

U skladu sa eIDAS-om i kvalifikovanom uslugom za čuvanje dokumenata

Praktična pravila kvalifikovanog čuvanja elektronskog dokumenta

Verzija 1.5

Sadržaj

1 Uvod 8

1.1 Pregled 8

1.2 Naziv i identifikacija dokumenta 9

1.2.1 Uskađenost 9

1.2.2 Politika čuvanja 9

1.2.3 Stupanje na snagu 9

Obim usluge 10

Vremenski okvir 10

Obim učesnika 10

Geografski obim 10

1.3 PKI Učesnici 11

1.3.1 Sertifikaciono telo 11

Podaci Pružaoca usluge čuvanja 11

Uvod o Pružaocu usluge čuvanja 11

Kvalitet i informaciona bezbednost 11

1.3.2 Pretplatnici 12

1.3.3 Oslanjajuće strane 12

1.4 Administracija dokumenta 12

1.4.1 Organizacija koja vrši administraciju dokumenta 12

1.4.2 Osoba ili organizacija odgovorna za prikladnost dokumenta Praktična pravila za kvalifikovano elektronsko čuvanja dokumenata 12

1.5 Definicije i akronimi 13

1.5.1 Definicije 13

1.5.2 Akronimi 21

2 Objavljivanje i obaveze 21

2.1 Repozitorijumi 21

2.2 Vreme ili učestalost objavljivanja 22

3 Usluga kvalifikovanog čuvanja 23

3.1 Šema čuvanja 23

3.1.1 Ciljevi čuvanja 23

3.1.2 Model skladišta čuvanja 24

3.1.3 Podržane operacije 24

3.1.4 Generisanje i validacija dokaza o očuvanju 24
3.1.5 Povećanje dokaza o čuvanju 25
3.2 Profil očuvanja 25
3.2.1 Identifikacija profila očuvanja 26
3.2.2 Ciljevi čuvanja 26
3.2.3 Model čuvanja skladišta 26
3.2.4 Podržane operacije 26
3.2.5 Tehničke odredbe 26
3.2.6 Rok važenja 26
3.2.7 Formati dokaza 27
3.2.8 Ljudski razumljiv format 27
3.2.9 Objavljivanje podržanih profila očuvanja 27
3.2.10 Dužina trajanja profila očuvanja 27
3.2.11 Podržana politika očuvanja dokaza 27
3.2.12 Podržana politika validacije potpisa 27
3.3 Politika očuvanja dokaza 28
3.3.1 Identifikator politike očuvanja dokaza 28
3.3.2 Format politike očuvanja dokaza 28
3.3.3 Kreiranje dokaza o očuvanju 28
3.3.4 Primenjeni kriptografski algoritmi 29
3.3.5 Korišćenje drugih usluga od poverenja 29
3.3.6 Validacija dokaza očuvanja 29
3.3.7 Produžavanje trajanja dokaza očuvanja 31
3.3.8 Format dokaza o očuvanju 31
3.3.9 Referenca potvrde prema usluzi čuvanja 31
3.4 Politika validacije potpisa 32
3.4.1 Identifikator politike validacije potpisa 32
3.4.2 Format politike validacije potpisa 32
3.4.3 Višejezičnost 32
3.4.4 Prikupljanje materijala za validaciju 32
3.5 Kriptografske kontrole 33
3.5.1 Vremenski žigovi 33
3.5.2 Kriptografski monitoring 33

3.6 Nadogradnja dokaza o očuvanju 34
3.7 Uvoz-izvoz paketa 34
3.8 Protokol očuvanja 34
3.8.1 Pristup dokazima o očuvanju i metapodacima e-dokumenta 34
3.8.2 Brisanje sačuvanih dokumenata 35
3.9 Protokol obaveštenja 35
3.10 Proces očuvanja 35
3.10.1 Dokazi o očuvanju 35
3.10.2 Očuvanje digitalnih potpisa 36
3.11 Mrežna bezbednost 36
3.11.1 Pristup sačuvanim dokumentima 36
3.12 Prestanak pružanja usluge i planovi ukidanja 37
3.12.1 Sačuvani dokumenti nakon raskida 37
3.13 Praktična pravila usluge čuvanja 37
3.13.1 Podržane politike usluge čuvanja 37
3.13.2 Podržani profili očuvanja 37
3.13.3 Kako se postižu ciljevi očuvanja 37
3.13.4 Dostupnost sačuvanih dokumenata 37
3.13.5 Obaveze svih spoljnih organizacija koje podržavaju uslugu čuvanja 37
3.13.6 Zahtevanje paketa za izvoz-uvoz 38
3.13.7 Upravljanje podacima na kraju perioda očuvanja 38
3.14 Kvalifikovana usluga čuvanja 38
3.14.1 Pružalac usluge izdavanja vremenskih žigova 38
3.14.2 Identifikator usluge 39
4 Opisivanje procesa usluge čuvanja 41
4.1 Otpremanje objekta očuvanja 42
4.2 Obezbeđivanje materijala za validaciju/Dostupnost dokaza o očuvanju – preuzimanje dokaza o očuvanju 45
4.3 Izdavanje potvrde 46
4.4 Raskid ugovora o usluzi 48
5 Tehničke mere bezbednosti 49
5.1 Sigurnosne garancije 49
5.2 Mere predostrožnosti za računarsku bezbednost 49

5.3 Tehničke mere predostrožnosti vezane za životni ciklus 50
5.4 Redovna sertifikcija 50
5.5 Ponovno šifrovanje arhive 51
5.6 Kontinuirano praćenje tehnologije 51
5.7 Prihvatanje izdavaoca sertifikata i vremenskog žiga 51
5.8 Dostupnost određenih elemenata usluge elektronskog očuvanja 52
6 Kontrole objekata, upravljanja i rada 53
6.1 Fizičke kontrole 53
6.1.1 Lokacija i izgradnja 53
6.1.2 Fizički pristup 54
6.1.3 Napajanje i klimatizacija 55
6.1.4 Izloženost vodi 55
6.1.5 Prevencija i zaštita od požara 55
6.1.6 Skladištenje medija 55
6.1.7 Odlaganje otpada 55
6.1.8 Bekap van lokacije 56
6.2 Proceduralne kontrole 56
6.2.1 Poverljive uloge 56
Menadžer Implementacije 56
Inženjer baza podataka 57
Sistem inženjer 57
Služenik obezbeđenja 57
Inženjer za podršku 57
Administrativni radnik 57
Pravni savetnik 57
Interni revizor 57
6.2.2 Broj potrebnih osoba po zadatku 58
6.2.3 Identifikacija i autentifikacija za svaku ulogu 58
6.2.4 Uloge koje zahtevaju razdvajanje dužnosti 58
6.3 Kontrola osoblja 59
6.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje 59
6.3.2 Procedure provere pozadine 60
6.3.3 Zahtevi za obuku 60

6.3.4 Učestalost i uslovi prekvalifikacije 60
6.3.5 Učestalost i redosled rotacije poslova 62
6.3.6 Sankcije za nedozvoljene radnje 62
6.3.7 Zahtevi nezavisnog izvođača 62
6.3.8 Dokumentacija dostavljena osoblju 63
6.4 Procedure evidentiranja revizije 63
6.4.1 Vrste snimljenih događaja 63
6.4.2 Učestalost obrade dnevnika revizije 67
6.4.3 Period zadržavanja za evidenciju revizije 67
6.4.4 Zaštita dnevnika revizije 67
6.4.5 Procedure rezervne kopije dnevnika revizije 68
6.4.6 Sistem prikupljanja revizije (interni naspram eksternog) 68
6.4.7 Obaveštenje subjektu koji izaziva događaj 68
6.4.8 Procene ugroženosti 68
6.5 Arhivski zapisi 69
6.5.1 Vrste arhiviranih zapisa 69
6.5.2 Period čuvanja arhive 70
6.5.3 Zaštita arhive 70
6.5.4 Procedure arhiviranja rezervnih kopija 71
6.5.5 Zahtevi za stavljanje vremenskog žiga na zapise 71
6.5.6 Sistem prikupljanja arhiva (interni ili eksterni) 71
6.5.7 Procedure za dobijanje i verifikaciju arhivskih informacija 72
6.6 Kompromis i oporavak od katastrofe 72
6.6.1 Procedure za rukovanje incidentima i kompromisima 72
6.6.2 Računarski resursi, softver i/ili podaci su oštećeni 73
6.6.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe 73
6.7 Prestanak usluge očuvanja 73
7 Tehničke bezbednosne kontrole 74
7.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula 75
7.1.1 Standardi i kontrole kriptografskog modula 75
7.1.2 Privatni ključ (N od M) Kontrola više osoba 76
7.1.3 Deponovanje privatnog ključa 76
7.1.4 Rezervna kopija privatnog ključa 76

7.1.5 Arhiva privatnih ključeva 76
7.1.6 Prenos privatnog ključa u ili iz kriptografskog modula 76
7.1.7 Skladištenje privatnog ključa na kriptografskom modulu 77
7.1.8 Način aktiviranja privatnog ključa 77
7.1.9 Metoda deaktiviranja privatnog ključa 78
7.1.10 Metoda uništavanja privatnog ključa 78
7.1.11 Ocena kriptografskog modula 78
7.2 Podaci o aktivaciji 79
7.2.1 Generisanje i instalacija aktivacionih podataka 79
7.2.2 Zaštita podataka aktivacije 79
7.2.3 Drugi aspekti aktivacionih podataka 79
7.3 Kontrole kompjuterske bezbednosti 79
7.3.1 Specifični tehnički zahtevi za bezbednost računara 79
7.3.2 Ocena računarske bezbednosti 80
7.4 Tehničke kontrole životnog ciklusa 80
7.4.1 Kontrole razvoja sistema 80
7.4.2 Kontrole za upravljanje bezbednošću 81
7.4.3 Sigurnosne kontrole životnog ciklusa 82
7.5 Kontrole mrežne bezbednosti 82
7.6 Stavljanje vremenskog žiga 84
8 Revizija usklađenosti i druge procene 85
8.1 Učestalost ili okolnost procene 86
8.2 Identitet/Kvalifikacije procenjivača 86
8.3 Odnos procenjivača prema procenjenom entitetu 86
8.4 Teme pokrivene procenom 86
8.5 Radnje preduzete kao posledica nedostatka 87
REFERENCE 88

1 Uvod

Ovaj dokument predstavlja Praktična pravila kvalifikovanog čuvanja koji se odnosi na kvalifikovanu uslugu čuvanja dokumenata kompanije Inception d.o.o. Beograd (u daljem tekstu: Inception ili Pružalac usluge čuvanja).

Pružalac usluge čuvanja pruža usluge svojim klijentima sa kojima ima ugovoreni odnos. Trenutna Praktična pravila čuvanja opisuju okvir za pružanje gore navedenih usluga i uključuje detaljne procedure i različita operativna pravila.

Praktična pravila čuvanja su u u skladu sa zahtevima propisanim eIDAS Uredbom[1], usluga koja se pruža u skladu sa ovim propisima je kvalifikovana za izdavanje:

- Elektronskih potpisa
- Elektronskih pečata

1.1 Pregled

Cilj trenutnih Praktičnih pravila čuvanja je da sumira sve informacije koje Klijenti treba da znaju kada dođu u kontakt sa Pružaocem usluge čuvanja. Ovaj dokument takođe ima za cilj da pomogne sadašnjim i budućim klijentima da:

- Budu upoznati sa detaljima, zahtevima i praktičnom pozadinom pružanja usluga koje pruža Inception.
- Razumeju rad kvalifikovane usluge čuvanja i da odluče da li su usluge usklađene i ispunjavaju li njihove potrebe i očekivanja.

Pored ovih Praktičnih pravila čuvanja, dodatni detalji i zahtevi mogu se naći u Politici čuvanja [2] i ugovoru o uslugama zaključenim sa Pružaocem usluge čuvanja, kao i drugim propisima ili dokumentima nezavisnim od Pružaoca usluge čuvanja.

1.2 Naziv i identifikacija dokumenta

Izdavač	Inception d.o.o Beograd
Naziv dokumenta	eIDAS compliant and qualified Praktična pravila kvalifikovanog čuvanja
OID	1.3.6.1.4.1.57738.40.2.1.5.0
Verzija dokumenta	1.5
Datum stupanja na snagu	

1.2.1 Uskađenost

Pružalac usluge čuvanja podržava sledeću politiku ETSI usluge:

- Normativni zahtevi definisani u ETSI TS 119 511 [3]

Pružalac usluge čuvanja izjavljuje da je usklađen sa ETSI politikom kroz dokument Praktična pravila kvalifikovanog čuvanja.

1.2.2 Politika čuvanja

Prvih sedam brojeva OID-a koji identifikuju Politiku čuvanja su jedinstveni identifikatori Pružaoca usluge kao što sledi: 1.3.6.1.4.1.57738

Usluga čuvanja je identifikovana sufiksom koji prati jedinstveni identifikator Pružaoca usluge: 1.3.6.1.4.1.57738.40

Usluga očuvanja se pruža u skladu sa ovim Praktičnim pravilima čuvanja koja je u skladu sa zahtevima Politike čuvanja, u nastavku identifikovanim na sledeći način:

OID	**Naziv**
1.3.6.1.4.1.57738.40.1.1.4.0	4. INCEPTION – Politika kvalifikovanog čuvanja

1.2.3 Stupanje na snagu

Praktična pravila čuvanja i Politika čuvanja zasnovanim na ovim dokumentima treba revidirati najmanje jednom godišnje i obezbediti njihovu dopunu potencijalno izmenjenim zahtevima i preduslovima.

Obim usluge

Praktična pravila kvalifikovanog čuvanja odnose se na isporuku i korišćenje usluga opisanih u ovom dokumentu.

Vremenski okvir

Trenutna verzija dokumenta Praktična pravila kvalifikovanog čuvanja je na snazi od datuma stupanja na snagu navedenog u odeljku 1.2 ovog dokumenta. Efekat automatski prestaje po prekidu pružanja usluge ili izdavanjem nove verzije dokumenta Praktična pravila kvalifikovanog čuvanja.

Obim učesnika

Efekat dokumenta Praktična pravila kvalifikovanog čuvanja proteže se 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 neophodne kontrole kako bi se pružene usluge mogle obavljati bezbedno i u skladu sa zakonom Republike Srbije.

Geografski obim

Trenutni dokument Praktična pravila kvalifikovanog čuvanja zasnovana je na zahtevima Evropske unije, ali 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 dokumentu Praktična pravila kvalifikovanog čuvanja. U uslugama koje se pružaju stranim klijentima, detaljni uslovi koji se razlikuju od dokumenta Praktična pravila kvalifikovanog čuvanja mogu biti regulisani posebnim ugovorom o uslugama.

Usluga koja se pruža u skladu sa ovim dokumentom Praktična pravila kvalifikovanog čuvanja dostupna je širom sveta. Valjanost dokumenta, materijal za dugoročnu validaciju i pripadajuće izdate potvrde arhiviraju se prema sadašnjoj usluzi kvalifikovanog čuvanja dokumenata.

Dokument Praktična pravila kvalifikovanog čuvanja je nezavisna od geografske lokacije na koju su poslati u arhivu i odakle su ispitivani. Usluga koja se pruža u skladu sa ovim dokumenta Praktična pravila kvalifikovanog čuvanja može se koristiti samo kako je opisano u ovoj dokumentu, kao i u Politici čuvanja.

1.3 PKI Učesnici

1.3.1 Sertifikaciono telo

Podaci Pružaoca usluge čuvanja

Naziv:	Inception d.o.o Beograd
Registarski broj kompanije:	20701242 (APR)
Sedište:	Admirala Vukovića 57
Telefon:	+381 (0)11 2920 355
Internet adresa:	https://inception.rs

Uvod o Pružaocu usluge čuvanja

"Inception d.o.o Beograd" je pružalac kvalifikovanih usluga od poverenja koji koriste najbezbednije tehnologije, uključujući siguran prenos podataka, za obavljanje svojih elektronskih kvalifikovanih usluga od poverenja, kvalifikovanog elektronskog potpisivanja, kvalifikovanog elektronskog pečatiranja, kvalifikovanog korišćenja vremenskog žiga, validacije i drugih usluga.

Pružalac usluge nudi pouzdane usluge u skladu sa važećim pravnim aktima Republike Srbije i Evropske unije, a posebno u skladu sa eIDAS Uredbom[1] i u skladu sa tehničkim zahtevima, smernicama i međunarodnim standardima, posebno ETSI SR 019 050 [4], EN 319 401 [5], EN 319 421 [6], ETSI TS 119 101 [7], ETSI EN 319 522-1 [8], ETSI EN 319 522-2 [9], ETSI EN 319 521 V1.1.1 (2019-02) [10].

Kvalitet i informaciona bezbednost

Pružalac usluge planira i primenjuje sve mere zaštite u skladu sa standardima ISO / IEC 27000, FIPS 140-2 nivo 3 i/ili uobičajenim kriterijumom EAL4+, i ETSI tehničkim zahtevima.

1.3.2 Pretplatnici

Pretplatnici definišu obim korisnika koji koriste uslugu, a pretplatnici pokrivaju i naknade za usluge 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 dokumenta

1.4.1 Organizacija koja vrši administraciju dokumenta

Podaci organizacije koja administrira ovaj dokument mogu se naći 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 Osoba ili organizacija odgovorna za prikladnost dokumenta Praktična pravila za kvalifikovano elektronsko čuvanja dokumenata

Lice odgovorno za usklađenost sa dokumentom Praktična pravila kvalifikovanog čuvanja i Politikom čuvanja koja se u njoj pominje je:

Odgovorno lice	Jovan Vistać
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

Praktična pravila čuvanja i pružanje usluge nadgleda Ministarstvo trgovine, turizma i telekomunikacija. Ministarstvo vodi registar sa politikama usluga i Pružaocima usluga čuvanja koji primenjuju ove politike.

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 rezultat pružanja usluge čuvanja 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 očuvanju radi produženja perioda važenja tog dokaza.
Cilj očuvanja	Jedan od sledećih 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 očuvanja	Generički skup procedura i pravila koji se odnose na model skladištenja čuvanja i jedan ili više ciljeva čuvanja koji opisuje kako se stvaraju i potvrđuju dokazi o očuvanju.
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.
Objekat očuvanja	Otkucani set podataka, koji se dostavlja, obrađuje ili preuzima od strane Pružaoca usluge 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)
Korisnik	Osoba ili organizacija koja potpisuje ugovor o usluzi sa pružaocem usluga očuvanja da bi koristila neke od njegovih usluga.

Pružalac usluge 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)
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.
Jedinica za posredničku sertifikaciju	Jedinica za sertifikaciju čiji je sertifikat izdala druga jedinica za sertifikaciju.
Dugoročno očuvanje	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.

Kriptografski ključ	Jedinstveni digitalni niz podataka koji kontroliše kriptografsku transformaciju, čije je poznavanje neophodno za šifrovanje, dešifrovanje, kreiranje i verifikaciju elektronskih potpisa i pečata.
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.
Kvalifikovana usluga od poverenja	"Usluga od poverenja koja ispunjava primenljive zahteve propisane eIDAS uredbom." (eIDAS [1] član 3. tačka 17.
Kvalifikovani pružalac usluge poverenja	"Pružalac usluga poverenja koji pruža jednu ili više kvalifikovanih usluga 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.
Klijent	Pretplatnik i korisnici usluga kojima Pretplatnik daje korisnička prava.
	Vanredna operativna situacija

Vanredna situacija koja uzrokuje smetnje u radu Pružaoca usluge čuvanja, kada	nastavak normalnog rada Pružaoca usluge očuvanja nije moguć ni privremeno ni trajno.
Praktična pravila usluge čuvanja	Praktična pravila pružaoca usluge od poverenja sa detaljnim procedurama ili drugim operativnim zahtevima koji se koriste u vezi sa pružanjem određenih usluga od 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.
Šifrovan 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. Autoritet za sertifikaciju 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 isteka 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
PO	Objekat čuvanja

2 Objavljivanje i obaveze

2.1 Repozitorijumi

Pružalac usluge čuvanja objavljuje ugovorne uslove i politike elektronskim putem na svojoj veb stranici na sledećem linku: https://incepition.rs/ca

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

Dokumenti koji su na snazi dostupni su na sajtu.

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 stavlja na raspolaganje Klijentu pojedinačni Ugovor o usluzi na papiru, overen svojeručnim potpisom i pečatom, ili u obliku elektronskog dokumenta u PDF formatu sa kvalifikovanim elektronskim potpisom.

Pružalac usluge čuvanja obaveštava svoje Klijente o promeni Opštih uslova.

2.2 Vreme ili učestalost objavljivanja

Najvažniji uslovi za pružanje usluge sadržani su u ugovoru o uslugama koji Klijent potpisuje prilikom zaključenja ugovora, ili u dokumentu Opštih uslova na koje se dokument poziva.

Pružalac usluge čuvanja vrši reviziju Opštih uslova jednom godišnje ili ranije u slučaju vanrednog zahteva za promenu sa prioritetom i vrši neophodne izmene.

Dokument će dobiti novi broj verzije sa svakom izmenom, bez obzira na složenost promene. Prihvaćeni dokument biće objavljen na internet stranici Pružaoca usluge čuvanja i biće poslat na uvid Ministarstvu trgovine, turizma i telekomunikacija 30 dana pre planiranog stupanja na snagu.

3 Usluga kvalifikovanog čuvanja

U ovom odeljku, ovaj dokument Praktična pravila kvalifikovanog čuvanja opisuje ciljeve čuvanja i modele skladištenja koji su dostupni u okviru usluge čuvanja koju nudi pružalac usluge čuvanja.

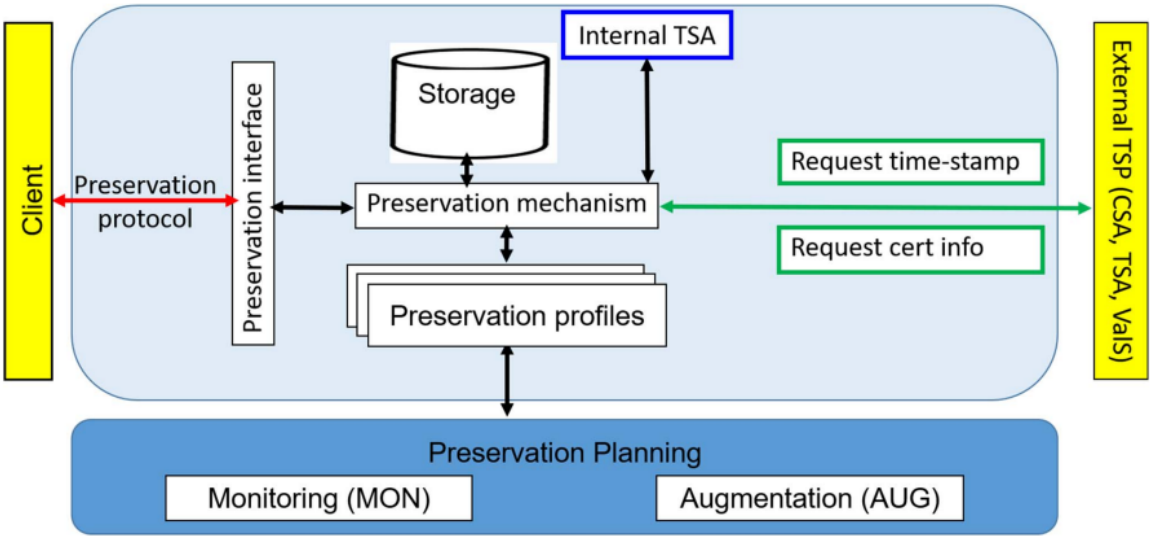


Figure 1: Functional model of a preservation service with storage [WST]

3.1 Šema čuvanja

Šema čuvanja sa skladištem zasnovana na evidenciji dokaza se nalazi na sledećem URL-u :

https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf

3.1.1 Ciljevi čuvanja

Sadašnja šema čuvanja podržava sledeće ciljeve čuvanja:

- **Očuvanje digitalnih potpisa (PDS)**

  Cilj očuvanja „Očuvanje digitalnih potpisa“ (PDS) proširuje na duže vremenske periode mogućnost validacije digitalnog potpisa, održavanja njegovog statusa validnosti i dobijanja dokaza o postojanju povezanih potpisanih podataka.

- **Nadogradnja (AUG)**

  Cilj očuvanja „Augmentacija“ (AUG) ukazuje na to da usluga očuvanja podržava nadogradnju dostavljenih dokaza o očuvanju.

Ovi ciljevi očuvanja su definisani šemom očuvanja i nametnuti zahtevima prema ETSI TS 119 512 [11] (aneks F, klauzula F2.2 i klauzula 7).

3.1.2 Model skladišta čuvanja

Sadašnja šema čuvanja podržava model skladišta čuvanja „Očuvanje sa skladištenjem (VST)“ prema klauzuli 4.1.2 ETSI TS 119 512 (klauzula 4.3.2).

3.1.3 Podržane operacije

Sa VST modelom skladištenja opisanim u odeljku 3.1.2 moguće su sledeće operacije.

Očuvanje - Podnošenje heš i metapodataka objekta za očuvanje servisu za očuvanje.

Povraćaj - Preuzimanje ranije dostavljenih dokaza o očuvanju od servisa za očuvanje.

Brisanje - Brisanje ranije dostavljenih dokaza o očuvanju i odgovarajućih hešova i metapodataka iz usluge čuvanja.

Preuzimanje - Preuzimanje elementa revizorskog traga iz servisa za očuvanje, koji sadrži informacije u vezi sa relevantnim događajima, koji su se desili u okviru usluge očuvanja za određeni dokaz podnošenja.

Validacija – Potvrđivanje dokaza o očuvanju.

Pretraga - Pretraživanje među dokazima o očuvanju, koji su dostupni naručiocu.

3.1.4 Generisanje i validacija dokaza o očuvanju

Sadašnja šema čuvanja generiše dokaze o čuvanju u obliku evidencije dokaza, koji se objavljuju u elementu Profil/Format dokaza sa sledećim standardima:

- https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.00_30/en_31910201v010100v.pdf

Usluga čuvanja podržava sledeće slučajeve:

čuvanje dokaza na osnovu heša i metapodataka dokumenta koji se čuva u prostorijama klijenta

3.1.5 Povećanje dokaza o čuvanju

Pružalac usluge čuvanja nadgleda podobnost kriptografskih algoritama na osnovu zahteva navedenih u sledećem normativu:

- ETSI TS 119 312 [12]

Na osnovu rezultata praćenja, Pružalac usluge čuvanja nadograđuje dokaze tako što vrši obnavljanje vremenskog žiga na dokazu prema specifičnom formatu potpisa pre nego što kriptografski algoritam postane slab.

3.2 Profil očuvanja

Podržani profil očuvanja je definisan u okviru ovog dokumenta Praktična pravila kvalifikovanog čuvanja u ovom odeljku.

Profil čuvanja je u potpunosti u skladu sa izjavama datim u odeljku Šema očuvanja.

3.2.1 Identifikacija profila očuvanja

Identifikator profila čuvanja:

OID	Naziv
1.3.6.1.4.1.57738.40.2.1.5.0	5. INCEPTION – Praktična pravila kvalifikovanog čuvanja

3.2.2 Ciljevi čuvanja

Videti odeljak 3.1.1

3.2.3 Model čuvanja skladišta

Videti odeljak 3.1.2

3.2.4 Podržane operacije

Videti odeljak 3.1.3

3.2.5 Tehničke odredbe

Sadašnja verzija ovih Praktičnih pravila kvalifikovanog čuvanja dostupna je samo u čitljivom obliku. Pružalac usluge čuvanja trenutno ne podržava automatsko tumačenje bilo koje mašinski čitljive politike.

3.2.6 Rok važenja

Usluga koju pruža Pružalac usluge čuvanja ispunjava zahteve postavljene u ovim Praktičnim pravilima kvalifikovanog čuvanja od njenog objavljivanja 2022.godine. Profil čuvanja je zvanično objavljen u ovom novom obliku u ovim Praktičnim pravilima čuvanja. Profil čuvanja nema datum završetka važenja, podržava ga Dobavljač usluge čuvanja tokom celog životnog veka usluge.

3.2.7 Formati dokaza

Sadašnji profil čuvanja koristi kvalifikovani vremenski žig za očuvanje valjanosti dokaza, koji su identifikovani sledećim URI vrednostima prema formatu elektronskog potpisa ili pečata:

- https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.00_30/en_31910201v010100v.pdf

3.2.8 Ljudski razumljiv format

Profil arhiviranja u ovim Praktičnim pravilima čuvanja je u ljudskom čitljivom formatu i nije namenjen za automatsku mašinsku obradu.

3.2.9 Objavljivanje podržanih profila očuvanja

Podržani profili očuvanja objavljeni su kao deo ovih Praktičnih pravila kvalifikovanog čuvanja.

3.2.10 Dužina trajanja profila očuvanja

Isti profil očuvanja primenjuje se tokom celog perioda čuvanja. Profil očuvanja se ne menja tokom vremena. Svi dinamički aspekti su specificirani izvan profila očuvanja, u politici evidencije o očuvanju ili u politici validacije potpisa. Primenjene smernice za čuvanje dokaza ili politike validacije potpisa mogu se promeniti tokom vremena. Sve verzije koje se odnose na određeni profil očuvanja su javno dostupne i jasno je koja verzija je primenjena u koje vreme.

3.2.11 Podržana politika očuvanja dokaza

Videti odeljak 3.3.

3.2.12 Podržana politika validacije potpisa

Videti odeljak 3.4.

3.3 Politika očuvanja dokaza

3.3.1 Identifikator politike očuvanja dokaza

Identifikator politike:

OID	Naziv
1.3.6.1.4.1.57738.40.2.1.5.0	Politika kvalifikovanog čuvanja

3.3.2 Format politike očuvanja dokaza

Politika dokaza o očuvanju dostupna je samo kao deo ovih Praktičnih pravila u ljudskom čitljivom obliku. Pružalac usluge čuvanja trenutno ne podržava automatsku interpretaciju bilo koje politike o čuvanju čitljivu na mašinskom jeziku.

3.3.3 Kreiranje dokaza o očuvanju

Pružalac usluge čuvanja sprovodi dugoročno očuvanje validnosti elektronskih potpisa redovnim ažuriranjem uskladištenih elektronskih potpisa. Prilikom produženja važenja, na elektronski potpis stavlja arhivski vremenski žig, koji obezbeđuje da se validnost zadržanog originalnog elektronskog potpisa može proveriti još nekoliko godina. Prilikom kreiranja dokaza o čuvanju, Pružalac usluge čuvanja proverava validnost datog elektronskog potpisa, elektronskog pečata i/ili vremenskog žiga.

Tokom verifikacije elektronskog potpisa, elektronskog pečata ili vremenskog žiga, Pružalac usluge čuvanja prati lanac sertifikata do pouzdanog osnovnog ili posredničkog sertifikata prihvaćenog sertifikacionog tela (ili vremenskih žigova) (videti odeljak 1.3.1).

Pružalac usluge čuvanja koristi OCSP uslugu da prikupi informacije o statusu opoziva za svaki element lanca valjanosti. Ako je OCSP period odziva za sve pružaoce u lancu sertifikata 0, sve potrebne informacije o opozivu se generišu za kratko vreme, čak i u sekundama. Ako postoji period odziva duži od 0, Pružalac usluge čuvanja vrši neophodne verifikacije nakon isteka odziva u skladu sa odgovarajućim standardima i međunarodnim preporukama.

Prilikom inicijalne verifikacije, Pružalac usluge čuvanja će odbiti čuvanje e-dokumenta ako verifikacija ne može da se završi u roku od 3 dana.

Pružalac usluge čuvanja gradi lance valjanosti za elektronske potpise, elektronske pečate ili vremenske žigove u e-dokumentima i na njih postavlja kvalifikovani arhivski elektronski vremenski žig. Tako dobijeni lanci validnosti čuvaju se u formatu koji odgovara formatu e-dokumenta kao arhivski potpis u e-dokumentu. Pružalac usluge čuvanja koristi softversku uslugu razvijenu u kompaniji za kreiranje i verifikaciju potpisa, kako bi kreirao dokaze o očuvanju.

3.3.4 Primenjeni kriptografski algoritmi

Pružalac usluge čuvanja nadgleda podobnost kriptografskih algoritama na osnovu zahteva navedenih u normativnom ETSI TS 119 312 [12].

Pružalac usluge čuvanja će koristiti samo kriptografske algoritme za kreiranje dokaza o očuvanju koji ispunjavaju primenljive zahteve i za koje se očekuje da će obezbediti validnost dokaza o očuvanju na duže vreme.

Trenutno, pružalac usluge čuvanja koristi vremenske oznake isključivo sa RSA ključem od 2048-bita za kreiranje dokaza o očuvanju.

Svaki e-dokument koji se šalje Pružaocu usluge čuvanja na čuvanje ima vremenski žig sa najmanje RSA ključem od 2048 bita ili ECC ključem od 256 bita.

3.3.5 Korišćenje drugih usluga od poverenja

Pružalac usluge čuvanja može koristiti usluge drugog pružaoca usluge od poverenja ili autentifikacije na sledeće načine tokom pružanja usluge:

- Usluga vremenskog žiga, koju obezbeđuje Pošta Srbije ili
- Usluga vremenskog žiga od Privredne komore Srbije
- Usluga validacije od Privredne komore Srbije

3.3.6 Validacija dokaza očuvanja

Prilikom validacije dokaza o očuvanju, Pružalac usluge čuvanja verifikuje validnost datog kvalifikovanog vremenskog žiga.

Osim standardnih koraka validacije, Pružalac usluge čuvanja potvrđuje da:

- Potvrda tela za stavljanje vremenskog žiga kojom se potvrđuje autentičnost vremenskog žiga je uključena u Registar kvalifikovanih pružalaca usluga od poverenja

- Sertifikat sertifikacionog tela vremenskog žiga je bio na listi Pružalaca usluga od poverenja

- Sertifikat sertifikacionog tela za vremenski žig je važeći u vreme validacije

- Sertifikat sertifikacionog tela vremenskog žiga pripada kvalifikovanoj usluzi za kvalifikovani vremenski žig sa aktivnim statusom

- izdati vremenski žig je kvalifikovan.

Pružalac usluge čuvanja koristi OCSP uslugu da proveri informacije o statusu opoziva. Dok je OCSP period odziva 0, potrebne informacije o opozivu se generišu za kratko vreme, u sekundama.

3.3.7 Produžavanje trajanja dokaza očuvanja

Pružalac usluge čuvanja nadgleda podobnost kriptografskih algoritama na osnovu zahteva navedenih u normativnom ETSI TS 119 312 [12];

Na osnovu rezultata praćenja, Pružalac usluge čuvanja nadograđuje potpis postavljanjem nove arhivske vremenske oznake na objekat očuvanja u skladu sa specifičnim formatom potpisa pre nego što kriptografski algoritam postane slab.

3.3.8 Format dokaza o očuvanju

Pružalac usluge čuvanja generiše potvrdu o čuvanju u vidu arhivskog vremenskog žiga, koji se postavlja na e-dokument kao njegov sastavni deo kao produžetak e-dokumenta.

Dokazi o očuvanju uključuju standardne PKI elemente:

- ITU X.509 [13] 48 format ROOT i intermediate CA sertifikati pružaoca usluga u lancu važenja
- OCSP odgovori prema IETF RFC 6960 [14] koji potvrđuje validnost sertifikata u lancu važenja
- opcioni dodatni standardni elementi (sertifikati, informacije o statusu opoziva) koji dokazuju validnost OCSP odgovora
- IETF RFC 3161 [15] Vremenski žig za zaštitu dokaza o očuvanju i objekte zaštite

3.3.9 Referenca potvrde prema usluzi čuvanja

Pružalac usluge čuvanja koristi standardne PKI elemente kao dokaze o očuvanju koji ne sadrže eksplicitnu referencu ka pružaocu usluge čuvanja.

3.4 Politika validacije potpisa

3.4.1 Identifikator politike validacije potpisa

Identifikator politike dokaza:

OID	Naziv
1.3.6.1.4.1.57738.40.2.1.5.0	Politika validacije potpisa

3.4.2 Format politike validacije potpisa

Politika validacije potpisa dostupna je samo kao deo ove Praktičnih pravila čuvanja u formatu koji je čitljiv. Pružalac usluge čuvanja trenutno ne podržava automatsku interpretaciju politike validacije potpisa na mašinskom jeziku.

3.4.3 Višejezičnost

Javni dokumenti Pružaoca usluga čuvanja dostupni su na srpskom i engleskom jeziku.

3.4.4 Prikupljanje materijala za validaciju

Pružalac usluge čuvanja proverava da su svi podaci o validaciji potrebni za validaciju potpisa dostupni, prikuplja nedostajuće podatke za validaciju, dodaje ih potpisu i štiti ga kvalifikovanom arhivskom vremenskim žigom koji odgovara datom formatu potpisa. Dokazi su sadržani u e-dokumentu.

Specifičan standard za format potpisa određuje kako se validiraju odgovarajući dokazi. Prilikom provere validnosti potpisa, Pružalac usluge čuvanja sledi shell model, odnosno period važenja svakog sertifikata u lancu važenja mora biti uključen u period važenja sertifikata pružaoca usluga koji ga izdaje.

3.5 Kriptografske kontrole

3.5.1 Vremenski žigovi

Pružalac usluge čuvanja koristi kvalifikovane vremenske žigove koje je izdalo sertifikaciono telo akreditovano za „uslugu izdavanja kvalifikovanog vremenskog žiga u skladu sa EIDAS regulativom“.

Korišćena usluga izdavanja kvalifikovanih vremenskih žigova je u skladu sa zahtevima ETSI EN 319 421 [16] i ETSI EN 319 422 [17] i navedena je u Registru kvalifikovanih pružalaca usluga od poverenja [18] kao kvalifikovana usluga izdavanja vremenskog žiga.

Status opoziva sertifikata vremenskog žiga koje koristi pružalac usluge izdavanja vremenskog žiga može se proveriti na osnovu CRL i OCSP usluge koju pruža pružalac usluge izdavanja vremenskog žiga. U slučaju opoziva sertifikata vremenskog žiga, informacije o statusu opoziva koje pruža Pružalac usluge vremenskog žiga uključuju razlog za opoziv („šifra razloga“).

3.5.2 Kriptografski monitoring

Pružalac usluge čuvanja nadgleda podobnost kriptografskih algoritama na osnovu zahteva navedenih u sledećem normativnom ETSI TS 119 312 [12].

Za svaki podržani aktivni profil čuvanja, Pružalac usluge čuvanja nadgleda kompleksnost svakog kriptografskog algoritma koji je korišćen u vezi sa ovim profilom.

U slučaju da se smatra da jedan od korišćenih algoritama ili parametara postaje manje bezbedan, on ili ažurira odgovarajući dokument o dokazima o očuvanju ili kreira novi profil očuvanja za rukovanje novodostavljenim e-dokumentima.
Tokom čitavog perioda čuvanja, Pružalac usluge čuvanja prati podobnost poslednjeg arhivskog vremenskog žiga postavljenog na svaki e-dokument za očuvanje valjanosti elektronskog potpisa. Pružalac usluge čuvanja stavlja novi arhivski vremenski žig na dati e-dokument u skladu sa aktuelnom politikom čuvanja dokaza, ako:

- bezbednost bilo kog kriptografskog algoritma ili parametra koji se koristi za generisanje poslednjeg vremenskog žiga postaje manje bezbedna ili je njegova upotreba zabranjena primenjivim kriptografskim zahtevima;

- Sertifikat koji se koristi za proveru autentičnosti poslednjeg vremenskog žiga ističe.

3.6 Nadogradnja dokaza o očuvanju

Pružalac usluge čuvanja nadgleda podobnost kriptografskih algoritama na osnovu zahteva navedenih u normativnom ETSI TS 119 312 [12];
Na osnovu rezultata praćenja, Pružalac usluge čuvanja dopunjava potpis stavljajući novi arhivski vremenski žig na e-dokument prema specifičnom formatu potpisa pre nego što kriptografski algoritam postane slab.

3.7 Uvoz-izvoz paketa

Pružalac usluge čuvanja obezbeđuje da Pretplatnik može preuzeti dokaz o očuvanju koji odgovara e-dokumentu koji je dat na čuvanje, tokom perioda važenja ugovora o usluzi.

Pretplatnik ima pristup samo dokazima o očuvanju koji se čuvaju u arhivi Pružaoca usluge očuvanja putem bezbednog kanala.

Preuzimanje se obično vrši preko Interneta korišćenjem interfejsa koji obezbeđuje Pružalac usluge čuvanja kao što je opisano u odeljku 4.3. u detalje.

U svim slučajevima, prenos dokaza o očuvanju se odvija nakon provere identiteta i ovlašćenja primaoca.

U slučaju upita zasnovanog na Internetu, autorizacija se proverava na osnovu podataka za autentifikaciju, IP adrese i drugih dogovorenih bezbednih metoda.

Pružalac usluge čuvanja evidentira sve prenose podataka kao što je opisano u odeljku 6.4. Podaci evidencije uključuju, ali nisu ograničeni na vreme događaja i ID-ove isporučenih dokaza o očuvanju i druge metapodatke povezane sa prenosom podataka.

3.8 Protokol očuvanja

3.8.1 Pristup dokazima o očuvanju i metapodacima e-dokumenta

Pretplatnik uspostavlja SSL/TLS vezu zasnovanu na međusobnoj identifikaciji sa serverom Pružaoca usluge čuvanja koristeći svoj sertifikat za autentifikaciju klijenta ili bezbedne akreditive.

Pružalac usluge čuvanja identifikuje pretplatnika na osnovu sertifikata o autentifikaciji klijenta, koji se koristi za uspostavljanje SSL/TLS veze i/ili bezbednih akreditiva.

Pružalac usluge čuvanja osigurava da Pretplatnik može preuzeti sve svoje dokaze o očuvanju tokom perioda važenja ugovora o usluzi.

Pretplatnik može da obezbedi heš i metapodatke prema Dublin Core [19] u vezi sa elektronskim dokumentima. Detalji su navedeni u odeljku 4.2. ovih Praktičnih pravila o čuvanju.

Pružalac usluge čuvanja verifikuje usklađenost e-dokumenta na osnovu heša i metapodataka otpremljenog e-dokumenta. Nakon provere validnosti elektronskih potpisa i elektronskih pečata pronađenih u metapodacima e-dokumenta, Pružalac usluge čuvanja šalje Pretplatniku potvrdu da je uspešno prihvatio zahtev za čuvanje u roku od 3 dana od postavljanja. Potvrda između ostalog sadrži heš vrednost otpremljenog e-dokumenta, koja se može koristiti kao identifikator e-dokumenta kasnije tokom različitih operacija.

3.8.2 Brisanje sačuvanih dokumenata

Pružalac usluge čuvanja ne briše dokaze o očuvanju koji se čuvaju u arhivi.

3.9 Protokol obaveštenja

Pružalac usluge čuvanja će koristiti elektronsku komunikaciju kao što su e-pošta ili interfejsi na nivou aplikacije (API) za slanje obaveštenja pretplatnicima.

Pružalac usluge čuvanja objavljuje opšte informacije na svojoj veb stranici.

Pružalac usluge čuvanja obaveštava svoje Pretplatnike o promenama javnih propisa putem svoje veb stranice na način opisan u poglavlju 2.1. Praktična pravila pružaoca usluge čuvanja sadrži sve informacije o profilima čuvanja koji se koriste i politikama usluga koje se u njima pominju.

3.10 Proces očuvanja

3.10.1 Dokazi o očuvanju

Pružalac usluge čuvanja koristi kvalifikovane vremenske žigove koje izdaje „Usluga kvalifikovanog vremenskog žigosanja usklađena sa eIDAS-om“ koju obezbeđuje Inception d.o.o za kreiranje arhivskih vremenskih žigova.

Korišćena usluga izdavanja vremenskog žiga navedena je u Registru kvalifikovanih pružalaca usluga od poverenja [18] kao kvalifikovana usluga izdavanja vremenskog žiga i u skladu je sa sledećim zahtevima:

- IETF RFC 3161 [15]

- ETSI EN 319 421 [16]

- ETSI EN 319 422 [17]

3.10.2 Očuvanje digitalnih potpisa

Pružalac usluge čuvanja prihvata samo metapodatke e-dokumenta sa važećim elektronskim potpisom ili pečatom. Učitani metapodaci e-dokumenta opciono mogu sadržati dokaze o validnosti elektronskog potpisa ili pečata, koje prikuplja Pretplatnik.

Kada prima metapodatke e-dokumenta za arhiviranje, Pružalac usluge čuvanja čini sve što može da prikupi i verifikuje podatke o validaciji u skladu sa politikom validacije potpisa koju podržava profil očuvanja, kao što je opisano u odeljku 4.2.

Pružalac usluge čuvanja može da koristi dokaze koje je postavio Pretplatnik, ali u ovom slučaju proverava dostavljene podatke o validaciji u skladu sa politikom validacije potpisa koju podržava profil očuvanja.

Da bi proširio mogućnost validacije elektronskog potpisa ili pečata i da bi zadržao njegov status validnosti, Pružalac usluge čuvanja stavlja arhivski vremenski žig na elektronski potpis ili pečat.

Arhivski vremenski žig na jednoj strani, pruža dokaz o postojanju elektronskog potpisa ili pečata i podatke o validaciji potrebni za validaciju elektronskih potpisa ili pečata, i na na drugoj strani dokaz o postojanju potpisanih podataka.

3.11 Mrežna bezbednost

3.11.1 Pristup sačuvanim dokumentima

Pretplatnici će moći da pristupe dokazima o očuvanju i metapodacima e-dokumenta koji su uskladišteni u servisu preko interfejsa za programiranje aplikacija (API) od strane Pružaoca usluge čuvanja.

Pretplatnici nemaju direktan pristup dokazima o čuvanju koji su povezani sa njima.

3.12 Prestanak pružanja usluge i planovi ukidanja

3.12.1 Sačuvani dokumenti nakon raskida

Pružalac usluge čuvanja ima detaljan plan ukidanja koji utvrđuje zadatke koje treba izvršiti tokom planiranog prekida usluge.
Poglavlje 6.7. ovog dokumenta Praktična pravila čuvanja opisuje glavne informacije o prekidu usluge, uključujući kako upravljati hešom i metapodacima uskladištenog e-dokumenta i dokazima o očuvanju.

3.13 Praktična pravila usluge čuvanja

3.13.1 Podržane politike usluge čuvanja

Poglavlje 1.2. Praktična pravila usluge čuvanja sadrži listu podržanih smernica usluge čuvanja.

3.13.2 Podržani profili očuvanja

Poglavlje 3.1.7. Praktična pravila čuvanja sadrži listu podržani profili očuvanja.

3.13.3 Kako se postižu ciljevi očuvanja

Pružalac usluge čuvanja obezbeđuje dugoročno očuvanje validnosti elektronskih potpisa ili pečata na arhiviranim metapodacima e-dokumenta tako što povremeno dopunjava elektronske potpise ili pečate postavljanjem arhivskog vremenskog žiga.

3.13.4 Dostupnost sačuvanih dokumenata

Poglavlje 5.9. Praktičnih pravilao čuvanja sadrži dostupnost sačuvanih metapodataka dokumenta.

3.13.5 Obaveze svih spoljnih organizacija koje podržavaju uslugu čuvanja

Pružalac usluge čuvanja može koristiti pomoć spoljnih organizacija tokom pružanja usluge, ali je odgovoran Pretplatniku za rad svih saradnika kao svojih. Obaveze bilo kog saradnika regulisane su ugovorom o saradnji zaključenim sa davaocem doprinosa.

3.13.6 Zahtevanje paketa za izvoz-uvoz

Poglavlja 4.2. i 4.3. Praktičnih pravila čuvanja sadrži informacije o otpremanju i preuzimanju podataka.

3.13.7 Upravljanje podacima na kraju perioda očuvanja

Do kraja perioda važenja ugovora o usluzi, Pružalac usluge čuvanja obezbeđuje da se validnost elektronskih potpisa ili pečata postavljenih na otpremljene objekte čuvanja može proveriti. Po isteku ugovora o usluzi, sačuvani objekti očuvanja i povezani arhivski dokazi biće trajno arhivirani.

3.14 Kvalifikovana usluga čuvanja

3.14.1 Pružalac usluge izdavanja vremenskih žigova

Ovaj sertifikat se koristi u produkcionom okruženju za potpisivanje odgovora sa kvalifikovanom vremenskim žigom. Sertifikat je skladišten na siguran način na HSM uređaju. Rok važenja sertifikata je 72 meseca.

Naziv polja sertifikata	**Vrednost polja sertifikata**
Važi od	Ponedeljak, 27. decembar, 2021 10:42:19
Važi do	Ponedeljak, 27. decembar, 2027 10:42:19
Subjekat	CN = Inception TSA 1 200035935 SERIALNUMBER = CA:RS-200035935 O = INCEPTION DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VOŽDOVAC) 2.5.4.97 = VATRS-106893018 2.5.4.97 = MB:RS-20701242 C = RS
Izdato za	Inception TSA 1
Izdavalac	CN = Pošta Srbije CA 1 O = Javno preduzeće Pošta Srbije 2.5.4.97 = VATRS-100002803 L = Beograd C = RS

Naziv polja sertifikata	Vrednost polja sertifikata
Glavna upotreba	Digitalni potpis, bez odbijanja (c0)
Identifikator	aa4cffb508a7b06796e80b26f94cf7b4ad964672
Root	Pošta Srbije CA Root
Intermediate	Pošta Srbije CA 1

3.14.2 Identifikator usluge

Ovaj sertifikat se koristi u produkcionom okruženju za sve druge kriptografske operacije kao što su elektronski izveštaji o isporuci, a takođe se koristi za uslugu čuvanja. Sertifikat je skladišten na siguran način na HSM uređaju. Rok važenja sertifikata je 72 meseca.

Naziv polja sertifikata	Vrednost polja sertifikata
Važi od	Ponedeljak, 27. decembar, 2021 10:50:43
Važi do	Sreda, 27. decembar, 2023 10:50:43
Subjekat	CN = INCEPTION DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VOŽDOVAC) 200035936 SERIALNUMBER = CA:RS-200035936 O = INCEPTION DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VOŽDOVAC) 2.5.4.97 = VATRS-106893018 2.5.4.97 = MB:RS-20701242 C = RS
Izdato za	INCEPTION DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VOŽDOVAC)
Izdavalac	CN = Pošta Srbije CA 1 O = Javno preduzeće Pošta Srbije 2.5.4.97 = VATRS-100002803 L = Beograd C = RS
Glavna upotreba	Digitalni potpis, bez odbijanja (c0)
Identifikator	c2317e5b13158dedcc58991ed8cf97826c859bec
Root	Pošta Srbije CA Root

Naziv polja sertifikata	Vrednost polja sertifikata
Intermediate	Pošta Srbije CA 1

4 Opisivanje procesa usluge čuvanja

Pružalac usluge čuvanja pruža pretplatniku uslugu elektronskog dugoročnog čuvanja kao eIDAS kvalifikovanog pružaoca usluga od poverenja u okviru Ugovora o usluzi. Servis sadrži sledeće glavne servisne jedinice:

- Pretplatnik može da otpremi elektronski potpisan heš i metapodatke e-dokumenta u arhivu kojom upravlja Pružalac usluge čuvanja. Prilikom prijema heš i metapodataka e-dokumenta, Pružalac usluge čuvanja proverava elektronski potpis(e) ili pečat(e) iz metapodataka e-dokumenta, dopunjava ili sastavlja dokaze o očuvanju, stavlja vremenski žig za elektronsku arhivu na dokaz o očuvanju, i čuva heš i metapodatke prihvaćenog e-dokumenta kao objekta za očuvanje. (videti odeljak 4.2).

- Pružalac usluga čuvanja na bezbedan način čuva objekat čuvanja – heš i metapodatke dokumenta i dokaze o očuvanju – i obezbeđuje da tokom celog perioda čuvanja:

  – samo ovlašćena lica imaju pristup sačuvanim podacima

  – ovlašćeni Pretplatnik ima kontinuiran pristup sačuvanim podacima

  – sačuvani podaci se ne mogu menjati bez ovlašćenja.

- Pružalac usluge čuvanja obezbeđuje dugoročnu validnost elektronskih potpisa i pečata postavljenih na e-dokumentima. Pružalac usluge čuvanja obezbeđuje dugoročnu čitljivost predmeta konzervacije tokom perioda čuvanja. Period čuvanja je trajan.

- Pretplatnik ima kontinuiran pristup objektu očuvanja u arhivi Pružaoca usluge očuvanja i odgovarajućim dokazima o očuvanju (pogledajte odeljak: 4.3).

- Na zahtev Pretplatnika, Pružalac usluge čuvanja izdaje autentičnu potvrdu da čuva predmet čuvanja, te da su u trenutku prijema u arhivu bili važeći elektronski potpisi ili pečati iz metapodataka e-dokumenta (videti odeljak: 4.4).

Pružalac usluge čuvanja u okviru ove usluge obezbeđuje dugoročno očuvanje validnosti elektronskih potpisa i pečata, pa prihvata samo heš i metapodatke e-dokumenta iz e-dokumenata sa važećim elektronskim potpisom ili pečatom u trenutku prijema.

Pružalac usluge čuvanja prihvata samo heš i metapodatke e-dokumenta iz e-dokumenata sa elektronskim potpisom ili pečatom, kada

- svi elektronski potpisi i pečati su opremljeni vremenskim žigom

- format elektronskih potpisa i pečata je u skladu sa zahtevima jednog od sledećih:

  - XAdES ETSI TS 101 903 [20] [21] [22] [23]
  - PAdES PDF/A format (ISO 19005) [24]
  - XAdES ETSI EN 319 132 [25], [26]
  - PAdES ETSI EN 319 142 [27], [28]
  - AdES ETSI TS 119 102 [29] [30]
  - JAdES (staviti etsi)

Sertifikat jedinice izdavaoca vremenskog žiga i sertifikat koji se koristi za kreiranje elektronskog potpisa ili pečata će se pratiti do izvora ili posrednika sertifikata
Pružaoca usluge čuvanja koji se smatra od poverenja.

4.1 Otpremanje objekta očuvanja

Pružalac usluge čuvanja prihvata samo heš i metapodatke e-dokumenta koji se arhiviraju nakon identifikacije Pretplatnika u okviru bezbedne procedure. Postupkom se obezbeđuje integritet, poverljivost e-dokumenata.

Otpremanje se obično odvija preko Interneta korišćenjem interfejsa koji obezbeđuje Pružalac usluge čuvanja na sledeći način:

1. Pretplatnik kreira SSL/TLS vezu sa Pružaocem usluge očuvanja na osnovu međusobne autentifikacije koristeći svoj klijentski sertifikat za autentifikaciju i/ili bezbedne akreditive. Pružalac usluge očuvanja identifikuje pretplatnika na osnovu sertifikata za autentifikaciju klijenta koji se koristi za uspostavljanje SSL/TLS veze i/ili bezbednih akreditiva. Pretplatnik može da otpremi heš i metapodatke e-dokumenta preko SSL/TLS veze u arhivu Pružaoca usluge očuvanja.

2. Pružalac usluge čuvanja proverava usklađenost e-dokumenta na osnovu metapodataka otpremljenog e-dokumenta prema sledećem:

   - u slučaju e-dosijea Pružalac usluge čuvanja proverava da li je otpremljeni e-dosije u ispravnom formatu, tako da je u skladu sa specifikacijom e-dokumenta objavljenom na veb stranici Pružaoca usluge čuvanja. Učitani e-dosije može da sadrži i jedan ili više elektronskih dokumenata. E-dosije može da sadrži elektronske potpise ili pečate na elektronskim dokumentima, ali može da sadrži i okvirni potpis, koji obezbeđuje integritet svakog elektronskog dokumenta i svakog potpisa, pečata i vremenskog žiga na elektronskom dokumentu u e-dokumentu. Ako e-dosije sadrži potpis okvira, pružalac usluge čuvanja samo verifikuje potpise okvira (unutrašnji potpisi i pečati nisu verifikovani). Ukoliko e-dosije ne sadrži okvirni potpis, Pružalac usluge čuvanja verifikuje svaki elektronski potpis i pečat

na elektronskim dokumentima uključenim u e-dosije. Ukoliko Pretplatnik treba da obezbedi validnost potpisa okvira i unutrašnjih potpisa i pečata onda mora da dostavi e-dosije sa i bez potpisa okvira. Bez okvirnog potpisa, na svaki elektronski dokument uključen u e-dosije stavlja se najmanje jedan važeći elektronski potpis ili pečat. Pružalac usluge čuvanja odbija one e-dosijee na kojima je elektronski potpis ili pečat overen prema bilo čemu od gore navedenih nevažeći ili one koji sadrže nepotpisane elektronske dokumente.

- u slučaju PAdES formatiranog e-dokumenta, dobavljač usluge čuvanja potvrđuje da je otpremljeni format e-dokumenta u PAdES formatu usklađen sa bilo kojim od podržanih formata. E-dokument u PAdES formatu može sadržati i druge elektronske dokumente. Pružalac usluge čuvanja proverava validnost svih potpisa i pečata, ali čuva validnost samo poslednjeg, spoljašnjeg potpisa ili pečata. Pružalac usluge čuvanja zahteva da postoji važeći elektronski potpis ili pečat i interni vremenski žig na otpremljenom e-dokumentu u PDF formatu. Pružalac usluge čuvanja ne prihvata u svoju arhivu objekat očuvanja bez vremenskog žiga ili sa spoljnim vremenskim žigom.

3. Prilikom provere valjanosti svakog elektronskog potpisa ili pečata Pružalac usluge čuvanja proverava da li potpis ili pečat odgovara metapodacima datog e-dokumenta. Nakon toga pokušava da uđe u trag datom potpisu ili pečatu do pouzdanog osnovnog sertifikata (pogledajte odeljak: 1.3.1), i proverava status opoziva svakog elementa lanca sertifikata na osnovu OCSP-a. Procedura prihvatanja se nastavlja samo ako se dokaže validnost svakog elektronskog potpisa, pečata i vremenskog žiga u metapodacima e-dokumenta. Pružalac usluge čuvanja koristi aplikaciju Inception kreator potpisa i validator za validaciju potpisa. Pružalac usluge čuvanja pruža uslugu dugoročnog čuvanja samo onih podataka – odnosno prihvata takve objekte čuvanja – na kojima se može naći barem napredni elektronski potpis ili pečat. Tokom verifikacije elektronskog potpisa, pečata ili usluge čuvanja vremenskog žiga, dobavljač usluge prati lanac sertifikata do pouzdanog osnovnog sertifikata prihvaćenog sertifikacionog tela (ili vremenskog žiga). Može se desiti da sertifikaciono telo izda testni sertifikat koji može biti verifikovan njegovim pouzdanim osnovnim sertifikatom. Pružalac usluge čuvanja ne može da razlikuje takav sertifikat od pravog sertifikata – prikladnog za kreiranje naprednih ili kvalifikovanih elektronskih potpisa ili pečata – i nije odgovoran za bilo kakvu nastalu štetu. U slučaju da Pružalac usluge čuvanja ne prihvati predmet čuvanja, on čuva 3 dana informacije koje mogu pomoći da se utvrdi uzrok odbijanja. Takve informacije su, između ostalog, elektronski potpis, pečat, potpisni sertifikat i njihovi lanci sertifikata, i sertifikati vremenskih žiga i njihovi lanci sertifikata i odgovarajući heš i usputni metapodaci uključeni u e-dokument.

4. Pružalac usluge čuvanja prikuplja informacije o statusu opoziva koje nedostaju koristeći OCSP uslugu. Ako je OCSP grejs period za svakog provajdera u lancu sertifikata 0, tada su informacije o opozivu dostupne – za samo nekoliko sekundi. Ako postoji grejs period duži od 0, onda pružalac usluge čuvanja vrši neophodne verifikacije nakon isteka grejs

perioda u skladu sa odgovarajućim standardima i međunarodnim preporukama. Pružalac usluge čuvanja odbija objekat očuvanja ako ne može da izvrši verifikaciju u roku od 3 dana. Pružalac usluge čuvanja sastavlja dokaze o očuvanju koji odgovaraju elektronskim potpisima i pečatima u metapodacima e-dokumenta i stavlja na njih kvalifikovani arhivski elektronski vremenski žig. On postavlja rezultujući dokaz o očuvanju u formatu ETSI TS 101 903 [20] [21] [22] [23], naime kao arhivski potpis u objekat zaštite.

5. Pružalac usluge čuvanja čuva nešifrovani objekat očuvanja da bi se arhivirao šifrovan u e-dosijeu sa ključem provajdera koristeći kriptografski algoritam i parametar ključa koji se smatraju sigurnim na duži rok. Nešifrovane kopije prihvaćenog objekta očuvanja uništava Pružalac usluge čuvanja korišćenjem takve procedure koja obezbeđuje da se heš i metapodaci e-dokumenta ne mogu vratiti (ili samo uz nerealno visoke finansijske izdatke).

6. Pružalac usluge čuvanja šalje Pretplatniku potvrdu da je uspešno prihvatio objekat čuvanja u najkraćem mogućem roku, a najviše u roku od 3 dana od otpremanja. Ako je proces negde prekinut, Dobavljač usluge čuvanja takođe obaveštava Pretplatnika. U ovom slučaju pretplatnik dobija poruku o grešci koja ga obaveštava da pružalac usluge očuvanja nije mogao da prihvati heš i metapodatke elektronskog dokumenta (na primer zato što nije mogao da izgradi lanac sertifikata). Pružalac usluge čuvanja šalje potvrde i poruke o greškama elektronskom poštom ili putem kanala koji je prethodno dogovoren sa Pretplatnikom. Potvrda sadrži heš e-dokumenta koji je dostavljen arhivi i da li je arhiva prihvatila heš i metapodatke elektronskog dokumenta. Osim toga, u slučaju uspešnog prijema uključuje:

    - heš e-dokumenta primljenog u arhivu – koji već sadrži arhivske elektronske potpise, pečate – koji u daljem tekstu služi kao jedinstveni identifikator,

    - identifikator Politike kvalifikovanog čuvanja,

    - jasna identifikacija da je usluga usluga dugoročnog čuvanja u skladu sa eIDAS-om i podleže Zakonu o elektronskoj upravi.

Potvrda može sadržati i druge informacije. Uspešna potvrda prihvatanja je potvrđena kvalifikovanim elektronskim pečatom i kvalifikovanim vremenskim žigom. Pretplatnik će se uveriti da potvrda zaista odgovara otpremljenom objektu čuvanja (odnosno da li sadrži heš učitanog e-dokumenta), kao i da je elektronski pečat na potvrdi validan. Potvrda je elektronski zapečaćeni dokument, tako da, ukoliko Pretplatnik treba da sačuva autentičnost potvrde na duži rok, postupi po normativima koji se odnose na očuvanje validnosti elektronski zapečaćenih dokumenata. Ukoliko Pretplatnik u ostavljenom roku ne dobije pozitivnu potvrdu, smatra se da Pružalac usluge očuvanja nije prihvatio heš i metapodatke e-dokumenta kao objekat čuvanja. Pružalac usluge očuvanja je isključivo odgovoran za očuvanje heš i metapodataka e-dokumenta i za obezbeđivanje dugoročne verodostojnosti uključenih elektronskih potpisa i pečata u slučaju slanja pozitivne potvrde.

Pružalac usluge očuvanja pruža višestruke mogućnosti za otpremanje putem interneta, na primer

- softver za otpremanje za Inception klijente (lokalno rešenje);
- funkcija za otpremanje arhive ugrađena u Inception klijenta na https://app.epismonosa.rs URL;
- funkcija automatskog arhiviranja integrisana u druge usluge preko APIs

4.2 Obezbeđivanje materijala za validaciju/Dostupnost dokaza o očuvanju – preuzimanje dokaza o očuvanju

Pružalac usluge čuvanja obezbeđuje da Pretplatnik može da preuzme odgovarajući dokaz o čuvanju e-dokumenta tokom perioda važenja ugovora o usluzi.
Pretplatnik ima pristup samo dokazima o očuvanju koji se čuvaju u arhivi Pružaoca usluge očuvanja putem bezbednog kanala.
Preuzimanje se vrši putem interneta korišćenjem interfejsa koji obezbeđuje dobavljač usluge očuvanja prema sledećem:

1. Pretplatnik uspostavlja SSL/TLS vezu zasnovanu na međusobnoj identifikaciji sa serverom Pružaoca usluge očuvanja koristeći svoj sertifikat za autentifikaciju klijenta. Pružalac usluge očuvanja identifikuje pretplatnika na osnovu sertifikata za autentifikaciju klijenta koji se koristi za uspostavljanje SSL/TLS veze.

2. Pretplatnik bira objekat čuvanja kome želi da pristupi. Da bi odabrao pravi objekat za očuvanje, on ima mogućnost da traži objekat za očuvanje preko Aplikacionog programskog interfejsa (API), koji obezbeđuje Pružalac usluge čuvanja. Selekcija se vrši prema identifikatoru na osnovu heša koji jasno identifikuje e-dokument.

3. Pružalac usluge čuvanja određuje da li Pretplatnik ima pravo na pristup izabranom objektu čuvanja i dokazima o očuvanju.

4. U slučaju odgovarajućih prava pristupa, Pružalac usluge čuvanja traži objekat očuvanja sačuvan u šifrovanom e-dosijeu u arhivi na osnovu navedenog heš baziranog identifikatora i šalje dokaz o očuvanju Pretplatniku u zavisnosti od tipa objekta očuvanja kao u nastavku:

- u slučaju e-dosijea kodira ga javnim ključem koji odgovara Sertifikatu za šifrovanje Pretplatnika, i putem zaštićene SSL/TLS veze šalje tako ponovo šifrovani e-dosije Pretplatniku.

- u slučaju PAdES formatiranog e-dokumenta, šalje dekodirani objekat očuvanja nešifrovan preko zaštićene SSL/TLS veze Pretplatniku.

Pružalac usluge čuvanja ne garantuje preuzimanje dokaza o čuvanju ako je Pretplatnik prethodno podneo zahtev za brisanje objekta za očuvanje.

5. U slučaju čuvanja na bazi e-dosijea, Pretplatnik poseduje privatni ključ koji odgovara njegovom Sertifikatu za šifrovanje prijavljen za korišćenje usluge dugoročnog čuvanja. Ovim ključem on dekodira e-dosije, dobijajući pristup dokazima o očuvanju koji se čuvaju u e-dosijeu.

Otpremljeni objekat očuvanja (heš i metapodaci e-dokumenta) su vlasništvo Pretplatnika (pogledajte odeljak: 1.3.2), tako da Pretplatnik takođe igra ulogu administratora podataka. Ako treća strana ima pristup predmetu čuvanja i dokazima o čuvanju, onda on nastupa u ime Pretplatnika.

4.3 Izdavanje potvrde

Na zahtev Pretplatnika, Pružalac usluge čuvanja izdaje potvrdu u vezi sa e-dokumentom. Priznanje se sastoji od sledećeg:

1. Izjava da su napredni ili kvalifikovani elektronski potpisi, pečati, vremenski žigovi na heš-u datog e-dokumenta, metapodaci i odgovarajući sertifikati bili važeći u vreme vremenskog žigosanja 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 u e-dosijeu sa kvalifikovanim elektronskim potpisom. Potvrdu kreira službeno lice odgovorno za izdavanje arhivskog potvrde, au slučaju elektronske potvrde stavlja svoj kvalifikovani elektronski potpis i kvalifikovani vremenski žig.

Izdavanje potvrde može se desiti na način da Pretplatnik pruži Pružaocu usluge čuvanja predmet čuvanja. Zatim, pod uslovom da arhiva Pružaoca usluge čuvanja sadrži objekat

očuvanja sa istim hešom kao i predstavljeni objekat zaštite, službeno lice Pružaoca usluge čuvanja izdaje potvrdu u vezi sa predstavljenim objektom čuvanja.

Pretplatnik može zahtevati izdavanje potvrde od Pružaoca usluge čuvanja podnošenjem elektronskog zahteva overenog najmanje naprednim elektronskim potpisom ili pečatom koji se zasniva na kvalifikovanom sertifikatu.
Izdavanje potvrde može zahtevati ovlašćeni predstavnik Pretplatnika ako je prethodno predočio ovlašćenje Pretplatnika u dokumentu koji sadrži i njegov potpis.
Za traženje potvrde Pretplatnik (ili njegov zastupnik) će dostaviti heš e-dokumenta u vezi sa kojim traži potvrdu. Ove informacije se mogu dobiti iz interfejsa za pretragu opisanog u odeljku 4.3. Potvrdu izdaje Pružalac usluge čuvanja Pretplatniku kome odgovaraju heš i metapodaci datog e-dokumenta prema IT sistemu Pružaoca usluge čuvanja. Pružalac usluge čuvanja izdaje potvrdu trećem licu samo u slučaju da predoči prethodno pomenuto ovlašćenje.

4.4 Raskid ugovora o usluzi

Pružalac usluge čuvanja stavlja na raspolaganje dokaze o čuvanju koji odgovaraju Pretplatniku za preuzimanje Pretplatniku ili drugom ovlašćenom licu 60 dana nakon raskida ugovora o usluzi. Nakon isteka roka, Pretplatnik neće moći da pristupi dokazima o čuvanju i podacima koji odgovaraju Pretplatnikovom objektu očuvanja.

5 Tehničke mere bezbednosti

5.1 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 očuvanja koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih modifikacija. I pružalac usluga očuvanja, i dobavljač sistema i izvođači montaže imaju značajno iskustvo u uslugama sertifikacije zgrada i koriste međunarodno priznatu tehnologiju.

Pružalac usluga čuvanja čuva arhivirane objekte zaštite u fizički zaštićenom okruženju, u skladu sa fizičkim i proceduralnim zahtevima opisanim u odeljku 6, čiju bezbednost garantuju politike unutrašnje bezbednosti i redovne unutrašnje i eksterne bezbednosne revizije. Pružalac usluge čuvanja dostavlja dokaze o čuvanju trećoj strani (npr. organu) samo ako to Pretplatnik ovlasti ili kada je to zakonom propisano.

Integritet uskladištenih e-dosijea obezbeđen je fizičkom zaštitom e-dosijea, kao i tehnologijama vezanim za elektronske potpise. Dostupnost evidencije o očuvanju obezbeđena je kvalitetnim sistemom Pružaoca usluge čuvanja 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 uništava arhivirane objekte čuvanja – na zahtev Pretplatnika. Pružalac usluge očuvanja kreira ključeve za potpisivanje koji se koriste u potvrdama, ključeve koji se koriste za šifrovanje/dešifrovanje arhiviranih e-dokumenata i infrastrukturne i sistemske kontrolne ključeve u kriptografskom hardverskom uređaju. Pružalac usluga čuvanja periodično menja ove ključeve. Pružalac usluge čuvanja prati razvoj tehnologije i ako otkrije da ključ više nije bezbedan ili algoritam više nije upotrebljiv prema odluci Ministarstva trgovine, turizma i telekomunikacija, odmah zamenjuje zahvaćeni ključ ili ključeve. Pružalac usluga čuvanja čuva objekte čuvanja u šifrovanim e-dosijeima.

5.2 Mere predostrožnosti za računarsku bezbednost

Pružalac usluga čuvanja koristi pouzdane IT sisteme i rešenja, tehnologije i razvio je redundantni sistem. Dve instance rade za sve kritične komponente sistema dobavljača usluga, a u slučaju kvara bilo koje od tih jedinica, druga jedinica preuzima operaciju. Ključevi za potpisivanje potvrde, ključevi potrebni za šifrovanje/dešifrovanje arhiviranih podataka i infrastrukturni i sistemski kontrolni ključevi se generišu u kriptografskom hardverskom uređaju.

5.3 Tehničke mere predostrožnosti vezane za životni ciklus

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

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

5.4 Redovna sertifikcija

Pružalac usluga očuvanja je obavezan da stavi vremenski žig koji je izdao kvalifikovani pružalac usluge od poverenja ili da stavi vremenski žig 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 čuvanja.

5.5 Ponovno šifrovanje arhive

Pružalac usluga čuvanja čuva arhivirane objekte čuvanja šifrovane u e-dosijeu u arhivi. Osigurava da su arhivirani objekti očuvanja šifrovani algoritmom za šifrovanje koji je siguran u svakom trenutku.
Pružalac usluge čuvanja trenutno koristi SHA 256 algoritam za šifrovanje sa jedinstvenim ključem za šifrovanje za svaki e-dosije. Jedinstveni simetrični ključ za šifrovanje je zaštićen RSA-baziranim ključem za šifrovanje od 2048 bita Pružaoca usluge čuvanja.

Pružalac usluge čuvanja obezbeđuje da se objekti čuvanja ponovo šifruju ako:

- algoritam koji se koristi za šifrovanje gubi poverenje – u ovom slučaju ih treba ponovo šifrovati algoritmom koji se smatra bezbednim u vreme šifrovanja;
- ugrožena je poverljivost ključa za dekodiranje Pružaoca usluge očuvanja;
- Izjava o kvalifikovanoj praksi čuvanja ili ugovor zaključen sa Pretplatnikom to zahteva.

Nakon što je Pružalac usluge čuvanja ponovo šifrovao arhivirane objekte čuvanja na bezbedan način, uništava prethodne kopije šifrovane na način koji se smatra nedovoljno bezbednim.

5.6 Kontinuirano praćenje tehnologije

Pružalac usluga čuvanja kontinuirano prati razvoj tehnologije u vezi sa elektronskim potpisom i kriptografijom. Ukoliko Pružalac usluge čuvanja sazna da kriptografski algoritam sa datim parametrom koji prihvata eIDAS ili nadležno ministarstvo u Srbiji više nije bezbedan, o tome obaveštava eIDAS ili nadležno ministarstvo u Srbiji i zahteva reviziju odluke koja se odnosi na kriptografske algoritme. 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 odlukom eIDAS-a ili nadležnog ministarstva u Srbiji.

5.7 Prihvatanje izdavaoca sertifikata i vremenskog žiga

Videti odeljak 3.3.5.

5.8 Dostupnost određenih elemenata usluge elektronskog očuvanja

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

- elektronsko preuzimanje dokaza o očuvanju odgovarajućih arhiviranih objekata zaštite 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 očuvanja. Služba za korisnike Pružaoca usluga čuvanja prihvata zahteve za izdavanje verifikacije svakog radnog dana tokom radnog vremena; izdavanje verifikacija se odvija manje od 3 dana.

Radno vreme korisničke službe Pružaoca usluga čuvanja je u odeljku 1.3.1.

6 Kontrole objekata, upravljanja i rada

Pružalac usluga čuvanja primenjuje fizičke, proceduralne i mere bezbednosti osoblja koje su u skladu sa priznatim standardima, zajedno sa administrativnim i upravnim procedurama koje ih primenjuju.
Pružalac usluge čuvanja koristi zaštitne mere proporcionalne rizicima u vezi sa pojedinačnim elementima.
Pružalac usluge čuvanja prati zahteve za kapacitetom i osigurava da su adekvatna procesorska snaga i skladištenje dostupni za pružanje usluge.

6.1 Fizičke kontrole

Pružalac usluga čuvanja vodi računa da fizički pristup kritičnim uslugama bude kontrolisan i da fizički rizik imovine koja se odnosi na kritične usluge drži na minimumu. Svrha fizičkih mera predostrožnosti je sprečavanje nezakonitog pristupa, oštećenja i neovlašćenog pristupa informacijama i fizičkim zonama Pružaoca usluge čuvanja.

Usluge koje obrađuju kritične i osetljive informacije implementiraju se na bezbednim lokacijama u sistemu Pružaoca usluga čuvanja.

Da biste obezbedili adekvatnu sigurnost:

- Pružalac usluga čuvanja implementira strogo zaštićene usluge na lokacijama centra podataka koje koristi. Data centre koje koristi pružalac usluge čuvanja su dizajnirani i konstruisani posebno za ovu svrhu, svojim dizajnom ujednačenim sprovođenjem različitih aspekata zaštite (pozicioniranje i struktura lokacije, fizički pristup (kontrola pristupa i nadzor), napajanje, klimatizacija, zaštita od curenja vode i poplava, prevencija i zaštita od požara, skladištenje medija itd.).

- Pružalac usluge čuvanja implementira svaku kritičnu uslugu i svaki neophodan alat u zasebnoj bezbednosnoj zoni.

6.1.1 Lokacija i izgradnja

IT sistem Pružaoca usluga čuvanja je raspoređen na tri obezbeđena data centra sa fizičkom i logičkom zaštitom koja sprečava nelegitiman pristup.

Odbrambena rešenja – kao što su na primer zaštita, sigurnosne brave, sistemi za detekciju upada, sistem video nadzora, sistem kontrole pristupa – primenjuju se tokom lociranja i uspostavljanja Data centra koji su međusobno izgrađeni i međusobno zavisni i zajedno pružaju

moćnu zaštitu. sistem za IT sisteme koji učestvuju u pružanju usluga i za očuvanje poverljivih podataka koje čuva Pružalac usluga čuvanja.

6.1.2 Fizički pristup

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

Pružalac usluga očuvanja obezbeđuje da:

- Svaki ulazak u Data centre bude registrovan;
- ulazak u Data centre može se desiti samo nakon istovremene identifikacije dva ovlašćena člana osoblja sa pouzdanim ulogama – a najmanje jedan od članova osoblja treba da bude administrator sistema;
- lica bez nezavisnog ovlašćenja mogu boraviti u Data centrima samo u opravdanim slučajevima, potrebno vreme i u pratnji osoblja sa odgovarajućim pravima
- će se dnevnici unosa kontinuirano arhivirati i evaluirati.

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 informaije su fizički van domašaja
- prijavljeni terminali ne ostaju bez nadzora;
- ne sprovodi se radni proces tokom kojeg se mogu otkriti poverljive informacije.

Prilikom napuštanja računarske sobe administrator će proveriti da:

- svaka oprema Data centra je u adekvatno bezbednom radnom stanju;
- nema terminala koji je ostao prijavljen,
- fizički uređaji za skladištnje su pravilno zaključani,
- sistemi, uređaji koji obezbeđuju fizičku zaštitu rade ispravno,
- alarmni sistem je aktiviran.

Imenovani su odgovorni ljudi koji vrše redovne procene fizičke bezbednosti. Rezultati ispitivanja se upisuju u odgovarajuće evidencije.

6.1.3 Napajanje i klimatizacija

Pružalac usluge čuvanja je obezbedio da njihovi provajderi Data centra imaju jedinice za neprekidno napajanje (UPS) i rezervne generatore koji:

- imaju adekvatan kapacitet da obezbede napajanje za svoje objekte i sisteme,
- štiti IT opremu od fluktuacija napona u spoljnoj mreži, nestanka struje, skokova i drugog
- u slučaju dugotrajnog nestanka struje imaju dovoljno kapaciteta i mogućnosti dopunjavanja goriva da pokreće generatore u bilo kom vrmenskom periodu.

6.1.4 Izloženost vodi

Oprema u Data centrima Pružaoca usluga čuvanja je adekvatno zaštićena od prodora vode i poplava.

6.1.5 Prevencija i zaštita od požara

Provajderi u Data centrima Pružaoca usluga čuvanja imaju sisteme za zaštitu od požara odobrene od nadležnih organa. Detektori dima i požara automatski upozoravaju vatrogasnu brigadu. Na jasno vidljivim mestima u svakoj prostoriji nalazi se vrsta i količina ručnih aparata za gašenje požara u skladu sa važećim propisima.

6.1.6 Skladištenje medija

Pružalac usluga čuvanja štiti svoje medijske skladišta od neovlašćenog pristupa i slučajnog oštećenja. Svi revizijski i arhivski podaci se kreiraju u duplikatu. Dve kopije se čuvaju fizički odvojene jedna od druge na različitim lokacijama Data centara i u Cloud-u.

Skladišteni mediji su zaštićeni od štetnih uticaja okoline kao što su niske ili visoke temperature, prljavština, vlaga, sunčeva svetlost, jaka magnetna polja, jako zračenje.

6.1.7 Odlaganje otpada

Pružalac usluga očuvanja obezbeđuje odlaganje suvišne imovine i medija u skladu sa ekološkim standardima.

Pružalac usluge čuvanja ne koristi elektronske medije za skladištenje koji sadrže informacije klasifikovane kao poverljive čak ni za skladištenje podataka koji su klasifikovani kao nepoverljivi nakon brisanja njihovog sadržaja i takvi uređaji se ne smeju iznositi van prostorija Pružaoca usluge čuvanja. Pružalac usluge čuvanja fizički uništava – u skladu sa pravilima odlaganja – neispravne iz bilo kog drugog razloga neupotrebljive, suvišne medijske skladišta koja sadrže poverljive poverljive informacije:

- secka papirna dokumenta u mašini za seckanje
- rastavlja čvrste diskove i razbija kritične komponente

6.1.8 Bekap van lokacije

Pružalac usluge čuvanja svakog dana kreira rezervne kopije iz kojih bi se cela usluga mogla vratiti u slučaju fatalne greške.

Rezervne kopije – barem uključujući poslednju potpunu rezervnu kopiju – čuvaju se na različitim lokacijama centra podataka sa fizičkom i operativnom zaštitom identičnom primarnoj lokaciji. Bezbedan prenos podataka sa primarnih na rezervne lokacije uspostavlja se preko VPN-a.

6.2 Proceduralne kontrole

Proceduralne mere predostrožnosti imaju za cilj da dopune, a istovremeno intenziviraju delotvornost fizičkih mera zaštite, zajedno sa onima koje se primenjuju na osoblje, putem imenovanja i izolovanja pouzdanih uloga, dokumentovanja odgovornosti različitih uloga, kao i preciziranja broja zaposlenih i uloge isključivanja neophodne za različite zadatke, štaviše identifikacija i autentifikacija koja se očekuje u različitim ulogama.

Pojedinci odgovorni za dati sistemski element ili proces se nedvosmisleno dodeljuju svakom elementu sistema i svakom procesu u njegovom sistemu. Zadaci vezani za razvoj i operacije oštro su razdvojeni u sistemu pružaoca usluga očuvanja.

6.2.1 Poverljive uloge

Pružalac usluga očuvanja definiše sledeće pouzdane uloge, sa sledećim odgovornostima:

Menadžer Implementacije

Osoba koja pruža usluge poverenja, operativno upravljanje.

Inženjer baza podataka

Odgovoran za upravljanje bazom podataka (instalacija, održavanje, strukturne promene). Planira trenutnu i buduću dostupnost, nadgleda i optimizuje bazu podataka.

Sistem inženjer

Inženjer infrastrukture, takođe sistem administrator. Pojedinac sa zadatkom upravljanja hardverom kao i administracije operativnog sistema i održavanja rezervnih kopija. Sistem inženjer je odgovoran za redovno održavanje sistema (nadogradnje, dopune).

Služenik obezbeđenja

Viši saradnik za obezbeđenje, lice sa ukupnom odgovornošću za bezbednost Službe, odnosno učešće u sprovođenju bezbednog rada sistema, sprovođenje internih kontrola itd.
Samo one osobe mogu imati ulogu od poverenja koje su u radnom odnosu sa Pružaocem usluga čuvanja. Uloge od poverenja neće se obavljati u kontekstu ugovora o proviziji.

Inženjer za podršku

Odgovoran za brigu o pretplatnicima, komunikaciju sa pretplatnicima, doprinos rešavanju incidenata.

Administrativni radnik

Odgovoran za upravljanje dokumentacijom kompanije, čuvanje dokumenata po klasifikacijama.

Pravni savetnik

Odgovoran je za poštovanje važnih zakona EU i Srbije, međunarodnih standarda i preporuka. Priprema predloga neophodnih izmena i dopuna usled zakonskih, tehnoloških ili organizacionih promena i saznanja u praksi.

Interni revizor

Odgovoran za procenu i proveru adekvatnosti i efektivnosti kontrola, sistema i procedura, predloge za unapređenje sistema upravljanja, savete o pripremi internih akata, smernica, obrazovnih programa, vođenje potrebnih evidencija i izveštaja za delatnost.

6.2.2 Broj potrebnih osoba po zadatku

Bezbednosna i operativna regulativa Pružaoca usluga očuvanja definiše da se sledeći poslovi mogu obavljati samo u zaštićenom okruženju, uz istovremeno prisustvo dva zaposlena koji imaju uloge od poverenja:

- generisanje sopstvenog para ključeva servisa Pružaoca usluga čuvanja;
- rezervnu kopiju 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.

Službenici za očuvanje odgovorni su za bezbedno upravljanje dešifrovanim objektom čuvanja i za njegovo uništavanje ako je potrebno.

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

6.2.3 Identifikacija i autentifikacija za svaku ulogu

Korisnici koji upravljaju IT sistemom Pružaoca usluge čuvanja imaju 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 se bez odlaganja opozivaju u slučaju prestanka prava korisnika.
Svaki korisnik IT sistema i svaki akter u administrativnom procesu identifikuje se pojedinačno.

6.2.4 Uloge koje zahtevaju razdvajanje dužnosti

Zaposleni kod Pružaoca usluga čuvanja mogu imati više pouzdanih uloga u isto vreme, ali Pružalac usluga čuvanja obezbeđuje da:

- službenik za bezbednost neće imati ulogu nezavisnog revizora sistema;
- administrator sistema neće imati ulogu službenika za bezbednost i nezavisnog revizora sistema;

- menadžer implementaije sa opštom odgovornošću za IT sistem neće imati ulogu službenika za bezbednost i nezavisnog revizora sistema.

Pored navedenog, Pružalac usluge čuvanja traži potpuno razdvajanje uloga od poverenja.

6.3 Kontrola osoblja

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

6.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje

Kao uslov za zapošljavanje, Pružalac usluga čuvanja zahteva najmanje diplomu srednjeg obrazovanja, ali Pružalac usluga čuvanja i dalje vodi računa o tome da zaposleni prođu odgovarajuću obuku. Neposredno po prijemu u radni odnos, Pružalac usluga čuvanja dodeljuje obuku za svoje novozaposlene, u okviru koje stiču znanja neophodna za obavljanje posla. Pouzdane uloge kod Pružaoca usluga 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:

- specijalizovana diploma (matematika, viša ili visoka stručna sprema informacionih tehnologija ili viša/visoka diploma stečena na inženjerskom odseku iz tehničke oblasti nauke);

- najmanje tri godine stručnog iskustva u profesionalnom radnom iskustvu u oblasti informacione bezbednosti

6.3.2 Procedure provere pozadine

Pružalac usluge čuvanja angažuje samo zaposlene za pouzdane ili vodeće uloge, koji

- imaju čist dosije i protiv njih nije u toku nikakav postupak koji može 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, zaposlenik Pružalac usluga čuvanja, izjavom, službenik nosioca uloge od poverenja sa sertifikatom o dobrom ponašanju starom manje od 3 meseca, opravdati čist krivični dosije. Pružalac usluge čuvanja proverava autentičnost relevantnih informacija navedenih u biografiji kandidata tokom procesa zapošljavanja, kao što su prethodno zaposlenje, profesionalne reference i najrelevantnije obrazovne kvalifikacije.

6.3.3 Zahtevi za obuku

Pružalac usluga čuvanja obučava novozaposlene zaposlene, tokom kojih oni stiču

- osnovno PKI znanje;
- specifičnosti i način rukovanja IT sistemom Pružaoca usluga čuvanja;
- neophodna posebna znanja za ispunjavanje 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.

6.3.4 Učestalost i uslovi prekvalifikacije

Pružalac usluge čuvanja obezbeđuje da zaposleni stalno poseduju neophodna znanja, pa se po potrebi održavaju dalje ili ponavljane obuke. Dalja obuka se održava ako dođe do promene u

procesima ili IT sistemu Pružaoca usluge čuvanja. Obuka je adekvatno dokumentovana, iz čega se jasno može odrediti nastavni plan i obim zaposlenih učesnika.

6.3.5 Učestalost i redosled rotacije poslova

Pružalac usluga čuvanja ne primenjuje obaveznu rotaciju između pojedinačnih rasporeda rada.

6.3.6 Sankcije za nedozvoljene radnje

Pružalac usluge čuvanja reguliše mogućnosti krivičnog gonjenja zaposlenih u ugovoru o radu 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. Po imenovanju svaki zaposleni od poverenja kao deo dokumenata o zapošljavanju:

- dobija pismene informacije o zakonskim obavezama, pravima, sertifikaciji i standardima upravljanja za tretman ličnih podataka,
- dobija opis posla koji uključuje bezbednosne zadatke,
- potpisuje ugovor o poverljivosti u kome se mogu naći i posledice nepoštovanja bezbednosnih mera (krivične sankcije).

Sve ovo uključuje radno zakonodavstvo ili krivične posledice koje sankcionišu drugačije discipline – radne obaveze – kršenje zakona.

6.3.7 Zahtevi nezavisnog izvođača

Pružalac usluge čuvanja dodeljuje samo pouzdane uloge svojim zaposlenima.

Pružalac usluga čuvanja bira osobe zaposlene sa ugovorom o angažovanju ili podugovorom za obavljanje drugih zadataka, po mogućnosti, sa liste prethodno kvalifikovanih dobavljača. Pružalac usluge čuvanja zaključuje pisani ugovor pre nego što počne da radi sa dobavljačima.

Svaka ugovorna strana – pre početka aktivnog rada – potpisuje izjavu o poverljivosti sa kojim se slaže da kasnije saznane poslovne/korporativne tajne neće biti prikrivene neovlašćena lica, i neće biti iskorišćavani na bilo koji drugi način. Praktična pravila uključuje sankcije u slučaju kršenja. Od spoljnih zaposlenih po ugovoru se očekuje da imaju odgovarajuće tehničke veštine, a Pružalac usluge čuvanja ne održava nikakvu obuku za njih.

6.3.8 Dokumentacija dostavljena osoblju

Pružalac usluge čuvanja kontinuirano obezbeđuje zaposlenima dostupnost aktuelne dokumentacije i propisa neophodnih za obavljanje njihovih uloga. Svi zaposleni se pisanim obaveštenjem obaveštavaju o promenama organizacionih bezbednosnih propisa.

Svaki zaposleni u pouzdanoj ulozi dobija sledeće dokumente u pisanoj formi:

- organizacioni bezbednosni propisi Pružaoca usluge čuvanja,
- potpisati ugovor o poverljivosti,
- lični opis posla,
- edukativni materijali povodom planirane ili posebne obuke za određeni oblik obrazovanja.

6.4 Procedure evidentiranja revizije

6.4.1 Vrste snimljenih događaja

Pružalac usluge čuvanja evidentira svaki događaj vezan za bezbednost 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, on čuva sledeće podatke:

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

Svi novi zapisi revizije se dodaju zapisima revizije. Ranije sačuvani zapisi revizije ne mogu se menjati ili brisati. Svi bitni zapisnici događaja dostupni su nezavisnim revizorima sistema, koji ispituju usklađenost rada Pružaoca usluge očuvanja.

Pružalac usluge čuvanja evidentira najmanje sledeće događaje:

- INTERNI SAT

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

- gubitak sinhronizacije;

- DUGOROČNO OČUVANJE

  - 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 dokaza o očuvanju, ispunjenje zahteva za izjavu i predaju arhive drugom pružaocu;

- EVIDENCIJA:

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

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

  - modifikacija ili brisanje sačuvanih podataka evidencije;

  - aktivnosti koje se obavljaju zbog kvara sistema evidencije.

- SISTEMSKA PRIJAVA:

  - uspešne prijave, neuspešni pokušaji prijavljivanja 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).

- KLJUČNO UPRAVLJANJE:

- svi događaji za ceo životni ciklus servisnih ključeva (generisanje ključeva, čuvanje, učitavanje, uništavanje itd.);

- TOKOVI PODATAKA:
  - bilo koju vrstu bezbednosno kritičnih podataka koji se ručno unose u sistem;
  - podaci relevantni za bezbednost, poruke koje sistem prima
- *Hardware Security Module*:
  - instaliranje hardverskog bezbednosnog modula;
  - uklanjanje hardverskog bezbednosnog modula;
  - odlaganje, uništavanje hardverskog bezbednosnog modula;
  - dostavljanje hardverskog bezbednosnog modula;
  - čišćenje (resetovanje) hardverskog bezbednosnog modula;
  - učitavanje ključeva, sertifikata u Hardverskom sigurnosnom modulu.
- PROMENA KONFIGURACIJE:
  - hardver;
  - softver;
  - operativni sistem;
  - patch;
  - instaliranje, ažuriranje i uklanjanje softvera na sistemu sertifikata;
- FIZIČKI PRISTUP, BEZBEDNOSNE LOKACIJE:
  - osoba koja ulazi i izlazi iz bezbednosne zone koja drži 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 Izjave o kvalifikovanoj praksi čuvanja;
  - brisanje sata operativnog sistema
- DRUGI DOGAĐAJI:
  - imenovanje lica na 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.

6.4.2 Učestalost obrade dnevnika revizije

Nezavisni sistemski revizori Pružalac usluge očuvanja procenjuju generisane datoteke evidencije svakog radnog dana. Tokom ocenjivanja obezbeđuje se autentičnost i integritet pregledanih dnevnika, proveravaju se poruke o greškama u evidenciji i po potrebi dokumentuju razlike i preduzimaju mere za otklanjanje uzroka odstupanja.

Za procenu IT sistema, Pružalac usluge čuvanja takođe koristi automatizovane alate za procenu, koji se koriste za praćenje rezultujućih unosa u dnevniku prema unapred postavljenim kriterijumima i, gde je potrebno, upozoravaju operativno osoblje. Obaveštenja dobijena od automatizovanih alata za evaluaciju obrađuju i procenjuju stručnjaci za IT poslovanje u roku od 24 sata.
Činjenica uviđaja, rezultati istrage i mere preduzete da bi se otklonili utvrđeni nedostaci su propisno dokumentovani.

6.4.3 Period zadržavanja za evidenciju revizije

Pre brisanja iz onlajn sistema, dnevnici se arhiviraju i njihovo bezbedno očuvanje obezbeđuje Pružalac usluge čuvanja tokom perioda definisanog u odeljku 6.5.2, ali najmanje 10 godina od datuma njihovog kreiranja.

Za taj vremenski period Pružalac usluge čuvanja obezbeđuje čitljivost arhiviranih podataka i održava softverske i hardverske alate neophodne za to.

6.4.4 Zaštita dnevnika revizije

Pružalac usluge čuvanja štiti kreirane dnevnike za potrebno vreme čuvanja. Tokom čitavog vremena čuvanja, obezbeđuju se sledeća svojstva podataka dnevnika:

- zaštita od neovlašćenog otkrivanja: samo ovlašćena lica – prvenstveno nezavisni revizori sistema – pristupaju evidencijama;

- dostupnost: ovlašćenim licima je odobren pristup evidenciji;

- integritet: sprečena je svaka promena podataka, brisanje u fajlovima evidencije i promena redosleda unosa itd.

Pružalac usluge čuvanja obezbeđuje zapise dnevnika sa kvalifikovanim vremenskim žigom i oni se čuvaju na način koji isključuje besprekorno umetanje i brisanje unosa u dnevnik. Datoteke evidencije su zaštićene od slučajnog i zlonamernog oštećenja rezervnim kopijama. U slučaju unosa u dnevnik koji sadrže lične podatke, Pružalac usluge čuvanja vodi računa o poverljivom čuvanju podataka. Samo oni pojedinci imaju pravo pristupa unosima u dnevnik, kojima je to apsolutno potrebno za njihov rad. Pružalac usluge čuvanja verifikuje pristupe na bezbedan način. Pružalac usluge čuvanja čuva datoteke evidencije u bezbednom okruženju. Čuva kopije datoteka na drugom mestu operacije.

6.4.5 Procedure rezervne kopije dnevnika revizije

Dnevni log fajlovi se kreiraju od kontinuirano generisanih unosa dnevnika tokom rada u svakom sistemu. Datoteke dnevne evidencije se arhiviraju u dve kopije nakon evaluacije i skladište fizički odvojene jedna od druge, na odvojenim lokacijama tokom potrebnog vremena.

Tačan proces pravljenja rezervnih kopija biće definisan u propisima za rezervne kopije Pružaoca usluge čuvanja.

6.4.6 Sistem prikupljanja revizije (interni naspram eksternog)

Svaka aplikacija automatski prikuplja i šalje zapise sistemu za evidentiranje. Funkcije evidentiranja pokreću se automatski u trenutku pokretanja sistema i rade se neprekidno tokom čitavog perioda rada sistema. U slučaju bilo kakve anomalije u sistemima za automatsko ispitivanje i evidentiranje, Pružalac usluge čuvanja obustavlja rad povezanih oblasti dok se incident ne reši.

6.4.7 Obaveštenje subjektu koji izaziva događaj

Lica, organizacije i aplikacije koje su izazvale događaj greške nisu uvek obaveštene, ali ako je potrebno, Pružalac usluge očuvanja ih uključuje u istragu događaja. Klijenti na koje utiče pokretanje događaja imaju obavezu da sarađuju sa Pružaocem usluge čuvanja kako bi istražili događaj.

6.4.8 Procene ugroženosti

Pored svakodnevne obrade log unosa, stručnjaci Pružaoca usluge čuvanja prate javno dostupne informacije o mogućim ranjivostima i novim softverskim zakrpama. Analiziraju informacije, klasifikuju ranjivost i po potrebi obaveštavaju menadžment o rezultatu i predlažu akcioni plan za povećanje bezbednosti sistema.

Svaki veći događaj značajnih nedostataka otkriven ili u slučaju spoljne pretnje u roku od 48 sati

nakon njegovog otkrivanja, ali najmanje jednom godišnje stručnjaci Pružaoca usluge čuvanja vrše sveobuhvatnu analizu ranjivosti koristeći mapiranje potencijalnih unutrašnjih i eksternih pretnji, što može dovesti do neovlašćenog pristupa.

Na osnovu rezultata analize Pružalac usluge čuvanja

- kreira i sprovodi plan za ublažavanje ugroženosti; ili

- dokumentuje činjeničnu osnovu za odluku da je preostali rizik prihvaćen i da ugroženost ne zahteva sanaciju.

Najpre se nove verzije softvera i softverskih pečeva instaliraju na test sistem Pružaoca usluge čuvanja, a tek nakon uspešno završenog testa se instaliraju na živi sistem koji se koristi za pružanje usluga.

Novi softverski pečevi se ne instaliraju na sistem uživo ako unose dodatne ranjivosti ili nestabilnosti koje prevazilaze prednosti njihove primene. Razlozi za neprimenu bezbednosnih pečeva su dokumentovani.

6.5 Arhivski zapisi

6.5.1 Vrste arhiviranih zapisa

Pružalac usluge čuvanja je spreman da na odgovarajući način obezbedi dugoročno arhiviranje elektronskih i papirnih dokumenata.

Pružalac usluge čuvanja arhivira sledeće vrste informacija:

- svaki dokument u vezi sa akreditacijom Pružaoca usluge čuvanja;
- sve izdate verzije Politika sertifikata;
- sve izdate verzije Praktičnih pravila čuvanja;
- sve izdate verzije Opštih uslova;
- ugovori u vezi sa radom Pružaoca usluge čuvanja;
- svaki elektronski i papirni unos u dnevnik.

6.5.2 Period čuvanja arhive

Pružalac usluge čuvanja čuva arhivirane podatke za dolenavedene vremenske periode:

- Politiku kvalifikovanog čuvanja u trajanju od najmanje 10 godina od datuma ukidanja;
- 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

6.5.3 Zaštita arhive

Pružalac čuva arhivirane podatke u 2 kopije na fizičkim lokacijama odvojene jedna od druge. Autentična papirna ili elektronska kopija se pravi u skladu sa važećim zakonom od jedine dostupne autentične kopije dokumenta na papiru. Svaka od dve lokacije ispunjava uslove za bezbednost arhiviranja i druge zahteve.

Prilikom čuvanja arhiviranih podataka obezbeđuje se:

- da je očuvan njihov integritet;
- da su zaštićeni od neovlašćenog pristupa;
- da su dostupni;

- da čuvaju autentičnost.

Arhivirani elektronski podaci imaju najmanje napredni elektronski potpis ili pečat i kvalifikovani vremenski žig.

6.5.4 Procedure arhiviranja rezervnih kopija

Pružalac usluge čuvanja čuva samo hešove e-dokumenata, metapodatke i dokaze o očuvanju. Čuvanje i arhiviranje fizičkih dokumenata je odgovornost Pretplatnika.

6.5.5 Zahtevi za stavljanje vremenskog žiga na zapise

Svaki unos u elektronskom dnevniku ima vremensku oznaku, na kojoj je vreme koje je obezbedio sistem naznačeno sa tačnošću od najmanje jedne sekunde.

Na ovaj način Pružalac usluge čuvanja garantuje da je odstupanje vremena naznačenog u vremenskim oznakama od UTC vremenske baze najviše 1 sekundu. Pružalac usluge čuvanja obezbeđuje dnevne datoteke evidencije sa kvalifikovanim vremenskim žigom.

Prilikom čuvanja arhiviranih podataka, ako je potrebno (na primer, istek promene algoritma originalne vremenske oznake) obezbeđuje se autentičnost podataka.

6.5.6 Sistem prikupljanja arhiva (interni ili eksterni)

Unosi u evidenciju se generišu u zaštićenom računarskom sistemu Pružaoca usluge čuvanja i samo datoteke evidencije koje su elektronski potpisane i zaštićene kvalifikovanim vremenskim žigom mogu da ih napuste.

Jedna originalna kopija dokumenata nastalih tokom pružanja usluge se čuva i štiti
od strane Pružaoca usluge čuvanja u unutrašnjem skladištu podataka kojim on upravlja.

6.5.7 Procedure za dobijanje i verifikaciju arhivskih informacija

Pružalac usluge čuvanja kreira datoteke evidencije ručno ili automatski. U slučaju automatskog sistema evidentiranja, sertifikovane datoteke evidencije se generišu svakodnevno. Arhivirane datoteke su zaštićene od neovlašćenog pristupa.

Kontrolisani pristup arhiviranim podacima dostupan je samo kvalifikovanim licima:

- Klijenti imaju pravo da vide uskladištene podatke koji im odgovaraju;
- u pravnim sporovima radi pružanja dokaza dostavljaju se potrebni podaci

6.6 Kompromis i oporavak od katastrofe

U slučaju havarije, Pružalac usluge čuvanja preduzima sve neophodne mere kako bi minimizirao štetu nastalu usled nedostatka usluge, i vraća usluge u najkraćem mogućem roku.

Na osnovu procene incidenta koji se dogodio, preduzima potrebne izmene, korektivne mere kako bi se sprečio nastanak incidenta u budućnosti.

Kada se problem reši, događaj se prijavljuje Ministarstvu trgovine, turizma i telekomunikacija, kao nadzornom organu.

6.6.1 Procedure za rukovanje incidentima i kompromisima

Pružalac usluge čuvanja ima plan kontinuiteta poslovanja.

Pružalac usluge čuvanja uspostavlja i održava potpuno funkcionalan rezervni sistem, koji je na bezbednoj udaljenosti od primarne lokacije, geografski lociran na drugom mestu i nezavisno je sposoban da pruži kompletan spektar usluga.

Pružalac usluge čuvanja svake godine testira prelazak na rezervni sistem i pregleda svoje planove za kontinuitet poslovanja.
Pružalac usluge čuvanja je povećao bezbednosne alate i sisteme kako bi sveo na minimum greške softvera i hardvera i oštećenja podataka. Povratnost usluga je zagarantovana osnovnim ugovorima i sopstvenim alatima za rezervne kopije Pružaoca usluge čuvanja.

Pružalac usluge čuvanja je konstruisao svoj IT sistem koji pruža usluge poverenja na način da u slučaju ispadanja bilo kog uređaja može da nastavi pružanje usluga od poverenja.

6.6.2 Računarski resursi, softver i/ili podaci su oštećeni

IT sistemi Pružaoca usluge čuvanja izgrađeni su od pouzdanih hardverskih i softverskih komponenti. Kritične funkcije se realizuju korišćenjem redundantnih elemenata sistema tako da u slučaju kvara stavke mogu dalje da rade.

Pružalac usluge čuvanja pravi potpunu dnevnu rezervnu kopiju svojih baza podataka i generisanih događaja evidencije.

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

Kada se problem reši i integritet vrati, Pružalac usluge čuvanja ponovo pokreće svoje usluge što je pre moguće.

6.6.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Definisani su zadaci koji se obavljaju u slučaju kvara usluge usled elementarne nepogode ili druge nepogode u planu za kontinuitet poslovanja Pružaoca usluge čuvanja. U slučaju havarije, propisi stupaju na snagu, počinje kontrola štete i obnavljanje usluga.

Lokacija sekundarnih usluga je toliko udaljena od primarne lokacije da je verovatna katastrofa ne može doći do obe lokacije istovremeno. Pružalac usluge čuvanja je dužan da u slučaju katastrofe obavesti ugrožene korisnike što je pre moguće.

Nakon oporavka usluge, pružalac usluge čuvanja vraća svoje uređaje oštećene tokom katastrofe i prvobitni nivo bezbednosti usluge što je pre moguće.

6.7 Prestanak usluge očuvanja

U slučaju planiranog prestanka pružanja usluge, Pružalac usluge čuvanja obaveštava krajnje korisnike i Ministarstvo trgovine, turizma i telekomunikacija najmanje 60 dana pre prestanka pružanja usluge.
Istovremeno sa obaveštenjem o prekidu usluge, Pružalac usluge čuvanja gasi sledeće usluge:

- prijem noviih predmeta zaštite u arhivu.

Pružalac usluge čuvanja raskida ugovore o usluzi najmanje 30 dana pre planiranog raskida i poziva Pretplatnike da preuzmu svoje dokaze o očuvanju koji se čuvaju u arhivi.

Pružalac usluge očuvanja najmanje 20 dana pre planiranog raskida, ali najmanje 14 dana nakon obaveštenja Klijenta, gasi sledeće usluge:

- izdavanje izvoda o uskladištenim objektima očuvanja.

U isto vreme raskida, Pružalac usluge čuvanja gasi sledeće usluge:

- preuzimanje dokaza o očuvanju sačuvanih u arhivi
- tehnička podrška
- pružanje informacija.

Pre planiranog raskida, Pružalac usluge čuvanja se upušta u pregovore o preuzimanju svojih usluga sa drugim pružaocem usluga od poverenja čiji je rejting identičan njegovom. U skladu sa članom 9.3, predaće svoju evidenciju, uključujući poverljive korisničke podatke, takvom pružaocu usluga od poverenja ili Ministarstvu trgovine, turizma i telekomunikacija šta može doći, zajedno sa svojim drugim uslugama, u zavisnosti od ishoda pregovora ili prestaje bez primopredaje.
Pružalac usluge čuvanja preduzima mere u vezi sa opozivom sertifikata provajdera (i uništavanjem privatnih ključeva) tokom perioda od 60 dana – u zavisnosti od ishoda pregovora.

Pružalac usluge čuvanja obaveštava Ministarstvo trgovine, turizma i telekomunikacija o konačnom ishodu pregovora. Pružalac usluga čuvanja obaveštava svoje klijente elektronskom poštom, a pouzdane strane putem publikacije na svojoj veb stranici.
Po okončanju usluge, Pružalac usluge čuvanja pravi rezervnu kopiju punog obima svojih podataka sadržanih u njegovom IT sistemu, zaštićenih kvalifikovanim vremenskim žigom. Da bi omogućio predaju svojih podataka drugom pružaocu usluga od poverenja, Pružalac usluge čuvanja postavlja podatke na medije iu formatu koji novi pružalac usluga od poverenja može da primi ili pruža novom pružaocu usluga od poverenja mogućnost da obrađuje podatke u originalnom formatu, i preda odgovarajuće alate, dokumentaciju i znanje za to.

Nakon prestanka usluge, Pružalac usluge čuvanja predaje pretplatniku arhivirane datoteke, potpise, pečate ili lance sertifikata u formatu koji je dogovoren sa Pretplatnikom i briše ih iz svoje arhive na nepovratan način opisan u odeljku 3.6.

7 Tehničke bezbednosne kontrole

Pružalac usluge čuvanja koristi sisteme koji se sastoje od pouzdane i sigurnosno tehnički procenjene opreme za pružanje svojih usluga. Pružalac usluge čuvanja upravlja kriptografskim privatnim ključevima dobavljača tokom celog njihovog životnog ciklusa u okviru HSM uređaja koji ima odgovarajući sertifikat.

I Pružalac usluge čuvanja i pružalac sistema i izvođači imaju značajno iskustvo u primeni PKI sistema i usluga od poverenja i koriste međunarodno priznatu tehnologiju.

7.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula

Pružalac usluge čuvanja obezbeđuje bezbedno upravljanje privatnim ključevima koje poseduje i sprečava otkrivanje, kopiranje, brisanje, modifikaciju i neovlašćeno korišćenje privatnog ključa. Pružalac usluge čuvanja može čuvati privatne ključeve sve dok pružanje usluge to definitivno zahteva.

7.1.1 Standardi i kontrole kriptografskog modula

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

- zahtevima ISO/IEC 19790 [37], ili
- zahtevima FIPS 140-2 [38] nivo 3 ili više, ili
- zahtevima FIPS 140-3 [39] nivo 3 ili više, ili
- zahtevima CEN 419 221-5 [40], ili
- oni su tako pouzdani sistemi koji se procenjuju na nivou garancije 4 ili više prema MSZ/ISO/IEC 15408 [41] 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.

Pružalac usluge čuvanja čuva privatne ključeve provajdera izvan hardverskog bezbednosnog modula samo u šifrovanom obliku. Za kodiranje se koriste samo oni algoritmi i ključni parametri koji odgovaraju aktuelnoj algoritamskoj odluci Ministarstva trgovine, turizma i telekomunikacija (1) b) i za koje se očekuje da će moći da izdrže kriptografske napade tokom celog životni vek ključeva.
Privatni ključevi Pružaoca usluge čuvanja čuvaju se na fizički bezbednoj lokaciji čak iu šifrovanom obliku, u sefu Data centra, gde su dostupni samo ovlašćenim osobama.

U slučaju slabljenja kriptografskih algoritama i parametara ključa, Pružalac usluge čuvanja uništava kodirane ključeve ili ih ponovo kodira koristeći algoritam i parametre ključa koji obezbeđuju veću zaštitu.

7.1.2 Privatni ključ (N od M) Kontrola više osoba

Pružalac usluge čuvanja implementira „n od m“ pri aktivaciji funkcija upravljanja ključevima u vezi sa privatnim ključem. Parametri se određuju tako da je istovremeno prisustvo najmanje dva; zaposleni nosioci uloge od poverenja su potrebni za kritične operacije koje se obavljaju sa privatnim ključevima njegovog dobavljača.

7.1.3 Deponovanje privatnog ključa

Pružalac usluge čuvanja ne deponuje privatne ključeve pružaoca.

7.1.4 Rezervna kopija privatnog ključa

Pružalac usluge čuvanja pravi sigurnosne kopije privatnih ključeva svog provajdera, pre nego što privatni ključ provajdera stavi u upotrebu kao što je opisano u odeljku 7.1.1. u zaštićenom okruženju, uz istovremeno prisustvo najmanje dve osobe koje imaju poverene uloge, sa isključenje drugih ljudi. Tokom pravljenja rezervne kopije, privatni ključ ostavlja modul u šifrovanom stanju, a ovaj šifrovani ključ se može učitati u drugi modul. I pravljenje rezervne kopije i vraćanje u prethodno stanje mogu se izvršiti samo zaštitnim mehanizmima opisanim u odeljku 7.1.2.
Pružalac usluge čuvanja čuva rezervnu kopiju u duplikatu, a najmanje jedna kopija se čuva na drugom mestu od lokacije Pružaoca usluge.

Na upravljanje i čuvanje rezervnih kopija primenjuju se isti strogi bezbednosni standardi kao i za rad proizvodnog sistema.

7.1.5 Arhiva privatnih ključeva

Pružalac usluge čuvanja ne arhivira svoje privatne ključeve.

7.1.6 Prenos privatnog ključa u ili iz kriptografskog modula

Svi privatni ključevi Pružaoca usluge čuvanja su kreirani u hardverskom bezbednosnom modulu koji ispunjava zahteve.
Privatni ključevi ne postoje u otvorenom obliku izvan hardverskog bezbednosnog modula. Pružalac usluge čuvanja samo izvozi privatni ključ iz hardverskog bezbednosnog modula u svrhu pravljenja bezbedne kopije. Izvoz i učitavanje privatnih ključeva Pružaoca se vrši prema odeljku 7.1.2.

7.1.7 Skladištenje privatnog ključa na kriptografskom modulu

Pružalac usluge čuvanja čuva svoje privatne ključeve koji se koriste za pružanje usluga u hardverskim bezbednosnim modulima u skladu sa odeljkom 7.1.1. Privatni ključevi se čuvaju i koriste u Hardverskom bezbednosnom modulu kako je navedeno u sertifikaciji uređaja uz punu usklađenost sa odgovarajućim uputstvima za upotrebu.

7.1.8 Način aktiviranja privatnog ključa

Pružalac usluge čuvanja čuva privatne ključeve svog provajdera u bezbednom hardverskom bezbednosnom modulu i u skladu je sa svojim korisničkim uputstvom i zahtevima navedenim u sertifikacionim dokumentima. Hardverski bezbednosni modul se može aktivirati samo pomoću odgovarajućih operaterskih kartica, a privatni ključevi unutar Hardverskog bezbednosnog modula se ne mogu koristiti pre aktiviranja modula. Pružalac usluge čuvanja čuva kartice operatera u bezbednom okruženju i do tih kartica mogu da dođu samo ovlašćeni zaposleni Pružaoca usluge čuvanja.

7.1.9 Metoda deaktiviranja privatnog ključa

Privatni ključ koji koristi Pružalac usluge čuvanja i kojim upravljaju kriptografski uređaji postaje deaktiviran ako se (na redovan ili nepravilan način) uređaj ukloni iz aktivnog statusa. Ovo se može desiti u sledećim slučajevima:

- korisnik deaktivira ključ,
- napajanje uređaja je prekinuto (isključeno ili problem sa napajanjem)
- uređaj ulazi u stanje greške.

Ovako deaktiviran privatni ključ ne može se koristiti dok modul ponovo ne bude u aktivnom stanju.

7.1.10 Metoda uništavanja privatnog ključa

Odbačeni, istekli ili kompromitovani privatni ključevi Pružaoca usluge čuvanja su uništeni na način koji onemogućava dalju upotrebu privatnih ključeva. Pružalac usluge čuvanja uništava privatne ključeve provajdera uskladištene u bezbednom hardverskom bezbednosnom modulu u skladu sa procedurama, zahtevima definisanim u korisničkom vodiču i u sertifikacionim dokumentima korišćenog hardverskog bezbednosnog modula, uz istovremeno prisustvo dva dobavljača usluga čuvanja zaposleni (administrator infrastrukture i službenik obezbeđenja) uz isključenje drugih lica. Pružalac usluge čuvanja uništava svaku rezervnu kopiju privatnog ključa na dokumentovan način na takav način da njegovo vraćanje i korišćenje postaje nemoguće.

7.1.11 Ocena kriptografskog modula

U skladu sa zahtevima odeljka 7.1.1, svaki privatni ključ Pružaoca usluge čuvanja se čuva u kriptografskom modulu koji

- ima sertifikat prema ISO/IEC 19790 [37], ili
- ima sertifikat prema FIPS 140-2 nivo 3 [38], ili
- ima sertifikat prema FIPS 140-3 nivo 3 [39], ili
- ima sertifikat zasnovan na zajedničkim kriterijumima najmanje EAL-4 nivoa [42] koji potvrđuje usklađenost sa zahtevima CEN 419 221-5 [40], 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

7.2 Podaci o aktivaciji

7.2.1 Generisanje i instalacija aktivacionih podataka

Privatni ključevi Pružaoca usluge čuvanja zaštićeni su u skladu sa procedurama, zahtevima definisanim u korisničkom vodiču za korišćeni hardverski bezbednosni modul i sertifikacionim dokumentima.
U slučaju korišćenja aktivacionih podataka zasnovanih na lozinki, lozinke su dovoljno složene da obezbede potreban nivo zaštite.

7.2.2 Zaštita podataka aktivacije

Zaposleni kod Pružaoca usluge čuvanja bezbedno upravljaju uređajima za aktivaciju privatnih ključeva i aktivacionim podacima, štite ih tehničkim i organizacionim merama, a lozinke se čuvaju samo u šifrovanom obliku.

7.2.3 Drugi aspekti aktivacionih podataka

Bez odredbe.

7.3 Kontrole kompjuterske bezbednosti

7.3.1 Specifični tehnički zahtevi za bezbednost računara

Tokom konfiguracije i rada svojih IT sistema, Pružalac usluge čuvanja se stara da sledeće bude ispunjeno:

- identitet korisnika se verifikuje pomoću dvofaktorskih kontrola autentifikacije korišćenjem VPN sertifikata uskladištenih na kartici pre nego što se odobri pristup sistemu ili aplikaciji;

- uloge se dodeljuju korisnicima i to obezbeđuje da svi korisnici imaju samo dozvole koje odgovaraju njihovim ili njenim ulogama;

- zapis u evidenciji se kreira za svaku transakciju, a zapisi se arhiviraju;
- za procese od ključne važnosti za bezbednost obezbeđuje se da su interni mrežni domeni Pružaoca usluge očuvanja dovoljno zaštićeni od neovlašćenog pristupa;

- primenjuju se odgovarajuće procedure da bi se obezbedio oporavak usluge nakon gubitka ključa ili otkaza sistema.

7.3.2 Ocena računarske bezbednosti

Inception naglašava važnost iskustva klijenata. U cilju održavanja visokog nivoa usluga, Inception upravlja sistemom kontrole kvaliteta u skladu sa standardom ISO 9001.
Inception pridaje visok prioritet bezbednosti sistema kojima upravlja, pa je stoga i bio upravljanje sistemom upravljanja bezbednošću informacija koji je u skladu sa ISO/IEC 27001 (ranije poznat kao BS 7799) u svojim glavnim oblastima aktivnosti.
Obim i sistema kontrole kvaliteta i sistema upravljanja bezbednošću informacija pokrivaju usluge poverenja koje pruža Inception.
Inception ima procenu rizika na dva nivoa koja osim rizika informacionih tehnologija pokriva celu organizaciju uključujući i poslovne rizike. Procena rizika se ažurira najmanje jednom godišnje.

Na osnovu rezultata procene rizika Pružalac usluge čuvanja

- postavlja nove mere za uklanjanje ranjivosti, ili/i
- prihvata identifikovane preostale rizike navodeći razlog za odluku.

7.4 Tehničke kontrole životnog ciklusa

7.4.1 Kontrole razvoja sistema

Pružalac usluge čuvanja koristi samo aplikacije i uređaje na svom produkcionom okruženju IT sistema koji je:

- komercijalni softver u kutiji, dizajniran i razvijen prema dokumentovanoj metodologiji dizajna, ili
- prilagođena hardverska i softverska rešenja razvijena od strane samog Pružaoca usluge čuvanja tokom kojih su korišćene strukturirane metode razvoja i kontrolisano razvojno okruženje, ili;
- prilagođena hardverska i softverska rešenja razvijena od pouzdane strane Pružaoca usluge čuvanja tokom kojih su korišćene strukturirane 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 IT alata se vrši na način koji isključuje promene na hardverskim i softverskim komponentama korišćenjem pouzdanih, redovno kvalifikovanih dobavljača.
Hardverske i softverske komponente primenjene za pružanje usluga Pružalac usluge čuvanja ne koristi u druge svrhe.

Pružalac usluge čuvanja odgovarajućim bezbednosnim merama sprečava zlonamerni softver da uđe u uređaje koji se koriste za usluge sertifikacije. Hardverske i softverske komponente se redovno proveravaju na zlonamerni softver pre prve upotrebe, a zatim i kasnije.

Pružalac usluge čuvanja zapošljava pouzdano, adekvatno obučeno osoblje tokom instaliranja softvera i hardvera.

Pružalac usluge čuvanja samo instalira softvere svom pružaocu usluga IT opremu neophodnu u svrhu pružanja usluge.

Pružalac usluge čuvanja ima sistem kontrole verzija gde se dokumentuje svaka promena IT sistema.

Pružalac usluge čuvanja upravlja automatskim sistemom praćenja za evidentiranje svih neovlašćenih promena, koji beleži sve promene u svakom fajlu iu slučaju promena u nadgledane datoteke generiše unos u dnevnik ili šalje upozorenje sistemskim operaterima.

7.4.2 Kontrole za upravljanje bezbednošću

Pružalac usluge čuvanja implementira procese za dokumentovanje, rad, verifikaciju, praćenje i održavanje sistema koji se koriste u usluzi, uključujući njihovu modifikaciju i dalji razvoj. Sistem kontrole verzija detektuje bilo koju vrstu neovlašćenih promena, unos podataka koji utiču na sistem, zaštitni zid, rutere, programe i druge komponente koje se koriste u servisu. Instaliranjem programa koji se koristi u servisu, Pružalac usluge čuvanja osigurava da je program koji treba instalirati odgovarajuća verzija i da nema bilo kakvih neovlašćenih modifikacija. Pružalac usluge čuvanja redovno proverava integritet softvera u svom sistemu koji se koristi u usluzi.

Svaki hardverski sigurnosni modul koji je primenio Pružalac usluge čuvanja je verifikovan, testiran i procenjen. Pružalac usluge čuvanja proverava integritet modula:

- praćenje nabavke uređaja tokom preuzimanja,
- neposredno pre prve upotrebe,
- redovno tokom rada.

Pružalac usluge čuvanja briše ključeve provajdera iz hardverskih bezbednosnih modula koji su trajno ili privremeno povučeni iz upotrebe.

Pružalac usluge čuvanja čuva neiskorišćene hardverske bezbednosne module na fizički zaštićenoj lokaciji.

7.4.3 Sigurnosne kontrole životnog ciklusa

Pružalac usluge čuvanja obezbeđuje zaštitu korišćenih hardverskih bezbednosnih modula tokom celog njihovog životnog ciklusa.
Tokom rada IT opreme i sistema koji se koriste za pružanje usluga, Pružalac usluge čuvanja uzima u obzir bezbednosne aspekte koji se odnose na životni ciklus opreme, prema kojima:

- koristi pravilno sertifikovane hardverske bezbednosne module u svojim sistemima;
- obezbediti, po prijemu hardverskih bezbednosnih modula, da kontrola kvaliteta obezbeđuje da je obezbeđena zaštita hardverskih bezbednosnih modula od neovlašćenja tokom transporta;
- skladišti hardverske bezbednosne module na bezbednom mestu i obezbeđuje zaštitu hardverskih bezbednosnih modula od neovlašćenja tokom skladištenja;
- kontinuirano je u skladu sa zahtevima navedenim u bezbednosnom cilju hardverskog bezbednosnog modula, uputstvima za upotrebu i izveštaju o sertifikaciji tokom rada;
- briše privatne ključeve uskladištene u njihovim prekinutim hardverskim bezbednosnim modulima na takav način da postaje praktično nemoguće vratiti ključeve;
- rukovati i odlagati prekinute hardverske bezbednosne module u skladu sa zahtevima njihovog bezbednosnog cilja, uputstvima za upotrebu i izveštajem o sertifikaciji.

7.5 Kontrole mrežne bezbednosti

Pružalac usluge čuvanja prati najbolje industrijske prakse za obezbeđivanje svojih mreža.

Pružalac uslug čuvanja drži svoju konfiguraciju IT sistema pod strogom kontrolom i dokumentuje svaku promenu uključujući i najmanju modifikaciju, razvoj, ažuriranje softvera.

Pružalac usluge čuvanja sprovodi odgovarajuće procedure za otkrivanje bilo kakve promene hardvera ili softvera, instalacije sistema i održavanja na IT sistemu.

Pružalac usluge čuvanja proverava autentičnost i integritet svake softverske komponente pri prvom učitavanju.

Pružalac usluge čuvanja primenjuje odgovarajuće mere bezbednosti mreže, na primer:

- deli svoj IT sistem na dobro odvojene bezbednosne zone;
- razdvaja namensku mrežu za administraciju IT sistema i operativnu mrežu Pružaoca usluge čuvanja;
- razdvaja proizvodne sisteme za TSP usluge od sistema koji se koriste u razvoju i testiranju;
- 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;
- upravlja IT sistemima koji se koriste za živu operativnu mrežu u bezbednim mrežnim zonama;
- ograničava pristup i komunikaciju između zona na one neophodne za rad usluge;
- onemogućava nekorišćene protokole i korisničke naloge;
- onemogućava neiskorišćene mrežne portove i usluge;
- pokreće samo mrežne aplikacije koje su bezuslovno neophodne za pravilan rad IT sistema.
- redovno pregleda utvrđeni skup pravila.

Pružalac usluge čuvanja prolazi kroz ili vrši skeniranje ranjivosti na javnim i privatnim IP adresama:

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

Pružalac usluge čuvanja proverava usklađenost konfiguracije komponenti lokalne mreže (npr. rutera) sa zahtevima koje je odredio Pružalac usluge čuvanja najmanje svaka tri meseca.

Pružalac usluge čuvanja naručuje test penetracije od spoljnog nezavisnog stručnjaka koji ima neophodne veštine, alate, stručnost i etički kodeks da obezbedi pouzdan izveštaj godišnje I u slučaju značajne promene u IT mreži.

7.6 Stavljanje vremenskog žiga

Za zaštitu integriteta datoteka evidencije i drugih elektronskih datoteka koje treba arhivirati, Pružalac usluge čuvanja koristi kvalifikovane elektronske vremenske žigove koje izdaje Inception autoritet za izdavanje sertifikata.

8 Revizija usklađenosti i druge procene

Rad Pružaoca usluge čuvanja nadzire Ministarstvo trgovine, turizma i telekomunikacija u skladu sa propisima Evropske unije. Ministarstvo trgovine, turizma i telekomunikacija održava inspekciju lokacije najmanje jednom godišnje na lokaciji Pružaoca usluge čuvanja. Pre inspekcije lokacije, Pružalac usluge čuvanja vrši skrining svog poslovanja od strane eksternog revizora i šalje detaljan izveštaj o pregledu 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 kvalifikovanog čuvanja i odgovarajućih Praktičnih pravila.

Predmet i metodologija skrininga je u skladu sa sledećim normativnim dokumentima:

- 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 [1];

- ETSI EN 319 403-1 Elektronski potpisi i infrastrukture (ESI); Procena usaglašenosti Pružaoa usluga od poverenja; Deo 1: Zahtevi za tela za ocenjivanje usaglašenosti koja ocenjuju Pružaoce usluga od poverenja; [43]

- ETSI EN 319 401 Elektronski potpisi i infrastrukture (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja [44]

- ETSI TS 119 511 Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji obezbeđuju dugoročno očuvanje digitalnih potpisa ili opštih podataka korišćenjem tehnika digitalnog potpisa [3]

Rezultat skrininga je poverljivi dokument koji je dostupan samo ovlašćenim licima.
Sertifikat o usaglašenosti izdat u skladu sa izveštajem o ocenjivanju usaglašenosti objavljuje se na veb stranici Pružaoca usluge čuvanja.
Pružalac usluge čuvanja primenjuje verifikovane i sertifikovane elemente (elemente IT sistema za proizvodnju elektronskog potpisa) u vezi sa uslugom.
Pružalac usluge čuvanja je ocenio svaki element sistema koji se koristi za pružanje usluga u bezbednosne klase na osnovu svog sistema procene rizika. Pružalac usluge čuvanja vodi evidenciju o ovim elementima sistema i bezbednosnim ocenama povezanim sa njima u okviru svog sistema upravljanja rizikom.

Pored eksterne revizije, Pružalac usluge čuvanja ima i svoj sopstveni sistem interne revizije, koji redovno proverava usklađenost sa prethodnim revizijama, i preduzima neophodne korake u slučaju odstupanja.

Pružalac usluge čuvanja ima sistem upravljanja kvalitetom u skladu sa standardom ISO 9001, štaviše, sistem upravljanja bezbednošću informacija usklađen sa ISO 27001 (ranije BS 7799), koji se kontinuirano revidira i pregleda od strane spoljne revizorske organizacije (pogledajte odeljak: 1.3.1)

8.1 Učestalost ili okolnost procene

Pružalac usluge čuvanja vrši procenu usklađenosti svake godine na svom IT sistemu koji obavlja pružanje usluga.

8.2 Identitet/Kvalifikacije procenjivača

Pružalac usluge čuvanja 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.

8.3 Odnos procenjivača prema procenjenom entitetu

Eksternu reviziju vrši 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.
- naknada ne zavisi od nalaza aktivnosti sprovedenih tokom revizije.

8.4 Teme pokrivene procenom

Pregled pokriva sledeće oblasti:

- usklađenost sa zakonima koji su trenutno na snazi;
- usklađenost sa tehničkim standardima;
- usklađenost sa Politikom sertifikacije i Praktičnim pravilima kvalifikovanog čuvanja;

- adekvatnost angažovanih procesa;
- dokumentacija;
- fizička bezbednost;
- adekvatnost osoblja;
- IT bezbednost;
- Usklađenost sa pravilima zaštite podataka.

8.5 Radnje preduzete kao posledica nedostatka

Nezavisni revizor rezimira rezultate skrininga u detaljan izveštaj o skriningu koji pokriva testirane komponente sistema, procese i sadrži dokaze koji se koriste u skriningu i revizorske izjave. Nesaglasnosti otkrivene 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 izmenu koje se opciono uzimaju u obzir;
- derogacije koje treba obavezno izbegavati.

Nezavisni revizor će bez odlaganja prijaviti uočene ozbiljne odstupanja Ministarstvu trgovine, turizma i telekomunikacija koje je ovlašćeno da preduzme potrebne mere.

Pružalac usluge čuvanja će pismeno odgovoriti na probleme koje je nezavisni revizor naveo i izvestiti o preduzetim merama za njihovo otklanjanje prilikom sledeće revizije od strane nadležnih organa.

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

REFERENCE

[1] Uredbe (EU) 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 [1].

[2] INCEPTION - Politika kvalifikovanog čuvanja

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

[4] ETSI SR 019 050 V1.1.1 (2015-06); Elektronski potpisi i infrastrukture (ESI); Racionalizovan okvir standarda za elektronske usluge registrovane dostave koje primenjuju elektronski potpis.

[5] ETSI EN 319 401 V2.3.1 (2021-05); Elektronski potpisi i infrastrukture (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja.

[6] EN 319 421 V1.1.1 (2016-03); Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji izdaju vremenske žige.

[7] ETSI TS 119 101 V1.1.1 (2016-03); Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za aplikacije za kreiranje potpisa i validaciju potpisa.

[8] ETSI EN 319 522-1 V1.1.1 (2018-09); Elektronski potpisi i infrastrukture (ESI); Elektronske usluge registrovane isporuke; Deo 1: Okvir i arhitektura .

[9] ETSI EN 319 522-2 V1.1.1 (2018-09); Elektronski potpisi i infrastrukture (ESI); Elektronske usluge registrovane isporuke; Deo 2: Semantički sadržaji.

[10] ETSI EN 319 521 V1.1.1 (2019-02); Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce elektronskih registrovanih usluga isporuke.

[11] ETSI TS 119 512 V1.1.1 (2020-01); Elektronski potpisi i infrastrukture (ESI); Protokoli za pružaoce usluga poverenja koji pružaju usluge dugoročnog čuvanja podataka.

[12] ETSI TS 119 312 V1.4.1 (2021-08); Elektronski potpisi i infrastrukture (ESI); Kriptografski paketi.

[13] ITU X.509 Informaciona tehnologija - Međusobno povezivanje otvorenih sistema - Direktorijum: okviri sertifikata javnog ključa i atributa.

[14] IETF RFC 6960: X.509 Infrastruktura internetskog javnog ključa – protokol statusa sertifikata na mreži (OCSP), Jun 2013.

[15] IETF RFC 3161: Internet X.509 Infrastruktura javnog ključa – protokol vremenske oznake (TSP), Avgust 2001.
[16] ETSI EN 319 421 V1.1.1 (2016-03); Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji izdaju vremenske žige.

[17] ETSI EN 319 422 V1.1.1 (2016-03); Elektronski potpisi i infrastrukture (ESI); Protokol vremenskog žiga i profili tokena sa vremenskim žigom.

[18] Registar pružalaca kvalifikovanih usluga od poverenja – Poverenička lista (https://epotpis.mtt.gov.rs/TrustedList/TSL-RS.xml)

[19] Dublin Core set elemenata metapodataka, Verzija 1.1, https://www.dublincore.org/specifications/dublin-core/dces/2006-12-18/

[20] ETSI TS 101 903 V1.2.2 (2004-04); Tehnička specifikacija XML Napredni elektronski potpisi (XAdES).

[21] ETSI TS 101 903 V1.3.2 (2006-03); Tehnička specifikacija XML napredni elektronski potpisi (XAdES).
[22] ETSI TS 101 903 V1.4.1 (2009-06); Tehnička specifikacija XML napredni elektronski potpisi (XAdES).

[23] ETSI TS 101 903 V1.4.2 (2010-12); Elektronski potpisi i infrastruktura tehničke specifikacije (ESI); XML napredni elektronski potpisi (XAdES).

[24] ISO 19005-1:2005 – Upravljanje dokumentima – Format elektronske datoteke dokumenta za dugoročno čuvanje – Deo 1: Korišćenje PDF-a 1.4 (PDF/A-1).

[25] ETSI EN 319 132-1 V1.2.0 (2021-09); Elektronski potpisi i infrastrukture (ESI); XAdES digitalni potpisi; Deo 1: Građevinski blokovi i XAdES osnovni potpisi.

[26] ETSI EN 319 132-2 V1.1.1 (2016-04); Elektronski potpisi i infrastrukture (ESI); XAdES digitalni potpisi; Deo 2: Prošireni XAdES potpisi.

[27] ETSI EN 319 142-1 V1.1.1 (2016-04); Elektronski potpisi i infrastrukture (ESI); PAdES digitalni potpisi; Deo 1: Građevinski blokovi i PAdES osnovni potpisi.

[28] ETSI EN 319 142-2 V1.1.1 (2016-04 Elektronski potpisi i infrastrukture (ESI); PAdES digitalni potpisi; Deo 2: Dodatni profili PAdES potpisa.

[29] ETSI EN 319 102-1 V1.1.0 (2016-02); Elektronski potpisi i infrastrukture (ESI); Procedure za kreiranje i validaciju AdES digitalnih potpisa; Deo 1: Kreiranje i validacija

[30] ETSI TS 119 102-2 V1.3.1 (2021-09); Elektronski potpisi i infrastrukture (ESI); Procedure za kreiranje i validaciju AdES digitalnih potpisa; Deo 2: Izveštaj o validaciji potpisa

[31] Inception Autoritet za sertifikate - Kvalifikovana usluga čuvanja - opšti uslovi.

[32] Inception Autoritet za sertifikate - Izjava o kvalifikovanoj praksi očuvanja

[33] ISO/IEC 646:1991, Informaciona tehnologija – ISO 7-bitni kodirani skup znakova za razmenu informacija.

[34] ISO/IEC 8859-2:1999 Informaciona tehnologija – 8-bitni jednobajtni kodirani grafički skupovi znakova – Deo 2: latinično pismo br.

[35] ISO/IEC 8859-5:1999 Informaciona tehnologija – 8-bitni jednobajtni kodirani grafički skupovi znakova – Deo 5: Latinica/ćirilično pismo

[36] Format obogaćenog teksta (RTF) Specifikacija, RTF verzija 1.7, Microsoft tehnička podrška, 2001.

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

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

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

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

[41] MSZ/ISO/IEC 15408-2002, Informacione tehnologije - Metode i sredstva obezbeđenja - Kriterijumi za procenu IT bezbednosti.

[42] Zajednički kriterijumi za procenu bezbednosti informacionih tehnologija, Deo 1 - 3.

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

[44] ETSI EN 319 401 V2.3.1 (2021-05); Elektronski potpisi i infrastrukture (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja

[45] 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 tih podataka i stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka).