Pošta
Crne Gore

Odbor direktora

P R A V I L N I K
o postupcima izrade kvalifikovanih elektronskih vremenskih pečata (QTSA Practice Statement)

Podgorica,30.10.2019.godine

Pošta Crne Gore AD Podgorica
Odbor direktora
Broj: 00010-13812/2
Podgorica, 30.10.2019.godine

Projekat:	Javni PKI - Pošta Crne Gore Akcionarsko Društvo Podgorica (u daljem tekstu Pošta Crne Gore AD)
Naziv dokumenta:	**Pravilnik o postupcima izrade kvalifikovanih elektronskih vremenskih pečata [PoštaCG-QTSA]** **(QTSA Practice Statement)**
Verzija:	Verzija 0.5
Datum:	09.10.2019
Autor:	Milan Martinović, Tatjana Popović, Andreja Vujačić, Ivan Brković - Pošta Crne Gore AD Dragomir Stevanović - S&T Crna Gora d.o.o. Rudi Ponikvar - OSI d.o.o, Ljubljana

Revizije dokumenta:

1. Radna verzija 0.1:
- Prvi draft,
- datum 12.09.2019
2. Radna verzija 0.2:
- Dodata sekcija "Certifikat javnog ključa elektronskog vremenskog pečata",
- datum 16.09.2019
3. Radna verzija 0.3:
- Usaglašavanje u okviru radionice održane u Podgorici,
- datum 23.09.2019
4. Radna verzija 0.4:
- Dopune u okviru radionice održane 23.9.2019,
- datum 24.09.2019
5. Radna verzija 0.5:
- Dopune u okviru radionice održane 09.10.2019,
- datum 09.10.2019

Sadržaj

Na osnovu Zakona o elektronskoj identifikaciji i elektronskom potpisu („Sl. list CG" 31/17) Odbor direktora Pošte Crne Gore AD na sjednici od 30.10.2019. donio je

Pravilnik o postupcima izrade kvalifikovanih elektronskih vremenskih pečata (QTSA Practice Statement)

1. UVOD

Pošta Crne Gore AD upravlja infrastrukturom javnih ključeva [PoštaCG-PKI] za javne potrebe.

U okviru [PoštaCG-PKI] za potrebe davanja usluga certifikovanja uspostavljeno je certifikaciono tijelo [PoštaCG-CA] i usluga izrade kvalifikovanih elektronskih vremenskih pečata [PoštaCG-QTSA]. Kvalifikovani davalac usluge elektronskih vremenskih pečata [PoštaCG-QTSA] izrađuje elektronske vremenske pečate u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu (Sl. list RCG 31/17). Svi elektronski vremenski pečati izdati od strane [PoštaCG-QTSA] su kvalifikovani elektronski vremenski pečati.

2. PREGLED

Međunarodno priznat etalon za mjerenje vremena je neophodan u današnjem društvu. Univerzalno koordinirano vrijeme (UTC) trenutno ispunjava ovu funkciju i pravno je priznato u mnogim zemljama. Elektronski vremenski pečati su veoma koristan alat u kontekstu elektronskih transakcija gdje datum igra značajnu ulogu u procesu provjere i autentičnosti različitih događaja, podataka, dokumenata, ugovora ili certifikata. To je svojevrsna potvrda vremena u elektronskoj formi koja povezuje bilo koju vrstu elektronskih podataka u određenom vremenu, dokazujući da su ti podaci postojali u to vrijeme.

Kvalifikovani elektronski vremenski pečati koje izrađuju kvalifikovani davaoci usluga povjerenja obezbeđuju korist na osnovu visokog nivoa sigurnosti i pravne sigurnosti usluga povjerenja. Kvalifikovani elektronski vremenski pečati zasnivaju se na pretpostavci o tačnosti datuma i vremena koji su u njima sadržani i integritetu podataka sa kojima su povezani datum i vrijeme.

Za kvalifikovani elektronski vremenski pečat podrazumijeva se tačnost datuma i vremena koji su u njima sadržani i integritet podataka sa kojima su datum i vrijeme povezani.

3. DEFINICIJE I SKRAĆENICE

3.1. Definicije

Koriste se definicije u skladu sa dokumentom Pravilnik o postupcima izdavanja certifikata i zaštiti sistema certifikovanja [1].

Pored toga uvode se dodatne definicije:

Elektronski vremenski pečat – je skup podataka u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa odredenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme;

Kvalifikovani elektronski vremenski pečat - je elektronski vremenski pečat koji ispunjava posebne zahtjeve, i to:

1) povezuje datum i vrijeme sa podacima tako da se sprječava svaka mogućnost promjene podataka;
2) zasnovan je na preciznom vremenskom izvoru koji je povezan sa koordiniranim univerzalnim vremenom (UTC); i
3) potpisan je naprednim elektronskim potpisom ili pečatiran pomoću naprednog elektronskog pečata kvalifikovanog davaoca usluga povjerenja.

Vremenski pečat – sinonim za Elektronski vremenski pečat

Davalac usluga povjerenja - pravno ili fizičko lice (preduzetnik) koje kao davalac usluga certifikovanja za elektronske transakcije pruža jednu ili više usluga u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu (Sl. list RCG 31/17).

Kvalifikovani davalac usluga povjerenja - pravno ili fizičko lice (preduzetnik) koje ispunjava zahtjeve propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu (Sl. list RCG 31/17) za kvalifikovanog davaoca usluga certifikovanja za elektronske transakcije za jednu ili više usluga u predmetnom zakonu.

TSA – Pravno ili fizičko lice koje izrađuje elektronske vremenske pečate - sistem IT proizvoda i drugih komponenti, koje osiguravaju izradu elektronskog vremenskog pečata.

TSU - jedinica za izradu zapisa vremenskog pečata – uređaj (aplikacija ili hardver) kojeg koristi davalac usluge povjerenja izrade elektronskog vremenskog pečata i ima samo jedan aktivan ključ za digitalno potpisivanje zapisa vremenskog pečata.

UTC - Koordinirano svjetsko vrijeme - Mjerenje vremena na bazi sekunde, kako je to definisano prema ITU-R (International Telecommunications Radio Committee) preporuci (ITU-R Recommendation TF.460-5).

UTC(k) - Vremenska skala koja je dobijena u laboratoriji "k", koja zadržava tačnost svog vremena sa UTC s mogućom greškom u okviru plus minus 100ns. (više u ITU-R preporuci TF.536-1).

NAPOMENA: Lista UTC(k) laboratorija dostupna u sekciji 1, CircularT koju objavljuje BIPM i dostupna je na BIPM stranicama (http://www.bipm.org/).

3.2. Skraćenice

Koriste se skraćenice u skladu sa dokumentom Pravilnik o postupcima izdavanja certifikata i zaštiti sistema certifikovanja PoštaCG-CA [1].

Pored toga uvode se dodatne skraćenice:

TSA	Pravno ili fizičko lice koje izrađuje elektronske vremenske pečate
TSU	Jedinica za izradu zapisa vremenskog pečata
TST	Zapis vremenskog pečata
UTC	Koordinirano svjetsko vrijeme
NTP	Network Time Protocol

4. UČESNICI

4.1. Davalac usluge povjerenja izrade elektronskih vremenskih pečata (TSA)

Davalac usluge povjerenja za izradu elektronskih vremenskih pečata (TSA) je tijelo koje svojim naručiocima izdaje potvrdu o vremenu neke transakcije odnosno, da je podatak u nekom momentu postojao.

TSA odgovara za siguran i ispravan rad jedne ili više TSU jedinica s kojima proizvodi ili digitalno potpisuje zapise vremenskog pečata. TSA ima obavezu izdavati takve zapise vremenskog pečata, koje je naknadno moguće pravilno verifikovati (u skladu sa 7.3.1).

TSU privatni ključ koji se koristi za potpisivanje zapisa vremenskog pečata je vlasništvo [PoštaCG-QTSA]. [PoštaCG-QTSA] ima punu odgovornost za pridržavanje svih obaveza prema ovom Pravilniku u vezi TSU privatnog ključa.

[PoštaCG-QTSA] može svoje servise izvoditi sa više TSU jedinica. Svaka jedinica u tom slučaju posjeduje vlastiti ključ s kojim se potpisuju zapisi vremenskog pečata. Svaku jedinicu moguće je pravilno identifikovati.

4.2. Naručioci

Naručilac može biti fizičko ili pravno lice.

Kada je naručilac pravno lice s jednim ili više krajnjih korisnika, tada dio obaveza koje važe za naručioca, istovremeno važe i za naručioceve krajnje korisnike. U svakom slučaju naručilac će biti odgovoran za sve obaveze koje nastanu kada njegovi krajnji korisnici ne ispunjavaju u potpunosti svoje obaveze. Naručilac je obavezan da sam na adekvatan način obavijesti svoje krajnje korisnike o obavezama i svim nastalim nepravilnostima.

Kada je naručilac fizičko lice odnosno pojedinačni krajnji korisnik, onda je on direktno odgovoran za sve obaveze propisane ovim Pravilnikom.

4.3. Naziv dokumenta

Ovaj dokument nosi naziv „Pravilnik o postupcima izrade kvalifikovanih elektronskih vremenskih pečata (QTSA Practice Statement)“ i sadrži opšta pravila i postupke pružanja usluge povjerenja izrade kvalifikovanih elektronskih vremenskih pečata, i pravila i postupke o zaštiti sistema kojeg [PoštaCG-QTSA] koristi za pružanje predmetne usluge povjerenjau (daljem tekstu: Pravilnik).

5. PRAVILA IZRADE KVALIFIKOVANIH ELEKTRONSKIH VREMENSKIH PEČATA

5.1. Uvod

Prema ovom Pravilniku, [PoštaCG-QTSA] izrađuje zapise vremenskog pečata s tačnošću od 1 sekunde ili tačnije.

Pravilnik podrazumjeva da su elektronski vremenski pečati zasnovani na tehnologiji infrastrukture javnih ključeva i digitalnog potpisa.

5.2. Identifikacija kvalifikovanih elektronskih vremenskih pečata

Identifikaciona oznaka (OID) za kvalifikovane elektronske vremenske pečate izdate po ovom Pravilniku je: 1.3.6.1.4.1.36737.2.1.1.
[PoštaCG-QTSA] će navedeni OID koristiti u svim zapisima vremenskog pečata koje izdaje naručiocima.

5.3. Korisnici i aplikacije

Kvalifikovani vremenski pečati izdati po ovom Pravilniku namijenjeni su za upotrebu u aplikacijama kao što su na primjer potvrda da je dokument postojao u određeno vrijeme i održavanje validnosti kvalifikovanog elektronskog potpisa ili kvalifikovanog elektronskog pečata na period koji je duži od validnosti samog certifikata kojim su izrađeni. Kvalifikovani vremenski pečat je moguće koristiti u svim drugim aplikacijama koje imaju slične ili iste zahtjeve.

6. OBAVEZE I ODGOVORNOSTI

6.1. TSA odgovornosti

6.1.1. Opšte

[PoštaCG-QTSA] treba ostvariti sve zahtjeve u skladu sa opisom u poglavlju 7.
[PoštaCG-QTSA] će osigurati usklađenost svojih postupaka s bilo kojim zahtjevom koji je naveden u ovom Pravilniku ili posredno u nekoj od izvedenih referenci.

6.1.2. Obaveze TSA prema naručiocima

[PoštaCG-QTSA] dužna je ostvariti sve obaveze prema naručiocima, uključujući obaveze o dostupnosti i tačnosti svojih servisa.

6.2. Obaveze naručioca

Naručilac mora po preuzimanju zapisa vremenskog pečata da provjeri digitalni potpis kvalifikovanog elektronskog vremenskog pečata, važenje certifikata s kojim se izvodi provjera i da posjeduje 'hash' vrijednost podataka za koje je tražio kvalifikovani elektronski vremenski pečat. Naručilac je odgovoran za tačnu izradu 'hash' vrijednosti podataka za koje je tražio kvalifikovani elektronski vremenski pečat.

6.3. Obaveze trećih lica

Treća lica (saglasno uslovima prema 7.1.2), prije nego što prihvate zapise vremenskog pečata kao važeće, dužni su:
a) provjeriti da je zapis vremenskog pečata ispravno potpisan;
b) provjeriti validnost TSU ključa s kojim je zapis potpisan;

Napomena: Provjera validnosti TSU javnog ključa vrši se provjerom liste opozvanih certifikata (CRL), ako odgovarajući certifikat nije opozvan i provjerom, da certifikat javnog ključa TSU nije istekao.

c) uzeti u obzir bilo koje ograničenje za upotrebu zapisa vremenskog pečata, kako je definisano ovim Pravilnikom.

6.4. Ograničenje odgovornosti

Ovaj dokument ne definiše dodatna ograničenja odgovornosti TSA.
Prema ovom Pravilniku, [PoštaCG-QTSA] može ograničiti svoje odgovornosti do nivoa koji nije suprotan zakonima Crne Gore.

7. ZAHTJEVI ZA TSA POSTUPKE

7.1. Izjava o TSA postupcima i obavještenje naručiocima i trećim licima

7.1.1. Izjava o TSA postupcima

Svi postupci koje realizuje [PoštaCG-QTSA] opisani su u ovom Pravilniku, i u Pravilniku o postupcima izdavanja certifikata i zaštiti sistema certifikovanja PoštaCG-CA [1].

7.1.2. Obavještenje naručiocima i trećim licima

[PoštaCG-QTSA] objavljuje obavještenje korisnicima i trećim licima o uslovima korišćenja kvalifikovanih elektronskih vremenskih pečata na veb lokaciji https://www.postacg-ca.me, koje sadrži odredbe usaglašene sa EN 319 421 [5], B.2 TSA disclosure statement structure.

7.2. Upravljanje ključevima

7.2.1. Generisanje privatnog ključa TSU

Par kriptografskih ključeva [PoštaCG-QTSA] za digitalno potpisivanje kvalifikovanih elektronskih vremenskih pečata je generisan prilikom instaliranja aplikacije TSU i tokom postupka generisanja ključa (Key Generation Ceremony) po definisanoj proceduri. U toku generisanja para kriptografskih ključeva za digitalno potpisivanje koristi se zaštita koja važi za prostorije [PoštaCG-CA], višestruka autentifikacija ovlašćenih lica i hardverski kriptografski modul (Hardware Security Module - HSM).

7.2.2. Zaštita privatnog ključa TSU

Sve operacije za generisanje [PoštaCG-QTSA] kriptografskih ključeva i potpisivanja kvalifikovanih elektronskih vremenskih pečata vrše se na hardverskom kriptografskom modulu koji posjeduje sertifikat o usaglašenosti sa standardom FIPS 140-2 Level 3.
U operacijama u kojima se upravlja hardverskim kriptografskim modulom [PoštaCG-QTSA] uvijek je potrebno prisustvo najmanje dva lica sa odgovarajućim punomoćjem

koji se identifikuju sa pametnom karticom hardverskog kriptografskog modula i tajnom lozinkom kartice.
Sigurnosne kopije privatnog ključa TSU obezbijeđene su sigurnosnim mehanizmima hardverskog kriptografskog modula.
Privatni ključevi TSU se ne arhiviraju.

7.2.3. Distribucija javnog ključa TSU

Javni ključ TSU se objavljuje u TSU digitalnom certifikatu . Korisnici mogu da dobiju TSU digitalni sertifikat u bilo kom trenutku na veb stranici https://www.postacg-ca.me ili ga traže u okviru zahtjeva za izdavanje kvalifikovanih elektronskih vremenskih pečata, ali je njihova odgovornost da provjere identitet TSU naveden u TSU digitalnom certifikatu i integritet TSU digitalnog certifikata.

7.2.4. Obnavljanje TSU ključeva

Rok važnosti ključeva i TSU digitalnih certifikata naveden je u odjeljku 6.3.2. dokumenta "Pravilnik o postupcima izdavanja certifikata i zaštiti sistema certifikovanja " [1].
Privatni ključ TSU obnavlja se pre isteka perioda korišćenja privatnog ključa TSU koji nije duži od dvije godine. Novi par ključeva generiše se tokom procesa obnove u skladu s odredbama odjeljka 7.2.1.

7.2.5. Kraj životnog vijeka ključeva TSU

[PoštaCG-QTSA] garantuje da neće koristiti privatne ključeve TSU nakon isteka roka važnosti istih.
Svaki zahtjev za izradu kvalifikovanih elektronskih vremenskih pečata sa privatnim ključem koji je istekao biće odbijen.
Privatni ključevi se uništavaju tako da ih nije moguće vratiti. Mediji koji sadrže privatni ključ se brišu na siguran način. U toku uništavanja privatnih ključeva uništava se i sigurnosna kopija privatnih ključeva. Proces se strogo kontroliše i dokumentuje.

7.2.6. Upravljanje životnim vijekom hardverskog kriptografskog modula

Hardverski kriptografski modul dobavljač šalje na adresu [PoštaCA-QTSA] u zatvorenoj pošiljci. Po prijemu pošiljke, operativno osoblje [PoštaCA-QTSA] provjerava da nije oštećena ili otvorena. Nakon otvaranja pošiljke, operativno osoblje [PoštaCA-QTSA] provjerava integritet hardverskog kriptografskog modula.
Hardverski kriptografski modul čuva se u sigurnim prostorijama [PoštaCG-QTSA].
Instalaciju i aktiviranje hardverskog kriptografskog modula vrši operativno osoblje [PoštaCG-QTSA] u sigurnim prostorijama. U procesu aktiviranja i generisanja ključeva koriste se tehničke i organizacione kontrole višestruke autorizacije (four-eyes principle).

7.2.7. Certifikat javnog ključa kvalifikovanog elektronskog vremenskog pečata

TSU certifikati koje koristi [PoštaCG-QTSA] su izdati od strane [PoštaCG-CA] kao kvalifikovani certifikat za napredni elektronski pečat. Certifikati imaju dodatno polje (extendedKeyUsage) timestamp koje je u certifikatu označeno kao kritično.

7.3. Kvalifikovani elektronski vremenski pečat

7.3.1. Izrada kvalifikovanih elektronskih vremenskih pečata

[PoštaCG-QTSA] izrađuje svaki kvalifikovani elektronski vremenski pečat na siguran način i on sadrži tačno vrijeme. Bitne karakteristike svakog kvalifikovanog elektronskog vremenskog pečata su:

a) Sadrži identifikacionu oznaku (OID) u skladu sa ovim Pravilnikom.
b) Svaki kvalifikovani elektronski vremenski pečat sadrži jedinstveni identifikator (`serialNumber`).
c) Izvor vremena kojeg koristi TSU prilikom izrade svojih zapisa, povezan je sa bar jednom od vrijednosti koje distribuira neki UTC (k) laboratorij sa liste koju objavljuje Bureau International des Poids et Mesures (BIPM).
d) Izvor vremena sinhronizovan je sa UTC sa odstupanjem ne većim od jedne (1) sekunde.
e) Kada se ustanovi, da sat TSU nije u okviru propisane tačnosti, kvalifikovani elektronski vremenski pečat se ne izdaje.
f) Zapis vremenskog pečata sadrži "hash" vrijednost, koju šalje naručilac u svom zahtjevu.
g) Kvalifikovani elektronski vremenski pečat potpisan je sa TSU ključem koji se koristi isključivo za tu svrhu.

7.3.1.1. Zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata

Zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata koji šalju korisničke aplikacije mora biti u skladu sa RFC 3161 [2] i RFC 5816 [3].
Zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata može sadržati slijedeća polja:

- `reqPolicy`,
- `nonce` i
- `certReq`.

'hash' podataka za koje se traži kvalifikovani elektronski vremenski pečat mora biti jedan od slijedećih algoritma:

- `sha-256 (OID: 2.16.840.1.101.3.4.2.1).`
- `sha-384 (OID: 2.16.840.1.101.3.4.2.2).`
- `sha-512 (OID: 2.16.840.1.101.3.4.2.3).`

7.3.1.2. Odgovor na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata

Odgovor na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata koji šalje [PoštaCG-QTSA] u skladu je sa RFC 3161 [2] i RFC 5816 [3].
Prema ETSI EN 319 422 [6] svaki odgovor sadrži sljedeća polja:

- accuracy i
- nonce (ako je bio proslijeđen u zahtjevu).

U odgovoru na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata polje nonce sadrži istu vrijednost koja je stavljena u istoimenom polju zahtjeva za izdavanje kvalifikovanog elektronskog vremenskog pečata.
Odgovor na zahtjev za izradu kvalifikovanog elektronskog vremenskog pečata potpisan je privatnim ključem TSU jedinice.
U skladu sa TS 119 312, algoritam koji se koristi za potpisivanje zapisa vremenskog pečata je:

- sha256-with-rsa (OID: 1.2.840.113549.1.1.11)

7.3.2. Sinhronizacija sata sa UTC

Satovi servera TSU usklađeni su sa GPS prijemnikom UTC vremena i dodatno sa izvorima vremena koji distribuiraju tačno vrijeme NTP protokolom i koji su na listi UTC(k) laboratorija dostupni u sekciji 1, CircularT koju objavljuje BIPM i dostupna je na BIPM stranicama (http://www.bipm.org/).
Serveri TSU za izdavanje kvalifikovanih elektronskih vremenskih pečata sinhronizuju svoje satove sa GPS prijemnikom vremena u skladu sa NTP mrežnim protokolom vremena.
GPS prijemnik vremena zaštićen je od neovlašćenog pristupa.

7.4. Upravljanje i izvršavanje operacija TSA

7.4.1. Sigurnosno upravljanje

Informacioni sistem [PoštaCG-QTSA] dio je cjelokupne [PoštaCG-PKI] infrastrukture i primjenjuju se iste kontrole nad računarskim resursima i životnim ciklusom softvera koje su opisane u Pravilniku o postupcima izdavanja certifikata i zaštiti sistema certifikovanja [1].
[PoštaCG-QTSA] sistem zasnovan je na pouzdanim hardverskim i softverskim komponentama, a sve operacije sistema podržane su redundantnim komponentama.

7.4.2. Upravljanje imovinom

[PoštaCG-QTSA] osigurava odgovarajući nivo zaštite imovine koja se koristi za pružanje usluga povjerenja izrade kvalifikovanih elektronskih vremenskih pečata. Kako bi se osiguralo adekvatno upravljanje i zaštita imovine te spriječilo neautorizirano otkrivanje, modifikacija, premještanje ili uništavanje informacija koje su sačuvane na medijima, uspostavljene su sigurnosne mjere u skladu sa Pravilnikom

o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement - CPS)[1].

7.4.3. Kontrola osoblja

Osoblje [PoštaCG-QTSA] su stalno zaposleni ili zaposleni na određeno vrijeme. Oni su angažovani na poslovima davaoca usluga povjerenja i adekvatno osposobljeni za izvršavanje radnih dužnosti.
Osoblje [PoštaCG-QTSA] se obavezuje da ne smije da objavljuje ili saopštava povjerljive informacije vezane za bezbjednost davaoca usluga povjerenja ili informacije o naručiocima i korisnicima.
Osoblju [PoštaCG-QTSA] se ne dodjeljuju poslovi izvan djelokruga poslova za koje su angažovani kod davaoca usluga povjerenja, a koji bi mogli dovesti do sukoba interesa sa ovim poslovima.
[PoštaCG-PKI] radi provjeru osoblja prema trenutno uspostavljenoj praksi u Pošti Crne Gore u skladu sa zakonom i propisima iz ove oblasti.

7.4.4. Fizička sigurnost sistema i sigurnost njegovog okruženja

[PoštaCG-QTSA] sistem je smješten u istom prostoru gdje je smještena [PoštaCG-CA] infrastruktura. Primjenjuju se mjere fizičke bezbjednosti kako je opisano u odjeljku 5.1 Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja [1].

7.4.5. Bezbjednost računarske mreže

Računarsku mrežu [PoštaCG-QTSA] čine povezani mrežni segmenti, na kojima se nalaze serveri i radne stanice. Segmenti su međusobno povezani firewall-ovima. Računarska mreža davaoca usluga povjerenja je preko više firewall-a povezana sa Internetom. Bezbjedonosna pravila na firewall-ovima dozvoljavaju saobraćaj samo protokolima koji su neophodno potrebni za pristup servisima davaoca usluga povjerenja.

7.4.6. Upravljanje kontrolom pristupa

Kao što je navedeno u 7.4.4.

7.4.7. Upravljanje kontinuitetom rada

[PoštaCG-QTSA] ima uspostavljen plan oporavka od nepredviđenih katastrofa, koji pokriva oporavak poslovanja nakon kvara računarskih resursa, softvera i podataka.
U slučaju prirodnih i drugih katastrofa [PoštaCG-QTSA] će obnoviti poslovanje usluge TSA u najkraćem mogućem roku koristeći podatke sa rezervnih kopija sistema.

7.4.8. Slučaj kompromitovanja TSA servisa

[PoštaCG-QTSA] ima implementirane procedure reagovanja na bezbjednosne incidente i kvarove u skladu sa pozitivnim zakonskim propisima.

7.4.9. Ukidanje TSA servisa

U slučaju ukidanja servisa kvalifikovanog elektronskog vremenskog pečata, [PoštaCG-QTSA] će učiniti sve razumne napore kako bi se minimizirao uticaj servisa na poslovni proces naručioca ili trećih lica.

Posebno:

a) Ukidanjem usluge, [PoštaCG-QTSA] će:
   - obavijestiti naručioce i treća lica o svojoj odluci o ukidanju TSA servisa
   - svoje obaveze u vezi održavanja arhive revizijskih dnevnika izradenih kvalifikovanih elektronskih vremenskih pečata, prenijeti na drugog davaoca usluga povjerenja.
   - na drugog davaoca usluga povjerenja prenijeti obaveze u vezi održavanja dostupnosti TSU javnog ključa , odnosno TSU certifikata .
   - uništiti TSU privatni ključ uključujući i sve njegove kopije na način koji garantuje da se privatni ključevi više ne mogu obnoviti.

7.4.10. Usaglašenost sa primjenljivim zakonom

Ovaj pravilnik usaglašen je sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu,
- i drugim propisima iz ove oblasti.

7.4.11. Prikupljanje dokaza (Collection of evidence)

Postupci vezani uz prikupljanje, obradu i zaštitu revizijskih zapisa kao dokaza provode se na način koji je opisan u odjeljku 5.4 Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja [1].

Pored toga, bilježe se specifične aktivnosti vezane za rad [PoštaCG-QTSA] što uključuje:

- aktivnosti vezane za generisanje i životni ciklus TSU ključeva i TSU certifikata,
- aktivnosti vezane za sinhronizaciju TSU sa UTC vremenom uključujući regularno kalibriranje satova,
- kvarove i ispade sistema uključujući gubitak sinhronizacije ili nemogućnost kalibriranja satova.

Prikupljeni revizijski dnevnici arhiviraju se minimalno sedam godina nakon njihovog nastanka, prema praksi koja je opisana u odjeljku 5.5 Pravilnika o postupcima izdavanja certifikata i zaštiti sistema certifikovanja [1].

Arhiva se čuva na lokaciji [PoštaCG-QTSA] i na drugoj udaljenoj lokaciji. Arhiva je zaštićena sa odgovarajućim sigurnosnim mehanizmima. Pristup arhivama je dozvoljen samo ovlašćenim licima.

8. REFERENCE

[1] Pravilnik o postupcima izdavanja certifikata i zaštiti sistema certifikovanja (Certification Practice Statement - CPS)

[2] RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"

[3] RFC 5816 "ESSCertIDv2 Update for RFC 3161"

[4] EN 319 401 "General Policy Requirements for Trust Service Providers"

[5] EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps"

[6] EN 319 422 "Time stamping protocol and electronic time-tamp profiles"

[7] TS 119 312 "Cryptographic Suites"

Ovaj Pravilnik stupa na snagu osmog dana od dana objavljivanja u Službenom poštanskom glasniku.

Dostaviti:
-Izvršnom direktoru
-a/a

Pošta Crne Gore AD 1 PODGORICA

PREDSJEDNIK
Mirsad Džudžević