Digitalni potpis

Skorić, Ivona

Undergraduate thesis / Završni rad

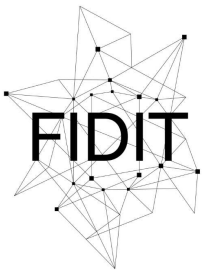
2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka / Sveučilište u Rijeci**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:195:495416

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-26**



Sveučilište u Rijeci
Fakultet informatike
i digitalnih tehnologija

Repository / Repozitorij:

Repository of the University of Rijeka, Faculty of Informatics and Digital Technologies - INFORI Repository

Sveučilište u Rijeci – Odjel za informatiku

Preddiplomski jednopredmetni studij informatike

Ivona Skorić

Digitalni potpis

Završni rad

Mentor: doc. dr. sc. Božidar Kovačić

Rijeka, rujan 2018.

Sažetak:

U ovom završnom radu opisan je pojam digitalni potpis (tehnika, algoritmi, primjena). Rad započinje kratkim povijesnim pregledom, a nakon toga se upoznajemo s tehnikama digitalnog potpisivanja te se navode tri najvažnija algoritma (RSA, DSA, EDSA). Detaljno je opisana primjena digitalnog potpisa u različitim područjima rada i upute za korištenje Finine internetske aplikacije Web e-Potpis. Rad je zaključen s nekoliko zakonskih članaka i predviđanja primjene digitalnog potpisa u budućnosti.

Ključne riječi:

Digitalni potpis, kriptografija, ključ, certifikat, DSA, EDSA, RSA, enkripcija, dekripcija, verifikacija

Sadržaj

1. Uvod 4

2. Povijest digitalnog potpisa 5

3. Tehnike digitalnog potpisa 7

3.1. Enkripcija s javnim ključem 7

3.2. Enkripcija s privatnim ključem 9

3.3. Digitalni certifikat 10

4. Algoritmi za digitalno potpisivanje 11

5. Primjena digitalnog potpisa 13

5.1. Digitalno potpisivanje dokumenta 13

5.2. Slijepi potpis 14

5.3. Digitalni potpis u internetskim aplikacijama 15

5.4. Digitalni potpis multimedijskih sadržaja 16

6. Digitalni potpis u praksi – aplikacija Web e-Potpis 17

6.1. Digitalni certifikati 17

6.2. Aplikacija Web e-Potpis 17

6.2.1. Prijava u aplikaciju 18

6.2.2. Registracija korisnika 19

6.2.3. Potpisivanje dokumenta 20

6.2.4. Potpisivanje PDF-a 21

6.2.5. Enkripcija 22

6.2.6. Dekripcija 22

6.2.7. Verifikacija potpisa 23

7. Zakonska regulativa 24

8. Zaključak 26

9. Literatura i izvori 27

10. Popis slika i tablica 28

1. Uvod

U informatičkom i poslovnom svijetu često se susrećemo s pojmom digitalni potpis (engl. *digital signature – DS*) koji nam omogućuje pojednostavljeno i ubrzano poslovanje uz veliku vremensku uštedu. Pojam digitalni potpis definiran je kao „šifriranje kojim se dokazuje autorstvo tj. izvor elektroničkog dokumenta“ prema Hrvatskom enciklopedijskom rječniku. To je, jednostavnije rečeno, digitalna verzija vlastoručnog potpisa koja uz određene zakone vrijedi isto kao i rukom potpisan dokument.

Digitalni potpis omogućuje utvrđivanje autentičnosti elektroničkog dokumenta, a dokument je autentičan ako je poznat identitet autora. Kako bi se provjerila vjerodostojnost potpisanog dokumenta koristi se postupak pod nazivom enkripcija kojim se podaci kodiraju prije slanja kako bi ih samo odgovarajuća osoba (primatelj) mogla razumjeti i dekodirati. Uz autentičnost, digitalni potpis osigurava i integritet (sigurnost da podaci nisu promijenjeni ili uništeni tokom prijenosa do primatelja) i neporecivost (pošiljatelj ne može poreći sudjelovanje u procesu jer je on jedini ima uvid u svoj privatni ključ kojim je poruka potpisana).
Funkcijom potpisa stvara se par kriptografskih ključeva (javni i privatni), a poruka koja se potpisuje sažima se *hash*[1] algoritmom. Privatni ključ (engl. *private key*) je u potpunosti tajan, a javni ključ (engl. *public key*) je dostupan svima. Zatim se iz sažete poruke i korisnikova privatnog ključa stvara digitalni potpis koji se objavljuje ili šalje zajedno s potpisanom porukom.

Ovaj rad obuhvaća pregled povijesnog razvoja digitalnog potpisa, principe i algoritme koji se najčešće koriste te primjenu digitalnog potpisa u praksi.

[1] Algoritam koji od podataka proizvoljne dužine stvara podatke fiksne dužine

2. Povijest digitalnog 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 (Alice), a *primatelj* osoba koja prima poruku (Bob). *Napadač* (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.

80-ih godina prošlog stoljeća faks uređaj je bio u velikoj upotrebi među tvrtkama i pojedincima za hitno slanje papirnatih dokumenata. 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.

1860. godine započinje korištenje Morseove abecede kako bi se poruke prenosile telegrafom, a desetak godina nakon presudom suda *New Hampshire Suprime Court* potpisi preneseni na ovaj način su proglašeni pravomoćnima.

1874. godine započinje razvoj kriptografije s javnim ključem 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. Tehnike digitalnog potpisa

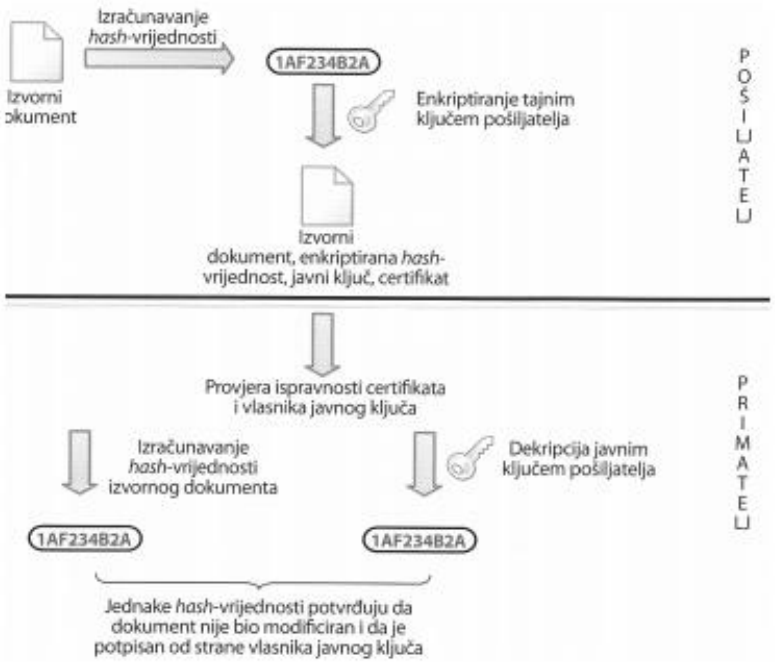
Kao što je navedeno u uvodnom poglavlju, digitalnim potpisom osigurava se autentičnost i integritet dokumenta ili autora, a to podrazumijeva da je identitet autora poznat i sigurnost da se dokument nije promijenio tokom prijenosa. Za provjeru vjerodostojnosti koristi se proces kodiranja podataka prije slanja kako bi ih samo odgovarajuća osoba mogla razumjeti i dekodirati tj. enkripcija. Vjerodostojnost podataka ili autora moguće je provjeriti korištenjem:

- enkripcije s javnim ključem
- enkripcije s privatnim ključem
- digitalnim certifikatima

3.1. Enkripcija s javnim ključem (engl. *Public key encription*)

Kod stvaranja digitalnog potpisa koristi se privatni ključ, a za njegovu provjeru javni koji odgovara, ali nije jednak privatnom ključu. Vlastiti privatni i javni ključ posjeduje svaki korisnik. Javni ključevi su dostupni svima i omogućuju svakom korisniku provjeru potpisa, a privatni ključ je poznat jedino svom vlasniku čime se onemogućuje krivotvorenje potpisa. Primatelj se koristi javnim ključem pošiljatelja te vlastitim privatnim ključem kako bi uspješno dešifrirao poruku.

Na Slici 1. prikazan je postupak stvaranja i provjere digitalnog potpisa. Podaci koji se digitalno potpisuju moraju se sažeti u inačicu poruke, a za to je potrebna sigurna jednosmjerna funkcija tj. SHA (engl. *Secure Hash Algorithm*) algoritam. To je funkcija koja se matematički lako izračunava, ali je teško pronaći inverznu funkciju. Tako dobivena sažeta inačica poruke se šifrira vlastitim tajnim ključem i potpisuje. Zajedno s potpisom, pošiljatelj šalje poruku primatelju. On prima sažetu poruku i pomoću pošiljateljevog javnog ključa dešifrira primljeni sažetak. Potpis je vjerodostojan u slučaju da se primljeni sažetak i sažetak kojeg je stvorio primatelj podudaraju. Potrebno je koristiti isti SHA algoritam kod provjere i prilikom stvaranja potpisa.



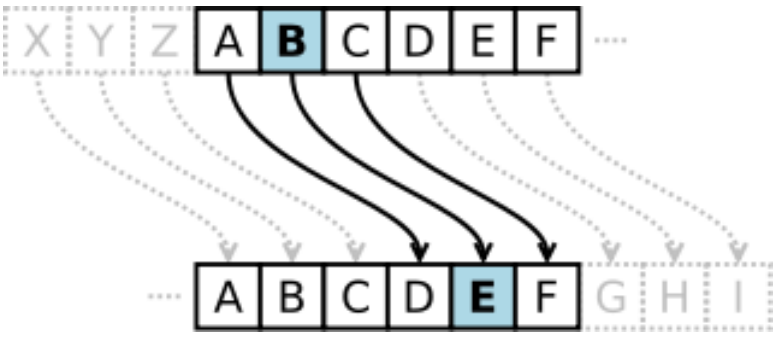
Slika 1: Shematski prikaz postupka stvaranja i provjere digitalnog potpisa

U opisanom postupku ne potpisuje se cijela poruka nego sažeta inačica poruke zbog efikasnosti (sveobuhvatni postupak će biti brži i potpis kraći), integriteta (poruka koja se potpisuje treba biti kraća od duljine privatnog ključa, a u većini slučajeva to nije pa je potrebno poruku razlomiti na dijelove, potpisati pojedinačno svaki dio i poslati) i javne dostupnosti dokumenta (javni dokumenti kao što su diplome, ugovori, potvrde itd. trebaju biti javno dostupni svima pa se prenose i spremaju bez enkripcije, a potpis garantira vjerodostojnost dokumenta).

3.2. Enkripcija s privatnim ključem (engl. *Private key encription*)

Svaki korisnik ili računalo imaju vlastiti privatni (tajni) ključ uz pomoć kojeg se podaci šifriraju prije slanja. Prije uspostave komunikacije je potrebno znati koji korisnici tj. računala će razmjenjivati poruke i na svako računalo instalirati privatne ključeve onih računala od kojih se očekuju poruke. Enkripciju s privatnim ključem možemo pojednostaviti kao komunikaciju pomoću tajnog koda, koji računala ili korisnici moraju znati ako žele dešifrirati poruku.

Kao primjer možemo navesti Cezarovu šifru (Slika 2.), a to je najjednostavniji tip zamjene (supstitucije) kod kojeg se svako slovo zamjenjuje određenim slovom iz abecede, pomaknutim za određeni broj mjesta. Vrijednost tog pomaka možemo smatrati privatnim ključem, a njegova vrijednost je poznata primatelju. Kada primatelj primi pošiljateljevu šifriranu poruku, s obzirom da zna za koliko je mjesta abeceda pomaknuta prilikom šifriranja, on će biti u mogućnosti uspješno ju dešifrirati. Ostali potencijalni napadači će vidjeti samo niz besmislenih znakova, pošto ne znaju vrijednost pomaka abecede.



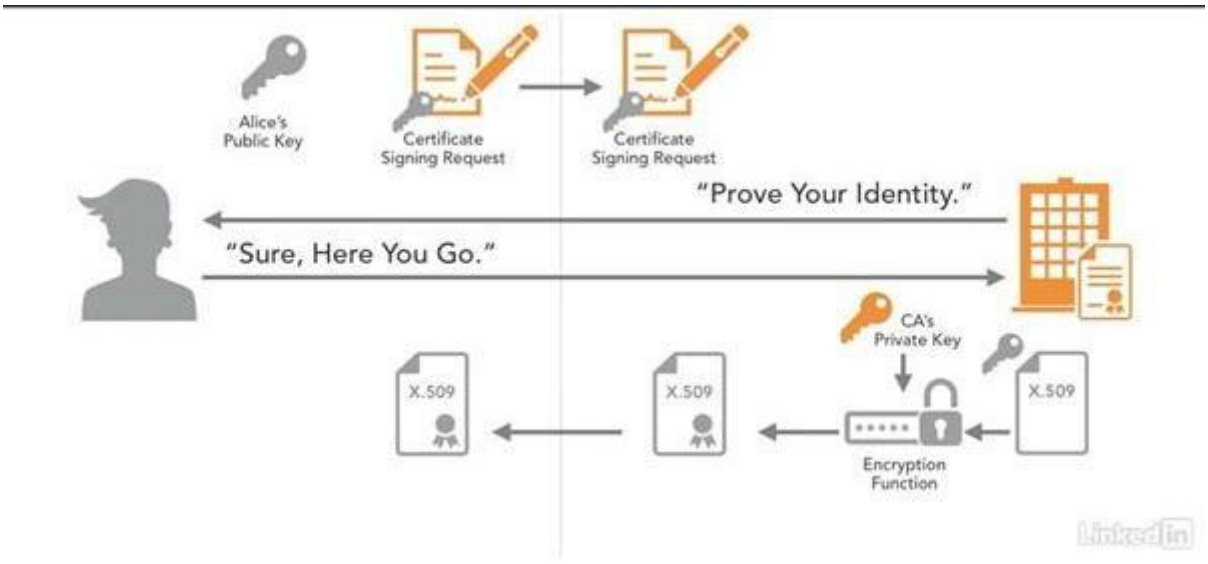
Slika 2. Cezarova šifra - supstitucija

3.3. Digitalni certifikat

Digitalni certifikati služe kao potvrda kod implementacije enkripcije s javnim ključem, a predstavljaju elektronički identitet u elektroničkim transakcijama i omogućuju povjerljivu i sigurnu komunikaciju internetom. Certifikat možemo nazvati digitalnom „osobnom iskaznicom“ jer njime dokazujemo da je informacija koju smo poslali autentična. Povezuje podatke o identitetu korisnika s njegovim javnim ključem.

Certifikacijska tijela (engl. *Certificate Authority*) ovlaštena su za provjeru i utvrđivanje identiteta i izdavanje digitalnog certifikata, a dio su PKI (engl. *public key infrastructure*) sustava. Trenutno važena norma je X.509 v3. Digitalni certifikat sadrži podatke o identitetu kao što su ime vlasnika, vlasnikov javni ključ, datum do kojega vrijedi javni ključ, naziv tijela koje je izdalo certifikat i sl.

Nakon stvaranja digitalnog certifikata, ovlašteno tijelo ga digitalno potpisuje svojim tajnim ključem, tako da se njegov sadržaj može pročitati isključivo korištenjem CA javnog ključa, i ne može se neovlašteno mijenjati. Proces stvaranja digitalnog certifikata prikazan je na Slici 3.



Slika 3. Shematski prikaz stvaranja digitalnog certifikata

4. Algoritmi za digitalno potpisivanje

Sustav digitalnog potpisivanja sastoji se od osnovnih koraka:

1) generiranje privatnog i javnog ključa – korištenjem privatnog ključa poruka se potpisuje, a verificira pomoću javnog ključa
2) stvaranje digitalnog potpisa – potpis se generira na temelju sažetka poruke i privatnog ključa
3) provjera potpisa – utvrđuje se vjerodostojnost potpisane poruke korištenjem javnog ključa

U nastavku su opisana tri najpouzdanija i najčešća algoritma koja se koriste kod digitalnog potpisivanja, a temelje se na algoritmima asimetrične kriptografije tzv. kriptografija javnog ključa:

- DSA (engl. *Digital Signature Algorithm*) algoritam odobren je od strane DSS (engl. *Digital Signature Standard*) standarda savezne vlade Sjedinjenih Američkih Država, a koriste ga sve civilne vladine organizacije i nevladine tvrtke koje su u suradnji s vladom. David W. Kravitz, bivši agent NSA (engl. *National Security Agency*) je osmislio algoritam 1991. godine, a može se besplatno koristiti. Navedeni algoritam za digitalno potpisivanje sastoji se od tri podalgoritama: generiranja parametra i izračuna ključeva, potpisivanja poruke te provjere vjerodostojnosti poruke.

- ECDSA (engl *Elliptic Curve Digital Signature Algorithm*) je nastao iz prethodno opisanog DSA algoritma, a koristi eliptične krivulje uz koje ovaj algoritam ima istu razinu zaštite, no rezultira manjim ključevima od DSA algoritma. Većina algoritama se u kriptografiji (prije korištenje eliptičnih krivulja) temeljila na problemu faktorizacije velikih brojeva. Miler i Koblitz su 1985. godine prvi primijenili eliptične krivulje na ovom području.

- RSA (*Rivest – Shamir – Adleman*) je jedan od prvih praktičnih kriptografskih algoritama za potpisivanje poruke. Ime algoritma potječe od prvih slova prezimena autora. Pošiljatelj potpisuje poruku pomoću vlastitog privatnog ključa, a šifrira korištenjem javnog ključa primatelja. Kada primatelj primi poruku, on ju dešifrira korištenjem vlastitog privatnog ključa, a provjeru vjerodostojnosti potpisa vrši uz

pomoć javnog ključa potpisane osobe. Algoritam RSA se sastoji od pet koraka: generiranja parametra i izračuna ključeva, potpisivanja poruke, šifriranje poruke, dešifriranje poruke te provjere vjerodostojnosti poruke.

RSA algoritam je jednostavniji za implementaciju, u usporedbi s ECDSA, no ECDSA algoritam se češće koristi zbog činjenice da se kod kriptosustava zasnovanih na eliptičnim krivuljama postiže veća sigurnost s puno kraćim ključevima. U Tablici 1. je usporedno prikazano predviđanje duljine ključeva u bitovima kod algoritma koji se zasnivaju na faktorizaciji (RSA) i zasnovana na polju eliptičnih krivulja (ECDSA). Vidimo da je omjer duljine ključeva kod ECDSA algoritma u stalnom porastu, a takvo je predviđanje i za budućnost.

RSA algoritam je brži u kodiranju i verifikaciji potpisa, u usporedbi s DSA, no DSA je brži u dekodiranju i generiranju ključeva. U slučaju digitalnog potpisivanja, češći je odabir DSA algoritma iako su podjednako jaki.

Godina	RSA duljina ključa	ECDSA duljina ključa	Omjer ECDSA/RSA
1990.	622	117	1:5
2000.	952	132	1:7
2010.	1369	146	1:9
2020.	1881	161	1:12
2030.	2493	176	1:14
2040.	3214	191	1:17
2050.	4047	206	1:20

Tablica 1. Usporedba duljine ključeva u prošlosti i budućnosti

5. Primjena digitalnog potpisa

Informatičko poslovanje je veoma važan i nezamjenjiv način komunikacije u današnje doba. Stoga, bez napredne zaštite i osiguranja, unatoč svim prednostima koje donosi, može biti izvor brojnih rizika. Zato digitalni potpis predstavlja sigurnost i povjerenje na širokom spektru djelatnosti i usluga, a najviše se koriste u područjima potpisivanja dokumenata, slijepog potpisa, potpisa u internetskim aplikacijama i kao zaštita multimedijalnih sadržaja.

5.1. Digitalno potpisivanje dokumenata

Kao što je već navedeno u ovom radu, digitalno potpisivanje je u mnogim zemljama po pravnoj važnosti izjednačeno s ručnim potpisom, a to znači da pravno obvezuje potpisnika prema uvjetima navedenim u potpisanom dokumentu. Zato se preporučuje korištenje različitih parova ključeva za šifriranje i potpisivanje. Korisnik sudjeluje u komunikaciji, ali to ne znači da se potpisuje svaka poslana poruka. Ona se potpisuje na kraju, parom ključeva za potpis, kada se postigne dogovor među dvjema zainteresiranim stranama.

Algoritmi i protokoli za digitalni potpis ne pružaju informaciju o vremenu kada je dokument potpisan. Jedno od rješenja je da potpisnik uključi vremensku oznaku (engl. *time stamp*) unutar digitalnog potpisa ili da u samom dokumentu spomene datum i vrijeme potpisivanja, što se ne preporučuje zbog mogućeg namjernog krivog navođenja krivog vremena. Kako bi spriječili zloupotrebu digitalnog potpisa, uvode se sigurne vremenske oznake (engl. trusted time stamp), a njih dodjeljuje pouzdana treća strana zvana TSA (engl. *Time Stamping Authority*) koja potvrđuje postojanje podataka prije nekog vremena.

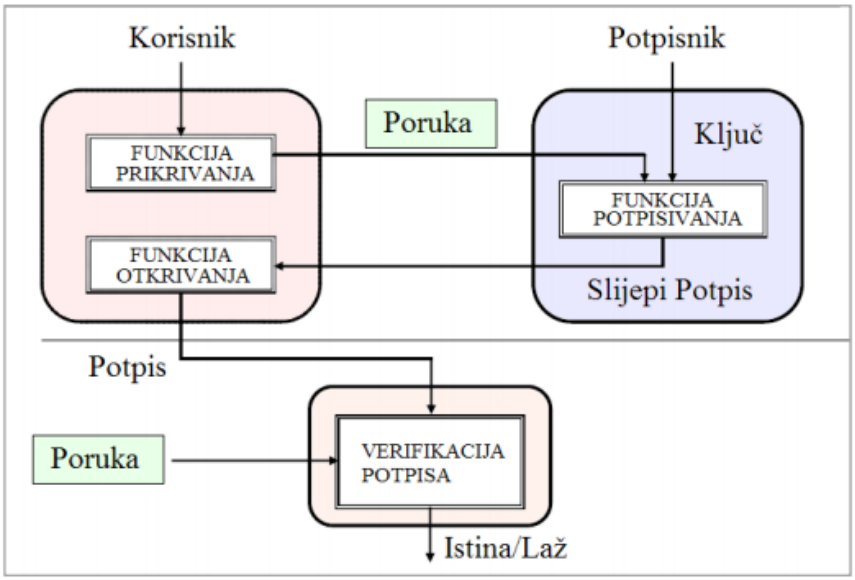
Kao najveću prednost korištenja digitalnog potpisa, uz autentičnost i integritet, jest onemogućavanje nepriznavanja dokumenta od strane osobe koja ga je potpisala. Potpisanu poruku potpisnik ne može zanijekati jer je ona potpisana privatnim ključem koji je dostupan samo njemu (jedino u slučaju otkrivanja potpisnikova privatnog ključa), a preporuča se taj ključ čuvati i držati u strogoj tajnosti npr. na pametnoj kartici ili osobnom računalu.

5.2. Slijepi potpis

Kod slijepog potpisa (engl. *blind signature*) sadržaj poruke koja se potpisuje skriven je od potpisnika. Vjerodostojnost originalne tj. otkrivene poruke može se provjeriti jednako kao i kod običnog digitalnog potpisa.

Najčešća primjena slijepog potpisa je u situacijama kada autor i potpisnik poruke nisu ista osoba (npr. elektronični platežni sustavi, kriptografski sustavi za glasovanje) ili kada je nužna anonimnost pojedinih sudionika.

Kriptosustav slijepog potpisa sastoji se od tri osnovne funkcije: funkcija prekrivanja, funkcija potpisivanja i funkcija otkrivanja. (Slika 4.)



Slika 4. Protokol slijepog potpisa

Osnovna svojstva slijepog potpisa su:

- Svojstvo digitalnog potpisa – potpis ima svojstva autentičnosti, integriteta i neporecivosti, a pomoću tajnog ključa potpisnika svatko može provjeriti da je potpis nastao kao rezultat slijepog potpisa
- Svojstvo slijepog potpisa – prikrivenu poruku koju je potpisnik dobio na potpis ne može povezati sa konačnom potpisanom porukom nastalom nakon funkcije otkrivanja (svojstvo nepovezivosti)
- Zaštita potpisa – primatelj potpisa može najviše dobiti jednu potpisanu poruku iz potpisane prikrivene poruke koju dobiva od potpisnika

5.3. Digitalni potpis u internetskim aplikacijama

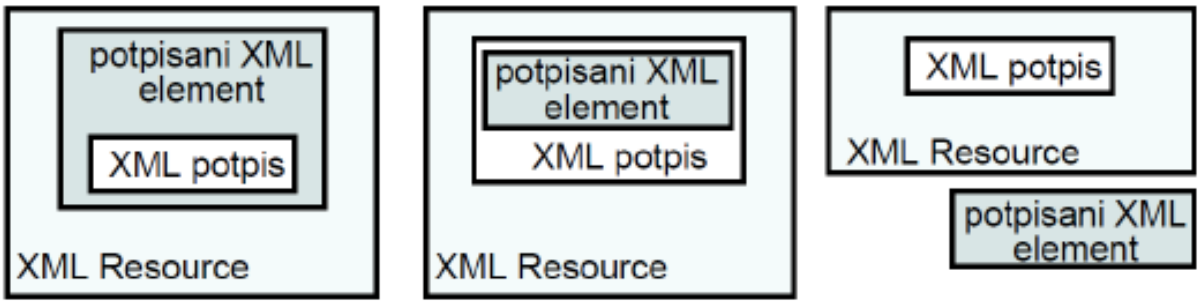
XML digitalnim potpisom je moguće potpisati razne sadržaje internetskih stranica. Takva vrsta potpisa regulirana je *W3C XML Signature* standardom, na području web tehnologija međunarodne organizacije *World Wide Web Consortium*. XML potpis koristi se za potpisivanje podataka kao što su:

- XML elementi, skupovi XML čvorova
- URI oznake
- Binarne datoteke
- Binarni podaci ugrađeni u XML dokument

Na određenoj internetskoj stranici može se potpisati njen bilo koji dostupan element. Najčešće se digitalno potpisuju dijelovi XML i HTML koda, različite vrste formulara kao i njihovi sadržaji.

Postoje tri vrste XML potpisa (Slika 5.):

1. Omotani (engl. *enveloped*) – potpis se nalazi unutar podataka koje potpisuje
2. Omotavajući (engl. *enveloping*) – potpisani podaci se nalaze unutar potpisa
3. Odvojeni (engl. *detached*) – potpis i potpisani podaci su međusobno razdvojeni



Slika 5. XML potpisi

5.4. Digitalni potpis multimedijskih sadržaja

Zaštita multimedijskih sadržaja moguća je korištenjem vodenog žiga (engl. *watermark*) ili digitalnim potpisivanjem.

Vodeni žig predstavlja skup informacija pohranjenih u neki signal (npr. slika, zvuk, video). Koristi se kao zaštita autorskih prava ili dodavanje određenih informacija kao što su naziv autora, godina izdanja itd. On može biti vidljiv ili sakriven krajnjem korisniku. Dodana informacija vodenim žigom ne smije značajno promijeniti originalni signal. Vidljivi žig se upotrebljava kako bi se ograničila upotreba sadržaja na koji je stavljen (Slika 6.), dok se skriveni žig koristi za utvrđivanje porijekla sadržaja (Slika 7.) Skriveni vodeni žig zahtjeva algoritamsku detekciju jer nije moguće vizualno razlikovati original i označenu sliku.

Slika 6. Vidljivi vodeni žig

Slika 7. Skriveni vodeni žig

Uz vodeni žig često se koristi digitalni potpis kao alternativa zaštite multimedijskih sadržaja. To je prikladniji način zaštite zbog krhkosti vodenih žigova tokom sažimanja sadržaja. Multimedijski sadržaji se često prenose sažimani, a veliki broj standarda za sažimanje podataka omogućuju umetanje digitalnog potpisa u poseban odjeljak unutar sažete datoteke. U slučaju da se koristi neki standard koji nema takav prostor, sadržaj je moguće potpisati u zasebnoj datoteci i poslati ju zajedno sa sadržajem koji se potpisuje. Potpisivanje multimedijskih sadržaja i ostalih dokumenata se ne razlikuje mnogo. Kod tekstualnih dokumenata ili dijelova koda se potpisuje niz bitova tako da se može odmah primijetiti promjena kod jednog znaka tijekom provjere vjerodostojnosti, dok se multimedijski sadržaji potpisuju tako da se zaštiti njihov sadržaj (vizualne i zvučne informacije). Takve informacije se ne gube sažimanjem, pa se ne gubi niti vjerodostojnost.

6. Digitalni potpis u praksi - aplikacija Web e-Potpis

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

6.1. Digitalni certifikati

Fina[2] 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 certifikata:

- Certifikati za elektronički potpis – koriste se za izradu potpisa. Usko su povezani s potpisnikom i omogućuju njegovu identifikaciju.
- Certifikati za autentikaciju – koriste se za izradu potpisa, jaku autentikaciju, enkripciju ključa.

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

6.2. 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 Fininim certifikatom.

Kako bi koristili aplikaciju Web e-Potpis treba imati:

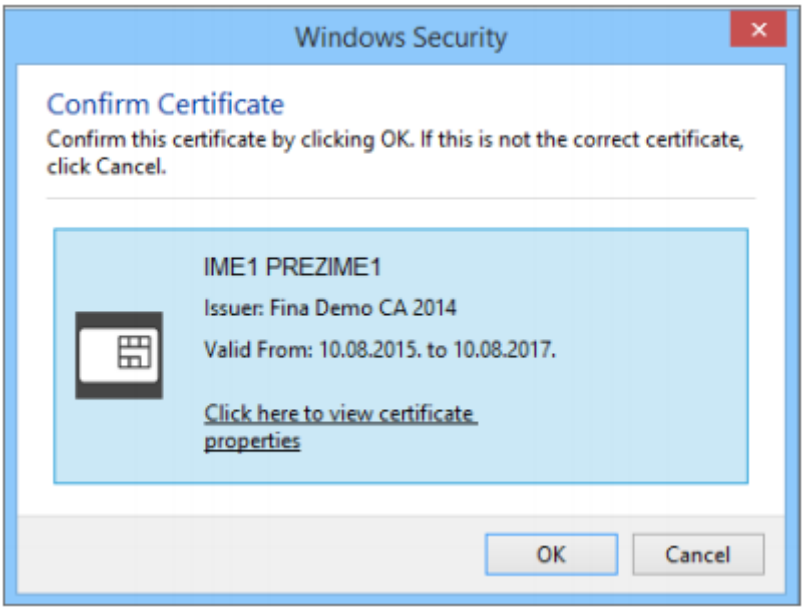
- Osobno računalo
- Operacijski sustav Windows 7 ili noviji
- Internetski pristup

[2] Financijska agencija

- Internetski preglednik Internet Explorer 10.0 ili noviji
- Java 8 ili novija verzija
- Digitalni certifikat koji je izdan na Fininoj pametnoj kartici ili USB tokenu
- Program za upravljanje pametnim karticama tj. tokenima
- Čitač pametnih kartica tj. tokena
- Najnovija verzija Adobe Reader-a

6.2.1. Prijava u aplikaciju

Unosom adrese https://webservisi.fina.hr/Web_e-Potpis u internetski preglednik ostvaruje se pristup aplikaciji. Pristupom stranici se otvara pop-up prozor za odabir certifikata (Slika 8.). U slučaju da se pop-up prozor ne pojavljuje, treba provjeriti je li kartica umetnuta u čitač ili USB token u računalo, uz ispunjene ostale tehničke preduvjete za aplikaciju Web e-Potpis.

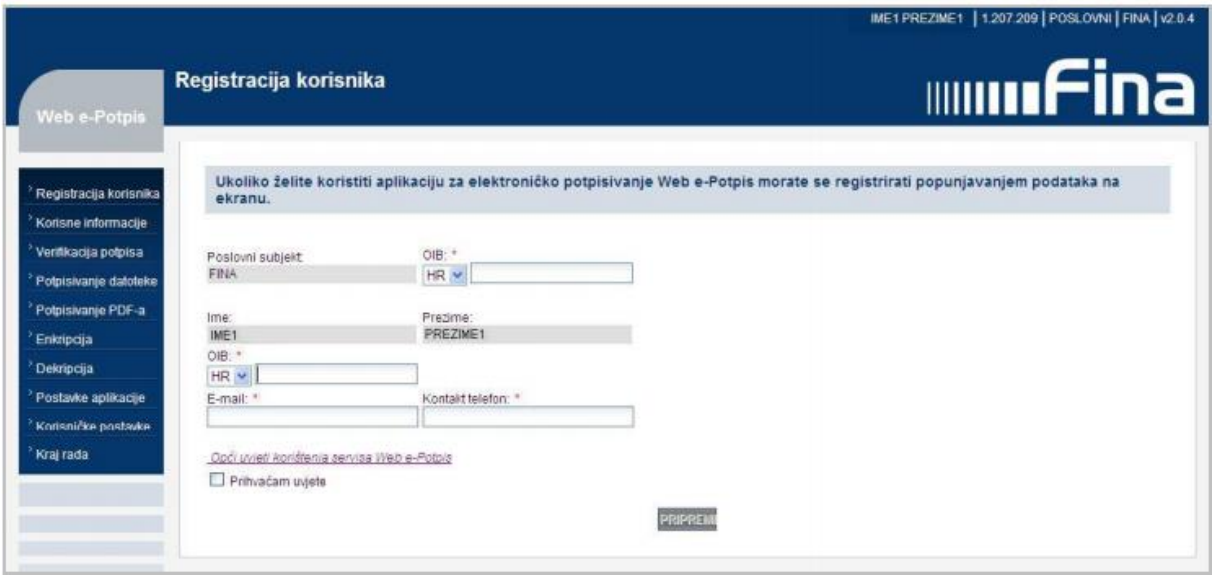


Slika 8. Odabir certifikata u internetskom pregledniku – pop up prozor

U pop-up prozoru nalaze se svi ponuđeni certifikati kojima se korisnik služio na računalu. Potrebno je izabirati odgovarajući certifikat za autentikaciju, a nakon toga se otvara prozor za unos PIN-a kako bi mogli koristiti odabrani certifikat. Zatim se otvara početni ekran aplikacije prije registracije, što je znak da smo se uspješno prijavili u aplikaciju.

6.2.2. Registracija korisnika

Nakon što smo se uspješno prijavili u aplikaciju, treba se registrirati tj. popuniti polja za unos obaveznih podataka i prihvatiti Opće uvjete korištenja aplikacije Web e-Potpis (Slika 9.).



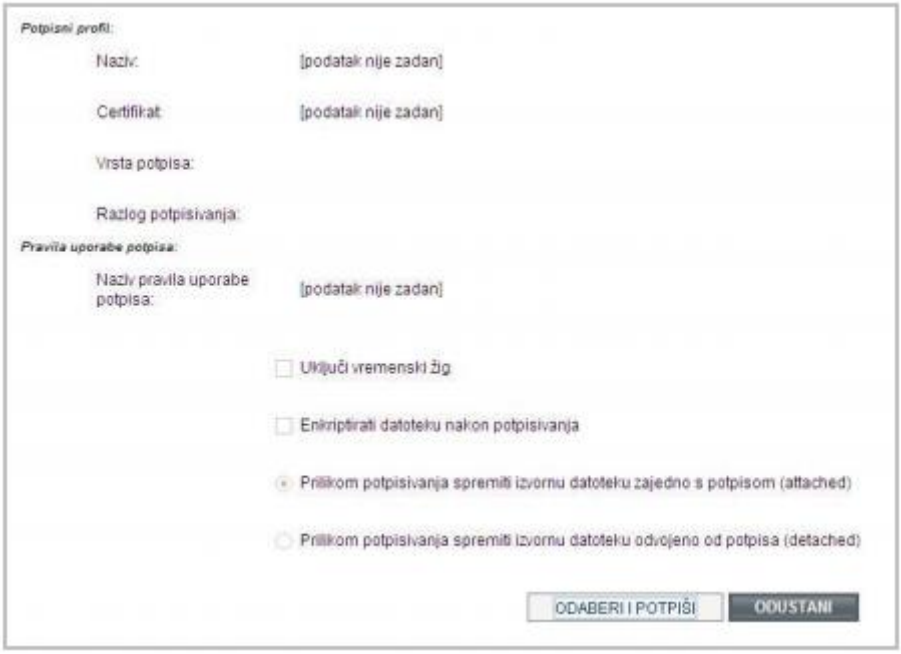
Slika 9. Upisivanje podataka pri registraciji

Kada smo unijeli podatke za registraciju otvara se ekran gdje trebamo odabrati biblioteku implementacije za potpisivanje registracije. Ona se odabire jedino prilikom prvog potpisivanja. Preporučuje se da prilikom korištenja aplikacije korisnik nema uključena dva uređaja istovremeno. Nakon ispravno odabrane implementacijske datoteke dolazi obavijest o uspješnoj registraciji i potvrda na navedeni e-mail u kojem piše:

„Poštovani,
veliko nam je zadovoljstvo što ste postali korisnik servisa Web e-Potpis.
Servisu možete pristupiti na www.fina.hr.
Putem FINA e-kartice moguće je pristupiti i drugim e-servisima Fine, državne uprave i javnih službi.
Za više informacija o e-servisima Fine posjetite www.fina.hr, pošaljite upit na adresu e-pošte info@fina.hr
ili nazovite besplatni broj telefona 0800 0080.
Zahvaljujemo Vam na suradnji i želimo Vam uspješno poslovanje.
S poštovanjem,
Vaša Fina“

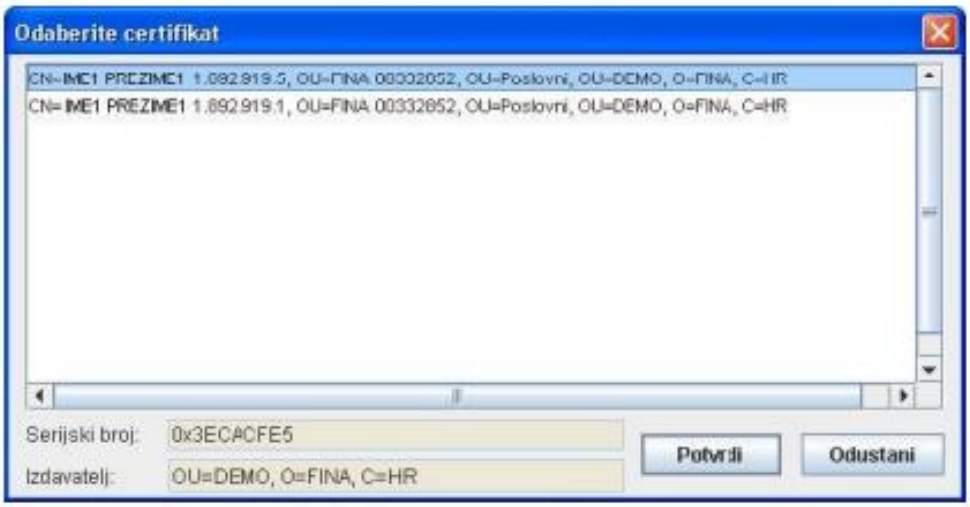
6.2.3. Potpisivanje datoteke

Odabirom opcije *Potpisivanje datoteke* se otvara početni ekran (Slika 10.).



Slika 10. Početni ekran za potpisivanje datoteke

Nakon klika na *Odaberi i potpiši* dobivamo ekran za odabir datoteke koju želimo potpisati (Slika 11.), a kad ju odaberemo, unosimo PIN za pristup pametnoj kartici ili USB tokenu. Zatim biramo certifikat kojim želimo potpisati datoteku.

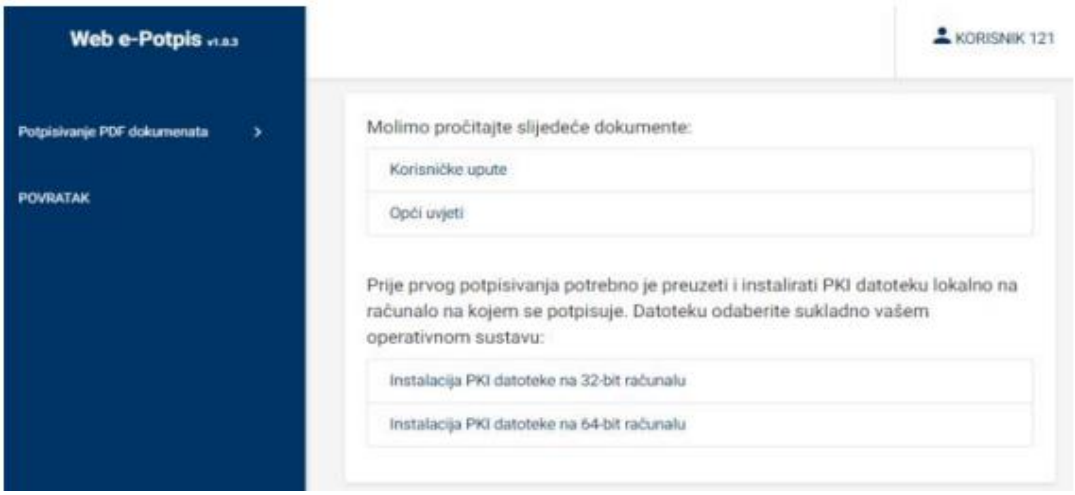


Slika 11. Odabir certifikata

Dokument spremamo u attached formatu (izvorna datoteka zajedno s potpisom) *.p7m

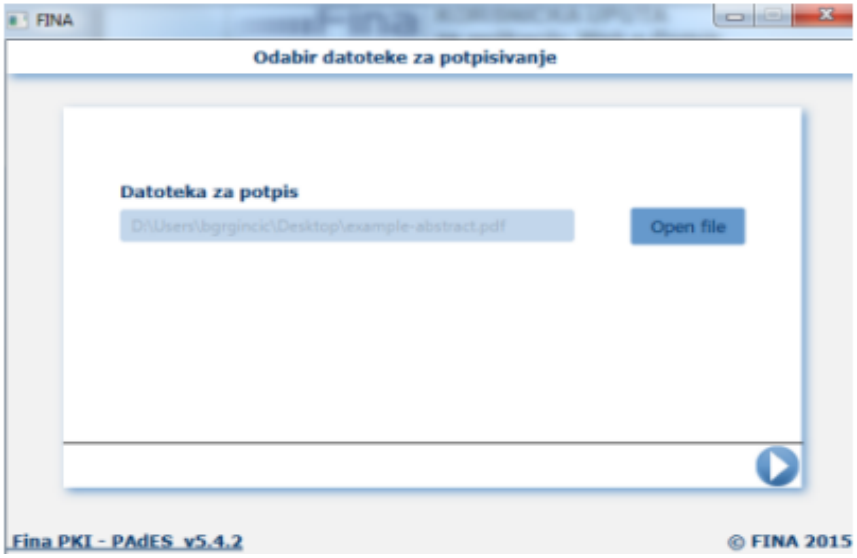
6.2.4. Potpisivanje PDF-a

Kod odabira opcije *Potpisivanje PDF-a* se otvara novi segment aplikacije (Slika 12.), a prije prvog potpisivanja potrebno je preuzeti i instalirati PKI datoteku na računalo na kojem se potpisuje.



Slika 12. Novi segment aplikacije za potpisivanje PDF-a

Za potpisivanje PDF-a, u padajućem izborniku biramo stavku *Potpisivanje PDF dokumenata –> Potpis.* Zatim se otvara početni ekran za potpisivanje, no prije procesa potpisivanja potrebno je pokrenuti PKI modul koji smo prethodno instalirali. Prilikom pokretanja modula, odabiremo datoteku koju želimo potpisati i odabir certifikata (Slika 13.).



Slika 13. PKI modul – odabir datoteke koju želimo potpisati

Kako bi uspješno završili potpisivanje unosimo PIN i definiramo lokaciju na kojoj pohranjujemo potpisanu datoteku.

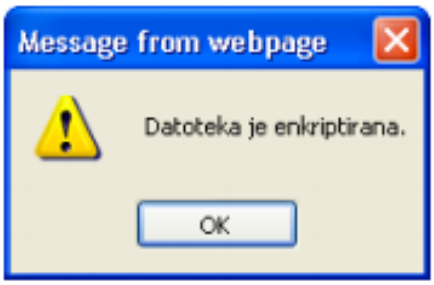
6.2.5. Enkripcija

Odabirom opcije *Enkripcija* otvara se početni ekran (Slika 14.).

Slika 14. Početni ekran enkripcije

Klikom na gumb *Enkriptiraj* dolazimo do ekrana za odabir datoteke za enkripciju. Nakon odabira datoteke, biramo mjesto gdje želimo spremiti tu enkriptiranu datoteku s ekstenzijom *.enc.

Zatim se otvara ekran za odabir certifikata tj. primateljevog javnog ključa i nakon toga dobivamo obavijest o uspješnoj enkripciji (Slika 15.).



Slika 15. Obavijest o uspješnoj enkripciji.

6.2.6. Dekripcija

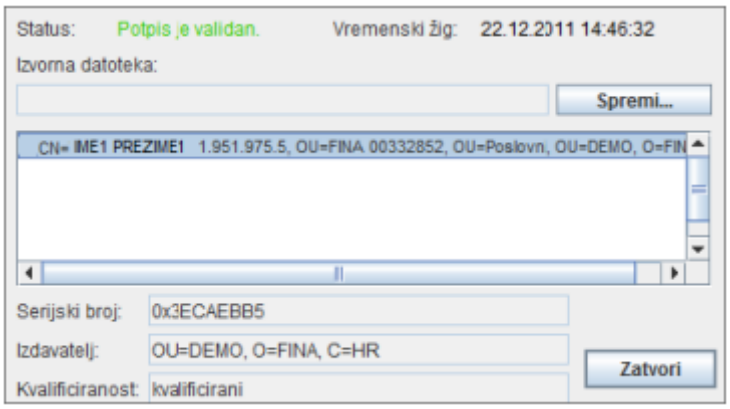
Postupak dekripcije je gotovo identičan enkripciji. Razlika je u tome što aplikacija automatski briše ekstenziju *.enc.

6.2.6. Verifikacija potpisa

Odabirom opcije *Verificiraj potpis* otvara se početni ekran u kojem biramo potpisanu datoteku (Slika 16.).

Slika 16. Početni ekran za verificiranje potpisa

Zatim se otvara prozor u kojem biramo oblik pohrane potpisa – objedinjen (attached format *.p7m) ili odvojen (detached format *.p7s). Nakon odabira dokumenta u odgovarajućem formatu dolazimo do ekrana koji nam daje informaciju o validnosti potpisa (Slika 17). U slučaju da je bila uključena oznaka vremenskog žiga prilikom potpisivanja, u desnom kutu bi bio prikazan točan datum i vrijeme potpisivanja dokumenta. U slučaju da je certifikat istekao ili je opozvan, onda potpis nije validan.



Slika 17. Status potpisa sa vremenskim žigom

7. Zakonska regulativa

Hrvatski Sabor je proglasio 17. siječnja 2002. godine Zakon o elektroničkom potpisu koji predstavlja temeljni zakonski akt u Republici Hrvatskoj.

Zakonom se 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.“[3]

U Zakonu se navodi da se može odbiti prihvaćanje potpisanog dokumenta koji je stvoren i izdan u elektroničkom obliku u slučajevima: pravnih poslova kojima se vrši prijenos vlasništva na nekretninama ili se uspostavljaju druga stvarna prava na nekretninama, oporučnih poslova, imovinskih predbračnih, odnosno bračnih ugovora, opterećenja i otuđenja imovine za koje je potrebno odobrenje centra za socijalnu skrb, ugovora o predaji i raspolaganju s imovinom za života, ugovora o doživotnom uzdržavanju i sporazume u svezi s nasljeđivanjem, darovnih ugovora, drugih pravnih poslova za koje je posebnim zakonom propisano da se sastavljaju u obliku javnobilježničkog akta, odnosno isprave, drugih pravnih poslova ili radnji za koje je posebnim zakonom ili na temelju zakona donesenim propisom izričito određena uporaba vlastoručnog potpisa u dokumentima na papiru ili ovjera vlastoručnog potpisa.[4]

Davatelj usluga izdavanja kvalificiranih certifikata dužan je osigurati rizik od odgovornosti za štetu koja nastaje obavljanjem usluga certificiranja (obvezno osiguranje) [5].

Davatelj usluga izdavanja kvalificiranih certifikata obavlja usluge na temelju dozvole koju izdaje Ministarstvo, na zahtjev davatelja usluge.[6]

Usluge certificiranja u Republici Hrvatskoj mogu obavljati samo registrirani, odnosno evidentirani davatelji usluga certificiranja.[7]

[3] Zakon o elektroničnom potpisu, čl. 1. (ZEP)
[4] ZEP, čl. 6.
[5] ZEP, čl. 11
[6] ZEP, čl. 18.
[7] ZEP, čl. 21.

Propisane su i novčane kazne za fizičku osobu koja neovlašteno pristupi i upotrijebi podatke i sredstva za izradu elektroničkog potpisa (2 000,00 kn – 10 000,00 kn), te za davatelja usluga certificiranja koji izdaje certifikat koji ne sadrži sve potrebne podatke, ne provodi odgovarajuće zaštitne mjere, ne vodi evidenciju certifikata i dr. (5 000,00 kn – 100 000,00 kn).[8]

Zakon je stupio na snagu osmog dana od objave u „Narodnim novinama“, a primjenio se od 1. travnja 2002. godine.[9]

Uz Zakon o elektroničkom potpisu možemo spomenutu još neke zakone koji omogućuju primjenu internetskog poslovanja: Zakon o tajnosti podataka (NN 79/2007), Zakon o institucijama za elektronički novac, Zakon o pravu na pristup informacijama (NN 172/03), Zakon o zaštiti potrošača (NN 79/2007, 125/2007), Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12) i drugi.

[8] ZEP, čl. 39, čl. 41.
[9] ZEP, čl. 45

8. Zaključak

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 i sl.

Mnogi poduzetnici više preferiraju osobnu komunikaciju, slabo se educiraju i nemaju povjerenje u tehnologiju digitalnog potpisa, a tu su također i veći troškovi zbog implementacije (certifikati, baza podataka, programska podrška). Unatoč tome, smatra se da će digitalni potpis postati u budućnosti prevladavajući način utvrđivanja autentičnosti dokumenta.

Digitalni potpisi se sve više približavaju klasičnim rukom pisanim potpisima i pitanje je vremena kada će se prestati koristiti. Sve češćom upotrebom digitalnog potpisa rasti će i učestalost pokušaja napada i zlouporabe potpisa. Zato je veoma važno razvijati sigurnosne mehanizme i algoritme kojima se to može spriječiti.

9. Literatura i izvori

- CARNet CERT, LS&S, *Digitalni potpis* https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf, kolovoz 2018.

- Mario Zovkić, Tedo Vrbanec, Učiteljski fakultet Sveučilišta u Zagrebu, *Digitalni potpis* https://bib.irb.hr/datoteka/481946.Zovkic-Vrbanec_-_Digitalni_potpis.pdf, Kolovoz 2018.

- Bernadin Ibrahimpašić, Edin Liđan, Osječki matematički list (2010) 139-148, *Digitalni potpis*

- Marijana Zelanto, Sveučilište u Zagrebu, Diplomski rad (2008), *Slijepi potpis*

- Službena stranica Fine https://www.fina.hr/default.aspx?sec=960, Kolovoz 2018.

- Zakon o elektroničkom potpisu (2002) https://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html, Kolovoz 2018.

10. Popis slika i tablica

Slika 1. Shematski prikaz postupka stvaranja i provjere digitalnog potpisa 8
Slika 2. Cezarova šifra – supstitucija 9
Slika 3. Shematski prikaz stvaranja digitalnog certifikata 10
Slika 4. Protokol slijepog potpisa 14
Slika 5. XML potpisi 15
Slika 6. Vidljivi vodeni žig 16
Slika 7. Skriveni vodeni žig 16
Slika 8. Odabir certifikata u internetskom pregledniku – pop up prozor 18
Slika 9. Upisivanje podataka pri registraciji 19
Slika 10. Početni ekran za potpisivanje datoteke 20
Slika 11. Odabir certifikata 20
Slika 12. Novi segment aplikacije za potpisivanje PDF-a 21
Slika 13. PKI modul – odabir datoteke koju želimo potpisati 21
Slika 14. Početni ekran enkripcije 22
Slika 15. Obavijest o uspješnoj enkripciji 22
Slika 16. Početni ekran za verificiranje potpisa 23
Slika 17. Status potpisa sa vremenskim žigom 23

Tablica 1. Usporedba duljine ključeva u prošlosti i budućnosti 12