

U skladu sa eIDAS-om and kvalifikovanom uslugom za validaciju

Praktična pravila

Verzija 1.1

SADRŽAJ

SADRŽAJ 2
1 Uvod 6
1.1 Pregled 6
1.2 Naziv i identifikacija dokumenta 7
1.2.1 Saglasnost 7
1.2.2 Politika validacije 7
1.2.3 Efekat 7
Obim predmeta 7
Vremenski obim 8
Lični obim 8
Geografski obim 8
1.3 PKI učesnici 8
1.3.1 Autoriteti za sertifikaciju 8
Bezbednost kvaliteta i informacija 9
1.3.2 Pretplatnici 9
1.3.3 Oslanjajuće strane 9
1.4 Uprava za politiku 10
1.4.1 Organizacija koja administrira dokument 10
1.4.2 Osoba ili organizacija odgovorna za prikladnost izjave o praksi za politiku validacije 10
1.5. Definicije i akronimi 10
1.5.1. Definicije 10
1.5.2. Akronimi 12
2 Odgovornosti za objavljivanje i skladište 14
2.1 Repozitorijumi 14
2.2 Vreme ili učestalost objavljivanja 14
3. Dizajn usluge validacije 15
3.1 Zahtevi procesa validacije 15
3.2 Zahtevi protokola validacije 16
3.3 Interfejs 16
3.3.1 Komunikacioni kanal 17
3.3.2 Pružalac usluge validacije - drugi Pružalac usluga od poverenja 17
3.4 Zahtevi izveštaja o validaciji potpisa 18
4 Tehničke mere bezbednosti 19

4.1 Sigurnosne garancije 19
4.2 Mere predostrožnosti za računarsku bezbednost 19
4.3 Tehničke mere predostrožnosti vezane za životni ciklus 19
4.4 Redovna sertifikacija 19
4.5 Kontinuirano praćenje tehnologije 20
4.6 Dostupnost određenih elemenata usluge validacije 20
5 Kontrole objekata, upravljanja i rada 20
5.1 Fizičke kontrole 21
5.1.1 Lokacija i izgradnja 21
5.1.2 Fizički pristup 21
5.1.3 Napajanje i klimatizacija 23
5.1.4 Izloženost vodi 23
5.1.5 Prevencija i zaštita od požara 23
5.1.6 Skladištenje medija 23
5.1.7 Odlaganje otpada 23
5.1.8 Bekap van lokacije 24
5.2 Proceduralne kontrole 24
5.2.1 Povereničke uloge 24
5.2.2 Broj potrebnih osoba po zadatku 25
5.2.3 Identifikacija i autentifikacija za svaku ulogu 26
5.2.4 Uloge koje zahtevaju razdvajanje dužnosti 26
5.3 Kontrola osoblja 27
5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje 27
5.3.2 Procedure provere pozadine 27
5.3.3 Zahtevi za obuku 28
5.3.4 Učestalost i uslovi prekvalifikacije 28
5.3.5 Učestalost i redosled rotacije poslova 28
5.3.6 Sankcije za nedozvoljene radnje 29
5.3.7 Zahtevi nezavisnog izvođača 29
5.3.8 Dokumentacija dostavljena osoblju 29
5.4 Procedure evidentiranja revizije 30
5.4.1 Vrste snimljenih događaja 30
5.4.2 Učestalost obrade dnevnika revizije 33
5.4.3 Period zadržavanja za evidenciju revizije 33
5.4.4 Zaštita dnevnika revizije 34
5.4.5 Procedure rezervne kopije dnevnika revizije 34

5.4.6 Sistem prikupljanja revizije (interni naspram eksternog) 34
5.4.7 Obaveštenje subjektu koji izaziva događaj 35
5.4.8 Procene ugroženosti 35
5.5 Oporavak od kompromitovanja i katastrofe 35
5.5.1 Procedure ya rukovanje incidentima i kompromitovanjem 36
5.5.2 Računarski resursi, softver i/ili podaci su oštećeni 36
5.5.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe 36
5.6 Prestanak usluge validacije 37
6 Tehničke bezbednosne kontrole 38
6.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula 38
6.1.1 Standardi i kontrole kriptografskog modula 38
6.1.2 Privatni ključ (N od M) Kontrola više osoba 39
6.1.3 Deponovanje privatnog ključa 39
6.1.4 Rezervna kopija privatnog ključa 39
6.1.5 Arhiva privatnog ključa 39
6.1.6 Prenos privatnog ključa u ili iz kriptografskog modula 40
6.1.7 Skladištenje privatnog ključa na kriptografskom modulu 40
6.1.8 Način aktiviranja privatnog ključa 40
6.1.9 Metoda deaktiviranja privatnog ključa 40
6.1.10 Metoda uništavanja privatnog ključa 40
6.1.11 Ocena kriptografskog modula 41
6.2 Podaci o aktivaciji 41
6.2.1 Generisanje i instalacija aktivacionih podataka 41
6.2.2 Zaštita podataka aktivacije 41
6.2.3 Drugi aspekti aktivacionih podataka 42
6.3 Kontrole kompjuterske bezbednosti 42
6.3.1 Specifični tehnički zahtevi za bezbednost računara 42
6.3.2 Ocena računarske bezbednosti 42
6.4 Tehničke kontrole životnog ciklusa 43
6.4.1 Kontrole razvoja sistema 43
6.4.2 Kontrole upravljanja bezbednošću 44
6.4.3 Sigurnosne kontrole životnog ciklusa 44
6.5 Kontrole mrežne bezbednosti 45
6.6 Vremensko žigosanje 46
7 Revizija usklađenosti i druge procene 46
7.1 Učestalost ili okolnosti procene 47

7.2 Identitet/Kvalifikacije procenjivača 47
7.3 Odnos procenjivača prema procenjenom entitetu 48
7.4 Teme obuhvaćene ocenjivanjem 48
7.5 Radnje preduzete kao rezultat nedostatka 48
REFERENCE 49

1 Uvod

Ovaj dokument je Izjava o praksi za kvalifikovanu uslugu validacije kvalifikovanih elektronskih potpisa i elektronskih pečata koja se odnosi na Kvalifikovanu uslugu validacije Inception d.o.o. (u daljem tekstu: Inception ili Pružalac usluga validacije).

Pružalac usluga validacije pruža svoje usluge svojim Klijentima sa kojima ima ugovorni odnos. Trenutna Izjava o praksi za uslugu kvalifikovane validacije za kvalifikovane elektronske potpise i elektronske pečate (u daljem tekstu: Izjava o praksi validacije) opisuje okvir za pružanje gore navedenih usluga i uključuje detaljne procedure i razna operativna pravila.

Izjava o praksi usluge validacije je u skladu sa zahtevima propisanim eIDAS Uredbom[1], usluga koja se pruža u skladu sa ovim propisima je kvalifikovana za validaciju:

- Elektronski potpisi
- Elektronski pečati

Struktura ovog dokumenta je u skladu sa Aneksom A ETSI TS 119 441 V1.1.1 (2018-08) [2].

1.1 Pregled

Cilj trenutne Izjave o praksi validacije je da sumira sve informacije koje Klijenti treba da znaju kada dođu u kontakt sa Pružaocem usluge validacije. Ovaj dokument takođe ima za cilj da pomogne sadašnjim i budućim klijentima da:

- se upoznaju sa detaljima, zahtevima i praktičnom pozadinom pružanja usluga koje pruža pružalac usluge validacije
- razumeju rad Službe za validaciju i može da odluči da li su usluge usklađene i ispunjavaju li njihove potrebe i očekivanja.

Pored ove Izjave o praksi validacije, dodatni detalji i zahtevi mogu se naći u Politici za uslugu provere kvalifikovanih elektronskih potpisa i elektronskih pečata i ugovoru o usluzi zaključenom sa Pružaocem usluga validacije, kao i drugim propisima ili dokumentima nezavisnim od Pružaoca usluge validacije.

1.2 Naziv i identifikacija dokumenta

Izdavač	Inception d.o.o
Naziv dokumenta	U skladu sa eIDAS-om i kvalifikovanom službom za validaciju Izjava o praksi
OID	1.3.6.1.4.1.57738.50.2.1.1.0
Verzija dokumenta	1.1
Datum stupanja na snagu	

1.2.1 Saglasnost

Pružalac usluge validacije podržava sledeću politiku ETSI usluge:

- normativni zahtevi definisani u ETSI TS 319 102 [3]

Pružalac usluge validacije izjavljuje usklađenost sa ETSI politikom kroz ovu Izjavu o praksi validacije.

1.2.2 Politika validacije

Prvih sedam brojeva OID-a koji identifikuju Politiku validacije je jedinstveni identifikator Pružalac usluge provere kako sledi: 1.3.6.1.4.1.57738

Usluga validacije je identifikovana sufiksom, koji prati jedinstveni identifikator dobavljača usluge: 1.3.6.1.4.1.57738.50

Usluga provere valjanosti se pruža u skladu sa ovom Izjavom o praksi provere valjanosti koja je u skladu sa zahtevima Politike validacije u nastavku identifikovanim na sledeći način:

OID	**Naziv**
1.3.6.1.4.1.57738.50.1.1.2.0	4. INCEPTION - Politika za kvalifikovanu uslugu validacije

1.2.3 Efekat

Izjavu o praksi validacije i Politika validacije zasnovanu na ovim politikama treba revidirati najmanje jednom godišnje i obezbediti njihovu izmenu potencijalno izmenjenih zahteva i preduslova.

Obim predmeta

Izjava o praksi validacije se odnosi na isporuku i korišćenje usluga opisanih u ovom dokumentu.

Vremenski obim

Trenutna verzija Izjave o praksi validacije je na snazi od datuma stupanja na snagu navedenog u odeljku 1.2 ovog dokumenta, do povlačenja. Efekat automatski prestaje po prestanku pružanja usluga ili pri izdavanju novije verzije Izjave o praksi validacije.

Lični obim

Efekat Izjave o praksi validacije proteže se na svakog od pomenutih učesnika.

Pružalac usluge validacije 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 validacije i kontrole. neophodno kako bi se pružene usluge mogle obavljati bezbedno i u skladu sa zakonom Republike Srbije.

Geografski obim

Trenutna Izjava o praksi validacije zasnovana je na zahtevima Evropske unije, ali takođe uključuje i zahteve specifične za Srbiju za usluge koje posluju po zakonu Srbije u Republici Srbiji.

Pružalac usluge validacije može proširiti geografski obim usluge, u ovom slučaju neće koristiti manje stroge zahteve od onih koji se primenjuju u Izjavi o praksi validacije. U uslugama koje se pružaju stranim klijentima, detaljni uslovi koji se razlikuju od Izjave o praksi validacije mogu biti regulisani posebnim ugovorom o usluzi.

Usluga koja se pruža u skladu sa ovom Izjavom o praksi validacije dostupna je širom sveta. Valjanost dokumenata, materijal za dugoročnu validaciju i pripadajuće izdate izjave arhiviraju se prema sadašnjoj Službi za validaciju.

Izjava o praksi je nezavisna od geografske lokacije odakle su poslati u arhivu i odakle su upitani.

Usluga koja se pruža u skladu sa ovom Izjavom o praksi validacije može se koristiti samo na način opisan u ovoj Izjavi o praksi validacije i u Politici validacije.

1.3 PKI učesnici

1.3.1 Autoriteti za sertifikaciju

Podaci pružaoca usluge validacije

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

Uvođenje Pružaoca usluge validacije

„Inception d.o.o“ je pružalac kvalifikovanih usluga od poverenja koji koristi najbezbednije tehnologije, uključujući siguran prenos podataka, za obavljanje svojih elektronskih kvalifikovanih usluga od poverenja, kvalifikovanog elektronskog potpisivanja, kvalifikovanog elektronskog pečaćenja, kvalifikovanog korišćenja vremenskog žiga, validacije i drugih usluga.

Pružalac usluga nudi pouzdane usluge u skladu sa važećim pravnim aktima Republike Srbije i Evropske unije, a posebno u skladu sa eIDAS Uredbom[1] iu 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].

Bezbednost kvaliteta i informacija

Pružalac usluga planira i primenjuje sve mere zaštite u skladu sa standardima ISO/IEC 27000, FIPS 140-2 nivo 3 i/ili uobičajenim kriterijumima 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

Oslanjajuća strana nije nužno u ugovornom odnosu sa Pružaocem usluga očuvanja.

1.4 Uprava za politiku

1.4.1 Organizacija koja administrira dokument

Podaci organizacije koja administrira ovu Izjavu o praksi validacije mogu se naći ovde:

Naziv organizacije	Inception d.o.o
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 izjave o praksi za politiku validacije

Lice odgovorno za usklađenost sa ovom Izjavom o praksi validacije i Politikom validacije koja se u njoj pominje je:

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

Izjave o praksi validacije i pružanje usluga nadgleda Ministarstvo trgovine, turizma i telekomunikacija. Ministarstvo trgovine, turizma i telekomunikacija vodi registar o politici sertifikata i o pružaocima usluga validacije koji primenjuju ove politike.

1.5. Definicije i akronimi

1.5.1. Definicije

Aplikacija za funkcionalnost	Aplikacija koja koristi sistem za kreiranje potpisa radi kreiranje potpisa ili aplikaciju za validaciju potpisa u cilju validacije digitalnih potpisa ili aplikaciju za povećanje potpisa radi povećanja digitalnih potpisa
eIDAS Uredba	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 .
Dokaz o postojanju	Dokaz koji dokazuje da je objekat postojao na određeni datum/vreme
Aplikacija za validaciju	Aplikacija koja validira potpis u odnosu na politiku validacije potpisa, koja se sastoji od skupa ograničenja validacije i koja daje indikaciju statusa (tj. status validacije potpisa) i izveštaj o validaciji potpisa
Politika validacije potpisa	Lista ograničenja koja obrađuje aplikacija za validaciju potpisa
Izveštaj o validaciji potpisa	Sveobuhvatan izveštaj o validaciji koji aplikacija za validaciju potpisa daje aplikaciji za vožnju i omogućava aplikaciji za vožnju da pregleda detalje odluka donetih tokom validacije i istražuje detaljne uzroke indikacije statusa koju obezbeđuje aplikacija za validaciju potpisa
Politika usluge validacije potpisa	Skup pravila koja ukazuju na primenljivost usluge validacije potpisa na određenu zajednicu i/ili klasu aplikacije sa zajedničkom bezbednošću
Validacija potpisa	Proces verifikacije i potvrđivanja da je digitalni potpis tehnički validan
Servis za validaciju potpisa	Sistem dostupan preko komunikacione mreže, koja potvrđuje digitalni potpis

Pretplatnik Pravno ili fizičko lice koje je ugovorom sa Inception-om vezano za sve obaveze	pretplatnika. U Inception ekosistemu, pretplatnici se sastoje i od kupaca (provajdera usluga) koji su potpisali ugovor sa Inception-om kao krajnji korisnici koji su prihvatili samo odredbe i uslove usluga koje koriste
Validacija kvalifikovanog elektronskog potpisa	Validacija kako je navedeno u Uredbi (EU) br. 910/2014 [i.1], član 32
Validacija kvalifikovanih elektronskih pečata	Validacija kako je navedeno u Uredbi (EU) br. 910/2014 [i.1], član 40
Validacija	Proces verifikacije i potvrđivanja da je sertifikat ili digitalni potpis važeći

1.3.2. Akronimi

AdES
AdES/QC

ASiC
BSP
CA
Napredni elektronski potpis
Napredni elektronski potpis kreiran sa kvalifikovanim sertifikatom
Associated Signature Container
Parametar poslovnog opsega
Autoritet za izdavanje sertifikata
DA
ESI
OCSP
OID
PAdES

PKI
QES
QTSP
QSCD
SCA
SD
SDO
SSCD
SVA
SVR
SVS
TSP
XAdES
XML
SVC
SVSP
SVSServ

Driving Application
Elektronski potpisi i infrastruktura
Online protokol statusa sertifikata
Identifikator objekta

Napredni format prenosivog dokumenta
Elektronski potpis
Infrastruktura javnog ključa
Kvalifikovani elektronski potpis
Kvalifikovani pružalac usluge poverenja
Kvalifikovani uređaj za kreiranje potpisa
Aplikacija za kreiranje potpisa
Potpisani dokument
Potpisani objekat podataka
Uređaj za bezbedno kreiranje potpisa
Aplikacija za validaciju potpisa
Izveštaj za validaciju potpisa
Usluga za validaciju potpisa
Pružalac usluge poverenja
XML Napredni elektronski potpis
eXtensible jezik za označavanje
Klijent za validaciju potpisa
Protokol usluge za validaciju potpisa
Server za validaciju potpisa

2 Odgovornosti za objavljivanje i skladište

2.1 Repozitorijumi

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

Nacrt verzija novih dokumenata koji će biti uvedeni se objavljuju na veb stranici 30 dana pre stupanja na snagu.

Dokumenti koji su na snazi dostupni su na sajtu.

Stvarna verzija politika i ugovornih uslova može se pročitati u korisničkoj službi Pružaoca usluge validacije.

Nakon zaključenja ugovora, Pružalac usluge validacije stavlja na raspolaganje Klijentu Opšte uslove i odredbe, Izjavu o otkrivanju podataka, Politiku validacije i Izjavu o praksi validacije u obliku elektronski potpisane PDF datoteke koja se može preuzeti sa svoje veb stranice.

Pružalac usluge validacije 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 validacije 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 koji se navodi u ugovoru.

Pružalac usluge validacije pregleda Opšte uslove godišnje ili ranije u slučaju izuzetnog 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 veb stranici Pružaoca usluge validacije i biće poslat na uvid Ministarstvu trgovine, turizma i telekomunikacija 30 dana pre planiranog stupanja na snagu.

3. Dizajn usluge validacije

3.1 Zahtevi procesa validacije

Inception-ova usluga validacije omogućava pretplatniku da obezbedi potpisane podatke i/ili potpise koji će biti validirani preko API-ja (trenutno nije dostupan ljudski interfejs). Usluga provere valjanosti obavlja obradu validacije prema algoritmu validacije definisanom u ETSI EN 319 102-1 [3]. Validacija na zahtevima AdES/KC i kvalifikovanog elektronskog potpisa/pečata se vrši prema ETSI TS 119 172-4 [4] politici validacije. Preko istog gore pomenutog API-ja, izveštaj o validaciji formatiran u KSML formatu, zapečaćen početnim kvalifikovanim elektronskim sertifikatom pečata čiji je privatni ključ zaštićen kvalifikovanim uređajem za potpis/kreiranje pečata, biće vraćen pretplatniku.

Na slici ispod, ekstrahovanoj iz ETSI EN 319 102-1 [3], postoji prikaz osnovnih građevnih blokova koji se koriste za implementaciju algoritma validacije i načina na koji su ovi blokovi povezani za postizanje validacije.

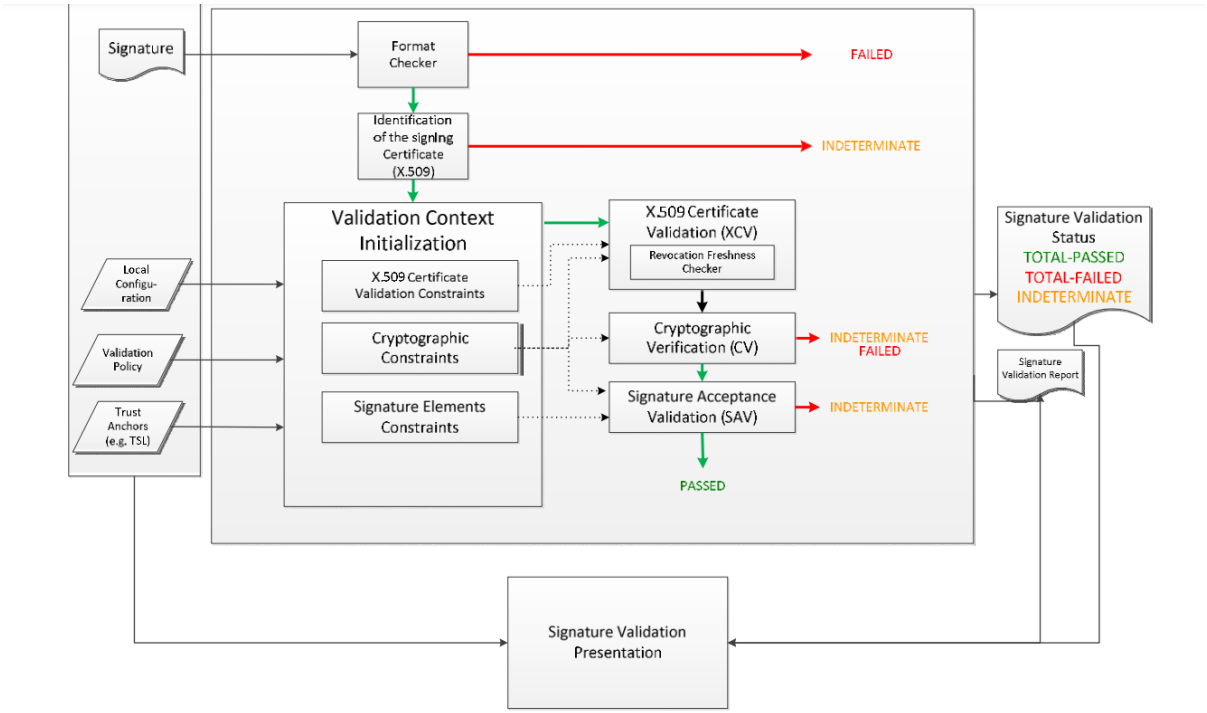


Figure 1 – Basic Signature Validation

Pružalac usluge validacije podržava samo jednu politiku validacije potpisa koja omogućava validaciju AdES/KC i kvalifikovanog elektronskog potpisa/pečata u skladu sa ETSI TS 119 172-4. Pružalac usluge validacije podržava validaciju sledećih formata potpisa:

- ETSI TS 103 172 i ETSI EN 319 142 za PAdES,
- ETSI TS 103 171 i ETSI EN 319 132 za XAdES,
- ETSI TS 119 182-1 za JAdES.

Proces koji obavlja Pružaoca usluge validacije može se podeliti u sledeća 4 koraka:

1. Pružalac usluge validacije prima zahtev za validaciju potpisa. Zahtev će sadržati:

    a. Potpisani objekat podataka sa ugrađenim potpisom(ima) ili
    b. dokument potpisnika i odgovarajuće odvojene potpise.

2. Pružalac usluge validacije obavlja proces validacije prema ETSI EN 319 102-1 specifikaciji.

3. Pružalac usluga provere priprema zapečaćeni izveštaj o validaciji u skladu sa specifikacijom ETSI TS 119 102-2 i uključuje ga u odgovor na validaciju potpisa.

4. Pružalac usluge validacije šalje odgovor na validaciju potpisa pretplatniku koji zahteva proveru potpisa. Sonda svakodnevno proverava integritet komponenti dobavljača usluge validacije. U slučaju otkrivanja neovlašćene izmene kritičnih komponenti pružaoca usluga validacije, kao što su na primer konfiguracioni fajlovi, takve komponente se popravljaju ili onemogućavaju dok njihova popravka nije moguća.

3.2 Zahtevi protokola validacije

Nije moguće da pretplatnik obezbedi politiku validacije. Pretplatnik će:

- pozvati Pružaoca usluge validacije preko obezbeđenog API-ja;
- proveriti kvalifikovani elektronski pečat na izveštaju o validaciji.

Oslanjajuće strane bi trebalo da:

- potvrde kvalifikovani elektronski pečat na izveštaju o validaciji.

3.3 Interfejs

U ovom trenutku pretplatnik može da prosledi Potpisnikov dokument/Prezentaciju potpisanog dokumenta i/ili potpis, ali mu nije dozvoljeno da pruži bilo koji drugi ulaz za proces validacije (to je bilo koji element koji može da parametariše proces validacije, kao što su ograničenja ili zahtevi usaglašenosti) . Pružalac usluge provere koristi bezbedne protokole kao što je bezbednost transportnog sloja ili veza preko bezbednog VPN-a. Zbog toga je komunikacioni kanal između **aplikacije za vožnju** i pružaoca usluge validacije obezbeđen, omogućavajući pružaocu usluge validacije da bude autentifikovan od strane **aplikacije za vožnju** i svi razmenjeni podaci budu zaštićeni enkripcijom koja obezbeđuje poverljivost podataka.

Pružalac usluge validacije ne čuva Potpisnikov dokument/predstavu potpisanog dokumenta ili potpis.

U skladu sa konceptualnim modelom procesa validacije potpisa/vremenskih oznaka definisanog u ETSI EN 319 102-1, aplikacija za validaciju prima zahteve od aplikacije za vožnju kao što je prikazano na donjoj slici izvučeno iz ETSI EN 319 102-1.

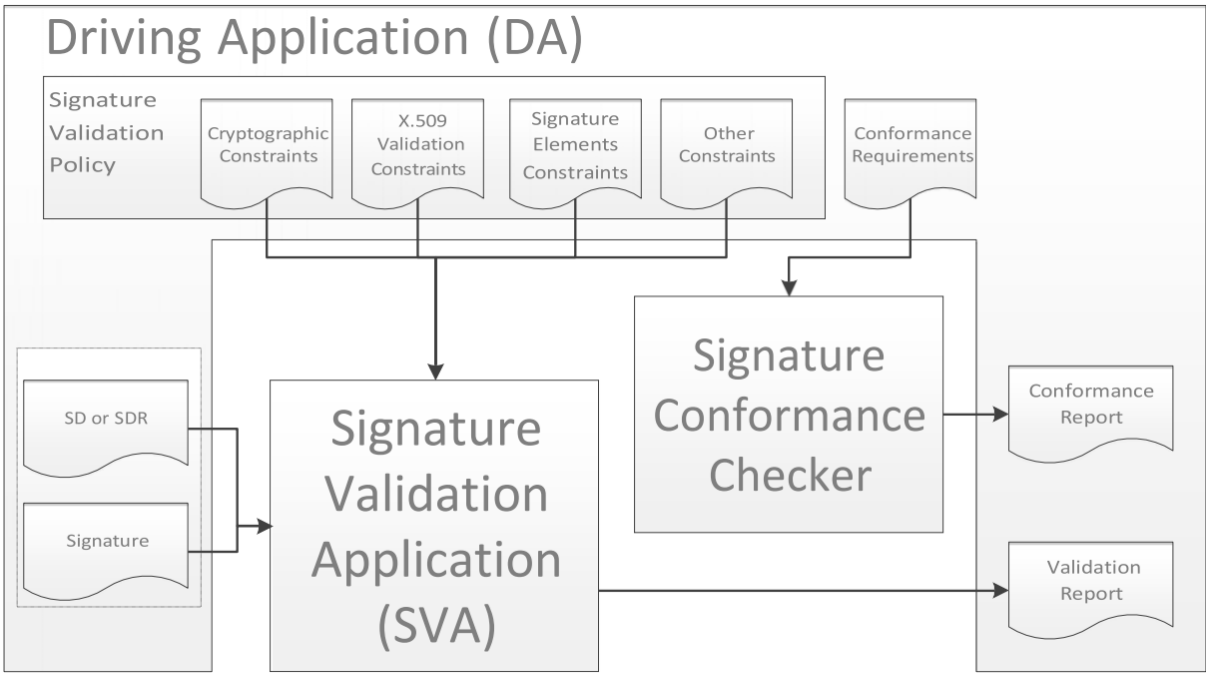


Figure 2 - Conceptual Model of Signature Validation

3.3.1 Komunikacioni kanal

Komunikacioni kanal između DA (klijenta) i Pružaoca usluge validacije nosi zahtev za validaciju potpisa i odgovor. Sinhroni je. Omogućava autentifikaciju Pružaoca usluge validacije preko TLS komunikacionog protokola.
Pretplatnici Pružaoca usluge validacije su autentifikovani.

Pružalac usluge validacije proverava podatke o statusu OCSP-a i/ili CRL-ove pomoću URL-ova ugrađenih u pristup informacijama autoriteta za potpisivanje i proširenja cRLDistributionPoints.

3.3.2 Pružalac usluge validacije - drugi Pružalac usluga od poverenja

Da bi izvršio pružanje usluge, Pružalac usluge validacije, prilikom provere opoziva, možda će morati da komunicira sa drugim kvalifikovanim dobavljačima usluga od poverenja koji traže njihove OCSP usluge i/ili tačke distribucije CRL-a. Prvenstveno se koristi OCSP protokol; ako interfejs nije dostupan ili ne pruža relevantne odgovore, koristi se CRL tačka distribucije, ako je dostupna. Na OCSP uslugu validacije utiču prakse, politike i SLA drugih kvalifikovanih

pružaoca usluga od poverenja koji nisu pod kontrolom Inceptiona. Prilikom validacije opoziva sertifikata, pretpostavlja se usklađenost OCSP usluga sa RFC6960 i drugih kvalifikovanih pružaoca usluga od poverenja sa RFC5280.

3.4 Zahtevi izveštaja o validaciji potpisa

Pružalac usluge validacije u svom odgovoru na zahtev za validaciju potpisa daje indikaciju statusa i izveštaj o validaciji koji su u skladu sa ETSI TS 119 102-2. Prema rezultatima obrade validacije potpisa, izveštaj o validaciji potpisa će ukazati na jedan od tri statusa TOTALPASSED, TOTAL-FAILED, INDETERMINATE i relevantne podindikacije kao što je definisano u ETSI EN 319 102-1. Izveštaj o validaciji potpisa ukazuje na upotrebu politike implicitne validacije potpisa za validaciju kvalifikovanog elektronskog potpisa/pečata, AdES KC, kvalifikovanih vremenskih žiga, vremenskih žiga priznatih na nacionalnom nivou i relevantnih ograničenja validacije.
Izveštaj o validaciji uključuje:

identitet Inception d.o.o. kao Pružaoca usluga validacije koji izveštava sledeće informacije:

- **X509Sertifikat**
- **X509ImePredmeta**
- **Ds:VrednostKljuča**
- X509SKI
- TSP Ime
- TSP Poštanska i elektronska adresa
- TSP Informacije URI

- identitet potpisnika
- indikacija bilo kakvih potpisanih atributa
- indikacija izvršenog procesa validacije o proces validacije za osnovne potpise procesa validacije za potpise sa vremenom i potpise sa materijalom za dugoročnu validaciju o proces validacije za potpise koji obezbeđuje dugoročnu dostupnost i integritet materijala za validaciju
- indikacija kvaliteta vremenskih oznaka, ako je prisutna u potpisima koji se validiraju
- indikacija o subjektu koji je izvršio heš računanje

- indikacija da je poreklo svakog POE iz potpisa. Izveštaj o validaciji potpisa je zapečaćen pomoću kvalifikovanog elektronskog sertifikata pečata registrovanog na Inception. Takav elektronski pečat je XAdES-B-T potpis.

4 Tehničke mere bezbednosti

4.1 Sigurnosne garancije

Pružalac usluge validacije 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 usluge validacije koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih modifikacija. I Pružalac usluga validacije, i Pružalac sistema i **izvođači instalatera** imaju značajno iskustvo u uslugama sertifikacije zgrada i koriste međunarodno priznatu tehnologiju.

4.2 Mere predostrožnosti za računarsku bezbednost

Pružalac usluga validacije koristi pouzdane IT sisteme i rešenja, tehnologije i razvija 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.

4.3 Tehničke mere predostrožnosti vezane za životni ciklus

Da bi se ispunio visok nivo bezbednosnih zahteva u svim projektima razvoja sistema Pružaoca usluga validacije, 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.

4.4 Redovna sertifikacija

Pružalac usluge validacije je obavezan da stavi vremenski žig izdat od kvalifikovanog provajdera ili da stavi vremenski pečat na materijal za dugoročnu validaciju u sledećim slučajevima:

- ukoliko Ministarstvo trgovine, turizma i telekomunikacija donese takvu odluku;

- nakon obaveznog dostavljanja obaveštenja Ministarstvu trgovine, turizma i telekomunikacija o pokretanju postupka raspuštanja ili izricanju likvidacije Pružaoca usluge validacije.

4.5 Kontinuirano praćenje tehnologije

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

4.6 Dostupnost određenih elemenata usluge validacije

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

- Usluga validacije

Pružalac usluge validacije ima pravo da suspenduje uslugu provere.

Radno vreme korisničke službe Pružaoca usluge validacije je u odeljku 1.3.1.

5 Kontrole objekata, upravljanja i rada

Pružalac usluge validacije 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 provere koristi zaštitne mere proporcionalne rizicima u vezi sa pojedinačnim elementima.

Pružalac usluge validacije prati zahteve za kapacitetom i osigurava da su adekvatna procesorska snaga i skladištenje dostupni za pružanje usluge.

5.1 Fizičke kontrole

Pružalac usluge validacije 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 da spreči nelegitiman pristup, oštećenje i neovlašćeni pristup informacijama i fizičkim zonama Pružaoca usluge provere.
Servisi koji obrađuju kritične i osetljive informacije implementiraju se na bezbednim lokacijama u sistemu Pružaoca usluge validacije.
Da biste obezbedili odgovarajuću bezbednost:

- Pružalac usluge validacije implementira snažno zaštićene usluge na lokacijama centra podataka koje koristi. Centri podataka koje koristi pružalac usluge validacije 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 validacije implementira svaku kritičnu uslugu i svaki neophodan alat u zasebnoj bezbednosnoj zoni.

5.1.1 Lokacija i izgradnja

IT sistem Pružaoca usluge provere 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 proveru poverljivih podataka koje čuva Pružalac usluge validacije.

5.1.2 Fizički pristup

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

Pružalac usluge validacije osigurava da:

- svaki ulazak u Data centre je 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 centru samo u opravdanim slučajevima, potrebno vreme iu pratnji osoblja sa odgovarajućim pravima;

- Dnevnici unosa će se kontinuirano arhivirati i evaluirati.

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

- mediji sa podacima koji sadrže osetljive informacije 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 centara je u adekvatno bezbednom radnom stanju;

- nema terminala koji je ostao prijavljen;

- fizički uređaji za skladištenje su pravilno zaključani;

- sistemi, uređaji koji obezbeđuju fizičku zaštitu ispravno funkcionišu;

- alarmni sistem je aktiviran.

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

5.1.3 Napajanje i klimatizacija

Pružalac usluga provere je osigurao da njihovi dobavljači centara podataka imaju jedinice za neprekidno napajanje (UPS) i rezervne generatore koji:

- adekvatan kapacitet za osiguranje napajanja za svoje objekte i sisteme
- štiti IT opremu od fluktuacija napona u spoljnoj mreži, nestanka struje, skokova i drugog
- u slučaju dugotrajnog nestanka struje ima dovoljno kapaciteta i mogućnosti dopunjavanja goriva da pokreće generatore u bilo kom vremenskom periodu

5.1.4 Izloženost vodi

Prodavci centara podataka dobavljača usluge validacije su adekvatno zaštićeni od prodora vode i poplava.

5.1.5 Prevencija i zaštita od požara

Prodavci Data centara Pružaoca usluge validacije imaju sisteme za zaštitu od požara odobrene od strane odgovarajućih vlasti. 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 relevantnim propisima..

5.1.6 Skladištenje medija

Pružalac usluge validacije 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 centra podataka i u oblaku.

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

5.1.7 Odlaganje otpada

Dobavljač usluga validacije obezbeđuje odlaganje suvišne imovine i medija u skladu sa ekološkim standardima.

Pružalac usluge validacije ne koristi elektronske medije za skladištenje podataka 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 validacije. Pružalac usluge validacije 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

5.1.8 Bekap van lokacije

Pružalac usluge validacije 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.

5.2 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 koji se očekuju u različitim ulogama.

Pojedinci odgovorni za dati sistemski element ili proces se nedvosmisleno dodeljuju svakom elementu sistema i svakom procesu u njegovom sistemu. Zadaci koji se odnose na razvoj i operacije oštro su razdvojeni u sistemu dobavljača usluga validacije.

5.2.1 Povereničke uloge

Pružalac usluge validacije definiše sledeće pouzdane uloge, sa sledećim odgovornostima:

Menadžer implementacije

Osoba koja pruža usluge poverenja; operativno upravljanje.

Inženjer baze podataka

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

Sistemski inženjer

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

Službenik 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 validacije. Pouzdane uloge se neće obavljati u kontekstu ugovora o proviziji.

Inženjer podrške

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

Administrativni radnik

Odgovoran za vođenje dokumentacije kompanije, čuvanje dokumenata po klasifikacijama.

Pravni savetnik

Odgovoran je za poštovanje važnih zakona EU i Srbije, međunarodnih standarda i preporuka. Priprema predloga potrebnih 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 obavljanje delatnosti..

5.2.2 Broj potrebnih osoba po zadatku

Bezbednosni i operativni propisi Pružaoca usluge validacije definišu da se sledeći zadaci mogu obavljati samo u zaštićenom okruženju, uz istovremeno prisustvo dvoje zaposlenih koji imaju uloge od poverenja:

- generisanje sopstvenog para ključeva Pružaoca usluge validacije;
- 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 validaciju su odgovorni za bezbedno upravljanje dešifrovanim objektom za validaciju i za njegovo uništavanje ako je potrebno.

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

5.2.3 Identifikacija i autentifikacija za svaku ulogu

Korisnici koji upravljaju IT sistemom Pružaoca usluge validacije 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.

5.2.4 Uloge koje zahtevaju razdvajanje dužnosti

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

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

Pored gore pomenutog, Pružalac usluge validacije traži potpuno razdvajanje uloga od poverenja.

5.3 Kontrola osoblja

Pružalac usluge validacije vodi računa o tome da njegova kadrovska politika i njegove prakse primenljive na zapošljavanje članova osoblja intenziviraju i podržavaju pouzdanost rada Pružaoca usluge validacije. Cilj mera predostrožnosti koje se primenjuju na osoblje je smanjenje rizika od ljudskih grešaka, krađe, prevare i slučajeva zloupotrebe.
Pružalac usluge validacije 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 Provajdera usluge validacije – treba da potpišu ugovor o neotkrivanju podataka.
Istovremeno, Pružalac usluge validacije obezbeđuje svojim zaposlenima sticanje i dalji razvoj zajedničkog, opšteg znanja i specijalizovanih stručnih znanja neophodnih za obavljanje različitih poslova.

5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje

Kao uslov za zapošljavanje, Pružalac usluga validacije zahteva najmanje srednju stručnu spremu, ali Pružalac usluga validacije nastavlja da vodi računa o tome da zaposleni prođu odgovarajuću obuku. Neposredno po prijemu u radni odnos, Pružalac usluge validacije dodeljuje obuku za svoje nove zaposlene, u okviru koje oni stiču znanja neophodna za obavljanje posla. Pouzdane uloge kod Pružaoca usluga validacije mogu obavljati samo osobe koje nemaju spoljni uticaj i koje poseduju neophodnu stručnost koju je proveravao Pružalac usluge validacije.
Svo osoblje u pouzdanim ulogama neće biti u sukobu interesa koji bi mogao ugroziti nepristrasnost operacija Pružaoca usluge validacije.

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

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

- najmanje tri godine stručnosti u profesionalnom radnom iskustvu u oblasti informacione bezbednosti.

5.3.2 Procedure provere pozadine

Pružalac usluga validacije 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 kod Pružaoca usluga validacije sa izjavom, službenik nosioca uloge od poverenja sa sertifikatom o dobrom ponašanju starom manje od 3 meseca opravdati čist krivični dosije.
Pružalac usluga provere verodostojnosti relevantnih informacija navedenih u biografiji kandidata tokom procesa zapošljavanja, kao što su prethodno zaposlenje, profesionalne reference i najrelevantnije obrazovne kvalifikacije.

5.3.3 Zahtevi za obuku

Pružalac usluge validacije obučava novozaposlene zaposlene, tokom koje oni stiču

- osnovno PKI znanje;
- specifičnosti i način rukovanja IT sistemom Pružaoca usluge validacije;
- neophodna posebna znanja za obavljanje njihovog delokruga;
- procesi i procedure definisane u javnom i internim propisima Pružaoca usluge validacije;
- pravne posledice pojedinačnih aktivnosti;
- važeći propisi o IT bezbednosti 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 validacije.

5.3.4 Učestalost i uslovi prekvalifikacije

Pružalac usluge validacije obezbeđuje da zaposleni poseduju neophodna znanja u kontinuitetu, pa se po potrebi održava dalja ili ponavljana obuka.
Dalja obuka se održava ako dođe do promene u procesima ili IT sistemu Pružaoca usluge validacije. Obuka je adekvatno dokumentovana, iz čega se jasno može odrediti nastavni plan i obim zaposlenih učesnika.

5.3.5 Učestalost i redosled rotacije poslova

Pružalac usluge validacije ne primenjuje obaveznu rotaciju između pojedinačnih rasporeda rada.

5.3.6 Sankcije za nedozvoljene radnje

Pružalac usluge validacije 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 validacije, 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 poslove bezbednosti,
- 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 ili kršenja zakona.

5.3.7 Zahtevi nezavisnog izvođača

Pružalac usluge validacije dodeljuje samo pouzdane uloge svojim zaposlenima.

Pružalac usluge validacije bira osobe zaposlene sa ugovorom o angažovanju ili podugovorom za obavljanje drugih zadataka, po mogućnosti, sa liste prethodno kvalifikovanih dobavljača. Pružalac usluge validacije 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. Izjava o poverljivosti uključuje sankcije u slučaju kršenja. Od spoljnih zaposlenih po ugovoru se očekuje da imaju odgovarajuće tehničke veštine, a Pružalac usluga validacije ne održava nikakvu obuku za njih.

5.3.8 Dokumentacija dostavljena osoblju

Pružalac usluge validacije 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:

- organizacione bezbednosne propise Pružaoca usluge validacije,

- ugovor o poverljivosti koji treba potpisati,
- lični opis posla,
- edukativni materijali povodom planirane ili posebne obuke za određeni oblik obrazovanja.

5.4 Procedure evidentiranja revizije

5.4.1 Vrste snimljenih događaja

Pružalac usluge validacije 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 je pokrenuo 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 Pružalac usluge validacije.

Pružalac usluge validacije evidentira najmanje sledeće događaje:

- UNUTRAŠNJI SAT
  - sinhronizaciju unutrašnjeg sata sa UTC vremenom, uključujući i operativne ponovne kalibracije;
  - gubitak sinhronizacije;
- VALIDACIJA
  - informacije koje se odnose na dostupnost podataka, integritet validiranih potpisa, autentičnost, održavanje čitljivosti i brisanje informacija;
  - informacije vezane za preuzimanje dokaza o validaciji, ispunjenje zahteva za izjavu i predaju arhive drugom provajderu;

- EVIDENCIJA:
  - gašenje, ponovno pokretanje sistema za evidentiranje ili neke njegove komponente;
  - izmenu bilo kog parametra podešavanja evidentiranja, na primer učestalosti, praga upozorenja i događaja koji treba ispitati;
  - izmenu 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 prijavljivanja u slučaju prijavljivanja korisnika;
    - ☐ blokiran ponovni prijem korisnika zbog neuspešnih pokušaja prijave;
  - promena tehnike autentifikacije (na primer sa lozinke na bazi PKI).
- UPRAVLJANJE KLJUČEM:
  - 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;
- *Hardverski sigurnosni modul*:
  - instaliranje Hardverskog sigurnosnog modula;
  - uklanjanje hardverskog bezbednosnog modula;
  - odlaganje, uništavanje hardverskog bezbednosnog modula;

  - isporuka Hardverskog sigurnosnog modula;
  - brisanje (resetovanje) hardverskog bezbednosnog modula;
  - učitavanje ključeva, sertifikata u Hardverski sigurnosni modul.
- PROMENA KONFIGURACIJE:
  - hardver;
  - softver;
  - operativni sistem;
  - peč;
  - instaliranje, ažuriranje i uklanjanje softvera na sistemu sertifikata;
- FIZIČKI PRISTUP, BEZBEDNOST LOKACIJE:
  - ulazak i izlazak lica iz bezbednosne zone u kojoj se nalaze komponente sistema koje se koriste za pružanje usluge poverenja;
  - pristup sistemskoj komponenti koja se koristi za pružanje usluge poverenja;
  - poznato ili sumnjivo kršenje fizičkog obezbeđenja;
  - saobraćaj zaštitnog zida ili rutera.
- OPERATIVNE ANOMALIJE:
  - pad sistema, kvar hardvera;
  - kvarovi u softveru;
  - greška u validaciji integriteta softvera;
  - netačne ili pogrešno adresirane poruke;
  - mrežni napadi, pokušaji napada;
  - kvar opreme;
  - kvarovi električne energije;
  - greška u neprekidnom napajanju;
  - suštinska greška u pristupu mrežnoj usluzi;

  - kršenje Izjave o praksi kvalifikovane validacije;
  - brisanje sata operativnog sistema.

- OSTALI 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.

5.4.2 Učestalost obrade dnevnika revizije

Nezavisni sistemski revizori Pružaoca usluge validacije 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, provajder usluga provere koristi takođe automatizovane alate za procenu, koji se koriste za praćenje rezultujućih unosa dnevnika 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.

5.4.3 Period zadržavanja za evidenciju revizije

Pre brisanja iz onlajn sistema, dnevnici se arhiviraju i njihovu bezbednu validaciju obezbeđuje Pružalac usluge provere za vreme definisano u odeljku 6.5.2, ali najmanje 10 godina od datuma njihovog kreiranja.

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

5.4.4 Zaštita dnevnika revizije

Pružalac usluge validacije štiti kreirane evidencije sve dok je validnost dokaza validacije, obezbeđena su sledeća svojstva podataka evidencije:

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

- dostupnost: ovlašćenim licima je omogućen pristup evidenciji;

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

Pružalac usluge validnosti obezbeđuje zapise dnevnika sa kvalifikovanim vremenskim oznakama i oni se čuvaju na način koji isključuje besprekorno umetanje i brisanje unosa u evidenciju.
Datoteke evidencije su zaštićene od slučajnog i zlonamernog oštećenja rezervnim kopijama. U slučaju unosa u dnevnik koji sadrže lične podatke, Pružalac usluge validacije 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 validacije verifikuje pristupe na bezbedan način. Pružalac usluge validacije čuva datoteke evidencije u bezbednom okruženju. Čuva kopije datoteka na drugom mestu operacije.

5.4.5 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 čuvaju fizički odvojeno jedna od druge, na odvojenim lokacijama tokom potrebnog vremena.

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

5.4.6 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 evidenciju, Pružalac usluge provere obustavlja rad povezanih oblasti dok se incident ne reši.

5.4.7 Obaveštenje subjektu koji izaziva događaj

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

5.4.8 Procene ugroženosti

Pored svakodnevne obrade log unosa, stručnjaci Pružaoca usluge provere provere 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 validacije vrše sveobuhvatnu analizu ranjivosti koristeći mapiranje potencijalnih unutrašnjih i eksternih pretnji što može dovesti do neovlašćenog pristupa.

Na osnovu rezultata analize Pružalac usluge validacije:

- kreira i sprovodi plan za ublažavanje ranjivosti; ili
- dokumentuje činjeničnu osnovu za odluku da je preostali rizik prihvaćen i da ranjivost ne zahteva sanaciju.

Najpre se nove verzije softvera i softverske zakrpe instaliraju na testni sistem Pružaoca usluge validacije, a tek nakon uspešno završenog testa se instaliraju na živi sistem koji se koristi za pružanje usluga.

Nove softverske zakrpe se ne instaliraju na sistem uživo ako unose dodatne ranjivosti ili nestabilnosti koje prevazilaze prednosti njihove primene. Razlozi za neprimenu bezbednosnih zakrpa su dokumentovani.

5.5 Oporavak od kompromitovanja i katastrofe

U slučaju havarije, Pružalac usluge validacije 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.

5.5.1 Procedure za rukovanje incidentima i kompromitovanjem

Pružalac usluge validacije ima plan kontinuiteta poslovanja.

Pružalac usluge validacije 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 čitav niz usluga.

Pružalac usluga validacije svake godine testira prelazak na rezervni sistem i pregleda svoje planove za kontinuitet poslovanja.
Pružalac usluge validacije 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 pravljenje rezervnih kopija Pružaoca usluge validacije.

Pružalac usluga validacije 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.

5.5.2 Računarski resursi, softver i/ili podaci su oštećeni

IT sistemi Pružaoca usluga validacije su izgrađeni 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 validacije pravi potpunu dnevnu rezervnu kopiju svojih baza podataka i generisanih događaja evidencije.

Pružalac usluge validacije 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, dobavljač usluge validacije ponovo pokreće svoje usluge što je pre moguće.

5.5.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Definisani su zadaci koji se obavljaju u slučaju kvara usluge usled elementarne nepogode ili druge nepogode
u planu kontinuiteta poslovanja Pružaoca usluga validacije. 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 validacije je dužan da u slučaju katastrofe obavesti pogođene korisnike što je pre moguće.

Nakon obnavljanja usluga, Pružalac usluge validacije vraća svoje uređaje oštećene tokom katastrofe i prvobitni nivo bezbednosti usluge što je pre moguće.

5.6 Prestanak usluge validacije

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

- Prihvatanje novih zahteva za validaciju

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

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

- Izdavanje izjava o pohranjenim Validacijskim dokazima

U isto vreme raskida, pružalac usluge provere isključuje sledeće usluge:

- Usluga validacije
- Tehnička podrška
- Obezbeđivanje informacija.

Pre planiranog raskida, Pružalac usluge validacije se upušta u pregovore o preuzimanju svojih usluga sa drugim provajderom 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 validacije preduzima mere u vezi sa opozivom sertifikata provajdera (i uništavanjem privatnih ključeva) tokom perioda od 60 dana – u zavisnosti od ishoda pregovora.

Pružalac usluge validacije obaveštava Ministarstvo trgovine, turizma i telekomunikacija o konačnom ishodu pregovora. Pružalac usluge validacije treba da obavesti svoje klijente elektronskom poštom, a pouzdane strane putem publikacije na svojoj veb stranici.
Po okončanju usluge, Pružalac usluge validacije pravi rezervnu kopiju punog obima svojih podataka sadržanih u njegovom IT sistemu, zaštićenih kvalifikovanom vremenskom oznakom.
Da bi omogućio predaju svojih podataka drugom pružaocu usluga od poverenja, Pružalac usluge provere 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 validacije 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.

6 Tehničke bezbednosne kontrole

Pružalac usluga validacije koristi sisteme koji se sastoje od pouzdane i sigurnosno tehnički procenjene opreme za pružanje svojih usluga. Pružalac usluge validacije upravlja kriptografskim privatnim ključevima provajdera tokom celog njihovog životnog ciklusa u okviru hardverskog bezbednosnog modula koji ima odgovarajući sertifikat.

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

6.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula

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

6.1.1 Standardi i kontrole kriptografskog modula

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

- zahtevima ISO/IEC 19790 [37], ili
- zahteve FIPS 140-2 [38] nivoa 3 ili više, ili
- zahteve FIPS 140-3 [39] nivoa 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 validacije 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 dobavljača usluga provere se čuvaju 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 validacije uništava kodirane ključeve ili ih ponovo kodira koristeći algoritam i parametre ključa koji obezbeđuju veću zaštitu.

6.1.2 Privatni ključ (N od M) Kontrola više osoba

Pružalac usluge validacije 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 pružaoca.

6.1.3 Deponovanje privatnog ključa

Pružalac usluge validacije ne deponuje privatne ključeve svog Pružaoca.

6.1.4 Rezervna kopija privatnog ključa

Pružalac usluge validacije 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 isključenjem 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 validacije čuva rezervnu kopiju u duplikatu, a najmanje jedna kopija se čuva na drugom mestu od lokacije dobavljača usluge.
Na upravljanje i validaciju rezervnih kopija primenjuju se isti strogi bezbednosni standardi kao i za rad proizvodnog sistema.

6.1.5 Arhiva privatnog ključa

Pružalac usluge validacije ne arhivira svoje privatne ključeve.

6.1.6 Prenos privatnog ključa u ili iz kriptografskog modula

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

6.1.7 Skladištenje privatnog ključa na kriptografskom modulu

Pružalac usluge provere 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.

6.1.8 Način aktiviranja privatnog ključa

Pružalac usluge validacije 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 i privatni ključevi unutar Hardverskog bezbednosnog modula se ne mogu koristiti pre aktiviranja modula. Pružalac usluge validacije čuva kartice operatera u bezbednom okruženju i do tih kartica mogu da dođu samo ovlašćeni zaposleni kod Pružaoca usluge validacije.

6.1.9 Metoda deaktiviranja privatnog ključa

Privatni ključ koji koristi Pružalac usluge validacije 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.

6.1.10 Metoda uništavanja privatnog ključa

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

6.1.11 Ocena kriptografskog modula

U skladu sa zahtevima odeljka 7.1.1, svaki privatni ključ Pružaoca usluge validacije 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

6.2 Podaci o aktivaciji

6.2.1 Generisanje i instalacija aktivacionih podataka

Privatni ključevi Pružaoca usluge validacije su zaštićeni 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.

6.2.2 Zaštita podataka aktivacije

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

6.2.3 Drugi aspekti aktivacionih podataka

Bez uslova.

6.3 Kontrole kompjuterske bezbednosti

6.3.1 Specifični tehnički zahtevi za bezbednost računara

Tokom konfiguracije i rada svog IT sistema, Pružalac usluga provere provere obezbeđuje usklađenost sa sledećim zahtevima:

- identitet korisnika se verifikuje pomoću kontrola autentifikacije sa dva faktora korišćenjem VPN sertifikata koji se čuvaju 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 dnevniku se kreira za svaku transakciju, a unosi se arhiviraju;

- za bezbednosno kritične procese obezbeđuje se da su interni mrežni domeni Pružaoca usluge provere dovoljno zaštićeni od neovlašćenog pristupa;

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

6.3.2 Ocena računarske bezbednosti

Početak naglašava važnost iskustva klijenta. U cilju održavanja visokog nivoa usluga, Inception upravlja sistemom kontrole kvaliteta u skladu sa standardom ISO 9001.
Inception pridaje visoki 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 validacije

- postavlja nove mere za uklanjanje ranjivosti, ili/i

- prihvata identifikovane preostale rizike navodeći razlog za odluku.

6.4 Tehničke kontrole životnog ciklusa

6.4.1 Kontrole razvoja sistema

Pružalac usluge validacije koristi samo aplikacije i uređaje u svojoj proizvodnji
IT sistem koji su:

- komercijalni softver u kutiji, dizajniran i razvijen prema dokumentovanoj metodologiji dizajna, ili;

- prilagođena hardverska i softverska rešenja razvijena od strane samog Pružaoca usluge validacije tokom kojih su korišćene strukturirane metode razvoja i kontrolisano razvojno okruženje, ili;

- prilagođena hardverska i softverska rešenja razvijena od strane pouzdane strane za Pružaoca usluge validacije tokom kojih su korišćene strukturisane metode razvoja i kontrolisano razvojno okruženje, ili;

- softver otvorenog koda koji je u skladu sa bezbednosnim zahtevima i njihova adekvatnost je obezbeđena verifikacijom softvera i strukturiranim razvojem i upravljanjem životnim ciklusom.

Nabavka IT alata se vrši na način koji isključuje promene na hardverskim i softverskim komponentama korišćenjem pouzdanih, redovno kvalifikovanih pružaoca.
Pružalac usluge validacije ne koristi hardverske i softverske komponente primenjene za pružanje usluga u druge svrhe.

Pružalac usluge validacije 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 usluga validacije upošljava pouzdano, adekvatno obučeno osoblje tokom instaliranja softvera i hardvera.

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

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

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

6.4.2 Kontrole upravljanja bezbednošću

Pružalac usluge validacije 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 kakvu 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 usluzi, dobavljač usluge provere provere obezbeđuje da je program koji treba da se instalira ispravna verzija i da nema bilo kakvih neovlašćenih modifikacija.
Pružalac usluge validacije redovno proverava integritet softvera u svom sistemu koji se koristi u usluzi.

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

- nakon preuzimanja uređaja prilikom preuzimanja,
- neposredno pre prve upotrebe,
- redovno tokom rada.

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

Pružalac usluge validacije skladišti neiskorišćene hardverske bezbednosne module na fizički zaštićenoj lokaciji.

6.4.3 Sigurnosne kontrole životnog ciklusa

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

- koristi pravilno sertifikovane hardverske bezbednosne module u svojim sistemima;
- obezbediti, po prijemu hardverskih bezbednosnih modula, da kontrola kvalteta 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 neovlašćenog pristupa tokom skladištenja;

- kontinuirano ispunjava zahteve postavljene u bezbednosnom cilju Hardverskog bezbednosnog modula, uputstvima za upotrebu i izveštaju o sertifikaciji tokom rada;

- briše privatne ključeve uskladištene u njihovim rastavljenim hardverskim bezbednosnim modulima na takav način da postaje praktično nemoguće vratiti ključeve;

- rukuje i odlaže prekinute hardverske bezbednosne module u skladu sa zahtevima njihovog bezbednosnog cilja, uputstvima za upotrebu i izveštajem o sertifikaciji.

6.5 Kontrole mrežne bezbednosti

Pružalac usluge validacije sledi najbolje industrijske prakse za obezbeđivanje svojih mreža.

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

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

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

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

- deli svoj IT sistem na dobro odvojene bezbednosne zone;

- odvaja namensku mrežu za administraciju IT sistema i operativnu mrežu Pružaoca usluge validacije;

- 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;

- deaktivira 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 validacije prolazi kroz ili vrši skeniranje ranjivosti na javnim i privatnim IP adresama:

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

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

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

6.6 Vremensko žigosanje

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

7 Revizija usklađenosti i druge procene

Rad Pružaoca usluge validacije nadzire Ministarstvo trgovine, turizma i telekomunikacija u skladu sa propisima Evropske unije. Ministarstvo trgovine, turizma i telekomunikacija održava inspekcije na lokaciji najmanje jednom godišnje na lokaciji pružaoca usluge validacije. Pre inspekcije na licu mesta, Pružalac usluge validacije vrši skrining svog poslovanja od strane eksternog revizora i šalje detaljan izveštaj o skriningu Ministarstvu trgovine, turizma i telekomunikacija u roku od 3 dana od njegovog prijema. Tokom skrininga treba da se utvrdi da li rad Pružaoca usluge validacije ispunjava zahteve eIDAS Uredbe [1] i srodnog srpskog zakonodavstva i zahteve primenjene Politike(e) kvalifikovane validacije i odgovarajuće Izjave o praksi kvalifikovane validacije. (s).

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

- UREDBA (EU) br. 910/2014 EVROPSKOG PARLAMENTA I
- SAVET 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 infrastruktura (ESI); Procena usaglašenosti provajdera povereničkih usluga; Deo 1: Zahtevi za tela za ocenjivanje usaglašenosti koja ocenjuju pružaoce usluga od poverenja; [43]

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

- ETSI TS 119 511 Elektronski potpisi i infrastruktura (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji obezbeđuju dugoročnu validaciju 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 usluga validacije.
Pružalac usluge validacije primenjuje verifikovane i sertifikovane elemente (elemente IT sistema za proizvodnju elektronskog potpisa) u vezi sa uslugom.
Pružalac usluge provere je ocenio svaki element sistema koji se koristi za pružanje usluga u bezbednosne klase na osnovu svog sistema procene rizika. Pružalac usluge validacije vodi evidenciju o ovim elementima sistema i bezbednosnim ocenama povezanim sa njima u okviru svog sistema upravljanja rizikom.

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

Pružalac usluga validacije ima sistem upravljanja kvalitetom usklađen 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)

7.1 Učestalost ili okolnosti procene

Pružalac usluge provere usaglašenosti sprovodi godišnje procenu usklađenosti na svom IT sistemu koji obavlja pružanje usluga.

7.2 Identitet/kvalifikacije ocenjivača

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

7.3 Odnos procenjivača prema procenjenom entitetu

Eksternu reviziju vrši lice koje:

- je nezavisan od vlasnika, menadžmenta i poslovanja ispitanog Pružaoca usluga validacije;
- je nezavisan od ispitane organizacije, odnosno, ni on ili ona, niti njegovi ili njeni najbliži srodnici nemaju nikakav radni ili poslovni odnos sa Pružaocem usluga validacije.
- naknada ne zavisi od nalaza aktivnosti sprovedenih tokom revizije.

7.4 Teme obuhvaćene ocenjivanjem

Pregled pokriva sledeće oblasti:

- usklađenost sa zakonima koji su trenutno na snazi;
- usklađenost sa tehničkim standardima;
- usklađenost sa Politikom sertifikacije i Izjavom o praksi kvalifikovane validacije;
- adekvatnost upotrebljenih procesa;
- dokumentacija;
- fizičko obezbeđenje;
- adekvatnost osoblja;
- IT bezbednost;
- poštovanje pravila zaštite podataka.

7.5 Radnje preduzete kao rezultat nedostatka

Nezavisni revizor rezimira rezultat 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 izmene koje se opciono uzimaju u obzir;

- derogacije koje treba izbegavati obavezno.

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

Pružalac usluge validacije će pismenim putem odgovoriti na probleme koje je naznačio nezavisni revizor i izvestiti o merama koje su preduzete da ih spreči prilikom sledeće revizije.

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

REFERENCE

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

[2] ETSI TS 119 441 V1.1.1 (2018-08) Aneks A (informativni): Sadržaj prakse usluge provere valjanosti potpisa
izjave

[3] ETSI EN 319 102-1 V1.1.1 Elektronski potpisi i infrastrukture (ESI); Procedure za kreiranje i validaciju AdES digitalnih potpisa; Deo 1: Kreiranje i validacija

[4] ETSI SR 019 050 V1.1.1 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 Elektronski potpisi i infrastrukture (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja

[6] ETSI EN 319 421 V1.1.1 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 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 Elektronski potpisi i infrastrukture (ESI); Elektronske usluge registrovane isporuke; Deo 1: Okvir i arhitektura

[9] Nacrt ETSI EN 319 522-2 V1.0.0 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 provajdere elektronskih registrovanih usluga isporuke