PRIMJENA ELEKTRONIČKIH POTPISA U DOMENI SIGURNOSTI I ZAŠTITE

Zanić, Marino

PRIMJENA ELEKTRONIČKIH POTPISA U DOMENI SIGURNOSTI I ZAŠTITE

Zanić, Marino

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Marino Zanić

PRIMJENA ELEKTRONIČKIH POTPISA U DOMENI SIGURNOSTI I ZAŠTITE

ZAVRŠNI RAD

Karlovac, 2022.

Karlovac University of Applied Sciences
Safety and Protection Department

Professional graduate study of Safety and Protection

Marino Zanić

APPLICATION OF ELECTRONIC SIGNATURES IN THE DOMAIN OF SECURITY AND PROTECTION

Final paper

Karlovac, 2022

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Marino Zanić

PRIMJENA ELEKTRONIČKIH POTPISA U DOMENI SIGURNOSTI I ZAŠTITE

ZAVRŠNI RAD

Mentor:

dr. sc. Damir Kralj, prof. v. š.

Karlovac, 2022.

PREDGOVOR

Stečenim znanjem kroz studij Sigurnosti i zaštite na Veleučilištu u Karlovcu te korištenjem stručne i znanstvene literature napisao sam ovaj rad. Zahvalu na pomoći pri pisanju ovog završnog rada želim izraziti mentoru dr.sc. Damiru Kralju. Na Veleučilištu sam stekao potrebno znanje za daljnji rad u području sigurnosti i zaštite kao i kompetencije za uspješnu komunikaciju i napredovanje u budućim izazovima koji su ispred mene. Zahvaljujem se svim profesorima Veleučilišta na prenesenom znanju. Također zahvaljujem se obitelji, prijateljima i kolegama koji su uvelike pridonijeli ovom uspjehu.

SAŽETAK

Predviđeni doprinos ovog rada je prikazati svojstva i mogućnosti primjene elektroničkog potpisa. Izvršena je analiza primjene elektroničkog potpisa kako u smislu opće poslovne primjene, tako i u domeni sigurnosti zaštite. U tom smislu je obrađen pojam elektroničkog potpisa, važnost, principi te primjena elektroničkog potpisa. Također su prikazane regulatorne odredbe primjene elektroničkog potpisa kako u Hrvatskoj, tako i u Europskoj Uniji. Eksperimentalni dio rada obrađuje analizu stvarnih primjera iz prakse kroz koje će se objasniti primjena elektroničkog potpisa. Na temelju analize teorijskog dijela te primjene elektroničkog potpisa u praksi, na kraju rada je dano mišljenje i procjena o dinamici korištenja na našem području.

Ključne riječi: elektronički potpis, elektronički dokumenti, certifikati, sigurnost i zaštita

SUMMARY

The intended contribution of this paper is to show the properties and possibilities of application of the electronic signature. An analysis of the application of the electronic signature was performed both in terms of general business application and in the domain of security and protection. In this sense, the concept of electronic signature, its importance, principles and application of electronic signature were discussed. Also presented are the regulatory provisions for the application of electronic signatures both in Croatia and in the European Union. The experimental part of the paper deals with the analysis of real examples from practice, through which the application of the electronic signature will be explained. Based on the analysis of the theoretical part and the application of the electronic signature in practice, at the end of the paper an opinion and assessment on the dynamics of use in our area was given.

Keywords: electronic signature, electronic documents, certificates, security and protection

SADRŽAJ

1. UVOD

U suvremenom svijetu sve češće se spominje pojam digitalni potpis. Većina dokumentacije u današnje vrijeme šalje se putem internetske mreže, posebno kada se radi o porukama, online sastancima, mailovima ili slično. Većina dokumenata koji se šalju “online” moraju biti potpisani. Kako se radi o online platformama za slanje dokumenata, jasno je da postoji šansa od lažiranja potpisa pojedinih dokumenata. Vrlo jednostavan način lažiranja tuđeg potpisa je skeniranje istog bilo sa neke prijašnje dokumentacije, osobne iskaznice ili sličnog dokumenta te ubacivanje skena na mjesto potpisa u dokumentu koji se šalje putem interneta. Da bi se izbjegle mogućnosti neovlaštenih potpisivanja uvodi se digitalni certifikat za potpisivanje koji dokazuje Vaš identitet. Ustanova za izdavanje certifikata slična je javnom bilježniku. Nakon dobivenog certifikata koji potvrđuje naš identitet možemo koristiti digitalni potpis. Kada pošaljemo digitalno potpisani dokument, zajedno sa dokumentom šaljemo i certifikat i javni ključ. Certifikat je obično valjan godinu dana ili duže, nakon čega potpisnik mora obnoviti ili dobiti novi potpisni certifikat da bi uspostavio identitet. U području zaštite na radu digitalni certifikat, odnosno digitalni potpis ima značajnu ulogu. Kada se radi o zapisnicima o osposobljavanju, naručivanju osobne zaštitne opreme, izdavanja uvjerenja o osposobljenosti, izradama liječničkih uputnica i slično, potrebno je od strane više osoba potpisati isti dokument. Iz tog razloga digitalni potpis omogućuje značajno ubrzan proces rješavanja zadataka koji ovise o potpisima više osoba.

Cilj rada je analizirati i pojasniti što su digitalni potpisu i digitalnom certifikat u općem smislu, a kroz u eksperimentalni dio detaljnije opisati stvarne situacije u poslovanju te prezentirati važnost i učinkovitost digitalnog potpisivanja u sustavu sigurnosti i zaštite.

Primijenjene metode istraživanja bile su analiza dostupnih pisanih i mrežnih izvora, kao i primjena vlastitih znanja i iskustava stečenih kroz dosadašnje školovanje.

2. ELEKTRONIČKO POSLOVANJE

2.1. Uvod u predmetno područje

U dinamičnom poslovnom okruženju današnjice, tržišni subjekti teže smanjenju vremena ciklusa razvoja proizvoda, poboljšanju usluga krajnjim korisnicima, te unapređenju kvalitete proizvoda i usluga. Za susret takvim izazovima, mnogi subjekti su razvili koncept bližih odnosa sa svojim potrošačima uz primjenu informatičkih tehnologija. Razvojem novih trendova u distribuciji, pojavljuju se i novi modeli razmjene informacija između subjekata na tržištu. Elektronička razmjena podataka (engl. EDI – *electronic data interchange*) ključna je tehnologija koja se koristi u sustavima za upravljanje lancem opskrbe uključujući logističke funkcije. [1]

2.2. Razmjena elektroničkih dokumenata

Kod elektroničke razmjene poslovnih dokumenata imamo sljedeći uporabni scenarij j (engl. - *use case)*::

- Pošiljatelj kreira i šalje poslovni dokument ili podatke.
- Prilikom transporta može doći do neželjenih događaja koji mogu rezultirati povredom privatnosti odnosno neisporučivanjem podataka.
- Primatelj prima poslovni dokument ili podatke.

Zahtjevi na uspješnost elektroničke razmjene podataka mogu se podijeliti na tri kategorije:

- Zahtjevi na jednostavnost korištenja
- Zahtjevi na sigurnost kod prijenosa
- Zahtjevi na pouzdanost prijenosa [1]

2.3. Jednostavnost korištenja

Faktor jednostavnosti implementacije jedan je od najvažnijih kod odabira načina komunikacije budući da izravno diktira cijenu sustava.

Što je sustav složeniji potrebno je više znanja za njegovu implementaciju. Nakon što je sustav implementiran potrebno je osigurati dodatno znanje u fazi održavanja sustava. Jednostavan sustav za elektroničku komunikaciju je elektronička pošta. Svaki korisnik može slijedeći jednostavne i kratke upute otvoriti svoju adresu elektroničke pošte i koristiti je. Implementacija i korištenje nisu niti vremenski niti financijski zahtjevni.

Složen sustav poput bankarske mreže zahtjeva pažljivo i detaljno planiranje, složenu implementaciju i održavanje. Ne postoje jednostavne upute i potrebno je puno visokostručnih ljudi za upravljanje takvom mrežom. Ljudski resursi namijenjeni za rad s složenim sustavima moraju se posebno obučavati što sustavu podiže cijenu. Specijalni uvjeti kod komunikacije, kao što su sigurnost i pouzdanost, daju okvire koje komunikacija mora zadovoljavati. Unutar tih okvira sustav mora težiti što većoj jednostavnosti da bi mu cijena bila što je moguće manja. [1]

2.4. Sigurnost

Faktor sigurnosti je najznačajnija karakteristika komunikacije između poslovnih partnera. Uvijek postoje sigurnosni rizici, jer poruke mogu biti ukradene, izgubljene ili promijenjene negdje na putu između krajnjih točaka komunikacije. Zbog toga postoji šest zahtjeva koji moraju biti ispunjeni kako bi se ostvarila sigurnost komunikacije:

- Autentičnost (engl. *authenticity*) osigurava da se uvijek zna tko je vlasnik pojedinog dokumenta ili informacije.
- Povjerljivost (engl. *confidentiality*) podataka osigurava da je informacija zaštićena od upada nepozvanih ("trećih") osoba.

- Kontrola pristupa (engl. *access control*) osigurava da je pristup pojedinim aplikacijama i podacima ograničena samo na one koji mogu pribaviti prihvatljiv dokaz o identitetu.
- Integritet (engl. *integrity*) se odnosi na dokaz da poruka nije modificirana (slučajno ili namjerno) u transportu.
- Neporicanje (engl. *non-repudation*) garantira da pošiljatelj poruke ne može poricati slanje poruke.
- Raspoloživost (engl. *availability*) je zahtjev da je pristup aplikacijama i podacima omogućen u što većoj mjeri. Raspoloživost se odnosi i na brzinu pristupa.

Slijedi opis mogućih scenarija koji se odnose na probleme nastale tijekom prijenosa podataka. [1]

2.5. Pouzdanost

Pod pojmom pouzdanost prijenosa podataka podrazumijeva se sigurna isporuka podataka na odredište. To znači da mehanizam za razmjenu podataka sam mora ustanoviti ukoliko je došlo do problema prilikom prijenosa.

Prilikom razmatranja pouzdanosti isporuke podataka treba naglasiti da je taj problem velikim dijelom povezan sa sigurnošću podataka. Ukoliko dođe do pogreške kod prijenosa u bilo kojem dijelu poruke ili poruka nije u cijelosti isporučena možemo taj slučaj smatrati ekvivalentnim slučaju neovlaštene promjene podataka. Jedina razlika je da digitalni potpis nije jedino moguće rješenje.

Kod gubitka cijele poruke ili dijela poruke potrebno je ostvariti mehanizam za otkrivanje i otklanjanje problema pogreške. Postoji velik broj mogućih rješenja od kojih ćemo spomenuti nekoliko najznačajnijih:

- Dodavanje dodatne informacije u poruku radi otkrivanja i ispravljanja manjih pogrešaka – najčešće na razini bitova o čemu se brinu transportni protokoli
- Zahtjev za potvrdom uspješnog prijema – ukoliko ne dođe potvrda nakon određenog vremena pokreće se za taj slučaj predviđena akcija - najčešće retransmisija [1]

U nastavku će biti prikazani proces identifikacije, autentikacije i autorizacije (slika 1.)

Slika 1**.** Proces identifikacije, autentikacije i autorizacije [1]

Identifikacija je postupak prilikom kojeg se od korisnika traži upisivanje imena i prezimena, identifikacijskog broja ili korisničkog imena koje je dobio od banke.

Autentikacija je postupak povezan s identifikacijom, a dokazuje da li je osoba koja se pokušava ulogirati na stranicu zaista ta osoba za koju se predstavlja, za autentifikaciju se koriste tri najčešća načina:

- Nešto što korisnik zna (npr. lozinka, PIN ili slično),
- Nešto što korisnik ima (npr. pametna kartica, stick, TAN tablica i sl.),
- Nešto što korisnik jest (biometrija – otisak prsta, rožnica oka, rukopis i sl.).

Autorizacija je postupak provjere sustava u kojoj se provjerava je li osoba koja se predstavila sustavu ima ovlasti pristupanja samom sustavu (provjera s unaprijed pohranjenim podacima unutar sustava). [1]

3. POJAM ELEKTRONIČKOG POTPISA

Predstavlja generički pojam koji podrazumijeva čitav niz različitih vrsta digitalno prikazanih podataka pomoću kojih se vrši identifikacija korisnika i provjera vjerodostojnosti potpisanog elektroničkog dokumenata. Dodatna vrijednost potpisanog elektroničkog dokumenta postiže se primjenom naprednog elektroničkog potpisa.

Predstavlja generički pojam koji podrazumijeva čitav niz različitih vrsta digitalno prikazanih podataka pomoću kojih se vrši identifikacija korisnika i provjera vjerodostojnosti potpisanog elektroničkog dokumenata. Dodatna vrijednost potpisanog elektroničkog dokumenta postiže se primjenom naprednog elektroničkog potpisa.

Pitanje definicije potpisa osobito je važno u vremenu kada intenzivno prelazimo na komunikaciju putem elektroničkih informacijskih sustava (slika 2.). Broj elektroničkih dokumenata u državnoj upravi, pravosuđu i gospodarstvu u stalnom je porastu. Kako informacijska tehnologija napreduje, tako se šire i mogućnost i njezine upotrebe. Budući da upotreba elektroničkih informacijskih sustava u društvu u cjelini raste, gospodarski subjekti i državna uprava, žele li (p)ostati efikasni, trebaju prihvatiti i upotrebljavati moderne informacijske tehnologije poput elektroničkog potpisa u svakodnevnom radu. [2]

Slika 2. Primjer elektroničnog potpisa [2]

3.1. Povijest elektroničkog potpisa

Kao društveno biće, čovjek je svakodnevno u nekom obliku komunikacije. Još u dalekoj povijesti čovječanstva javila se potreba za komunikacijom. No neke informacije ponekad želimo podijeliti samo sa jednom osobom, a ne sa svima. Tada dolazimo do znanstvene discipline koja se naziva kriptografija, a razvila se zbog potrebe da se omogući komunikacija među dvjema osobama preko nesigurnog komunikacijskog kanala, tako da ih nitko osim njih ne razumije. Riječ kriptografija dolazi od grčkog pridjeva „skriven“ i glagola „pisati“.

Osnovni kriptografski pojmovi su: šifriranje (kodiranje), dešifriranje (dekodiranje) i ključ. *Pošiljatelj* je osoba koja šalje poruku (alias Alice), a *primatelj* osoba koja prima poruku (alias Bob). *Napadač* (alias Eve) je treća osoba koja želi presresti tu poruku. Pošiljatelj najprije transformira (šifrira) poruku pomoću unaprijed dogovorenog ključa i šalje primatelju šifrat (šifrirana poruka). U slučaju da napadač presretne tu poruku i otkrije sadržaj šifrata, za razliku od primatelja on ne može razumjeti sadržaj poruke zbog nepoznavanja ključa. Primatelj prima poruku, dešifrira ju pomoću ključa i čita podatke. Kako bi ovaj algoritam radio potrebno je da primatelj i pošiljatelj imaju isti ključ, koji je nedostupan drugim osobama.

Faks uređaj bio je u velikoj upotrebi među tvrtkama i pojedincima za hitno slanje papirnatih dokumenata u 80-im godinama prošlog stoljeća. Unatoč tome što se kod takvog prijenosa podataka potpis nalazi fizički na papiru, dohvaćanje i prijenos se vrši elektronički. Digitalni potpis podskup je elektroničkog potpisa koji koriste razne kriptografske metode i zbog toga je razvoj digitalnog potpisa usko vezan uz razvoj kriptografije.

Morseova abeceda počela se koristiti 1860. godine kako bi se poruke prenosile telegrafom, a desetak godina nakon presudom suda *New Hampshire Suprime Court* potpisi preneseni na ovaj način su proglašeni pravomoćnima.

Razvoj kriptografije (slika 3) s javnim ključem započinje 1874. godine gdje se opisuju jednosmjerne enkripcijske funkcije u knjizi „*The Principles of Science: A Treatise on Logic and Scientific Method*“ koju potpisuje William Stanley Jevons.

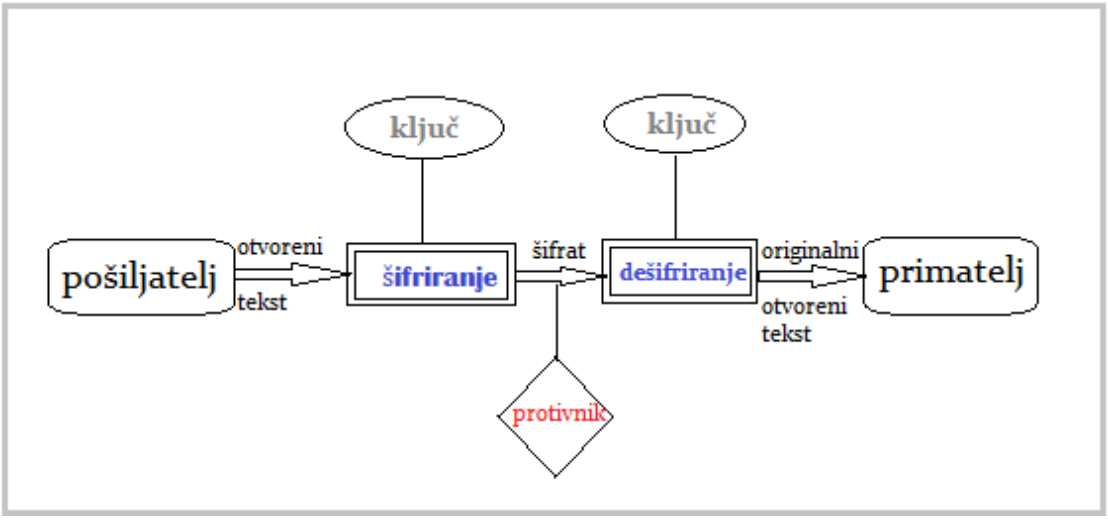
Clifford Cocks, James H Ellis i Malcom Williamson 70-ih godina 20. stoljeća osmišljaju prve algoritme koji se temelje na asimetričnom ključu no ne objavljuju svoje ideje.

Whitfrield Diffie i Martin Hellman 1976. godine objavljuju prvu praktično upotrebljivu metodu razmjene ključeva, kasnije poznata kao *Diffie-Hellman* razmjena ključeva, a predstavlja poseban slučaj RSA algoritma.

Roven Rivest, Adi Shamir i Leonard Adleman su 1977. godine iskoristili ideju Diffiea i Hellmana i izumili prvi kriptosustav s javnim ključem pod nazivom RSA algoritam. Naziv algoritma dolazi od početnih slova prezimena autora, a to je prvi siguran algoritam koji je prikladan za enkripciju podataka i potpisivanje pod pretpostavkom da se koriste dovoljno drugih ključeva.

Neal Koblitz i Victor S. Miller 1985. godine koriste eliptičke krivulje nad konačnim poljima u kriptografskim algoritmima s javnim ključem. Na temelju toga se razvio ECDSA (engl. *Elliptic Curve DSA)* algoritam, varijanta DSA (engl. *Digital Signature Algorithm*) algoritma.

Standardizacija DS algoritama u Sjedinjenim Američkim Državama započinje sredinom 1990-ih godina, a u Europi krajem 1990-ih i početkom 2000-ih godina, na razini Europske Unije i pojedinih zemalja. [3]



Slika 3. Prikaz postupka kriptografije [4]

3.2. Važnost elektroničkog potpisa

Pitanje definicije potpisa osobito je važno u vremenu kada intenzivno prelazimo na komunikaciju putem elektroničkih informacijskih sustava. Broj elektroničkih dokumenata u državnoj upravi, pravosuđu i gospodarstvu u stalnom je porastu. Kako informacijska tehnologija napreduje, tako se šire i mogućnosti njezine upotrebe.

Elektronički potpis kao pravni ekvivalent ručnom potpisu i pečatu sposoban je znatno ubrzati poslovanje, omogućujući neusporedivo više poslovnih transakcija istodobno čuvajući sigurnost i povjerljivost poslovne komunikacije u digitalnom okružju. Budući da upotreba elektroničkih informacijskih sustava u društvu u cjelini raste, gospodarski subjekti i državna uprava, žele li (p)ostati efikasni, trebaju prihvatiti i upotrebljavati moderne informacijske tehnologije poput elektroničkog potpisa u svakodnevnom radu. [5]

U tijelima državne uprave Republike Hrvatske u nedavnoj prošlosti događali su se razni nedorečeni pokušaji “informatizacije” i “internetizacije” bez čvrstog plana i cilja. O

tome svjedoče brojne strategije i drugi okvirni dokumenti koji su iz godine u godinu usvajani bez većeg efekta u smislu konkretnijih promjena u načinu na koji državna uprava funkcionira, po uzoru na slične dokumente iz zapadnih uzora.

Reguliranje elektroničke trgovine i s njom povezanih tehnologija i postupaka ozbiljnije je ušlo u fokus hrvatskog zakonodavca tek početkom novog tisućljeća, desetak godina kasnije nego na Zapadu. U vrijeme kada su doneseni zakoni poput Zakona o elektroničkoj trgovini, Zakona o elektroničkom potpisu i Zakona o elektroničkoj ispravi dolazi do promjene u stajalištu zakonodavca prema utjecaju informacijske tehnologije na društvo i do osvještavanja potrebe da se isti odgovarajuće regulira, a sve (uglavnom) pod utjecajem relevantne zakonodavne prakse u susjednim, teorijski i sustavno bliskim zakonodavstvima u postupku preuzimanja europske pravne stečevine.

Od svih pravnih pitanja i nedoumica koje prate pojavu elektroničke trgovine osobito se ističe ono o regulaciji elektroničkog potpisa. Bez elektroničkog potpisa, već smo istaknuli, nema zadovoljavajuće razine pravne sigurnosti prilikom sklapanja pravnih poslova u elektroničkom obliku. [5]

Elektronički potpis osnovna je tehnologija provjere autentičnosti digitalnog dokumenta. O kvalitetnom pravnom i tehničkom okviru uvođenja elektroničkog potpisa u svakodnevni život ovisi i kvaliteta usluga državne uprave i gospodarstva u dobu elektroničke komunikacije. Bez legalne upotrebe elektroničkog potpisa nema ni prostora za legalizaciju rada elektroničkih agenata, svakako ne u široj poslovnoj primjeni. Prije analize hrvatskog i poredbenog pravnog okvira regulacije institute elektroničkog potpisa treba istaknuti nekoliko zahtjeva koji se stavljaju pred zakonodavca i tijela državne uprave kako bi elektronički potpis zaživio.

Osnovni zahtjev koji se stavlja pred elektronički potpis je pitanje potvrđivanja izvornosti, odnosno autentičnosti potpisnika i sadržaja potpisane komunikacije.

Elektronički potpis baziran na bilo kojoj tehnologiji koja neće jamčiti, u najvećoj mogućoj mjeri, da je elektronički dokument njime potpisan autentičan, sadržajno i u pogledu oznake autora, neće biti prihvaćen u pravnom prometu.

Nadalje, elektronički potpis treba biti jednostavan za upotrebu i za korisnike i za tijela koja jamče njegovu autentičnost. Treće, radi promicanja upotrebe elektroničkog potpisa, ali i radi više razine pravne sigurnosti, osim komercijalnih pružatelja usluge certificiranja nužan je i javni institucionalni okvir, odnosno tijelo državne uprave koje će voditi bazu podataka s registriranim elektroničkim potpisima. Četvrti uvjet kvalitetnog usvajanja elektroničkog potpisa u svakodnevni život je izjednačavanje vrijednosti elektroničkog i vlastoručnog potpisa. Iako će se taj uvjet moći ispuniti tek nakon što prva tri budu zadovoljena, bez ovog koraka elektronički će potpis ostati samo tehnološki kuriozitet ograničen na neke aspekte elektroničke trgovine.

Donošenje Zakona o elektroničkom potpisu i s njime povezanih provedbenih propisa nužan je prvi korak, no nikako i posljednji kad je riječ o regulaciji elektroničkog potpisa i usvajanju njegove upotrebe i od javnih i od privatnih tijela, no ovu konstataciju ne treba shvatiti kao poziv na donošenje nove regulative prije nego što se teorijski i praktično ne ispita doseg i učinak postojeće.

4. ELEKTRONIČKI MEDIJI

Elektronički mediji postaju neizostavni u našem privatnom i poslovnom životu. Podatke preko mreže razmjenjujemo sa osobama koje ne poznajemo i u koje ne možemo imati povjerenja, kao ni u to da nam poslani podaci stižu u nepromijenjenom obliku.

Tehnika elektroničkog potpisa predstavlja rješenje ovih problema jer omogućuje da se sa pravnom sigurnošću utvrdi tko je poslao elektroničku poruku i da li su podaci u toku svog puta mijenjani. U takvim uvjetima postavlja se pitanje kako osigurati vjerodostojnost komunikacije. Jedan od odgovora na ovo pitanje upravo je institut “elektroničkog potpisa”, koji ukoliko se koristi u zakonom određenim uvjetima, zamjenjuje tradicionalni potpis na papiru. [6]

4.1. Sredstva za elektronički potpis

Sredstvo za elektronički potpis čini računalna oprema, program ili njihovi relevantni sastojci koji su namijenjeni za primjenu od strane davatelja usluga certificiranja za davatelja usluga u vezi s elektroničkim potpisom ili su namijenjeni za primjenu kod izrade ili verificiranja elektroničkog potpisa.

Sredstvo za verificiranje potpisa označava odgovarajuću računalnu opremu ili računalni program koji se koristi za primjenu podataka za verificiranje potpisa.

Verifikacija je proces ispitivanja poruke ili integriteta elektroničkog potpisa izvođenjem *hash* funkcije na strani pošiljatelja i primatelja poruke i uspoređivanje rezultata. [6]

4.2. Vremenski žig

Vremenski žig, odnosno digitalni vremenski biljeg metoda je označavanja nastanka elektroničkog dokumenta i bilježenja promjena njegova sadržaja kroz vrijeme, odnosno riječ je o mehanizmu provjere kada je digitalni dokument kreiran, odnosno promijenjen, što je važno za utvrđivanje vjerodostojnosti dokumenta.

Financijska agencija (FINA) je trenutno jedini evidentirani izdavatelj vremenskog žiga u RH. Omogućuje pouzdano dokazivanje da je podatak, elektronički zapis, elektronički dokument i sl. postojao prije trenutka u vremenu koji je naznačen u vremenskom žigu. Svaka naknadna promjena u dokumentu i u ugrađenom vremenskom žigu se lako otkriva.

Vremenski žig osigurava:

- Da je dokument u tom obliku postojao prije vremena navedenog u ugrađenom vremenskom žigu
- Da dokument nije mijenjan nakon vremena navedenog u ugrađenom vremenskom žigu
- Da se verifikacija elektroničkog potpisa dokumenta može pouzdano obaviti i nakon opoziva ili isteka potpisnog certifikata
- Da je dokument poslan ili zaprimljen u vrijeme navedeno u vremenskom žigu [6]

5. NAČIN FUNKCIONIRANJA ELEKTRONIČKOG POTPISA

5.1. Pouzdanost elektroničkog potpisa

Pouzdani popis predstavlja javno objavljen popis nadziranih i dobrovoljno akreditiranih davatelja usluga izdavanja kvalificiranih certifikata te mora pružati osnovne informacije o istima. Pouzdani potpis treba biti objavljen u strojno čitljivom obliku (XML), a može biti objavljen i u običnom textu (txt).

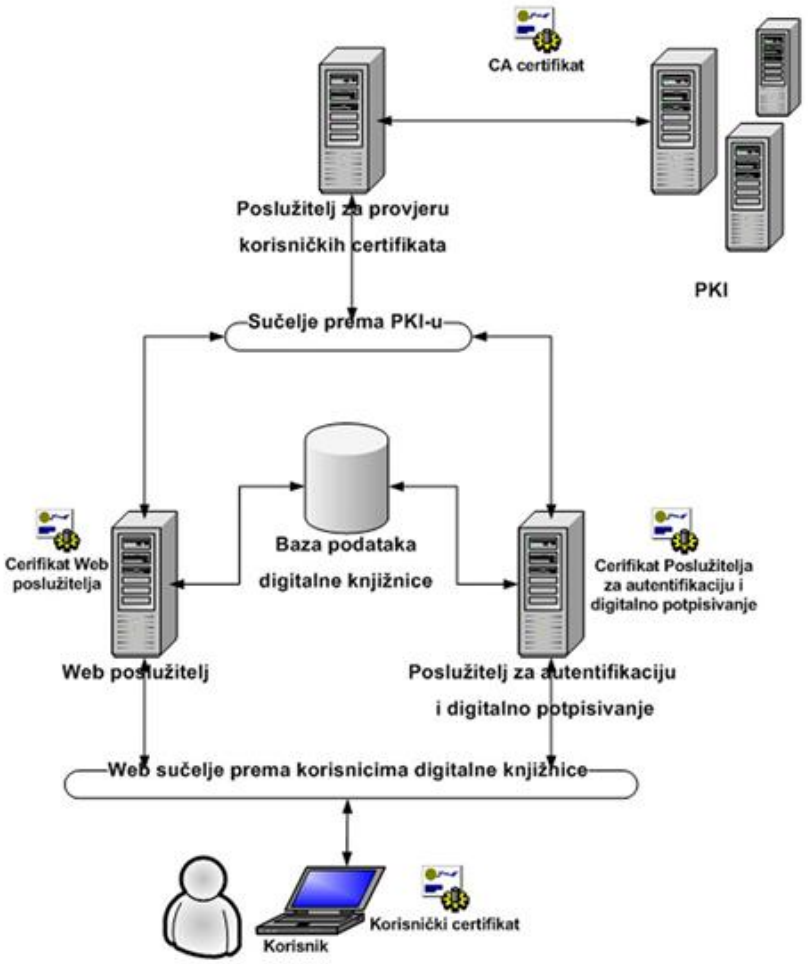
Sigurnost i pouzdanost poslovanja putem interneta jamči najsuvremenija infrastruktura javnog ključa (engl. PKI - public key infrastructure) tehnologija koja se temelji na pametnim karticama s digitalnim certifikatima. Korištenje elektroničkog potpisa postaje iznimno važan, siguran i nezamjenjiv vid komunikacije.

engl. IETF (Internet engineeringt task force) definicija PKI sustava glasi: PKI je skup sklopovlja, programske opreme, ljudi, pravila i funkcija potrebnih za stvaranje, upravljanje, pohranjivanje, distribuiranje i opozivanje certifikata baziranih na kriptografiji javnim ključem (slika 4). NCARH (Nacionalni CA za Republiku Hrvatsku) je nacionalni ovjerovitelj za RH koji omogućuje povezivanje domena povjerenja unutar HR PKI domene. Povezivanje omogućuje cross certificiranje glavnih ovjerovitelja različitih PKI domena unutar HR PKI domene.

Povjerenstvo za HR PKI postavlja, upravlja i objavljuje politike u domeni HR PKI i upravlja radom NCARH-a i repozitorijom. Odgovoran je za certificiranje i akreditaciju unutar cjelokupne HR PKI domene te ima odgovornost za nadzor svih PKI operacija, te je zaduženo za:

- identifikaciju međunarodnih i europskih normi iz područja PKI i njihovu implementaciju u HR PKI,
- uspostavu, odobravanje i održavanje politike certificiranja za NCARH
- odobravanje operativnih postupaka u HR PKI

- uspostavu i odobravanje prikladnih mehanizama kontrola i izvještajnih procedura za HR PKI,
- prihvaćanje zahtjeva od strane davatelja usluga certificiranja koji se žele udružiti u HR PKI te odobravanje, izdavanje povezujućih certifikata za glavnog ovjerovitelja davatelja usluga certificiranja,
- odobravanje, izdavanje povezujućih certifikata za glavnog ovjerovitelja davatelja usluga certificiranja
- poticanje na suradnju s prekograničnim PKI domenama
- donošenje smjernica za rad i daljnji razvoj NCARH-a. [7]



Slika 4. PKI sustav [7]

5.2. Napredni elektronički potpis

Napredni elektronički potpis ima istu snagu kao vlastoručni potpis i otisak pečata na papiru ukoliko je izrađen u skladu sa odredbama Zakona o elektroničkom potpisu, a povezan je isključivo s potpisnikom te ga nedvojbeno identificira. Elektroničkim potpisom osigurava se:

- AUTENTIČNOST – osigurava da je pošiljatelj stvarno onaj koji tvrdi da on jest
- INTEGRITET – jamči cjelovitost i nepromijenjenost poruke

U zakonu, napredni elektronički potpis je:

1. Povezan isključivo s potpisnikom
2. Nedvojbeno identificira potpisnika
3. Nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika
4. Sadrži izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka. [8]

5.3. Tehnologije električnog potpisa

Postoji više načina da čovjek ostavi svoj jedinstveni potpis kojima ga možemo identificirati, a najpoznatiji načini su:

- Skenirani ručni potpis
- Biometrijski potpis (engl. *Biometrics Signature Verification*)
- Digitalni potpis (kriptografija javnog ključa)

Skenirani ručni potpis digitalizirani je ručni potpis u seriju bitova i upisan u datoteku potpisa, potpis se provjerava usporedbom primljenog potpisa sa onim iz datoteke, mijenjanje dokumenta nema utjecaja na izgled potpisa.

Biometrijski potpis koristi dijelove tijela za identifikaciju (DNK, mrežnica oka, obrazi, govor, ruke, otisak prsta), karakteristike dijelova tijela se pohranjuju u datoteku radi identifikacije. Primjenu nalazi kod kreditnih kartica, sigurnosnih bedževa i kod ulaza u kontrolirane prostore. [8]

5.4. Principi oblikovanja elektroničkog potpisa

Provjeru vjerodostojnosti autora ili podataka moguće je provesti korištenjem:

- zaporki – najčešća metoda dokazivanja vjerodostojnosti je pomoću korisničkog imena i uz njega vezane zaporke,
- ispitnog zbroja (eng. *checksum*) - koristi se prvenstveno za provjeru ispravnosti primljenih podataka, ali može poslužiti i za provjeru autentičnosti istih jer neispravan ispitni zbroj ukazuje na neovlaštenu izmjenu podataka,
- CRC provjere (engl. *Cyclic Rendundancy Check*) – konceptualno slično ispitnom zbroju, ali koristi dijeljenje polinoma kako bi se utvrdila ispravnost podataka,
- enkripcije s privatnim ključem,
- enkripcije s javnim ključem i
- digitalnim certifikatima. [9]

Enkripcija s privatnim ključem

Kod enkripcije s privatnim ključem svako računalo ili korisnik posjeduje tajni ključ pomoću kojega se podaci, prije slanja računalnom mrežom, kriptiraju. Primatelj treba znati pošiljateljev tajni ključ kako bi mogao dekriptirati tako primljene podatke. Zbog toga

je prije uspostavljanja komunikacije potrebno znati koja računala (tj. korisnici) će razmjenjivati poruke te na svako računalo instalirati privatne ključeve računala s kojih se očekuju poruke. [9]

Enkripcija s javnim ključem

Prilikom stvaranja digitalnog potpisa koristi se privatni ključ dok se za njegovu provjeru koristi javni ključ koji odgovara, ali nije jednak, privatnom ključu. Svaki korisnik posjeduje vlastiti privatni i javni ključ. Javni ključevi su javno dostupni i svakom korisniku omogućuju provjeru potpisa. Privatni ključevi dostupni su samo svojim vlasnicima čime je onemogućeno krivotvorenje potpisa. Podaci koji se obilježavaju digitalnim potpisom skraćeno se nazivaju porukom. U postupku stvaranja digitalnog potpisa za dobivanje sažete inačice poruke (engl. message digest) koristi se sigurna jednosmjerna funkcija, tzv. SHA (engl. Secure Hash Algorithm) algoritam. To su funkcije koje se matematički vrlo jednostavno izračunavaju, ali im je vrlo teško pronaći inverznu funkciju. Iz tako dobivene sažete inačice poruke DS algoritmom stvara se digitalni potpis. Poruka se, zajedno s pripadnim potpisom, šalje primaocu koji pomoću pošiljateljeva javnog ključa utvrđuje vjerodostojnost poruke i samog digitalnog postupka. U postupku provjere potrebno je koristi SHA algoritam jednak onom korištenom prilikom stvaranja potpisa.

U opisanom postupku potpisuje se sažeta inačica poruke, a ne cijela poruka, iz sljedećih razloga:

- Efikasnost: potpis će biti puno kraći pa će i cjelokupni postupak biti brži jer je u praksi stvaranje sažetka poruke puno brže od stvaranja potpisa.
- Javna dostupnost dokumenta: npr. razne diplome, potvrde, dozvole, ugovori i sl., trebaju biti javno dostupni pa se spremaju i prenose bez enkripcije, a priloženi potpis garantira vjerodostojnost pojedinog dokumenta.
- Integritet: tekst koji se potpisuje treba biti kraći od duljine privatnog ključa. Kako to poruka koju se potpisuje najčešće nije, potrebno ju je, u slučaju potpisivanja

bez sažimanja, razlomiti na dijelove, pojedinačno potpisati svaki dio i poslati. Primatelj tako razlomljene poruke ne bi mogao znati je li koji njezin dio izgubljen ili izbrisan tijekom prijenosa. [9]

5.5. Certifikat

Certifikat je elektronička identifikacija sudionika u mreži , identificira računalo, osobu, pouzeće te pošiljatelj dostavlja svoj svoj elektronički potpis. Pomoću certifikata primatelj identificira pošiljatelja i to na način da dešifrira poruku javnim ključem pošiljatelja i provjeri u bazi certifikata.

Certifikat znači potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe.

Usluga certificiranja označava pravnu ili fizičku osobu koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima. Digitalna omotnica osigurava trajnost ali ne i besprijekornost informacije. Digitalni pečat je digitalno potpisana digitalna omotnica.

Certifikat se koristi za potvrdu identiteta, označava potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa (javni ključ) s nekom osobom i potvrđuje identitet te osobe.

5.6. Digitalni certifikat

Digitalni certifikati koriste se kod zahtjevnijih implementacija enkripcije s javnim ključem, npr. kod web poslužitelja. Radi se o certifikatu kojega izdaje jedno ili više ovlaštenih tijela (engl. Certificate Authority), a koja predstavljaju dio PKI (engl. public key infrastructure) sustava. Spomenuto tijelo djeluje kao posrednik između dva računala ili korisnika, ono potvrđuje njihove identitete i razmjenjuje njihove javne ključeve. Certifikati

koriste digitalne potpise za povezivanje javnih ključeva s podacima o identitetu vlasnika, kao što su ime osobe ili organizacije, adresa i sl., i time sprječavaju neovlašten pristup podacima objavljivanjem lažnog javnog ključa. [10]

5.7. Primjena elektroničkog potpisa

5.7.1. Potpisnik elektroničkog potpisa

Potpisnik elektroničkog potpisa je osoba koja posjeduje sredstvo za izradu elektroničkog potpisa koji potpisuje. Navedena osoba djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja. Navedenim potpisom može se služiti svaka fizička osoba u vlastito ime, kao i osobe koje imaju pravo zastupanja pravnih osoba ili ako imaju pravo nad zastupanjem drugih fizičkih osoba što je regulirano zakonom. [11]

5.7.2. Potpisivanje dokumenata

Prednost korištenja digitalnog potpisa u dokumentima je osiguravanje autentičnosti, integriteta te onemogućuje nepriznavanje dokumenta od strane potpisnika. Digitalni potpis je pravno obvezujući kao i vlastoručni potpis, te obvezuje potpisnika prema uvjetima u potpisanom dokumentu. Za dokumente koji se šalju nesigurnim komunikacijskim kanalom, digitalni potpis daje potvrdu da je dokument poslan upravo onaj za kojega se tvrdi da je pošiljatelj te daje dokaz o izvornosti podataka. Također, digitalni potpis je teže krivotvoriti od vlastoručnog potpisa.

Kada korisnik potpisuje dokument, potpis je kreiran korištenjem korisnikovog privatnog ključa, koji je poznat samo njemu. Sažeta inačica poruke se kriptira korištenjem privatnog ključa, a vjerodostojnost potpisa utvrđuje se javnim ključem.

5.7.3. Potpis u Web aplikacijama

XML potpisi mogu biti primijenjeni na bilo koji digitalni sadržaj, uključujući XML. W3C XML Signature standard međunarodne standardizacijske organizacije World Wide Web Consortium je zadužen za reguliranje XML potpisa. Postoje tri vrste XML potpisa: omotani (engl. enveloped), gdje se potpis nalazi unutar istog dokumenta kao i podaci; omotavajući (engl. enveloping), gdje su podaci ugrađeni u XML potpis, te odvojeni (engl. detached), potpis je odvojen od podataka koji se potpisuju. XML potpis moguće je koristiti za potpisivanje XML elemenata, skupove XML čvorova te njihov sadržaj, vanjske URI oznake, vanjske binarne datoteke te binarne podatke ugrađene u XML dokument. [12]

5.7.4. Multimedijski sadržaji

Autentikacija multimedijskog sadržaja se obično temelji na dvije mogućnosti: digitalni potpis ili vodeni žig (engl. *watermark*). Vodeni žig sadrži informacije kao što su autor, godina nastanka te mogu biti skriveni ili vidljivi korisniku. Vidljivi vodeni žigovi služe za ograničavanje korištenja multimedijskog sadržaja, dok skriveni vodeni žigovi služe za utvrđivanje porijekla.

Postoje dvije vrste autentikacije multimedijskog sadržaja: potpuna autentikacija koja ne dopušta nikakve manipulacije ili transformacije, te autentičnost sadržaja, gdje se dopuštaju modifikacije kao što je sažimanje podataka no bez promjene samog sadržaja.

Za neobrađene i nesažete multimedijske sadržaje pogodnije je koristiti vodeni žig iz sljedećih razloga:

- Žig je izravno vezan za podatke i moguće ga je brzo i jednostavno provjeriti,

- Žig je moguće ugraditi bilo gdje unutar multimedijskog sadržaja bez da narušava kvalitetu (nevidljivi žig).

Standardi za kompresiju kao što su JPEG ili MPEG imaju unaprijed definiran prostor za smještanje digitalnog potpisa. Ako je sadržaj izmijenjen, to je moguće otkriti zbog nepodudaranja hash vrijednosti datoteke i potpisa. Potpis je također moguće spremiti u zaseban dokument koji se onda dobavlja uz multimedijski sadržaj ako je potrebna autentikacija.

Potpisivanje multimedijskih sadržaja je slično potpisivanju ostalih dokumenata, glavna razlika su informacije koje se koriste za stvaranje potpisa. Multimedijski sadržaj se potpisuje tako da se zaštite vizualne i zvučne informacije. [13]

6. SVRHA ELEKTRONIČKOG POTPISA

Elektroničko poslovanje je oblik rada u razmjeni strukturiranih i nestrukturiranih poslovnih dokumenata elektroničkim putem između poslovnih partnera, a uključuje i elektroničku trgovinu.

6.1. Način dobivanja elektroničkog potpisa

Kako bi koristili e-potpis potreban Vam je certifikat koji smo spominjali ranije u tekstu koji u RH izdaje FINA. Kvalificirani certifikati davatelja usluga certificiranja sa sjedištem u EU jednako su valjani kao i kvalificirani certifikati izdani u RH.

1. Ako davatelj usluga certificiranja ispunjava uvjete za izdavanje kvalificiranih certifikata iz Zakona o elektroničkom potpisu te je dobrovoljno akreditiran u RH ili jednoj od zemalja članica EU
2. Ako neki domaći davatelj usluga certificiranja koji ispunjava uvjete za izdavanje kvalificiranih certifikata iz Zakona o elektroničkom potpisu jamči za takve certifikate jednako kao da su njegovi
3. Ako tako odredi bilateralni ili multilateralni sporazum između RH i drugih zemalja ili međunarodnih organizacija
4. Ako tako odredi bilateralni ili multilateralni sporazum između EU i trećih zemalja ili međunarodnih organizacija

Po općim odredbama Zakona o osobnoj iskaznici NN 11/2002, 62/15, navedena iskaznica je isprava kojom hrvatski državljanin dokazuje identitet, državljanstvo, spol, datum rođenja i prebivalište u RH.

Prema Zakonu o osobnoj iskaznici navedeno je da svaka iskaznica sadržava električni nosač podataka koji može pohraniti jedan ili dva certifikata. Identifikacijski certifikat je kvalificirani certifikat koji se koristi za elektroničku identifikaciju i autentifikaciju radi pristupa elektroničkim uslugama. [11]

6.2. Nadzor elektroničkog potpisa

Davateljima usluga certificiranja nije potrebna dozvola za obavljanje usluga certificiranja, ali su Ministarstvu gospodarstva dužni prijaviti početak obavljanja usluga certificiranja, najmanje 8 dana prije početka rada. Uz prijavu i ili u slučajevima promjena u obavljanju usluge, davatelj usluga certificiranja prilaže svoje interne akte o načinu i postupcima pružanja usluga certificiranja te o tehničkoj infrastrukturi.

Prilikom provođenja nadzora, utvrđuje se jesu li ispunjeni svi uvjeti propisani Zakonom o elektroničkom potpisu i pripadajućim pod zakonskim propisima. Nadzire se pravilnost primjene propisanih postupaka i organizacijsko tehničkih mjera te primjena internih pravila u skladu sa Zakonom o elektroničkom potpisu. [10]

6.3. Dokazivanje sadržaja elektroničkog potpisa

Dođe li pri ispunjenju ugovora do problema ili sporova, svatko mora, tko se na neki ugovor poziva, ili ga želi pobijati, dokazati sadržaj ugovora, odnosno dokazati razloge pobijanja.

Stoga se postavlja pitanje, na koji način u okviru sudskog postupka mogu biti dokazani ugovori koji se temelje na elektroničkom očitovanju volje.

Polazna točka za pitanje dokazne vrijednosti elektroničkog očitovanja volje je stanje stalne mogućnosti mijenjanja web stranica. Zbog toga ona u elektroničkom obliku – bez osiguranja elektroničkim potpisom – ne može služiti kao dokazno sredstvo pred sudom, odnosno ugovor sklopljen putem interneta ne može pred sudom biti dokazan. Zato je potrebno primijeniti druga pravilnija dokazna sredstva za očitovanja volje putem interneta.

Ispisom ili pohranjivanjem na računalo prikazano je stanje samo u određenom trenutku, što također predstavlja manjkav dokaz. Protokol o poslanim i primljenim e-

mailovima je također nedostatan, jer su tehničke manipulacije relativno lako provedive. Zbog toga izjave preko e-maila za sada imaju samo ograničenu dokaznu snagu, one podliježu slobodnoj ocjeni dokaza, što znači da sudac prema osobnom nahođenju odlučuje o njihovoj dokaznoj vrijednosti.

U praksi se iz tog razloga događa da mnogi ponuditelji potvrđuju svoje internetske narudžbe uobičajenim putem. Takva primjena uobičajene pošte kao rješenje ove dokazne problematike u proturječju je sa ulogom elektroničkog poslovanja, no ne mora biti zapreka daljnjem razvitku elektroničkog poslovanja kroz nove tehnologije. [6]

7. POJAM KRIPTOGRAFIJE

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda slanja poruka u takvom obliku da ih može pročitati samo onaj kome su namijenjene. Riječ kriptografije dolazi iz grčkog podrijetla i znači tajnopis. Za razliku od dešifriranja, dekriptiranje je disciplina koja se bavi proučavanjem postupaka čitanja skrivenih poruka bez poznavanja ključa. Kriptologija je znanost koja obuhvaća kriptografiju i kriptoanalizu. [14]

7.1. Elektronički potpis

Elektronički potpis je kombinacija dvije kriptografske metode – *hash* funkcije koja se koristi za utvrđivanje integriteta poruke i asimetričnog algoritma enkripcije kojom se najprije izračunava *hash* vrijednost poruke, a zatim se ta vrijednost šifrira ključem potpisnika.

Zajedno sa certifikatom autentičnosti koji je izdan od kvalificiranog agenta koristi se za utvrđivanje vjerodostojnosti potpisa. Neophodno je da primatelj javnim ključem potpisnika dešifrira *hash* i usporedi ga sa primljenom porukom. Ukoliko je bilo koji element potpisa ili poruke ne odgovarajući, doći će do otkrivanja problema. [6]

7.2. Izrada elektroničkog potpisa

Elektronički potpis izrađuje se na osnovu tajnog ključa pošiljatelja i samog sadržaja, te se ugrađuje u sam sadržaj ili se šalje kao zasebna informacija uz pripadajući sadržaj. Da bi primatelj sadržaja mogao provjeriti elektronički zapis, uz sadržaj i signaturu potrebna mu je i informacija javnog ključa pošiljatelja koju obično pribavi iz drugog nezavisnog izvora, a ne iz same poruke. Kada bi pribavili informaciju javnog ključa iz

elektroničkog potpisa, sama autentičnost izvornosti javnog ključa imala bi smisla samo ako bismo informaciju javnog ključa mogli provjeriti na neki drugi način. [14]

7.3. Protokol šifrirane i potpisane poruke

1. Sudionik A odabire simetrični ključ K (npr. uz pomoć generatora slučajnih brojeva) i pomoću njega šifrira DES postupkom jasni tekst informacije koji želi poslati sudioniku B, a time je određen sadržaj digitalne omotnice
2. Iz izvornog sadržaja informacije sudionik A izračunava sažetak S
3. Sudionik A svojim tajnim ključem K (koji zna samo on) šifrira odabrani simetrični ključ K i sažetak S te šifrirani tekst E (K, S, K) kao zapečaćenu omotnicu pridodaje sadržaju omotnice
4. Po primitku zapečaćene omotnice, sudionik B otvara omotnicu tako da javnim ključem KEA doznaje simetrični ključ K i sažetak S
5. Sudionik B dobivenim simetričnim ključem K dešifrira sadržaj omotnice i tako dolazi do informacije koja mu je poslana
6. Iz dešifriranog sadržaja informacije sudionik B izračunava sažetak i uspoređuje ga s dešifriranim primljenim sažetkom S i ako su te dvije vrijednosti jednake, smatra primljenu informaciju vjerodostojnom, a pošiljatelja poruke autentičnim. [14]

8. REGULATORNE ODREDBE KORIŠTENJA ELEKTRONIČKOG POTPISA

8.1. Zakoni u hrvatskoj

Zakon o elektroničkom potpisu donesen je 24. siječnja 2002. godine. Prema Članku 1., ovim se Zakonom uređuje pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama, te prava, obveze i odgovornosti fizičkih i pravnih osoba u svezi s davanjem usluga certificiranja elektroničkog potpisa, ako posebnim zakonom nije drukčije određeno.[19]

Prema Članku 3., Elektronički potpis u smislu ovoga Zakona je skup podataka u elektroničkom obliku koji služe za identifikaciju potpisnika i potvrdu vjerodostojnosti potpisanoga elektroničkog zapisa. [15]

Unutar Zakona definiraju se certifikat, kvalificirani certifikat te davatelji usluga certificiranja. Certifikat je, u smislu ovoga Zakona, svaka elektronička potvrda kojom se potvrđuje identitet potpisnika u postupcima razmjene elektroničkih zapisa. Prema Članku 10., da bi certifikat mogao biti kvalificirani, mora sadržavati kriterije navedene u Zakonu, a koji su istovjetni onima navedenima u Direktivi 1999/000/EC. Za izdavanje certifikata nadležno je Ministarstvo gospodarstva te za davatelje usluga certifikata ne postoji posebna dozvola. Početak obavljanja djelatnosti izdavanja certifikata obrazloženo u je člancima 15 i 16. [15]

Članak 15: Davatelj usluge certificiranja mora prijaviti Ministarstvu početak obavljanja usluga certificiranja najmanje osam dana prije početka rada. Uz prijavu iz stavka 1. ovoga članka ili u slučajevima promjena u obavljanju usluge, davatelj usluge certificiranja mora dostaviti Ministarstvu dokumentaciju o internim pravilima poslovanja u svezi s izradom i ovjerom elektroničkih potpisa te o unutarnjoj organizaciji, kao i dokumentaciju kojom dokazuje ispunjavanje uvjeta iz članka 12. ovoga Zakona. [15]

Članak 16: Ministarstvo upisuje davatelje usluga certificiranja u Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj (u daljnjem tekstu: evidencija), odmah nakon što davatelj usluge certificiranja podnese prijavu kojom obavještava Ministarstvo o početku obavljanja usluga. [15]

Upis u evidenciju ne podliježe vođenju upravnog postupka. Ministar gospodarstva propisat će pravilnikom sadržaj evidencije, način vođenja evidencije, kao i obrasce prijave za upis u evidenciju te prijave za upis promjena. Ministarstvo Gospodarstva održava evidenciju o davateljima usluga certificiranja te Registar davatelja usluga izdavanja kvalificiranih certifikata u Republici Hrvatskoj u koji se upisuju davatelji usluga izdavanja kvalificiranih certifikata. Evidencije su javne te se vode u elektroničkom obliku. Davatelj usluga certificiranja dužan je prekinuti uslugu certificiranja potpisnicima koji su to tražili, za koje je utvrđena netočnost podataka, koji su umrli ili izgubili poslovnu sposobnost te obavijestiti Ministarstvo gospodarstva o svakom opozivu. Davatelj usluga certificiranja dužan je osigurati sve tehničke i organizacijske mjere zaštite certifikata i podataka te upoznati potpisnika sa svim tehničkim zahtjevima potrebnim za usluge certificiranja.

Zakon o elektroničkom potpisu prestao je važiti danom stupanja na snagu Zakona 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.

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 na snazi je od 08.07.2017. godine te se njime utvrđuju nadležna tijela i zadaće nadležnih tijeka za provedbu Uredbe, utvrđuju tijela za inspekcijski nadzor nad provedbom Uredbe, određuje tijelo nadležno za akreditaciju tijela za ocjenu sukladnosti, utvrđuju prava, obveze i odgovornosti potpisnika i pružatelja usluga povjerenje te određuju prekršajne odredbe za postupanje protivno Uredbi. Nadležno tijelo za provedbu Uredbe je središnje tijelo državne uprave nadležno za poslove e-Hrvatske. Tijelo nadležno za akreditaciju

tijela za ocjenjivanje sukladnosti kvalificiranih pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža je nacionalno akreditacijsko tijelo.

Inspekcijski nadzor nad provedbom Uredbe provode državni službenici središnjeg tijela državne uprave nadležnog za poslove e-Hrvatske ovlašteni za provedbu nadzora. Prava, obveze i odgovornosti potpisnika te pružatelja usluga povjerenja se usklađuju s onima navedenim u Uredbi.

Novčane kazne određuju se za fizičke osobe i pravne osobe. Prema članku 18, (1) Novčanom kaznom od 2000,00 do 10.000,00 kuna kaznit će se za prekršaj fizička osoba koja neovlašteno pristupi i uporabi podatke i sredstva za izradu elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata. Novčanom kaznom od 2000,00 do 10.000,00 kuna kaznit će se za prekršaj potpisnik, odnosno fizička osoba ili odgovorna osoba pravne osobe koja zastupa potpisnika, a koja:

1. ne koristi sredstva i podatke za izradu elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata s pažnjom dobrog domaćina (članak 9. ovoga Zakona)
2. davatelju usluga certificiranja u roku od sedam dana od nastalih promjena ne dostavi potrebne podatke i informacije o promjenama koje utječu ili mogu utjecati na točnost elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata (članak 10. ovoga Zakona)
3. davatelju usluga certificiranja pravodobno ne dostavi zahtjev za opoziv certifikata, odnosno ako odmah po saznanju ne zatraži opoziv svog certifikata u slučajevima gubitka ili oštećenja sredstava/podataka za izradu svog elektroničkog potpisa (članak 10. ovoga Zakona).

Prema Članku 19, novčanom kaznom od 5000,00 do 100.000,00 kuna kaznit će se za prekršaj kvalificirani pružatelj usluga povjerenja koji:

1. ne utvrdi pravovaljano identitet fizičke ili pravne osobe za koju izdaje kvalificirani certifikat,
2. ne obavijesti nadzorno tijelo o svim promjenama u vezi s pružanjem svojih kvalificiranih usluga povjerenja te o namjeri prestanka obavljanja te djelatnosti najmanje 3 (tri) mjeseca prije isteka ugovorom povjerenih mu usluga povjerenja,
3. ne zapošljava osoblje i/ili podizvođače koji posjeduju potrebna stručna znanja, pouzdanost, iskustvo i kvalifikacije i koji su prošli odgovarajuće osposobljavanje u vezi sa sigurnošću i propisima o zaštiti osobnih podataka te ne primjenjuju upravne i upravljačke postupke u skladu s europskim ili međunarodnim normama,
4. ne raspolaže dostatnim financijskim sredstvima i/ili nije sklopio odgovarajuće osiguranje od odgovornosti za štetu,
5. ne obavijesti prije stupanja u ugovorni odnos, na jasan i sveobuhvatan način, svaku osobu koja želi koristiti kvalificiranu uslugu povjerenja o točnim uvjetima korištenja tom uslugom, uključujući bilo kakva ograničenja korištenja,
6. ne koristi vjerodostojne sustave i proizvode koji su zaštićeni od preinaka te osiguravaju tehničku sigurnost i pouzdanost postupaka koje ti sustavi i proizvodi podržavaju,
7. ne koristi vjerodostojne sustave za pohranu podataka koji su mu dostavljeni, u obliku koji se može provjeriti,
8. ne poduzima odgovarajuće mjere protiv krivotvorenja i krađe podataka,
9. ne bilježi i ne čini dostupnim tijekom odgovarajućeg razdoblja, uključujući razdoblje nakon prestanka obavljanja djelatnosti kvalificiranog pružatelja usluga povjerenja, sve bitne informacije u vezi s podacima koje izdaje i prima kvalificirani pružatelj usluga povjerenja, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge,
10. nema uspostavljen i ažuriran plan prekida pružanja usluge radi osiguravanja njezina kontinuiteta u skladu s odredbama koje je potvrdilo nadzorno tijelo,
11. ne osigurava zakonitu obradu osobnih podataka,
12. ne uspostavi i ne ažurira bazu podataka certifikata, kada se radi o kvalificiranim pružateljima usluga povjerenja koji izdaju kvalificirane certifikate. [15]

8.2. Zakoni u EU

Pravila EU o elektroničkim potpisima, pečatima, vremenskim žigovima, uslugama elektroničke dostave i autentifikaciji na internetskim stranicama te o elektroničkim dokumentima utvrđena u Uredbi o eIDAS-u (Uredba o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu) izravno će se primjenjivati u svim državama članicama. To znači da će se, primjerice, elektronički potpis diljem EU-a priznavati jednako kao i onaj napisan rukom i da će biti jednako pravno valjan.

E potpisi u EU-u

Utvrđuje se pravni okvir na europskoj razini za elektroničke potpise (e-Potpisi) te se priznaju davatelji usluga certificiranja. Njihov cilj je podijeljen u dvije stavke, a to su:

1. Pojednostavniti uporabu e-Potpisa
2. Pomoći im da postanu pravno priznati u svim zemljama EU-a

S ciljem osiguravanja ispravnog funkcioniranja unutarnjeg tržišta, istodobno težeći primjerenoj razini sigurnosti sredstava elektroničke identifikacije i usluga povjerenja, ovom se Uredbom:

- utvrđuju uvjeti pod kojima države članice priznaju sredstva elektroničke identifikacije fizičkih i pravnih osoba koja su obuhvaćena prijavljenim sustavom elektroničke identifikacije druge države članice;
- utvrđuju pravila za usluge povjerenja, posebno za elektroničke transakcije; i
- uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate, elektroničke vremenske žigove, elektroničke dokumente, usluge elektroničke preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica.

Uredba EU o Elektroničkom potpisu 910/2014 se primjenjuje na sustave elektroničke identifikacije koje je prijavila država članica, kao i na pružatelje usluga povjerenja koji imaju poslovni nastan u Uniji. Ova se Uredba ne primjenjuje na pružanje usluga povjerenja koje se isključivo koriste unutar zatvorenih sustava koji proizlaze iz

nacionalnog prava ili iz sporazumâ među utvrđenom skupinom sudionika i ne utječe na nacionalno pravo ili pravo Unije koje se odnosi na sklapanje i valjanost ugovorâ ili drugih pravnih ili postupovnih obveza u pogledu forme. Navedenom direktivom definiraju se nove ideje:

1. elektronički potpis nam označuje podatke u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje;
2. Napredan elektronički potpis mora ispunjavati sljedeće zahtjeve:
    - na nedvojben način je povezan s potpisnikom;
    - omogućava identificiranje potpisnika;
    - izrađen je korištenjem podacima za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom;
    - povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.
3. kvalificirani certifikat koji posebice mora obuhvaćati
    - naznaku da se izdaje kao kvalificirani certifikat
    - identifikaciju davatelja usluga certificiranja
    - ime potpisnika
    - mogućnost uvođenja specifičnog dodatnog elementa ovjere, poput datuma rođenja, potpisnika (ovisno o svrsi za koju je certifikat namijenjen)
    - podatke o verifikaciji potpisa: moraju odgovarati podacima o izradi potpisa koji su pod kontrolom potpisnika
    - datume početka i kraja razdoblja valjanosti certifikata
    - identifikacijsku oznaku certifikata
    - napredni elektronički potpis davatelja usluga certificiranja koji izdaje taj certifikat. [16]

Certifikat mora izdati davatelj usluga certificiranja koji zadovoljava specifične zahtjeve utvrđene u Uredbi.

Kvalificirani certifikati za elektroničke potpise mogu uključivati dodatna posebna obilježja koja nisu obvezna. Ta obilježja ne utječu na interoperabilnost i priznavanje kvalificiranih elektroničkih potpisa. No ako je kvalificirani certifikat za elektroničke potpise opozvan nakon početne aktivacije, on gubi valjanost od trenutka opoziva i njegov se status ni u kojem slučaju ne može vratiti u prijašnje stanje. [16]

Pristup tržištu EU

Zemlje EU-a ne smiju isporučivati usluge certificiranja koje podliježu dobivanju prethodnog odobrenja bilo koje vrste. Zemlje EU-a mogu imati vlastite sheme poticanja certifikacije poboljšanih značajki. Ne mogu ograničavati broj ovlaštenih davatelja usluga certificiranja. Također ne mogu ograničavati opskrbu uslugama certificiranja iz druge zemlje EU-a. Zemlje EU-a mogu učiniti uporabu elektroničkih potpisa u javnome sektoru podložnom potencijalnim dodatnim zahtjevima. Ti zahtjevi moraju biti objektivni, transparentni, razmjerni i ne diskriminirajući. [16]

Pravni učinci u EU

Napredni e-Potpis koji se zasniva na kvalificiranom certifikatu udovoljava pravnim zahtjevima potpisa u odnosu na podatke u elektroničkom obliku na isti način na koji vlastoručni potpis udovoljava tim zahtjevima u odnosu na podatke u pisanom obliku.

E-potpis ne može se pravno odbiti kao dokaz u sudskim postupcima isključivo na temelju toga što je:

- u elektroničkom obliku
- nije izrađen uporabom sigurnog sredstva za izradu potpisa. [16]

Zemlje članice EU

Zemlje članice moraju osigurati da davatelj usluga certificiranja koji izdaje kvalificirani certifikat preuzme određene obveze. One uključuju odgovornost za štetu prouzročenu bilo kojoj osobi ili subjektu, koji se u razumnoj mjeri oslanjaju o tom certifikatu:

- u vezi s točnošću svih podataka sadržanih u kvalificiranom certifikatu u vrijeme izdavanja
- u vezi s činjenicom da certifikat sadržava sve detalje propisane za kvalificirani certifikat u vrijeme izdavanja te da je potpisnik identificiran u certifikatu osoba kojoj je on izdan

Davatelj usluga certificiranja može naznačiti granicu vrijednosti transakcija za koje se certifikat može koristiti. Ta granica mora biti vidljiva trećim stranama. Davatelj ne smije biti odgovoran za štetu prouzrokovanu uporabom kvalificiranog certifikata koji prekoračuje utvrđena ograničenja.

Zemlje EU-a moraju osigurati uzajamno pravno priznavanje kvalificiranih certifikata i ePotpisa iz zemalja koje nisu članice EU-a. Moraju biti ispunjeni određeni uvjeti o pouzdanosti kao što su:

- davatelji koji nisu iz EU-a moraju ispunjavati uvjete utvrđene ove Uredbe te biti ovlašteni prema programu dragovoljnog ovlašćivanja utvrđenog u zemlji EU-a; ili
- davatelj iz EU-a koji ispunjava uvjete utvrđene ovom Uredbom može jamčiti za certifikate davatelja koji nisu iz EU-a u jednakoj mjeri kao i za vlastite certificate

Europska komisija može donijeti prijedloge kako bi se osigurala potpuna provedba međunarodnih standarda i sporazuma. [16]

Zaštita podataka EU

Zemlje EU-a moraju osigurati da davatelji usluga certificiranja i nacionalna tijela odgovorna za ovlašćivanje ili nadzor udovoljavaju Direktivi 95/46/EZ o zaštiti osobnih podataka. Donesena nova Uredba o elektroničkoj identifikaciji i uslugama povjerenja (eIDAS) Uredba eIDAS (Uredba (EU) br. 910/2014) donesena je 2014. godine. Na snagu je stupila 17.9.2014., a primjenjivat će se od 1.7.2016., osim određenih članaka navedenih u članku 52. te Uredbe. Uredba (EU) br. 910/2014 od 30.6.2016. stavlja izvan snage Direktivu 1999/93/EZ. [16]

8.3. EU potpis u Hrvatskoj u usporedbi sa EU

U Hrvatskoj se trenutačno na dva kolosijeka traže rješenja za problem dodatne birokratizacije računa, gdje se od početka godine prisiljava tvrtke da printaju, ručno potpisuju i pečate račune koje su primili e-mailom te ih se traži da izmisle novo radno mjesto “likvidatora računa” i time plate dodatan, birokratski trošak.

Elektroničkom pečatu se kao dokazu u sudskim postupcima ne smije uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalificirani elektronički pečat.

Sustav elektroničkog potpisa je zaživio u gospodarstvu u Agrokoru i Ini. E-račune za Agrokor obrađuje mStart. Njihova razmjena definirana je ugovorom i točno definiranim formatom e-računa, a pohranjuju se na specijalne poslužitelje s obzirom na to da se računi moraju arhivirati određeni broj godina. U Hrvatskoj, za razliku od Slovenije, nije posebno propisano da se takve arhive moraju certificirati, već svatko radi svoje rješenje. Time se rješava pitanje arhive računa, ali ne i ostalih dokumenata. Ne postoji razlog zašto bi tvrtka koja ima ERP koristila papir. [16]

9. EKSPERIMENTALNI DIO

9.1. Elektronički certifikat i elektroničke isprave

Upotreba informacijske tehnologije u različitim životnim aspektima za sobom povlači brojne socijalne, pravne i ekonomske posljedice. Utjecaj informacijske tehnologije na društvene odnose je u porastu te se razvija jednakom brzinom kao i sama tehnologija.

Kao primjer može poslužiti električna trgovina. Pojam električna trgovina odnosi se na kupnju ili prodaju usluga putem informacijskih sustava i posredstvom elektroničke komunikacije. Razvoj trgovine putem interneta ubrzao je i razvoj široko prihvaćenih tehnologija poput internetskog marketinga te automatske pohrane i analize podataka. Elektronički potpis ključan je element uspjeha elektroničke trgovine te je uvjet bez kojeg elektronička komunikacija, a time i elektronička trgovina, ostaje pravno nepouzdana i nesigurna. Elektroničkim potpisom možemo autorizirati poruke elektroničke pošte, elektroničke isprave i druge dokumente (npr. ugovor) u elektroničkom obliku.

Čin stavljanja potpisa, osobnog pečata ili kakvog drugog osobnog traga na rukom ili strojem ispisani dokument bilo koje vrste stoljećima se smatra temeljnim uvjetom nastanka presumpcije slaganja potpisnika sa sadržajem isprave. Bez valjana potpisa kojim stranka ugovora ili podnositelj nekog zahtjeva ili bilo koji drugi sudionik pravnog prometa izravno prihvaća sadržaj isprave koju potpisuje, sama isprava koliko god pažljivo i detaljno sročena nema pravnu snagu jer se u pravilu ne može smatrati valjanim očitovanjem volje.

9.2. Pribavljanje digitalnog certifikata radi stvaranja digitalnog potpisa

Često u praksi dolazi do zabune da su digitalni odnosno elektronički potpis istoznačnice, iako se ta dva pojma bitno razlikuju. Digitalni potpis (engl. digital signature) ustvari je digitalna inačica vlastoručnog potpisa, ali to ipak nije skenirani ili fotografiran vlastoručni potpis. Svrha je digitalnog potpisa zaštititi korisnika, kad neko nakani nezakonito iskoristiti njegov identitet pri potpisivanju elektroničkih dokumenata. Njegova je prednost u uštedi vremena i novca u postupcima što zahtijevaju uporabu vlastoručnog potpisa, jer se sve radi putem interneta, a ne u papirnom obliku, uz uporabu obilja papirne konfekcije itd. Digitalni potpis osigurava autentičnost kojom se potvrđuje identitet potpisnika, integritet kojim se potvrđuje da nije došlo do izmjena sadržaja nakon što je upotrijebljen digitalni potpis, neporecivost gdje se pošiljatelju onemogućuje da porekne slanje određene poruke kakvu je potpisao osobnim, tajnim ključem te nekrivotvorljivost kada se za potpis rabi tajni ključ poznat samo osobi potpisniku dokumenta. Da bi se u praksi izbjeglo ne zakonitu višestruku uporabu istoga potpisanog dokumenta, navodi se uz potpis vrijeme i datum, odnosno vremenski žig (engl. *timestamp*). Ovaj način zaštite potpisa od nezakonite višestruke uporabe potpisanoga dokumenta, u Poreznoj upravi primjenjuje se pri potpisivanju elektroničkih ovršnih akata u sustavu eOvrha. Na svaki se elektronički potpis dodjeljuje elektronički potpisanu potvrdu sadržaja tih podataka u određenom vremenu.

S obzirom da je digitalni potpis dio elektroničkog potpisa, elektroničkim potpisom smatra se slijed digitalno prikazanih podataka što omogućuju identifikaciju potpisnika i provjeru vjerodostojnosti potpisana elektroničkog sadržaja. To je način izvedbe za sve metode kojima se može potpisati neki elektronički sadržaj, pa može biti skeniran vlastoručni potpis, digitalni potpis kojeg čini slijed znakova u digitalnom obliku te biometrijski potpis - otisak prstiju, mrežnica oka, prepoznavanje glasa... U praksi mora biti jedinstven za osobu koja ga uporabljuje i biti isključivo pod kontrolom te osobe, mora omogućiti provjeru identiteta korisnika te osigurati vezu potpisa popisane isprave, odnosno sadržaja.

Identifikaciju potpisnika što je omogućuje elektronički potpis rješava se certifikatima. Digitalni certifikat skup je podataka u elektroničkom obliku u funkciji - digitalne osobne iskaznice u procesu elektroničkoga poslovanja u različitima elektroničkim interakcijama te sigurne i povjerljive internetske komunikacije. Služi kao sredstvo dokazivanja identiteta i stoga sadrži ime vlasnika certifikata, vlasnikov javni ključ, datum valjanost certifikata, ime CA izdavatelja, serijski broj i ostale podatke za identifikaciju.

9.3. Primjeri primjene elektroničkog potpisa u praksi

Elektronički potpis ima široku primjenu u elektroničkoj razmjeni podataka. Neki od primjera su: korištenje e-potpisa za potpisivanja poruka elektroničke pošte, potpisivanje dokumenata u pdf formatu.

Za digitalno potpisivanje dokumenata potrebno je imati digitalne certifikate i aplikativno rješenje koje omogućuje uspješan proces potpisa.

Digitalni certifikati

Fina je u Republici Hrvatskoj jedina institucija koja je registrirana u Ministarstvu gospodarstva kao davatelj usluga certificiranja tj. kao izdavatelj kvalificiranih digitalnih certifikata.

FINA izdaje sljedeće vrste digitalnih certifikata:

- FINA RDC što se dijeli na poslovne osobne digitalne certifikate. Poslovne se rabi za osobe u poslovnih subjekata kao autentifikacijske popisne certifikate te za IT-opremu kao certifikat za servere, aplikacije i za potpis koda (u Poreznoj upravi za sustav OLB, eOvrha, ePorezna, PBZO, proces fiskalizacije). Osobne digitalne

certifikate rabe građani kao autentifikacijske odnosno potpisne certifikate (eRegos, ePorezna, eMirovinsko...).

- FINA RDC-TDU certifikate što ih se primjenjuje za zaposlenike TDU kao autentifikacijske odnosno potpisne certifikate (npr. sustav ePorezna)
- FINA DEMO certifikate što ih se primjenjuje za provjeru različitih tehnoloških rješenja prije negoli ih se pusti u proizvodnju, odnosno u komercijalnu uporabu.

Digitalni certifikati izdaju se na multifunkcionalnoj pametnoj kartici ili USB tokenu.

FINA je za svaku kategoriju korisnika digitalnih cenifikata vrste certifikata propisala postupak izdavanja. Poslovni subjekt digitalni certifikat može zahtijevati postupkom registracije. Pri registraciji poslovnog subjekta identificira se osoba ovlaštena za zastupanje poslovnog subjekta i to se obavlja jednokratno. Fizička osoba poslovnog subjekta podnosi »Zahtjev za izdavanje poslovnog certifikata i potpisuje Ugovor o obavljanju usluga certificiranja Potpisane pečatirane obrasce dostavlja se u poslovnicu FINA-e gdje se pokreće postupak izdavanja. Pri preuzimanju certifikata fizička osoba poslovnog subjekta identificira se kao zahtjevatelj certifikata. Fizička osoba (građanin) podnosi obrasce Zahtjev za izdavanje osobnog certifikata i Ugovor o obavljanju usluga certificiranja te ih vlastoračne potpisuje poput ostalih podnositelja zahrieva, i pri preuzimanju certifikata identificira se kao zahtjevatelj.

Pri izdavanju poslovnih certifikata za aplikacije poslužitelje takoder se mora proći procedura izdavanja. Ovlaštena osoba za zastupanje podnosi Zahtjev za izdavanje certifikata za poslužitelje, uređaje ili aplikacije te potpisuje Ugovor o obavljanju usluga certificiranja. U zahtjevu se navodi podatke o skrbniku certifikata te ga potpisuju ovlaštena osoba za zastupanje i skrbnik. Pri preuzimanju certifikata identificiraju se i skrbnik i ovlaštena osoba.

Digitalne certifikate za TDU primjenjuje se radi dobivanja I davanja informacija, pristupa različitim servisima u nadležnosti TDU-a te enkripciju dekripciju. I u postupku izdavanja digitalnih certifikata za TDU podnosi se Zahtjev za izdavanje certifikata za TU te Ugovor o obavljanju usluga certificiranja. U Poreznoj upravi sve delegirane službene

osobe u radu s uslugom ePorezna i eOvrha morale su proći postupak izdavanja digitalnih certifikata. U sustavu ePorezna digitalne certifikate rabi se za autentifikaciju autorizaciju dostavi elektroničkih obrazaca. U sustavu eOvrha certifikate uporabljuju ovlaštene osobe za potpisivanje elektroničkih ovršnih akata.

U Hrvatskoj primjenu elektroničkog potpisa možemo vidjeti na primjeru internetskog servisa *hitro.hr* koji, uz ostalo, obavlja usluge e-Katastar, e-Regos, e-Mirovinsko, e-Zdravstveno, Brojne aplikacije poput ePorezne, elektroničke razmjene dokumenata, elektroničke pošte i ostalih online servisa primjenjuju elektronički popis I digitalne certificate.

ePorezna kao elektronička usluga Porezne uprave omogućuje elektroničko popunjavanje, potpisivanje i slanje elektroničkih obrazaca putem interneta. Takve se obrasce potpisuje naprednim elektroničkim potpisom koji im osigurava pravnu valjanost. Ta usluga zamjenjuje ručno ispunjavanje papirnih obrazaca I njihovu dostavu u ispostavu Porez uprave.

eOvrha omogućuje potpisivanje dokumenata (elektroničkog ovršnog akta) naprednim elektroničkim potpisom. Pri slanju elektroničkog akta primatelj, npr. FINA, zna točno tko je potpisnik dokumenta i u svakom se trenutku može utvrditi je li u procesu slanja/primanja nastala i najmanja izmjena.

Zanimljivo je i lako primjenljivo potpisivanje elektroničke pošte (e-mail) uz pomoć programa za primanje/slanje elektroničke pošte, MS Outlook. U procesu slanja elektroničke pošte najprije treba prilagoditi MS Outlook za elektroničko potpisivanje. Brojnim korisnicima sustava ePorezna i eOvrha pri instalaciji programske podrške za očitavanje digitalnih certifikata ova opcija u MS Outlooku aktivirala se automatski, pa su je korisnici mogli uporabiti. No u protivnom, ovu prilagodbu je vrlo lako aktivirati odabirom naredbe Pomoć→ Mogućnosti privatnosti→Dodaj digitalni popis izlaznim porukama. Novu kreiranu elektroničku poštu pri slanju se potpisuje automatizmom te

šalje na uobičajeni način. Elektronička pošta potpisana certifikatom primatelju jamči neporecivost pošiljatelja poruke. [13]

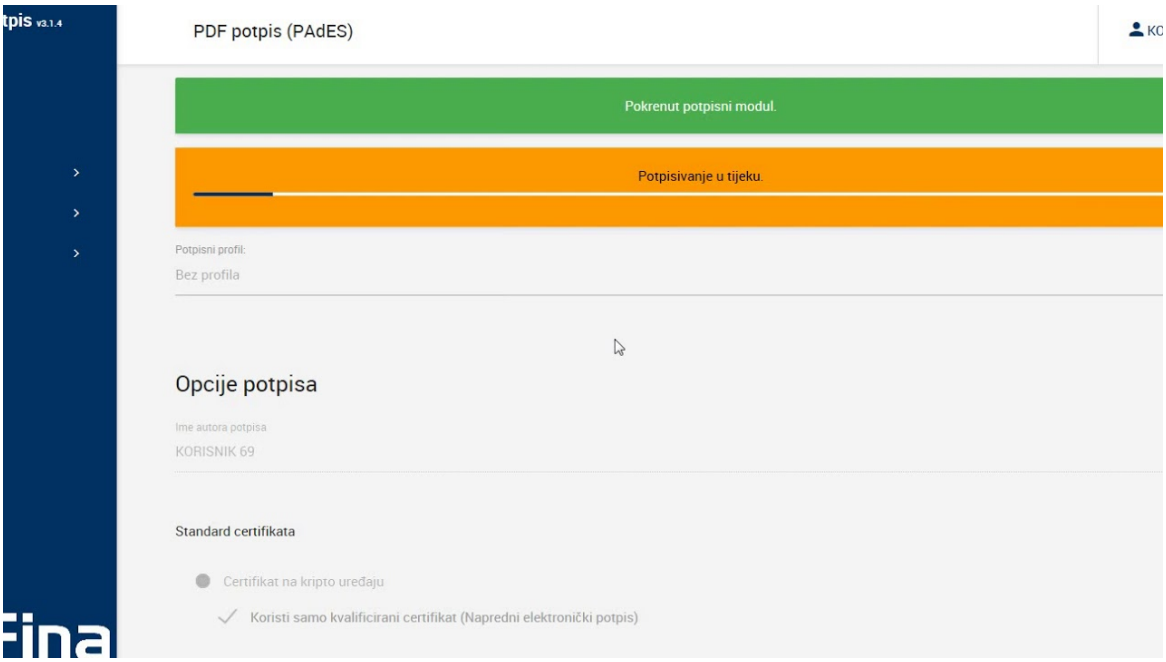
Aplikacija Web e-Potpis

Fina je razvila aplikaciju Web e-Potpis koja ima svrhu zaštititi dokumente i podatke, a nudi usluge podešavanja korisničkih postavki, digitalnog potpisivanja dokumenata, enkripcije, verifikacije potpisa, dekripcije te ugradnje vremenskog žiga. Aplikacija je dostupna na Internetu, tako da nije potrebna računalna instalacija, a pristup je omogućen sa pametnom karticom ili USB tokenom i FINA certifikatom.

Kako bi koristili aplikaciju Web e-Potpis treba imati:

- Osobno računalo
- Operacijski sustav Windows 7 ili noviji
- Internetski pristup
- Internetski preglednik Internet Explorer 10.0 ili noviji
- Java 8 ili novija verzija
- Digitalni certifikat koji je izdan na FINA-inoj pametnoj kartici ili USB tokenu
- Program za upravljanje pametnim karticama tj. tokenima
- Čitač pametnih kartica tj. tokena
- Najnovija verzija Adobe Reader-a

Dodatna je funkcionalnost aplikacija izrade verifikacije elektroničkoga naprednog elektroničkog potpisa za bilo koji format dokumenta, word, excel, notepad, ill PDF-dokument. Takav se unaprijeđen sustav potpisivanja već primjenjuje u nekim tijelima javne uprave. [17]



Slika 5. Web e-Potpis

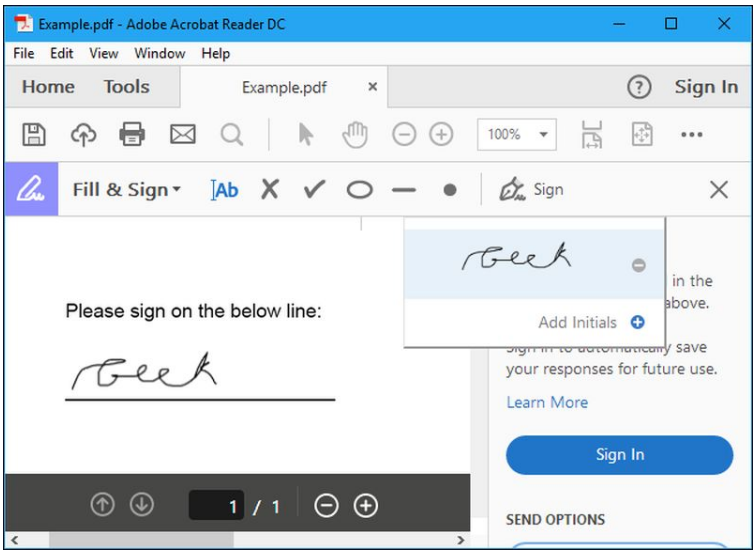
9.4. Elektronički potpis u području sigurnosti i zaštite

Kada govorimo o zaštiti na radu kao djelatnosti, možemo zaključiti da se vrlo velik dio djelatnosti bazira na papirologiji koja nije valjana bez potpisa i pečata ovlaštene osobe odnosno ustanove. Neki od dokumenata zaštite na radu su zapisnici o ispitivanju radne opreme, zapisnici o praktičnoj osposobljenosti radnika za rad na siguran način, zapisnici o stručnim osposobljavanjima i slično. Člankom 10. stavcima 4. i 5. Pravilnika o pregledu i ispitivanju radne opreme (NN 16/16) te člankom 9. stavcima 4. i 5. Pravilnika o ispitivanju radnog okoliša (NN 16/16) propisana je obveza vlastoručnog potpisivanja Zapisnika.

U tom smislu vlastoručnim potpisom podrazumijeva se i kvalificirani elektronički potpis, koji prema članku 25. stavku 2. 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, te isti ima jednaki pravni učinak kao vlastoručni potpis.

Također stručnjaci zaštite na radu obavljaju i poslove nabave osobne zaštitne opreme na način da se unese potreba za određenu osobnu zaštitnu opremu koju potpisuje direktor ili njegov ovlaštenik. Ukoliko je potreba odobrena, sa dobavljačem se dogovara količina osobne zaštitne opreme te dobavljač šalje ponudu. Ukoliko je ponuda zadovoljavajuća ona mora biti potpisana od strane naručitelja, u ovom slučaju to je stručnjak zaštite na radu, direktora ili njegovog ovlaštenika. Nakon što je ponuda potpisana, naručeni artikli idu u isporuku. Ovo je idealan slučaj u kojemu je za ponudu dovoljan naručitelj i sam vlasnik odnosno direktor tvrtke. Ukoliko se radi o većim tvrtkama, odnosno tvrtkama koje imaju zaposlene stručnjake zaštite na radu kao vanjske suradnike u odjelu kontrole kvalitete, situacija postaje složenija. U navedenom slučaju stručnjak zaštite na radu u situaciji kada je potrebna osobna zaštitna oprema, za unos potrebe mora kontaktirati rukovoditelja svog odjela (rukovoditelj kontrole kvalitete). Rukovoditelj ima ovlasti potpisati potrebu. Nakon potpisa rukovoditelja, stručnjak zaštite na radu šalje mail dobavljaču o količini i vrsti potrebne osobne zaštitne opreme. Nakon dobivene ponude, stručnjak istu prosljeđuje svom nadređenom rukovoditelju. Ukoliko je ponuda veća od interno propisane cijene, rukovoditelj odjela mora istu slati na potpis direktoru proizvodnje, koji nakon odobrenja te vlastitog potpisa šalje istu ponudu direktoru tvrtke koji svojim potpisom potvrđuje ponudu. Tek nakon svih potpisa stručnjak zaštite na radu ima ovlasti da ponudu prihvati te ju realizira sa dobavljačem. S obzirom na obujam posla rukovoditelja, direktora i ostalih viših pozicija u tvrtki ne možemo očekivati da će svatko od njih u svakom trenutku biti u tvrtki radi potpisa potrebnih narudžbi. Iz tog razloga elektronički potpis je nešto što je uvelike olakšalo i ubrzalo nabavu u svim tvrtkama. U današnje vrijeme pristup mailu možemo imati u svakom trenutku putem našim mobilnih uređaja na kojemu možemo pristupiti mailu. Ukoliko je tvrtki nešto neophodno, direktor ponudu dobiva na mail koju može proslijediti ovlaštenoj osobi koja je u mogućnosti ponudu potpisati odmah te istog trena potpisanu vratiti osobama u tvrtki koje mogu vrlo brzo realizirati potrebne materijale.



Slika 6. Primjer digitalnog potpisa

9.5. Elektronička kartica

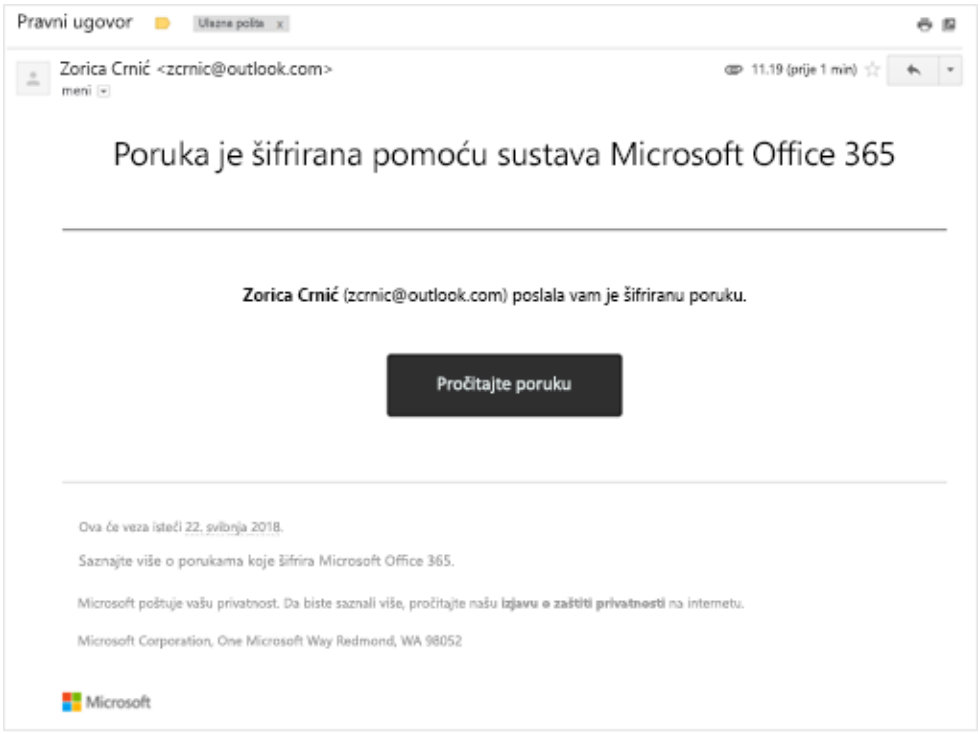
U današnje vrijeme sve više tvrtki koristi elektroničke (pametne) kartice koje imaju višenamjenska svojstva. Primarno, kartice se koriste za "*check in*" odnosno za prijavu pri dolasku na posao te odlasku s posla. Uređaji za skeniranje kartica povezani su mrežom tvrtke te ovlaštene osobe imaju uvid u situaciju tko je na poslu dostupan a tko ne. Također na mjesečnoj bazi uređaji za svakog radnika broje sate provedene u tvrtki koje na kraju mjeseca pretvaraju u osobni dobit odnosno plaću. U gore navedenom tekstu spominjali smo elektroničko potpisivanje koje ne bi bilo moguće bez elektroničke kartice. Naime, svaka osoba ima ovlaštenja na samoj kartici koja joj omogućuju određene radnje. Ovlaštenja koja pruža ovisi o poziciji u tvrtki te radnom mjestu. Konkretno kada se radi o poslovima zaštite na radu, elektronička kartica ima nekoliko funkcija.

Slika 7. Elektronička kartica

9.5.1. Šifrirani mail

Osoba u odjelu zaštite na radu mora biti u stalnom kontaktu sa kadrovskom službom koja vrši upis i zaprimanje novih radnika. Svaki radnik pri promjeni radnog mjesta mora biti osposobljen za rad na siguran način koje provodi stručnjak zaštite na radu. Kadrovska služba šalje informacije stručnjaku zaštite na radu o zaposlenju novog radnika te terminu početka rada navedenog radnika. Stručnjak da bi proveo osposobljavanje za rad na siguran način mora zatražiti osobne podatke novog radnika kao što su, ime i prezime, OIB, ime oca/majke, datum rođenja, stručna sprema te posao koji će radnik obavljati. Da ne bi došlo do krađe osobnih podataka prilikom slanja ovakvih mailova koristi se već spomenuta elektronička kartica koja se poveže sa računalom te ona omogućuje slanje šifriranog maila. Nakon slanja maila, osoba koja primi šifrirani mail neće moći otvoriti mail dok ne spoji elektroničku karticu koja ima ovlaštenje za čitanje šifriranih mailova. U ovom slučaju ukoliko se mail pošalje na krivu adresu ili nepoznata osoba pristupi ovakvom mailu neće moći pročitati sadržaj maila dok

god nema elektroničku karticu koja to omogućuje. Prilikom slanja šifriranog maila, postoji dodatna sigurnosna značajka koja omogućuje da osoba koja je mail poslala u svakom trenutku može vidjeti tko je mail pročitao te u kojem trenutku.



Slika 8. Šifrirani mail

9.5.2. Interne informacije

Kada se radi o internim informacijama kao što su slanje uputnica za liječnički pregled, odluke o zabrani rada za pojedinog radnika, obavijesti o pristigloj opremi i slično, nije obavezno da mail koji sadrži takve informacije bude šifriran. No s druge strane stručnjaci zaštite na radu provode testiranje na opojna sredstva te alkotestiranje koje se smatraju delikatnim informacijama te prilikom pisanja izvještaja o takvim situacijama moraju poštivati određena pravila. Alkotestiranje unutar tvrtke radi se ne

najavljeno. Elektronička kartica omogućuje stručnjaku koji provodi alkotestiranje da putem programa na računalu ima uvid u "*check in*" radnika. To je važno iz razloga što se *alkotestiranje* najavljuje 10-ak minuta prije samog izvršenja putem maila u koji su uključeni rukovoditelji odjela koji će biti alkotestiran, podaci o radnicima su već zaprimljeni prije slanja maila te ukoliko se dogodi da je određeni radnik prijavljen na posao no nije prisustvovao alkotestiranju smatrat će se da je pod utjecajem alkohola. Nakon provedenog alkotestiranja ukoliko ima radnika koji su "pozitivni" na alkotest, sastavlja se zapisnik koji potpisuje radnik koji je bio pozitivan na alkotestu, njegov rukovoditelj te stručnjak zaštite na radu koji je proveo alkotestiranje. Dužnost rukovoditelja je zabraniti rad alkoholiziranom radniku, a dužnost stručnjaka zaštite na radu je zapisnik poslati osobama zaduženim za takve situacije u tvrtki. Zapisnik se šalje također putem maila no ovoga puta šifriranjem maila prve kategorije što znači da osoba koja je primila takav mail mora imati posebno ovlaštenje na svojoj elektroničkoj kartici i slanje takvog maila moguće je isključivo jednoj osobi. Nakon što navedena osoba dešifrira mail ima određeni period da datoteku obradi te nakon isteka vremena mail se automatski briše.

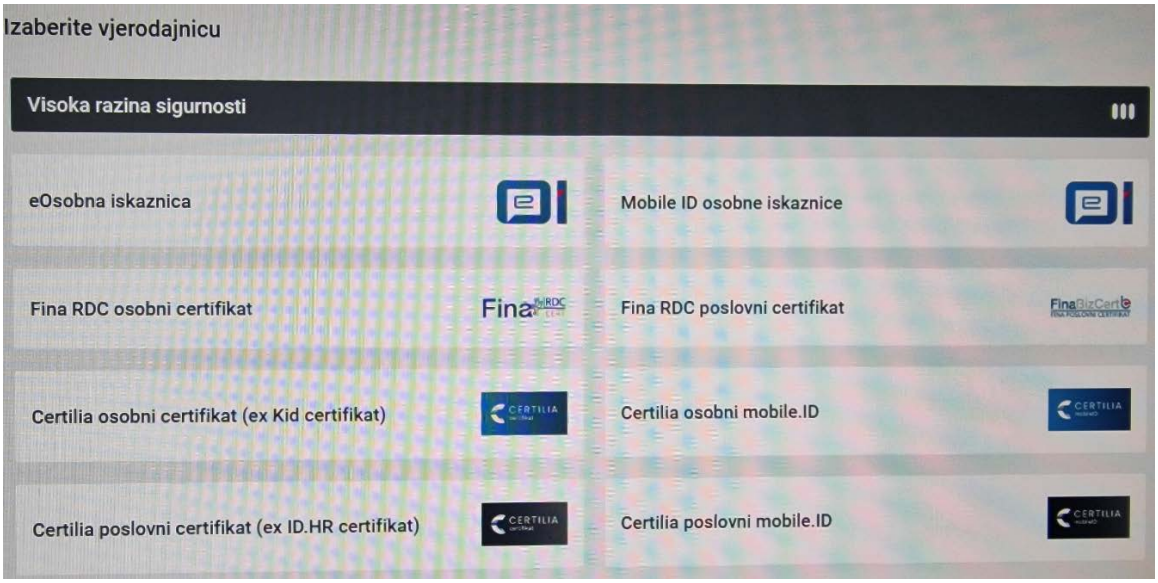
9.6. eOI

Iskaznica naime uz podatke ispisane na samoj kartici, ima do dva certifikata, identifikacijski i potpisni. Identifikacijski certifikat koristi se za elektroničku potvrdu identiteta i autentikaciju prilikom pristupa elektroničkim uslugama, dok potpisni služi kao podrška naprednom elektroničkom potpisu i zamjenjuje vlastoručni potpis, sukladno zakonu kojim je reguliran elektronički potpis. To ustvari znači da je elektronička osobna iskaznica vjerodajnica visoke razine sigurnosti, uz koju građanin može koristiti sve usluga sustava e-Građani, ali i druge elektroničke usluge u Hrvatskoj, neovisno o pružatelju. Uz to, hrvatska e-osobna iskaznica je kao vjerodajnica visoke razine sigurnosti prihvaćena i na području Europskog gospodarskog prostora (zemlje EU-a, Norveška, Island i Lihtenštajn).

9.6.1. Korištenje eOI

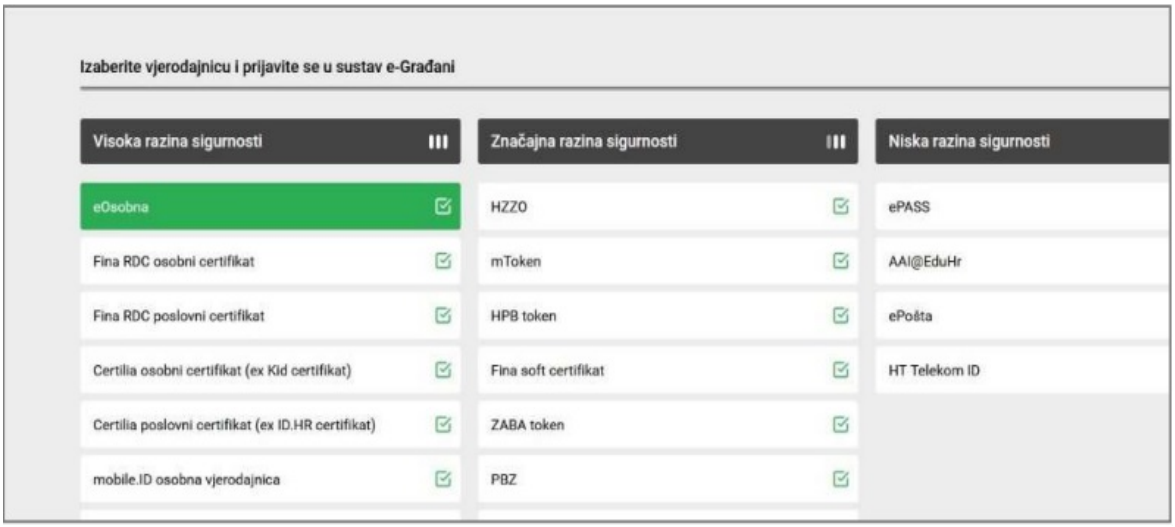
Sustav e-građani uvelike je olakšao pronalaženje odnosno dohvat podataka iz osobnog života kao što je rodni list, vjenčani list, porezna kartica, uvjerenja o školovanju i slično. Na primjeru koji slijedi pokazat ćemo kako doći do rodnog lista putem elektroničke osobne iskaznice koja služi kao vjerodajnica da smo to uistinu mi te nam tako omogućuje da iz vlastitog doma bez nepotebnog putovanja i gubljenja vremena u općini dođemo do traženog dokumenta.

Na sustavu e-građani odaberemo “ Katalog usluga “ te odaberemo poveznicu “ Obitelj i život” nakon čega nam se otvore sve podmape koje su vezane za obitelj i život. Odabirom na “ e-matične knjige” dolazimo do sustava za prijavu da bi došli do traženog dokumenta.



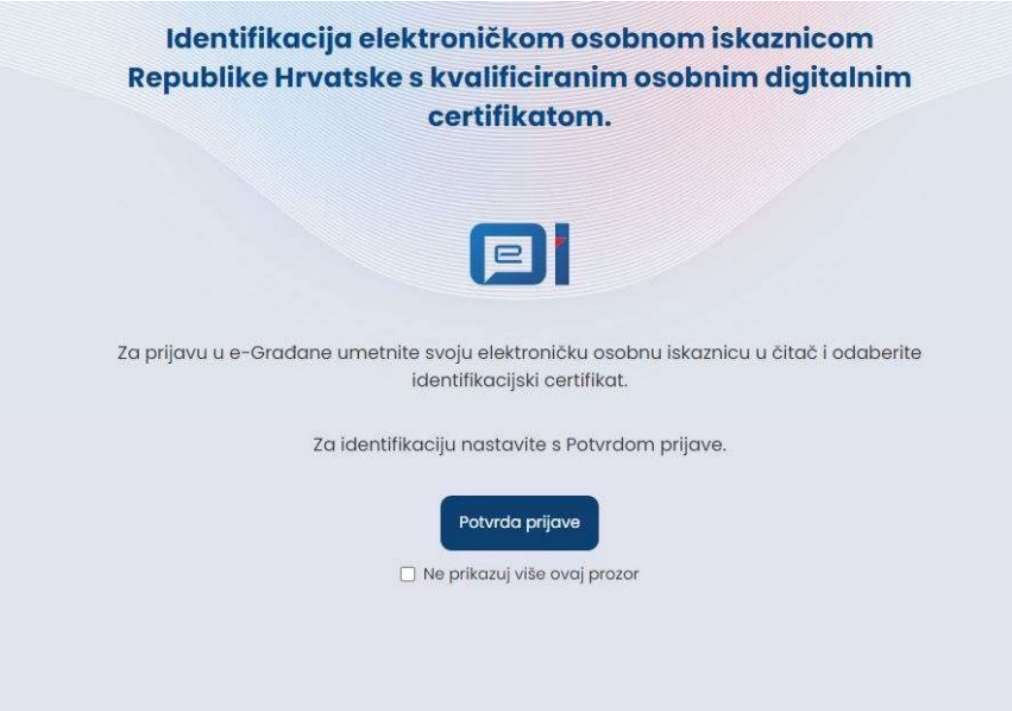
Slika 9. Odabir vjerodajnice

U sustavu za prijavu na slici 9 odaberemo “eOsobna iskaznica”. Nakon odabira navedenog dolazimo na sljedeći korak koji se nalazi na slici 10 gdje se nalaze razni certifikati pomoću kojih se možemo prijaviti. Na slici su vidljive različite razine sigurnosti. Razlika u razinama je ta što određene dokumente ne možemo dobiti online načinom ukoliko nemamo certifikat koji spada pod visoku razinu sigurnosti. Primjerice kada bismo sa sustava “e-građani” željeli pristupiti dokumentu o školovanju, to bismo mogli učiniti sa jednim od načina koji su na slici navedeni u stupcu “ Niska razina sigurnosti”. No ukoliko želimo osobni dokument koji sadrži naše privatne podatke kao što je naš traženi rodni list moramo koristiti jedan od načina koji se nalaze u stupcu “ Visoka razina sigurnosti”.



Slika 10. Pristupanje sustavu putem eOsobne

Nakon odabira eOsobna, dolazimo do sljedećeg koraka koji se nalazi na slici 11.



Slika 11. Identifikacija elektroničkom osobnom iskaznicom

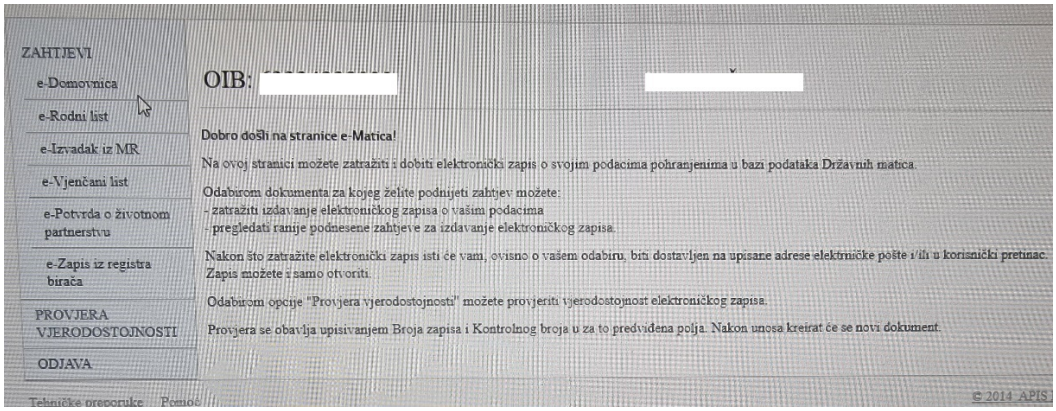
Da bi nastavili prijavu, važeću elektroničku osobnu iskaznicu moramo umetnuti u čitač kartica povezan na naše računalo ili mobilni uređaj kao što je prikazano slikom 12 .

Slika 12. Umetanje osobne iskaznice u čitač kartica

Ukoliko je kartica uspješno očitana sustav nas vodi na sljedeći korak na slici 13 nam daje mogućnost odabiranja certifikata za prijavu koji se nalazi na elektroničkoj iskaznici te potreban pin koji smo sami dodijelili svom certifikatu prilikom aktivacije osobne iskaznice koja nam je izdana od strane MUP-a.

Slika 13. Odabir identifikacijskog certifikata

Nakon uspješnog odabira certifikata i pripadajućeg pina ulazimo u sustav gdje vidimo mogućnost izdavanja željenih dokumenata.



Slika 14. Odabir željenog dokumenta

Nakon odabira željenog dokumenta, u našem slučaju e-Rodni list, dolazimo do dijela sustava u kojem upisujemo željenu adresu e-pošte na koju želimo da nam dokument bude poslan i na taj način imamo valjan i jednako vrijedan dokument kao da smo ga osobno zatražili i dobili u općini.

10. ZAKLJUČAK

Uvođenje i širenje upotrebe elektroničkih isprava nužno je zbog općenitog smanjenja troškova poslovanja na razini cijeloga gospodarstva, jer utječe na stvaranje veće dodane vrijednosti, pridonosi uštedama te, što je možda najvažnije, smanjuje sivu ekonomiju i korupciju. Elektroničko poslovanje postupno prestaje biti nepoznanicom i sve smo bliže vremenu kada će tradicionalne oblike poslovanja posve nadomjestiti elektroničko. Dotad predstoje brojne promjene i izazovi, prihvaćanje novih tehnologija, ustrojstvene promjene na svim razinama poslovanja te daljnja prilagodba zakonskih propisa. Primjena elektroničkog potpisa kao sigurnog rješenje za takav oblik poslovanja sve je raširenija i utjelovljuje višu razinu povjerenja, što privlači sve veći broj sudionika (korisnika).

Kako živimo u naprednom dobu, u dobu tehnologije, elektronički potpis za nas je svakodnevica. Bilo da se radi o digitalnom potpisu, ili o skeniranom potpisu, on nam je glavno sredstvo za hvatanje koraka s tempom suvremenog poslovanja. Digitalni potpis predstavlja ključ povjerenja i sigurnosti u suvremenom internetskom poslovanju. Omogućuje jednostavnije i brže potpisivanje, uštedu poštanskih troškova, lakše sklapanje ugovora, elektroničko slanje dokumenata, zahtjeva, narudžbi i sl. Digitalni potpisi se danas koriste svakodnevno, od razmjene email poruka do bankovnih transakcija. Mnoge institucije danas umjesto ručnog potpisa koriste digitalni potpis, koji ima istu važnost, te je pravno u potpunost potkrijepljeno. Iako svi znamo da imamo pravnu zaštitu mnogi ljudi se boje digitalnog potpisa, jer su uvjereni da se njihov potpis može iskoristiti u bilo koje druge svrhe. Za takve slučajeve imamo zaštitu koja je regulirana zakonom. Glavni čimbenik koji potiče rast korištenja digitalnih potpisa je razvoj online poslovanja. To dovodi i do smanjenja korištenja papira i slanja dokumenata poštom, što značajno smanjuje troškove poslovanja. Digitalni potpisi omogućuju brže i jeftinije poslovanje što će značajno pridonijeti njegovom isključivom korištenju u budućnosti. Sa sve većom zastupljenošću digitalnih potpisa, rastu i pokušaji napada te zlouporabe. Stoga je važno dalje razvijati sigurnosne mehanizme koji će omogućiti još veću sigurnost digitalnog potpisa. Mnogi poduzetnici više preferiraju osobnu

komunikaciju, slabo se educiraju i nemaju povjerenje u tehnologiju digitalnog potpisa, a tu su također i veći inicijalni troškovi zbog implementacije (certifikati, baza podataka, programska podrška). Za sada tržište nije u potpunosti doraslo da se potpuno okrene elektroničkom potpisu, što iz neopremljenosti i nedostatak sredstava, što zbog manjka stručnosti. Unatoč tome, možemo očekivati u budućnosti da će digitalni potpis biti glavna metoda potpisivanja, dok će vlastoručni potpis ostati u primjeni u određenim slučajevima. U ovom radu objašnjeno je značenje elektroničkog i digitalnog potpisa, elektroničkog certifikata i svih povezanih elemenata.

Kada govorimo o zaštiti na radu dolazimo do zaključka da je elektronički potpis nešto što je prijeko potrebno u suvremenom funkcioniranju društva. Svjesni smo učestalih promjena radnih mjesta zbog razno raznih razloga, samim time nužna su osposobljavanja koja zahtijevaju potpisivanje dokumentacije. Također osobna zaštitna oprema kao i radna oprema neophodna je za rad tvrtke te iz tog razloga proizlazi potreba za naručivanjem i nabavom iste i taj proces mora biti brz i kratkotrajan da tvrtka ne bi negativno poslovala odnosno bila u zaostacima. U provođenju zaštite na radu unutar tvrtke proizlazi potreba za elektroničkom karticom koja omogućuje tajnost i sigurnost osobnih podataka koji se šalju putem maila. Na osnovu svega navedenog dolazimo do zaključka kako je i iz perspektive sigurnosti i zaštite elektronički potpis neophodan za funkcioniranje poslovanja tvrtki u suvremenom svijetu.

11. LITERATURA

[1] Whitman M. E., Mattord H. J. (2017.), "Principles of Information Security, Cengage.Learning" https://books.google.hr/books?id=Hwk1EAAAQBAJ&pg=PA1&hl=hr&source=gbs_toc_r&cad=3#v=onepage&q&f=false (pristupljeno 16.10.2022)

[2] Hrvatska liječnička komora *"Uputa za elektroničko potpisivanje PDF dokumenata"* www.hlk.hr (pristupljeno 17.10.2022)

[3] Katulić T.*: " Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u Hrvatskom i poredbenom pravu"*, Zbornik pravnog fakulteta u Zagrebu, Zagreb, (2011.), str.1342.

[4] Kriptografija https://ematematika.hr/hr/kriptografija/bpid/89 (pristupljeno 17.10.2022.)

[5] Nikšić S.: "*Elektronički potpis u skladu sa smjernicom 1999/93/EC"*, Pravo u gospodarstvu, vol. 39. no. 5, Zagreb, (2000.), str. 258.

[6] Ledinski S. *"Sustavna programska potpora"*, Varaždin 2003.

[7] POS sustav, "*Što je PKI"* https://www.astrum.hr/konobar/2012/10/sto-je-pki/ (pristupljeno 13.10.2022)

[8] Katulić T: "*Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u Hrvatskom i poredbenom pravu"*, Zbornik pravnog fakulteta u Zagrebu 2011, str.1342.

[9] Rebac F. *"Digitalna knjižnica u sustavu javnih ključeva",* http://sigurnost.zemris.fer.hr/pki/2006_rebac/index.html (pristupljeno 17.10.2022)

[10] Narodne novine, *"Zakon o elektroničkom potpisu"* NN 10/2002 https://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html (pristupljeno 17.10.2022)

[11]MINGO HR, Ministarstvo gospodarstva, e-Potpis. https://mingor.gov.hr/#index.php?query=page/kategorija/e-potpis(pristupljeno03.11.2022.)

[12] Nives T. *" Digitalni potpisi i CA certifikati"*

[13] FINA, *"Digitalni certifikati i vremenski žig"* https://www.fina.hr/finadigicert (pristupljeno 14.10.2022)

[14] Dujella A., Maretić M. *"Kriptografija"*, Element Zagreb 2007, str.3

[15] Uredba EU br.910/2014 EUROPSKOG PARLAMENTA I VIJEĆA *o "elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ" https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-%28EU%29-br.-910-2014-Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999-93-EZ (pristupljeno 17.10.2022)*

[16] Vojković G.: "*Elektronički potpis"*, Godišnjak 12 Hrvatskog društva za građanskopravne znanosti i praksu, Zagreb, (2005.), str. 463.

[17] FINA, *"Usluga Web e-Potpis"* https://www.fina.hr/web-e-potpis1 (pristupljeno 16.10.2022)

12. PRILOZI

12.1. Popis slika