Sanja Prodan

Pošiljatelj: Tijana Licul
Poslano: 23. siječnja 2023. 8:29
Primatelj: Sanja Prodan
Predmet: FW: Odgovor na podnesak
Privici: Dopis_ocitovanje_ts_pazin_potpisano.pdf

Sutkinja Tijana Licul

REPUBLIKA HRVATSKA
TRGOVAČKI SUD U PAZINU
Držićevka 1
52000 Pazin

Tel: +385 (0)52 619-902
E-pošta: tijana.licul@tspa.pravosudje.hr
Web: http://sudovi.pravosudje.hr/tspa

From: Miroslav Bača <prof.dr.sc.miroslavbaca@gmail.com>
Sent: Saturday, January 21, 2023 7:57 AM
To: Tijana Licul <Tijana.Licul@tspa.pravosudje.hr>
Subject: Odgovor na podnesak

Poštovana sutkinjo Licul
U prilogu Vam dostavljam podnesak koji sam uplodao na sustav,
Ako je potrebno još što pojasniti molim da mi javite
Želim Vam ugodan vikend
Srdačno
M. Bača

* * * * * * * * * * * * * * * * * *

Prof dr sc Miroslav Bača
CLFE, CLCM, CSLPI, CLPTP, EPS
Stalni sudski vještak za informatiku telekomunikacije i biometriju
Bana Josipa Jelačića 13 HR-35400 Nova Gradiška
GSM +385(0)919436584

Prof.dr.sc. Miroslav Bača

Stani sudski vještak za biometriju, informatiku i telekomunikacije
Bana Josipa Jelačića13, 35400 Nova Gradiška
GSM:+385 (91)9436584 e-mail: miroslav.baca@me.com

Trgovački sud u Pazinu
4 S- 103/2018-1200
Držćevka 1
52 000 Pazin

OIB: 46543732715

Predmet: Dostava očitovanja

Poštovana sutkinjo Licul,

Temeljem dostavljenih podataka vezanih za podnesak gospodina Mate Ćurića od 05.12.2022, očitujem se kako slijedi:

ID nadmetanja: **35504** (završilo 02.03.2022. u 12:05:26.432)
ID ponuditelja: **28913** (korisnik 2728, Mato Ćurić)

1) Logovi koje je korisnik dostavio logovi su **Programske podrške za korištenje naprednog elektroničkog potpisa (Potpisni modul) koja je instalirana na korisničkom računalu.**

   U aplikaciji se naprednim elektroničkim potpisom potpisuje prijava u aplikaciju, prijava za sudjelovanje u nadmetanju, a u aplikaciji je moguće izvršiti i testni potpis (provjera funkcionira li potpisivanje).

   Proces potpisivanja prijave u aplikaciju izgleda ovako:

   a) nakon klika na gumb „*Nastavite s prijavom*" front-end dio web aplikacije e-Dražba od back-enda zatraži generiranje autorizacijskog ključa. Upit se prosljeđuje na servis PKIvalidacija (autorizacijski ključ kao i ID transakcije generira Finin servis PKIvalidacija – taj servis ne koristi samo e-Dražba nego i razne druge aplikacije)

   b) na osnovu dobivenog autorizacijskog ključa i ID-ja transakcije na korisničkom računalu se pokreće aplikacija Potpisni modul (aplikacija čije logove je korisnik dostavio)

Stalni sudski vještak za biometriju, informatiku i telekomunikacije
Bana Josipa Jelačića13, 35400 Nova Gradiška
GSM:+385 (91)9436584 e-mail: miroslav.baca@me.com

c) paralelno s pokretanjem Potpisnog modula i potpisivanjem, front-end dio web aplikacije e-Dražba započinje s periodičkom provjerom statusa potpisa (u logovima web servera vidljivo kao npr. /pki/get_status?authKey=5399448e...)

2) Nakon što je provjerom statusa potpisa utvrđeno da je proces potpisivanja završen, front-end na back-end šalje zahtjev za dohvat i provjeru potpisanih podataka – ako je potpis uspješan, korisniku se dozovoljava rad u aplikaciji dražbovanja.

Potpisni modul događaje na računalu zapisuje u dva loga:
`FinaPkiValidationServiceUpdateVersionApplet.log`
- Odnosi se na wrapper – zapisi vezani uz pokretanje aplikacije (provjera verzije itd.)

`XAdESAppletLogFile.log`
- Zapisi vezani uz pokretanje i rad specifičanog modula aplikacije koji je vezan uz XAdES tip potpisa (koristi se u e-Dražbi)

3) Treba napomenuti da je iz aplikativnog loga e-Dražbe vidljivo da sat na korisničkom računalu u to vrijeme konstantno <u>kasni</u> ~53 sekunde (podatak `timeDiff` koji se ispisuje prilikom određenih upita, usporedba vremena u logu i podatka clientTime,...). pa to treba imati u vidu prilikom analize vremena zabilježenih u logovima korisničkog računala. To kašnjenje sata svakako <u>nema utjecaja</u> na tijek nadmetanja, budući da se vremena u aplikaciji e-Dražba ne ravnaju prema satu na korisničkom računalu nego se usklađuju sa serverskim realnim vremenom.

4) Iz logova `Potpisnog modula` koje je korisnik skenirao i priložio u PDF dokument može se zaključiti sljedeće:

- U 09:57:53.867 prema satu na korisničkom računalu (tj. u ~09:58:46 prema serverskom vremenu) pokreće se na korisničkom računalu aplikacija Potpisni modul. Kako bi se Potpisni modul mogao pokrenuti, prethodno je trebao biti generiran autorizacijski ključ. Iz zapisa u aplikativnom logu e-Dražbe i u logovima web servera (webp3) vidljivo je da je autorizacijski ključ u tom slučaju zatražen (zapis „`INVOKED generateAuthKey...`" u aplikativnom logu e-Dražbe)
- u 09:58:36 prema serverskom vremenu. Dakle, 10-tak sekundi prije pokretanja aplikacije `Potpisni modul` generiran je autorizacijski ključ (to trajanje često ovisi i o samom korisniku, budući da računalo uobičajeno traži potvrdu korisnika da smije otvoriti drugu aplikaciju na zahtjev iniciran iz preglednika). Nakon toga uredno se izvršava potpisivanje.

Prof.dr.sc. Miroslav Bača

Stani sudski vještak za biometriju, informatiku i telekomunikacije
Bana Josipa Jelačića13, 35400 Nova Gradiška
GSM:+385 (91)9436584 e-mail: miroslav.baca@me.com

- Slično je i s procesom potpisivanja koji je započet u 12:09:28 (12:08:35 prema satu na korisničkom računalu) – Iz korisnikovog loga je vidljivo da se Potpisni modul uredno pokrenuo u 12:08:38 prema satu na korisničkom računalu, tj. u 12:09:31 prema satu na serveru – 3 sekunde nakon klika na gumb „*Nastavite s prijavom*".

5. U dostavljenim preslikama logova s korisničkog računala uočen je po jedan neobičan zapis:

   U datoteci `FinaPkiValidationServiceUpdateVersionApplet.log` zabilježen je zapis „...Pokrenut main appleta" s vremenom 12:05:21.412 (prema serverskom vremenu bi to bilo ~**12:06:14**). Nakon toga bi u nekoliko desetaka milisekundi trebao u istom logu uslijediti zapis „...*Pokrenut start appleta*", međutim, tog zapisa nema. Unatoč tome, u `XAdESAppletLogFile.log` datoteci u 12:05:27.184 također postoji zapis „...*Pokrenut mail appleta*", no nakon toga niti u tom logu nema niti jednog drugog zapisa koji bi bio vezan uz taj proces. Inače se logovi u `XAdESAppletLogFile.log` datoteci počinju zapisivati nekoliko sekundi nakon što se u `FinaPkiValidationServiceUpdateVersionApplet.log` datoteci ispiše „...*Pokrenut start appleta*" (u ovom slučaju tog zapisa uopće nema u to vrijeme). Kako je iz dostavljenih log zapisa FINA vidljivo u periodu između 11:31 i 12:09:22 s korisnikove IP adrese prema `edrazba.fina.hr` nije upućen niti jedan upit, a aplikacija `Potpisni modul` pokreće se tek na osnovu generiranog autorizacijskog ključa i ID-ja transakcije.

   Uočavam da bi se gore spomenuto vrijeme 12:05:21.412 koje je navedeno u zapisu u logu na korisničkom računalu odnosilo još uvijek na period trajanja dražbe (5s prije završetka) da je sat na računalu bio usklađen sa serverskim vremenom. Budući da treba uračunati razliku od ~53s, taj zapis se mogao odnositi jedino na period **nakon što je dražba već završila**. No, kao što je navedeno, tom zapisu ne prethodi serversko generiranje autorizacijskog ključa koje je nužno za pokretanje Potpisnog modula.

6. Napominjem da logovi Potpisnog modula na korisničkom računalu **nisu kriptirani**, to konkretno znači da se ne može jamčiti njihova autentičnost te da ih je lako modificirati.

7. Dodatno, što se tiče zapisa u logovima Potpisnog modula u kojima je zabilježena riječ „*Greška*", ne radi se o pogrešci u radu aplikacije za dražbovanje već o načinu detekcije kripto uređaja (i pripadajućeg middlewarea) koji korisnik koristi na svom računalu a što spada u normalan rad te aplikacije.

Prof.dr.sc. Miroslav Bača

Stani sudski vještak za biometriju, informatiku i telekomunikacije
Bana Josipa Jelačića13, 35400 Nova Gradiška
GSM:+385 (91)9436584 e-mail: miroslav.baca@me.com

Zaključno:

Dostavljeni log zapisi ne odnose se na rad aplikacije za dražbovanje već za sustav koji se koristi za identifikaciju korisnika a koji se uz aplikaciju za dražbovanje koristi i za različite druge servise. Radi se o programskoj podršci za korištenje naprednog elektroničkog potpisa a koja je instalirana na korisničkom računalu. Aplikacija za dražbovanje nema nikakav utjecaj na rad aplikacije za korištenje naprednog elektroničkog potpisa. Vidljivo je da sat korisnika u odnosu na realno vrijeme kasni 53 sekunde (pod pretpostavkom da su podaci koji su dostavljeni u podnesku autentični). To znači da je korisnik izvršio određene radnje tek po isteku vremena nakon zaključenja procesa dražbovanja.

U odnosu na sam podnesak zaključujem kako se dostavljeni podaci odnose na aplikaciju za korištenje naprednog elektroničkog potpisa a ne na aplikaciju za dražbovanje stoga u cijelosti ostajem kod nalaza i mišljenja koji sam dostavio ovom Sudu.

Srdačno,

Nova Gradiška, 21.01.2023.

Stalni sudski vještak:

Prof.dr.sc. Miroslav Bača
CLFE, CLCM, CSLPI, CLPTP, EPS

MIROSL
AV BAČA

Digitally signed by MIROSLAV BAČA
Date: 2023.01.21 07:51:22 +01'00'