KLASA: UP/I 034-03/19-01/023
URBROJ: 580-10/63-2021-031
Zagreb, 3. ožujka 2021.

Agencija za zaštitu tržišnog natjecanja, na temelju članka 30. točke 2., članka 31. i članka 58. stavka 1. točke 13. Zakona o zaštiti tržišnog natjecanja („Narodne novine“, br. 79/09. i 80/13.), postupajući po inicijativi poduzetnika yottabyte j.d.o.o., sa sjedištem u Velikoj Gorici, Zagrebačka 126, za pokretanje postupka utvrđivanja sprječavanja, ograničavanja ili narušavanja tržišnog natjecanja zlouporabom vladajućeg položaja protiv poduzetnika Agencija za komercijalnu djelatnost proizvodno, uslužno i trgovačko d.o.o., sa sjedištem u Zagrebu, Savska cesta 31, po službenoj dužnosti, na temelju odluke Vijeća za zaštitu tržišnog natjecanja u sastavu: Vesna Patrlj, dipl. iur., zamjenica predsjednika Vijeća, dr. sc. Mirta Kapural, Denis Matić, dipl. iur. i mr. sc. Ljiljana Pavlic, članovi Vijeća, sa sjednice 6/2021., održane 3. ožujka 2021., donosi sljedeće

RJEŠENJE

Utvrđuje se da Agencija za komercijalnu djelatnost proizvodno, uslužno i trgovačko d.o.o. sa sjedištem u Zagrebu, Savska cesta 31, nije spriječila, ograničila ili narušila tržišno natjecanje zlouporabom vladajućeg položaja na mjerodavnom tržištu distribucije međusoftvera za elektroničku osobnu iskaznicu, u smislu članka 13. Zakona o zaštiti tržišnog natjecanja.

Obrazloženje

1. Inicijativa za pokretanje postupka

Agencija za zaštitu tržišnog natjecanja (dalje u tekstu: AZTN) zaprimila je 3. prosinca 2019., sukladno članku 37. Zakona o zaštiti tržišnog natjecanja („Narodne novine“, br. 79/09 i 80/13; dalje u tekstu: ZZTN), inicijativu poduzetnika yottabyte j.d.o.o., sa sjedištem u Velikoj Gorici, Zagrebačka 126 (dalje u tekstu: yottabyte i/ili podnositelj inicijative), za pokretanje postupka utvrđivanja zlouporabe vladajućeg položaja protiv poduzetnika Agencija za komercijalnu djelatnost proizvodno, uslužno i trgovačko d.o.o., sa sjedištem u Zagrebu, Savska cesta 31, zastupanog po odvjetnicima iz Odvjetničkog društva [...] (dalje u tekstu: AKD).

U predmetnoj se inicijativi navodi kako je prema Zakonu o osobnoj iskaznici svaki državljanin Republike Hrvatske obvezan s AKD-om sklopiti ugovor o obavljanju usluga certificiranja. Također, da bi koristio svoj virtualni identitet, odnosno eOI - elektroničku osobnu iskaznicu, korisnik je dužan preuzeti i instalirati AKD-ov programski paket eID Middleware.

Kao isporučitelj tog softvera, prema mišljenju podnositelja inicijative, AKD je dužan objaviti specifikaciju programskog sučelja, odnosno pojasniti kako se taj programski paket koristi, no AKD odbija objaviti tehničke specifikacije.

Podnositelj inicijative posebno skreće pozornost na Signer.exe komponentu, koja je pokrenuta kao servis na računalu i stalno zauzima port 5555 te troši sistemske resurse računala korisnika. Prema njegovom mišljenju, isporučitelj je dužan opisati način korištenja web servisa, kako se oni pozivaju, s kojim parametrima te što je njihov rezultat.

Dodaje kako u potpunosti poštuje autorsko pravo AKD-a i trećih strana nad programskim paketom eID Middleware te ga promatra kao „crnu kutiju“, bez zadiranja u izvršni i izvorni kod. Međutim, smatra kako nema pravne osnove da isključivo pravo korištenja tog softvera ima AKD te bi zbog zaštite tržišnog natjecanja AKD trebao objaviti aplikacijska programska sučelja (eng. *API - application programming interface*) eID Middlewarea.

Nadalje, podnositelj inicijative navodi da AKD pruža komercijalne usluge bazirane na eID Middleware komponenti, gdje za njeno korištenje navodi inicijalnu naknadu od 35.000,00 kuna, a zatim se, ovisno o broju potpisanih dokumenata, dodatno plaća naknada za korištenje tog servisa do 200.000,00 kuna godišnje. Podnositelj inicijative smatra kako je takav iznos nerazmjeran pruženoj i još k tome nepotrebnoj, a moguće i nelegalnoj usluzi posredovanja u apliciranju digitalnog potpisa. Pri tome ističe kako treba imati na umu da je taj program već u potpunosti plaćen javnim novcem.

Monopolom nad eID Middleware softverom, AKD se, prema mišljenju podnositelja inicijative, dovodi u povlaštenu poziciju ekskluzivnog korištenja javne IT infrastrukture, očekujući značajna financijska sredstva od posredništva kod apliciranja digitalnog potpisa na dokumente. Tehničkim i financijskim zaprekama, smatra podnositelj inicijative, AKD onemogućava razvoj eko sustava baziranog na javnoj IT infrastrukturi i značajno usporava digitalizaciju Republike Hrvatske, kao i razvoj informatičkih usluga s dodanom vrijednošću baziranih na digitalnom identitetu građana. Također, povrijeđena su i načela Zakona o državnoj informacijskoj infrastrukturi, pogotovo u segmentu interoperabilnosti.

Podnositelj inicijative smatra važnim istaknuti kako postoji besplatna *open source* verzija potpisne komponente bazirana na referentnoj implementaciji elektroničkog potpisa Europske unije, zvana DSS (eng. *Digital Signature Services*). DSS nudi i biblioteke za digitalni potpis razvijene kroz CEF inicijativu (eng. *The Connecting Europe Facility*). Imajući to u vidu, smatra podnositelj inicijative, kako AKD-ov razvoj vlastitog rješenja služi samo tome da isključivo on može koristiti komponentu digitalnog potpisa i to onda komercijalno naplaćivati.

Primjer ranije navedenog AKD-ovog ePotpisa jest, između ostaloga, i usluga „e-Zahtjev za izdavanje vozačke dozvole“ na mrežnim stranicama Ministarstva unutarnjih poslova, kada nakon 12 provedenih koraka i formirane PDF datoteke dolazi do preusmjeravanja korisnika na mrežne stranice AKD-a, gdje se dokument potpisuje korištenjem eID Middleware komponente za potpis, odnosno eSigner servisa.

Podnositelj inicijative ističe da se u slučaju preusmjeravanja radi o značajno kompleksnijem rješenju u odnosu na rješenje da se na samim stranicama MUP-a obavi digitalno potpisivanje dokumenta, bez ikakve potrebe za preusmjeravanjem na stranice AKD-a, naravno kada bi specifikacija komponente za potpis bila dostupna odnosno kada bi ona proslijedila potpis koji generira čip na samoj osobnoj iskaznici.

U samom navedenom postupku izdavanja vozačke dozvole elektroničkim putem, smatra podnositelj inicijative, AKD ne dodaje nikakvu dodanu vrijednost niti preuzima bilo kakvu odgovornost u pravnom poslu u kojem posreduje za apliciranje digitalnog potpisa na dokument pa je, osim AKD-ove želje za naplatom naknada za potpisivanje, nejasno zašto bi uopće AKD trebao u tome sudjelovati. Upitno je zašto bi poduzetnik u državnom vlasništvu želio ostvarivati profit, i to čak i na račun toga da građane te iste države drži digitalno nepismenima.

Osim za javne usluge u sustavu e-Građana, smatra podnositelj inicijative, eOI bi se svakako trebao koristiti u bilo kojoj prilici kada je potrebno u virtualnom svijetu nepobitno dokazati identitet osobe i digitalnim potpisom ovjeriti sadržaj, bilo da je pružatelj usluge javna institucija ili privatni poduzetnik.

Kao postojeću sudsku praksu, podnositelj inicijative navodi odluku Europske komisije u sporu s Microsoftom (predmet COMP/C-3/37.792 Microsoft), gdje je Europska komisija zaključila kako je nužno omogućiti interoperabilnost s operativnim sustavom Windows trećim stranama korištenjem tehničke specifikacije sučelja odnosno objavom API-ja.

Zaključno, podnositelj inicijative navodi kako je 8. kolovoza 2019. AKD-u preporučenom pošiljkom uputio dopis za objavu tehničkih specifikacija komponente za digitalno potpisivanje dokumenata, međutim AKD odbija bilo kakvu komunikaciju i nije voljan dostaviti API pa je posebno potrebno spomenuti kršenje članka 102. Ugovora o funkcioniranju Europske unije (Službeni list C 115, 9. svibnja 2008.; dalje u tekstu: UFEU) i članka 54. Sporazuma o Europskom gospodarskom prostoru (Službeni list L1, 3. siječnja 1994.).

2. Prethodno ispitivanje stanja na mjerodavnom tržištu

Na temelju predmetne inicijative, kako bi utvrdio ima li u konkretnom slučaju uvjeta za pokretanje postupka utvrđivanja sprječavanja, ograničavanja ili narušavanja tržišnog natjecanja sukladno odredbama članka 38. stavka 1. i stavka 3. te članka 39. ZZTN-a, a vezano uz primjenu članka 13. ZZTN-a, AZTN je u okviru svoje nadležnosti iz članka 32. točki 1. a) i b) ZZTN-a zatražio očitovanje, podatke i relevantnu dokumentaciju od poduzetnika AKD, podnositelja inicijative te poduzetnika [...] (dalje u tekstu: [...]).

2.1. Očitovanje AKD-a

AZTN je 17. siječnja 2020. zaprimio očitovanje poduzetnika AKD, u kojem se navodi kako je eID Middleware aplikacija / driver koju je AKD napravio za upotrebu s elektroničkom osobnom iskaznicom (eOI), a koja osobama koje imaju eOI omogućava sigurno korištenje elektroničkih certifikata na elektroničkom nosaču.

AKD eID Middleware ustupljen je bez naknade na korištenje svim osobama koje posjeduju eOI te je kompatibilan i može se koristiti sa standardnim aplikacijskim programskim sučeljem PKCS#11. PKCS je *Public-Key Cryptography Standard*, a PKCS#11 je standardno API sučelje kojem se pristupa sigurnim kriptografskim uređajima kakav je i eOI. Standard PKCS#11 definira aplikacijsko programsko sučelje (API) za rad s kriptografskim uređajima, koje je neovisno o platformi (operativnom sustavu računala), što uključuje i rad s pametnim karticama, kakva je i eOI.

Taj API definira najčešće korištene kriptografske tipove objekata (RSA ključevi, X.509 certifikati, DBS / Triple DBS tipke itd.) i sve funkcije potrebne za upotrebu, stvaranje / generiranje, izmjenu i brisanje tih objekata.

AKD eID Middleware kompatibilan je i može se koristiti sa standardnim aplikacijskim programskim sučeljima MS-CAPI. Sučelje za kriptografsko programiranje specifično za Microsoft Windows platformu (također poznato i kao CryptoAPI, Microsoft Cryptography API, MS-CAPI ili jednostavno CAPI) jest sučelje aplikacijskog programiranja koje je uključeno u operacijske sustave Microsoft Windows za omogućavanje zaštite Windows aplikacija korištenjem kriptografije. To je skup dinamički povezanih biblioteka koje pružaju sloj apstrakcije koji programere izolira od koda koji se koristi za šifriranje podataka.

AKD navodi kako ne koristi javnu IT infrastrukturu te nema govora o monopolu korištenja javne infrastrukture, a sve osobe imatelji eOI-ja mogu korištenjem besplatnih alata poput Adobe

Acrobat Readera ili DSS servisa Europske unije bez naknade izrađivati elektroničke potpise na svojim računalima. AKD ne dobiva nikakva financijska sredstva na ime posredništva kod izrade elektroničkih potpisa korištenjem eOI-ja. eOI (točnije certifikate) može koristiti bilo koja aplikacija, i to putem PKCS#11 i MS-CAPI sučelja za koje se podrška isporučuje s instalacijom Windowsa.

Kao dokaz navedenom, AKD navodi uslugu e-Porezna, gdje se koriste certifikati putem PKCS#11 sučelja za potrebe izrade elektroničkog potpisa s eOI karticama podržanim eID Middleware driverom. Također, Adobe Reader jest primjer upotrebe eOI certifikata u aplikaciji korisnika implementacijom MS-CAPI sučelja. Prema navodima AKD-a, Signer.exe je servisna aplikacija koja izdavatelju certifikata omogućava alternativni način komunikacije s karticom te njena specifikacija ne može biti objavljena bez potencijalnog ugrožavanja sigurnosti kartice i podataka na njoj. Nadalje, njenom objavom ne bi bila omogućena nikakva dodatna funkcionalnost vezana za potpisivanje certifikatima s eOI-ja koja već nije javno dostupna.

AKD smatra kako je iz gore navedenog razvidno da nije tehničkim i financijskim zaprekama onemogućio digitalizaciju Republike Hrvatske, kako to navodi podnositelj inicijative.

Nadalje, AKD navodi kako je eOI kartica u osnovi hardverski uređaj, pri čemu eID Middleware aplikacija djeluje kao driver za karticu. Stoga ga može koristiti svaka standardna implementacija elektroničkog potpisa, bez ikakve dogradnje za koju je potrebno posjedovanje traženih tehničkih specifikacija.

Pružatelji usluga koji žele koristiti eOI za izradu elektroničkog potpisa mogu korištenjem standardiziranih PKCS#11 ili MS-CAPI sučelja, čije su specifikacije javno objavljene i dostupne na internetu i putem eID Middleware softvera, pristupati i koristiti svoje certifikate na iskaznici. Navedena standardna i javna sučelja (PKCS#11 ili MS-CAPI) mogu bez ograničenja koristiti svi koji žele u svojim aplikacijama implementirati elektroničko potpisivanje certifikatima s eOI-ja.

AKD-ova eID Middleware aplikacija djeluje kao driver za karticu koji omogućava korištenje autentikacijskog i potpisnog certifikata koji su pohranjeni u elektroničkom nosaču podataka. Bez eID Middleware aplikacije / drivera nije moguće korištenje certifikata na eOI-ju, kao što bez pripadajućeg drivera nije moguće korištenje gotovo niti jedne računalne hardverske komponente. eID Middleware se koristi uvijek kad se koristi autentikacijski ili potpisni certifikat pohranjen u elektroničkom nosaču podataka eOI-ja.

AKD navodi kako eID Middleware nije rješenje za izradu elektroničkih potpisa, poput DSS rješenja, kako bi se dalo zaključiti iz inicijative, te ne služi tome, kako se u inicijativi navodi, da samo AKD može koristiti komponentu digitalnog potpisa i komercijalno ju naplaćivati, jer se za korištenje eID Middleware komponente u svim scenarijima korištenja ne plaća naknada, uključujući i za korištenje komponente Signer.exe.

eID Middleware softver za eOI spada u kategoriju driver aplikacija i obveza je proizvođača da korisnicima koji žele koristiti elektroničke certifikate pohranjene na elektroničkom nosaču podataka osigura taj driver (eID Middleware) kako bi mogli na siguran način pristupati i koristiti svoje elektroničke certifikate. eID Middleware nije zamjena za DSS servis izrade i validacije elektroničkih potpisa i obrnuto, već upravo suprotno, bez eID Middlewarea osobe imatelji eOI-ja ne bi mogli potpisivati dokumente korištenjem DSS servisa niti korištenjem Adobe Readera ili drugih potpisnih rješenja.

AKD navodi kako nije uspio pronaći da je neki izdavatelj certifikata u Republici Hrvatskoj (Financijska agencija, Zagrebačka banka) i u Europskoj uniji javno objavio specifikacije driver aplikacija (eID Middleware) i pomoćnih programa za web potpisivanje, poput programa eSigner.

elD Middleware omogućuje, pomoću standardiziranih PKCS#11 ili MS-CAPI sučelja, čije su specifikacije javno objavljene i dostupne na internetu, koristiti eOI s bilo kojim rješenjem za izradu elektroničkih potpisa. Signer.exe program, koji omogućava sigurno korištenje eOI-ja u internetskim preglednicima, korisnik može isključiti ako koristi elektroničke certifikate eOI-ja putem drugih programa, poput Adobe Acrobat Readera ili DSS usluge.

Kao dokaz, AKD navodi najčešće korišteni alat za potpisivanje PDF dokumenata, besplatni program Adobe Acrobat Reader, s kojim je, bez korištenja spornog programa Signer.exe, a korištenjem standardiziranih PKCS#11 ili MS-CAPI biblioteka, omogućeno korištenje eOI-ja za izradu elektroničkih potpisa, što se ne može jednostavno dokazati pisanim putem, ali ako je potrebno može se demonstrirati i dokazati na bilo kojem podržanom računalu. AKD je dao prikaz kako Adobe Acrobat Reader, korištenjem Windows sučelja za digitalne ID-ove (MS-CAPI) i PKCS#11, omogućava besplatno korištenje eOI-ja.

Također, korištenjem standardiziranih PKCS#11 ili MS-CAPI biblioteka i korištenjem u inicijativi spomenutog DSS servisa, ali i s mnogim drugim besplatnim i komercijalnim rješenjima za izradu elektroničkog potpisa koji se nalaze na tržištu, omogućena je izrada elektroničkih potpisa svim državljanima Republike Hrvatske koji su aktivirali elektroničke certifikate na svojoj osobnoj iskaznici, što se, ako je potrebno, također može demonstrirati i dokazati na bilo kojem računalu.

AKD dalje navodi kako, suprotno navodima iz inicijative, elD Middleware ne koristi „isključivo AKD“. AKD u stvari ne koristi taj program, već ga je besplatno dao na korištenje imateljima eOI-ja.

Također, podnositelj inicijative pogrešno je povezao komercijalni proizvod kID Middleware, koji se nalazi na tržištu, i besplatni proizvod elD Middleware, koji se koristi s elektroničkim osobnim iskaznicama (eOI).

Državljani Republike Hrvatske, imatelji eOI-ja, koriste drugi program, besplatni elD Middleware (koji niti nije tržišni proizvod). AKD prilaže dokaz da se radi o pogrešno ustanovljenom činjeničnom stanju, što se lako može utvrditi uvidom u sadržaj komercijalne mrežne stranice AKD-a, s koje se preuzima paket kID Middleware (https://id.hr/hr/podrska/download-obiave), a ne elD Middleware, kako tvrdi podnositelj inicijative.

Nadalje, AKD navodi kako ne koristi javnu IT infrastrukturu, niti kad imatelji eOI-ja koriste certifikate s eOI-ja za autentikaciju ili izradu elektroničkih potpisa, niti kad kupci koriste komercijalni servis ePotpis. U oba slučaja koristi se IT infrastruktura AKD-a i vlastita računala fizičkih ili pravnih osoba. Budući da se državna informacijska infrastruktura ne koristi, nisu niti povrijeđena načela Zakona o državnoj informacijskoj infrastrukturi.

Nadalje, AKD navodi kako nije točno da se tehničkim i financijskim preprekama, kako tvrdi podnositelj inicijative, onemogućava razvoj eko sustava baziranog na javnoj infrastrukturi, niti da se usporava digitalizacija Republike Hrvatske. U inicijativi je naveden primjer kako je prilikom korištenja servisa e-Zahtjeva za izdavanje vozačke dozvole za izradu elektroničkog potpisa potrebna naknada AKD-u, što ne stoji, jer se za izradu potpisa u tom servisu i u svim prethodno navedenim servisima u sustavu e-Građani ne naplaćuje naknada.

Pored toga, naglašava AKD, ne stoji niti činjenica iz inicijative da u postupku e-Zahtjeva AKD ne dodaje nikakvu vrijednost, budući da se za izradu elektroničkog potpisa koristi AKD-ova IKT infrastruktura bez naknade.

Republika Hrvatska među prvih je 6 članica Europske unije čije je identifikacijsko sredstvo najviše razine povjerenja (eOI) prepoznato kao nacionalno identifikacijsko sredstvo (eID) koje moraju prihvatiti sve države članice Europske unije za „korištenje u virtualnom svijetu za nepobitno dokazivanje identiteta osobe“, u što se lako uvjeriti uvidom u Službeni list Europske unije C 309/9, od 13. rujna 2019., pod nazivom Obavijesti država članica, Sustavi elektroničke identifikacije prijavljeni u skladu s člankom 9. stavkom 1. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (2019/C 309/09), kao i na mrežnoj adresi Europske komisije na kojoj su objavljena priznata identifikacijska sredstva država članica Europske unije.

Dakle, ističe AKD, upravo je Europska komisija navela Republiku Hrvatsku kao primjer jedne od prvih 6 članica Europske unije koje su omogućile građanima da koriste svoje nacionalno identifikacijsko sredstvo za prekograničnо korištenje europskih elektroničkih javnih servisa.

EID Middleware je dokumentiran korisničkim uputama za instalaciju i korištenje te je besplatan za korištenje svim imateljima eOI-ja i upravo se njegovim korištenjem ubrzava digitalizacija Republike Hrvatske, što je vidljivo i iz sve većeg broja državnih servisa kojima se putem Nacionalnog identifikacijskog i autentifikacijskog sustava (dalje u tekstu: NIAS), unutar sustava e-Građani, može pristupiti s eOI-jem i u kojima se on može koristiti. Na eOI portalu imatelji eOI-ja imaju i mogućnost prijave eventualnih problema ili upita vezano za korištenje eOI-ja.

AKD je kao pružatelj usluga povjerenja, sukladno Uredbi (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Zakonu o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, koji je Hrvatski sabor donio na sjednici 19. lipnja 2017., te sukladno Pravilniku o pružanju i korištenju usluga povjerenja, svake godine auditiran od tijela za ocjenu sukladnosti s eIDAS uredbom te je svaki puta uspješno prošao nadzor, što je vidljivo iz eIDAS certifikata koji su javno dostupni na internetu.

2.2. Očitovanje podnositelja inicijative

Na navode AKD-a iz podneska zaprimljenog 17. siječnja 2020., podnositelj inicijative očitovao se podneskom zaprimljenim 21. veljače 2020.

Podnositelj inicijative ističe kako nisu točni navodi AKD-a da je eID Middleware aplikacija / driver. Riječ je o programskom paketu, odnosno instalacijskom čarobnjaku koji omogućuje instalaciju pet komponenti, što je jasno vidljivo iz PDF dokumenta „eOI Middleware upute za instalaciju“.

Yottabyte dalje navodi kako, bez obzira na to što je AKD eID Middleware bez naknade dan na korištenje svim osobama koje posjeduju eOI, to ne znači da proizvođač tog softvera nije dužan omogućiti interoperabilnost prema drugim stranama i ne objaviti REST WS API Signer.exe komponente.

Navod AKD-a kako je Signer.exe servisna aplikacija koja izdavatelju certifikata omogućava alternativni način komunikacije s karticom apsolutno je točna i tu je prema podnositelju inicijative i bit problema jer ona nije dostupna za korištenje drugim poduzetnicima iako nema razloga da tome ne bude tako. Navod kako bi objava specifikacije REST WS API Signer.exe komponente ugrožavala sigurnost kartice i podataka na njoj nije točna jer, kako kasnije i sam AKD navodi, i DSS servis omogućava potpisivanje putem weba pa niti na koji način ne ugrožava sigurnost kartice i podataka na njoj.

Nadalje, podnositelj inicijative smatra točnom i tvrdnju AKD-a da objavom specifikacije ne bi bila omogućena nikakva funkcionalnost vezana za potpisivanje certifikatima s eOI-ja, a koja već nije javno dostupna, ali putem druge programske podrške. AKD sam navodi da postoje alternative eOI Signer.exe komponenti te pritom pogrešno navodi program Adobe Acrobat Reader, s obzirom na to da je Adobe Acrobat Reader desktop aplikacija i ne služi kao podrška za digitalni potpis te svakako nije alternativa web aplikacijama. DSS servis predstavlja web aplikaciju koja omogućava digitalno potpisivanje oslanjanjem na NexU komponentu koja je pandan Signer.exe komponenti te upravo pruža REST WS API koji omogućava dohvat certifikata s pametne kartice, kao i prosljeđivanje sadržaja na kriptiranje privatnim ključem koji obavlja pametna kartica.

Podnositelj inicijative ističe kako Signer.exe komponenta ne može biti „trojanski konj“ odnosno stražnja vrata (eng. *backdoor*) putem kojih isključivo AKD preko web aplikacije ima mogućnost komunikacije s pametnom karticom, čime se dovodi u prednost u tržišnom natjecanju.

Upravo je u tome i bit inicijative jer sama Signer.exe komponenta dolazi u sklopu eOI Middleware paketa te je već unaprijed zadana za instalaciju (eng. *by default*), zajedno sa svim ostalim komponentama, čime AKD dolazi u prednost pred ostalim hrvatskim, europskim i ostalim poduzetnicima jer su u tom slučaju korisnici eOI-ja već instalirali programsku podršku za apliciranje digitalnog potpisa u web aplikacijama, s kojom jedino i isključivo upravlja AKD, dok bi ostali poduzetnici trebali korisnika navoditi da pored već instalirane Signer.exe komponente instalira i, primjerice, programsku podršku za DSS servis tj. NexU komponentu, a što je dodatna tehnička zapreka.

Podnositelj inicijative dalje navodi praksu Europske komisije u predmetu T-201/04 protiv poduzetnika Microsoft, iz koje je razvidno da dominantni poduzetnici imaju posebnu odgovornost osigurati da njihov način poslovanja ne sprječava konkurenciju i koristi i ne šteti potrošačima i inovacijama. U konkretnom slučaju Microsoft je morao obustaviti isporuku programa za reprodukciju multimedije Windows Media Player u kompletu s operativnim sustavom Windows. Za monopolističko ponašanje u navedenom slučaju Europska komisija odredila je kaznu od 497.2 milijuna eura.

S obzirom na to da program Signer.exe nije nužno potreban za pružanje usluge certificiranja i da postoje alternative (primjerice *open source* NexU program), podnositelj inicijative smatra kako AKD treba ili obustaviti distribuciju te komponente zajedno s ostalim komponentama potrebnim za rad eOI-ja ili omogućiti svima jednake uvjete korištenja navedene komponente.

Dodatno, yottabyte ističe i notu Europske komisije upućenu poduzetniku Microsoft vezano uz isporuku programa Internet Explorer, gdje se također vidi povreda tržišnog natjecanja. No za razliku od Internet Explorera, koji po tvrdnjama poduzetnika Microsoft predstavlja jezgreni dio operativnog sustava Windows, Signer.exe nije neophodan za pružanje usluge certificiranja, mada je ta komponenta itekako korisna jer omogućava apliciranje digitalnog potpisa u web aplikacijama pa bi u interesu cjelokupnog hrvatskog gospodarstva bila objava REST WS API-ja.

Nadalje, navod AKD-a kako nije uspio pronaći javno objavljene specifikacije pomoćnih programa za web potpisivanje, poput njegovog programa Signer.exe, očigledno je netočan i neistinit kada i sam AKD navodi DSS servis koji je u potpunosti otvorenog izvornog koda, kao i komponenta tog servisa koja je pandan Signer.exe program NexU. NexU je besplatna *open source* verzija potpisne komponente bazirana na referentnoj implementaciji elektroničkog potpisa DSS.

Podnositelj inicijative navodi kako je Signer.exe uistinu servisna aplikacija, koja nažalost isključivo izdavatelju certifikata omogućava alternativni način komunikacije s karticom, te

apsolutno nikako ne ugrožava sigurnost kartice i podataka na njoj, već isključivo služi kao premosnica (eng. *proxy*) između web aplikacija i same pametne kartice.

Podnositelj inicijative navodi kako je njegova supruga pod njegovim nadzorom izvršila testiranje navedenog DSS servisa te je evidentno kako je dokument potpisan „identifikacijskim“, a ne „potpisnim“ certifikatom, dok AKD navodi kako je DSS servis izradio elektronički potpis korištenjem potpisnog certifikata.

Suprotno navodima AKD-a, Signer.exe u stvari nije driver aplikacija, već zasebna komponenta, što je i ranije konstatirano. AKD točno navodi kako Signer.exe omogućava da preglednici na siguran način dozvoljavaju pristupanje i korištenje s elektroničkim certifikatima na eOI-ju te kako je takvo rješenje potrebno nakon zabrana *Java appleta* u internetskim preglednicima i kako bez njega oni ne bi dozvoljavali rad s eOI-jem. Podnositelj inicijative smatra kako je stoga pitanje zašto bi onda za digitalno potpisivanje putem interneta tu komponentu koristio isključivo AKD, a ne i HT, Zagrebački Holding, Vodovod i odvodnja, Plinara, HEP, vrtići, škole i svi ostali s kojima fizičke i pravne osobe potpisuju ugovore i drugu dokumentaciju.

Tvrdnja AKD-a, cit: „*Ako neka osoba nema potrebu potpisivanja dokumenata u web preglednicima slobodno može isključiti Signer.exe program/Signer.exe servis*“, prema podnositelju inicijative, u najmanju je ruku sramotna u 21. stoljeću, kada je računarstvo u oblacima postalo uobičajeno i kada se događa digitalna transformacija gospodarstva.

Tvrdnja AKD-a, cit: „*AKD eID Middleware ne koristi „isključivo AKD“, AKD u stvari ne koristi taj program, već ga je besplatno dao na korištenje osobama imateljima eOI.“*, nastavlja yottabyte, teško vrijeđa zdrav razum s obzirom na to da AKD nikome nije dostavio API programa Signer.exe, a upravo AKD korištenjem komponente Signer.exe posreduje u apliciranju digitalnog potpisa u slučaju potpisivanja zahtjeva za izdavanje vozačke dozvole, putovnice ili prijave novorođenčeta te je isto navedeno u uputama za pobrojane eUsluge.

Podnositelj inicijative dalje navodi kako se AKD služi različitim smicalicama kako bi zadržao povlašteni položaj. Jedan od tih trikova jest da taj jedan te isti softver koji se kod instalacije prikazuje kao eID Middleware, u slučaju kada ga distribuira kao javnu infrastrukturu naziva eOI Middleware, a u slučaju kada traži značajna financijska sredstva naziva kID Middleware.

Dokaz tome upravo je na stranici koju AKD navodi za preuzimanje „komercijalnog“ kID Middleware paketa (https://id.hr/hr/podrska/download-objave). U dijelu „Korisničke upute“ vidljiva je poveznica naziva „Upute za korištenje softvera, PDF“ te „Upute za Windows instalaciju, PDF“. Uvidom u same instalacijske upute, ističe yottabyte, evidentno je da se radi o istom softveru koji je objavljen kao „nekomercijalan“ eOI Middleware, odnosno da se radi o eID Middleware softveru.

Nadalje, podnositelj inicijative navodi kako je prilikom usporedbe eOI-ja i kID-a evidentno da se radi o istom softveru. AKD jednom prilikom softver naziva eOI, a to je kada radi za javne i državne tvrtke, a kID kada taj isti softverski paket nudi uz značajne naknade. Softver je stvarnog naziva eID Middleware, kako i stoji na instalacijskom čarobnjaku. U oba poslovna slučaja (naplata od državnog sektora odnosno naplata od privatnog sektora), a zapravo se radi o jednom proizvodu, AKD ima monopol nad korištenjem komponente Signer.exe, iako bi u oba poslovna slučaja AKD trebao omogućiti interoperabilnost odnosno objaviti API. Upute za instalaciju identične su, uz razliku imenovanja softvera i pripadajućeg vizualnog znaka (moguće zaštićenog figurativnog žiga) za eOI odnosno za kID (gdje „k“ moguće dolazi od riječi komercijalno).

Podnositelj inicijative dalje dodaje kako sam eOI, kao i pripadajuća programska podrška, svakako predstavlja javnu IT infrastrukturu, gdje je operater AKD, što i dokazuje izvod iz službenog lista Europske unije na koji se AKD poziva, jer je tamo navedeno kako je tijelo

dogovorno za sustav Ministarstvo uprave, a radi se o NIAS-u, posebice eOI-ju koji omogućava visoku razinu sigurnosti. Svakako da je za korištenje eOI-ja potrebna programska podrška, a sam PKI (eng. *public key infrastructure*) sustav podrazumijeva i postojanje certifikacijskog tijela CA (engl. *certified authority*) koje operativno vodi AKD. AKD nas uvjerava da je eOI zapravo njegovo vlasništvo i da nam pruža besplatnu uslugu certifikacije, a tu infrastrukturu opetovano plaćaju porezni obveznici, dakle ona nije besplatna.

Yottabyte kao primjer navodi izvadak iz Službenog lista Europske unije 2019/C 309/06, od 13. rujna 2019., gdje su vidljiva i sredstva postizanja visoke razine sigurnosti elektroničke identifikacije Republike Estonije, koja uključuju i mogućnost korištenja pametnih telefona u navedenu svrhu. Podnositelj inicijative smatra kako je svakako pohvalno da je Republika Hrvatska među prvih 6 zemalja koje su uspostavile identifikacijsko sredstvo najviše razine povjerenja i to je bitna referenca i samog prijavitelja koja nije sporna. Nažalost, zbog monopolističkog pristupa isto nije značajnije zaživjelo u upotrebi, što je evidentno iz DESI indeksa. Kako to navodi Europska komisija, cit.: *„Prema analizi DESI (eng. The Digital Economy and Society Index) za 2019., koju provodi Europska komisija i koja prati evoluciju digitalne kompetitivnosti članica EU-a, Hrvatska je 21. od 29 država članica Europske unije te se nalazi u kategoriji manje uspješnih zemalja.“*

Nadalje, podnositelj inicijative navodi kako se na primjeru Estonije može vidjeti adekvatan uključiv pristup digitalnoj transformaciji, gdje na stranici posvećenoj identifikacijskoj kartici postoji i poseban dio za razvojne inženjere, na kojem je, uz javno dostupan izvorni kod s primjerima za digitalno potpisivanje u različitim programskim jezicima, dostupan i testni sustav, s dostupnim programskim sučeljem na GitHubu.

Nadalje, vezano uz svrhu za koju mu je potrebna specifikacija programskog sučelja paketa eID Middleware, odnosno pripadajuće komponente Signer.exe, podnositelj inicijative navodi da mu je ona potrebna kako bi s kupcima mogao zaključivati pravno valjane narudžbe i ugovore na daljinu korištenjem nacionalne digitalne infrastrukture - eOI-ja te potrebne pripadajuće programske podrške, odnosno paketa Signer.exe, a sve kako bi na vlastitim internetskim stranicama omogućio digitalno potpisivanje narudžbi i ugovora.

Također, podnositelj inicijative ističe kako je onemogućen u izradi vlastitih komercijalnih programskih rješenja koje bi putem interneta omogućavale digitalno potpisivanje korištenjem eOI-ja i komponente Signer.exe, primjerice web aplikaciju „udruzi.se“, za učlanjenje u udruge, za što je potrebno potpisati pristupni obrazac i ugovor. S obzirom na to da se radi o potrebi apliciranja potpisa na internetu, odnosno web aplikaciji, nije potrebno nabrajati izuzetno velik broj mogućnosti.

Podnositelj inicijative smatra kako REST WS API programa Signer.exe mora biti javno objavljen kako bi hrvatska IT industrija vodila hrvatsko gospodarstvo u nacionalnoj digitalnoj transformaciji i kako bi hrvatske tvrtke ponudile moderne web bazirane usluge apliciranjem digitalnog potpisa na zahtjeve, narudžbenice, ugovore i ostale dokumente gdje je to potrebno.

Vezano uz tržište na kojem djeluje, podnositelj inicijative navodi kako djeluje na teritoriju Europske unije i prvenstveno Republike Hrvatske, mada ne isključuje globalne ambicije u narednom razdoblju, te dodaje kako AKD dovodi njega, kao i sve ostale poduzetnike, u nepovoljniji položaj odbijanjem objave specifikacije programskog sučelja paketa eID Middleware te pripadajuće komponente Signer.exe, prvenstveno na tržištu Republike Hrvatske, ali i na svim ostalim tržištima, uključujući i tržište Europske unije ili globalno.

Kao primjer, navodi mogući posao s, primjerice, poduzetnikom fiktivnog naziva XYZ iz Slovenije/Argentine/Čilea koji bi angažirao podnositelja inicijative za implementaciju digitalnog potpisa na internetskim stranicama tvrtke XYZ. Digitalnim potpisom na web stranicama tvrtke

XYZ omogućilo bi se pravno valjano ugovaranje usluga između tvrtke XYZ i državljana Republike Hrvatske korištenjem eOI-ja.

Osim u privatne svrhe, podnositelj inicijative navodi kako je eOI jednako tako moguće koristiti i u poslovne svrhe, što proizlazi iz Uredbe (EU) Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (Službeni list, 28. kolovoza 2014.; dalje u tekstu: Uredba o elektroničkoj identifikaciji).

Podnositelj inicijative zaključno smatra kako bi AZTN u ovom postupku svakako trebao angažirati sudskog vještaka koji bi iznio svoje neovisno mišljenje i uz nalaz i mišljenje priložio i Izjavu o nepostojanju sukoba interesa (da nije bio u ranijem kontaktu niti s podnositeljem inicijative niti AKD-om).

2.3. Drugo očitovanje AKD-a

Na navode podnositelja inicijative, AKD se očitovao podneskom zaprimljenim 3. travnja 2020., u kojem navodi kako je u svom prvom očitovanju koristio pojam „aplikacija / driver“ jer se u eID Middleware datoteci koja se preuzima s mrežnih stranica AKD-a nalaze aplikacije, PKCS#11 biblioteka, minidriver za eOI, korisnička aplikacija za aktivaciju kartice i upravljanje s aktivacijskim podacima, Signer.exe koji omogućava da web preglednici, nakon prestanka podrške *Java Appleta*, na siguran način komuniciraju s karticom, pa tako i s eOI-jem, i na kraju tzv. HRIDCA i ADKCA Root certifikati AKD-a. Stoga ne smatra da njegov navod „aplikacija / driver“ nije točan jer se ne radi o nazivu paketa nego o opisu. Naziv paketa nije tajni podatak jer je objavljen javno u uputi za instalaciju te datoteke i AKD ga također i sam službeno naziva „Programski paket eOI Middleware“.

Dalje, AKD navodi kako ne tvrdi da je Adobe Acrobat Reader alternativa Signer.exe komponenti. To nije točno, Adobe Acrobat Reader dan je kao primjer kako drugi proizvođači programa mogu i bez Signer.exe API specifikacije pristupati eOI-ju i izrađivati e-potpise te dokazuje tvrdnje AKD-a da je za to dovoljno koristiti standard poput MS CAPI i PKCS#11. U praksi, prema spoznajama AKD-a, najviše građana izrađuje e-potpise svojih PDF dokumenata lokalno na svojim računalima upravo korištenjem Adobe Acrobat Reader programa, zato smatra da je taj primjer važan.

Činjenica da NexU *open source* komponenta koju spominje podnositelj inicijative ne ugrožava sigurnost eOI-ja, dodaje AKD, ne znači da AKD-ova Signer.exe komponenta ne ugrožava sigurnost eOI-ja. Signer.exe sadržava u sebi funkcije za rad s eOI-jem koje su sigurnosno osjetljive i javna bi objava API specifikacije otvorila kanal putem kojeg bi bilo moguće ostvariti visoki napadački potencijal za napad na osobnu iskaznicu, koja u čipu (QSCD) čuva 2 privatna ključa građana.

AKD ističe da je u svom prvom odgovoru AZTN-u naveo DSS web servis upravo kao primjer da bilo koji internetski servis ne mora nužno koristiti Signer.exe da bi komunicirao s eOI-jem, budući da on koristi javno objavljenu i svakome dostupnu komponentu NexU, koju ne smatra tehničkom preprekom, a koja omogućava sigurnu komunikaciju s eOI-jem, ali ne omogućava druge sigurnosno kritične funkcije koje Signer.exe omogućava te samim time ne ugrožava sigurnost privatnog ključa građana za slučaj da izgube eOI i u razdoblju dok ne zatraže suspenziju ili opoziv certifikata na izgubljenom eOI-ju.

Nadalje, AKD navodi citat podnositelja inicijative iz njegovog očitovanja zaprimljenog u AZTN-u 21. veljače 2020.: *„S obzirom da program Signer.exe nije nužno potreban za pružanje usluge certificiranja i da postoje alternative (primjerice open source NexU program) AKD treba ili obustaviti distribuciju te komponente zajedno sa ostalim komponentama potrebnim za rad eOI ili omogućiti svima jednake uvijete korištenja navedene komponente.“* AKD naglašava kako

nigdje nije niti naveo da je program Signer.exe nužan za pružanje usluga certificiranja niti je to prijavitelj potkrijepio dokazom. Štoviše, niti Signer.exe niti DSS NexU, ili neki drugi sličan program, nisu potrebni niti se koriste na bilo koji način za pružanje usluge certificiranja koju AKD kao kvalificirani pružatelj usluga certificiranja pruža sukladno regulativi te stoga AKD smatra da je taj prijedlog podnositelja inicijative potpuno neutemeljen.

Kao dokaz, AKD predlaže uvid u dokument „AKD HRIDCA Pravilnik o postupcima certificiranja“, prema kojem AKD pruža uslugu certificiranja za potrebe izdavanja certifikata za eOI i prema kojem je AKD nadziran i certificiran sukladno Uredbi 910/2014 EU (eIDAS uredbi). Signer.exe koristi se isključivo prilikom izrade e-potpisa putem web preglednika, i to u internetskim servisima e-Novorođenče, e-Vozačka i e-Putovnica, za koje su nadležna ministarstva odlučila da se koristi AKD Signer.exe komponenta, umjesto da sami rješavaju problem web preglednika, koji nakon zabrane izvršavanja *Java appleta* ne dozvoljavaju izravnu komunikaciju s eOI-jem i umjesto da građani, kao što je to slučaj s DSS rješenjem, prije korištenja moraju instalirati *open source* rješenje poput NexU-a, koje omogućava izradu e-potpisa u tim internetskim servisima.

Nadalje, AKD navodi kako Signer.exe nije pandan komponenti NexU, suprotno tvrdnji podnositelja inicijative. Primjer da EU DSS web servis može, korištenjem NexU *open source* komponente i bez korištenja programa Signer.exe izraditi e-potpis korištenjem eOI-ja dan je upravo zato da se dokaže da Signer.exe nije obavezna komponenta da bi bilo koji web servisi mogli izraditi e-potpis korištenjem eOI-ja pa bilo koji poduzetnik koji putem web servisa i vlastitih rješenja želi koristiti eOI za izradu e-potpisa može na isti način kao i DSS web servis, bilo korištenjem NexU rješenja, bilo korištenjem nekog svojeg vlastitog rješenja, a bez korištenja Signer.exe komponente, izraditi e-Potpis. Stoga nije točna tvrdnja podnositelja incijative da je Signer.exe, cit.: „*trojanski konj*“.

AKD navodi kako s certifikatima i privatnim ključem na osobnoj iskaznici državljana Republike Hrvatske (eOI) mogućnost komunikacije ima svaka e-usluga / program / rješenje koje koristi PKCS#11 ili MS CAPI protokole, poput javne usluge ePorezna Porezne uprave Ministarstva financija, u kojoj se ne koristi Signer.exe, već se koristi rješenje poduzetnika [...], koji je taj servis izgradio za Poreznu upravu i koji radi i s eOI-jem i s drugim sigurnim kriptografskim uređajima prema PKCS#11 i MS CAPI standardima. AKD naglašava kako ničime ne uvjetuje korištenje Signer.exe programa drugim poduzetnicima te kako nije stekao prednost u tržišnom natjecanju time što se Signer.exe koristi u web preglednicima za potrebe izrade e-potpisa. Kako je pokazano na primjeru DSS web servisa i javnog servisa ePorezna, korištenje komponente Signer.exe iz internetskog preglednika prilikom izrade e-potpisa za potrebe mrežnih usluga nije obavezno, nego je opcija, koju prethodno navedena internetska usluga ePorezna i DSS servis ne koriste. DSS koristi drugu *open source* komponentu NexU, koja je dostupna svima, pa i podnositelju inicijative, a koja svima omogućava izradu e-potpisa putem eOI-ja bez programa Signer.exe, pa i podnositelju inicijative.

Ujedno, AKD navodi kako poduzetnik koji zna otvorene standarde PKCS ili MS CAPI nije spriječen izraditi vlastiti program ili aplikaciju koja bi mu omogućila pružanje usluge posredovanja u apliciranju digitalnog potpisa na dokumente preko interneta, odnosno kojom bi omogućio korisnicima, imateljima eOI paketa, elektroničko potpisivanje dokumenata preko interneta korištenjem njegove aplikacije ili programa, bez REST WS API-ja Signer.exe komponente, kao što je to napravio poduzetnik [...] za potrebe potpisivanja u servisu ePorezna.

Nadalje, AKD ističe kako bi javna objava REST WS API servisa za komunikaciju s karticom (QSCD uređajem) ugrozila sigurnost tako što bi otvorila kanal putem kojeg je moguće ostvariti visoki napadački potencijal za napad na QSCD uređaj koji čuva 2 privatna ključa građana - identifikaciju i kvalificirani elektronički potpis. Dolaskom u posjed privatnog ključa identifikacijskog certifikata bilo koje treće strane, ukraden je identitet osobe. Napadač se može dalje elektronički predstavljati kao oštećeni građanin s najvišom razinom, a da oštećeni

građanin ne zna ništa o tome. Dolaskom u posjed privatnog ključa certifikata za kvalificirani elektronički potpis, napadač može potpisivati elektroničke dokumente koji ostvaruju pravnu snagu opisanu u članku 25. stavku 2. Uredbe eIDAS EU 910/2014. Drugim riječima, s obzirom na to da se upotrebom ovog certifikata ostvaruje jednak pravni učinak kao vlastoručnim potpisom, napadač može na štetu oštećenog građanina učiniti bilo koju pravno valjanu radnju za koju je potreban vlastoručni potpis građanina (primjerice, prodati svu njegovu imovinu, sklopiti štetne ugovore i drugo). S obzirom na spomenute rizike, prema saznanjima AKD-a, ne postoji primjer proizvođača koji je javno objavio specifikacije ovakve komponente.

Prema AKD-u, DSS servis omogućava među ostalim uslugama i izradu elektroničkog potpisa. U nastavku je AKD dao opis izbora certifikata s kojim korisnik želi potpisati dokument ili podatke pomoću internetskog servisa DSS. Navedenim opisom, AKD smatra kako je dokazao da je tvrdnja podnositelja inicijative da DSS izrađuje potpis identifikacijskim certifikatom netočna, tj. kako je dokazao da DSS izrađuje potpis onim certifikatom koji je potpisnik prethodno izabrao, bilo to identifikacijski, potpisni, autentikacijski, soft, SSl, web ili bio koji drugi certifikat koji potpisnik posjeduje i s njime želi potpisati dokument.

AKD zaključuje kako je iz svega prethodno navedenog razvidno kako je inicijativa poduzetnika yottabyte za pokretanje postupka utvrđivanja zlouporabe vladajućeg položaja protiv AKD-a u cijelosti neosnovana te da AKD postupa u potpunosti sukladno nacionalnim i europskim pozitivnim propisima.

2.4. Drugo očitovanje podnositelja inicijative

Dana 17. travnja 2020. AZTN je zaprimio očitovanje podnositelja inicijative na navode poduzetnika AKD iz podneska zaprimljenog 3. travnja 2020., u kojem u bitnome navodi kako je u tehničkom smislu vrlo jasna distinkcija kategorije softvera između upravljačkog odnosno pogonskog programa (eng. *driver*), operativnog sustava (eng. *operating system*), međusoftvera (eng. *middleware*) te aplikacije (eng. *application*). Sporna komponenta Signer.exe upravo je komponenta tipa međusoftver koja se izvršava na operativnom sustavu i pruža potporu aplikacijama za primjenu digitalnog potpisa putem web baziranih aplikacija. Tvrdi kako AKD namjerno ubacuje riječ *driver* da bi stvorio konfuziju i naginjao tvrdnjama kako su sve komponente neophodne za rad i pružanje usluge certificiranja, što nije točno.

Podnositelj inicijative navodi kako AKD tvrdi kako u praksi, prema njegovim spoznajama, najviše građana do sad izrađuje e-potpise svojih PDF dokumenata lokalno na svojim računalima korištenjem Adobe Acrobat Reader programa, što je najvjerojatnije točno, a i djelomično posljedica toga što je sam AKD stvorio tehničke i financijske prepreke da se pokrene ekosustav u IKT industriji koji bi omogućavao jednostavna i jeftina web rješenja za digitalno potpisivanje bazirana na Signer.exe komponenti. Tvrdnje AKD-a da njegova Signer.exe komponenta ugrožava sigurnost eOI-ja krajnje su zabrinjavajuće te bi se istima trebao pozabaviti UVNS - Ured Vijeća za nacionalnu sigurnost, kao i šira javnost. Upravo čip osobne iskaznice predstavlja kvalificirano sredstvo za izradu elektroničkog potpisa (eng. *a Secure Signature Generation Device* - QSCD) te on ni na koji način ne omogućuje pristup privatnim ključevima, već isključivo po pozivu aplikacijskog programskog sučelja vrši enkripciju ili dekripciju poruke.

Nadalje, AKD je upoznat s tehnologijom digitalnog potpisa te također navodi i NexU *open source* komponentu, za koju pak tvrdi da ne ugrožava sigurnost eOI-ja pa sada nije jasno zašto bi Signer.exe ugrožavao sigurnost eOI-ja kada bi javno bila dostupna objava REST WS API-ja za dvije primarne funkcije potpisa, koje se programski koriste bilo s NexU komponentom ili recimo Estonskom eID komponentom hwcrypto. Potrebno je omogućiti REST WS API za dohvat potpisnog certifikata te enkripciju poslane poruke (sažetka) privatnim ključem.

Ujedno, podnositelj inicijative navodi kako se AKD slaže s izjavom da sama komponenta Signer.exe nije potrebna za uslugu certificiranja, ali zahtjev da prestane pakirati navedenu komponentu s ostalim komponentama neophodnim za rad eOI-ja ili pak javnu objavu gore navedenih REST WS API poziva smatra neutemeljenim. Prema podnositelju inicijative, AKD koristi svoju povlaštenu poziciju pružatelja usluga certificiranja koju po sili zakona svi državljani Republike Hrvatske moraju koristiti, odnosno sklopiti ugovor s AKD-om, te osim softvera neophodnog za pružanje te usluge (poput upravljačkog programa za pametnu karticu eOI) pakira i dodatan međusoftver (eng. *middleware*) (komponentu Signer.exe) koji mu omogućava tržišno pozicioniranje i monopol, pri čemu građani udomljuju instalirani servis (eng. *hosting*). Samim time, kod korištenja usluge elektroničkog potpisa (ne usluge javnog certificiranja) građani ne moraju ništa dodatno instalirati na računalo, dok bi svi ostali pružatelji usluge morali upućivati građane na instalaciju i pokretanje dodatnog softvera, bilo postojećih rješenja kao NexU-a, eID-a ili vlastitog programskog rješenja. Time je upravo stvorena tehnička prepreka ostalim sudionicima na tržištu jer nije omogućena interoperabilnost sa softverom Signer.exe, a što je i prema ranije navedenoj sudskoj praksi Europske komisije nepošteno.

Nadalje, podnositelj inicijative ističe kako i sam AKD navodi da upravo pomoću navedene komponente pruža uslugu digitalnog potpisa ministarstvima te kako građani ne moraju instalirati *open source* rješenja poput NexU-a koje omogućava izradu e-potpisa u internetskim servisima. Time je AKD zaključao korisnike (eng. *vendor lock-in*) te im nitko drugi ne može ponuditi uslugu digitalnog potpisa bez, kako i sam navodi, instalacije rješenja prije korištenja internetskog servisa (bilo državnog ili privatnog). AKD bi jednako tako u svoj instalacijski čarobnjak mogao pakirati i NexU komponentu, odnosno da se koristi bilo koja druga *open source* komponenta tada bi i svi ostali sudionici tržišta imali mogućnost korištenja REST WS API-ja.

Dodatno, podnositelj inicijative navodi kako je NexU pandan AKD-ovoj komponenti Signer.exe, bez obzira na suprotne tvrdnje AKD-a, a s obzirom na to da se obje komponente pokreću na klijentskom računalu, obje rješavaju problem pristupa eOI-ju kroz web preglednik i obje služe za podršku digitalnog potpisa u web aplikacijama, te bi istinitost ovih navoda trebao provjeriti neovisni sudski vještak za informatiku.

Podnositelj inicijative ističe kako nije upitno da postoje različita programska rješenja, neka razvijena za Poreznu upravu, neka za FINU. Moguće je da bi i ta programska rješenja trebala biti interoperabilna, ali nema se vremena baviti i s njima.

Nadalje, podnositelj inicijative navodi kako nije upitno da postoje otvoreni standardi PKCS ili MS CAPI s kojima se mogu razvijati rješenja koja su pandan komponenti Signer.exe. Također nije upitno niti da u Republici Hrvatskoj nemamo strategiju digitalizacije pa imamo gomilu parcijalnih ili vlasničkih rješenja, jedno od njih spominje i AKD kao rješenje tvrtke [...] za potrebe internetskog potpisivanja u servisu ePorezna. Međutim, navedeno ne isključuje vladajući položaj AKD-a uslijed zakonske obveze propisane Zakonom o osobnoj iskaznici niti isključuje obvezu pružanja interoperabilnosti. Nije niti Windows jedini operativni sustav na svijetu pa je Europska komisija svejedno zaključila kako treba staviti API na raspolaganje radi postizanja interoperabilnosti.

Također, uz Windows Media Player postoji i velik broj drugih softvera za reprodukciju audio i video sadržaja, ali je Europska komisija također zaključila kako njegovo pakiranje uz operativni sustav narušava tržišno natjecanje pa je ono zabranjeno, kao što bi trebalo zabraniti i pakiranje Signer.exe komponente u eOI Middleware softverski paket ako se ne može postići interoperabilnost. Pa onda neka građani instaliraju NexU i digitalno potpisuju eZahjeve za vozačke, putovnice, prijave novorođenčeta, a da i ostali sudionici tržišta mogu koristiti taj međusoftver za potpis ugovora i dokumenata s komunalnim društvima, telekomima, vrtićem, školom, vodovodom, plinarom, komunalnim, pogrebnim poduzećem, opskrbljivačima električnom energijom i dalje.

Što se tiče autorskih prava i međunarodnih ugovora, oni nisu sporni. Jednako je tako Windows operativni sustav tvrtke Microsoft Inc. koji je zaštićen autorskim pravima pa je Europska komisija ipak donijela odluku da zbog interoperabilnosti mora objaviti API.

Nadalje, podnositelj inicijative navodi kako AKD daje lažan iskaz AZTN-u kada navodi da bi REST WS API servis koji omogućava dva poziva, jedan za dohvat potpisnog certifikata, a drugi za enkripciju sažetka ugrozio sigurnost eOI pametne čip kartice. Upravo navedeno rade komponente kao NexU, odnosno Estonski eID, kao i mnoge druge komponente, nužno i programska potpora FINE, Porezne uprave i svih ostalih, jer je to način rada digitalnog potpisa nekog sadržaja (bilo .pdf datoteke bilo .xml datoteke ili drugog sadržaja). AZTN bi u ovom slučaju trebao angažirati neovisnog sudskog vještaka. eOI sukladno zakonskim odredbama za osobe do 5 godina ne sadrži certifikate, za osobe od 5 do 18 godina jedan certifikat (upitno da li ga možemo zvati identifikacijski), za osobe od 18 do 65 godine dva certifikata, a osobe iznad 65 godina mogu birati i osobnu iskaznicu bez čipa pa samim time i nemaju certifikat. Evidentno je da nisu uvijek dva privatna ključa.

Na poseban upit AZTN-a može li yottabyte razviti vlastito programsko rješenje (aplikaciju) koje može omogućiti imateljima eOI-ja lokalno potpisivanje dokumenata (na vlastitom računalu) bez posjedovanja REST WS API-ja Signer.exe komponente poduzetnika AKD, podnositelj inicijative odgovara potvrdno. S obzirom na to da se radi o lokalnoj aplikaciji, moguće je koristiti PKCS ili MS CAPI standard. Nije isključeno da lokalna aplikacija poziva REST WS API Signer.exe komponente te da se na taj način riješi digitalni potpis korištenjem eOI-ja, što bi bilo zapravo i jednostavnije jer nije potrebno uključivati biblioteke koje su implementirale navedene PKCS ili MS CAPI standarde, već se koristi biblioteka za pozivanje HTTP(S) protokola koji su danas sastavni dio skoro svih aplikacija.

Na poseban upit AZTN-a može li razviti vlastito programsko rješenje (aplikaciju) koje može omogućiti imateljima eOI-ja udaljeno potpisivanje dokumenata (na internetu kroz web aplikaciju) bez posjedovanja REST WS API-ja Signer.exe komponente poduzetnika AKD, podnositelj inicijative odgovara negativno, ističući da i sam AKD navodi kako cit.: *„Signer.exe koji omogućava da web preglednici, nakon prestanka podrške Java Appleta, na siguran način komuniciraju s karticom.“* Stoga je evidentno da takav međusloj mora postojati.

Podnositelj inicijative navodi kako postoje supstitucije za program Signer.exe, primjerice ranije spomenuti program NexU, a također bi mogao i sam izraditi takav međusloj, mada to nema smisla pored već dostupnih gotovih komponenti.

Inicijativa se odnosi na AKD, dodaje yottabyte, jer nije omogućio interoperabilnost svog međusloja s drugim rješenjima koja bi omogućavala web potpis te također jer kroz zakonsku obvezu korištenja usluga certificiranja pakira i međusloj za koji i sam navodi da nije potreban za uslugu certificiranja, a onda si uzima za isključivo pravo korištenje tog međusloja.

AKD je u prednosti pred ostalim tržišnim natjecateljima jer nakon instalacije programskog paketa eID Middleware ima sposobnost primjene digitalnog potpisa korištenjem eOI-ja u svojoj web aplikaciji, dok svi ostali sudionici moraju navoditi korisnika na instalaciju dodatne programske podrške, odnosno korisnik mora instalirati eID Middleware koji sadrži upravljačke programe (to nije moguće preskočiti) i dodatan program koji će služiti kao međusloj. Ponekad samu instalaciju ne rade korisnici na računalu niti imaju administratorska prava da bi to uopće mogli učiniti pa će ta prepreka biti još značajnija odnosno nepremostiva.

3. Postupak utvrđivanja sprječavanja, ograničavanja ili narušavanja tržišnog natjecanja zlouporabom vladajućeg položaja

3.1. Zaključak o pokretanju postupka

Na temelju podataka i dokumentacije koje je prikupio tijekom prethodnog ispitivanja stanja na mjerodavnom tržištu, AZTN je zaključkom od 2. lipnja 2020., na temelju članka 30. točke 2., članka 31., članka 38. stavka 1. i 3. i članka 39. ZZTN-a, a u svezi s člankom 13. ZZTN-a, pokrenuo postupak po službenoj dužnosti protiv AKD-a radi utvrđivanja sprječavanja, ograničavanja ili narušavanja tržišnog natjecanja zlouporabom vladajućeg položaja na mjerodavnom tržištu izdavanja kvalificiranih certifikata na elektroničkoj osobnoj iskaznici državljanima Republike Hrvatske te posredovanja u apliciranju kvalificiranog digitalnog potpisa s elektroničke osobne iskaznice putem interneta, na teritoriju Republike Hrvatske.

Postupak je pokrenut radi utvrđivanja je li AKD-ov proizvod eID Middleware tj. njegova komponenta Signer.exe objektivno nužan za učinkovito tržišno natjecanje na tržištu posredovanja u apliciranju kvalificiranog digitalnog potpisa putem interneta te može li AKD-ovo uskraćivanje pristupa toj komponenti drugim poduzetnicima, njegovim konkurentima, dovesti do narušavanja tržišnog natjecanja, čime bi mogla nastati šteta za potrošače.

3.2. Stranka u postupku

AKD je osnovan Ugovorom o osnivanju društva s ograničenom odgovornošću od 19. lipnja 1991. Upisan je pod matičnim brojem subjekta 080020427 u sudski registar Trgovačkog suda u Zagrebu te je registriran za obavljanje niza djelatnosti, od kojih su za konkretan predmet najvažnije: pružanje usluga povjerenja, izrada magnetskih kartica, kartica sa chipom i visoko zaštićenih ID-kartica, pružanje dijeljenih usluga tijelima javnog sektora i drugim korisnicima te računalne i srodne djelatnosti. AKD je u stopostotnom vlasništvu Republike Hrvatske, koja je jedini osnivač i član društva. Osoba ovlaštena za zastupanje jest direktor Jure Sertić.

3.3. Primijenjeni propisi

AZTN je u konkretnom predmetu primijenio odredbe ZZTN-a, Uredbe o načinu i kriterijima utvrđivanja mjerodavnog tržišta („Narodne novine", br. 9/11; dalje u tekstu: Uredba o mjerodavnom tržištu) te odredbe Zakona o općem upravnom postupku („Narodne novine", br. 47/09; dalje u tekstu: ZUP), u smislu članka 35. stavka 1. ZZTN-a i članka 3. stavka 1. ZUP-a.

Također, AZTN je podredno na odgovarajući način primjenjivao kriterije iz pravne stečevine Europske unije, koja služi kao interpretativni instrument za primjenu odredbi ZZTN-a, a osobito u slučaju pravnih praznina ili dvojbi pri tumačenju propisa, u skladu s člankom 1. Ugovora o pristupanju Republike Hrvatske Europskoj uniji („Narodne novine - Međunarodni ugovori", br. 2/12), a kako je to propisano člankom 74. ZZTN-a. Slijedom navedenog, izvršen je uvid u Priopćenje Komisije - Uputu o provedbenim prioritetima Komisije u primjeni članka 82. Ugovora o EZ-u na postupanja poduzetnika u vladajućem položaju koja za posljedicu mogu imati zlouporabu u smislu isključivanja konkurenata s tržišta (Službeni list C 045, 24. veljače 2009.) te u Presudu Općeg suda od 17. rujna 2007. u predmetu T-201/04, Microsoft Corp. protiv Komisije Europskih zajednica (dalje u tekstu: predmet *Microsoft*).

Uz navedeno, AZTN je izvršio uvid i u posebne propise koji reguliraju predmetnu materiju:

- Uredbu (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (dalje u tekstu: eIDAS uredba);
- Zakon o osobnoj iskaznici („Narodne novine“, br. 62/15 i 42/20; dalje u tekstu: ZOI);

- Zakon o provedbi uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ („Narodne novine“, br. 62/17; dalje u tekstu: Zakon o provedbi eIDAS uredbe) te

Pravilnik o pružanju i korištenju usluga povjerenja („Narodne novine“, br. 60/19; dalje u tekstu: PPKUP).

4. Mjerodavno tržište

Mjerodavno tržište, u smislu članka 7. ZZTN-a, određuje se kao tržište određene robe i/ili usluga koje su predmet obavljanja djelatnosti poduzetnika na određenom zemljopisnom području.

Sukladno članku 3. stavku 2. Uredbe o mjerodavnom tržištu, svrha utvrđivanja mjerodavnog tržišta određivanje je robe i/ili usluga s kojima se poduzetnici tržišno natječu te zemljopisnog područja na kojem se natječu.

Mjerodavno tržište, sukladno članku 4. stavku 1. Uredbe o mjerodavnom tržištu, utvrđuje se na način da se utvrdi njegova proizvodna dimenzija (mjerodavno tržište u proizvodnom smislu) i zemljopisna dimenzija (mjerodavno tržište u zemljopisnom smislu).

4.1. Mjerodavno tržište u proizvodnom smislu

Prema članku 5. Uredbe o mjerodavnom tržištu, mjerodavno tržište u proizvodnom smislu obuhvaća sve proizvode za koje potrošači smatraju da su međusobno zamjenjivi s obzirom na njihove bitne značajke, cijenu ili način uporabe, odnosno navike potrošača.

U konkretnom predmetu AZTN je promatrao tri međusobno povezana mjerodavna tržišta:

1. tržište izdavanja kvalificiranih certifikata na elektroničkoj osobnoj iskaznici državljanima Republike Hrvatske (dalje u tekstu: tržište izdavanja certifikata za eOI),
2. tržište distribucije međusoftvera za eOI,
3. tržište posredovanja u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta (dalje u tekstu: tržište posredovanja u apliciranju elektroničkog potpisa).

U nastavku se opisuju mjerodavna tržišta.

4.1.1. Tržište izdavanja certifikata za eOI

Certifikati se koriste za potvrdu identiteta potpisnika. Certifikat označava potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa (javni ključ) s nekom osobom i potvrđuje identitet te osobe. Napredni elektronički potpis temelji se na kvalificiranom certifikatu. Kvalificirani certifikat jest elektronička potvrda kojom davatelj usluga izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis potpisnika tj. nedvojbeno potvrđuje identitet potpisnika.

U suštini, certifikati sadrže identifikacijske podatke osobe i njezin javni ključ u elektroničkom obliku. Javni ključ omogućuje da se na nedvojben način s fizičkom osobom povežu podaci za verificiranje elektroničkog potpisa i potvrdi identitet te osobe. Certifikati na elektroničkoj osobnoj iskaznici (dalje u tekstu: eOI) kvalificirani su.

Kvalificirani elektronički potpis jest napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.

Da bi mogao izdavati kvalificirane certifikate, poduzetnik u Republici Hrvatskoj mora dobiti suglasnost Ministarstva gospodarstva, poduzetništva i obrta, sa sjedištem u Zagrebu, Ulica grada Vukovara 78 (dalje u tekstu: MINGPO) te biti uvršten na pouzdani popis kvalificiranih pružatelja usluga povjerenja, sukladno eIDAS uredbi te Zakonu o provedbi eIDAS uredbe. Trenutno u Republici Hrvatskoj djeluju tri poduzetnika koja se nalaze na pouzdanom popisu kvalificiranih pružatelja usluga povjerenja, i to AKD, Financijska agencija - FINA, sa sjedištem u Zagrebu, Ulica grada Vukovara 70 (dalje u tekstu: FINA) i Zagrebačka banka d.d., sa sjedištem u Zagrebu, Trg bana Josipa Jelačića 10 (dalje u tekstu: ZABA).

Iako su, osim AKD-a, FINA i ZABA kvalificirani pružatelji usluga povjerenja, odnosno certificiranja, AKD jedini od njih izdaje certifikate za osobnu iskaznicu. FINA posjeduje vlastite certifikate koji se mogu koristiti za identifikaciju i elektroničko potpisivanje putem interneta, ali korisnik, fizička osoba, mora od FINE osobno zatražiti certifikat, uz plaćanje određene naknade, pri čemu nije zakonom dužan niti obvezan zatražiti njen certifikat.

S druge strane, svi državljani Republike Hrvatske dužni su posjedovati osobnu iskaznicu te u sklopu troškova izrade osobne iskaznice dobit će i pripadajući certifikat na osobnoj iskaznici (ovisno o životnoj dobi i u određenim slučajevima vlastitom izboru). Pored propisane naknade za izdavanje same osobne iskaznice, nemaju nikakvog dodatnog troška za izdavanje certifikata za eOI.

AKD pruža usluge povjerenja od 2015. godine, kada je počeo s izdavanjem certifikata koji se nalaze na osobnoj iskaznici. Navedeno je razvidno i iz odredbi ZOI-ja. Sukladno članku 1. stavku 1. ZOI-ja, osobna je iskaznica elektronička javna isprava kojom hrvatski državljanin dokazuje identitet, hrvatsko državljanstvo, spol, datum rođenja i prebivalište u Republici Hrvatskoj. U članku 2. ZOI-ja navedeno je sljedeće:

(1) Osobna iskaznica sadržava elektronički nosač podataka na koji se uz podatke iz članka 1. stavka 1. ovoga Zakona može pohraniti jedan ili dva certifikata.
(2) Certifikati koji se mogu pohraniti na elektronički nosač podataka iz stavka 1. ovoga članka su identifikacijski certifikat i potpisni certifikat.
(3) Identifikacijski certifikat je kvalificirani certifikat koji se koristi za elektroničku identifikaciju i autentifikaciju radi pristupa elektroničkim uslugama.
(4) Potpisni certifikat je kvalificirani certifikat koji se koristi za podršku naprednom elektroničkom potpisu koji ima istu pravnu snagu i zamjenjuje vlastoručni potpis sukladno propisima kojima je reguliran elektronički potpis.
(5) Davatelj usluga certificiranja koji obavlja poslove izdavanja certifikata iz stavaka 3. i 4. ovoga članka je pravna osoba ovlaštena za izradu osobnih iskaznica.
(6) Davatelj usluga certificiranja iz stavka 5. ovoga članka dužan je uspostaviti Portal elektroničke osobne iskaznice na kojem će objavljivati sve informacije potrebne za korištenje osobne iskaznice, donijeti interni akt o postupcima certificiranja te se upisati u evidenciju ministarstva nadležnog za poslove gospodarstva kao davatelj usluga certificiranja koji obavlja usluge izdavanja kvalificiranih certifikata te provesti integraciju u sustav e-Građani sukladno propisima o državnoj informacijskoj infrastrukturi.

Ovisno o dobi korisnika, eOI može sadržavati jedan ili dva certifikata, što jasno proizlazi iz članka 4. ZOI-ja. Tako osobna iskaznica izdana djeci do 5 godina starosti ne sadržava niti jedan certifikat, osobna iskaznica izdana djeci od 5 do navršenih 18 godina starosti sadržava identifikacijski certifikat, dok osobna iskaznica izdana osobama između 18 i 65 godina starosti sadržava oba certifikata. Osobe starije od 65 godina mogu ishoditi osobnu iskaznicu s oba certifikata ili bez njih, po vlastitom izboru.

Dakle, iz navedenih je odredbi razvidno kako je, za razliku od ostalih kvalificiranih pružatelja usluga povjerenja, AKD na temelju ZOI-ja određen kao davatelj usluga certificiranja, i to identifikacijskog i potpisnog certifikata za osobnu iskaznicu. Ujedno, AKD jedini izrađuje osobne iskaznice, odnosno eOI za sve državljane Republike Hrvatske.

4.1.2. Tržište distribucije međusoftvera za eOI

Da bi se korisnici mogli služiti certifikatima pohranjenima na eOI-ju, potreban je programski sloj koji omogućuje povezivanje tih certifikata s aplikacijama u kojima se vrši sam elektronički potpis. Taj se programski sloj naziva *middleware* odnosno međusoftver te posreduje u komunikaciji između samih certifikata na eOI-ju i aplikacija u kojima se koristi eOI. U nedostatku takvog „posredničkog" programskog rješenja, ne bi bilo moguće potpisivanje dokumenata korištenjem eOI-ja.

AKD je razvio programski paket (međusoftver) eID Middleware koji korisnici eOI-ja mogu bez dodatne naknade preuzeti s interneta i nakon instalacije na osobno računalo koristiti za izradu elektroničkih potpisa i pristupanje raznim elektroničkim servisima (poput servisa e-Građani).

Budući da podnositelj inicijative spornom smatra komponentu AKD-ovog međusoftvera koja omogućuje elektroničko potpisivanje dokumenata putem interneta (Signer.exe), AZTN je promatrao samo taj uži segment tržišta, isključujući lokalno potpisivanje, što je podrobnije objašnjeno u sljedećem poglavlju.

4.1.3. Tržište posredovanja u apliciranju elektroničkog potpisa

Na ovom tržištu djeluju poduzetnici koji svojim programskim rješenjima omogućuju imateljima eOI-ja da, koristeći certifikate sadržane na njemu, putem interneta potpisuju dokumente, ugovore i slično. Predmetni poduzetnici zapravo su posrednici koji omogućavaju korisnicima, imateljima eOI-ja, da putem interneta, koristeći internetske preglednike, ulaze u određeni oblik poslovne suradnje s drugim pravnim ili fizičkim osobama, potpisujući ugovore ili druge dokumente putem programskog rješenja posrednika. Na taj način korisnici, imatelji eOI-ja, ne moraju potpisivati fizički, materijalni primjerak nekog dokumenta niti moraju biti fizički prisutni u blizini druge strane s kojim ulaze u poslovni odnos, što uvelike olakšava poslovanje objema stranama, posebno ako se one ne nalaze u istom mjestu prebivališta.

Kako je prethodno navedeno, broj certifikata prisutnih na osobnoj iskaznici ovisi o životnoj dobi imatelja osobne iskaznice. Kao što je razvidno iz članka 2. ZOI-a, postoji razlika između identifikacijskog i potpisnog certifikata, preciznije njihove svrhe i namjene. Identifikacijski certifikat koristi se za elektroničku identifikaciju i autentifikaciju radi pristupa elektroničkim uslugama. Najbolji je primjer za to sustav e-Građani, kojem korisnik, između ostalih načina (poput tokena raznih banaka, certifikata FINE i slično), može pristupiti koristeći identifikacijski certifikat koji dokazuje njegov identitet. S druge strane, potpisni certifikat služi za potpisivanje raznih dokumenata te ima istu pravnu snagu i zamjenjuje vlastoručni potpis sukladno propisima kojima je reguliran elektronički potpis.

Gore navedeno proizlazi i s eOI-jeve mrežne stranice (https://www.eid.hr/hr/certifikati/clanak/uporaba-certifikata), gdje je kod objašnjenja upotrebe certifikata jasno navedeno kako se certifikati upotrebljavaju za dvije svrhe, za identifikaciju i za izradu kvalificiranog elektroničkog potpisa. Vezano uz identifikaciju, navedeno je kako eOI s aktivnim identifikacijskim certifikatom služi za prijavu u sustav e-Građani i druge e-usluge. Vezano uz izradu kvalificiranog elektroničkog potpisa, navedeno je kako, uz potpisni certifikat, eOI služi za obavljanje aktivnosti vezanih uz ovjeru dokumenata elektroničkim potpisom, kao valjanom zamjenom za vlastoručni potpis.

Dakle, evidentno je kako je potrebno razlikovati identifikacijski i potpisni certifikat sadržan na eOI-ju prema namjeni i upotrebi. Međutim, iz očitovanja, kako podnositelja inicijative, tako i AKD-a, proizlazi kako se dokument može potpisati i identifikacijskim certifikatom. Iz navedenog razloga definicija mjerodavnog tržišta u konkretnom predmetu obuhvaća oba navedena certifikata.

Dodatno, treba istaknuti kako postoji razlika između lokalnog elektroničkog potpisa i elektroničkog potpisa putem interneta. Pojam „lokalno potpisivanje“ u konkretnom postupku podrazumijeva potpisivanje dokumenata na vlastitom računalu korisnika u *desktop* aplikacijama bez korištenja interneta, dakle korisniku nije potrebna internetska veza za potpisivanje određenih dokumenata. To bi se primjerice odnosilo na potpisivanje dokumenata u Microsoft Office Word programu ili putem Adobe Acrobat Reader programa.

Za potpisivanje dokumenata putem interneta, korisnik mora imati pristup internetu te koristiti internetski preglednik, pri čemu je potrebno koristiti dodatno, posebno programsko rješenje, odnosno međusoftver, koje će omogućiti potpisivanje korištenjem internetskih preglednika.

Slijedom svega prethodno navedenog, AZTN je u konkretnom predmetu kao povezano tržište promatrao tržište posredovanja u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta.

Predmetna definicija ne obuhvaća lokalno potpisivanje dokumenata koje se vrši u *desktop* aplikacijama (MS Word, Adobe Acrobat Reader, i sl.) jer za takvu vrstu potpisivanja nije niti potrebna sporna komponenta Signer.exe, kao ni pristup, odnosno korištenje interneta.

4.2. Mjerodavno tržište u zemljopisnom smislu

Sukladno odredbi članka 6. Uredbe o mjerodavnom tržištu, mjerodavno tržište u zemljopisnom smislu obuhvaća zemljopisno područje na kojem poduzetnici sudjeluju u ponudi ili nabavi proizvoda.

S obzirom na to da AKD izdaje eOI s pripadajućim certifikatima isključivo za državljane Republike Hrvatske, neovisno o mjestu prebivališta, AZTN je za mjerodavno tržište izdavanja certifikata za eOI u zemljopisnom smislu odredio teritorij Republike Hrvatske.

Kod silaznih tržišta moguće je zaključiti kako je riječ o širem zemljopisnom području, najmanje teritoriju Europske unije, budući da u ponudi ili nabavi proizvoda sudjeluju odnosno mogu sudjelovati i poduzetnici koji posluju izvan teritorija Republike Hrvatske. Primjerice, kao međusoftver za eOI može se koristiti servis Europske unije DSS i pripadajuća komponenta NexU, koju je razvio poduzetnik iz Luksemburga, a slično tome nema nikakvih prepreka da posredovanje u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta obavljaju i poduzetnici koji posluju izvan teritorija Republike Hrvatske.

5. Položaj poduzetnika AKD na mjerodavnim tržištima

U nastavku se izlažu okolnosti vezane za položaj poduzetnika AKD na dva uzlazna mjerodavna tržišta. Budući da položaj AKD-a na tržištu posredovanja u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta u konkretnom slučaju nije relevantan jer se na njemu mogu samo manifestirati možebitne posljedice eventualne zlouporabe na nekim od uzlaznih tržišta, navedeno se neće posebno utvrđivati.

5.1. Položaj AKD-a na tržištu izdavanja certifikata za eOI

Kao što je već navedeno, AKD izrađuje osobne iskaznice te izdaje certifikate za eOI. AKD je jedini poduzetnik u Republici Hrvatskoj koji je ovlašten za izdavanje certifikata za eOI. Za navedene potrebe, dakle izdavanje certifikata, u AKD-u je uspostavljena PKI (*Public Key Infrastructure*) infrastruktura.

Sukladno dokumentu AKD PKI Opća pravila pružanja usluga certificiranja, Izdanje 2.2, od 30. rujna 2018. (dalje u tekstu: AKD PKI pravila), AKD PKI uređen je hijerarhijski te se sastoji od krovnog ovjerovitelja AKDCA Root, koji samom sebi izdaje certifikat, te podređenih ovjerovitelja HRIDCA-e, koji izdaje certifikate fizičkim osobama isključivo za potrebe izdavanja eOI-ja, te kIDCA-e, koji izdaje certifikate za komercijalnu namjenu i za potrebe servisa za izdavanje kvalificiranih elektroničkih vremenskih žigova.

Iz navedenog se može zaključiti kako se AKD nalazi u vladajućem položaju na mjerodavnom tržištu izdavanja certifikata za eOI, u smislu članka 12. ZZTN-a.

5.2. Položaj AKD-a na tržištu distribucije međusoftvera za eOI

AKD u sklopu izdavanja certifikata za eOI korisnicima nudi i programski paket (međusoftver) eID Middleware, koji omogućava imateljima eOI-ja korištenje identifikacijskog i/ili potpisnog certifikata sadržanog na njihovim osobnim iskaznicama. Jedna od komponenti tog programskog paketa jest i Signer.exe, međusoftver koji omogućuje pristupanje elektroničkim certifikatima na eOI-ju i korištenje tih certifikata putem internetskih preglednika.

Iz očitovanja AKD-a i podnositelja inicijative proizlazi kako je nakon zabrane *Java appleta* u internetskim preglednicima bilo potrebno razviti dodatno programsko rješenje koje bi omogućilo da oni na siguran način pristupe elektroničkim certifikatima na eOI-ju i koriste ih jer bez tog rješenja internetski preglednici ne bi dozvoljavali rad s eOI-jem.

Java applet jest programsko rješenje poduzetnika Oracle koje je omogućavalo da se izravno iz internetskog preglednika pokreću određene aplikacije, između ostalog i međusoftver za elektroničko potpisivanje. Međutim, od 2015. nadalje svi su vodeći internetski preglednici prestali pružati podršku za NPAPI arhitekturu na kojoj su se temeljili *Java appleti* tako da se oni više nisu mogli izvršavati u njima. Stoga je bilo potrebno razviti dodatno programsko rješenje (međusoftver) koje bi omogućilo da korisnici na siguran način mogu pristupati elektroničkim certifikatima na eOI-ju i da ih koriste za elektroničku identifikaciju i potpisivanje.

Na ovom tržištu, osim AKD-a, djeluje i poduzetnik [...], koji je samostalno razvio programsko rješenje za Poreznu upravu - ePorezna, putem kojeg korisnici eOI-ja također mogu koristiti pripadajuće certifikate za potpisivanje obrazaca, dokumenata i slično.

Također, potrebno je istaknuti i *open source* (besplatno) rješenje Europske unije - Digital Signature Service (dalje u tekstu: DSS), koje je razvila tvrtka Nowina Solutions iz Luksemburga koristeći fondove Europske unije, a koje imateljima eOI-ja omogućuje potpisivanje dokumenata putem interneta, za što je potrebno preuzeti i instalirati komponentu NexU.

Slijedom navedenog, moguće je zaključiti kako je na ovom tržištu AKD suočen s određenom razinom konkurencije.

Međutim, uzevši u obzir činjenicu da je instalacija AKD-ovog međusoftvera eID Middleware nužna da bi se eOI uopće mogao aktivirati te da se bez tog koraka korisnik uopće ne može služiti certifikatima na eOI-ju, može se zaključiti kako se i na ovom tržištu AKD nalazi u vladajućem položaju, u smislu članka 12. ZZTN-a.

6. Očitovanja AKD-a, podnositelja inicijative i trećih strana

6.1. Očitovanje AKD-a

Na navode iz zaključka o pokretanju postupka, poduzetnik AKD očitovao se podneskom zaprimljenim 20. kolovoza 2020., u kojem u bitnome navodi da, suprotno navodima podnositelja inicijative, on ne koristi javnu IT infrastrukturu te nema nikakav monopol na njeno

korištenje, pri čemu sve osobe imatelji eOI-ja mogu, korištenjem besplatnih alata poput Adobe Acrobat Readera i DSS rješenja/servisa EU-a, bez naknade izrađivati elektroničke potpise na svojim računalima. AKD ne dobiva nikakva financijska sredstva radi posredništva kod izrade elektroničkih potpisa korištenjem eOI-ja. Iz navedenog proizlazi kako je netočna tvrdnja da je AKD tehničkim i financijskim zaprekama onemogućio digitalizaciju Republike Hrvatske.

Također navodi kako su netočni navodi podnositelja inicijative da je AKD elD Middleware isti proizvod kao u prijavi spomenuti kID Middleware, koji se koristi zajedno s komercijalnim AKD kID pametnim karticama i komercijalnim AKD ePotpis servisom. Komercijalni AKD kID Middleware ne koristi se s elektroničkom osobnom iskaznicom (eOI) državljana Republike Hrvatske, stoga ne stoji tvrdnja iz inicijative da AKD pruža komercijalne usluge bazirane na elD Middleware paketu. Signer.exe jest servisna aplikacija koja internetskim preglednicima omogućava siguran način komunikacije s karticom, dok izdavatelju certifikata omogućava alternativni način komunikacije s karticom te njena specifikacija ne može biti objavljena bez potencijalnog ugrožavanja sigurnosti kartice i podataka na njoj.

AKD ističe kako bilo koji internetski servis ne mora nužno koristiti Signer.exe da bi komunicirao s eOI-jem i izradio e-potpis te kako ničime ne uvjetuje korištenje Signer.exe programa drugim poduzetnicima i nema prednost u tržišnom natjecanju time što se navedeni program koristi u web preglednicima za potrebe izrade e-potpisa. Naime, korištenje navedenog programa iz internetskog preglednika prilikom izrade e-potpisa za potrebe mrežnih usluga nije obvezno, nego je opcija. AKD također naglašava kako drugi poduzetnici nisu spriječeni izraditi vlastiti program ili aplikaciju koja bi omogućila pružanje usluge posredovanja u apliciranju digitalnog potpisa na dokumente preko interneta, bez REST WS API-ja Signer.exe komponente.

Nadalje, AKD navodi kako se certifikati na elektroničkoj osobnoj iskaznici mogu koristiti za digitalno potpisivanje dokumenata putem interneta bez prethodne instalacije elD Middleware paketa te AKD predlaže da eksperti AZTN-a sami pokušaju koristiti certifikate na eOI-ju za elektroničko potpisivanje dokumenata, na primjeru spomenutog internet servisa EU DSS za izradu elektroničkih potpisa i korištenjem predmetne NexU *open source* komponente, umjesto odnosno bez eOI Middleware i bez programa Signer.exe, pri čemu je detaljno opisao postupak kako napraviti navedeno.

AKD smatra kako navedeno potvrđuje da se certifikati na eOI-ju mogu koristiti za elektroničko potpisivanje dokumenata bez prethodne instalacije eOI Middleware paketa ili bilo koje njegove komponente, korištenjem internetske usluge DSS i NexU komponente te AKD u svrhu dokaza po potrebi predlaže demonstrirati gore navedeno i pred nadležnim tijelom AZTN-a.

AKD dalje navodi kako je razlika između NexU komponente i eOI Middlewarea u tome da je NexU komponentu potrebno aktivirati svaki put kad se računalo ponovno pokrene nakon gašenja, dok za korištenje eOI Middlewarea nije potrebna ponovna aktivacija nakon pokretanja računala, zatim nije potrebno znanje formata, pakiranja i algoritama izrade elektroničkog potpisa te ne postoji mogućnost izrade nezakonitog potpisa autentikacijskim certifikatom, što je čest slučaj kad se koristi DSS, Adobe programi i slični, jer eOI Middleware za potpis koristi isključivo potpisni certifikat pa su upravo zbog toga servisi u sklopu e-Građana izabrali njegovo korištenje. Također, valja napomenuti da je u međuvremenu FINA, bez da im je AKD dao tehničke detalje kakve traži podnositelj inicijative, omogućila da korisnici web aplikacije FINA e-Račun elektronički potpisuju račune korištenjem AKD-ovih elektroničkih certifikata i kartica.

Kao dokaz navedenih tvrdnji, odnosno da treće tvrtke mogu samostalno razvijati potpisna rješenja koja koriste osobnu iskaznicu, AKD ističe da postoje i druga trgovačka društva koja su izradila rješenje za potpisivanje PDF dokumenata s eOI-jem, bez dobivanja tehničke specifikacije koju traži i bez koje navodno ne može raditi podnositelj inicijative.

Kao jedan od primjera potencijalnog ugrožavanja sigurnosti eOI kartice, AKD navodi povjerljivu informaciju da [...].

Također, valja napomenuti kako AKD-ove pametne kartice ne zadovoljavaju strogi sigurnosni QSCD standard kako je navedeno, već zadovoljavaju prijelaznu mjeru danu u članku 51. stavku 1. eIDAS uredbe. Da je tome tako, vidljivo je iz javno objavljene liste obavijesti država članica Europske unije o SSCD i QSCD uređajima, koju objavljuje Europska komisija. Iz priloženog je vidljivo da Republika Hrvatska nije prijavila niti jednu QSCD karticu te da je kao izdavatelja eID kartice na popisu SSCD uređaja prijavila AKD.

AKD još jednom ističe kako AKD kID Middleware i eOI Middleware nisu identičan programski paket. Radi se o paketima koji rade sukladno istim standardima (PKCS#11 i MS CAPI) i koji imaju istu arhitekturu, no iako je dio koda zajednički, dio koda se razlikuje te se kID Middleware ne koristi s elektroničkom osobnom iskaznicom (eOI) državljana Republike Hrvatske.

Nadalje, iako AKD-u nisu poznate prepreke tehničke prirode da se u instalaciju programskog paketa eID Middleware priključi i NexU komponenta, AKD smatra da navedeno ne bi bilo svrsishodno te se time ne bi doprinijelo tržišnom natjecanju, odnosno njegovoj većoj zaštiti. Kao što je naveo, imatelji elektroničke osobne iskaznice ionako mogu komponentu NexU samostalno koristiti za digitalno potpisivanje dokumenata, bez potrebe da ona već bude instalirana u paketu eID Middelware. Činjenica da bi NexU komponentna već bila instalirana ne bi doprinijela njenom lakšem korištenju. S druge strane, eOI se može koristiti u svim javnim web servisima dostupnima kroz platformu e-Građani bez NexU komponente, a servis DSS, koji se ne koristi u hrvatskim javnim servisima na platformi e-Građani, u servisu FINA e-Račun i u e-Poreznoj, onima koji ga žele koristiti, daje obavijest da je prethodno potrebno instalirati NexU komponentu i daje upute za to. Dakle, sve su komponente eID Middlewarea uvjetovane tehničkim zahtjevima te AKD ni na bilo koji način utječe na poduzetnike na tržištu posredovanja apliciranja digitalnog potpisa.

AKD se dodatno očitovao podneskom zaprimljenim 14. listopada 2020. te vezano za pitanje AZTN-a bi li uključivanje NexU *open source* komponente bilo tehnički izvodivo, AKD moli AZTN da svakako uzme u obzir i druge razloge, povrh strogo gledane tehničke izvodivosti. Naime, NexU je proizvod koji AKD nije razvio. AKD stoga ne poznaje NexU i ne bi mogao davati podršku građanima za tu komponentu - za ilustraciju, trenutno na *github* stranicama otvorenog projeta NexU ima prijavljenih 5 pogrešaka u radu koje još nisu ispravljene. NexU je proizvod tvrtke Nowina iz Luksemburga koja ga održava i dalje razvija te NexU licenčni model nije isti kao licenčni model eOI Middlewarea.

Što je najvažnije, ističe AKD, intervencija poput dodavanja NexU komponente utjecala bi na već izvršeni strogi postupak notifikacije Republike Hrvatske u smislu članka 9. eIDAS Uredbe, već izvršeni *peer review* te već izdano pozitivno mišljenje Suradničke mreže (Cooperation Network) u smislu članka 14. (i) Provedbene odluke Komisije (EU) 2015/296 o zadovoljavanju zahtjeve eIDAS Uredbe za elektronski identifikacijski sustav te bi bili značajno ugroženi svi do sada izvršeni napori na ovom području, uključujući i na ostvareno priznavanje eOI-ja kod drugih zemalja članica. S tim u vezi, AKD naglašava kako ne postoji primjer države članice Europske unije koja bi zakonski propisala obvezu javne objave tehničke specifikacije programskog sučelja identifikacijske kartice, niti to traži eIDAS uredba.

Nadalje, AKD navodi kako je instalacija NexU-a za građane (krajnje korisnike) tehnički zahtjevnija od instalacije eOI Middlewarea, a nakon svake odjave i prijave korisnika na računalo potrebno je ponovno pokrenuti NexU, što bi sve dodatno opteretilo korisnike certifikata na eOI-ju te bi odvraćalo od korištenja samog eOI-ja i sustava e-Građani. NexU je bio dan kao primjer jednog od rješenja kako iz web usluge putem internetskog preglednika komunicirati s certifikatima na eOI-ju, nakon što je u njima zabranjeno korištenje *Java appleta* iz sigurnosnih razloga.

Informacija kako je u Estoniji dan javno dostupan kod posvećen estonskoj identifikacijskoj kartici točan je, no AKD ističe kako se ne radi o kodu koji je ekvivalentan Signer.exe kodu, niti o kodu koji je razvio, isporučio i održava pružatelj usluga certificiranja, već se radi o dodatnim rješenjima koja su napravili razni estonski poduzetnici. Da bi estonski građani mogli koristiti svoju elektroničku osobnu iskaznicu, oni, slično kao i državljani Republike Hrvatske za eOI, trebaju prvo preuzeti i instalirati programsku podršku („elD software“).

Točno je da je za izradu potpisa, enkripciju i upravljanje PIN i PUK brojevima s estonskom ID karticom javno dostupan izvorni kod (koji nije izradio proizvođač estonske ID kartice) - no s tim se rješenjem izrađuju tzv. ASiC napredni potpisi, koji se u Republici Hrvatskoj ne koriste i stoga nema potrebe za tim formatom potpisa, već državljani Republike Hrvatske u pravilu za svoje privatne potrebe izrađuju PDF elektroničke potpise (za što postoji nekoliko besplatnih alata za izradu potpisa ili rješenja koja su osigurali javni servisi unutar sustava e-Građani), a u e-poslovanju izrađuju se osim potpisa PDF dokumenata još i potpisi XML podataka.

Nadalje, AKD navodi kako certifikati izdani državljanima Republike Hrvatske na eOI-ju nisu namijenjeni za enkripciju, a za potrebe upravljanja PIN i PUK brojevima na kartici državljani Republike Hrvatske nakon instaliranja elD Middlewarea za to imaju na raspolaganju program eClient.exe, tako da estonski primjer davanja rješenja za izradu ASiC potpisa, enkripciju i upravljanje PIN/PUK brojevima i izvornog koda tog rješenja nije relevantan niti primjenjiv za eOI. Kao ilustraciju koliko je važna sigurnosna zaštita certifikata i privatnih ključeva osobnih iskaznica, AKD navodi da je u kolovozu 2017. otkrivena sigurnosna prijetnja koja je zahvatila 750.000 estonskih osobnih iskaznica i boravišnih kartica izdanih između 16. listopada 2014. i 26. listopada 2017., radi čega su morali biti opozvani svi certifikati sadržani na tim iskaznicama.

AKD ističe kako je od približno [...] izdanih eOI-ja u Republici Hrvatskoj samo približno [...] državljana koristilo svoj autentikacijski certifikat za prijavu na sustav e-Građani putem NIAS-a. Objavom tehničke specifikacije programa Signer.exe iz elD Middlewarea stoga ne bi bila omogućena nikakva funkcionalnost vezana za potpisivanje certifikatima s eOI-ja, a koja već nije javno dostupna.

Kao potvrdu prethodne tvrdnje, AKD navodi primjenu eOI-ja u web uslugama koje građani koriste iz internetskog preglednika, a koje su razni poslovni subjekti izradili bez da im je AKD dao tehničku specifikaciju programa Signer.exe, već se s certifikatima na kartici komunicira putem jednog od dva standardna protokola, PKCS#11 i/ili MS CAPI:

- poduzetnik [...] razvojem vlastitog rješenja omogućio je portalu ePorezna korištenje AKD-ovih certifikata, što je i navedeno na portalu ePorezna;
- FINA je omogućila korištenje AKD-ovih certifikata u servisu eračun;
- poduzetnik Nowina iz Luksemburga (usluga je dostupna na https://ydss.noyyina.lu/sign-adocument), korištenjem fondova Europske unije, izgradio je, implementirao i održava Digital Signature Service (DSS) web uslugu i NexU komponentu, koja zaobilazi zabranu izvođenja *Java appleta* u internetskim preglednicima te koja za komunikaciju s karticama i certifikatima izdanim od svih pružatelja usluga povjerenja koji izdaju certifikate u Europskoj uniji (koju komponentu potpisnik mora sam pronaći, instalirati i nakon svakog pokretanja računala ponovno pokrenuti) koristi sljedeće protokole javno objavljenih tehničkih specifikacija: PKCS#11, MS CAPI (za komunikaciju s pametnim karticama) i PKCS#12 (za komunikaciju s datotekama s certifikatima, nije primjenljivo za eOI);
- poduzetnik [...] omogućuje potpisivanje građevinskih projekata koristeći AKD-ove certifikate s eOI-ja, kojima se pristupa bez korištenja Signer.exe programa;
- poduzetnik [...] prihvaća certifikate s eOI-ja za utvrđivanje elektroničkog identiteta u svojem [...] a da mu AKD prethodno nije učinio dostupnom tehničku specifikaciju programa Signer.exe.

AKD također ponovno napominje da su eID Middleware i komercijalni kID Middleware arhitekturalno, namjenom i brojem komponenti slična, ali funkcionalno odvojena programska rješenja. Certifikati koji se izdaju na komercijalnim (kID) karticama sadržajno se razlikuju od certifikata koji se izdaju građanima jer kID certifikati dodatno sadržavaju informaciju (identifikator i naziv) poslovnog subjekta s kojima je osoba subjekt certificiranja povezana te u tom smislu predstavljaju posebno rješenje za specifične komercijalne potrebe nekih klijenata, npr. strukovnih udruženja.

Oba Signer.exe programa (u sklopu eID i kID Middleware) javno su dostupna svim krajnjim korisnicima, fizičkim osobama koje žele koristiti AKD kartice i certifikate, a poslovnim subjektima, pravnim osobama, tvrtkama i poduzetnicima koji trebaju tehničku specifikaciju kako komunicirati s AKD-ovim karticama i certifikatima na raspolaganju su PKCS#11 i MS CAPI javno objavljene tehničke specifikacije, s kojima sve AKD-ove kartice s certifikatima mogu komunicirati.

AKD posebno ističe kako će se, radi usklađivanja s regulativom Europske unije o identifikacijskim dokumentima, za manje od godine dana državljanima Republike Hrvatske početi izdavati eOI kartice druge generacije, na kojoj će biti biometrijski podaci nositelja, i uz koju će dobiti pravo na korištenje udaljenog osobnog kvalificiranog potpisnog certifikata, sukladno članku 2. prijedloga izmjene Zakona o osobnoj iskaznici: *„(7) Osoba koja je aktivirala programsko rješenje za pokretne uređaje iz stavka 6. ovoga članka i ima izdan potpisni certifikat na osobnoj iskaznici, ostvaruje pravo na udaljeni osobni kvalificirani potpisni certifikat.“* Udaljenim potpisnim certifikatom u ime osobe subjekta certificiranja upravljat će kvalificirani pružatelj usluge certificiranja, što je u trenutku pisanja ovog teksta AKD.

Za korištenje udaljenog certifikata (za izradu kvalificiranog elektroničkog potpisa) građanima će biti potreban pametni telefon s instaliranom aplikacijom za identifikaciju i lozinka koju su prilikom aktivacije udaljenog certifikata zadali i koju samo oni znaju, što će u znatnoj mjeri povećati opseg korištenja osobnih certifikata građana. Za korištenje udaljenih certifikata neće biti potreban Middleware niti Signer.exe niti driver za čitač kartica.

Zaključno, AKD navodi da su sve komponente eID Middlewarea uvjetovane tehničkim zahtjevima te AKD ni na bilo koji način ne utječe na poduzetnike na tržištu posredovanja u apliciranju digitalnog potpisa. Slijedom svega navedenog, razvidno je da otkrivanje Signer.exe programa uopće nije nužno potrebno drugim poduzetnicima te da oni već mogu razvijati svoja rješenja bazirana na čak dva otvorena standarda (PKCS#11 i MS CAPI), a što neki već i čine. Stoga nije točno da bi AKD na bilo koji način narušio tržišno natjecanje zlouporabom vladajućeg položaja u smislu članka 13. ZZTN-a te su navodi podnositelja inicijative u cijelosti neosnovani.

6.2. Dodatno očitovanje podnositelja inicijative

AZTN je 8. listopada 2020. zaprimio očitovanje podnositelja inicijative, u čijem je privitku dostavio presudu Upravnog suda u Zagrebu od [...], kojom se odbija tužbeni zahtjev za poništenje rješenja Ministarstva unutarnjih poslova, Policijske uprave zagrebačke, Sektora za imigraciju, državljanstvo i upravne poslove, [...]. Osporavanim rješenjem tuženika (MUP) odbijen je zahtjev tužitelja (podnositelja inicijative) za izdavanje osobne iskaznice.

Podnositelj inicijative navodi kako je priloženom presudom Upravni sud u Zagrebu odbacio njegovu tužbu protiv rješenja MUP-a kojom mu se odbija izdavanje osobne iskaznice bez potpisivanja ugovora s AKD-om te smatra kako je presuda važna jer dokazuje zakonsku obvezu potpisa ugovora s AKD-om i samim time AKD stavlja u povlašteni položaj u odnose na ostale poduzetnike.

6.3. Očitovanja trećih strana

AKD je u svojim očitovanjima prema AZTN-u naveo tri poslovna subjekta u Republici Hrvatskoj koji su razvili vlastite usluge, a da im AKD prethodno nije dao tehničku specifikaciju programa Signer.exe, koje omogućavaju korisnicima eOI-ja da s pripadajućim certifikatima preko interneta komuniciraju putem jednog od dva standardna protokola, PKCS#11 i/ili MS CAPI. Riječ je o poduzetnicima [...], [...] i [...]. Stoga je AZTN zatražio očitovanja od navedenih poduzetnika.

Iz njihovih očitovanja, zaprimljenih u AZTN-u u razdoblju od 22. travnja 2020. do 1. prosinca 2020., proizlazi kako poduzetnici [...] i [...] nemaju razvijena vlastita rješenja koja bi omogućavala imateljima eOI-ja potpisivanje dokumenata putem interneta korištenjem eOI-ja i pripadajućih certifikata, dok je [...] razvio vlastito rješenje za Poreznu upravu Ministarstva financija Republike Hrvatske (dalje u tekstu: Porezna uprava) koje omogućava potpisivanje dokumenata preko interneta.

Poduzetnik [...] naveo je u svojim očitovanjima, zaprimljenim 22. travnja 2020. i 6. svibnja 2020. tijekom prethodnog ispitivanja stanja na mjerodavnom tržištu, kako je Poreznoj upravi pružio uslugu projektiranja i razvoja programske podrške (softvera) prema [...]. Predmet i opseg usluga opisani su u dokumentu Opis poslova, koji je dostavio u privitku očitovanja. [...] navodi kako ne pruža niti je pružao druge usluge Poreznoj upravi vezane za predmet upita AZTN-a.

Kao poslovni korisnik sustava ePorezna, [...] navodi da se sustav elektroničkih usluga ePorezna ne može koristiti za generiranje identifikacijskog i potpisnog certifikata i izdavanje certifikata na kriptografskim uređajima (pametne kartice, USB tokeni) ili „na daljinu“ te kako su korištenje sustava elektroničkih usluga i podržane funkcionalnosti sustava ePorezna opisani na stranicama Porezne uprave i u korisničkom priručniku.

Nadalje, [...] navodi kako nikad nije razvio vlastito programsko rješenje korištenjem javno nedostupnih komponenti. Sva njegova programska rješenja koja se tiču kriptografskih operacija bazirana su na PKCS#11 standardu i Microsoft Crypto APl bibliotekama, koje su dio operativnog sustava Microsoft Windows. Komponente navedene u upitu AZTN-a (REST WS API, Signer.exe) [...] nije nikada koristio u razvoju svojih programskih rješenja.

Sva prava na programsko rješenje po predmetnom ugovoru [...]. Kao poslovni korisnik sustava ePorezna, [...] navodi da imatelj eOI-ja korištenjem sustava ePorezna može elektronički potpisivati porezne obrasce / dokumente stvorene isključivo u sustavu ePorezna preko internetskog preglednika kojim se pristupa tom istom sustavu. Proces potpisivanja odvija se lokalno na računalu korištenjem standardnog programskog sučelja PKCS#11 / Microsoft CryptoAPI koje je dio operativnog sustava Microsoft Windows.

Prema navodima [...], usluge projektiranja i razvoja programske podrške (softvera) koje su bile predmet [...] mogu pružiti i svi drugi poduzetnici registrirani za predmetnu djelatnost, bez ograničenja, sukladno svojim tehničkim i stručnim kapacitetima.

7. Činjenice utvrđene u postupku

U nastavku se analizira postupanje poduzetnika AKD u konkretnom postupku.

7.1. Opis usluge AKD-a

U sklopu izdavanja certifikata za eOI, AKD korisnicima nudi i upute za preuzimanje i instaliranje programskog paketa eID Middleware. Predmetni paket integrira eOI s računalom na kojem se koriste njegove funkcionalnosti te omogućava imateljima eOI-ja korištenje identifikacijskog i/ili potpisnog certifikata sadržanog na osobnim iskaznicama. Zahvaljujući certifikatima koji se nalaze na osobnim iskaznicama, građani imaju mogućnost, posredstvom tog programskog paketa te kupnjom pripadajućeg čitača pametnih kartica, pristupati određenim servisima putem identifikacijskog certifikata (npr. e-Građani) ili potpisivati dokumente i slično potpisnim certifikatom.

Navedeni programski paket korisnici mogu preuzeti na mrežnim stranicama www.eid.hr, a sastoji se od sljedećih komponenti:

1. eID Mini Driver - upravljački program,
2. eID PKCS#11 (eng. *Public Key Cryptography Standard*) - standardno aplikacijsko programsko sučelje za rad s kriptografskim uređajima,
3. eID Client - grafička aplikacija,
4. eID Signer - komponenta koja omogućava komunikaciju mrežnim aplikacijama s eOI-jem i
5. eID CA Certificates - prisutni certifikati autorizacijskog tijela.

Korisnici, imatelji eOI-ja, mogu slobodno preuzeti i instalirati eID Midleware programski paket bez dodatne naknade, za što im je samo potrebno računalo i internetska veza. Instaliranjem predmetnog paketa na osobno računalo, imatelji eOI-ja, koji sadrži identifikacijski i potpisni certifikat, imaju mogućnost pristupanja javnim elektroničkim servisima, poput e-Građana i drugih servisa, te imaju mogućnost potpisivati dokumente kvalificiranim elektroničkim potpisom putem interneta.

Prema očitovanju podnositelja inicijative i AKD-a, nakon zabrane *Java appleta* u internetskim preglednicima bilo je potrebno razviti dodatno programsko rješenje, međusoftver, koji bi omogućio da oni na siguran način dozvoljavaju pristupanje i korištenje elektroničkim certifikatima na eOI-ju, bez čega internetski preglednici ne bi dozvoljavali rad s eOI-jem. Upravo iz navedenog razloga AKD je razvio eID Signer (Signer.exe).

Signer.exe servisna je aplikacija koja izdavatelju certifikata omogućava komunikaciju s karticom. Upravo je predmetna aplikacija predmet ove inicijative. Podnositelj inicijative smatra kako je AKD dužan objaviti *Representational state transfer Web services Application programming interface* (dalje u tekstu: REST WS API), odnosno aplikacijsko programsko sučelje predmetne komponente, te omogućiti interoperabilnost njemu, kao i ostalim zainteresiranim poduzetnicima na mjerodavnom tržištu, kako bi i oni mogli nesmetano pružati uslugu posredovanja u apliciranju kvalificiranog elektroničkog potpisa putem interneta.

Istovremeno, AKD pruža i komercijalnu uslugu, koja je, prema navodima podnositelja inicijative, bazirana na eID Middleware programskom paketu.

Sam AKD navodi kako za komercijalne potrebe izrađuje lepezu kartica i niz certifikata koji su namijenjeni svima, uglavnom poslovnim subjektima, ali i građanima koji žele imati vlastitu poslovnu ili osobnu karticu ili iskaznicu, s opcijom instalacije autentikacijskog i/ili potpisnog certifikata sukladnog s eIDAS uredbom. Sljedeće kartice izrađuje AKD, a što je razvidno i na pripadajućim mrežnim stranicama (https://www.id.hr/hr/proizvodi-i-usluge):

- Poslovna kartica, koja omogućava korisniku sigurnu *online* elektroničku identifikaciju. S njom se korisnici mogu prijaviti na računalo, bilo koju aplikaciju ili pristupati državnim servisima dostupnim iz e-Građana. Na kartici se nalazi i kvalificirani elektronički certifikat. Korisniku omogućava elektroničko potpisivanje Word, Excel ili PDF dokumenata;

- Poslovna NFC kartica, koja omogućava sigurnu *online* elektroničku identifikaciju. S njom se korisnici mogu prijaviti na računalo, bilo koju poslovnu aplikaciju ili pristupati državnim servisima dostupnim iz e-Građana. Na kartici se nalazi i kvalificirani elektronički certifikat. Korisniku omogućava elektroničko potpisivanje Word, Excel ili PDF dokumenata. Uz certifikate, kartica sadrži i dodatan beskontaktni čip. Koristiti se može za evidencije radnog vremena (ERV), parking rampe, otvaranje vrata, kontrolu printanja i slično;
- Kartica s pečatom, koja omogućava zamjenu fizičkog pečata. To znači da korisnici te kartice dokument ne trebaju printati kako bi ga pravovaljano ovjerili. Korisniku omogućava elektroničko pečatiranje Word, Excel ili PDF dokumenata.

Navedene se kartice dodatno mogu personalizirati, dodavati dodatni korisnički podaci na čip, dizajnirati tijelo kartice prema potrebi korisnika i dodavati 1D/2D barkod.

Sljedeće komercijalne certifikate izdaje AKD uz naknadu:
- certifikati za autentikaciju,
- certifikati za potpis,
- certifikati za pečat,
- udaljeni certifikati za potpis i
- udaljeni certifikati za pečat.

Kako bi korisnicima i internetskim servisima omogućio korištenje komercijalnih kartica, AKD na web stranicama za podršku nudi softverski paket kID Middleware, koji sadrži program za aktivaciju kartice i upravljanje PIN-ovima, standardnu PKCS#11 biblioteku za rad s karticom (za autentikaciju i izradu elektroničkih potpisa), minidriver za korporativnu karticu, aplikaciju koja omogućava da web preglednici komuniciraju s karticom (Signer.exe), iz razloga što je u web preglednicima iz sigurnosnih razloga zabranjeno izravno komuniciranje s kriptografskim uređajima, te AKD KIDCA i AKD Root CA certifikate.

AZTN je izvršio uvid u komponente eID Middleware programskog paketa i kID Middleware programskog paketa te je njihova usporedba prikazana u tablici 1. Naime, oba programska paketa javno su dostupna za preuzimanje putem interneta na pripadajućim internetskim stranicama te je prilikom instalacije moguće odabrati koje komponente korisnik želi instalirati.

Tablica 1. Pripadajuće komponente programskih paketa eID Middleware i kID Middleware

eID Middleware komponente	**kID Middleware komponenete**
eID Mini Driver	eID Mini Driver > AKD kID Card
eID PKCS#11	eID PKCS#11
eID Client	eID Client
eID Signer	eID Signer
eID CA Certificates	kID CA Certificates

Izvor: mrežne stranice www.eOI.hr i www.id.hr
Obrada: AZTN

Iz tablice je razvidno kako, izuzev pripadajućih certifikata, sve ostale komponente imaju isti naziv te se odnose na eID, odnosno eOI. Jedino komponenta eID Mini Driver kod programskog paketa sadrži i podkomponentu AKD kID Card. Sporna komponenta Signer.exe, odnosno eID Signer, ista je kod oba programska paketa. Podnositelj inicijative i sam je naveo kako se radi o istom softveru, odnosno kako AKD softver koji je razvio za javne potrebe, a koji je plaćen javnim sredstvima, koristi za svoje komercijalne potrebe, čime stječe prednost na tržištu pred ostalim potencijalnim konkurentima.

Međutim, AKD napominje da su elD Middleware i komercijalni kID Middleware arhitekturalno, namjenom i brojem komponenti slična, ali funkcionalno odvojena programska rješenja. Certifikati koji se izdaju na komercijalnim (kID) karticama sadržajno se razlikuju od certifikata koji se izdaju građanima, jer kID certifikati dodatno sadržavaju informaciju (identifikator i naziv) poslovnog subjekta s kojima je osoba subjekt certificiranja povezana te u tom smislu predstavljaju posebno rješenje za specifične komercijalne potrebe nekih klijenata, npr. strukovnih udruženja.

Oba Signer.exe programa (u sklopu elD i kID Middleware) javno su dostupna svim krajnjim korisnicima, fizičkim osobama koje žele koristiti AKD kartice i certifikate, a poslovnim subjektima, pravnim osobama, tvrtkama i poduzetnicima koji trebaju tehničku specifikaciju kako komunicirati s AKD karticama i certifikatima, na raspolaganju su PKCS#11 i MS CAPI javno objavljene tehničke specifikacije, s kojima sve AKD kartice s certifikatima mogu komunicirati.

EID Mini Driver komponenta upravljački je program, tj. upravljačka komponenta. PKCS#11, skraćenica za *Public Key Cryptography Standard*, sukladno objašnjenju AKD-a, definira aplikacijsko programsko sučelje (API) za rad s kriptografskim uređajima, koje je neovisno o platformi tj. operativnom sustavu računala, što uključuje i rad s pametnim karticama, kakav je i eOI. Taj API definira najčešće korištene kriptografske tipove objekata (RSA ključevi, X.509 certifikati, DBS / Triple DBS tipke itd.) i sve funkcije potrebne za upotrebu, stvaranje / generiranje, izmjenu i brisanje tih objekata.

AKD zaključno još jednom ističe kako AKD kID Middleware i eOI Middleware nisu identičan programski paket. Radi se o paketima koji rade sukladno istim standardima (PKCS#11 i MS CAPI) i koji imaju istu arhitekturu, no iako je dio koda zajednički, dio koda se razlikuje te se kID Middleware ne koristi s eOI-jem.

7.2. Navodi o odbijanju poslovanja

Podnositelj inicijative navodi kako AKD odbija objaviti REST WS API komponente Signer.exe te na taj način onemogućava ostale zainteresirane poduzetnike u izradi vlastitih komercijalnih programskih rješenja kojim bi korisnicima eOI-ja omogućili elektroničko potpisivanje putem interneta.

Sukladno kriterijima iz Priopćenja Komisije - Upute o provedbenim prioritetima Komisije u primjeni članka 82. Ugovora o EZ-u na postupanje poduzetnika u vladajućem položaju koja za posljedicu mogu imati zlouporabu u smislu isključivanja konkurenata s tržišta (Službeni list C 045, 24. veljače 2009.; dalje u tekstu: Uputa Komisije), odbijanje poslovanja obuhvaća postupanje poduzetnika u vladajućem položaju kada odbija prodati svoj proizvod ili pružiti uslugu drugom poduzetniku na silaznom tržištu (točka 76.). U biti, riječ je o uskrati onog proizvodnog čimbenika nužnog na silaznom tržištu, koji taj poduzetnik kontrolira s razine onog tržišta na kojem se nalazi u vladajućem položaju. Tipični slučajevi odbijanja poslovanja stoga su oni u kojima sudjeluje vertikalno integrirani poduzetnik u vladajućem položaju.

U točki 81. navedenih Uputa Komisije, tri uvjeta moraju biti kumulativno ispunjena da bi mogla biti riječ o zlouporabnom odbijanju poslovanja:

- odbijanje opskrbe odnosi se na proizvod ili uslugu koji su objektivno nužni za učinkovito tržišno natjecanje na silaznom tržištu,
- postoji vjerojatnost narušavanja učinkovite tržišne utakmice na silaznom tržištu i
- postoji vjerojatnost nanošenja štete potrošačima.

Slijedom navedenog, primarno je potrebno utvrditi je li proizvod, u ovom slučaju eID Middleware odnosno njegova komponenta Signer.exe, objektivno nužan za učinkovito tržišno

natjecanje na silaznom tržištu, odnosno tržištu posredovanja u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta.

Pritom valja naglasiti kako, sukladno točki 83. Uputa Komisije, kriterij nužnosti inputa ne znači da bez odbijenog inputa niti jedan konkurent nikada ne bi mogao ući na silazno tržište ili na njemu opstati, već je on nužan kada ne postoji stvaran ili potencijalan zamjenski proizvod (supstitut) na koji bi se konkurenti na silaznom tržištu mogli osloniti kako bi dugoročno barem ublažili negativne posljedice odbijanja opskrbe predmetnim inputom.

Signer.exe komponenta jest međusoftver koji omogućava nesmetanu i sigurnu komunikaciju drugih aplikacija ili programskih rješenja s certifikatima sadržanim na eOI-ju putem internetskog preglednika. Prilikom instalacije eID Middleware programskog paketa, komponenta eSigner, odnosno Signer.exe, instalira se i automatski pokreće s Windowsima (ili drugim operativnim sustavom) te se koristi prilikom potpisivanja dokumenata putem interneta. Signer.exe je kompatibilan s najčešće korištenim internetskim preglednicima i za njegov rad nije potrebna nikakva intervencija korisnika u vidu konfiguracije programa.

AKD u svom očitovanju ističe kako korištenje komponente Signer.exe nije preduvjet da bi internetski servisi mogli izraditi elektronički potpis korištenjem eOI-ja te da bilo koji poduzetnik koji putem internetskih servisa i vlastitih rješenja želi koristiti eOI za izradu elektroničkog potpisa može, bilo korištenjem nekog svojeg vlastitog rješenja, bilo putem NexU komponente DSS servisa, a bez korištenja Signer.exe komponente, izraditi e-potpis. Dodatno, prema AKD-u svaki poduzetnik koji zna otvorene standarde PKCS ili MS CAPI nije spriječen izraditi vlastiti program ili aplikaciju koja bi mu omogućila pružanje usluge posredovanja u apliciranju elektroničkog potpisa na dokumente putem interneta, odnosno kojom bi omogućio imateljima eOI-ja elektroničko potpisivanje dokumenata putem interneta korištenjem njegove aplikacije ili programa, bez REST WS API-ja Signer.exe komponente.

MS CAPI, ili Microsoft Crypto API, standardno je aplikacijsko programsko sučelje koje je dio operativnog sustava Microsoft Windows. To je skup dinamički povezanih biblioteka koje pružaju sloj apstrakcije koji programere izolira od koda koji se koristi za šifriranje podataka. PKCS *(Public Key Cryptography Standards)* jest aplikacijsko programsko sučelje koje nije vezano za određeni operativni sustav, već je platformski neovisno. Razvio ga je poduzetnik RSA Laboratories zajedno s ostalim zainteresiranim sudionicima.

AKD tvrdi kako s certifikatima i privatnim ključem na osobnoj iskaznici državljana Republike Hrvatske, odnosno eOI-jem, mogućnost komunikacije ima svaka e-usluga / program / rješenje koje koristi PKCS#11 ili MS CAPI protokole, poput javne usluge Porezne uprave -ePorezna, koja ne koristi AKD-ov Signer.exe, već koristi rješenje poduzetnika [...], koji je taj servis izgradio za Poreznu upravu, a koje radi s eOI-jem i drugim sigurnim kriptografskim uređajima baziranim na PKCS#11 i MS CAPI standardima.

Iz [...] očitovanja proizlazi kako je na temelju [...] razvio programsko rješenje za elektronički sustav e-Porezna, koje, pored ostalih usluga, omogućava imateljima eOI-ja da u njemu potpisuju dokumente i obrasce putem interneta. Kako sam navodi, navedeno je rješenje razvio na temelju PKCS#11 standarda i MS Crypto API biblioteka koje su dio operativnog sustava Microsoft Windows, a takvo programsko rješenje mogu razviti bez ograničenja i bilo koji drugi poduzetnici registrirani za predmetnu djelatnost, sukladno svojim tehničkim i stručnim kapacitetima.

Dakle, na primjeru [...] proizlazi kako je zaista moguće samostalno razviti programsko rješenje koje će omogućiti imateljima eOI-ja potpisivanje dokumenata putem interneta, bez ulaznih inputa (Signer.exe komponente) AKD-a.

Nadalje, kao međusoftver za eOI moguće je koristiti i servis Europske unije DSS. Riječ je o *open source* softverskom rješenju poduzetnika Nowina Solutions iz Luksemburga, kojim se omogućava elektroničko potpisivanje dokumenata putem interneta. DSS je aplikacija koja je besplatno dostupna na internetu svim korisnicima bez ikakve naknade, a pomoću komponente NexU omogućava potpisivanje dokumenata koristeći internetske preglednike. NexU je rješenje slično Signer.exe rješenju i potrebno je radi omogućavanja komunikacije s pametnim karticama, odnosno certifikatima, nakon zabrane *Java appleta* u internetskim preglednicima. Dakle, ako imatelj eOI-ja želi potpisati neki dokument koristeći DSS servis, a pod pretpostavkom da je deinstalirao ili isključio Signer.exe, može preuzeti i instalirati NexU komponentu, nakon čega može nesmetano potpisivati dokumente putem interneta.

Podnositelj inicijative potvrdio je u svom očitovanju kako postoje supstitucije za program Signer.exe, primjerice ranije spomenuti program NexU, a također navodi kako bi i on mogao izraditi takav međusloj, ali da to nema smisla pored već dostupnih gotovih komponenti , pri čemu ističe kako korisnik prilikom instalacije eID Middleware paketa već ima instaliran međusloj (Signer.exe) koji mu omogućava potpisivanje dokumenata u internetskoj aplikaciji AKD-a, dok on i svi ostali konkurenti AKD-a moraju korisnika navoditi na instalaciju dodatne programske podrške, odnosno korisnik mora instalirati eID Middleware, a pored njega i dodatan program koji će služiti kao međusloj, pri čemu ponekad samu instalaciju ne rade korisnici na računalu niti imaju administratorska prava da bi to uopće mogli učiniti. Navedeno podnositelj inicijative smatra tehničkom preprekom, i to nepremostivom.

Međutim, navedeni stav podnositelja inicijative AZTN ne smatra utemeljenim, budući da se instalacija konkurentskog programskog rješenja, iako predstavlja određenu dodatnu aktivnost u odnosu na AKD-ov prethodno instalirani međusoftver, u kontekstu ocjene neophodnog inputa nikako ne može smatrati nepremostivom tehničkom preprekom. Riječ je o radnji koju je potrebno napraviti samo jednom, nakon čega je međusoftver instaliran i može se koristiti kao supstitut komponente Signer.exe eID Middleware paketa. Pritom se, budući da je kod DSS-a riječ o *open source* rješenju i izvorni je kod programa dostupan svima, instalacija tog paketa može prilagoditi različitim potrebama korisnika.

Slijedom navedenog, utvrđeno je kako Signer.exe komponenta ne predstavlja neophodan *input* za djelovanje na silaznom tržištu posredovanja u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta. Budući da time nije ispunjen jedan od prethodno obrazložena tri kumulativna uvjeta za postojanje zlouporabe vladajućeg položaja odbijanjem poslovanja, utvrđeno je kako AKD nije niti mogao počiniti tu zlouporabu, u smislu članka 12. ZZTN-a.

7.3. Navodi o vezanoj prodaji

U očitovanju zaprimljenom u AZTN-u 21. veljače 2020., podnositelj inicijative spominje praksu Europske komisije u Predmetu *Microsoft*, a u odnosu na vezivanje Windows Media Playera s operativnim sustavom Windows, gdje je Europska komisija utvrdila zlouporabu vladajućeg položaja te nametnula obvezu Microsoftu da obustavi isporuku Windows Media Playera u kompletu s operativnim sustavom Windows. S tim u vezi, podnositelj inicijative u očitovanju zaprimljenom u AZTN-u 21. veljače 2020. navodi da, s obzirom na to da Signer.exe nije nužno potreban za pružanje usluge certificiranja i da postoje alternative, AKD treba ili obustaviti distribuciju te komponente zajedno sa svim ostalim komponentama potrebnim za rad eOI-ja ili omogućiti svima jednake uvjete korištenja navedene komponente.

Sukladno točki 869. presude Općeg suda u predmetu *Microsoft*, koja je dio pravne stečevine Europske unije, da bi došlo do zlouporabe vladajućeg položaja vezanom prodajom, odnosno vezivanjem, trebaju biti ispunjena četiri uvjeta, i to:

a) vezujući i vezani proizvod dva su različita proizvoda,
b) poduzetnik se nalazi u vladajućem položaju na tržištu vezujućeg proizvoda,

c) poduzetnik ne daje kupcima mogućnost pribavljanja vezujućeg proizvoda bez vezanog proizvoda,
d) vezivanje ograničava tržišno natjecanje.

AZTN je u postupku utvrdio kako je prilikom preuzimanja i instalacije eID Middleware programskog paketa moguće odabrati instalaciju paketa bez Signer.exe komponente, isto kao i u slučaju komercijalne kID kartice, odnosno kID Middleware paketa. Budući da time nije ispunjen jedan od četiri kumulativno potrebna uvjeta, pod točkom c), ne postoje indicije da je AKD zlouporabio vladajući položaj vezanom prodajom Signer.exe komponente.

7.4. Ostali navodi podnositelja inicijative

Što se tiče navoda podnositelja inicijative kako se postupanjem AKD-a krše načela Zakona o državnoj informacijskoj infrastrukturi („Narodne novine“, br. 92/14) te Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, AZTN za navedeno nije nadležan.

U konkretnom slučaju nije prihvaćen prijedlog podnositelja inicijative za izvođenjem dokaza vještačenjem budući da su činjenice bitne za donošenje odluke u ovom predmetu o postojanju stvarnih i potencijalnih zamjenskih rješenja koja omogućuju imateljima eOI-ja potpisivanje dokumenata putem interneta bez potrebe korištenja AKD-ovog međusoftvera eID Middleware i njegove komponente Signer.exe, utvrđene, između ostalog, i navodima samog podnositelja inicijative.

8. Odluka Vijeća za zaštitu tržišnog natjecanja

Na temelju dostavljene dokumentacije i utvrđenog činjeničnog stanja, savjesnom i detaljnom ocjenom svakog dokaza posebno i svih dokaza zajedno, Vijeće za zaštitu tržišnog natjecanja (dalje u tekstu: Vijeće), na sjednici 6/2021., održanoj 3. ožujka 2021. godine, razmatralo je navedeni predmet te je na temelju članka 30. točke 2., članka 31. i članka 58. stavka 1. točke 13. ZZTN-a donijelo odluku kojom se utvrđuje da AKD nije narušio tržišno natjecanje zlouporabom vladajućeg položaja na mjerodavnom tržištu distribucije međusoftvera za elektroničku osobnu iskaznicu, u smislu članka 13. ZZTN-a.

Vijeće svoju odluku obrazlaže kako slijedi:

Predmetni je postupak pokrenut povodom inicijative poduzetnika yottabyte u kojoj se navodi da AKD-ovo odbijanje ustupanja REST WS API-ja komponente međusoftvera eID Middleware Signer.exe predstavlja zlouporabu vladajućeg položaja, u smislu članka 13. ZZTN-a. Također, u tijeku postupka, podnositelj inicijative naznačio je kako smatra spornim i vezanu prodaju Signer.exe komponente unutar eID Middleware paketa.

AZTN je u postupku utvrdio kako je AKD jedini poduzetnik na tržištu u Republici Hrvatskoj koji je ovlašten za izradu eOI-ja i izdavanje kvalificiranih certifikata na eOI-ju (identifikacijskih i potpisnih), a koje koriste, odnosno koje su dužni posjedovati svi državljani Republike Hrvatske. S obzirom na navedeno, zaključeno je da se AKD nalazi u vladajućem položaju na tržištu izdavanja certifikata za eOI, u smislu članka 12. ZZTN-a.

Budući da je za aktivaciju eOI-a potrebno prethodno instalirati AKD-ov međusoftver eID Middleware te se bez tog koraka nije moguće koristiti pripadajućim certifikatima, utvrđeno je kako se AKD nalazi u vladajućem položaju, u smislu članka 12. ZZTN-a, i na tržištu distribucije međusoftvera za eOI.

Analizom postupanja AKD-a u kontekstu potencijalne zlouporabe vladajućeg položaja odbijanjem ustupanja REST WS API-ja komponente međusoftvera eID Middleware Signer.exe podnositelju inicijative, zaključeno je kako nije ispunjen prvi od tri kumulativna uvjeta za utvrđivanje zlouporabe iz Uputa Komisije, a to je da se odbijanje opskrbe odnosi na proizvod ili uslugu koji su objektivno nužni za učinkovito tržišno natjecanje na silaznom tržištu.

Naime, utvrđeno je kako postoje stvarna i potencijalna zamjenska rješenja koja omogućuju imateljima eOI-ja potpisivanje dokumenata putem interneta bez potrebe korištenja AKD-ovog međusoftvera eID Middleware i njegove komponente Signer.exe.

Konkretno, riječ je o programskom rješenju Europske unije DSS i njegovoj komponenti NexU, koja omogućava imateljima eOI-ja alternativan način potpisivanja dokumenata putem interneta korištenjem pripadajućih certifikata.

Također, iz očitovanja poduzetnika [...], koji je razvio programsko rješenje za Poreznu upravu u sklopu sustava ePorezna, proizlazi kako ga je taj poduzetnik razvio bez bilo kakvih *inputa* od strane AKD-a, koristeći javno dostupne PKCS#11 standarde i MS Crypto API biblioteke za Microsoft Windows sustav, što može učiniti i bilo koji drugi zainteresirani poduzetnik, a što izrijekom potvrđuje i sam podnositelj inicijative.

Slijedom navedenog, utvrđeno je kako komponenta Signer.exe ne predstavlja neophodan *input* za učinkovito tržišno natjecanje na silaznom tržištu posredovanja u apliciranju kvalificiranog elektroničkog potpisa izrađenog korištenjem kvalificiranih certifikata s eOI-ja putem interneta. Budući da time nije ispunjen jedan od tri kumulativna uvjeta za postojanje zlouporabe vladajućeg položaja odbijanjem poslovanja, utvrđeno je kako AKD nije niti mogao počiniti tu zlouporabu, u smislu članka 13. ZZTN-a.

Pritom AZTN nije uvažio navode podnositelja inicijative kako instalacija dodatnog programa, pored eID Middlewarea, predstavlja nepremostivu tehničku prepreku, budući da je riječ o radnji koju je potrebno napraviti samo jednom, nakon čega je međusoftver instaliran i može se koristiti kao supstitut komponente Signer.exe eID Middleware paketa, pri čemu se zbog otvorene dostupnosti izvornog koda DSS-a taj paket može prilagoditi različitim potrebama korisnika.

Također, utvrđeno je kako AKD u pogledu Signer.exe komponente ne provodi vezanu prodaju, budući da se programski paket eID Middleware može instalirati i bez nje, pa tako nije ispunjen jedan od četiri kumulativna uvjeta iz Presude Općeg suda u predmetu *Microsoft*.

Stoga je AZTN, na temelju odluke Vijeća, odlučio kao u izreci ovoga rješenja.

Uputa o pravnom lijeku

Protiv ovog rješenja nije dopuštena žalba, ali se u roku od trideset (30) dana od dana dostave ovoga rješenja može tužbom pokrenuti upravni spor pred Visokim upravnim sudom Republike Hrvatske.

Zamjenica predsjednika Vijeća
za zaštitu tržišnog natjecanja

Vesna Patrlj, dipl. iur.

Napomena:
Sukladno članku 53. ZZTN-a, podaci koji predstavljaju poslovnu tajnu izuzeti su od objavljivanja te su u tekstu navedeni podaci označeni [...].