uslove, Izjavu o otkrivanju podataka(Disclosure Statement), Politiku čuvanja i Praktična pravila čuvanja dostupnim Klijentu na trajnom mediju, ili na način koji može biti preuzeto od strane Klijenta.

Pružalac usluge čuvanja obaveštava svoje Klijente o promeni Opštih uslova.

2.2 Vreme ili učestalost objavljivanja

2.2.1 Učestalost objavljivanja Opštih uslova

Najvažniji uslovi za pružanje usluge sadržani su u ugovoru o uslugama koji Klijent potpisuje prilikom zaključenja ugovora.

Pružalac usluge čuvanja pregleda Opšte uslove godišnje ili u slučaju vanrednog zahteva za promenu sa prioritetom i vrši neophodne izmene.

Dokument će i nakon najmanje izmene dobiti novi broj verzije, a uzimajući u obzir vreme potrebno za proces odobravanja, odrediće se i planirani datum stupanja na snagu.

Prihvaćeni dokument biće objavljen na veb stranici Pružaoca usluga očuvanja i biće poslat na uvid Ministarstvu trgovine, turizma i telekomunikacija 30 dana pre stupanja na snagu planiranog unosa.

Pružalac usluge čuvanja će prihvatiti komentare u vezi sa Opštim uslovima i odredbama objavljenim 14 dana pre njihovog stupanja na snagu, na kontakt podatke definisane u odeljku 1.4.1.

U slučaju zapažanja koja zahtevaju suštinske izmene, dokument će biti izmenjen. Pružalac usluge čuvanja će zatvoriti i objaviti verziju Opštih uslova sa izmenama i dopunama 7. dan pre stupanja na snagu.

3 Elektronski servis za čuvanje

U okviru usluge elektronskog čuvanja moraju se obezbediti sledeći zadaci:

- Pretplatnik može da otpremi heš i metapodatke elektronski potpisanih e-dokumenata u arhivu kojom upravlja Pružalac usluga čuvanja. Prilikom prijema heš i metapodataka e-dokumenta, Pružalac usluge čuvanja proverava elektronski potpis(e) ili pečat(e) na predmetu očuvanja, kompletira ili sastavlja dokaze o očuvanju, stavlja vremensku oznaku elektronske arhive na dokaz o očuvanju, i čuva heš i metapodatke e-dokumenta. (videti odeljak 3.2).

- Pružalac usluge čuvanja bezbedno čuva prihvaćeni objekat čuvanja – heš, metapodatke i dokaze o očuvanju e-dokumenta – i obezbeđuje tokom celog perioda čuvanja da:

  – samo ovlašćena lica imaju pristup sačuvanim podacima;

  – ovlašćeni Pretplatnik ima neprekidan pristup sačuvanim podacima;

  – sačuvani podaci se ne mogu menjati ili brisati bez ovlašćenja.

- Pružalac usluge čuvanja obezbeđuje dugoročnu validnost elektronskih potpisa i pečata koji se stavljaju na e-dokumente i čuvaju u objektu čuvanja. Period čuvanja je neograničen (očuvanje dokaza o čuvanju je trajno), osim ako ugovor o usluzi prestane pre isteka ovog perioda (za detalje pogledajte odeljak 4).

- Pretplatnik ima kontinuiran pristup odgovarajućim dokazima o očuvanju i može ih preuzeti (pogledajte odeljak 3.3).

- Na zahtev Pretplatnika Pružalac usluge čuvanja izdaje autentičnu potvrdu da čuva objekat čuvanja (heš i metapodatke e-dokumenta), te da u trenutku prijema u arhivu elektronski potpisi ili pečati u metapodacima dokumenta su bili validni (pogledajte odeljak 3.4).

Primarni zadatak službe dugoročnog čuvanja je očuvanje valjanosti elektronskog potpisa ili pečata stavljenog na elektronski dokument. Pružalac usluge čuvanja može pretplatniku da pruži i druge usluge osim pružanja osnovnog zadatka, npr.:

- očuvanje metapodataka elektronskog dokumenta elektronskim potpisom ili pečatom,

- obavljanje konverzija formata datoteka koje postanu neophodne.

Ova politika čuvanja definiše uslove za dugoročnu garanciju validnosti elektronskih potpisa i pečata, tako da ne omogućava prihvatanje i čuvanje predmeta zaštite bez ikakvog elektronskog potpisa ili pečata.

Pružalac usluga čuvanja može specifikovati i ograničiti u Praktičnim pravilima čuvanja format prihvaćenih elektronskih potpisa ili pečata, prihvaćenih sertifikacionih tela i bilo kog drugog parametra.

3.1 Zaključivanje Ugovora o uslugama

Pre korišćenja usluge, Pretplatnik će zaključiti ugovor o usluzi sa Pružaocem usluge čuvanja.

Praktična pravila o praksi čuvanja i drugi propisi navedeni u njoj će jasno odrediti detalje usluge koja će se pružiti i alate potrebne za korišćenje usluge.

3.2 Učitavanje objekta za očuvanje

1. Pružalac usluge čuvanja prihvata samo da se objekat čuvanja arhivira nakon identifikacije Pretplatnika u okviru bezbedne procedure. Postupkom se obezbeđuje integritet, poverljivost predmeta zaštite.

   Valjanost elektronskog potpisa ili pečata na primljenom predmetu čuvanja će se proveriti korišćenjem kompletnog dokaza o očuvanju. Verifikacija se može zasnivati na delimičnom ili potpunom dokazu o očuvanju koji je priložen uz elektronski potpis(e) ili pečat(e). Sve informacije koje su još neophodne za validaciju će prikupiti Pružalac usluge čuvanja i sačuvaće one povezane sa objektom čuvanja. Nakon prikupljanja dokaza o čuvanju, Pružalac usluga čuvanja će staviti kvalifikovanu arhivsku vremensku oznaku na svaki dokaz o čuvanju.

2. Pružalac usluge čuvanja će u najkraćem mogućem roku, a najkasnije u roku od 3 dana od prijema, verifikovati primljeni predmet konzervacije i poslati potvrdu Pretplatniku da je dokaz o očuvanju uspešno sastavljen, te da je prihvatio heš e-dokumenta i metapodatke. Ako je proces negde prekinut, Pružalac usluge čuvanja će obavestiti Pretplatnika porukom o grešci. Na osnovu poruke o grešci mora se jasno identifikovati koji e-dokument je u pitanju i koji je razlog odbijanja.

   Ukoliko potvrda o prihvatanju predmeta čuvanja ne stigne Pretplatniku u navedenom roku, smatraće se da Pružalac usluge čuvanja nije prihvatio heš i metapodatke e-dokumenta. Pružalac usluge čuvanja je isključivo odgovoran za čuvanje predmeta čuvanja i za osiguranje verodostojnosti uključenih elektronskih potpisa i pečata u slučaju slanja pozitivne potvrde.

3.3 Obezbeđivanje materijala za validaciju/Dostupnost dokaza o čuvanju – preuzimanje dokaza o čuvanju

Pružalac usluge čuvanja će obezbediti da Pretplatnik može da preuzme svoj dokaz o čuvanju tokom perioda važenja ugovora o usluzi.

1. Pretplatnik ima pristup samo dokazima o čuvanju, koji se čuvaju u arhivi Pružaoca usluge čuvanja, preko bezbednog kanala.

2. Pružalac usluga čuvanja će obezbediti da svaki Pretplatnik ima pristup samo dokazima o čuvanju na koje zaista ima pravo da pristupi.

3.4 Izdavanje potvrde

Na zahtev Pretplatnika, Pružalac usluge čuvanja izdaje potvrdu u vezi sa objektom čuvanja. Potvrda se sastoji u sledećem:

1. Izjava da su napredni ili kvalifikovani elektronski potpisi, pečati, vremenski žigovi na datom objektu čuvanja i odgovarajući sertifikati bili važeći u vreme stavljanja vremenskog žiga i validacije nakon njihovog učitavanja.

2. Heš e-dokumenta, naziv i identifikator Pretplatnika.

3. Izjava da dati objekat čuvanja ima dati heš, pa je identičan e-dokumentu sa istim hešom koji je Pretplatnik predstavio, ili kreiran uz pomoć Pružaoca usluge čuvanja.

4. Vreme prijema predmeta zaštite u arhivu.

Pružalac usluge čuvanja izdaje potvrdu na papiru ili u e-dosijeu sa kvalifikovanim elektronskim potpisom. Potvrdu kreira službeno lice odgovorno za izdavanje arhivske potvrde i stavlja svoj kvalifikovani elektronski potpis i kvalifikovani vremenski žig.

Za izdavanje potvrde nije potrebno poznavanje arhiviranog objekta čuvanja, ono se izdaje na osnovu heša nešifrovanog e-dokumenta koji će biti sačuvan u objektu čuvanja. Iz heš vrednosti se ne mogu dobiti nikakve informacije u vezi sa sadržajem elektronskog dokumenta.

Izdavanje potvrde može se desiti na način da Pretplatnik pruži Pružaocu usluge čuvanja heš e-dokumenta. Zatim, pod uslovom da arhiva Pružaoca usluge čuvanja sadrži objekat čuvanja sa istim hešom kao i predstavljeni e-dokument, službeno lice Pružaoca usluge čuvanja izdaje potvrdu u vezi sa predstavljenim objektom čuvanja.

Izdavanje potvrde može zahtevati ovlašćeni predstavnik Pretplatnika ako je prethodno predočio ovlašćenje Pretplatnika u dokumentu koji sadrži i njegov potpis.

3.5 Raskid ugovora o usluzi

U slučaju raskida ugovora, Pružalac usluge čuvanja će učiniti dostupnim dokaze o čuvanju koje je Pretplatnik kreirao, kao i da mu se omogući preuzimanje, Pretplatniku ili drugom ovlašćenom licu.
Nakon isteka roka, Pretplatnik neće moći da pristupi dokazima o čuvanju i podacima koji odgovaraju objektu očuvanja Pretplatnika.

4 Tehničke mere bezbednosti

4.1 Sigurnosne garancije

Pružalac usluga očuvanja koristi pouzdane sisteme i proizvode zaštićene od modifikacija. Za pružanje svojih usluga koristi jedinstven IT sistem koji se sastoji od pouzdanih, tehnički procenjenih i sertifikovanih bezbednosnih proizvoda.
Pružalac usluga čuvanja koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih modifikacija.

Ako Pružalac usluge čuvanja koristi uslugu od poverenja treće strane, on će proveriti da li je ta treća strana u skladu sa svim neophodnim zahtevima.

Pružalac usluga čuvanja čuva arhivirane objekte zaštite u fizički zaštićenom okruženju, u skladu sa fizičkim i proceduralnim zahtevima opisanim u odeljku 5, čiju bezbednost garantuju politike unutrašnje bezbednosti i redovne unutrašnje i eksterne bezbednosne revizije. Pružalac usluge čuvanja predaje objekte očuvanja trećoj strani (npr. organu) samo ako ga pretplatnik za to ovlasti ili kada je to propisano zakonom.

Integritet uskladištenih e-dosijea obezbeđen je fizičkom zaštitom e-dosijea, kao i tehnologijama vezanim za elektronske potpise. Dostupnost objekata zaštite obezbeđena je kvalitetnim sistemom Pružaoca usluga očuvanja i internim propisima koji regulišu sistem, procedurama za kontinuitet poslovanja i upravljanjem vanrednim situacijama i drugim procedurama za upravljanje vanrednim situacijama.
Pružalac usluga očuvanja čuva arhivirane objekte zaštite na dve fizičke lokacije udaljene jedna od druge.

Pružalac usluge očuvanja kreira ključeve za potpisivanje koji se koriste u potvrdama, ključeve koji se koriste za šifrovanje/dešifrovanje objekata očuvanja i infrastrukturnih i sistemskih kontrolnih ključeva u kriptografskom hardverskom uređaju. Pružalac usluga očuvanja periodično menja ove ključeve. Pružalac usluge čuvanja prati razvoj tehnologije i ukoliko otkrije da ključ više nije bezbedan ili da algoritam više nije upotrebljiv prema odluci Ministarstva trgovine, turizma i telekomunikacija Republike Srbije, odmah zamenjuje pogođeni ključ ili ključeve.

Pružalac usluga čuvanja čuva objekte čuvanja u šifrovanim e-dosijeima. Pružalac usluge čuvanja šifruje objekte očuvanja koristeći algoritam koji se smatra bezbednim u datom stanju tehnologije. Ako je bezbednost ovog algoritma ugrožena tokom razvoja tehnologije, Provajder usluga očuvanja obezbeđuje ponovno šifrovanje objekta očuvanja pomoću bezbednog algoritma zasnovanog na sopstvenim internim propisima.

4.2 Mere predostrožnosti za računarsku bezbednost

Pružalac usluga očuvanja koristi pouzdane IT sisteme i rešenja, tehnologije i razvio je redundantni sistem. Dve instance rade za sve kritične komponente sistema pružalaca usluga, a u slučaju kvara bilo koje od tih jedinica, druga jedinica preuzima operaciju.

IT sistem pružaoca usluga očuvanja zaštićen je višestepenim zaštitnim zidom. Svaki zaštitni zid ima dve kopije, u slučaju kvara jedinice druga instanca iste jedinice preuzima njenu funkciju koristeći klaster.

4.3 Tehničke mere predostrožnosti vezane za životni ciklus

Da bi se ispunio visok nivo bezbednosnih zahteva u svim projektima razvoja sistema Pružaoca usluga čuvanja, povišeni zahtevi će se uzeti u obzir u celokupnom procesu razvoja (čak i u fazi planiranja i definisanja zahteva).

Proizvodi koji se koriste za pružanje usluga primenjuju se uzimajući u obzir bezbednosna pitanja vezana za životni ciklus.

4.4 Redovna sertifikacija

Pružalac usluga čuvanja je obavezan da stavi vremenski žig koji je izdao kvalifikovani provajder ili da stavi vremenski pečat na materijal za dugoročnu validaciju u sledećim slučajevima:

- ukoliko Ministarstvo trgovine, turizma i telekomunikacija donese takvu odluku;
- nakon obaveznog dostavljanja obaveštenja Ministarstvu trgovine, turizma i telekomunikacija o pokretanju postupka raspuštanja ili izricanju likvidacije Pružaoca usluga očuvanja.

4.5 Ponovno šifrovanje arhive

Arhivirani objekti čuvanja čuvaju se šifrovani u arhivi. Osigurava se da su arhivirani objekti čuvanja šifrovani algoritmom za šifrovanje koji je siguran u svakom trenutku. Objekti očuvanja će biti ponovo šifrovani, ako:

- algoritam koji se koristi za šifrovanje gubi poverenje – u ovom slučaju treba ga ponovo šifrovati algoritmom koji se smatra bezbednim u vreme šifrovanja;

- kompromitovana je poverljivost ključa za dekodiranje pružalaca usluge čuvanja;
- Praktična pravila čuvanja ili ugovor zaključen sa Pretplatnikom to zahteva.

Nakon ponovnog šifriranja arhiviranih objekata čuvanja, prethodne kopije šifrovane na način koji se smatra nedovoljno bezbednim biće uništene.

4.6 Kontinuirano praćenje tehnologije

Pružalac usluga čuvanja će kontinuirano pratiti razvoj tehnologije u vezi sa elektronskim potpisom i kriptografijom. Ukoliko Pružalac usluge čuvanja sazna da kriptografski algoritam sa datim parametrom koji je prihvaćen rešenjem Ministarstva trgovine, turizma i telekomunikacija Republike Srbije više nije bezbedan, o tome će obavestiti Ministarstvo trgovine, turizma i telekomunikacija. i zahtevati reviziju odluke u vezi sa kriptografskim algoritmima. Pružalac usluge čuvanja može u bilo kom trenutku da odluči da promeni korišćene skupove kriptografskih algoritama i njihove parametre u slučaju da je algoritam i parametar prihvaćen rešenjem Ministarstva trgovine, turizma i telekomunikacija.

4.7 Prihvatanje sertifikata i vremenskog žiga Pružalaca usluga

Pružalac usluga očuvanja može da navede pod kojim uslovima prihvata sertifikate datog sertifikacionog tela i koja tela za sertifikaciju prihvata, zajedno sa kriterijumima za to da sertifikaciona tela budu uključena u ovu listu ili da budu isključeni sa nje u okviru usluga dugoročnog očuvanja.

4.8 Dostupnost određenih elemenata usluge elektronskog čuvanja

Godišnja dostupnost sledećih elemenata elektronske usluge dugoročnog čuvanja je 99,7%, a povremeni prekidi usluge ne smeju biti duži od 1 dana:

- elektronsko preuzimanje arhiviranih dokaza o čuvanju i lanaca validnosti;
- pretraga arhiviranih objekata zaštite;
- primanje zahteva za brisanje;
- traženje informacija o statusu prethodno poslatih zahteva.

Pružalac usluge čuvanja ima pravo da suspenduje uslugu otpremanja objekata za čuvanje.

5 Objekti, upravljanje i operativne kontrole

Pružalac usluga čuvanja će primeniti fizičke, proceduralne i mere bezbednosti osoblja koje su u skladu sa priznatim standardima, zajedno sa administrativnim i upravnim procedurama koje ih primenjuju.

Pružalac usluga čuvanja vodi evidenciju o sistemskim jedinicama i resursima koji se odnose na pružanje usluga i vrši procenu rizika za njih. Koristiće zaštitne mere proporcionalne rizicima u vezi sa pojedinačnim elementima.

Pružalac usluge čuvanja će pratiti zahteve za kapacitetom i obezbediće da su adekvatna procesorska snaga i skladištenje dostupni za pružanje usluge.

5.1 Fizičke kontrole

Pružalac usluga čuvanja će se pobrinuti da fizički pristup kritičnim uslugama bude kontrolisan i da će fizički rizik imovine u vezi sa kritičnim uslugama držati na minimumu. Svrha fizičkih mera predostrožnosti je sprečavanje nezakonitog pristupa, oštećenja i neovlašćenog pristupa informacijama i fizičkim zonama Pružalaca usluge očuvanja.

Usluge koje obrađuju kritične i osetljive informacije biće implementirane na bezbednim lokacijama. Obezbeđena zaštita biće proporcionalna identifikovanim pretnjama analize rizika koju je izvršio Pružalac usluge očuvanja.

5.1.1 Lokacija i izgradnja

IT sistem Pružaoca usluga čuvanja biće lociran i funkcionisan u okviru propisno obezbeđenog Data centra sa fizičkom i logičkom zaštitom koja sprečava nelegitimne pristupe. Odbrambena rešenja – na primer zaštita, sigurnosne brave, sistemi za detekciju upada, sistem video nadzora, sistem kontrole pristupa – primenjivaće se tokom lociranja i uspostavljanja Data centara koji su međusobno izgrađeni i međusobno zavisni i zajedno pružaju moćan sistem zaštite IT sistema koji učestvuju u pružanju usluga, kao i za očuvanje poverljivih podataka koje čuva pružalac.

5.1.2 Fizičku pristup

Pružalac usluga čuvanja štiti uređaje i opremu koji učestvuju u pružanju usluge od neovlašćenog fizičkog pristupa kako bi sprečio neovlašćeno korišćenje uređaja.

Pružalac usluga očuvanja će obezbediti da:

- svaki ulazak u data centar bude registrovan;
- ulazak u Data centar može se desiti samo nakon istovremene identifikacije dva ovlašćena člana osoblja sa poverenim ulogama – a najmanje jedan od članova osoblja treba da bude administrator sistema;
- lica bez nezavisnog ovlašćenja mogu boraviti u Data centru samo u opravdanim slučajevima, u pratnji osoblja sa odgovarajućim pravima;
- Dnevnici unosa će se arhivirati kontinuirano i evaluirati sedmično.

Aktivacioni podaci (lozinke, PIN kodovi) uređaja ne smeju se otvoreno čuvati čak ni u Data centru.

U prisustvu neovlašćenih lica:

- mediji sa podacima koji sadrže osetljive informacije treba da budu fizički van domašaja;
- prijavljeni terminali ne smeju ostati bez nadzora;
- ne bi trebalo da se sprovodi nijedan radni proces tokom kojeg se mogu otkriti poverljive informacije.

Prilikom napuštanja server sobe administrator će proveriti sledeće:

- svaka oprema Data centra je u adekvatno bezbednom radnom stanju;
- Nijedan korisnik nije ostao prijavljen;
- Fizički uređaji za skladištenje su pravilno zaključani;
- Sistemi, uređaji koji pružaju fizičku zaštitu rade ispravno;
- Alarmni sistem je aktiviran.

Trebalo bi da budu imenovani odgovorni ljudi koji će vršiti redovne procene fizičke bezbednosti. Rezultati ispitivanja se upisuju u odgovarajuće evidencije.

5.1.3 Napajanje i klimatizacija

Pružalac usluge čuvanja će u Data centru primeniti jedinicu za neprekidno napajanje koja:

- ima adekvatan kapacitet da obezbedi napajanje za IT sisteme i sisteme pomoćnih objekata Data centra;

  štiti IT opremu od fluktuacija napona u spoljnoj mreži, nestanka struje, naponskih skokova i drugo;

- u slučaju trajnog nestanka struje ima sopstvenu opremu za proizvodnju električne energije, koja je – omogućavanjem dopune – u stanju da obezbedi neophodnu energiju za bilo koji vremenski period.

Vazduh iz spoljašnje sredine ne sme da ulazi direktno u Data centar. Čistoća vazduha u Data centru će biti obezbeđena adekvatnim sistemom filtera za otkrivanje raznih zagađivača iz vazduh (prašina, zagađivači i korozivni materijali, toksične ili zapaljive materije). Ventilacioni sistem treba da obezbedi neophodnu količinu svežeg vazduha sa odgovarajućom filtracijom za bezbede uslove rada operatera. Vlažnost treba smanjiti na nivo koji zahtevaju IT sistemi. Sistemi za hlađenje sa odgovarajućim performansama treba da se koriste da bi se obezbedio neophodnu radnu temperaturu, kako bi se sprečilo pregrevanje IT uređaja.

5.1.4 Izloženost vodi

Data centar pružaoca usluga čuvanja mora biti adekvatno zaštićen od prodora vode i poplava.

5.1.5 Prevencija i zaštita od požara

Detektori dima i požara biće instalirani u Data centru pružaoca usluga čuvanja koji automatski upozoravaju vatrogasnu jedinicu. Ručne aparate za gašenje požara odgovarajuće vrste i količine u skladu sa relevantnim propisima treba postaviti na vidno mesto u svakoj prostoriji.
U Data centru se primenjuju automatski aparati za gašenje požara.

5.1.6 Skladištenje medija

Pružalac usluge čuvanja će zaštititi svoja skladišta medija od neovlašćenog pristupa i slučajnog oštećenja. Svi revizijski i arhivski podaci kreiraju se kao duplikati. Dve kopije treba da se čuvaju odvojeno jedna od druge fizički, na lokacijama na bezbednoj udaljenosti jedna od druge. Skladišteni mediji moraju biti zaštićeni od štetnih uticaja okoline kao što su niske ili visoke temperature, prljavština, vlaga, sunčeva svetlost, jaka magnetna polja, jako zračenje.

5.1.7 Odlaganje otpada

Pružalac usluge čuvanja će se pobrinuti za uništavanje svojih uređaja, kada skladišta medija postaju suvišna u skladu sa ekološkim propisima. Takvi uređaji i skladišta medija biće trajno obrisani ili neupotrebljivi u skladu sa široko prihvaćenim metodama pod ličnim nadzorom zaposlenih pružaoca usluge čuvanja..

5.1.8 Bekap van lokacije

Pružalac usluge čuvanja će sedmično kreirati rezervnu kopiju iz koje bi se cela usluga mogla vratiti u slučaju fatalne greške. Rezervne kopije – barem uključujući poslednju potpunu rezervnu kopiju – biće uskladištene na spoljnoj lokaciji čija je fizička i operativna zaštita identična primarnoj lokaciji. Bezbedan prenos podataka sa primarnih na rezervne lokacije će biti rešen. Na osnovu nasumično odabranih rezervnih podataka, test vraćanja podataka će se raditi najmanje jednom godišnje. Glavne okolnosti i rezultati testa vraćanja podataka biće zabeleženi u izveštaju revizije.

5.2 Proceduralne kontrole

Pružalac usluga čuvanja će se pobrinuti da njegovi sistemi rade bezbedno, u skladu sa pravilima i sa minimalnim rizikom od kvarova. Proceduralne mere predostrožnosti imaju za cilj da dopune i u isto vreme pojačaju delotvornost fizičkih zaštitnih mera, zajedno sa onima koje se primenjuju na osoblje, putem imenovanja i izolovanja pouzdanih uloga, dokumentovanje odgovornosti različitih uloga, kao i preciziranje broja zaposlenih i uloga isključivanja neophodnih za različite zadatke, štaviše identifikacija i autentifikacija koja se očekuje u različitim ulogama.

Interni sistem upravljanja Pružaoca usluga čuvanja osigurava da je njegov rad u skladu sa zakonskim, kao i internim propisima. U njegovom sistemu će za svaku datu sistemsku jedinicu i proces jasno biti određena odgovorna osoba.

Pojedinci odgovorni za dati element sistema ili proces biće nedvosmisleno dodeljeni svakom elementu sistema i svakom procesu u njegovom sistemu. Zadaci vezani za razvoj i operacije oštro su razdvojeni u sistemu pružaoca usluga čuvanja. Revizijska aktivnost nezavisnog revizora sistema i internog revizora pružaoca usluga očuvanja obezbeđuje odgovarajući rad sistema.

5.2.1 Uloge od poverenja

Pružalac usluge čuvanja će stvoriti uloge od poverenja za obavljanje svojih zadataka. Prava i funkcije će biti podeljene među različitim ulogama na način da jedan korisnik sam ne može da zaobiđe mere bezbednosti.
Pouzdane uloge koje treba primeniti:

- Menadžer implementacije za IT sistem pružaoca;
- službenik za obezbeđenje: osoba sa opštom odgovornošću za bezbednost usluge;
- sistemski administrator: pojedinac koji obavlja instalaciju, konfiguraciju IT sistema i održavanje
- operater: pojedinac koji obavlja kontinuirani rad IT sistema, pravljenje rezervnih kopija i vraćanje u prethodno stanje;
- nezavisni revizor sistema: lice koje vrši reviziju evidentiranog, kao i arhiviranog skupa podataka provajdera, odgovorno za proveru sprovođenja kontrolnih mera koje provajder sprovodi u interesu poslovanja u skladu sa propisima, štaviše za kontinuiranu reviziju i praćenje postojećih procedura.
- službenik za čuvanje: moguće je dešifrovati objekat za čuvanje uz saradnju dva službenika za trajno čuvanje. Službenici za trajno čuvanje odgovorni su za bezbedno upravljanje dešifrovanim objektom za čuvanje i za njegovo uništenje.
- službenik odgovoran za izdavanje izjave o trajnom čuvanju: njegova dužnost je izdavanje i overa izjava o trajnom čuvanju.

Za obezbeđivanje uloga od poverenja, menadžer odgovoran za bezbednost Pružaoca usluge čuvanja će formalno imenovati zaposlene Pružaoca usluga čuvanja. Samo osobe koje su u radnom odnosu sa pružaocem usluga mogu imati ulogu od. Uloge od poverenja se neće obavljati u kontekstu ugovora o delu. Vodiće se ažurna evidencija o poverenim ulogama I u slučaju bilo kakve promene, Ministarstvo trgovine, turizma i telekomunikacija biće obavešteno bez odlaganja.

5.2.2 Broj potrebnih osoba po zadatku

Bezbednosnim i operativnim propisima Pružaoca usluga čuvanja će biti definisano da se sledeći poslovi mogu obavljati samo u zaštićenom okruženju, uz istovremeno prisustvo dva zaposlena u poverenim ulogama:

- generisanje sopstvenog para ključeva servisa Pružaoca usluge čuvanja;

- rezervna kopija privatnog ključa Pružaoca;
- aktiviranje privatnog ključa Pružaoca;
- uništavanje privatnog ključa Pružaoca.

Najmanje jedno od lica koja obavljaju gore navedene procedure mora biti administrator sistema, a drugo lice ne može biti nezavisni revizor sistema.
Saradnja dva službenika za zaštitu je neophodna za dešifrovanje šifrovanog objekta čuvanja koji se čuva u arhivi. Službenici za čuvanje odgovorni su za bezbedno upravljanje dešifrovanim objektom zaštite i za njegovo uništenje.

U toku sprovođenja navedenih radnji neovlašćeno lice ne sme biti prisutno u prostoriji.

5.2.3 Identifikacija i autentifikacija za svaku ulogu

Korisnici koji upravljaju IT sistemom Pružaoca usluga čuvanja moraju imati jedinstvene identifikacione podatke, koji omogućavaju sigurnu identifikaciju i autentifikaciju korisnika. Korisnici mogu pristupiti IT sistemima koji su kritični sa aspekta pružanja usluge sertifikacije tek nakon identifikacije i autentifikacije.
Podaci za identifikaciju i autentifikaciju će se bez odlaganja opozvati u slučaju prestanka prava korisnika.

5.2.4 Uloge koje zahtevaju razdvajanje dužnosti

Zaposleni u pružaocu usluga čuvanja mogu imati više pouzdanih uloga u isto vreme, ali je pružalac usluge čuvanja obavezan da obezbedi da:

- službenik za bezbednost i službenik za registraciju neće imati ulogu nezavisnog revizora sistema;
- administrator sistema neće imati ulogu službenika za bezbednost i nezavisnog revizora sistema;
- menadžer sa opštom odgovornošću za IT sistem neće imati ulogu službenika za bezbednost i nezavisnog revizora sistema.

5.3 Kontrola zaposlenih

Pružalac usluga čuvanja će se pobrinuti da njegova kadrovska politika i njegove prakse primenljive na zapošljavanje članova osoblja intenziviraju i podržavaju pouzdanost rada Pružaoca usluge čuvanja.
Cilj mera predostrožnosti koje se primenjuju na osoblje je smanjenje rizika od ljudskih grešaka, krađe, prevare i slučajeva zloupotrebe.
Pružalac usluga čuvanja će se pozabaviti bezbednošću osoblja već tokom faze zapošljavanja, uključujući zaključivanje ugovora, kao i njihovu validaciju kada su zaposleni. U slučaju svih uloga od poverenja, kandidati će imati važeće uverenje o neosuđivanosti u vreme podnošenja prijave. Svaki zaposleni u ulozi od poverenja i spoljne strane koje stupe u kontakt sa uslugama Pružaoca usluge čuvanja potpisaće ugovor o neotkrivanju podataka. Istovremeno, Pružalac usluga čuvanja će svojim zaposlenima obezbediti sticanje i dalje razvijanje zajedničkog, opšteg znanja uz specijalizovana stručna znanja neophodna za obavljanje različitih poslova.

5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje

Svaki zaposleni u Pružaocu usluga čuvanja mora imati potrebno obrazovanje, praksu i profesionalno iskustvo za pružanje aktivnosti unutar svog delokruga.

Pouzdane uloge kod Pružaoca usluge čuvanja mogu obavljati samo osobe koje nemaju spoljni uticaj i poseduju neophodnu stručnost potvrđenu od strane Pružaoca usluga čuvanja. Svo osoblje u pouzdanim ulogama neće biti u sukobu interesa koji bi mogao ugroziti nepristrasnost operacija Pružaoca usluge čuvanja.

Menadžer sa ukupnom odgovornošću za IT sistem može biti samo osoba koja ima:

- specijalizovanu (matematika, informacione tehnologije) višu ili fakultetsku diplomu ili višu/visoku diplomu stečenu na inženjerskom odseku iz oblasti tehničkih nauka);

- najmanje tri godine stručnosti u profesionalnom radnom iskustvu u vezi sa informacionom bezbednošću.

5.3.2 Procedure provere zaposlenih

Pružalac usluga čuvanja će angažovati samo zaposlene za pouzdane ili vodeće uloge, koji

- imaju čist dosije i protiv kojih nije u toku nikakav postupak koji bi mogao uticati na nekažnjivost.

- ne podležu profesionalnim diskvalifikacijama koje zabranjuju korišćenje usluga u vezi sa elektronskim potpisom.

Da li će u vreme imenovanja, nosilac vodeće uloge, zaposleni kod Pružaoca usluge čuvanja izjavom, sa potvrdom o dobrom ponašanju ne starijom od 6 meseci, opravdati čist krivični dosije.

Pružalac usluga čuvanja će potvrditi autentičnost relevantnih informacija navedenih u biografiji kandidata tokom procesa zapošljavanja, kao što su prethodno zaposlenje, profesionalne reference i najrelevantnije obrazovanje.

5.3.3 Zahtevi za obuku

Pružalac usluga čuvanja će obučiti novoprimljene zaposlene, tokom koje stiču

- osnovno PKI znanje;
- specifičnosti i način rukovanja IT sistemom Pružaoca usluga čuvanja;
- neophodna posebna znanja za obavljanje njihovog delokruga;
- procesi i procedure definisane u javnom i internim propisima Pružaoca usluge čuvanja;
- pravne posledice pojedinačnih aktivnosti;
- primenljive IT bezbednosne propise u meri u kojoj je to neophodno za specifičan obim aktivnosti;
- pravila o zaštiti podataka.

Samo zaposleni koji su prošli obuku dobijaju pristup proizvodnom IT sistemu Pružaoca usluge čuvanja.

5.3.4 Učestalost i uslovi prekvalifikacije

Pružalac usluge čuvanja će obezbediti da zaposleni stalno poseduju potrebna znanja, pa će se po potrebi održati dodatna ili ponavljajuća obuka.
Dalja obuka će se održati ako dođe do promene u procesima ili IT sistemu Pružaoca usluge čuvanja.
Obuka mora biti adekvatno dokumentovana, iz čega se može jasno odrediti nastavni plan i obim zaposlenih učesnika.

5.3.5 Učestalost i redosled rotacije poslova

Bez uslova.

5.3.6 Sankcije za nedozvoljene radnje

Pružalac usluge čuvanja će ugovorom o radu regulisati mogućnosti gonjenja zaposlenih u slučaju propusta, grešaka, slučajnog ili namernog oštećenja.
Ukoliko zaposleni – zbog nemara ili namerno – prekrši svoje obaveze, protiv njega može biti izrečena sankcija od strane Pružaoca usluge čuvanja, koje on odredi s obzirom na prekršaj i posledice. Sankcije mogu uključivati disciplinski postupak, razrešenje, opoziv imenovanja, krivičnu odgovornost.

5.3.7 Zahtevi nezavisnog izvođača

Na radnike zaposlene na ugovor o delu primenjuju se ista pravila kao i na zaposlene.

Nosilac uloge od poverenja mora biti u radnom odnosu sa Pružaocem usluga čuvanja.

5.3.8 Dokumentacija dostavljena osoblju

Pružalac usluge čuvanja će kontinuirano obezbeđivati zaposlenima dostupnost aktuelne dokumentacije i propisa neophodnih za obavljanje njihove uloge.

5.4 Procedure evidentiranja revizije

Da bi održao bezbedno IT okruženje, Pružalac usluge očuvanja će implementirati i upravljati sistemom za beleženje događaja i kontrolnim sistemom koji pokriva njegov kompletan IT sistem.

5.4.1 Vrste evidentiranih događaja

Pružalac usluge čuvanja će evidentirati svaki događaj u vezi sa bezbednošću koji može da pruži informacije o događajima, promenama koje se dešavaju u IT sistemu ili u njegovom fizičkom okruženju u skladu sa opšteprihvaćenom praksom bezbednosti informacija. U slučaju svakog unosa u dnevnik, biće sačuvani sledeći podaci:

- vreme događaja;
- vrsta događaja;
- identifikacija korisnika ili sistema koji/šta je pokrenulo događaj;
- uspeh ili neuspeh revidovanog događaja.

Revizorski zapisi se ne smeju menjati ili brisati.
Svi bitni dnevnici događaja biće dostupni nezavisnim revizorima sistema, koji ispituju usklađenost rada Pružaoca usluge čuvanja.

Naredne događaje trebalo bi logovati na minimum:

- Interni sat

- sinhronizaciju internog sata sa UTC vremenom, uključujući i operativne ponovne kalibracije;

- gubitak sinhronizacije;

- TRAJNO ČUVANJE

  - informacije vezane za postavljanje e-dosijea i validaciju elektronskih potpisa u njima;

  - informacije koje se odnose na dostupnost podataka, očuvanje integriteta, očuvanje autentičnosti i neporicanja, održavanje čitljivosti i brisanje informacija;

  - informacije vezane za preuzimanje e-dosijea, ispunjenje zahteva za izjašnjenje i predaju arhive drugom pružaocu;

- EVIDENCIJA:

  - isključivanje, ponovno pokretanje sistema evidentiranja ili nekih njegovih komponenti;

  - izmenu bilo kog parametra podešavanja evidentiranja, na primer učestalosti, praga upozorenja i događaja koji treba da se ispita;

  - modifikacija ili brisanje sačuvanih podataka evidencije;

  - aktivnosti koje se obavljaju zbog kvara sistema evidencije.

- PRIJAVA NA SISTEM:

  - uspešne prijave, neuspešni pokušaji prijave za pouzdane uloge;
  - u slučaju autentifikacije zasnovane na lozinki:

    ✳ promena broja dozvoljenih neuspešnih pokušaja;

    ✳ dostizanje granice dozvoljenog broja neuspešnih pokušaja prijave u slučaju prijavljivanja korisnika;

    ✳ ponovni prijem korisnika blokiran zbog neuspešnih pokušaja prijave;

    promena tehnike autentifikacije (na primer sa lozinke na PKI).

- UPRAVLJANJE KLJUČEM:

svi događaji za ceo životni ciklus ključeva servisa (generisanje ključeva, čuvanje, učitavanje, uništenje itd.);

- TOKOVI PODATAKA:
  - bilo koju vrstu bezbednosno kritičnih podataka koji se ručno unose u sistem;
  - podaci relevantni za bezbednost, poruke koje sistem prima;
- Hardverski sigurnosni modul:
  - instaliranje hardverskog sigurnosnog modula;
  - uklanjanje hardverskog bezbednosnog modula;
  - odlaganje, uništavanje hardverskog bezbednosnog modula;
  - isporuka hardverskog sigurnosnog modula;
  - brisanje (resetovanje) hardverskog bezbednosnog modula;
  - učitavanje ključeva, sertifikata u hardverski sigurnosni modul.
- PROMENA KONFIGURACIJE:
  - hardver;
  - softver;
  - operativni sistem;
  - zakrpa;
  - instaliranje, ažuriranje i uklanjanje softvera na sistemu sertifikata;
- FIZIČKI PRISTUP, BEZBEDNOST LOKACIJE:
  - ulazak i izlazak lica iz bezbednosne zone u kojoj se nalaze komponente sistema koje se koriste za pružanje usluge poverenja;
  - pristup sistemskoj komponenti koja se koristi za pružanje usluge poverenja;
  - poznato ili sumnjivo kršenje fizičkog obezbeđenja;

- saobraćaj zaštitnog zida ili rutera.

- OPERATIVNE ANOMALIJE:
  - pad sistema, kvar hardvera;
  - kvarovi u softveru;
  - greška u validaciji integriteta softvera;
  - netačne ili pogrešno adresirane poruke;
  - mrežni napadi, pokušaji napada;
  - kvar opreme;
  - –kvarovi električne energije;
  - –greška u neprekidnom napajanju;
  - –suštinska greška u pristupu mrežnoj usluzi;
  - kršenje Praktičnih pravila za čuvanje;
  - brisanje tačnog vremena operativnog sistema.
- DRUGI DOGAĐAJI:
  - imenovanje lica za bezbednosnu ulogu;
  - instalacija operativnog sistema;
  - instalacija PKI aplikacije;
  - pokretanje sistema;
  - pokušaj ulaska u PKI aplikaciju;
  - izmena lozinke, pokušaj podešavanja;
  - čuvanje unutrašnje baze podataka i vraćanje iz rezervne kopije;
  - operacije sa datotekama (na primer kreiranje, preimenovanje, premeštanje);

– pristup bazi podataka.

5.4.2 Učestalost obrade log fajlova

Pružalac usluge čuvanja će obezbediti redovnu procenu kreiranih dnevnika. Kreirani dnevni log fajlovi će se proceniti sledećeg radnog dana ako je moguće, ali najkasnije u roku od 1 nedelje.
Procenu datoteka evidencije će izvršiti nezavisni revizor sistema sa odgovarajućom stručnošću, sistemskim privilegijama i imenovanjem.
Pružalac usluge čuvanja može da koristi automatizovane alate da pomogne u proceni elektronskih dnevnika. Obaveštenja dobijena od automatizovanih alata za praćenje biće obrađena i procenjena u roku od 24 sata.

Tokom ocenjivanja treba da se obezbedi autentičnost i integritet pregledanih dnevnika. Tokom evaluacije, sistemski generisane poruke o grešci će biti analizirane.
Značajne promene u saobraćaju treba analizirati statističkim metodama. Svrha logovanje, rezultati revizije i mere preduzete u cilju otklanjanja svih utvrđenih nedostataka moraju biti propisno dokumentovani.

5.4.3 Period zadržavanja log fajlova

Pre brisanja iz onlajn sistema, logovi će biti arhivirani i njihovo bezbedno očuvanje će biti obezbeđeno tokom perioda definisanog u odeljku 5.5.2..

5.4.4 Zaštita logova

Pružalac usluge čuvanja će zaštititi kreirane logove za potrebno vreme čuvanja. Tokom čitavog vremena čuvanja, sledeća svojstva podataka logova biće obezbeđena:

- zaštita od neovlašćenog korišćenja: samo ovlašćena lica – prvenstveno nezavisni revizori sistema – imaju pristup logovima;
- dostupnost: ovlašćenim licima će biti odobren pristup logovima;
- integritet: biće sprečena svaka promena podataka, brisanje u fajlovima logova, promena redosleda unosa itd.

5.4.5 Procedure za pravljenje rezervnih kopija log fajlova

Dnevni log fajlovi će se kreirati od kontinuirano generisanih unosa logova tokom operacija u sistemu. Dnevni log fajlovi će se arhivirati u dva primerka nakon evaluacije i skladištiti fizički odvojeno jedan od drugog, na odvojenim lokacijama na potrebno vreme. Tačan proces pravljenja rezervnih kopija biće definisan u Praktičnim pravilima za čuvanje.

5.4.6 Sistem prikupljanja revizije (interni naspram eksternog)

Pružalac usluge čuvanja specificira rad svojih procesa evidentiranja u svojim Praktičnim pravilima čuvanja.
Pružalac usluge čuvanja može da koristi automatske sisteme revizije i evidentiranja ako može da obezbedi da su aktivni u vreme pokretanja sistema i da rade neprekidno do isključivanja sistema.

Ako postoji bilo kakva anomalija u sistemima za automatsku reviziju i evidentiranje, rad Pružaoca usluge čuvanja biće obustavljen dok se incident ne reši.

5.4.7 Obaveštenje subjektu koji izaziva događaj

U slučaju otkrivenih grešaka, Pružalac usluge čuvanja po svom nahođenju može odlučiti da li će obavestiti osobu, ulogu, uređaj ili aplikaciju o grešci koja je do nje dovela.

5.4.8 Procene ugroženosti

Procenu ugroženosti će svake godine sprovoditi Pružalac usluge očuvanja kako bi pomogao u otkrivanju potencijalnih unutrašnjih i spoljašnjih pretnji, koje mogu dovesti do neovlašćenog pristupa.

Takođe će se mapirati verovatnoća nastanka događaja i očekivana šteta.
Redovno procenjuje sprovedene procese, mere bezbednosti, informacione sisteme, tako da su u stanju da pravilno izdrže otkrivene pretnje. Nakon procene uočenih grešaka, po potrebi će se izvršiti dopuna sistema odbrane sprečiti slične greške u budućnosti.

5.5 Arhivski zapisi

5.5.1 Vrste arhiviranih zapisa

Pružalac usluge čuvanja biće spreman za pravilno i bezbedno arhiviranje elektronskih i papirnih dokumenata.

Pružalac usluga čuvanja arhivira sledeće vrste informacija:

- svaki dokument u vezi sa akreditacijom Pružaoca usluge čuvanja;
- sve izdate verzije dokumenta Politika čuvanja;
- sve izdate verzije dokumenta Praktična pravila čuvanja;
- sve izdate verzije dokumenta Opšti uslovi;
- ugovori u vezi sa radom Pružaoca usluge čuvanja;
- svaki elektronski i papirni unos u log.

5.5.2 Period čuvanja arhive

Pružalac usluge čuvanja je obavezan da sačuva arhivirane podatke za vremenske periode u nastavku:

- Politiku čuvanja najmanje 10 godina od datuma stavljanja van snage;
- Praktična pravila čuvanja najmanje 10 godina od datuma ukidanja;
- Opšti uslovi poslovanja najmanje 10 godina od dana prestanka;
- svi ostali dokumenti da se arhiviraju najmanje 10 godina od dana nastanka.

5.5.3 Zaštita arhive

Pružalac usluga čuvanja je obavezan da čuva sve arhivirane podatke u dve kopije na lokacijama koje su fizički odvojene jedna od druge. Svaka od dve lokacije treba da ispunjava uslove za bezbednost arhiviranja i druge uslove.

Prilikom čuvanja arhiviranih podataka obezbediće se da:

- njihov integritet bude očuvan;
- zaštićeni su od neovlašćenog pristupa ;
- dostupni su;
- čuvaju autentičnost.

Arhivirani elektronski podaci će biti opremljeni najmanje naprednim elektronskim potpisom ili pečatom i kvalifikovanim vremenskim žigom.

5.5.4 Procedure arhiviranja rezervnih kopija

Duplikat arhiviranih podataka biće uskladišten na fizički odvojenoj lokaciji od sajta pružaoca usluga čuvanja u skladu sa zahtevima iz Odeljka 5.1.8..

5.5.5 Zahtevi za označavanje zapisa vremenskim žigom

Svaki unos u elektronskom logu biće obeležen vremenskim žigom, na koji je sistem ugradio tačno vreme sa tačnošću od najmanje jedne sekunde.
Pružalac usluga čuvanja će obezbediti da se sistemski sat u svojim sistemima pružaoca usluga maksimalno razlikuje od referentnog vremena za 1 sekundu. Sistemsko vreme koje se koristi za generisanje vremenskog žiga biće sinhronizovano sa UTC vremenom najmanje jednom dnevno.

Dnevni log fajlovi će biti opremljeni sa vremenskim žigom. Prilikom čuvanja arhiviranih podataka, ako je potrebno (na primer, istek promene algoritma originalnog vremenskog žiga) obezbediće se autentičnost podataka.

5.5.6 Sistem prikupljanja arhiva (interni ili eksterni)

Unosi u evidenciju će se generisati u zaštićenom računarskom sistemu Pružaoca usluge čuvanja i samo log fajlovi koji su elektronski potpisani i zaštićeni sa kvalifikovanim vremenskim žigom mogu da ga napuste.

5.5.7 Procedure za dobijanje i verifikaciju informacija arhive

Pružalac usluge čuvanja može da kreira log fajlove ručno ili automatski. U slučaju automatskog sistema evidentiranja, sertifikovane log datoteke će se generisati svakodnevno. Arhivirani fajlovi moraju biti zaštićeni od neovlašćenog pristupa.

Kontrolisani pristup arhiviranim podacima biće dostupan kvalifikovanim licima:

- Klijenti imaju pravo da vide podatke sačuvane o njima;
- u pravnim sporovima radi pružanja dokaza dostavljaju se potrebni podaci.

5.6 Oporavak od kompromitovanja i katastrofe

U slučaju katastrofe, Pružalac usluge čuvanja je dužan da preduzme sve neophodne mere kako bi štetu nastalu usled nedostatka usluge sveo na najmanju moguću meru i u najkraćem mogućem roku obnavlja usluge. Na osnovu procene incidenta koji se dogodio, preduzeće izvršava potrebne izmene, korektivne mere za sprečavanje budućeg nastanka incidenta.
Kada se problem reši, događaj će biti prijavljen Ministarstvu trgovine, turizma i telekomunikacija, kao nadzornom organu.

5.6.1 Procedure za rukovanje incidentima i kompromitovanjem informacija

Pružalac usluge čuvanja ima plan kontinuiteta poslovanja.
Pružalac usluge čuvanja će uspostaviti i održavati potpuno funkcionalan rezervni sistem, koji je na bezbednoj udaljenosti od primarne lokacije, geografski lociran na drugom mestu i nezavisno je sposoban da pruži pun spektar usluga.
Pružalac usluge čuvanja će kontinuirano testirati rad sistema rezervnih kopija i pregledati svoje planove za kontinuitet poslovanja svake godine.
U slučaju katastrofe, dostupnost usluga će se vratiti što je pre moguće.

5.6.2 Oštećenje računarskih resursa, softvera i/ili podataka

IT sistemi Pružaoca usluge čuvanja treba da budu izgrađeni od pouzdanih hardverskih i softverskih komponenti. Kritične funkcije će se realizovati korišćenjem redundantnih elemenata sistema, tako da u slučaju kvara, mogu da nastave sa radom.

Pružalac usluge čuvanja će napraviti kompletnu dnevnu rezervnu kopiju svojih baza podataka i generisanih logova.

Pružalac usluge čuvanja će kreirati potpune rezervne kopije onoliko često koliko je potrebno da bi mogao da vrati punu uslugu u slučaju katastrofe.

Plan kontinuiteta poslovanja Pružaoca usluge čuvanja će uključiti tačne zahteve za zadatke koje treba izvršiti u slučaju kvara kritične komponente sistema.
Kada se problem reši i integritet povrati, Pružalac usluge čuvanja će ponovo pokrenuti svoje usluge što je pre moguće.

5.6.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Poslovi koje treba izvršiti u slučaju kvara usluge usled elementarne nepogode ili druge nepogode definišu se u planu kontinuiteta poslovanja Pružaoca usluge čuvanja.

U slučaju katastrofe, propisi stupaju na snagu, kreće kontrola štete i obnavljanje usluge. Lokacija sekundarnih usluga biće postavljena tako daleko od primarne lokacije da verovatna katastrofa ne može istovremeno uticati na obe lokacije.
Pružalac usluge čuvanja je dužan da u slučaju katastrofe obavesti ugrožene korisnike što je pre moguće.

Nakon obnavljanja usluga, Pružalac usluge čuvanja će vratiti svoje uređaje oštećene tokom katastrofe u prvobitni nivo bezbednosti usluge što je pre moguće.
.

5.7 Prestanak usluge čuvanja

Pružalac usluge čuvanja će se pridržavati uslova propisanih zakonima u slučaju prestanka usluge.

Prilikom prestanka rada, prioritetni zadaci su:

- Treće strane i Pretplatnici će biti blagovremeno obavešteni o planiranom prekidu;
- Pružalac usluge čuvanja će učiniti sve da obezbedi da najkasnije do prestanka usluge drugi pružalac usluge preuzme evidenciju i obaveze usluge;
- nakon prestanka usluge, izvršiće se kreiranje potpune rezervne kopije i arhiviranje sistema;
- arhivirani podaci predaju se telu koji preuzima usluge, odnosno Ministarstvo trgovine, turizma i telekomunikacija.

6 Tehničke kontrole bezbednosti

Pružalac usluge čuvanja će koristiti pouzdane sisteme i opremu zaštićenu od modifikacija za upravljanje kriptografskim ključevima i podacima za aktivaciju tokom celog životnog ciklusa. Potrebe za kapacitetom će se kontinuirano pratiti kao i procenjivati buduće potrebe za kapacitetom, kako bi se obezbedila neophodna dostupnost potrebna za obradu i skladištenje.

6.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula

Pružalac usluge čuvanja će obezbediti bezbedno upravljanje privatnim ključevima koje poseduje i sprečiće otkrivanje, kopiranje, brisanje, modifikovanje i neovlašćeno korišćenje privatnog ključa. Pružalac usluge čuvanja može čuvati privatne ključeve sve dok pružanje usluge to zahteva.

Tokom upravljanja hardverskim sigurnosnim modulima, potpisani privatni ključevi koji nisu u funkciji biće obrisani tako da je praktično nemoguće vratiti ih.

6.1.1 Standardi i kontrole kriptografskog modula

Sistemi pružaoca usluge čuvanja čuvaju privatne ključeve u takvim bezbednim hardverskim uređajima koji su u skladu sa sledećim:

- zahtevima ISO/IEC 19790 [2], ili
- zahtevima FIPS 140-2 [3] nivoa 3 ili više, ili
- zahtevima FIPS 140-3 [4] nivoa 3 ili više, ili
- zahtevima CEN 419 221-5 [5], ili
- predstavljaju pouzdane sisteme koji se procenjuju na nivou garancije 4 ili više prema ISO/IEC 15408 [6] ili ekvivalentnom sistemu bezbednosnih kriterijuma. Procena će se zasnivati ili na odgovarajućem planu sistema bezbednosti koji ispunjava zahteve ovog dokumenta, ili na aproprijacijama za bezbednost.

Ključevi pružaoca mogu da se čuvaju samo u šifrovanim oblicima izvan hardverskog bezbednosnog modula. Za kodiranje će se koristiti samo oni algoritmi i parametri ključa za koje se očekuje da će moći da izdrže kriptografske napade tokom čitavog životnog veka ključeva.

Privatni ključevi pružaoca usluge će se čuvati na fizički bezbednoj lokaciji čak i u šifrovanom obliku, gde su dostupni samo ovlašćenim licima.

U slučaju slabljenja kriptografskih algoritama i parametara ključa, kodirani ključevi će biti uništeni ili će se ponovo kodirati korišćenjem algoritma i ključnih parametara koji obezbeđuju veću zaštitu.

6.1.2 Privatni ključ (N od M) Kontrola više osoba

Pružalac usluga čuvanja će obezbediti da istovremeno prisustvuju najmanje dvoje; zaposleni nosioci uloge od poverenja koji su potrebni za kritične operacije koje se obavljaju sa privatnim ključevima pružaoca.

6.1.3 Deponovanje privatnog ključa

Pružalac usluge čuvanja može da deponuje privatne ključeve sopstvenog provajdera samo u šifrovanom obliku.

6.1.4 Rezervna kopija privatnog ključa

Pružalac usluge čuvanja će napraviti sigurnosne kopije privatnih ključeva, a najmanje jedna kopija njih će biti uskladištena na drugom mestu od lokacije pružaoca usluge.
Pravljenje rezervnih kopija se može vršiti samo u zaštićenom okruženju, uz istovremeno prisustvo najmanje dve osobe koje imaju poverene uloge, uz isključenje drugih ljudi.
Najmanje isti strogi bezbednosni standardi biće primenjeni na upravljanje i očuvanje rezervnih kopija kao i za rad produkcionog sistema.

6.1.5 Arhiviranje privatnog ključa

Pružalac usluge čuvanja neće arhivirati svoje privatne ključeve.

6.1.6 Prenos privatnog ključa u ili iz kriptografskog modula

Svi privatni ključevi Pružaoca usluge čuvanja biće kreirani u kriptografskom modulu koji ispunjava zahteve.

Privatni ključevi neće postojati u otvorenom obliku izvan HSM uređaja.

Pružalac usluge čuvanja može samo da eksportuje privatni ključ iz HSM uređaja u svrhu pravljenja rezervne kopije.

Prenos privatnog ključa između HSM uređaja je dozvoljen samo u obliku bezbedne rezervne kopije.

6.1.7 Skladištenje privatnog ključa na kriptografskom modulu

Pružalac usluge čuvanja će čuvati privatne ključeve koji se koriste za pružanje usluge u skladu sa ovim smernicama sertifikata u HSM uređaju.
Ne postoji ograničavajući termin koji se primenjuje za obrazac za skladištenje u Hardverskom bezbednosnom modulu.

6.1.8 Način aktiviranja privatnog ključa

Privatni ključevi Pružaoca usluge čuvanja biće aktivirani u skladu sa procedurama i zahtevima definisanim u korisničkom uputstvu za korišćeni kriptografski modul i sertifikacionim dokumentima.

6.1.9 Metoda deaktiviranja privatnog ključa

Privatni ključevi Pružaoca usluge čuvanja biće deaktivirani u skladu sa procedurama, zahtevima definisanim u korisničkom uputstvu za korišćeni hardverski bezbednosni modul i sertifikacionim dokumentima.

6.1.10 Metoda uništavanja privatnog ključa

Odbačeni, istekli ili kompromitovani privatni ključevi Pružaoca usluge čuvanja biće uništeni na način koji onemogućava dalju upotrebu privatnih ključeva.
Privatni ključevi Pružaoca biće uništeni u skladu sa procedurama, definisanim zahtevima u korisničkom uputstvu i sertifikacionoj dokumentaciji korišćenog Hardverskog bezbednosnog modula, uz istovremeno prisustvo dva radnika Pružaoca usluge čuvanja (administratora infrastrukture i službenika obezbeđenja) uz isključenje drugih lica.

Svaka rezervna kopija privatnog ključa biće uništena na dokumentovan način na način da njegovo obnavljanje i korišćenje postaje nemoguće.

6.1.11 Ocena kriptografskog modula

U skladu sa zahtevima odeljka 6.1.1, svaki privatni ključ Pružaoca usluge čuvanja biće uskladišten u kriptografskom modulu koji

- ima sertifikat prema ISO/IEC 19790 [2], ili

- ima sertifikat prema FIPS 140-2 nivo 3 [3], ili
- ima sertifikat prema FIPS 140-3 nivo 3 [4], ili
- ima sertifikat zasnovan na zajedničkim kriterijumima najmanje EAL-4 nivoa [7] koji potvrđuje usklađenost sa zahtevima CEN 419 221-5 [4], ili
- ima sertifikat izdat u tu svrhu od nezavisnog sertifikacionog tela kvalifikovanog za procenu proizvoda elektronskog potpisa, registrovanog od strane Ministarstva trgovine, turizma i telekomunikacija, ili u državi članici Evropske unije.

6.2 Podaci o aktivaciji

6.2.1 Aktivacija generisarnih podataka i instalacija

Privatni ključevi Pružaoca usluga čuvanja biće zaštićeni u skladu sa procedurama, zahtevima definisanim u korisničkom uputstvu za korišćeni hardverski bezbednosni modul i sertifikacionim dokumentima.
U slučaju korišćenja aktivacionih podataka na osnovu lozinke, lozinke moraju biti dovoljno složene da bi se obezbedio potreban nivo zaštite.

6.2.2 Zaštita podataka aktivacije

Uređaje, podatke za aktivaciju neophodne za aktivaciju privatnog ključa čuvaju na bezbedan način zaposleni Pružaoca usluge čuvanja. Lozinke se smeju čuvati samo kodirane.

6.2.3 Drugi aspekti aktivacije podataka.

Bez uslova.

6.3 Kontrole računarske bezbednosti

6.3.1 Specifični tehnički zahtevi za bezbednost računara

Tokom konfiguracije i rada IT sistema Pružaoca usluge čuvanja obezbediće se usaglašenost sa sledećim zahtevima:

- identitet korisnika se verifikuje pre odobravanja pristupa sistemu ili aplikaciji;
- uloge se dodeljuju korisnicima i mora se obezbediti da svi korisnici imaju samo dozvole u skladu sa svojim ulogama;
- zapis u logu se kreira za svaku transakciju, a unosi se arhiviraju;
- za bezbednosno kritične procese obezbeđuje se da su interni mrežni domeni Pružaoca usluge čuvanja dovoljno zaštićeni od neovlašćenog pristupa;
- primenjuju se odgovarajuće procedure da bi se obezbedio oporavak usluge nakon gubitka ključa ili otkaza sistema.

6.3.2 Ocena računarske bezbednosti

U cilju obezbeđivanja IT bezbednosti i kvaliteta usluge, Pružalac usluge čuvanja će implementirati sistem kontrole po međunarodno prihvaćenim metodologijama, a adekvatnost istih će biti potvrđena sertifikatom izdatim od nezavisnog sertifikacionog tela.

6.4 Tehničke kontrole životnog ciklusa

6.4.1 Kontrole razvoja sistema

Pružalac usluge čuvanja koristi samo aplikacije i uređaje u svom proizvodnom IT sistemu koji:

- komercijalni softver, dizajniran i razvijen prema dokumentovanoj metodologiji dizajna, ili;
- prilagođena hardverska i softverska rešenja razvijena od strane samog Pružaoca usluge čuvanja tokom kojih su korišćene strukturisane metode razvoja i kontrolisano razvojno okruženje, ili;
- prilagođena hardverska i softverska rešenja razvijena od strane pouzdane strane za Pružaoca usluga očuvanja tokom kojih su korišćene strukturisane metode razvoja i kontrolisano razvojno okruženje, ili;
- softver otvorenog koda koji je u skladu sa bezbednosnim zahtevima i njihova adekvatnost je obezbeđena verifikacijom softvera i strukturiranim razvojem i upravljanjem životnim ciklusom.

Nabavka se sprovodi na način koji isključuje modifikaciju hardverskih i softverskih komponenti. Hardverske i softverske komponente primenjene za pružanje usluga od poverenja ne smeju se koristiti u druge svrhe.

Pružalac usluge čuvanja sa odgovarajućim merama zaštite će sprečiti zlonamerni softver da uđe u uređaje koji se koriste u servisu sertifikacije. Pre prve upotrebe i kasnije, hardverske i softverske komponente će se redovno proveravati u potrazi za zlonamernim kodovima.

Pružalac usluge čuvanja će postupati sa istom pažnjom u slučaju kupovine ažuriranja programa kao pri nabavci prve verzije.
U toku instaliranja softvera biće angažovano pouzdano, adekvatno obučeno osoblje hardvera. Pružalac usluge čuvanja može da instalira softver samo na IT opremi pružaoca usluge koja je neophodna za potrebe pružanja usluge.

Pružalac usluge čuvanja mora imati sistem kontrole verzija u kome će svaka promena biti dokumentovana. Pružalac usluge čuvanja sprovodi procedure za otkrivanje neovlašćenih promena.

6.4.2 Kontrole upravljanja sigurnošću

Pružalac usluge čuvanja će implementirati procese za dokumentovanje, rad, verifikaciju, praćenje i održavanje sistema koji se koriste u usluzi, uključujući njihovu modifikaciju i dalji razvoj.
Sistem kontrole verzija će otkriti bilo koju vrstu neovlašćenih promena, unosa podataka koji utiču na sistem, zaštitni zid, rutere, programe i druge komponente koje se koriste prilikom rada usluge. Instaliranjem programa koji se koristi u servisu, Pružalac usluge čuvanja će obezbediti da program koji se instalira bude odgovarajuće verzija i da nema bilo kakvih neovlašćenih modifikacija.
Pružalac usluge čuvanja će redovno proveravati integritet softvera u svom sistemu koji se koristi u okviru usluge.

6.4.3 Životni ciklus sigurnosnih kontrola

Pružalac usluge čuvanja će obezbediti zaštitu korišćenih hardverskih bezbednosnih modula tokom celog njihovog životnog ciklusa.

- Korišteni hardverski sigurnosni moduli moraju imati odgovarajuću sertifikaciju;

- po prijemu hardverskih bezbednosnih modula, proveriće se da li je obezbeđena zaštita hardverskih bezbednosnih modula od neovlašćenog pristupa tokom transporta;

- zaštita hardverskih bezbednosnih modula od neovlašćenog pristupa će biti obezbeđena tokom skladištenja;

- tokom rada, ciljevi potrebni da bi se obezbedila sigurnost HSM uređaja zahtevaju stalni nadzor i korišćenje korisničkog uputstva kao i izveštaja sertifikacije

- privatni ključevi uskladišteni na hardverskim bezbednosnim modulima koji su povučeni iz upotrebe biće obrisani na takav način da je nemoguće povratiti ključeve.

- Stavljanje van rada HSM uređaja podrazumeva rukovanje i odlaganje u skladu sa bezbedonosnim procedurama, uputstvom za upotrebu i dokumentaciji za sertifikaciju.

6.5 Bezbedonosne kontrole mrežnog okruženja

Pružalac usluge čuvanja će držati svoju konfiguraciju IT sistema pod strogom kontrolom i dokumentovati svaku promenu uključujući i najmanju modifikaciju, razvoj ili ažuriranje softvera. Pružalac usluge čuvanja će primeniti odgovarajuće procedure za otkrivanje bilo kakve promene hardvera ili softvera, instalacije sistema i održavanja na IT sistemu. Pružalac usluge čuvanja će proveriti autentičnost i integritet svake softverske komponente pri prvom učitavanju.

Pružalac usluge čuvanja će primeniti odgovarajuće mere bezbednosti mreže:

- Da će svoj IT sistem podeliti na odvojene bezbednosne zone;

- Da će odvojiti namensku mrežu za administraciju IT sistema i produkcionu operativnu mrežu;

- treba da odvoji proizvodne sisteme za TSP usluge od sistema koji se koriste u razvoju i testiranju;

- da uspostavlja komunikaciju između različitih sistema od poverenja samo preko pouzdanih kanala koji se logički razlikuju od drugih kanala komunikacije i obezbeđuju sigurnu identifikaciju njegovih krajnjih tačaka i zaštitu podataka kanala od modifikacije ili otkrivanja;

- da će upravljati IT sistemima koji se koriste za produkcionu operativnu mrežu u zonama bezbedne mreže;

- da će ograničiti pristup i komunikaciju između zona na one koje su neophodne za rad usluge;

- da će onemogućiti nekorišćene protokole i naloge;

- da će onemogućiti nekorišćene mrežne portove i usluge;
- da se pokreće samo mrežna aplikacija koja je neophodna za pravilan rad IT sistema;
- da se redovno pregledava utvrđeni skup pravila.

Pružalac usluge čuvanja će proći ili izvršiti proveru ugroženosti javnih i privatnih IP adresa:

- u roku od jedne nedelje od prijema zahteva od CA/browser Foruma;
- nakon bilo kakvih promena sistema ili mreže za koje CA utvrdi da su značajne;
- najmanje svaka tri (3) meseca.

6.6 Stavljanje vremenskog žiga

Pružalac usluge čuvanja koristiće vremenske žigove koje daje kvalifikovani pružalac za izdavanje vremenskog žiga koji je naveden na listi pružalaca usluga od poverenja Republike Srbije radi zaštite integriteta log fajlova i drugih elektronskih datoteka koje treba arhivirati.

7 Revizija usklađenosti i druge procene

Rad Pružaoca usluge čuvanja nadzire Ministarstvo trgovine, turizma i telekomunikacija u skladu sa propisima Evropske unije i zakonima Republike Srbije.
Ministarstvo trgovine, turizma i telekomunikacija održava inspekciju lokacije najmanje jednom godišnje na lokaciji pružaoca usluge čuvanja. Pre inspekcije, Pružalac usluge čuvanja će izvršiti skrining svog poslovanja od strane eksternog revizora i detaljan izveštaj o pregledu poslati Ministarstvu trgovine, turizma i telekomunikacija u roku od 3 dana od dana prijema.
Tokom skrininga treba da se utvrdi da li rad Pružaoca usluge čuvanja ispunjava zahteve eIDAS Uredbe [1] i srodnog srpskog zakonodavstva i zahteve primenjene Politike(a) čuvanja i odgovarajućih Praktičnih pravila).

Predmet i metodologija skrininga moraju biti u skladu sa sledećim normativnim dokumentima:

- UREDBA (EU) br. 910/2014 EVROPSKOG PARLAMENTA I SAVETA od 23. jula 2014. o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC [1];

- ETSI EN 319 403-1 Elektronski potpisi i infrastruktura (ESI); Procena usaglašenosti pružaoca povereničkih usluga; Deo 1: Zahtevi za tela za ocenjivanje usaglašenosti koja ocenjuju pružaoce usluga od poverenja; [8]

- ETSI EN 319 401 Elektronski potpisi i infrastruktura (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja [9]

- ETSI TS 119 511 Elektronski potpisi i infrastruktura (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji obezbeđuju očuvanje digitalnih potpisa ili opštih podataka korišćenjem tehnika digitalnog potpisa [10]

Rezultat skrininga je poverljivi dokument koji je dostupan samo ovlašćenim licima.
Sertifikat o usaglašenosti izdat u skladu sa izveštajem o oceni usaglašenosti biće objavljen na internet stranici Pružaoca usluge čuvanja.

Pružalac usluga čuvanja zadržava pravo da u bilo kom trenutku, uz angažovanje nezavisnog stručnjaka, izvrši inspekciju rada pružaoca koji posluju u skladu sa sadašnjom politikom kako bi proverio usklađenost sa zahtevima.

7.1 Učestalost ili okolnosti procene

Pružalac uslug3 čuvanja će izvršiti procenu usaglašenosti svake godine.

7.2 Identitet/Kvalifikacije procenjivača

Pružalac uslug3 očuvanja može da obavlja interne revizije uz pomoć svojih zaposlenih koji imaju ulogu nezavisnog revizora sistema. Procenu usaglašenosti sa eIDAS i ETSI vrši organizacija, koja ima kvalifikacioni mandat izdat od strane nacionalne organizacije za akreditaciju države članice EU.

7.3 Odnos procenjivača prema procenjenom entitetu

Eksternu reviziju može vršiti samo lice koje:

- je nezavisno od vlasnika, menadžmenta i poslovanja ispitanog pružaoca usluge čuvanja;
- je nezavisno od ispitane organizacije, odnosno ni on ili ona, ni njegovi ili njeni najbliži rođaci nemaju nikakav radni ili poslovni odnos sa pružaocem usluge čuvanja.

7.4 Teme obuhvaćene ocenjivanjem

Pregled će obuhvatiti najmanje sledeće oblasti:

- usklađenost sa zakonima koji su trenutno na snazi;
- usklađenost sa tehničkim standardima;
- usklađenost sa Politikom sertifikacije i Praktičnim pravilima usluge;
- adekvatnost upotrebljenih procesa;
- dokumentacija;
- fizičko obezbeđenje;
- adekvatnost osoblja;

- IT bezbednost;
- poštovanje pravila zaštite podataka.

7.5 Radnje preduzete kao rezultat nedostatka

Nezavisni revizor će rezimirati rezultat skrininga u detaljnom izveštaju o skriningu koji pokriva testirane komponente sistema, procese i sadrži dokaze korišćene u skriningu i revizorske izjave. Utvrđene neusaglašenosti tokom ispitivanja i rokovi za njihovo otklanjanje evidentiraju se u posebnom poglavlju izveštaja.

Nezavisni revizor može evidentirati razlike i neslaganja na osnovu njihove ozbiljnosti otkriveno tokom pregleda:

- sugestije za izmene koje se opciono uzimaju u obzir;
- odstupanja koja treba obavezno izbegavati.

Nezavisni revizor će bez odlaganja prijaviti uočena ozbiljna odstupanja Ministarstvu trgovine, turizma i telekomunikacija koje je ovlašćeno da preduzme potrebne mere.
Pružalac usluge čuvanja će pismenim putem odgovoriti na probleme koje je nezavisni revizor naveo i izvestiti o preduzetim merama za njihovo otklanjanje prilikom sledeće revizije.

Nezavisni revizor šalje izveštaj o proceni Ministarstvu trgovine, turizma i telekomunikacija.

7.6 Saopštavanje rezultata

Pružalac usluge čuvanja objavljuje zbirni izveštaj o proceni. Nije potrebno otkrivati odstupanja otkrivena tokom nezavisne procene sistema, ona se mogu tretirati kao poverljive informacije.

REFERENCE

[1] Uredba (EU) br. 910/2014 Evropskog parlamenta i Saveta od 23. jula 2014. o elektronskoj identifikaciji i uslugama poverenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC.

[2] ISO/IEC 19790:2012: Informaciona tehnologija – Tehnike bezbednosti – Zahtevi za bezbednost za kriptografske module.

[3] FIPS PUB 140-2 (25. maj 2001.): Bezbednosni zahtevi za kriptografske module.

[4] FIPS PUB 140-3 (22. mart 2019.): Bezbednosni zahtevi za kriptografske module.

[5] CEN 419 221-5; Profili zaštite za TSP kriptografske module - Deo 5: Kriptografski Modul za usluge od poverenja.

[6] MSZ/ISO/IEC 15408-2:2022, Informaciona tehnologija – Metode i sredstva obezbeđenja – Kriterijumi za procenu IT bezbednosti .

[7] Zajednički kriterijumi za procenu bezbednosti informacionih tehnologija, deo 1 - 3.

[8] ETSI EN 319 403-1 V2.3.1 (2020-06) Elektronski potpisi i infrastrukture (ESI); Poverenje Procena usaglašenosti pružaoca usluga; Deo 1: Zahtevi za tela za ocenjivanje usaglašenosti koja ocenjuju pružaoce usluga od poverenja.

[9] ETSI EN 319 401 V2.3.1 (2021-05); Elektronski potpisi i infrastruktura (ESI); General Uslovi politike za pružaoce usluga od poverenja.

[10] ETSI TS 119 511 V1.1.1 (2019-06); Elektronski potpisi i infrastruktura (ESI); Polici i bezbednosni zahtevi za provajdere usluga poverenja koji obezbeđuju dugoročno očuvanje digitalnih potpise ili opštih podataka pomoću tehnika digitalnog potpisa.

[11] (Srpski) Zakon o zaštiti podataka o ličnosti („Službeni glasnik RS“ br. 87/2018).

[12] Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka i stavljanju van snage Direktive 95/ 46/EC (Opšta uredba o zaštiti podataka).

[13] Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju („Službeni glasnik RS”, br. 94/2017 i 52/21).