



REPUBLIKA HRVATSKA
MINISTARSTVO GOSPODARSTVA, RADA I PODUZETNIŠTVA
10000 ZAGREB - Ulica grada Vukovara 78

Klasa: 330-01/04-01/30
Urbroj: 526-01/04-04

NACIONALNI CA ZA REPUBLIKU HRVATSKU (NCARH)

OPĆA PRAVILA CERTIFICIRANJA (CP)
Verzija 1.0
Datum 22.01.2004.

AUTORSKA PRAVA

Ovaj dokument je u vlasništvu Ministarstva gospodarstva, rada i poduzetništva i FINE i podložan je zaštiti autorskih prava prema zakonima Republike Hrvatske.

KRATICE, REFERENCE I DEFINICIJE

Cjelokupna se dokumentacija referencira na zakone, pravilnike, direktive, standarde i NCARH dokumentaciju, nadalje definirani su standardi za tumačenja pojedinih kratica i pojmova koje se koriste u HR PKI i NCARH dokumentaciji.

Dokument **Kratice, reference i definicije** je u prilogu.

PRIMJEDBE I PROMJENE

Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene Povjerenstvu za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure.

Obavijest o finalnim promjenama

Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure odredit će period za obavijest o finalnim promjenama.

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene

OBJAVA

Na temelju odluke o prihvaćanju i objavi dokumenata NCARH-a donijete na sjednici Povjerenstva za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure održanoj dana 22. siječnja 2004. godine Ministarstvo gospodarstva rada i poduzetništva objavljuje navedene dokumente.

U Zagrebu 15. ožujka 2004.g.



MINISTAR
Branko Vukelić

REPUBLICA HRVATSKA
MINISTARSTVO
GOSPODARSTVA
RADE I
PODUZETNIŠTVA
ZAGREB

Sadržaj

1.	UVODNE OZNAKE I TEMELJNI PODACI	1
1.1.	Opis usluga.....	1
1.1.1.	Pregled.....	1
1.2.	Identifikacijski podaci i OID oznaka.....	2
1.2.1.	OID za NCARH CP.....	2
1.3.	Davatelji usluga, korisnici i područje primjene usluga.....	2
1.3.1.	PMA HR PKI	2
1.3.2.	NCARH	3
1.3.3.	Operativna organizacija NCARH (OA NCARH).....	3
1.3.4.	Glavni (Principal) CA CSP	3
1.3.5.	Krajnji korisnici.....	4
1.3.6.	Područje primjene.....	4
1.4.	Adresni podaci.....	5
2.	OPĆE ODREDBE.....	7
2.1.	Obveze davatelja usluga, subjekata i korisnika.....	7
2.1.1.	Obveze CA	7
2.1.2.	Obveze RA	7
2.1.3.	Obveze Subjekata	7
2.1.4.	Obveze pouzdajuće strane	7
2.1.5.	Obveze repozitorija	7
2.2.	Odgovornost.....	8
2.3.	Financijska odgovornost.....	8
2.3.1.	Odšteta od pouzdajuće strane ili potpisnika	8
2.3.2.	Administrativni procesi	8
2.4.	Usklađenost sa zakonom	8
2.4.1.	Odjeljenost odredbi	8
2.4.2.	Procedure za rješavanje nesuglasica.....	8
2.5.	Objava i repozitorij certifikata	8
2.5.2.	Učestalost objavljivanja.....	9
2.5.3.	Kontrole pristupa.....	9
2.5.4.	Repozitoriji.....	9
2.6.	Provjera usklađenosti.....	9
2.6.1.	Učestalost	9
2.6.2.	Identitet i kvalifikacije inspektora	9
2.6.3.	Neutralnost inspektora	9
2.6.4.	Svrha revizije i inspekcije	10
2.6.5.	Poduzimanje akcija kao rezultat inspekcije.....	10
2.7.	Povjerljivost i tajnost (poslovanja i podataka).....	10
2.8.	Prava intelektualnog vlasništva	10
3.	IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA	11
3.1.	Registracija Subjekta.....	11
3.1.1.	Potreba da ime ima značenje	11
3.1.2.	Pravila za interpretiranje različitih formi imena.....	11
3.1.3.	Metode dokazivanja posjedovanja privatnog ključa.....	11

3.1.4.	Autentifikacija identiteta organizacije.....	11
3.1.5.	Certifikati za pripadajuće osobe.....	12
3.1.6.	Identifikacija i autentifikacija osoba.....	12
3.1.7.	Ovlaštene osobe.....	13
3.2.	Plansko obnavljanje certifikata.....	13
3.2.1.	Obnavljanje ključeva.....	13
3.2.2.	Obnova certifikata.....	14
3.2.3.	Izmjene informacija u certifikatu.....	14
3.3.	Obnavljanje nakon opoziva ili isteka certifikata.....	14
3.4.	Zahtjev za opoziv.....	15
4.	OSNOVNI ZAHOTJEVI U RADU SA CERTIFIKATIMA.....	17
4.1.	Zaprimanje zahtjeva za izdavanje certifikata.....	17
4.1.1.	Dostava javnog ključa za izdavanje certifikata.....	17
4.2.	Izdavanje certifikata.....	17
4.2.1.	Dostava subjektova privatnog ključa subjektu.....	18
4.2.2.	Dostava i uporaba javnog ključa NCARH.....	18
4.3.	Prihvatanje certifikata.....	18
4.4.	Opoziv i suspenzija certifikata.....	18
4.4.1.	Uvjeti za opoziv certifikata koje je izdao NCARH ili CA CSP.....	18
4.4.2.	Suspenzija.....	20
4.4.3.	Lista opozvanih certifikata.....	20
4.4.4.	Raspoloživost online provjere opoziva/statusa.....	21
4.5.	Postupci provjere sigurnosnih mjera.....	21
4.5.1.	Tipovi događaja koji će se bilježiti.....	21
4.5.2.	Učestalost procesiranja log-a.....	25
4.5.3.	Period čuvanja revizijskog loga.....	26
4.5.4.	Zaštita revizijskog loga.....	26
4.5.5.	Backup procedure revizijskog loga.....	26
4.5.6.	Sustav revizije (unutarnja ili vanjska).....	27
4.5.7.	Obavijest subjektu koji je izazvao događaj.....	27
4.5.8.	Procjene ranjivosti.....	27
4.6.	Arhiviranje certifikata i podataka.....	27
4.6.1.	Tipovi pohranjenih podataka.....	27
4.6.2.	Period arhiviranja.....	28
4.6.3.	Zaštita arhive.....	28
4.6.4.	Back-up arhive.....	29
4.6.5.	Zahtjevi za vremenski žig zapisa.....	29
4.6.6.	Sustav prikupljanja arhivske građe (unutarnji ili vanjski).....	29
4.6.7.	Procedure pribavljanja i provjere arhivskih informacija.....	29
4.7.	Zamjena certifikata (ključeva).....	29
4.8.	Postupci otklanjanja posljedica elementarnih nepogoda i incidenata.....	29
4.8.1.	Oštećenje računalnih resursa, softvera i/ili podataka.....	29
4.8.2.	Sigurnosne prilike nakon elementarnih nepogoda ili incidenata.....	29
4.8.3.	Opoziv NCARH potpisnog ključa ili potpisnog ključa CA CSP.....	30
4.8.4.	Kompromitiranje NCARH potpisnog ključa ili potpisnog ključa CA CSP.....	30

Sadržaj

4.9. Prestanak rada - davanja usluga	30
5. KONTROLE TEHNIČKE SIGURNOSTI RADA SUSTAVA CERTIFICIRANJA...31	
5.1. Kontrola prostora, opreme i sredstava..... 31	
5.1.1. Lokacija prostorije i njena konstrukcija	31
5.1.2. Fizički pristup.....	31
5.1.3. Sustav za napajanje i klima uređaji	32
5.1.4. Opasnost od poplave.....	32
5.1.5. Protupožarna zaštita.....	33
5.1.6. Čuvanje medija za pohranu podataka	33
5.1.7. Rješavanje otpada.....	33
5.1.8. Backup na drugoj lokaciji.....	33
5.2. Kontrola postupaka i provedbe radnih zadataka	33
5.2.1. Osobe od povjerenja	33
5.2.2. Broj osoba potrebnih za izvođenje operacija.....	33
5.2.3. Identifikacija i autentifikacija za izvršenje određene korisničke uloge.....	34
5.3. Kontrola osoblja - broj, stručnost i ovlaštenja	34
5.3.1. Zahtjevi životopisa, kvalifikacije i iskustva	34
5.3.2. Postupci provjere životopisa.....	34
5.3.3. Zahtjevi za obukom	35
5.3.4. Zahtjevi za ponovnom obukom i njezinom učestalosti	35
5.3.5. Rotiranje posla – učestalost i redosljed	35
5.3.6. Sankcije za neautorizirane akcije	35
5.3.7. Zahtjevi za osobe pod ugovorom.....	35
5.3.8. Dokumentacija koja se isporučuje osoblju	35
6. KONTROLE TEHNIČKE SIGURNOSTI RADA SUSTAVA CERTIFICIRANJA...37	
6.1. Izrada certifikata..... 37	
6.1.1. Generiranje para ključeva.....	37
6.1.2. Dostavljanje privatnog ključa.....	37
6.1.3. Dostavljanje javnog ključa izdavatelju certifikata.....	37
6.1.4. Dostava NCARH certifikata i javnog ključa glavnom CA CSP-u	38
6.1.5. Duljine ključeva.....	38
6.1.6. Generiranje parametara javnog ključa	38
6.1.7. Provjera kvalitete parametara	38
6.1.8. Generiranje CA i RA ključeva.....	38
6.1.9. Svrha uporabe ključa	39
6.2. Zaštita podataka za izradu vlastitog elektroničkog potpisa	39
6.2.1. Standardi za kriptomodule.....	39
6.2.2. Kontrola privatnog ključa od više osoba (multi person control)	39
6.2.3. Čuvanje privatnog ključa.....	40
6.2.4. Backup privatnog ključa.....	40
6.2.5. Arhiviranje privatnog ključa.....	40
6.2.6. Upis privatnog ključa u kriptomodul.....	40
6.2.7. Metoda aktiviranja privatnog ključa.....	40
6.2.8. Metoda deaktiviranja privatnog ključa	40
6.2.9. Metoda uništenja privatnog ključa	40

6.3. Upravljanje podacima za izradu elektroničkog potpisa	40
6.3.1. Arhiviranje javnog ključa	40
6.3.2. Period valjanosti	41
6.4. Podaci za pristup privatnom ključu (aktivacijski podaci).....	41
6.4.1. Generiranje i instaliranje aktivacijskih podataka.....	41
6.4.2. Zaštita aktivacijskih podataka	41
6.4.3. Drugi vidovi aktivacije	41
6.5. Kontrole sigurnosti računalnog sustava.....	41
6.5.1. Posebni tehnički zahtjevi sigurnosti računalnog sustava.....	41
6.5.2. Razina sigurnosti računalnog sustava.....	42
6.6. Kontrola sigurnosti radnog vijeka sustava	42
6.6.1. Kontrole razvoja sustava	42
6.6.2. Kontrole upravljanja sigurnošću.....	43
6.7. Kontrola sigurnosti mrežnog sustava	43
6.8. Kontrola sigurnosti kriptografskih modula.....	43
7. SADRŽAJ CERTIFIKATA I LISTE OPOZVANIH CERTIFIKATA.....	45
7.1. Sadržaj certifikata.....	45
7.1.1. Broj verzije i osnovna polja.....	45
7.1.2. Ekstenzije certifikata	46
7.1.3. OID za algoritme	46
7.1.4. Forme imena.....	46
7.1.5. Imenska ograničenja.....	46
7.1.6. OID za CP.....	46
7.2. Sadržaj liste opozvanih certifikata (ARL/CRL).....	46
7.2.1. Broj verzije	46
7.2.2. ARL i CRL ulazne ekstenzije.....	46
8. POSTUPCI S DOKUMENTACIJOM.....	47
8.1. Postupci pri promjeni sadržaja dokumentacije.....	47
8.1.1. Dijelovi koji se mogu mijenjati bez obavijesti	47
8.1.2. Dijelovi koji zahtijevaju obavijest.....	47
8.1.3. Period za primjedbe i provedba.....	47
8.2. Objavljivanje dokumentacije	47
8.2.1. Kopija CP-a	47
8.2.2. Obavijest o promjenama.....	47
8.3. Postupci prihvaćanja/odobravanja CPS-a	48

1. UVODNE OZNAKE I TEMELJNI PODACI

Opća pravila certificiranja (u daljnjem tekstu CP) definiraju četiri politike certificiranja kojima se koristi NCARH radi omogućavanja interoperabilnosti između NCARH i PKI domena drugih davatelja usluga certificiranja (dalje u tekstu CSP - Certification Service Provider).

Četiri politike predstavljaju četiri različite razine sigurnosti (standardnu, srednju i visoku) za digitalne certifikate, plus jedna razina sigurnosti koja se koristi samo u testnim uvjetima. Riječ "sigurnost" korištena u ovom CP-u govori o razini pouzdanja pouzdajuće strane u sigurnost veze između javnog ključa i subjekta čije je ime navedeno u certifikatu. Pouzdajuća strana također treba biti sigurna da subjekt čije je ime navedeno u certifikatu kontrolira uporabu privatnog ključa koji korespondira javnom ključu u certifikatu.

NCARH podržava interoperabilnost između PKI domena različitih CSP izdavanjem certifikata samo onim CA-ovima koji su od pojedinog CSP naznačeni kao glavni CA-ovi (Principal CA). NCARH certifikati izdani glavnim CA-ovima djeluju kao provoditelji povjerenja.

CA CSP-a neće primjeniti OID CP NCARH u certifikatima koje on izdaje, osim u Policy Mappings ekstenziji gdje se uspostavlja ekvivalentnost između OID-a CP NCARH i OID-a CP-a CA CSP.

U Policy Mappings ekstenziji, CSP može koristiti OID samo nakon što PMA HR PKI odredi Policy Mapping Determination i odobri korištenje OID-a.

1.1. Opis usluga

1.1.1. Pregled

1.1.1.1. Opća pravila certificiranja (CP)

Certifikati NCARH imaju registrirani OID za CP, koji mogu koristiti pouzdajuće strane radi odluke hoće li se pouzdati u certifikat. Svaki će certifikat koji izdaje NCARH u Policy Mappings ekstenziji naznačiti koja je mapiranja PMA HR PKI odredio između CP-a NCARH i CP-a određenog CSP.

1.1.1.2. Veza između CP-a i CPS-a NCARH

CP NCARH navodi koje se razine sigurnosti mogu primjeniti u certifikatima koje izdaje NCARH. CPS NCARH navodi kako se postiže ta sigurnost.

1.1.1.3. Veza između CP-a NCARH i CP-a CSP

PMA HR PKI mapira razine sigurnosti certifikata koje izdaje NCARH s razinama sigurnosti certifikata koje izdaje CA nekog CSP. Policy Mappings informacija se nalazi na certifikatima koje izdaje NCARH.

NCARH

Opća pravila certificiranja (CP)

1.1.1.4. Svrha

NCARH je uspostavljen radi omogućavanja povjerljivog elektroničkog poslovanja na nacionalnoj razini. Pojam "CSP" korišten u ovom CP-u (PKI CSP ili CA CSP) odnosi se na PKI neke organizacije ili PKI koji obavlja neki komercijalni servis.

1.2. Identifikacijski podaci i OID oznaka

Postoji četiri razine sigurnosti u ovom CP-u, one će biti definirane u narednim poglavljima. Svaka razina sigurnosti ima OID, koji će biti naveden u certifikatima koje izdaje NCARH.

Od BSI (British Standards Institution) je dodjeljen OID za Ministarstvo gospodarstva, rada i poduzetništva u obliku:

1.3.124.1105

- 1 - ISO
- 3 - Identifikacija organizacije
- 124 - ICD (International Code Designator)
- 1105 - Ministarstvo gospodarstva, rada i poduzetništva

1.2.1. OID za NCARH CP

Ministarstvo je odredilo OID za NCARH CP v.1.0. u obliku:

1.3.124.1105.5.1

- 5 - PKI objekti
- 1 - NCARH CP v.1.0

1.3. Davatelji usluga, korisnici i područje primjene usluga

1.3.1. PMA HR PKI

PMA je odgovoran za:

- NCARH - Opća pravila o certificiranju (CP)
- NCARH - Izjava o postupcima izdavanja certifikata (Certification Practice Statement – CPS)
- prihvaćanje molbi od CSP koji žele interoperirati sa NCARH
- određivanje mapiranja između certifikata koje izdaje CSP koji je predao molbu i razina sigurnosti koje su postavljene u CP NCARH-u (što uključuje objektivnu i subjektivnu procjenu sadržaja CP-a) CSP i druge činjenice koje se smatraju relevantnim za PMA HR PKI, i
- osiguranje kontinuirane usklađenosti tog CSP sa zahtjevima koji su uvjet za neprekinutu interoperabilnosti sa NCARH.

PMA HR PKI sklopiti će ugovor sa CSP navodeći odgovornosti i obveze obje strane i mapiranja između razina sigurnosti certifikata koje se nalaze u ovom CP-u i onima iz CP-a CSP.

1.3.2. NCARH

NCARH je dobio odobrenje od PMA HR PKI za kreiranje, potpisivanje i izdavanje certifikata i javnog ključa glavnim CA-ovima. NCARH je odgovoran za sve aspekte izdavanja i upravljanja certifikatima uključujući:

- kontrolu registracijskog procesa
- proces identifikacije i autentifikacije
- proces izrade certifikata
- objavu certifikata
- opoziv certifikata
- obnovu ključeva
- osiguranje da se svi aspekti NCARH servisa i NCARH operacije i infrastruktura koja se odnosi na certifikate izdane prema ovom CP-u, provode u skladu s uvjetima i jamstvima iz ovog CP-a.

1.3.3. Operativna organizacija NCARH (OA NCARH)

OA NCARH je organizacija koja po ugovoru s Ministarstvom gospodarstva, rada i poduzetništva provodi operativne poslove izdavanja NCARH certifikata kada dobije nalog od PMA HR PKI, bilježenja tih certifikata i ARL (Authority Revocation Lists) u NCARH repozitorij, i osiguranja kontinuirane dostupnosti repozitorija svim korisnicima.

1.3.3.1. Voditelj OA NCARH

Voditelj OA NCARH je osoba čija je glavna dužnost nadgledanje propisanog rada NCARH uključujući NCARH repozitorij.

1.3.3.2. Osoblje OA NCARH

To su osobe u OA koje vrše operativne CA poslove za NCARH i njegov repozitorij uključujući provođenje PMA HR PKI naloga o izdavanju NCARH certifikata glavnim CA-ovima, ili poduzimanje drugih akcija radi uspostavljanja interoperabilnosti.

1.3.4. Glavni (Principal) CA CSP

Glavni CA je CA u okviru neke PKI domene koji je određen za direktno interoperiranje sa NCARH (npr. razmjenom cross-certifikata), i koji izdaje ili certifikate za krajnje korisnike ili cross-certifikate.

CSP može zahtijevati da NCARH interoperira s više nego jednim CA u okviru CSP, tj CSP može imati više od jednog glavnog CA. Također, ovaj CP se može odnositi na CA-ove koji su subordinirani glavnom CA-u. Ovaj izraz se proširuje na bilo koji CA CSP kojem je glavni CA izdao certifikat, ili bilo koji CA koji je subordiniran glavnom CA-u.

NCARH

Opća pravila certificiranja (CP)

1.3.4.1. Registracijski ured

RA sakuplja i verificira sve informacije o identitetu potpisnika koje su potrebne za izdavanje certifikata. OA NCARH ima funkciju RA za NCARH.

1.3.5. Krajnji korisnici

1.3.5.1. Subjekti

Subjekt je krajnji korisnik čije se ime pojavljuje kao subjekt certifikata, koji potvrđuje da koristi svoj ključ i certifikat u skladu sa CP-om. NCARH potpisnici su jedino OA NCARH osoblje.

1.3.5.2. Pouzdajuće strane

Pouzdajuća je strana krajnji korisnik koji se pouzda u valjanost veze između imena potpisnika i njegova javnog ključa. Pouzdajuća je strana odgovorna za odluku da li i kako ispitati valjanost certifikata. Pouzdajuća strana koristi certifikat radi verificiranja integriteta digitalno potpisane poruke, identificiranja pošiljatelja poruke, ili radi uspostave povjerljive komunikacije s imateljem certifikata. Pouzdajuća strana može koristiti informacije iz certifikata (primjerice, CP identifiers) za određivanje prikladnosti certifikata za određenu uporabu.

1.3.6. Područje primjene

Osjetljivost informacija koje se obrađuju i štite uporabom certifikata koje izdaje NCARH ili CA CSP znatno se razlikuje. CSP moraju procijeniti okolinu, prijetnje i ranjivosti koje se na nju odnose i odrediti razinu rizika koju su voljni prihvatiti s obzirom na osjetljivost i važnost informacija. Tu procjenu provodi svaki korisnik za svaku aplikaciju i ona nije kontrolirana ovim CP-om. Ovaj CP specificira sigurnosne zahtjeve za tri razine sigurnosti: standardnu, srednju i visoku. NCARH će raditi na visokoj razini sigurnosti.

Ovaj CP također definira testnu razinu sigurnosti, koju primjenjuje testni NCARH i CA-ovi kada provode test interoperabilnosti. Produkcijski NCARH ne izdaje certifikate s testnom razinom sigurnosti.

Razine sigurnosti certifikata koje su sadržane u ovom CP-u navedene su u sljedećoj tablici, kao i kratki opis primjene u aplikacijama koje odgovaraju svakoj razini.

Razina sigurnosti	Područje primjene
Test	Ova se razina koristi za testiranje interoperabilnosti između NCARH i glavnih CA-ova. koristi se isključivo u testne svrhe i ne prenosi povjerljive informacije.
Standardna	Ova razina omogućuje standardnu razinu sigurnosti prikladnu u okolinama u kojima postoje rizici i posljedice prouzrokovane kompromitiranjem podataka, ali nemaju veće značenje. To može biti pristup tajnim podacima gdje vjerojatnost zlonamjernog pristupa nije velika. U ovoj sigurnosnoj razini se podrazumjeva da je vjerojatnost da korisnici budu zlonamjerni mala.

Razina sigurnosti	Područje primjene
Srednja	Ova je razina prikladna za okoline u kojima su rizici i posljedice kompromitiranja podataka umjereni. Može se koristiti u transakcijama koje imaju znatnu novčanu vrijednost ili rizik od krivotvorenja, ili u onim koje imaju pristup tajnim informacijama u kojima je vjerojatnost zlonamjernog pristupa znatna.
Visoka	Ova je razina prikladna za uporabu u transakcijama u kojima je ugroženost podataka visoka, ili su posljedice propusta u sustavu zaštite velike. To su transakcije vrlo visoke vrijednosti ili s velikim rizikom od krivotvorenja.

1.3.6.1. Faktori koji određuju korištenje certifikata

Pouzdajuća strana mora najprije odrediti razinu sigurnosti koja se zahtijeva za aplikaciju i nakon toga odabrati certifikat koji zadovoljava potrebe aplikacije. To će biti određeno procjenom različitih faktora rizika uključujući vrijednost informacije, ugroženost okoline, i postojeću zaštitu informacijskog sustava. Ovu odluku donosi pouzdajuća strana, bez utjecaja PMA HR PKI ili OA NCARH. Pouzdajuća strana može koristiti gore navedene osnovne upute u donošenju odluke.

1.4. Adresni podaci

PMA HR PKI je odgovoran za sve što se odnosi na ovaj CP.

Pitanja koja se odnose na ovaj CP mogu se uputiti PMA HR PKI.

Osobe za kontaktiranje

1. Ema Culi
2. Leopold Eke
3. Vesna Petković

Osobe koje određuju primjerenost CPS-a ovom CP-u

1. Ema Culi
2. Leopold Eke
3. Vesna Petković

PMA HR PKI će odobriti CP NCARH. CSP su odgovorni da ustanove je li CPS određenog CA CSP u skladu sa CP-om toga CA, i posebno pridržava li se pravilno Policy Mappings koje je odobrio PMA HR PKI, između CP-a NCARH i CP-a glavnog CA CSP. Od CSP će se zahtijevati da potvrde tu usklađenost periodički, prema zahtjevima PMA HR PKI. Nadalje, PMA HR PKI rezervira pravo revizije usklađenosti CSP kao što je navedeno u ovom CP-u i u ugovoru između PMA HR PKI i CSP.

2. OPĆE ODREDBE

2.1. Obveze davatelja usluga, subjekata i korisnika

Obveze koje su niže opisane odnose se na NCARH (uključivo OA NCARH), i na glavne ili druge CA-ove, koji ili interoperiraju sa NCARH ili su u lancu povjerenja prema glavnom CA koji interoperira sa NCARH. Obveze CA CSP su usredotočene na one koje se odnose na interoperabilnost sa NCARH.

2.1.1. Obveze CA

CA CSP koji izdaje certifikate mapirane od PMA HR PKI sa NCARH politikama definiranim u ovom CP-u, za koje je PMA HR PKI odobrio izdavanje NCARH certifikata koji sadrži ta mapiranja s glavnim CA CSP, zadovoljavat će uvjete koji su navedeni u ugovoru, jednako tako kao što će i osiguravat zadovoljenje zahtjeva CP CSP.

2.1.2. Obveze RA

RA CSP koji provodi registracijske funkcije u ime CA CSP, čije su obveze opisane u 2.1.1 također će udovoljavati zahtjevima koji su postavljeni u ugovoru, jednako tako kao što će i osiguravati zadovoljenje zahtjeva CP CSP.

2.1.3. Obveze Subjekata

Od Subjekata koji dobivaju certifikate od CA CSP ili NCARH zahtijevat će se da zadovoljavaju zahtjeve ugovora, kao i zahtjeve iz CP-a CSP, odnosno CP-a NCARH

2.1.4. Obveze pouzdajuće strane

CP NCARH ne specificira koje bi korake trebala poduzeti pouzdajuća strana da bi odlučila treba li se pouzdati u certifikat. Pouzdajuća strana odlučuje, prema vlastitoj politici, koje korake treba poduzeti. NCARH samo nudi alate koji su potrebni za kreiranje i validaciju staze povjerenja i mapiranja CP-a.

2.1.5. Obveze repozitorija

OA NCARH može koristiti različite mehanizme za bilježenje informacija u repozitorij. Ti mehanizmi će kao minimum sadržati sljedeće:

- X.500 Directory Server System koji je dostupan preko LDAP-a
- Mogućnost pristupa informacijama
- Mehanizme kontrole pristupa radi zaštite informacija u repozitoriju

NCARH

Opća pravila certificiranja (CP)

2.2. Odgovornost

Certifikati se izdaju i opozivaju po odluci PMA HR PKI. PMA HR PKI pregledava CP CSP-a u svrhu odluke je li interoperabilnost moguća, i u kojem se opsegu CP CSP-a mapira sa CP-om NCARH.

2.3. Financijska odgovornost

Ovaj CP ne ograničava korištenje certifikata koje izdaje NCARH ili CA-ovi CSP. Korisnici koji djeluju kao pouzdajuće strane, odlučuju koje će financijske limite postaviti za certifikate pri provođenju transakcija. Tako, neki korisnik može prihvatiti certifikat standardne ili srednje razine sigurnosti za transakcije financijske vrijednosti za koje će drugi korisnik zahtijevati certifikat visoke razine sigurnosti. To je u potpunosti predmet odluke CSP i pouzdajuće strane i ovisi o nekoliko faktora (npr. vjerojatnost krivotvorenja, proceduralne kontrole, specifičnost politike CSP-a ili ograničenja postavljena zakonom i propisima).

2.3.1. Odšteta od pouzdajuće strane ili potpisnika

Nema uvjeta.

2.3.2. Administrativni procesi

Administrativne će procese koji se odnose na ovaj CP odrediti OA NCARH, u skladu s ugovorom sa PMA HR PKI za operativno vođenje NCARH.

2.4. Usklađenost sa zakonom

2.4.1. Odjeljenost odredbi

Ako se donese odluka da je neka točka ovog CP-a netočna, druge točke će ostati na snazi dok se CP ne ispravi. Proces ispravljanja CP-a opisana je u točki 8.1.

2.4.2. Procedure za rješavanje nesuglasica

PMA HR PKI će nesuglasice među stranama u HR PKI rješavat onda kada nastanu problemi koji su rezultat uporabe certifikata koje je izdao NCARH.

2.5. Objava i repozitorij certifikata

2.5.1.1. Objava informacija o CA

OA NCARH će objaviti informacije koje se odnose na NCARH i koje su neophodne za održavanje uporabe i operativnog rada NCARH. CSP će publicirati obavijesti o njihovim CA-ovima, kako je navedeno u ugovoru sa NCARH.

2.5.2. Učestalost objavljivanja

Certifikati NCARH i CSP se objavljuju kako je specificirano u ovom CP-u (za certifikate CSP) i u CP-u CSP. Statusne informacije o certifikatima se objavljuju kako je specificirano u ovom CP-u (za certifikate CSP) i u CP-u CSP.

2.5.3. Kontrole pristupa

OA NCARH će štititi informacije koje se nalaze u repozitoriju, a nisu namjenjene za javno objavljivanje ili izmjenu. Javni ključevi i informacije o statusu certifikata iz repozitorija NCARH bit će javno dostupni preko Interneta. Pristup će se informacijama iz repozitorija CA CSP odrediti u skladu s propisima i zakonima koji se odnose na taj CSP.

2.5.4. Repozitoriji

CSP-ovi koji interoperiraju sa NCARH-om moraju uspostaviti interoperabilnost svojih imenika s repozitorijem NCARH-a, i njihovi imenici moraju sadržati informacije neophodne za podržavana interoperiranja PKI domena CSP koji koriste NCARH za tu svrhu.

2.6. Provjera usklađenosti

CA-ovi CSP moraju imati mehanizme provjere usklađenosti radi osiguranja da zahtjevi njihova CP, CPS i uvjeti ugovora budu primjenjeni i provedeni. OA NCARH će imati sličan mehanizam na djelu, pokrivajući zahtjeve ovog CP-a, CPS-a i ugovora potpisanog sa subjektom.

2.6.1. Učestalost

NCARH, glavni CA-ovi CSP i njihovi subordinirani CA-ovi biti će podvrgnuti periodičnoj provjeri usklađenosti barem jednom godišnje za visoku i srednju razinu sigurnosti i barem jedanput u dvije godine za standardnu razinu sigurnosti. Provjera usklađenosti nije potrebna za testnu razinu sigurnosti.

PMA HR PKI ima pravo u bilo koje vrijeme zahtijevati provjeru usklađenosti glavnih CA-ova CSP (i kada je potrebno njihovih subordiniranih CA-ova) koji interoperiraju sa NCARH po ovom CP-u. PMA HR PKI će navesti razloge izvanrednih provjera usklađenosti.

2.6.2. Identitet i kvalifikacije inspektora

Inspektori moraju:

- imati kvalifikacije u skladu s najboljom poslovnom praksom
- kao svoju primarnu odgovornost provoditi provjeru rada CA ili provjeru sigurnosti informatičkog sustava
- biti dobro upoznati s djelatnošću CA

2.6.3. Neutralnost inspektora

Inspektori za provjeru usklađenosti i CA moraju imati definirani odnos za provedbu inspekcije i moraju biti dovoljno organizacijski odvojeni od CA da bi izveli neovisnu/neutralnu procjenu.

NCARH

Opća pravila certificiranja (CP)

2.6.4. Svrha revizije i inspekcije

Inspektori moraju postupiti u skladu s odredbama Zakona [1] i pravilnika [2, 3, 4, 5], uputama PMA HR PKI, odnosno provjeravati postupa li CA prema tehničkim i proceduralnim uputama PMA HR PKI, i prema pravilnicima o osoblju koji su sastavni dio ovog CP-a.

2.6.5. Poduzimanje akcija kao rezultat inspekcije

PMA HR PKI može zaključiti da NCARH ili CA CSP ne ispunjava obveze koje su navedene u ovom CP-u ili u odgovarajućem ugovoru. Nakon donošenja takve odluke PMA HR PKI može suspendirati rad NCARH-a ili može narediti OA NCARH-u da prekine interoperiranje glavnog CA CSP-a (primjerice, opozivom certifikata koji je NCARH izdao glavnom CA-u), ili može odrediti druge korektivne akcije koje omogućuju nastavak interoperiranja. Kada inspekcija ustanovi neslaganje u radu NCARH-a ili CA CSP-a i zahtjeva ovog CP-a, CP-a CSP-a, ugovora ili CPS-a koji se primjenjuje poduzimaju se sljedeće akcije:

- inspektor će evidentirati neslaganja
- inspektor će obavjestiti CSP o neslaganjima. CSP će obavjestiti promptno PMA HR PKI.
- strana koja je odgovorna za ispravak neslaganja će odlučiti o akcijama koje je potrebno poduzeti u skladu sa zahtjevima ovog CP-a i ugovora.

U ovisnosti o prirodi i težini neslaganja i vremenu potrebnom za ispravljanje, PMA HR PKI može odlučiti privremeno zaustaviti rad NCARH-a, da opozove certifikat koji je izdao NCARH ili poduzeti druge akcije koje smatra prikladnim.

2.7. Povjerljivost i tajnost (poslovanja i podataka)

Informacije NCARH-a koje ne zahtijevaju zaštitu bit će javno objavljene. Pristup PMA HR PKI informacijama CSP-u bit će naznačen u ugovoru s tim korisnikom. Javni pristup informacijama CSP-a odredit će sam CSP.

2.8. Prava intelektualnog vlasništva

Ministarstvo gospodarstva, rada i poduzetništva zadržava isključivo pravo na informacije i produkte koji nastaju u skladu s ovim CP-om

3. IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

3.1. Registracija Subjekta

NCARH (i kada je potrebno CA-ovi CSP) moći će generirati i potpisivati certifikate koji sadrže X.500 DN. Certifikati koji se izdaju CA-ovima CSP koristit će DN i imati razinu sigurnosti jednaku ili veću od najviše razine sigurnosti certifikata koje CA izdaje Subjektima ili drugim CA-ovima.

3.1.1. Potreba da ime ima značenje

NCARH će uporebljavati DN u certifikatima koje izdaje.

3.1.2. Pravila za interpretiranje različitih formi imena

Pravila će za interpretiranje formi imena bit sadržana u profilu certifikata koji treba primjeniti. Ta pravila će ustanovit PMA HR PKI. Pravila za interpretiranje formi imena CA CSP bit će navedena u CP-u CSP-a.

3.1.2.1. Jedinstvenost imena

PMA HR PKI je odgovoran za osiguranje jedinstvenosti imena u certifikatima koje izdaje NCARH.

3.1.2.2. Procedura za rješavanje sporova o imenu

PMA HR PKI će rješavat sporove o imenu koji su mu upućeni, a koji mogu utjecati na interoperabilnost preko NCARH.

3.1.3. Metode dokazivanja posjedovanja privatnog ključa

Od tražitelja se zahtijeva, da u zahtjevu za certifikat dokaže posjedovanje privatnog ključa koji odgovara javnom ključu, što se može učiniti potpisivanjem zahtjeva privatnim ključem. CA će omogućiti takav postupak u skladu s odgovarajućim sigurnosnim protokolom primjerice, protokolom opisanim u IETF PKIX Certificate Management Protocol. U slučajevima kada je privatni ključ generiran direktno na kriptomodul, ili na generator ključa koji sigurno šalje ključ na kriptomodul, tada se smatra da Subjekt posjeduje privatni ključ u vrijeme generiranja ili prijenosa. Ako Subjekt ne posjeduje kriptomodul u vrijeme generiranja ključa, tada će se kriptomodul poslati odmah Subjektu sigurnim transportom.

3.1.4. Autentifikacija identiteta organizacije

Zahtjevi organizacije za certifikat mogu biti poslani elektroničkim putem i moraju sadržavati naziv i adresu organizacije. Minimalni I&A koji su potrebni po ovom CP-u zahtijevaju sljedeću potvrdu:

- da organizacija pravno postoji i posluje na adresi koja se nalazi u zahtjevu za certifikat,
- da su informacije koje se nalaze u zahtjevu točne

Kada se I&A informacije prikupljaju u RA, RA će provesti I&A u skladu s uspostavljenim postupcima identificiranja organizacije, što primjerice, može biti upit u razne registre.

3.1.5. Certifikati za pripadajuće osobe

Certifikati za pripadajuće osobe (Poslovni certifikati) izdavat će se osobama ovlaštenim za potpisivanje u skladu s točkama 3.1.6. i 3.1.7. CP-a.

3.1.6. Identifikacija i autentifikacija osoba

Izdavanje certifikata temelji se na postupku I&A koje izvode CA i RA. Osoba koja se identificira mora dostaviti potpisani dokument (u pisanom ili digitalnom obliku) kojim se može pravilno odrediti identitet osobe. Broj i vrste identifikacijskih dokumenata (ID), način procesiranja dokumentacije i autentifikacijski zahtjevi pri izdavanju certifikata ovisit će o razini sigurnosti certifikata.

CA može u CPS-u, ili u drugoj dokumentaciji opisati način prijelaza korisnika certifikata na certifikat višeg stupnja, uz uvjet da te procedure nisu u suprotnosti s odredbama ovog odjeljka CP-a.

3.1.6.1. Pribavljive vrste identifikacijskih dokumenata

Sve osobe koje traže certifikat moraju predložiti zadovoljavajući dokaz o identitetu. Po ovom CP-u prihvatljivi identifikacijski dokumenti su:

- osobna iskaznica,
- putovnica ili
- europska iskaznica (europska identifikacijska kartica).

3.1.6.2. Provođenje identifikacije na licu mjesta

Identifikacija na licu mjesta može se provesti u nazočnosti:

- CA ili njegovog povjerljivog agenta ili
- RA ili njegovog povjerljivog agenta (LRA službenik) ili
- Javnog bilježnika.

Sve informacije koje prilaže tražitelj za identifikaciju na licu mjesta, moraju biti pregledane da se ustanovi konzistentnost s informacijama koje se nalaze u zahtjevu za izdavanje certifikata. Tako ustanovljen identitet bit će potpisan u pismenom ili digitalnom obliku i poslan CA-u s naznakom da je tražitelj pravilno identificiran.

3.1.6.3. Verificiranje i validacija informacija

Verificiranje i validacija informacija potrebnih za registraciju sastojat će se u usporedbi tih informacija i povjerljivih informacija te procesa potvrde drugim kanalom (Out of-band). Usporedba se može izvršiti i elektronički ili na druge povjerljive načine (primjerice, vizualni

pregled po primitku podataka). Informacije za registraciju, koje je poslao tražitelj, moraju sadržati najmanje ime, adresu, telefonski broj, e-mail adresu, JMBG ili serijski broj putovnice ili europske iskaznice. Povjerljive informacije koje se upotrebljavaju za usporedbu mogu biti podatkovna osnovica koju održava CA ili RA, i informacije koje daje treća strana (javni i drugi registri).

3.1.6.4. Utvrđivanje identiteta Subjekata s kojima već postoji poslovni odnos

Ako je RA već ustanovio identitet osobe, RA i osoba već imaju poslovne odnose, RA se može pouzdati u prijašnju identifikaciju da bi zadovoljio I&A zahtjeve ovog CP-a i procesirao zahtjeve za izdavanje certifikata. Također, RA može izvršiti potvrdu drugim kanalom u odnosu na takvu osobu:

- osobnom isporukom s obzirom na RA-ovo poznavanje osobe (primjerice, kao zaposlenika) ili razumne identifikacije u vrijeme isporuke ili
- uporabom enkriptiranih poruka između RA i osobe

RA će osigurati prikupljanje, kontrolu i čuvanje informacija koje se odnose na identitet osobe.

3.1.6.5. Autentifikacija

CA mora osigurati da se informacije o identitetu tražitelja i javni ključ na pravi način povežu. Ovo povezivanje se može uspostaviti uporabom SS (primjerice, zaporka, kod ili broj) razmijenjenim između RA, tražitelja certifikata i CA. Ako se upotrebljava SS moraju biti poduzete mjere koje osiguravaju da su tražitelj certifikata i CA ili RA jedini primatelji SS. Ako se upotrebljava PIN, RA ga ne bi trebao dati CA-u. Ostali mehanizmi za postizanje ovog pridruživanja mogu biti uporaba PKI podatkovne osnovice, sustav korisničkih računa, ili slični autentifikacijski mehanizmi.

3.1.7. Ovlaštene osobe

Ovlaštene osobe mogu se autentificirati provodeći procedure naznačene u točkama 3.1.4 i 3.1.6. CP-a i potvrdom poslovnog subjekta da je osoba povezana sa certifikatom. Verificiranje identiteta osoba za najviši stupanj certifikata temeljit će se na identifikacijskim dokumentima i zahtjevima za autentifikaciju koji su navedeni u točki 3.1.6. CP-a.

3.2. Plansko obnavljanje certifikata

3.2.1. Obnavljanje ključeva

Obnavljanje ključeva je važno zbog sprječavanja krivotvorenja.

Novi certifikati moraju biti izdani glavnim CA-ovima od NCARH-a kada NCARH obnavlja ključeve i obrnuto. Nakon obnove ključeva bilo koje od ovih komponenti, NCARH će identificirati i autentificirati glavni CA na sljedeći način:

- a. provodeći inicijalni registracijski proces definiran u 3.1. ili
- b. ako je prošlo manje od tri godine da je glavni CA identificiran kako se zahtijeva u točki 3.1., uporabom trenutno važećeg certifikata kojeg je NCARH izdao glavnom CA-u.

Subjekti CA CSP će se identificirati za potrebe obnove certifikata na način naveden u sljedećoj tablici:

Razina sigurnosti	Zahtjevi za identitetom za plansko obnavljanje potpisnog i enkripcijskog ključa
Test	Opisan u ugovoru sa CSP
Standardna	Identitet se može ustanoviti uporabom trenutno važećeg potpisnog ključa. Najmanje svakih 15 godina od vremena zadnje inicijalne registracije provest će se inicijalna registracija.
Srednja	Identitet se može ustanoviti uporabom trenutno važećeg potpisnog ključa. Najmanje svakih 9 godina od vremena zadnje inicijalne registracije provest će se inicijalna registracija.
Visoka	Identitet se može ustanoviti uporabom trenutno važećeg potpisnog ključa. Najmanje svake 3 godine od vremena zadnje inicijalne registracije provest će se inicijalna registracija.

3.2.2. Obnova certifikata

Obnova certifikata znači kreiranje novog certifikata sa istim imenom, javnim ključem i autorizacijama, ali sa novim periodom valjanosti i novim serijskim brojem. Certifikat se može obnoviti ako paru ključeva nije istekla valjanost, ako privatni ključ nije kompromitiran te ako su i ime i informacije o subjektu ispravni. Tako CA može izabrati uvođenje trogodišnjeg perioda za obnovu ključeva, s inicijalnim izdavanjem i dvije godišnje obnove certifikata prije potrebe izdavanja novog para ključeva. Stari certifikat ne treba biti opozvan, ali ne smije se za njega tražiti obnova ili promjena informacija u certifikatu.

3.2.3. Izmjene informacija u certifikatu

Izmjena informacija u certifikatu znači kreiranje novog certifikata, koji:

- ima isti ili različiti javni ključ,
- ima novi serijski broj,
- razlikuje se od starog certifikata u jednom polju ili u više njih.

Primjerice, CA može izabrati izmjenu informacija u certifikatu Subjekta koji je u postupku dobivanja autorizacije. Certifikat može ali ne mora biti opozvan, ali ne smije biti više obnovljen ili izmijenjen.

3.3. Obnavljanje nakon opoziva ili isteka certifikata

Certifikat koji je istekao ili je opozvan ne može biti predmet zahtjeva za izdavanje novog para ključeva, obnovu ili izmjenu. Tražitelj će certifikata za dobivanje novog certifikata biti podvrgnut svim procedurama inicijalne registracije.

3.4. Zahtjev za opoziv

Subjekt može u svakom trenutku, iz bilo kojeg razloga, zatražiti opoziv svog certifikata. CA u trenutku primitka takvog zahtjeva za opoziv mora provesti mehanizme autentifikacije, kako bi se utvrdilo da se radi o pravom Subjektu. Ako je zahtjev poslan elektronički, identitet će se utvrditi elektroničkim potpisom.

4. OSNOVNI ZAHTJEVI U RADU SA CERTIFIKATIMA

4.1. Zaprimanje zahtjeva za izdavanje certifikata

Ova točka se primjenjuje na CSP koji traže NCARH certifikate za svoje glavne CA-ove. PMA HR PKI će ustanoviti procedure koje će CSP koristiti pri predaji zahtjeva za izdavanje certifikata.

Glavni CA CSP će imati DN prema X.509 i ono će biti upisano u polje **subject name** certifikata. Ime u certifikatu će biti službeno ime CSP povezanog sa CA-om koji se cross - certificira.

CSP može poslati zahtjev PMA HR PKI za cross-certificiranje za više glavnih CA-ova tog CSP. U zahtjevu će biti predložena mapiranja između razine sigurnosti CP-a CSP i CP-a NCARH.

PMA HR PKI će procijeniti zahtjev u skladu s procedurama koje će razviti i objaviti, te će donijeti odluku o izdavanju certifikata i koja mapiranja će navesti u certifikatima. PMA HR PKI i CSP će sklopiti ugovor i PMA HR PKI će dati nalog OA NCARH-u za izdavanje certifikata. Nakon izdavanja, svaki će certifikat koji izdaje NCARH, a prije slanja certifikata CSP-u biti ručno provjeren da bi se osigurala ispravna popunjenost svakog polja i ekstenzije.

4.1.1. Dostava javnog ključa za izdavanje certifikata

Javni ključevi moraju biti dostavljeni radi izdavanja certifikata na način koji potvrđuje vezu CSP i privatnog ključa. Za sve razine sigurnosti ovo se povezivanje može postići uporabom kriptografije. Za srednju i standardnu razinu sigurnosti povezivanje se može postići uporabom ne-kriptografskih fizičkih sredstava. To može biti disketa poslana preporučenom poštom ili dostavljačem, ili dostava hardverskog ili softverskog kriptografskog modula izdavatelju certifikata za lokalno generiranje ključeva u trenutku izdavanja certifikata.

Ako se par ključeva generira u NCARH ili CA CSP u ime subjekta, NCARH ili CA CSP će implementirati sigurne mehanizme osiguranja da kriptomodul na kojem se nalazi par ključeva bude sigurno poslan subjektu. NCARH ili CA CSP će također primijeniti procedure koje osiguravaju da kriptomodul ne može biti aktiviran od neautorizirane osobe.

4.2. Izdavanje certifikata

Nakon procesa primitka zahtjeva za izdavanje certifikata i provedenih svih procesa provjere i odobrenja, CA će:

- izdati zahtjevani certifikat.
- obavijestiti tražitelja o izdavanju,
- učiniti certifikat dostupnim tražitelju radi postupka prihvaćanja

Procedure za izvješćivanje tražitelja za isporuku, ili omogućavanje da certifikat bude dostupan tražitelju moraju biti sigurne i tajne.

4.2.1. Dostava subjektova privatnog ključa subjektu

U najvećem broju slučajeva privatni ključ se generira i ostaje u kriptografskom modulu. Ako vlasnik modula generira ključ, onda nema potrebe za dostavom privatnog ključa. Modul treba biti sigurno dostavljen subjektu. Subjekt treba potvrditi primitak modula. Onaj tko generira privatni potpisujući ključ za subjekta ne smije zadržati kopiju ključa nakon dostave privatnog ključa subjektu. Hardverski kriptomoduli koji sadrže NCARH ili privatni potpisni ključ CA CSP mogu se kopirati u skladu sa sigurnosnim uvjetima definiranim u točki 4.5.1. ovog CP-a.

4.2.2. Dostava i uporaba javnog ključa NCARH

Javni ključ NCARH-a mora biti dostupan za kreiranje i provjeru certifikacijske staze povjerenja. Taj ključ će se pojaviti u cross certifikatu koji izdaje glavni CA CSP NCARH-u. Da bi se izdvojio ključ iz toga certifikata sa sigurnošću da nije bio mijenjan, glavni CA CSP mora osigurati da njegovi korisnici imaju njegov samopotpisani root certifikat koji su dobili na pouzdan način. Pouzadane metode za dostavu CA certifikata su sljedeće:

- CA sprema svoj certifikat na kriptomodule koje dostavlja pouzdajućim stranama pomoću sigurnih metoda dostave,
- preuzimanje certifikata preko web stranica koje su osigurane certifikatom koji je trenutno valjan i koji ima razinu sigurnosti veću ili jednaku kao i certifikat koji se preuzima.

4.3. Prihvaćanje certifikata

Ugovor između PMA HR PKI i CSP navodi obveze obje strane. Kada je certifikat izdan, njegovim prihvaćanjem od CSP započinje interoperabilnost sa NCARH i time započinju njegove obveze navedene u ugovoru i u ovom CP-u.

4.4. Opoziv i suspenzija certifikata

4.4.1. Uvjeti za opoziv certifikata koje je izdao NCARH ili CA CSP

Postoje tri razloga zbog kojih će certifikati koje je izdao NCARH biti opozvani.

- Prvi je razlog kada PMA HR PKI zahtijeva da se opozove certifikat koje je izdao NCARH. To će biti mehanizam opoziva u slučajevima kada PMA HR PKI zaključi da PKI CSP-a nije u skladu sa HR PKI zahtjevima.
- Drugi je razlog kada OA NCARH primi autentificirani zahtjev za opoziv od autorizirane osobe glavnog CA CSP.
- Treći je razlog kada operativno osoblje NCARH zaključi da se dogodio incident koji može imati utjecaj na integritet certifikata koji je izdao NCARH. Pod takvim okolnostima osobe koje mogu odobriti hitan opoziv certifikata su:
 - predsjedavajući PMA HR PKI,
 - druge osobe koje ovlasti predsjedavajući PMA HR PKI.

PMA HR PKI će se sastat čim to bude moguće radi ispitivanja okolnosti pod kojima se dogodio hitan opoziv.

Certifikat koji se opozove objavljuje se u sljedećem izdanju CRL-a. Opozvani će certifikati bit uključeni u sve nove objave informacija o statusu certifikata sve do isteka certifikata.

4.4.1.1. Tko može zahtijevati opoziv certifikata kojeg izdaje NCARH i CA CSP

NCARH certifikat može biti opozvan nakon odluke PMA HR PKI ili nakon autentificiranog zahtjeva autorizirane osobe CSP koja je odgovorna za glavni CA (takvo osoblje će bit navedeno u ugovoru, kao osoblje koje može izdati takve zahtjeve).

Proces za opoziv certifikata subjekta kojeg izdaje CA CSP bit će naveden u CP-u ili CPS-u CSP. Opoziv će uslijediti nakon što je:

- CSP dobio dovoljno dokaza o kompromitiranosti ili gubitku privatnog ključa subjekta.
- Subjekt poslao autentificirani zahtjev za opoziv

4.4.1.2. Procedure za opoziv certifikata

U zahtjevu za opoziv certifikata treba navesti certifikat koji treba biti opozvan, obrazložiti razloge opoziva. Zahtjev mora biti autentificiran (elektronički ili ručno potpisan). Samo PMA HR PKI ili ovlaštena osoba CSP koji je odgovoran za glavni CA mogu zahtijevati od OA NCARH da opozove certifikate koje je izdao NCARH. Glavni CA CSP može uvijek opozvati certifikate koje je izdao NCARH-u.

Autentifikacija zahtjeva za opoziv certifikata je važna radi sprečavanja zlonamjernog opoziva certifikata od neautoriziranih strana. Napose, ako je zahtjev za opoziv bio poslan iz razloga kompromitiranja ključeva ili se sumnja na lažnu uporabu, tada zahtjev subjekta ili RA mora sadržavati te razloge. Ako RA ovo provodi u ime subjekta, koristit će format poruke koji je poznat CA-u, potpisati je i poslati CA-u. Svi zahtjevi će biti autentificirani, za potpisane zahtjeve subjekta ili RA dovoljna je provjera potpisa.

Nakon zaprimanja zahtjeva za opoziv koji se odnosi na NCARH certifikat, OA NCARH će autentificirati zahtjev i obavijestiti PMA HR PKI. PMA HR PKI može po svom nahođenju (sudu) poduzeti mjere koje smatra prikladnim za provjeru potrebe za opoziv. Ako se pokaže da je zahtjev za opoziv valjan, PMA HR PKI će narediti OA NCARH-u da opozove certifikat, stavljajući njegov serijski broj i druge informacije koje ga indentificiraju na ARL/CRL i nakon toga objaviti ARL/CRL u repozitoriju NCARH-a. CA-ovi CSP mogu koristiti OCSP radi distribuiranja statusnih informacija umjesto ARL/CRL.

Ako subjekt koji koristi HW kriptomodul prekida vezu s poslovnim subjektom, on će prije odlaska predati cijeli kriptografski HW koji je koristio. Ako subjekt napušta organizaciju, a HW kriptomoduli nisu vraćeni, tada svi certifikati subjekta povezani s nevraćenim kriptomodulima moraju se hitno opozvati. kriptomodul će biti prebrisan (zeroized) ili uništen odmah nakon predaje i bit će zaštićen od zlonamjerne uporabe u vremenu između predaje i prebrisanja ili uništavanja.

NCARH

Opća pravila certificiranja (CP)

4.4.1.3. Opoziv NCARH certifikata

Opoziv NCARH certifikata može se izvesti generiranjem i objavom u repozitoriju NCARH statusne informacije koja naznačava da je certifikat opozvan, i identificira certifikat koji je opozvan, i razlog za opoziv u skladu s točkom 4.4.3.1. Također, bit će poslana hitna usmena ili elektronička obavijest od OA NCARH svim ovlaštenim osobama CSP-a čiji glavni CA interoperira sa NCARH.

4.4.1.4. Opoziv certifikata koji izdaje CA CSP

Opoziv će stupiti na snagu nakon objave statusnih informacija (koje naznačuju razloge opoziva, koji mogu biti gubitak, kompromitiranost ili prestanak zaposlenja), u vremenskim granicama koje su specificirane u točki 4.4.3. (počevši od vremena kada je zahtjev autentificiran ili je primljeno dovoljno dokaza o kompromitiranju ili o gubitku). Informacija o opozvanom certifikatu će biti u CRL sve do isteka certifikata. Certifikat se može isključiti iz CRL koja se izdaje poslije datuma isteka certifikata.

4.4.2. Suspenzija

NCARH neće koristiti suspenziju. CSP će koristiti suspenziju prema CP-u.

4.4.3. Lista opozvanih certifikata

CA-ovi CSP će izdavati liste opozvanih certifikata CA (ARL) i liste opozvanih certifikata (CRL). Sadržaj ARL i CRL će se provjeravati prije izdavanja da bi se osiguralo da su sve informacije točne.

4.4.3.1. Učestalost izdavanja ARL/CRL

ARL i CRL će se izdavati periodično, čak i kada nema promjena, da bi se osigurala pravodobnost informacija. Informacije o statusu certifikata mogu se izdavati s većom učestalošću od učestalosti niže opisanih. NCARH će osigurati da prethodne informacije o statusu certifikata budu izbrisane iz repozitorija nakon objave najnovije informacije o statusu certifikata.

Informacije o statusu certifikata će se objaviti ne kasnije nego što je predviđeno u niže navedenoj tablici. To će olakšati lokalno spremanje informacija o statusu certifikata za offline ili remote rad. CSP će se uskladiti s repozitorijama u kojima objavljuju informacije o statusu certifikata da bi se umanjio vremenski period između kreiranja i raspoloživosti.

U sljedećoj tablici navedeni su zahtjevi za izdavanje ARL/CRL:

Razina sigurnosti	Učestalost izdavanja ARL/CRL za CA CSP (redovni)	Učestalost izdavanja ARL/CRL za CA CSP (gubitak ili kompromitacija ključa)
Test	Prema ugovoru	Prema ugovoru
Standardna	Prema odluci CSP	U roku od 24 sata po obavijesti
Srednja	Barem jednom dnevno	U roku od 18 sati po obavijesti
Visoka	Barem jednom dnevno	U roku od 6 sati po obavijesti

4.4.3.2. Zahtjevi za provjeru opoziva

Uporaba opozvanih certifikata može imati štetne ili katastrofalne posljedice. Pouzdajuća će strana odrediti koliko će često preuzimat nove podatke o opozvanim certifikatima, uzimajući u obzir rizik, odgovornost i posljedice uporabe certifikata čiji se status opoziva ne može jamčiti.

4.4.4. Raspoloživost online provjere opoziva/statusa

Osim ARL/CRL CA-ovi CSP i SW pouzdajuće strane mogu alternativno podržati online provjeru statusa. SW klijenta koji koristi online provjeru statusa ne treba preuzimati ARL/CRL. PMA HR PKI će odrediti kada i pod kojim će okolnostima OA NCARH omogućit online provjeru statusa NCARH certifikata.

4.5. Postupci provjere sigurnosnih mjera

Revizijski će se logovi generirat za sve događaje koji se odnose na sigurnost NCARH ili CA CSP. Gdje je to moguće revizijski će se logovi automatski prikupljati. Ako to nije moguće, upotrebljavat će se dnevnik, papirnati obrazac ili drugi fizički način bilježenja. Svi revizijski logovi, elektronički i neelektronički, bit će čuvani i dostupni kod revizije usklađenosti. Revizijski će se logovi za svaki događaj koji može biti predmet revizije održavat u skladu s točkom 4.6.2. – Period arhiviranja.

4.5.1. Tipovi događaja koji će se bilježiti

Sve sigurnosne revizijske mogućnosti koje imaju operativni sustavi NCARH ili CA CSP i PKI aplikacije CSP koje zahtijeva ovaj CP bit će u uporabi. Kao rezultat toga, većina će se događaja koji su navedeni u tablici bilježiti automatski. Kao minimum, svaki će revizijski log sadržat sljedeće (napravljen ili elektronički ili ručno za svaki događaj koji treba bilježiti):

- tip događaja,
- datum i vrijeme događaja,
- indikator uspjeha ili neuspjeha pri izvođenju procesa potpisivanja od NCARH ili CA CSP,
- indikator uspjeha ili neuspjeha pri provođenju postupka opoziva certifikata,
- identitet CSP i/ili operatora (od NCARH ili CA CSP) koji je prouzročio događaj,
- poruka za NCARH ili CA CSP iz bilo kojeg izvora koja zahtijeva akciju je događaj koji je predmet revizije. Poruka mora sadržati datum i vrijeme poruke, izvor, odredište i sadržaj.

Događaj koji je predmet revizije	Razina sigurnosti		
	Standardna	Srednja	Visoka
SIGURNOSNA REVIZIJA			

NCARH

Opća pravila certificiranja (CP)

Događaj koji je predmet revizije	Razina sigurnosti		
	Standardna	Srednja	Visoka
Bilo koja promjena parametra revizije, primjerice, učestalost revizije, tip događaja koji je predmet revizije	X	X	X
Pokušaj brisanja ili izmjene revizijskog loga	X	X	X
IDENTIFIKACIJA I AUTENTIFIKACIJA			
Uspješan i neuspješan pokušaj preuzimanja uloge	X	X	X
Izmjena broja maksimalnih pokušaja autentificiranja	X	X	X
Maksimalni broj neuspjelih pokušaja autentificiranja prilikom prijave korisnika	X	X	X
Administrator otključava korisnički račun koji je bio zaključan zbog neuspjelog pokušaja autentifikacije	X	X	X
GENERIRANJE KLJUČEVA			
Kada NCARH ili CA CSP generira ključ.	X	X	X
PUNJENJE I POHRANA PRIVATNOG KLJUČA			
Punjenje privatnih ključeva sastavljenih od komponenti	X	X	X
Svaki pristup privatnom ključu subjekta koji se čuva u NCARH ili CA CSP radi potrebe vraćanja ključa	X	X	X
UPIS, BRISANJE I POHRANA JAVNOG KLJUČA			
Sve promjene kod javnih ključeva, uključujući dodavanja i brisanja	X	X	X
EXPORT JAVNOG KLJUČA			
Export javnih ključeva	X	X	X

Dogadaj koji je predmet revizije	Razina sigurnosti		
	Standardna	Srednja	Visoka
REGISTRACIJA CERTIFIKATA			
Svi zahtjevi za certifikat	X	X	X
OPOZIV CERTIFIKATA			
Svi zahtjevi za opoziv certifikata	X	X	X
ODOBRENJE PROMJENE STATUSA CERTIFIKATA			
Odobrenje ili odbijanje zahtjeva za promjenu statusa certifikata	X	X	X
KONFIGURACIJA NCARH ILI CA CSP			
Promjene koje se odnose na sigurnost konfiguracije NCARH ili CA CSP	X	X	X
ADMINISTRIRANJE KORISNIČKIH RAČUNA			
Uloge i korisnici se dodaju ili brišu	X	X	X
Ovlasti za kontrolu pristupa korisničkom računu ili mijenjaju se uloge	X	X	X
UPRAVLJANJE SADRŽAJEM CERTIFIKATA			
Sve izmjene sadržaja certifikata	X	X	X
UPRAVLJANJE SADRŽAJEM LISTE OPOZVANIH CERTIFIKATA			
Sve promjene sadržaja liste opozvanih certifikata	X	X	X
RAZNO			
Instaliranje operativnog sustava	X	X	X

NCARH

Opća pravila certificiranja (CP)

Dogadaj koji je predmet revizije	Razina sigurnosti		
	Standardna	Srednja	Visoka
Instaliranje NCARH ili CA CSP	X	X	X
Instaliranje HW kriptografskih modula		X	X
Skidanje HW kriptografskih modula		X	X
Uništavanje HW kriptografskih modula	X	X	X
Start up sustava	X	X	X
Pokušaji prijave (logon-a) na NCARH aplikacije ili aplikacije CA CSP	X	X	X
Primitak HW ili SW		X	X
Pokušaj postavljanja zaporke	X	X	X
Pokušaj mijenjanja zaporke	X	X	X
Back up interne podatkovne osnovice NCARH ili CA CSP	X	X	X
Restore (vraćanje) interne podatkovne osnovice NCARH ili CA CSP	X	X	X
Rad s datotekama (primjerice, kreiranje, promjena imena, premještanje)		X	X
Objava bilo kojeg materijala u repozitoriju		X	X
Pristup internoj podatkovnoj osnovici NCARH ili CA CSP		X	X
Svi zahtjevi o prijavi o kompromitiranju certifikata	X	X	X
Punjenje kriptomodula certifikatima		X	X
Slanje kriptomodula		X	X
Brisanje (zeroize) kriptomodula	X	X	X
Obnavljanje ključeva NCARH ili CA CSP	X	X	X
Promjene konfiguracije CA poslužitelja koje uključuju:			
<i>Hardware</i>	X	X	X
<i>Software</i>	X	X	X
<i>Operativni sustav</i>	X	X	X
<i>Promjene</i>	X	X	X

Događaj koji je predmet revizije	Razina sigurnosti		
	Standardna	Srednja	Visoka
<i>Sigurnosni sadržaji</i>	X	X	X
FIZIČKI PRISTUP/SIGURNOST PROSTORA			
Pristup osoblja u prostor u kojem se nalazi NCARH ili CA CSP		X	X
Pristup NCARH poslužitelju ili poslužitelju CA CSP		X	X
Poznati ili sumnjivi prekršaji fizičke sigurnosti	X	X	X
NEPRAVILNOSTI			
SW pogreške	X	X	X
Neuspješna provjera integriteta SW	X	X	X
Primitak neispravne poruke		X	X
Krivo usmjerena poruka		X	X
Napadi na mrežu (sumnjivi ili potvrđeni)	X	X	X
Kvarovi opreme	X	X	X
Ispad sustava za napajanje el. energijom		X	X
Kvarovi na UPS-u		X	X
Očiti i bitni kvarovi mrežnog servisa ili pristupa		X	X
Narušavanje CP-a	X	X	X
Narušavanje CPS-a	X	X	X
Ponovno postavljanje sata operativnog sustava	X	X	X

4.5.2. Učestalost procesiranja log-a

Operativni će se logovi pregledavati u skladu s podacima u niže navedenoj tablici. OA NCARH će obrazložiti sve važne događaje koji se nalaze u izvještaju revizijskog loga. Takvi pregledi uključuju provjeru da log nije bio neovlašteno mijenjan, a potom brzu kontrolu svih log zapisa s detaljnijim ispitivanjem nepravilnosti u logovima. Akcije koje se poduzimaju kao rezultat tih pregleda bit će dokumentirane.

Razina sigurnosti	Pregled revizijskog loga
Test	Prema ugovoru
Standardna	Zahtijeva se ako postoji razlog
Srednja	Najmanje jednom svaka dva mjeseca Statistički bitan skup revizijskih podataka nastalih u CA-u CSP će se nakon zadnjeg pregleda ispitivat (povjerljivi intervali za svaku kategoriju revizijskih podataka određuju se sigurnosnim granicama kategorije i raspoloživošću alata da izvode takve preglede), kao i razumno istraživanje dokaza zlonamjerne aktivnosti.
Visoka	Najmanje jednom mjesečno Statistički bitan skup revizijskih podataka nastalih u CA-u CSP će se nakon zadnjeg pregleda ispitivat (povjerljivi intervali za svaku kategoriju revizijskih podataka određuju se sigurnosnim granicama kategorije i raspoloživošću alata da izvode takve preglede), kao i razumno istraživanje dokaza zlonamjerne aktivnosti.

Za NCARH bit će ispitani svi revizijski podaci koji nastaju u NCARH nakon zadnjeg pregleda.

4.5.3. Period čuvanja revizijskog loga

Revizijski će se logovi zadržati na CA opremi najmanje dva mjeseca. Osoba koja premješta revizijske logove NCARH sustava ili sustava CA CSP bit će službenik koji ne upravlja NCARH potpisujućim ključem ili potpisujućim ključem CA CSP.

4.5.4. Zaštita revizijskog loga

Konfiguracija i procedure sustava NCARH (ili CA CSP) moraju biti primjenjeni zajedno da bi se osiguralo da:

- samo autorizirano osoblje ima pristup čitanju logova,
- samo autorizirano osoblje može arhivirati revizijske logove i
- revizijski logovi nisu promjenjeni.

Osoba koja arhivira revizijske logove ne smije imati ovlast za mijenjanje logova. Osim toga moraju biti primjenjene procedure koje štite arhivske podatke od uništenja prije kraja perioda čuvanja revizijskog loga.

Revizijski logovi će biti preneseni na sigurno mjesto koje je različito od lokacije NCARH sustava.

4.5.5. Backup procedure revizijskog loga

Revizijski će logovi i izvještaji biti backupirani najmanje jednom mjesečno. Kopija će revizijskog loga bit poslana na udaljenu lokaciju u skladu sa CPS-om jednom mjesečno.

4.5.6. Sustav revizije (unutarnja ili vanjska)

Nema zahtjeva da sustav prikupljanja revizijskih logova bude vanjski u odnosu na CA sustav. Revizijski će se proces vršiti neovisno i neće biti nikada pod kontrolom CA operatora. Revizijski će proces započeti kod starta sustava i prekinut će se samo kod shutdown-a. Ako se primijeti da se automatski revizijski sustav pokvario, rad će se sustava NCARH ili CA CSP prekinuti, dok se revizijski sustav ponovno ne uspostavi. Ako je neprihvatljivo da se CA operacije prekinu, mogu se uspostaviti drugi načini koji omogućavaju revizijske funkcije. To se mora prethodno dogovoriti sa CA-ovim revizorom.

4.5.7. Obavijest subjektu koji je izazvao događaj

Kada je događaj zabilježen sustavom prikupljanja revizijskih logova, nije potrebno poslati obavijest osobi, organizaciji, uređaju ili aplikaciji koja je prouzročila događaj.

4.5.8. Procjene ranjivosti

Događaji se bilježe u procesu revizije, dijelom i zbog toga da bi se promatralo ranjivost sustava. CA mora osigurati da se procjene ranjivosti sustava provedu, nadgledaju i obnove provedbom istraživanja događaja koji su bili promatrani.

4.6. Arhiviranje certifikata i podataka

4.6.1. Tipovi pohranjenih podataka

Pohranjeni će slogovi NCARH-a ili CA CSP biti dovoljno detaljni da bi se ustanovila ispravnost rada NCARH-a ili CA CSP-a, ili valjanost bilo kojeg certifikata (uključivo opozvanih ili isteklih) koje je izdao NCARH ili CA CSP.

Kao minimum, sljedeći će podaci činiti arhivsku građu u skladu s razinama sigurnosti (zahtjevi će za testnu razinu biti u ugovoru).

Podaci koji se arhiviraju	Razina sigurnosti		
	Standardna	Srednja	Visoka
Akreditacija NCARH ili CA (ako je primjenjivo)	X	X	X
CPS	X	X	X
Ugovorne obveze	X	X	X
Konfiguracija sustava i opreme	X	X	X
Izmjene i dopune konfiguracije	X	X	X
Zahtjevi za izdavanje certifikata	X	X	X
Zahtjevi za opoziv certifikata	X	X	X
Autentifikacijski podaci subjekta kao u 3.1.9.	X	X	X

Podaci koji se arhiviraju	Razina sigurnosti		
	Standardna	Srednja	Visoka
Dokumentacija o prijemu i prihvatu certifikata	X	X	X
Dokumentacija o primitku kriptomodula	X	X	X
Svi certifikati koji su izdani ili objavljeni	X	X	X
Zapisi obnove ključa NCARH ili CA CSP	X	X	X
Svi ARL i CRL koji su izdani ili objavljeni	X	X	X
Svi revizijski logovi	X	X	X
Svi podaci ili aplikacije za provjeru sadržaja arhive	X	X	X
Dokumentacija koju zahtijevaju revizori usklađenosti	X	X	X

4.6.2. Period arhiviranja

Svi će se arhivirani podaci čuvati najmanje 10 godina. Ako originalni medij ne može držati podatke u zahtijevanom periodu, arhivar će definirati mehanizam za periodički transfer arhiviranih podataka na nove medije. SW aplikacije koje procesiraju arhivske podatke također će se održavati koliko je potrebno. Po završetku perioda arhiviranja, davatelji usluga certificiranja su odgovorni za održavanje autentičnosti i cjelovitosti svojih vrijednih dokumenata.

Minimalni period arhiviranja je naveden u sljedećoj tablici:

Razina sigurnosti	Minimalni period arhiviranja
Test	Prema ugovoru
Standardna	10 godina i 6 mjeseci
Srednja	10 godina i 6 mjeseci
Visoka	20 godina i 6 mjeseci

Prije kraja perioda arhiviranja, NCARH će arhivske podatke i aplikacije za čitanje arhive predati instituciji koju je odobrio PMA HR PKI i koja će tu arhivu trajno čuvati.

4.6.3. Zaštita arhive

Neovlaštene osobe neće moći zapisivati, modificirati ili brisati arhivu. Podaci iz arhive daju se na uvid u slučaju sudskih sporova ili drugih zahtjeva u skladu sa zakonom. Arhivirani podaci mogu biti preneseni na drugi medij. Prikazivanje cjelokupnog sadržaja arhive neće biti dopušteno osim ako se zahtijeva zakonom. Zapisi pojedinačnih transakcija mogu biti prikazani nakon zahtjeva bilo kojeg CSP koji je uključen u transakciju ili njegovog opunomoćenika. Arhivski mediji će biti spremljeni na poseban sigurni uređaj.

4.6.4. Back-up arhive

Arhiva mora imati sigurnosnu kopiju (backup). Backup arhive mora biti čuvan na sigurnom mjestu te u slučaju potrebe mora omogućavati restore arhiviranih podataka u kratkom vremenu.

4.6.5. Zahtjevi za vremenski žig zapisa

Validacije certifikata i potpisivanje dokumenata pred svjedocima (notarizacija) nosit će vremenski žig.

4.6.6. Sustav prikupljanja arhivske građe (unutarnji ili vanjski)

NEMA UVJETA.

4.6.7. Procedure pribavljanja i provjere arhivskih informacija

Procedure za pribavljanje i provjeru arhivskih informacija i procedure koje detaljno opisuju kako kreirati, pakirati i poslati arhivske informacije bit će publicirane u priručniku za procedure u CA-u ili u pripadajućem CPS-u. Samo će autoriziranim osobama bit dopušten pristup arhivi. Tijekom inspekcija koje su zahtijevane u ovom CP-u inspektor će provjeravati integritet arhive.

4.7. Zamjena certifikata (ključeva)

Potpisujući će ključ NCARH-a imat period valjanosti u duljini trajanja polovine perioda životnog ciklusa njegova korespondirajućeg certifikata.

CSP mogu odabrati za svoje CA ključeve period valjanosti koji je različit od ½ perioda valjanosti korespondirajućeg certifikata. U odabiranju perioda valjanosti potpisuljućeg ključa, CSP će uzeti u obzir duljinu potpisujućeg ključa, kako je on zaštićen i kontroliran, ima li njihov PKI hijerarhijsku ili mrežnu arhitekturu i druge faktore.

4.8. Postupci otklanjanja posljedica elementarnih nepogoda i incidenata

4.8.1. Oštećenje računalnih resursa, softvera i/ili podataka

CA mora imati odgovarajući plan za otklanjanje posljedica šteta i nezgoda te plan za nastavak rada. Plan mora postaviti i učiniti operativnim uređaje koji su smješteni na drugoj lokaciji. Ti uređaji moraju biti u mogućnosti provoditi CA servise u skladu s ovim CP-om u roku od 48 sati nakon pada produkcijskog sustava. Takav plan uključuje kompletne i periodičke testove tih uređaja. Taj plan treba biti naveden u drugoj prikladnoj dokumentaciji te biti dostupan pouzdajućim stranama.

4.8.2. Sigurnosne prilike nakon elementarnih nepogoda ili incidenata

CA mora izraditi plan za otklanjanje od posljedica elementarnih nepogoda i drugih šteta i nezgoda, u njemu se moraju navesti koraci koje treba poduzeti da bi se ponovno uspostavile prvotne sigurnosne prilike (uvjeti). Kada repozitorij nije pod kontrolom CA-a, CA mora

NCARH

Opća pravila certificiranja (CP)

osigurati da u ugovoru sa repozitorijem stoji da repozitorij ima isti plan za slučaj prirodnih nepogoda i drugih nezgoda.

4.8.3. Opoziv NCARH potpisnog ključa ili potpisnog ključa CA CSP

Ako NCARH ili CA CSP ne mogu izdati ARL/CRL na vrijeme specificirano za sljedeće izdavanje, tada PMA HR PKI i svi njegovi članovi trebaju biti obaviješteni na siguran način, u najkraćem mogućem roku i na način koji je naveden u ugovoru. To će omogućiti zaštitu interesa CSP i pouzdajućih strana. PMA HR PKI će odlučiti hoće li opozvati NCARH certifikat izdan CA-u CSP. NCARH ili glavni CA CSP će ponovo uspostaviti postupke izdavanja ARL/CRL što je brže moguće, u skladu s procedurama navedenim u pripadajućem CPS-u. NCARH ili CA CSP će u najkraćem mogućem vremenu obavijestiti PMA HR PKI i sve članove CSP dođe li do elementarne nepogode ili incidenta u kojem bi instalacija NCARH ili glavnog CA CSP bila fizički oštećena i uništene sve kopije NCARH potpisnih ključeva ili potpisnih ključeva CA CSP.

4.8.4. Kompromitiranje NCARH potpisnog ključa ili potpisnog ključa CA CSP

Ako je potpisni ključ NCARH ili CA CSP kompromitiran ili izgubljen:

- PMA HR PKI i svi njegovi članovi CSP će bit na siguran način i u najkraće moguće vrijeme obaviješteni (tako da CSP mogu izdati ARL-ove u kojima se opoziva cross certifikat koji se izdaje NCARH-u)
- novi par ključeva za NCARH ili CA CSP će generirati NCARH ili CA CSP u skladu s procedurama NCARH ili CA CPS-a
- izdaće se novi NCARH certifikati ili certifikati CA CSP u skladu s procedurama NCARH ili CA CPS-a

OA NCARH ili CA CSP će također istražiti i dat izvještaj PMA HR PKI o uzrocima koji su prouzrokovali kompromitiranost ili gubitak te koje su mjere poduzete za sprečavanje ponavljanja takvih incidenata.

4.9. Prestanak rada - davanja usluga

U slučaju prestanka rada NCARH-a, certifikati koje je izdao NCARH biti će opozvani i PMA HR PKI će obavijestiti CSP koji imaju ugovor s njim da je NCARH prestao raditi da mogu opozvati certifikate koje su izdali NCARH-u. Prije prestanka rada, NCARH će predat arhivske podatke instituciji koje je odobrio PMA HR PKI za trajno čuvanje arhivske građe.

U slučaju da CA CSP prekida rad, CSP će obavijestiti PMA HR PKI prije prestanka rada.

5. KONTROLE TEHNIČKE SIGURNOSTI RADA SUSTAVA CERTIFICIRANJA

5.1. Kontrola prostora, opreme i sredstava

NCARH i CA-ovi CSP moraju postaviti zahtjeve za fizičku sigurnost koji omogućuju slične razine zaštite. Svi zahtjevi za fizičku sigurnost jednako se primjenjuju NCARH i CA CSP.

5.1.1. Lokacija prostorije i njena konstrukcija

Mjesto na kojem je instaliran CA poslužitelj mora udovoljavati zahtjeve zone visoke sigurnosti uključujući sljedeće:

- da bude nadgledano osobno ili elektronički radi sprečavanja neautoriziranog ometanja/ulaženja u bilo koje vrijeme,
- osigurati da pristup CA poslužitelju bude ograničen samo na osoblje koje se nalazi na pristupnoj listi, te zahtijevati dvostruku kontrolu pristupa CA poslužitelju za te osobe;
- osigurati da se osoblje koje nije na listi pristupa pravilno prati i nadgleda,
- osigurati da se bilježenje (log) pristupnog mjesta održava i periodički provjerava,
- osigurati da se svi pokretni mediji i papir koji sadrži osjetljive informacije pohranjuju u sigurne i zaštićene kontejnere.

Mjesto na kojem je instaliran RA sustav, mora se nalaziti u prostorima koji zadovoljavaju kontrole za prijemne zone. Ako se RA radna stanica koristi za online unos podataka o korisnicima i vezu prema CA, radna stanica mora biti smještena u:

- sigurnosnoj zoni ili
- operativnoj zoni pod nadzorom (čuvana) ili bez nadzora uz zaštitu sigurnosti medija

CA mora osigurati da RA provodi primjerenu sigurnosnu zaštitu kriptomodula, cijelog sistemskog SW i privatnih ključeva. Primjerice, kriptomodul i RA-ov privatni ključ trebao bi biti čuvan u sigurnom kontejneru ili sefu, ako je potreban PIN ili zaporka, oni moraju biti čuvani u sigurnom kontejneru do kojeg ima pristup samo određeno osoblje. Zaposlenici RA ne smiju napustiti svoje radne stanice, odnosno radna stanica ne može ostati bez nadzora, kada je kriptografija u nezaključanom statusu (tj. kada su PIN ili zaporka već unijeti). Radna stanica koja sadrži privatne ključeve na tvrdom disku mora biti fizički zaštićena s odgovarajućim produktom za kontrolu pristupa. HW kriptomoduli moraju biti zaštićeni fizički, što se može postići zaštitom mjesta na kojem se nalaze.

5.1.2. Fizički pristup

Oprema CA će uvijek biti zaštićena od neautoriziranog pristupa. Oprema RA će biti zaštićena od neautoriziranog pristupa za vrijeme dok je modul aktivan. RA će uvesti fizičku kontrolu pristupa da bi smanjio rizik fizičkog oštećenja opreme čak i kada kriptomodul nije aktivan. Ovi sigurnosni mehanizmi bit će u skladu sa razinom opasnosti u okolini u kojoj se nalazi oprema

RA. Primjerice, RA oprema koja se nalazi u okolini u kojoj radi RA osoblje s kontroliranim pristupom neće trebati dodatnu razinu kontrole pristupa. RA će oprema u manje sigurnim okolinama zahtijevati dodatnu zaštitu, primjerice, da se nalazi u sobi koja je zaključana kada autorizirano osoblje nije nazočno. CA kriptomoduli koji se mogu prenositi bit će inaktivirani i smješteni u zaključane kontejnere. Bilo koji aktivacijski podaci koji se koriste za pristup kriptomodulu ili CA opremi bit će odvojeno čuvani. Takve informacije trebale bi biti memorirane i neispisane. Ako je takva informacija ispisana, mora biti sigurno čuvana u zaključanom kontejneru.

Provjera sigurnosti uređaja koji se nalaze u CA opremi će se odvijati najmanje jednom u 24 sata. Provjera bi trebala osigurati sljedeće:

- da je oprema u stanju prikladnom za operativni rad (primjerice da su kriptomoduli i prenosivi tvrdi diskovi na mjestu kada su "otvoreni" i na sigurnom kada su "zatvoreni");
- da su svi sigurnosni kontejneri pravovaljano osigurani;
- da sistemi fizičke sigurnosti (zaključavanje vratiju, pokrivanje otvora) funkcioniraju pravilno; i
- da je prostor osiguran od neautoriziranog pristupa

Korisnička će uloga/osoba biti eksplicitno odgovorna za izvođenje ovih provjera. Kada je korisnička uloga odgovorna, održavat će se log koji identificira osobu koja je izvršila provjeru. Čuvat će se zapisi koji sadrže tipove izvršenih provjera, vrijeme i osobu koja ih je izvršila. Ako se CA oprema nalazi pod stalnim nadzorom, provjera sigurnosti obavljat će se jednom u smjeni. Ako oprema nije pod stalnim nadzorom, zadnja osoba koja odlazi inicirat će "sign out" listu, koja osigurava da se ulazna vrata zaključaju i da se aktivira sustav za otkrivanje nedopuštenog pristupa. Ako su uređaji koji se nalaze u CA opremi bez nadzora za period dulji od 24 sata, bit će zaštićeni sustavom za otkrivanje nedopuštenog pristupa. Najmanje će se jednom u 24 sata to provjeriti, da bi se osiguralo da su sva vrata koja vode do opreme zaključana, i da nije bilo pokušaja nasilnog ulaska.

5.1.3. Sustav za napajanje i klima uređaji

Uređaji koji se nalaze u opremi CA bit će opskrbljeni napajanjem i klimatizacijom dovoljnom da osiguraju odgovarajuću radnu okolinu. Područje za osoblje mora biti opskrbljeno dodatnim pomagalima da bi se zadovoljilo operativne, zdravstvene i sigurnosne potrebe. Stvarna će količina i kvaliteta korisničkih servisa ovisiti o radu CA, primjerice, radno vrijeme (24 sata 7 dana ili 8 sati 5 dana), ili je li omogućena online provjera statusa certifikata. CA će oprema imati backup mogućnost dovoljnu da automatski zatvori ulaz u sustav, završi sve akcije koje su u redu čekanja, i zabilježi stanje opreme prije nego li nastupi shutdown zbog nestanka električne energije. Mehanizmi opoziva certifikata bit će omogućeni pomoću uređaja za neprekinuto napajanje (UPS).

5.1.4. Opasnost od poplave

Ovaj CP ne postavlja uvjete na preventivu od poplave više od onoga što se smatra kao najbolja poslovna praksa. Oprema CA će biti instalirana tako da nije u opasnosti od poplave, primjerice,

na stolovima ili podignutim podovima. Detektori će vlage bit instalirani u područjima koja mogu biti izložena poplavi.

5.1.5. Protupožarna zaštita

Ovaj CP ne postavlja uvjete na preventivu zaštite od požara više od onoga što se smatra kao najbolja poslovna praksa. Automatski će se sustav za zaštitu od požara instalirati u skladu s lokalnim pravilima. CA će imati plan za izvanredne okolnosti, koji će računati na moguće štete prouzrokovane vatrom.

5.1.6. Čuvanje medija za pohranu podataka

Da bi se sačuvalo od slučajnog oštećenja (voda, vatra, elektromagnetsko zračenje) mediji će se pohraniti na siguran način. Mediji na kojima su pohranjeni kontrolni podaci, arhivske ili backup informacije bit će sačuvani na lokaciji odvojenoj od CA opreme.

5.1.7. Rješavanje otpada

Normalni će otpad iz ureda bit odnesen ili uništen u skladu s poslovnom praksom. Mediji koji se koriste za prikupljanje ili prijenos informacija o kojima se govorilo u 2.8. bit će uništeni prije odnošenja tako da se informacija ne može rekonstruirati.

5.1.8. Backup na drugoj lokaciji

Backup-i sustava, dovoljni da se sustav oporavi, bit će urađeni po periodičnom planu kako je opisano u CPS-u. Backup-ovi će se provesti i spremiti na udaljenu lokaciju barem jednom tjedno. Najmanje će jedna backup kopija bit sačuvana na drugoj lokaciji (odvojeno od CA opreme). Samo posljednji backup mora biti sačuvan. Backup će bit sačuvan na mjestu s fizičkim i proceduralnim kontrolama, koje su u skladu s kontrolama CA sustava.

5.2. Kontrola postupaka i provedbe radnih zadaća

5.2.1. Osobe od povjerenja

Za korisničke uloge od povjerenja treba postaviti povjerljive osobe, jer bi se na ovakvim poslovima mogli pojaviti problemi sigurnosti, ako se ne provode pravilno, bilo slučajno ili zlonamjerno. Ljudi koji se izaberu za povjerljive korisničke uloge moraju biti brižljivi i primljeni na način koji je opisan u 5.3. Korisničke uloge koje izvode povjerljive osobe čine temelj povjerenja u cijeli PKI.

5.2.2. Broj osoba potrebnih za izvođenje operacija

CA će koristiti komercijalno razumnu praksu da se osigura da jedna osoba koja radi sama ne može zaobići sustav zaštite.

CA mora osigurati da jedna osoba ne može pristupiti privatnom ključu subjekta koji je čuvan kod CA. Kao minimum, proceduralni i radni mehanizmi moraju se poštivati pri vraćanju

ključeva (kao Split-Knowledge Technique) da bi se spriječilo otkrivanje enkripcijskog ključa neautoriziranoj osobi.

Više osoba treba sudjelovati pri generiranju CA ključa kako je naznačeno u 6.2.2. Sve ostale dužnosti povezane s korisničkim ulogama u CA može izvoditi jedna osoba sama. CA mora osigurati proces nadzora svih aktivnosti koje izvode imatelji privilegiranih korisničkih uloga.

Da bi se najbolje osigurao integritet i rad CA-ove opreme, preporučuje se da se gdje god je to moguće identificira posebna osoba za svaku povjerljivu korisničku ulogu. Nizom provjera dobiva se odvajanje uloga. Nema okolnosti pod kojima bi osoba koja obavlja povjerljivu korisničku ulogu obavljala reviziju svoga posla.

5.2.3. Identifikacija i autentifikacija za izvršenje određene korisničke uloge

Za cjelokupno CA-ovo osoblje mora biti izvršen I&A prije nego li:

- se uključe na pristupnu listu fizičke lokacije CA,
- se uključe na pristupnu listu za fizički pristup CA sustavu,
- dobiju certifikat za izvođenje njihove korisničke uloge u CA,
- dobiju korisnički račun na PKI sustavu.

Svaki od tih certifikata i korisničkih računa (s iznimkom CA potpisnog certifikata) mora:

- biti direktno vezan na osobu;
- ne smije se razmjenjivati, i
- mora biti ograničen na akcije za koje je ta korisnička uloga autorizirana uporabom CA SW, operativnog sustava i proceduralnih kontrola.

Kada se CA-u pristupa kroz zajedničke mreže, CA operacije moraju biti sigurne, što se postiže uporabom mehanizama, kao što je stroga autentifikacija i enkripcija bazirana na kriptomodulu.

5.3. Kontrola osoblja - broj, stručnost i ovlaštenja

5.3.1. Zahtjevi životopisa, kvalifikacije i iskustva

Svaki će CSP identificirati barem jednu osobu ili grupu odgovornu za upravljanje radom svakog CA u tom CSP. Za NCARH to su PMA NCARH i OA NCARH.

CA, RA, i repozitorij će formulirati i slijediti pravilnike o osoblju koji su dovoljni da omogućе razumno osiguranje pouzdanosti i stručnosti njihovih zaposlenika, i zadovoljavajuće obavljanje njihovih dužnosti na način koji je u skladu s ovim CP-om.

Osoblje će OA NCARH imat sigurnosni rang visoke sigurnosti/tajnosti.

5.3.2. Postupci provjere životopisa

CA će provest odgovarajuće istraživanje osoblja koje će obavljat povjerljive korisničke uloge (prije zaposlenja i poslije s vremena na vrijeme), da bi provjerio njihovu pouzdanost i sposobnost u skladu sa zahtjevima ovog CP-a. Osoblje koje ne uspije zadovoljiti uvjete pri

inicijalnom ili povremenom istraživanju, neće vršiti ili nastaviti vršiti povjerljive korisničke uloge.

5.3.3. Zahtjevi za obukom

CA mora osigurati da cjelokupno osoblje koje ima vodeće korisničke uloge u odnosu na rad u CA i RA dobije opsežnu obuku:

- CA/RA sigurnosni principi i mehanizmi,
- svjesnost o sigurnosti,
- svim verzijama PKI SW koje se koriste na CA sustavu,
- svim dužnostima za koje se očekuje da će ih vršiti,
- procesu za oporavak od nepogode i nastavka posla.

5.3.4. Zahtjevi za ponovnom obukom i njezinom učestalosti

Zahtjevi u točki 5.3.3. moraju se stalno obavljati da bi se udovoljio promjenama CA sustava. Ponovna obuka mora se obavljati po potrebi i CA mora pregledati te potrebe najmanje jedanput godišnje.

5.3.5. Rotiranje posla – učestalost i redosljed

Ovaj CP ne postavlja uvjete u odnosu na učestalost i redosljed rotiranja posla. Pravilnici CSP koji uspostavljaju zahtjeve, omogućit će kontinuitet i cjelovitost PKI servisa..

5.3.6. Sankcije za neautorizirane akcije

PMA HR PKI ili PMA CSP provodit će odgovarajuće administrativne i disciplinske postupke protiv osoblja koje je izvelo akcije koje se odnose na NCARH ili njegov repozitorij za koje nije autorizirano ovim CP-om, CPS-om NCARH-a ili drugim procedurama koje je objavio OA NCARH.

U slučaju stvarne neautorizirane akcije ili sumnje na neautoriziranu akciju, koju je izvela osoba koja vrši dužnosti u CA ili RA, CA treba suspendirati pristup te osobe CA sustavu.

5.3.7. Zahtjevi za osobe pod ugovorom

Sigurnosni su zahtjevi za osoblje pod ugovorom isti kao i za uposlenike.

5.3.8. Dokumentacija koja se isporučuje osoblju

NCARH ili CA CSP će učiniti dostupnim CA i RA osoblju CP-ove koje podržavaju, relevantne dijelove CPS-ova, i sve potrebne propise i ugovore.

Dokumentacija koja je dovoljna da definira radne zadaće i procedure za svaku korisničku ulogu bit će dostavljena osobi koja izvršava te korisničke uloge.

6. KONTROLE TEHNIČKE SIGURNOSTI RADA SUSTAVA CERTIFICIRANJA

6.1. Izrada certifikata

6.1.1. Generiranje para ključeva

Par ključeva za sve davatelje usluga certificiranja i subjekte mora biti generiran na takav način da privatni ključ nije poznat nikome osim imatelju ključa. Prihvatljivi načini za postizanje ovoga sadrže sljedeće:

- zahtjev da svi sudionici generiraju svoje vlastite ključeve uporabom pouzdanog sustava.
- upute sudionicima da ne otkrivaju privatne ključeve nikome, i/ili
- zahtjev da su ključevi generirani u HW kriptomodulima iz kojih se ne može ekstrahirati privatni ključ.

U svakom slučaju, svi ključevi davatelja usluga certificiranja (onih koji nisu repozitorij) i ključ certifikata najvišeg stupnja moraju biti generirani i sačuvani na kriptomodulima. Par ključeva za repozitorije i subjekte (uključujući standardni i srednji stupanj) može se generirati i čuvati u HW ili SW modulima.

6.1.2. Dostavljanje privatnog ključa

U najvećem broju slučajeva, privatni će se ključ generirati i ostati u modulu. Ako vlasnik modula generira ključ, tada nema potrebe slanja privatnog ključa. Ako ključ nije generiran od vlasnika kojemu je i namijenjen, tada osoba koja generira ključ u kriptomodul (npr. Smart Card) mora sigurno dostaviti modul imatelju ključa. Evidencija će se mjesta i stanja kriptomodula voditi do uručenja subjektu. Primatelj će potvrditi prijem kriptomodula CA-u ili RA-u. Ako subjekt generira ključ i ključ bude spremljen i korišten pomoću aplikacije koja ga je generirala, ili spremljen na HW kriptomodul koji je u posjedu subjekta, tada nije potrebna daljnja akcija. Ako ključ mora biti ekstrahiran za uporabu u drugim aplikacijama ili na drugim lokacijama, biti će korišten sustav zaštite podataka (primjerice, onaj definiran u PKCS #12). Rezultirajuća se datoteka može čuvati na magnetskom mediju ili se prenosi elektronički (6.4.1.).

6.1.3. Dostavljanje javnog ključa izdavatelju certifikata

Javni ključ mora biti dostavljen CA-u na siguran i povjerljiv način, kao što je poruka zahtjeva za izdavanje certifikata. Isporuka se može obaviti preko ne elektroničkog sredstva. To sredstvo može biti disketa koja je poslana preporučenom poštanskom pošiljkom ili po posebnom dostavljaču, ili isporuka kriptomodula CA-u za generiranje lokalnog ključa, pri predaji zahtjeva za certifikatom ili kod izdavanja certifikata. Pri offline načinu tražit će se provjera identiteta i dokaz posjedovanja korespondirajućeg privatnog ključa. Metode koje se primjenjuju za isporuku javnog ključa bit će navedene u CPS-u ili u ugovoru o certifikatu. U slučajevima kada je par ključeva generiran u CA u ime subjekta, CA će primijeniti sigurnosne mehanizme koji

osiguravaju da kriptomodul na kojem se nalazi par ključeva bude sigurno poslan subjektu, i da kriptomodul neće biti aktiviran prije potvrde pravog subjekta.

6.1.4. Dostava NCARH certifikata i javnog ključa glavnom CA CSP-u

NCARH će objaviti certifikate koje izdaje u repozitorij NCARH. Od glavnog će se CA CSP-a također zahtijevati da izda certifikat NCARH i da ga objavi u repozitoriju NCARH, istodobno s izdavanjem NCARH certifikata glavnom CA CSP-u. Kopija će javnog ključa NCARH tada biti dostupna i certifikatu glavnog CA CSP-a, što omogućuje provjeru povjerljive staze. Kada glavni CA CSP izdaje cross certifikat NCARH, NCARH će poslati svoj javni ključ glavnom CA CSP-u na siguran način drugim kanalom.

6.1.5. Duljine ključeva

Za ključeve koji nisu temeljeni na algoritmima eliptične krivulje minimalna duljina je 1024 bita. Minimalna duljina ključa za algoritme temeljene na eliptičnim krivuljama je 170 bitova.

Duljine ključeva su sljedeće:

- subjektov par ključeva za elektronički potpis 1024 bita RSA,
- subjektov par ključeva za enkripciju 1024 bita RSA,
- CA-ov par ključeva za elektronički potpis 2048 bita RSA,
- ključevi za PKIX-CMP sesiju su CAST-64.

6.1.6. Generiranje parametara javnog ključa

Parametri se za kreiranje ključeva za enkripciju generiraju u CA aplikaciji. Parametri se za kreiranje ključeva za elektronički potpis generiraju u PKI klijent aplikaciji subjekta ili u CA aplikaciji.

CA podržava DSA algoritam koji generira parametre u skladu s Digital Signature Standard (DSS) FIPS 186 ali za generiranje ključeva koristi RSA algoritam

6.1.7. Provjera kvalitete parametara

Kvalitetu parametara javnog ključa provjerava CSP koji ga je generirao, tj CA aplikacije ili subjektove PKI klijent aplikacije. Usklađenost s tim standardima se provjerava tijekom FIPS 186 validacije kriptografskih modula.

6.1.8. Generiranje CA i RA ključeva

Svi ključevi za CA i RA i certifikati visokog stupnja moraju se generirati u kriptomodulu koji:

- zadovoljava zahtjeve prema FIPS 140-1 razina 3 ili više,
- je pouzdani sustav koji je osiguran na EAL 4 ili viši u skladu sa ISO 15408, ili jednakim sigurnosnim kriterijima (ISO 15408 – protection profile se definira od CEN/ISSS koji specificira zahtjeve za pouzdane sisteme generiranja CA ključeva i CA potpisa)

6.1.9. Svrha uporabe ključa

Ključevi se mogu koristiti za autentifikaciju, neoporicanje i integritet poruke. CA privatni ključ za potpis je jedini ključ kojem je dopuštena uporaba za potpisivanje certifikata i CRL. Polje koje sadrži podatak o uporabi certifikata mora biti korišteno u skladu sa PKIX-1 - sadržaj certifikata i CRL. U tom polju mora se nalaziti:

- elektronički potpis, ili
- neoporicanje.

Jedna od sljedećih dodatnih vrijednosti mora se nalaziti u CA certifikatu za potpisivanje certifikata:

- potpis certifikata ili
- potpis CRL-a.

Uporaba specifičnog ključa se određuje pomoću ekstenzije polja uporabe ključa u X.509 certifikatu. Ovo ograničenje ne zabranjuje uporabu protokola (kao što je SSL) koji omogućuje autentificirano povezivanje uporabom certifikata za upravljanje ključevima.

6.2. Zaštita podataka za izradu vlastitog elektroničkog potpisa

Svaki davatelj usluga certificiranja mora čuvati svoje privatne ključeve u skladu s odredbama ovog CP-a.

6.2.1. Standardi za kriptomodule

Odgovarajući standard za kriptomodul je FIPS 140-1 razina 3 ili viši, ali PMA može odrediti da se mogu koristiti i drugi standardi za validaciju, certificiranje i provjeru. Ove će standarde objaviti PMA. Kriptomoduli će biti valjani za FIPS razinu koja je naznačena u ovom odjeljku ili će biti validirani, certificirani i provjereni preko nekog standarda koji je objavio PMA. Subjekt će koristiti kriptomodule koji zadovoljavaju kriterije najmanje za razinu 1. RA treba najmanje razinu 2 za HW kriptomodule. Može se koristiti i viša razina ako je dostupno ili poželjno. CA može koristiti HW ili SW kriptomodule za generiranje i zaštitu CA ključeva koji su validirani na razini 3 ili višoj. Certifikati će biti potpisani uporabom HW kriptomodula koji je na razini 3 ili višoj.

6.2.2. Kontrola privatnog ključa od više osoba (multi person control)

Kontrola od više osoba je sigurnosni mehanizam koji zahtijeva višestruke autorizacije za pristup CA privatnom ključu za potpis. Primjerice, pristup CA privatnom ključu za potpisivanje trebao bi biti obavljen uz autorizaciju i validaciju s više strana, uključujući CA osoblje i posebno osoblje za sigurnost. Ovaj mehanizam sprečava jednu stranu (CA ili neko drugi) da sama pristupi CA privatnom ključu za potpis.

CA privatni ključ za potpis može se pohraniti samo pod kontrolom dviju osoba. Strane koje sudjeluju u toj kontroli bit će evidentirane na listi koja je dostupna osoblju CSP-a zaduženom za revizijske poslove.

6.2.3. Čuvanje privatnog ključa

Privatni ključ koji služi samo u svrhu enkriptiranja i dekriptiranja, a ne za elektronički potpis, može biti sačuvan u svrhu vraćanja ključa.

6.2.4. Backup privatnog ključa

Sudionik može po izboru izvršiti backup svog privatnog ključa. Ako je tako, ključ mora biti kopiran i sačuvan u šifriranoj formi i zaštićen na razini koja nije niža od one uvjetovane za primarnu verziju ključa.

6.2.5. Arhiviranje privatnog ključa

Ako CA djeluje kao agent za vraćanje ključa, tada će on arhivirati ključeve za upravljanje privatnim ključevima kao dio svoga servisa. Privatni ključevi koji podržavaju neoporicanje neće se nikad arhivirati. Sudionik može po izboru arhivirati svoj privatni ključ.

6.2.6. Upis privatnog ključa u kriptomodul

Privatni ključevi davatelja usluga certificiranja trebaju biti generirani pomoću kriptomodula i u kriptomodulu. U slučaju da privatni ključ treba prenijeti iz jednog kriptomodula u drugi, privatni ključ mora biti enkriptiran tijekom prijenosa. Privatni ključevi ne smiju nikada biti kao običan tekst obrazac, van granica kriptomodula.

6.2.7. Metoda aktiviranja privatnog ključa

Prije aktiviranja privatnog ključa korisnici se moraju autentificirati kriptomodulu unošenjem PIN-a. Ova autentifikacija može biti u obliku zaporke. Privatni ključevi moraju se čuvati u šifriranom obliku kada su deaktivirani.

6.2.8. Metoda deaktiviranja privatnog ključa

Kriptomoduli koji su aktivirani ne smiju biti ostavljeni bez nadzora. Nakon uporabe moraju biti deaktivirani, uporabom manualnog log-outa ili pasivnim timeoutom. Kada nisu u uporabi HW kriptomoduli trebaju biti odloženi i spremljeni, osim ako su pod isključivim nadzorom subjekta.

6.2.9. Metoda uništenja privatnog ključa

Privatni ključ treba biti uništen ako korisniku više nije potreban, ako je njegov pripadajući certifikat opozvan ili mu je isteklo vrijeme valjanosti. Za SW kriptomodule to se može učiniti brisanjem podataka. Za kriptomodule to se može učiniti "zeroize" (brisanje) komandom. Fizičko uništenje HW nije potrebno.

6.3. Upravljanje podacima za izradu elektroničkog potpisa

6.3.1. Arhiviranje javnog ključa

CA mora čuvati sve javne ključeve za verificiranje.

6.3.2. Period valjanosti

CA-ov se privatni ključ za potpis neće koristiti više od polovine perioda valjanosti certifikata. Period je valjanosti certifikata najviše do 20 godina.

6.4. Podaci za pristup privatnom ključu (aktivacijski podaci)

6.4.1. Generiranje i instaliranje aktivacijskih podataka

Zaporka, PIN ili drugi aktivacijski podaci koriste se za zaštitu pristupa privatnom ključu. Ako aktivacijski podaci moraju biti preneseni subjektu, to treba učiniti kanalom koji ima prikladnu zaštitu, i u različito vrijeme i mjesto od pripadajućeg kriptomodula. Ako to nije urađeno osobno, subjekt treba biti obaviješten o vremenu, načinu slanja i o očekivanom datumu isporuke aktivacijskih podataka. Subjekt može potvrditi prijem kriptomodula i aktivacijskih podataka ovisno o načinu isporuke. Također subjekt može primiti informacije koje se odnose na uporabu i kontrolu kriptomodula (6.1.2.).

6.4.2. Zaštita aktivacijskih podataka

Aktivacijske podatke korisnik treba pamtit i ne zapisivati. Ako su zapisani moraju biti osigurani na razini sigurnosti kriptomodula i neće biti čuvani zajedno s kriptomodulom.

6.4.3. Drugi vidovi aktivacije

Ovaj CP ne postavlja uvjete za životni ciklus korisnikovih aktivacijskih podataka. Podaci se mogu mijenjati periodički da bi se smanjila mogućnost da budu otkriveni. CA može definirati zahtjeve za aktivacijske podatke u pripadajućem CPS-u ili u ugovoru o certifikatu.

6.5. Kontrole sigurnosti računalnog sustava

6.5.1. Posebni tehnički zahtjevi sigurnosti računalnog sustava

Svi CA poslužitelji moraju imati dolje navedenu funkcionalnost koja se dobiva s operativnim sustavom, ili kombinacijom operativnog sustava, PKI aplikacije i fizičke zaštite:

- kontrola pristupa CA servisima i PKI korisničkim ulogama zaposlenika,
- stroga razdvojenost dužnosti PKI korisničkih uloga zaposlenika,
- I&A PKI korisnička uloga zaposlenika,
- uporaba kriptografije za uspostavu komunikacija i zaštitu podatkovne osnovice,
- arhiviranje povijesnih i revizijskih podataka CA i krajnjeg korisnika,
- revizija događaja koji se odnose na sigurnost,
- CA-ov vlastiti test servisa koji se odnose na sigurnost,
- povjerljivost podataka za identifikaciju PKI korisničkih uloga i osoba koje ih provode,
- mehanizmi za vraćanje ključeva i obnovu funkcionalnosti CA sustava,
- čvrste granice područja za procese koji su osjetljivi na sigurnost.

6.5.2. Razina sigurnosti računalnog sustava

CA-ova oprema mora imati ISO/IEC 15408 i ISO/IEC 17799 razinu ili ekvivalent. Na CA opremi će kao minimum biti implementirana:

- samozaštita,
- izolacija procesa,
- diskrecijska kontrola pristupa,
- kontrola ponovne uporabe objekata,
- I&A za osoblje,
- zaštita revizijskih zapisa.

6.6. Kontrola sigurnosti radnog vijeka sustava

CA oprema HW i SW na kojima se obavlja PKI treba biti takva da umanju mogućnost da se bilo koja kopija može oštetiti. CA oprema za PKI bit će izrađena u kontroliranoj okolini i proces izrade će bit kontroliran i dokumentiran.

CA oprema će bit zaštićeno pakirana i isporučena povjerljivom metodom. CA oprema će bit specijalno pakirana ili će bit dostavljena na mjesto instalacije po posebnom donositelju. CA oprema će bit određena za vođenje infrastrukture o ključevima, ona neće sadržati druge aplikacije koje nisu dio CA konfiguracije. Nadogradnja opreme će bit nabavljena na isti način kao originalna oprema i bit će instalirana od povjerljive i izvježbane osobe na definirani način.

6.6.1. Kontrole razvoja sustava

CA mora koristiti CA SW koji je opisan i razvijen po metodologiji kao što je ISO/IEC 17799-1 ili MIL-STD-498 - Information system security. Procesi dizajna i razvoja moraju imati zadovoljavajuću dokumentaciju koja osigurava jamstvo kakvoće da bi bila moguća procjena sigurnosti od treće strane.

Kontrole razvoja sustava za NCARH i CA-ove CSP su sljedeće:

- uporaba softvera koji je razvijen po formalnoj i dokumentiranoj metodologiji (ISO/IEC 17799-1 ili MIL-STD-498)
- HW i SW koji je nabavljen za CA mora biti kupljen na način koji smanjuje vjerojatnost kvara
- HW i SW koji se razvija posebno za CA, bit će razvijan u kontroliranoj okolini, razvojni će proces bit definiran i dokumentiran
- sav HW mora bit transportiran i ispučen kontrolnim metodama koje omogućuju neprekinuti lanac odgovornosti, od lokacije kupnje do CA lokacije
- CA hardware i software bit će namijenjen za provođenje certifikacijskih servisa. Ne smije biti drugih aplikacija, hardverskih uređaja, mrežnih povezivanja, ili softverskih komponenti koje nisu dio CA operacija
- dopune HW i SW bit će kupljene ili razvijene na jednak način kao i originalna oprema, a instalirat će ih povjerljivo i obučeno osoblje na definirani način

6.6.2. Kontrole upravljanja sigurnošću

Formalna metodologija za upravljanje konfiguracijom mora se koristiti kod instalacija i održavanja CA sustava. CA SW kada je prvi put instaliran mora omogućiti metodu verifikacije od strane CA kojom se utvrđuje da je SW koji je na sustavu:

- izvorni SW proizvođača SW,
- da nije bio modificiran prije instalacije,
- da je to verzija koja se namjerava koristiti.

CA mora osigurati mehanizam za periodičnu provjeru integriteta SW. CA također mora osigurati mehanizme i pravila za kontrolu i nadgledanje konfiguracije CA sustava. Nakon instalacije najmanje jednom u 24 sata treba provjeriti integritet CA sustava.

6.7. Kontrola sigurnosti mrežnog sustava

CA uređaji bi trebali biti povezani na najviše dvije mrežne domene u isto vrijeme. CA oprema koja će biti povezana na više od jedne mrežne domene imat će definirane procedure u CPS ili drugom dokumentu koji će biti dostupan revizorima, a koje sprečavaju da se informacijama iz jedne domene može pristupiti iz druge domene (npr. shutdown opreme, promjenjivi tvrdi diskovi, prespajane mreže). Treba osigurati zaštitu CA opreme protiv svih poznatih vidova napada na mrežu. Svi mrežni portovi i servisi koji se ne upotrebljavaju bit će isključeni. Na CA opremi instalirat će se samo mrežni SW koji je potreban za CA aplikacije. Root CA oprema bit će stand alone ili offline konfiguracije.

6.8. Kontrola sigurnosti kriptografskih modula

Zahtjevi za kriptografske module navedeni su u točki 6.2. CP-a.

7. SADRŽAJ CERTIFIKATA I LISTE OPOZVANIH CERTIFIKATA

7.1. Sadržaj certifikata

Certifikati će sadržavati javne ključeve koji se upotrebljavaju za autentifikacije pošiljatelja elektroničkih poruka i provjeru integriteta tih poruka, tj. javne ključeve koji se koriste za provjeru elektroničkog potpisa. Certifikati će biti izdani u skladu s tehničkom specifikacijom ETSI 101862 (v. 1.2.1-2001-06 ili novije) - Qualified Certificate Profile, i koji se temelji na Qualified Certificate Profile obrascu RFC 3039, osim ako je drugi format neophodan za uspostavljanje sigurne bežične komunikacije ili interoperabilnosti s uređajima koji upotrebljavaju protokole za bežične aplikacije (WAP) ili druge tehnologije. U ovom CP-u neće biti zahtjeva prema pouzdajućoj strani da upotrebljava nestandardne certifikate. Gdje je to potrebno, certifikati će sadržavati referencu na OID u odgovarajućem polju za tip certifikata koji je identificiran ovim CP-om. CPS ili drugi javno dostupan dokument identificirat će podržane ekstenzije certifikata i razinu podrške za te ekstenzije.

7.1.1. Broj verzije i osnovna polja

CA mora izdavati certifikate u skladu sa ETSI 101862 (v 1.2.1-2001-06 ili novije) - Qualified Certificate Profile. SW krajnjeg korisnika mora podržavati sva osnovna (bez ekstenzija) X.509 polja.

7.1.1.1. Verzija

Verzija X.509 certifikata, verzija 3. (2.)

7.1.1.2. Serijski broj

Jedinstveni serijski broj za certifikat kao i za definirane ekstenzije certifikata

7.1.1.3. Potpis

CA potpis radi autentificiranja certifikata

7.1.1.4. Izdavatelj

Ime CA

7.1.1.5. Period valjanosti

Datum aktiviranja i isteka certifikata

7.1.1.6. Subjekt

DN subjekta

7.1.1.7. Informacija o javnom ključu subjekta

Javni ključ subjekta

7.1.2. Ekstenzije certifikata

Ekstenzije neće promijenit ili degradirat uporabu X.509 osnovnih polja. Dodatno:

7.1.2.1. Opća pravila o certificiranju (CP)

NEMA UVJETA.

7.1.2.2. Kritične ekstenzije

PKI SW svih sudionika mora korektno procesirati ekstenzije koje su označene kao kritične u sadržaju certifikata koji će se nalaziti u dodacima ovog CP-a.

7.1.2.3. Podržane ekstenzije

CPS ili drugi dokument javno objavljen mora definirati uporabu ekstenzija koje su podržane od CA, RA i subjekta.

7.1.3. OID za algoritme

RSA i HAS-1 algoritmi koje upotrebljava CA i podržava ih subjekt, odnosno RSA, DSA, MD5 i HAS-1 algoritmi koje upotrebljava subjekt.

7.1.4. Forme imena

Svaki DN mora biti u formi X.501, odnosno niza znakova koji se mogu tiskati (vizualno prezentirati) bez vodećih (lijevih) blenkova.

7.1.5. Imenska ograničenja

NCARH će zahtijevati imenska ograničenja u certifikatima izdanim glavnim CA-ovima, primjereno PKI koja se certificira.

7.1.6. OID za CP

CA mora osigurati da se OID CP-a o certificiranju nalazi u svim certifikatima koje on izdaje.

7.2. Sadržaj liste opozvanih certifikata (ARL/CRL)

NCARH i CA CSP će izdat X.509 verzija 2 format ARL/CRL. CPS ili drugi javno dostupni dokumenti će identificirati CRL ekstenzije koje su podržane i razinu podrške za te ekstenzije.

7.2.1. Broj verzije

CA mora izdavati ARL/CRL po X.509 verzija 2 u skladu sa PKIX – sadržajem certifikata i CRL.

7.2.2. ARL i CRL ulazne ekstenzije

PKI SW subjekta mora korektno procesirati sve CRL ekstenzije koje su identificirane u CRL sadržaju. CPS ili drugi javno dostupni dokument mora definirati uporabu ekstenzija koje podržava CA, RA i subjekti.

8. POSTUPCI S DOKUMENTACIJOM

8.1. Postupci pri promjeni sadržaja dokumentacije

Ovaj CP će se periodično revidirati (godišnje). Ispravak pogrešaka, nadopune i predložene izmjene ovog dokumenta mogu se poslati PMA-u uz dopis. Dopis treba sadržavati opis promjene i kontakt informaciju za osobu koja je poslala promjenu. Sve izmjene CP-a koje su u nadležnosti PMA bit će poslane svim zainteresiranim stranama na period razmatranja od najmanje jednog mjeseca. PMA će prihvatiti ili odbiti predložene promjene poslije isteka tog perioda.

8.1.1. Dijelovi koji se mogu mijenjati bez obavijesti

Izdavačke i tipografske ispravke, promjene kontakt detalja i druge manje ispravke koje ne utječu bitno na sudionike mogu se mijenjati bez obavijesti.

8.1.2. Dijelovi koji zahtijevaju obavijest

Sve izmjene ovog CP-a koji mogu bitno utjecati na sudionike zahtijevaju obavješćivanje. Prije nego što se izvrše takve izmjene CP-a, PMA će obavijestiti sve CA koji su direktno cross certificirali sa CA.

8.1.3. Period za primjedbe i provedba

Sudionici na koje utječu promjene mogu poslati primjedbe PMA-u, u roku od 30 dana nakon originalne obavijesti. Ako je predložena promjena modificirana kao rezultat primjedbe, uradit će se nova obavijest o promjeni.

8.2. Objavljivanje dokumentacije

8.2.1. Kopija CP-a

Kopija CP-a dostupna je u elektroničkoj formi u PDF formatu na Internetu i preko e-maila na adresi: pma.hrpki@mingo.hr.

8.2.2. Obavijest o promjenama

PMA će obavijestiti CA koji je autoriziran za izdavanje certifikata po ovom CP-u o predloženim promjenama zadnjeg datuma prijema primjedbi, i predloženom datumu primjene promjene. PMA može zahtijevati da CA obavijesti RA i Subjekte o predloženim promjenama.

8.2.2.1. Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene u PMA. Odluke koje se odnose na predložene promjene su diskreciono pravo PMA.

8.2.2.2. Obavijest o finalnim izmjenama

PMA će odredit period za obavijest o finalnim izmjenama.

NCARH

Opća pravila certificiranja (CP)

8.2.2.3. Izmjena dijelova koja zahtijeva novi CP

Ako je izmjena CP-a određena od PMA koji jamči izdavanje novog CP-a, PMA može odrediti novi OID za modificirani CP.

8.3. Postupci prihvaćanja/odobravanja CPS-a

Odobranje CA-ovog CPS-a mora biti u skladu s procedurama koje je odredio PMA. Kada CPS sadrži informacije koje se odnose na sigurnost CA, svi dijelovi CPS-a neće bit javno dostupni.