Pošta Srbije kao izdavalac vremenskih žigova

Dragan Spasić
Javno preduzeće PTT saobraćaja "Srbija"
Beograd, Srbija
dspasic@ptt.rs

Stevan Milinković
Računarski fakultet Univerziteta Union
Beograd, Srbija
smilinkovic@raf.edu.rs

Branislav Milojković
Računarski fakultet Univerziteta Union
Beograd, Srbija
bmilojkovic07@raf.edu.rs

Ljubomir Lazić
Državni univerzitet u Novom Pazaru
Novi Pazar, Srbija
llazic@np.ac.rs

Sadržaj **- U ovom radu je opisana arhitektura i redundantnost TSA (Time-Stamping Authority) sistema Pošte Srbije. Objašnjeno je izdavanje vremenskog žiga i životni ciklus kriptografskih ključeva TSA servera. Dat je pregled operativnog rada TSA tela. Na kraju, navedene su aktivnosti u slučaju prestanka rada TSA tela.**

Ključne reči - Pošta Srbije; izdavalac vremenskih žigova; vremenski žig; Zakon o elektronskom dokumentu

I. UVOD

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je izgradilo sistem za izdavanje vremenskih žigova i postalo je izdavalac vremenskih žigova (Time-Stamping Authority - TSA) u Republici Srbiji, u skladu sa Zakonom o elektronskom dokumentu [1] i Pravilnikom o izdavanju vremenskog žiga [2]. Vremenski žigovi Pošte namenjeni su svim učesnicima elektronskog poslovanja u Republici Srbiji, i fizičkim i pravnim licima (državna uprava, lokalna samouprava, javne službe, preduzeća, banke, osiguravajuća društva, organizacije, institucije,...).

Ministarstvo kulture, informisanja i informacionog društva upisalo je Javno preduzeće PTT saobraćaja "Srbija" u Registar izdavalaca vremenskog žiga, Rešenjem broj 345-01-00283/2011-07 od 9.3.2012. godine.

Pošta (u daljem tekstu TSA telo Pošte) izdaje vremenske žigove u skladu sa Politikom izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" [3]. Izdati vremenski žigovi su sa tačnim UTC vremenom (koordinisano univerzalno vreme - Coordinated Universal Time) uz odstupanje od najviše ±1 sekunde. Vreme odziva TSA sistema, kao razlika između vremena primljenog zahteva i vremena u vremenskom žigu, je manje od jednog minuta.

TSA telo Pošte za potpisivanje vremenskih žigova koristi tajne (privatne) ključeve generisane isključivo za tu namenu, sa periodom korišćenja od najviše tri meseca. TSA telo Pošte koristi TSA elektronske sertifikate koje izdaje Sertifikaciono telo Pošte, Javnog preduzeća PTT saobraćaja "Srbija", koje je registrovano u skladu sa Zakonom o elektronskom potpisu [4] od strane Ministarstva nadležnog za informaciono društvo. Rok važnosti TSA elektronskog sertifikata je pet godina.

Cene vremenskih žigova TSA tela Pošte svrstane su u tri tarifna modela:

- PREPAID model naplate,
- POSTPAID model naplate i
- FLAT RATE model naplate.

II. ARHITEKTURA I REDUNDANTNOST TSA SISTEMA POŠTE

Arhitektura TSA sistema Pošte prikazana je na Sl. 1. Tok zahteva za izdavanje vremenskih žigova od korisnika ka TSA serverima je sledeći:

- Zahtevi za izdavanje vremenskih žigova se od korisnika (klijenata) ravnomerno raspoređuju na dva TSA Proxy servera. Ako je jedan od TSA Proxy servera nedostupan (hardverski ili softverski kvar, isključenje, restar,...), svi zahtevi korisnika se automatski usmeravaju na drugi TSA Proxy server. TSA Proxy serveri su u *load balancer* konfiguraciji.
- Zahtevi korisnika za izdavanje vremenskih žigova se od TSA Proxy servera ravnomerno raspoređuju na dva (2) TSA servera. Ako je jedan od TSA servera nedostupan (zamena TSA tajnog ključa i sertifikata, hardverski ili softverski kvar, isključenje, restar,...), svi zahtevi korisnika se automatski usmeravaju na drugi TSA server. TSA serveri su u *load balancer* konfiguraciji.

Redundantnost i velika raspoloživost sistema i servisa TSA sistema Pošte postignuta je instalacijom dva TSA Proxy servera i dva TSA server. Sistem je modularan, tako da je jednostavno dodati nove TSA Proxy servere i TSA servere, u slučaju otkaza ili većeg opterećenja postojećih servera.

Na TSA Proxy serverima instalisana je TSA proksi aplikacija Pošte koja je razvijena u skladu sa zahtevima Pošte, i ona je integrisana sa Aplikacijom za naplatu i evidentiranje izdatih vremenskih žigova Pošte (Billing aplikacija) koja je instalisana na Billing serveru [5]. TSA Proxy serveri izvršavaju sledeće poslove:

- Odbijaju TSA zahteve korisnika koji nisu kreirani u skladu sa standardom RFC 3161 [6].

- Odbijaju TSA zahteve korisnika koji sadrže hash algoritam koji nije podržan.
- Odbijaju TSA zahteve korisnika koji sadrže TSA Policy OID koji nije podržan.
- Odbijaju TSA zahteve korisnika kojima se ne traži TSA sertifikat u vremenskom žigu (certReq=False).
- Prosleđuju identifikacione podatke o korisnicima ka Billing aplikaciji (serveru) za potrebe autentifikacije korisnika na TSA sistem.
- Prosleđuju TSA zahteve registrovanih korisnika ka Billing aplikaciji (serveru) i TSA serverima.

TSA Proxy serveri značajno rasterećuju TSA servere jer prema njima prosleđuju samo ispravne TSA zahteve od registrovanih korisnika, čime sprečavaju DoS napade na TSA servere.

TSA serveri su najvažniji serveri TSA sistema jer su oni nadležni za izdavanje vremenskih žigova. TSA serveri imaju HSM (Hardware Security Module) uređaje za generisanje i čuvanje TSA tajnog (privatnog) ključa za potpisivanje vremenskih žigova. Na TSA serverima instalisan je TSA softver kompanije Thales e-Security [7].

Hardverski uređaji za balansiranje saobraćaja (Hardware Load Balancer - HLB) kompanije Barracuda Networks postavljen je ispred TSA Proxy servera i TSA servera. Barracuda HLB uređaji podržavaju dva algoritma za balansiranje saobraćaja [8]:

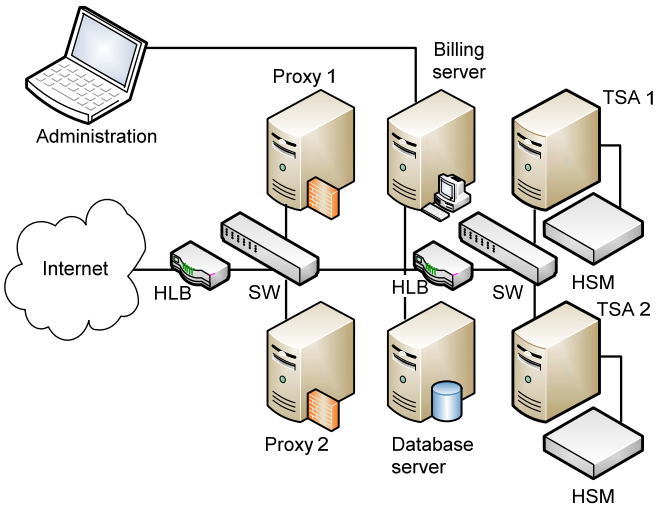
- *Weighted Round-Robin*. Kod ovog algoritma broj konekcija ka serverima zavisi od težinskih koeficijenata koji se unapred dodele tim serverima, tako da oni serveri koji imaju veće težinske koeficijente dobiće i više konekcija. Nedostatak ovog algoritma je to što se ne proverava da li su prethodno uspostavljene konekcije još uvek aktivne, a što je problematično u slučaju konekcija koje dugo traju.
- *Weighted Least Connections*. Kod ovog algoritma broj konekcija ka serverima zavisi od težinskih koeficijenata koji se unapred dodele tim serverima i od broja aktivnih konekcija. Ovaj algoritam je preporučen i zato se koristi u TSA sistemu Pošte.

Na oba HLB uređaja startovan je IPS (Intrusion Prevention System) servis, čime se TSA sistem dodatno štiti od eventualnih zlonamernih napada.

Korisnici sa Interneta pristupaju TSA sistemu Pošte, pri čemu korisnici prethodno moraju da budu registrovani. Registrovani korisnici mogu na dva načina da se autentifikuju prilikom podnošenja zahteva za izdavanje vremenskih žigova:

- Korisničkim imenom i lozinkom.
- Elektronskim sertifikatom.

Korisnici mogu da podešavaju svoje identifikacione podatke preko Portala za pregled Time-Stamp profila korisnika i izdatih vremenskih žigova Pošte Srbije (https://tsa.ca.posta.rs).



Slika 1. Arhitektura i redundantnost TSA sistema Pošte

III. IZDAVANJE VREMENSKOG ŽIGA

A. *Struktura podataka vremenskog žiga*

TSA telo Pošte osigurava da vremenski žig bude izdat na siguran način i da sadrži tačno vreme. TSA telo Pošte izdaje samo jednu vrstu vremenskog žiga, u skladu sa Politikom [3]. Svaki žig sadrži identifikacioni broj Politike izdavanja vremenskog žiga (TSA Policy OID) i jedinstveni serijski broj izdatog žiga.

Vremenski žig je elektronski potpisan tajnim (privatnim) ključem TSA servera. TSA telo Pošte za formiranje elektronskog potpisa vremenskog žiga koristi RSA algoritam primenom standarda PKCS#1, uz dužinu RSA ključa od 2048 bita. Žig sadrži TSA elektronski sertifikat kojim se proverava elektronski potpis vremenskog žiga.

Vremenski žig sadrži UTC vreme uporedivo sa UTC tačnim vremenom, uz maksimalno dozvoljeno odstupanje u odnosu na UTC tačno vreme od ±1 sekundi. Očekivano vreme važenja vremenskog žiga određeno je rokom važenja TSA elektronskog sertifikata, kojim se proverava elektronski potpis vremenskog žiga.

B. *Sinhronizacija vremena sa UTC*

TSA telo Pošte osigurava da vreme, u izdatom vremenskom žigu, odstupa najviše ±1 sekundu u odnosu na UTC tačno vreme i ne izdaje vremenske žigove izvan navedene tačnosti.

TSA telo Pošte obezbeđuje automatsku sinhronizaciju vremena TSA servera sa izvorom tačnog vremena, u skladu sa predviđenom preciznošću. TSA telo Pošte koristi izvor tačnog vremena sa NTP (Network Time Protocol) sinhronizacijom i internim satom, a NTP sinhronizacija se vrši sa Stratum 1 i 2 serverima.

Ukoliko dođe do gubitka sinhronizacije vremena TSA servera sa izvorom tačnog vremena, TSA server prestaje da izdaje vremenske žigove, do postizanja sinhronizacije.

Sinhronizacija vremena TSA servera vrši se tako da se ne očekuje odstupanje veće od deklarisane tačnosti.

IV. ŽIVOTNI CIKLUS KLJUČEVA TSA SERVERA

A. Generisanje ključeva

U TSA telu Pošte, asimetrični parovi ključeva TSA servera za elektronski potpis formiranih vremenskih žigova, uvek su generisani pod kontrolisanim uslovima, a što podrazumeva sledeće:

- generisanje ključeva TSA servera za potpisivanje vrši se u fizički obezbeđenoj sredini od strane najmanje dve osobe tj. TSA administratora sa poverljivim ulogama,
- generisanje ključeva TSA servera za potpisivanje vrši se u okviru HSM uređaja koji je sertifikovan u skladu sa sigurnosnim kriterijumima EAL 4+ i FIPS 140-2 nivo 3.

B. Zaštita tajnog ključa

TSA telo Pošte obezbeđuje da tajni (privatni) ključevi TSA servera ostanu tajni i sačuvaju svoj integritet, a što podrazumeva sledeće:

- tajni ključevi TSA servera za potpisivanje se čuvaju i koriste u HSM uređaju, koji je sertifikovan u skladu sa sigurnosnim kriterijumima EAL 4+ i FIPS 140-2 nivo 3,
- ne prave se kopije tajnih ključeva TSA servera za potpisivanje.

C. Distribucija javnog ključa

TSA telo Pošte objavljuje na Web strani TSA elektronske sertifikate koji sadrže javni ključ za proveru elektronskog potpisa vremenskog žiga, kao i sve zavisne parametre, uključujući i period aktivnog korišćenja.

TSA telo Pošte osigurava dostupnost ovih podataka, kao i to da objavljeni podaci sačuvaju svoj integritet i verodostojnost tokom distribucije zainteresovanim stranama.

D. Obnavljanje ključeva

Na najviše svaka tri meseca TSA telo Pošte generiše novi asimetrični par ključeva za potpisivanje vremenskog žiga.

E. Kraj životnog ciklusa tajnog ključa

TSA telo Pošte osigurava da se tajni (privatni) ključevi TSA servera ne koriste posle isteka planirane upotrebe. Tajni ključ se zamenjuje pre isteka planirane upotrebe, što označava prestanak upotrebe ključa, a zamenjeni tajni ključ se trajno uništava.

Ako istekne period planirane upotrebe tajnog ključa od tri meseca, TSA telo Pošte neće izdavati vremenske žigove, sve dok istekli tajni ključ ne bude zamenjen novim tajnim ključem.

F. Upravljanje HSM uređajem

TSA telo Pošte tokom rada osigurava zaštitu HSM uređaja, u kome se kreiraju i čuvaju ključevi TSA servera za potpisivanje i u kome se obavlja potpisivanje formiranog vremenskog žiga.

Pre premeštanja ili drugog narušavanja bezbednog okruženja HSM uređaja, TSA telo Pošte će prestati da koristi i trajno će uništiti tajne ključeve TSA servera.

V. FIZIČKO OBEZBEĐENJE

TSA telo Pošte osigurava da je fizički pristup sistemu za izdavanje vremenskih žigova kontrolisan:

- fizički pristup je dozvoljen samo autorizovanom osoblju,
- uvedene su internim pravilima definisane procedure kontrole pristupa za sprečavanje gubitka, oštećenja ili kompromitovanja sistema, krađe podataka i narušavanja poslovnog procesa,
- uvedene su internim pravilima definisane procedure kontrole pristupa HSM uređaju, u skladu sa sigurnosnim zahtevima za generisanje i čuvanje ključeva,
- sistem tj. infrastruktura TSA tela Pošte je u sistem sali, koja fizički štiti servere od neovlašćenog pristupa i ne deli se sa drugim organizacijama,
- oprema, podaci, mediji i softver TSA sistema Pošte ne mogu da se iznesu iz prostorija TSA tela Pošte bez odgovarajućeg odobrenja.

VI. UPRAVLJANJE OPERTIVNIM RADOM

TSA telo Pošte osigurava da komponente za izdavanje vremenskog žiga budu zaštićene i da ispravno funkcionišu, sa minimalnim rizikom od kvara, a što podrazumeva sledeće:

- integritet TSA sistema Pošte je zaštićen od virusa i nedozvoljenog softvera,
- primenjuje se sigurno rukovanje sa medijima korišćenim u okviru TSA tela Pošte, kako bi se mediji zaštitili od oštećenja, krađe i neovlašćenog pristupa,
- uspostavljene su i implementirane procedure za sve poverljive i administratorske uloge, koje učestvuju u obavljanju TSA usluga,
- TSA sigurnosne uloge su razdvojene od ostalih uloga,
- kapaciteti se prate i predviđaju, kako bi se obezbedilo da dovoljna procesorska snaga i smeštajni kapaciteti budu na raspolaganju,
- uvedeno je izveštavanje o sigurnosnim incidentima, a procedure reagovanja su takve da šteta od sigurnosnih incidenata bude minimalna,
- TSA administratori reaguju brzo na sigurnosne incidente, kako bi se ograničio uticaj incidenata, a u najkraćem roku biće sačinjen izveštaj o svakom sigurnosnom incidentu.

VII. KONTROLA PRISTUPA

TSA telo Pošte daje pristup samo ovlašćenim osobama:

- zaštita interne računarske mreže TSA tela Pošte od neovlašćenog pristupa je izvršena upotrebom firewall i IPS (Intrusion Prevention System) sistema,

- osigurana je efektivna administracija korisničkih naloga za pristup sistemu, kako bi se obezbedio potreban nivo zaštite,
- pristup podacima i aplikacijama je ograničen u skladu sa politikom kontrole pristupa,
- osoblje TSA tela Pošte se identifikuje pomoću sertifikata pre administracije kritičnih aplikacija,
- evidentiraju se sve aktivnosti TSA osoblja,
- lokalne mrežne komponente (firewall, hardware load balancer, switch) se čuvaju u sistem sali, u fizički zaštićenom okruženju. Njihova konfiguracija se periodično proverava, u skladu sa zahtevima.

VIII. Čuvanje podataka o radu usluge izdavanja vremenskog žiga

TSA telo Pošte osigurava da se svi relevantni podaci u vezi izdatog vremenskog žiga čuvaju u periodu od najmanje pet godina od datuma izdavanja žiga, tako što se:

- zapisuju i bezbedno arhiviraju svi događaji i podaci u vezi rada TSA tela Pošte,
- održava poverljivost i integritet aktuelnih i arhiviranih zapisa u vezi rada TSA tela Pošte,
- kompletno i poverljivo čuvaju zapisi u vezi rada TSA servisa,
- obezbeđuje dostupnost zapisa u vezi rada TSA servisa, ukoliko je potrebno dokazati pravilno funkcionisanje TSA servisa za potrebe sudskog postupka,
- evidentira tačno vreme značajnih promena u okruženju, upravljanja ključevima i sinhronizacije vremena,
- čuvaju zapisi u vezi TSA servisa, dovoljno dugo, posle isteka važenja TSA sertifikata, radi mogućnosti pružanja odgovarajućeg pravnog dokaza,
- čuvaju zapisi događaja, na način koji obezbeđuje da se ne mogu lako obrisati ili uništiti,
- poverljivo čuvaju svi podaci o korisnicima, osim ako se sa korisnikom dogovori da podaci mogu da budu javno objavljeni,
- zapisuju događaji koji se tiču:
- životnog ciklusa TSA ključeva za potpisivanje i sertifikata,
- sinhronizacije vremena TSA servera sa izvorom tačnog vremena,
- gubitka sinhronizacije vremena TSA servera sa izvorom tačnog vremena.

IX. Kompromitovanje usluge izdavanja vremenskog žiga

U slučaju kompromitovanja ili sumnje u kompromitovanje svog tajnog (privatnog) ključa ili poremećaja sistema kalibracije i sinhronizacije sa izvorom tačnog vremena, TSA telo Pošte:

- prestaje sa izdavanjem vremenskih žigova,
- informiše sve korisnike i druge zainteresovane strane o kompromitaciji i drugim događajima,
- javno objavljuje informacije o tome kako ustanoviti koji vremenski žigovi nisu važeći, na način da se ne ugrozi zaštita podataka o ličnosti.

X. Prestanak rada izdavaoca vremenskog žiga

TSA telo Pošte će obezbetiti da u slučaju prestanka rada potencijalna šteta korisnicima i trećim stranama bude minimalna, i da se održi mogućnost provere ispravnosti izdatih vremenskih žigova.

Pre prestanka rada, TSA telo Pošte će:

- obavestiti sve korisnike o prestanku rada,
- pouzdanoj organizaciji preneti obavezu čuvanja svih relevantnih podataka neophodnih za dokazivanje ispravnosti izdatih vremenskih žigova, u vremenskom periodu koji je propisan zakonom,
- pouzdanoj organizaciji preneti obavezu da TSA elektronski sertifikat koji sadrži javni ključ za proveru elektronskog potpisa izdatih vremenskih žigova bude raspoloživ svim zainteresovanim stranama, u vremenskom periodu koji je propisan zakonom,
- uništiti tajni (privatni) ključ TSA servera.

Zahvalnica

Rad je deo istraživanja koje finansira Ministarstvo prosvete i nauke Republike Srbije, projekti: III-45003 i TR-35026.

Literatura

[1] Zakon o elektronskom dokumentu ("Službeni glasnik Republike Srbije", br. 51/2009).

[2] Pravilnik o izdavanju vremenskog žiga ("Službeni glasnik Republike Srbije", br. 112/2009).

[3] Politika izdavanja vremenskog žiga Javnog preduzeća PTT saobraćaja "Srbija" kao izdavaoca vremenskog žiga ("Službeni PTT glasnik", br. 782/2012).

[4] Zakon o elektronskom potpisu ("Službeni glasnik Republike Srbije", br. 135/2004).

[5] D. Spasić, I. Lazarević, S. Milinković, B. Milojković, "Aplikacija za naplatu i evidentiranje izdatih vremenskih žigova Sertifikacionog tela Pošte", XXX simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2012", Zbornik radova, str. 149-158, Saobraćajni fakultet, Beograd, decembar 2012.

[6] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", August 2001.

[7] "Thales Time Stamp Server Administrator Guide", Thales e-Security, March 2012.

[8] "Barracuda Load Balancer Administrator's Guide Version 3.6", Barracuda Networks, 2011.

ABSTRACT

This paper describes the architecture and redundancy of TSA system that was built by Serbian Post. Issuance of time-stamp is explained as well as a lifecycle of TSA cryptographic keys. An overview of operational work of the TSA is given. Actions to be taken in the case of TSA's termination of its time-stamping services are listed in the end.

SERBIAN POST AS A TIME-STAMPING AUTHORITY

D. Spasić, S. Milinković, B. Milojković and Lj. Lazić