Zaštita i sigurnost informacijskih sustava

Sigurnost u sustavima za elektroničko poslovanje

prof. dr. sc. Boris Vrdoljak
dr. sc. Luka Humski

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.

Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

Elektroničko poslovanje

Primjeri elektroničkog poslovanja

- elektroničko komuniciranje s drugim poduzećima radi narudžbe proizvoda i usluga te njihovo elektroničko plaćanje
  - poslovanje medu tvrtkama – B2B (Business-to-Business)

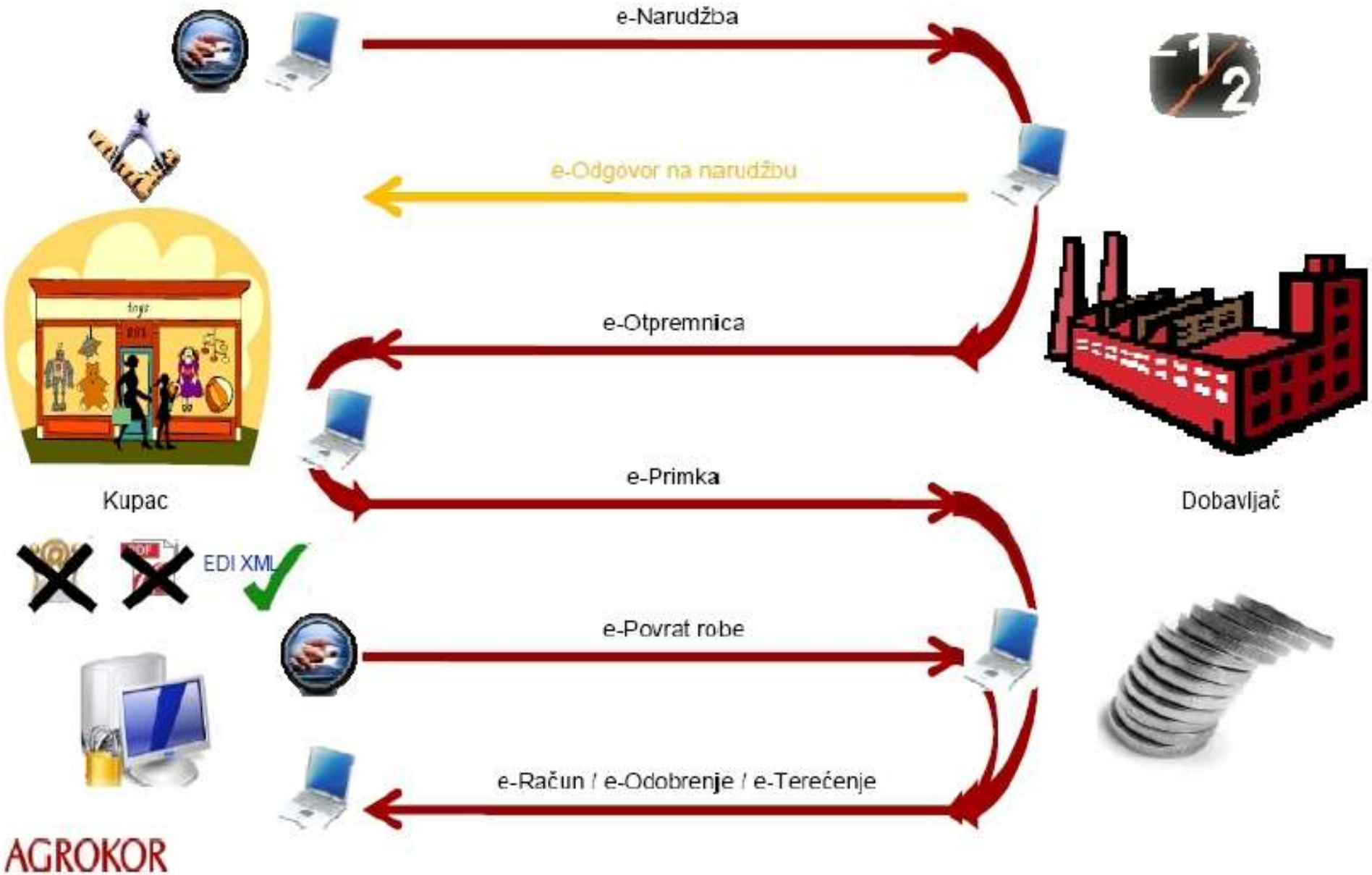
- prodavanje proizvoda i usluga preko Web sjedišta
  - e-trgovina, poslovanje tvrtke s krajnjim potrošačem – B2C (Business-to-Consumer)

Elektroničko poslovanje B2B - razmjena poslovnih dokumenata

Osnovni poslovni procesi u dobavnom lancu i elektronički dokumenti koji se razmjenjuju:

- Katalog *e-katalog*
- Naručivanje *e-narudžbenica*
- Otpremanje *e-otpremnica*
- Primanje *e-primka*
- Fakturiranje *e-račun*
- Plaćanje e-nalog za plaćanje

Primjer razmjene e-dokumenata



Dobavni lanac – osnovni poslovni procesi i dokumenti

- Suvremeni elektronički dokumenti koji se razmjenjuju u elektroničkom poslovanju većinom su **u formatu XML**.

- Postoje i starije norme **EDI** (*Electronic Data Interchange*), od kojih je najvažnija norma **EDIFACT** (*Electronic Data Interchange For Administration, Commerce and Transport).*

- razmjena suvremenih poslovnih elektroničkih dokumenata – tehnologije: XML i usluge Weba
- SIGURNOST?

Sigurnost elektroničkog poslovanja

- B2B - razmjena XML dokumenata i korištenje Web usluga
- Osiguravanje autentičnosti (deklarirani pošiljatelj je stvarni pošiljatelj) i integriteta (nemogućnost izmjene poruke)
  - E-potpis
- Kad istekne digitalni certifikat, kako dokazati da je u doba potpisivanja dokumenta certifikat vrijedio?
  - Vremenska ovjera, vremenski žig (*timestamp*)
- Potpisivanje i šifriranje u formatu XML
  - XML Signature i XML Encryption
- Sigurnost Web usluga
  - Web Services Security (WSS) i druge norme (WS-Extensions)
  - WS-I Basic Security Profile
  - Sigurnost RESTful Web usluga

Sigurnost pri razmjeni elektroničkih dokumenata

- **e-račun** je najrašireniji elektronički poslovni dokument

- sve zemlje članice EU trebaju omogućiti primanje **e-Računa** za porezne svrhe (PDV) ako su ispunjena dva uvjeta:

  1) **primatelj se mora složiti** s primanjem računa u elektroničkom formatu;

  2) **integritet** (nemogućnost izmjene) **i autentičnost** (deklarirani pošiljatelj je stvarni pošiljatelj) moraju biti osigurani pri prijenosu i arhiviranju.

Ovaj drugi zahtjev može se ispuniti bilo **naprednim elektroničkim potpisom** ili kroz elektroničku razmjenu podataka (EDI) s ugovorenim sigurnosnim mjerama.

Elektronički (digitalni) potpis

- U poslovnom i ICT-svijetu često susrećemo pojam digitalni potpis, elektronički potpis, e-potpis ili engleski naziv *e-signature*.
- Hrvatski enciklopedijski rječnik kaže da je digitalni potpis „*šifriranje kojim se dokazuje autorstvo, tj. izvornost elektroničkog dokumenta*”.
- Elektronički potpis je uredbom eIDAS (koju je donijela EU) definiran na sljedeći način: *„podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje“.*

- U sklopu ovog predmeta:
  - pojmove elektronički potpis i digitalni potpis koristit ćemo kao sinonime,
  - pojam elektronički potpis neće uključivati i sliku ručnog potpisa (iako se i ona u širem smislu može smatrati vrstom elektroničkog potpisa).

Asimetrična kriptografija

Za digitalno potpisivanje koristi se **asimetrična kriptografija**.

- jedan algoritam i **par ključeva**: jedan ključ za šifriranje, drugi za dešifriranje

- Šifriranje: transformira se **otvoreni tekst** (*plaintext*) koristeći unaprijed dogovoreni ključ
- Rezultat šifriranja naziva se **šifrat** (*ciphertext*) ili **kriptogram**
- matematički algoritam određuje kako se šifrira otvoreni tekst
- složenost ovisi o duljini ključa (broj bitova)
- snaga sustava za šifriranje počiva na ključu
  - napadač može imati šifrirane tekstove i znati algoritme, ranjivost sustava ovisi o snazi ključa
  - dulje ključeve teže je probiti (vrijeme, novac)
  - duljina ključa: 128, 192 ili 256 bita

Asimetrična kriptografija

- u asimetričnoj kriptografiji ključevi su međusobno vezani
- neizvedivo je poznavajući algoritam i jedan ključ otkriti drugi
- često: svejedno je kojim ključem se šifrira, a kojim dešifrira
  - rade isključivo u paru

- **jedan od dva** ključa mora ostati tajan

Svaki korisnik ima par ključeva:

- **privatni** (tajni) ključ
  - Dostupan isključivo korisniku, ne smije se distribuirati
- **javni** ključ
  - Dostupan svima, mora se distribuirati

Asimetrična kriptografija

- ono što se šifrira javnim ključem, može se dešifrirati samo privatnim
- ono što se šifrira privatnim ključem, može se dešifrirati samo javnim

- poznavanjem javnog ključa ne može se izračunati tajni ključ u nekom razumnom vremenu
- vrijeme potrebno za izračunavanje tajnog ključa iz poznatog javnog ključa, tj. razbijanje šifre, mjeri se milijunima godina na danas najjačim raspoloživim računalima

- Asimetrična kriptografija naziva se i **kriptografijom javnog ključa.**

Algoritmi za asimetričnu kriptografiju

- **RSA** (Rivest-Shamir-Adleman) - MIT
  - najpopularniji algoritam, razvijen 1977.
- Diffie-Hellman
  - razvijen 1976.
- Eliptic Curves Cryptosystem (ECC)
- ostali:

  ElGamal, Rabin, Knapsack, McEliece, NTRU, Braid Groups, Lucas

Hash funkcija i digitalno potpisivanje

- prije **digitalnog potpisivanja** treba **generirati sažetak** (hash, digest) poruke
- hash funkcija
  - ulaz: niz znakova proizvoljne duljine
  - izlaz: niz znakova fiksne duljine (npr. 256 bita)
- osnovna svojstva hash funkcije:
  - *hash* je jednosmjerna funkcija
    - nije moguće na osnovu izlaza regenerirati ulaznu poruku
    - nije moguće odrediti ulaznu poruku koja bi imala zadani hash
  - „primjena” i „promjena” će dati potpuno drugačiji sažetak (*hash)*
  - promjenom jednog bita ulaza dobiva se potpuno drugačiji izlaz

Hash-algoritmi

- Secure Hash Algorithm (SHA-1) – ne preporučuje se koristiti
  - algoritam američke vlade (NSA)
  - daje *hash* vrijednost duljine 160 bita iz niza znakova bilo koje duljine
  - **kolizija** otkrivena u 2^{69} hasheva, 2005. godine

- **SHA-2** (varijante SHA2-224, SHA2-256, SHA2-384, SHA2-512)

- **SHA-3** (varijante SHA3-224, SHA3-256, SHA3-384, SHA3-512)

- Message Digest Algorithm 5 (MD5) – ne preporučuje se koristiti
  - daje *hash* duljine 128 bita
  - MD5 probijen 2008. godine

Postupak digitalnog potpisivanja

izračuna se
sažetak *(hash)* poruke

sažetak poruke potpiše
se **vlastitim**
privatnim ključem

na izvornu poruku
se doda potpisani sažetak i
sve se šalje primatelju
kao tekst

iz poruke se vadi
šifrirani sažetak

sažetak se dešifrira
javnim ključem
pošiljatelja

iz izvorne poruke
se računa novi sažetak

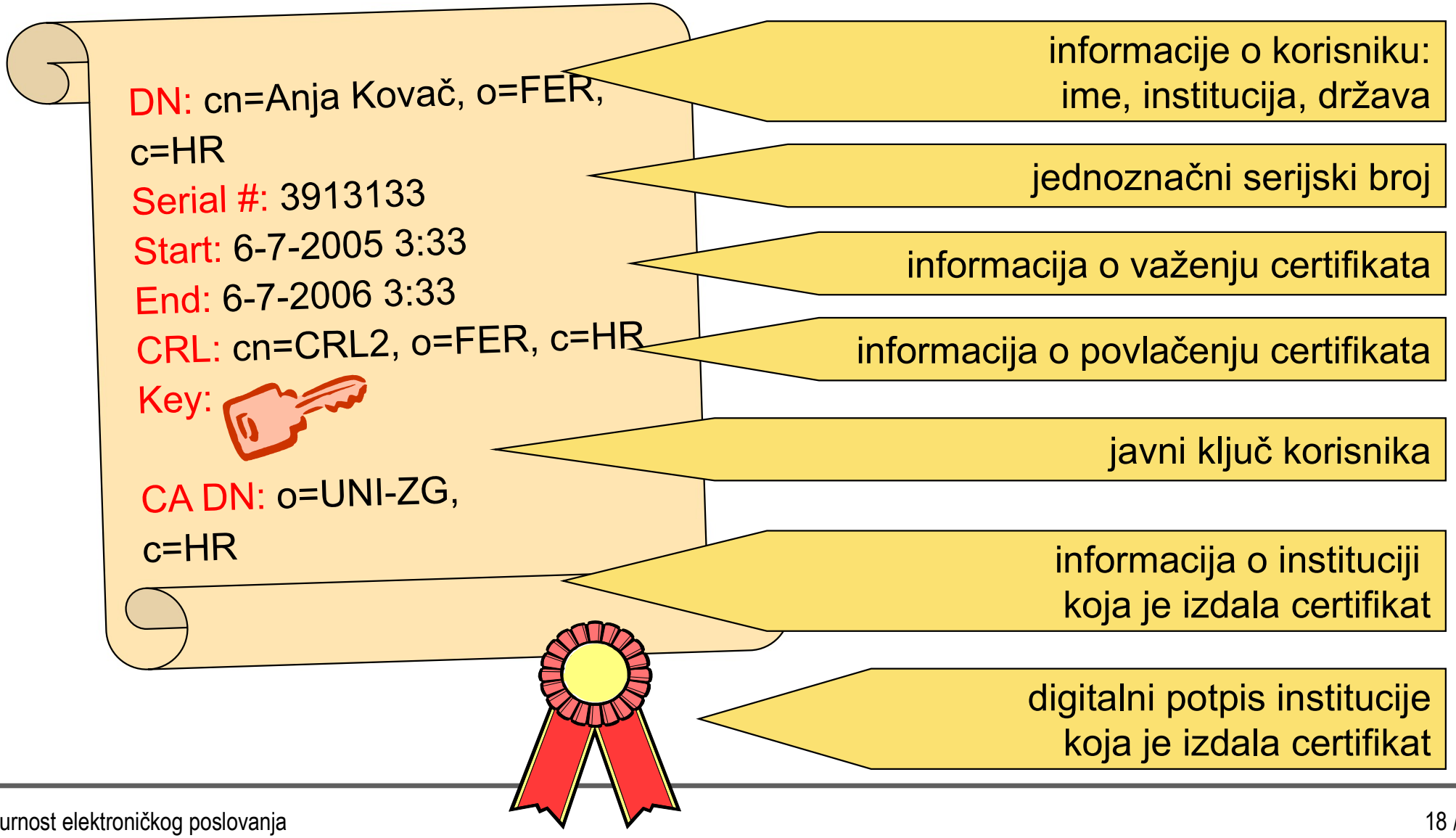
ako su sažetci jednaki,
dokazan je identitet pošiljatelja
i integritet sadržaja

Digitalni certifikat

- Rješava problem dokazivanja identiteta
- Povezuje identitet korisnika s njegovim javnim ključem - **potvrđuje da je određeni korisnik vlasnik određenog javnog ključa**
- Skup podataka koji identificira korisnika i davatelja usluge certificiranja

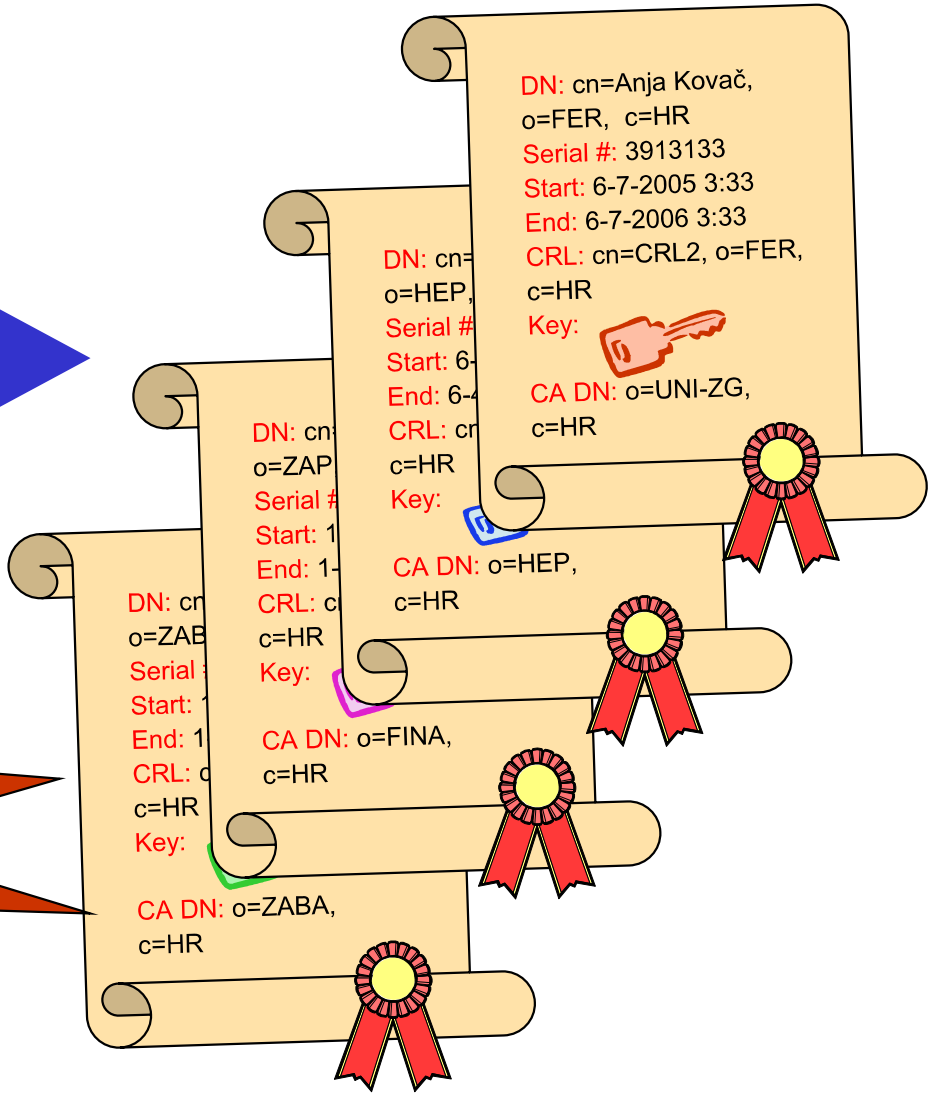
- Norma:
  - za digitalne certifikate koristi se norma **X.509**
  - imena su u certifikatima prikazana kao parovi: ime – vrijednost

Sadržaj certifikata



Izdavanje certifikata

Certifikacijsko tijelo (CA – *Certificate Authority*)



Certifikacijsko tijelo
(davatelj usluga certificiranja)

Digitalni certifikat

- Ako pošiljatelj potpiše poruku svojim privatnim ključem, primatelj može **znati da se radi upravo o tom pošiljatelju**:
  - ako može **dešifrirati** digitalni potpis **javnim ključem pošiljatelja i**
  - ako **digitalni certifikat potvrđuje** da je korišteni javni ključ upravo **javni ključ tog pošiljatelja**.
  - ako digitalni certifikat **nije istekao ili opozvan**

- Pretpostavka za ovaj postupak je da korisnici imaju **povjerenje u certifikacijsko tijelo** (tj. davatelja usluga certificiranja) koje je izdalo certifikat i potpisalo ga svojim privatnim ključem ili u certifikacijsko tijelo koje je certificiralo certifikacijsko tijelo koje je izdalo certifikat.

Infrastruktura javnog ključa

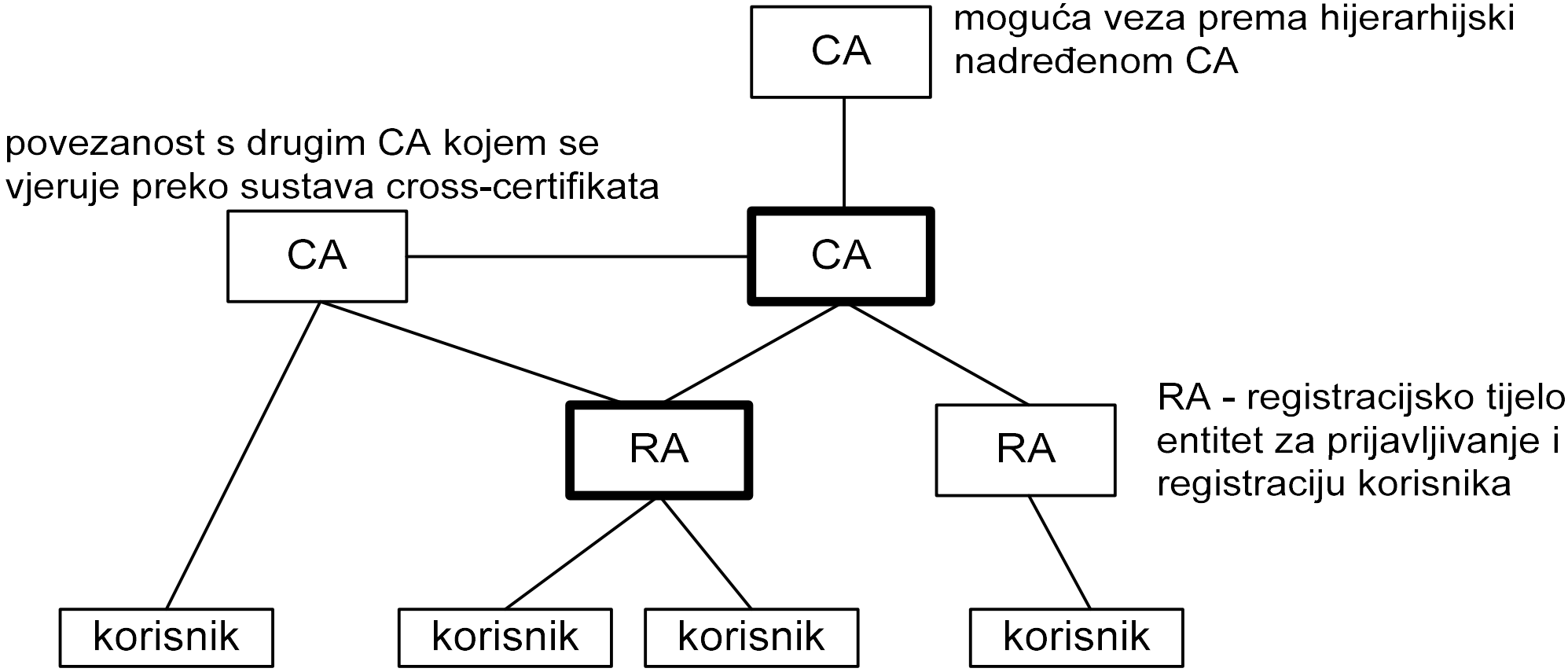
- **PKI - Public Key Infrastructure**
  - skup sklopovlja, programske podrške, ljudi, politika i procedura potrebnih za stvaranje, upravljanje, izdavanje, korištenje, pohranjivanje i opozivanje digitalnih certifikata
  - osnova za stvaranje sigurne i povjerljive razmjene podataka između sudionika u sustavu
  - osigurava:
    - cjelovitost elektroničke komunikacije onemogućavajući izmjene podataka tijekom njihovog prenošenja mrežom
    - potvrđivanje identiteta strana koje sudjeluju u komunikaciji
    - neporecivost sudjelovanja bilo koje strane u komunikaciji

Dijelovi PKI

- **certifikacijsko tijelo** (**CA** – *Certificate Authority*)
  - obavlja izdavanje i povlačenje certifikata, održavanje informacija o stanju certifikata, objava važećih certifikata...
- **registracijsko tijelo** (**RA** – *Registration Authority*)
  - obavlja registraciju korisnika (provjerava sadržaj certifikata za CA, obavlja identifikaciju i autentifikaciju strana koje se prijavljuju za dobivanje certifikata)
- **repozitorij**
  - sadrži bazu izdanih certifikata i bazu opozvanih certifikata (CRL – engl. *Certification Revocation List*)
- **klijenti (aplikacije)**
  - provjeravaju digitalne potpise i certifikate kod CA
- **korisnici sustava PKI**
  - vlasnici certifikata
- **centar za pouzdano vremensko označavanje** (**TSA** – engl. *Timestamp Authority*)
  - stvara vremenske žigove

Odnos RA i CA

- jedan CA može imati više RA za različite skupine korisnika
- jedan RA može biti povezan s više CA



Hijerarhija certifikacijskih tijela

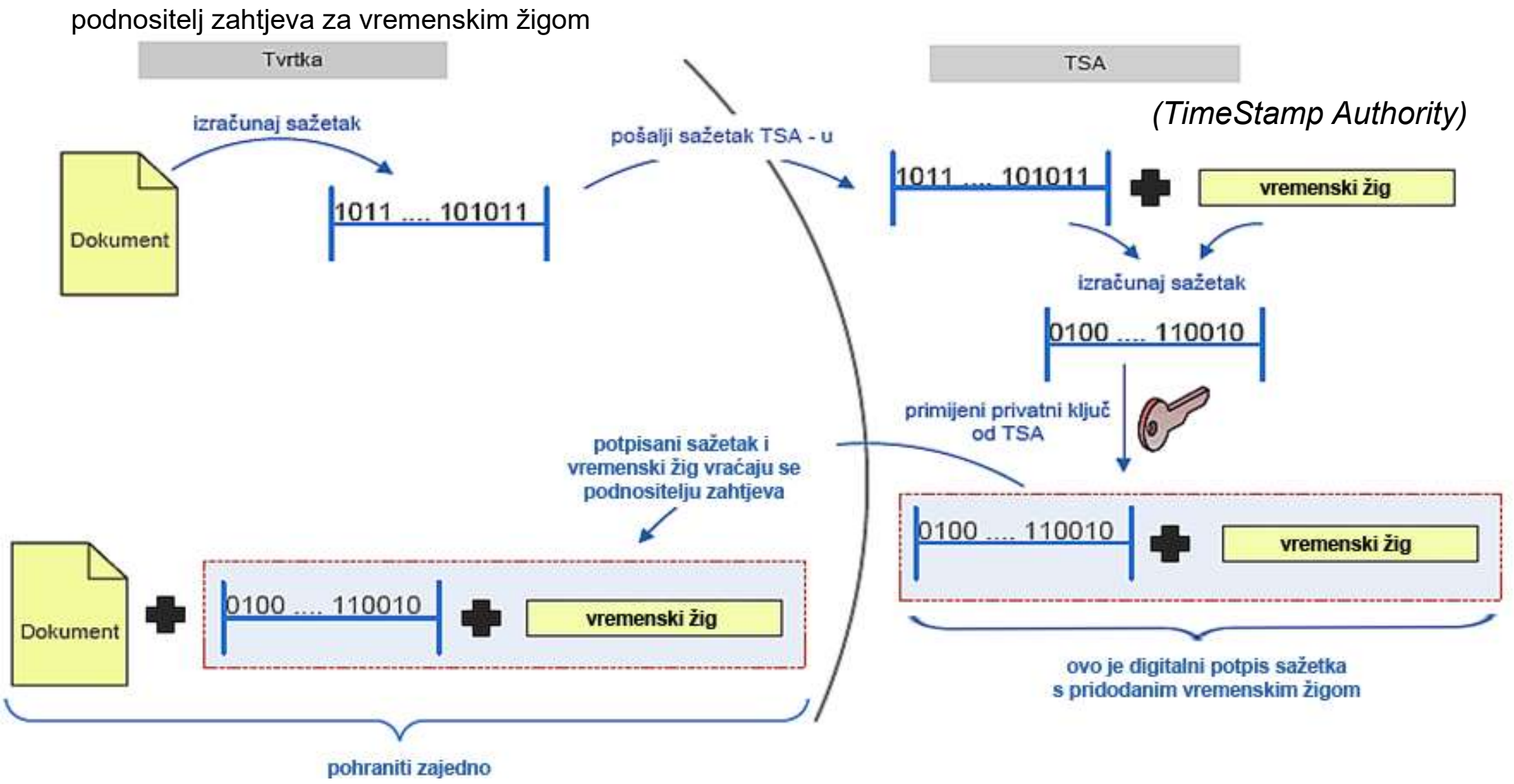
- Jedan CA može potpisati certifikat drugog CA
- Može se napraviti **hijerarhija certifikacijskih tijela (CA)**
- Ako nemamo povjerenja u neki CA, možda imamo povjerenja u CA koji je u hijerarhiji iznad njega. Time stječemo povjerenje i u CA na nižoj razini hijerarhije
- CA na najvišoj razini sam potpisuje svoj certifikat – to je onda samopotpisani certifikat. CA sa samopotpisanim certifikatom je korijenski CA

Centar za pouzdano vremensko označavanje (TSA)

- Stvara vremenske žigove kako bi se dokazalo da su određeni podaci postojali prije određenog vremena

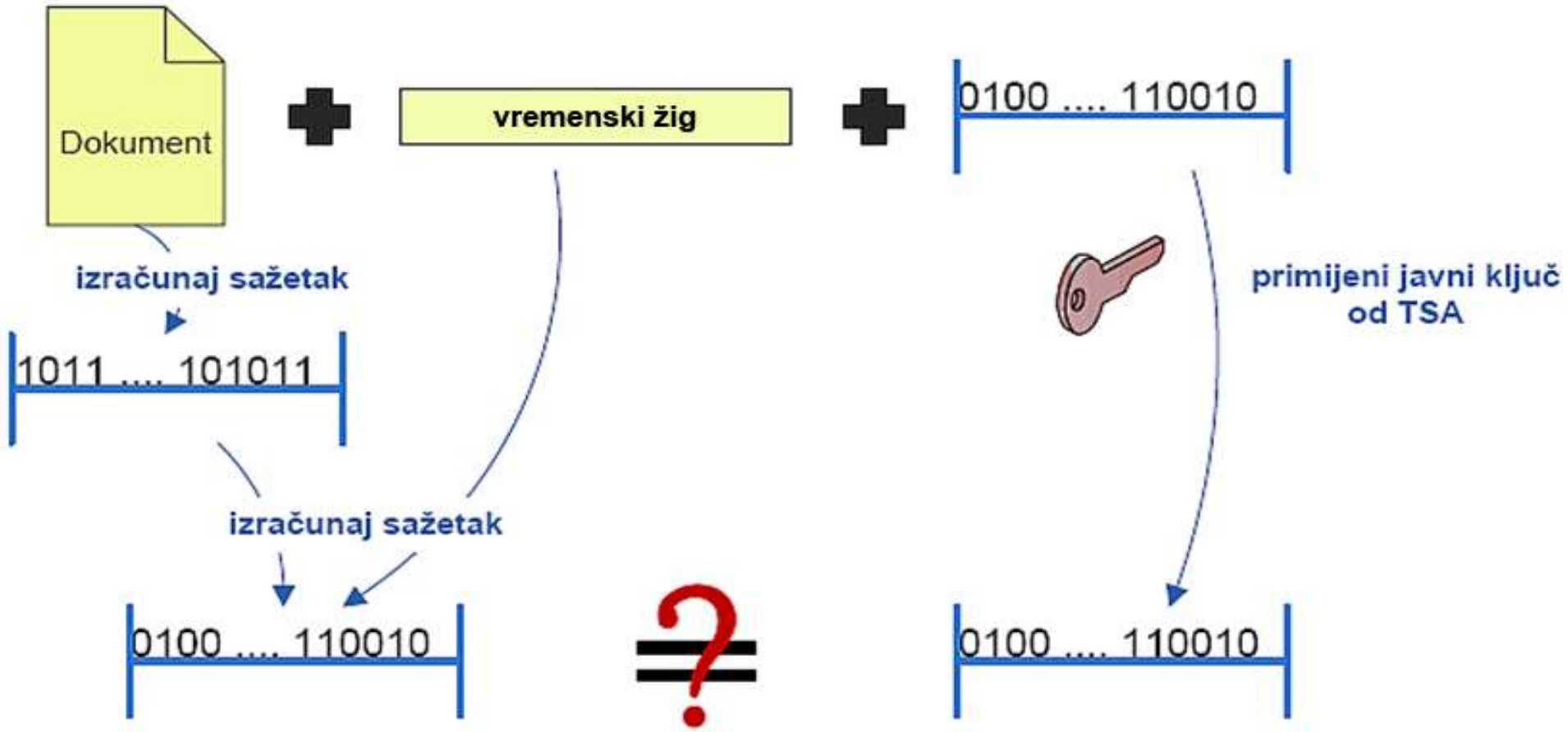
- **VREMENSKI ŽIG**
  - Vremenski žig, vremenski pečat, vremenska oznaka, vremenska ovjera, engl. ***timestamp***
  - **Osigurava pouzdanost digitalnog potpisa i poslije isteka valjanosti ili opoziva certifikata potpisnika**
    - Pomoću vremenskog žiga **može se dokazati da je potpis napravljen prije isteka valjanosti certifikata**

Postupak dodjeljivanja vremenskog žiga



- TSA ne prima originalne podatke od podnositelja zahtjeva već uvijek barata sažetcima

Postupak provjere vremenskog žiga



Postupak provjere vremenskog žiga

- Ako su sažetci jednaki, dokazano je da su i vremenska oznaka i dokument nepromijenjeni te da je TSA izdao vremensku oznaku
  - **Ne može se poreći da je podnositelj zahtjeva za vremenskom oznakom bio u posjedu originalnog dokumenta u vremenu naznačenom vremenskom oznakom**.
- Ako sažetci nisu jednaki, to znači
  - da su vremenska oznaka ili dokument promijenjeni
  - ili da vremensku oznaku nije izdao navedeni TSA

Davatelji usluga certificiranja (CA) u RH

1. **Financijska agencija (FINA)**
   - Datum upisa u evidenciju: 16. 7. 2008.
   - Usluge: *kvalificirani certifikat za e-potpis, kvalificirani certifikat za e-pečat, kvalificirani certifikat za autentifikaciju mrežnih stranica, kvalificirani vremenski žig, certifikat za elektronički potpis (prepoznat na nacionalnoj razini*
   - Izdaje certifikate fizičkim i pravnim osobama za opću namjenu
2. **Agencija za komercijalnu djelatnost (AKD)**
   - Datum upisa u evidenciju: 29. 5. 2015.
   - Usluge: *kvalificirani certifikat za e-potpis, kvalificirani certifikat za e-pečat, kvalificirani vremenski žig*
   - Certifikati za eOI – *pametna* osobna iskaznica
3. **Zagrebačka banka (ZABA)**
   - Datum upisa u evidenciju: 7. 6. 2016.
   - Usluge: *kvalificirani certifikat za e-potpis, kvalificirani vremenski žig*
   - Certifikati primarno za bankarske usluge

Evidenciju davatelja usluga certificiranja u RH vodi Ministarstvo gospodarstva i održivog razvoja

Vremenska ovjera u RH

FINA TSA – davatelj usluga javne vremenske ovjere

- FINA (kao **TSA**) pružatelj je usluge **ovjere elektroničkog potpisa**

- FINA TSA vremenskim žigom ovjerava potpis potpisnika
- potvrđuje se da su **podaci i elektronički potpis postojali prije stavljanja vremenskog žiga**

Digitalni potpis u EU (i RH) – tri vrste potpisa

- **Elektronički potpis**
  - podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje
- **Napredni elektronički potpis** mora ispunjavati sljedeće zahtjeve:
  - na nedvojben način je povezan s potpisnikom
  - omogućava identificiranje potpisnika
  - izrađen je korištenjem podataka 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
- **Kvalificirani elektronički potpis**
  - napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na **kvalificiranom certifikatu** za elektroničke potpise

Problemi s primjenom e-potpisa u EU

- zemlje članice prihvatile su kvalificirane elektroničke potpise kao pravno ekvivalentne ručnim potpisima te ih prihvaćaju kao dokaz u pravnim postupcima – **pravna osnova za korištenje digitalnih potpisa postoji**
- neke zemlje još uvijek imaju formalne prepreke širem uvođenju digitalnog potpisivanja (npr. zahtjevi za pisanim potpisom na dva primjerka na posebno obrascu)
- korištenje digitalnog potpisa u zemljama EU još nije doseglo svoj vrhunac, ali se dogodio porast korištenja za vrijeme *lockdowna* izazvanog pandemijom COVID-a
- **pravna neodređenost** – nedostatak većeg broja ranijih sudskih slučajeva značajan je problem

Uredba eIDAS

- *eIDAS – Electronic Identification and Signature (hrv. elektronička identifikacija i potpis)*
- Uredba Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu – donesena 23. 7. 2014.
  - Obvezujući zakonodavni akt za sve države članice
- Donesena zbog neusklađenosti nacionalnih zakonodavstava
  - Razlike u provedbi normi i pravila u praksi
  - **Kako pouzdano validirati e-potpis potpisnika iz druge države?**
  - Nedostatak pouzdanih informacija potrebnih za potpunu validaciju e-potpisa
- **Cilj: uspostava povjerenja i uzajamnog priznavanja e-potpisa i e-pečata unutar EU**

Digitalni potpis u EU (i RH)

- Do **7. 7. 2017.** u RH Zakon o elektroničkom potpisu (iz 2002. godine)
- **23. 7. 2014.** Europski parlament i vijeće donose uredbu eIDAS
- **Od 1. 7. 2016.** Zakon o elektroničkom potpisu prestaje vrijediti u dijelu koji je u suprotnosti s uredbom eIDAS
- **19. 6. 2017.** Hrvatski sabor donosi Zakon o provedbi Uredbe (…)

Elektronički pečat

- Tri vrste pečata:

Uvodi se uredbom eIDAS

  - **Elektronički pečat**
    - podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka
  - **Napredni elektronički pečat** mora ispunjavati sljedeće zahtjeve:
    - na nedvojben način je povezan s autorom pečata
    - omogućava identificiranje autora pečata
    - izrađen je korištenjem podataka za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata
    - povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka
  - **Kvalificirani elektronički pečat**
    - napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat

Elektronički potpis i pečat

Elektronički potpis	Elektronički pečat
Potpisnik: **fizička osoba** koja izrađuje elektronički potpis	Autor pečata: **pravna osoba** koja izrađuje elektronički pečat
Elektronički potpis: podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi **za potpisivanje**	Elektronički pečat: podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi **osiguravanja izvornosti i cjelovitosti** tih podataka
Sredstvo za izradu elektroničkog potpisa	Sredstvo za izradu elektroničkog pečata
Certifikat za elektronički potpis	Certifikat za elektronički pečat

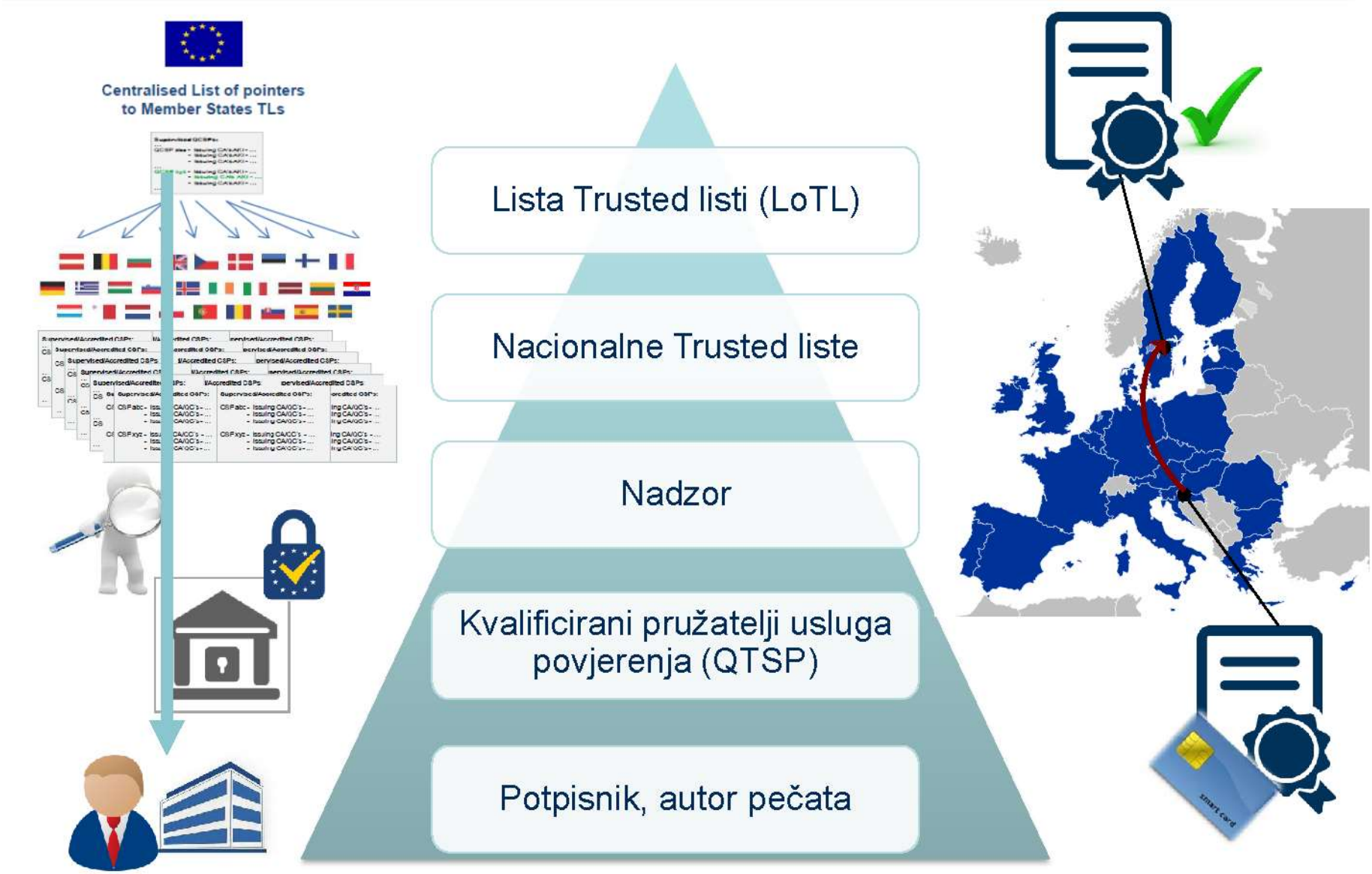
preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, travanj 2015.

Elektronički potpis i pečat (2)

Elektronički potpis	Elektronički pečat
Napredan elektronički potpis • 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 se otkriti bilo koja naknadna izmjena podataka	**Napredan elektronički pečat** • Na nedvojben način je povezan s autorom pečata • Omogućava **identificiranje autora pečata** • Izrađen je korištenjem podacima za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i **pod svojom kontrolom**, koristiti za izradu elektroničkog pečata • Povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka
Kvalificirani certifikat za elektronički potpis Izdaje ga kvalificirani pružatelj usluga povjerenja i ispunjava posebne uvjete	**Kvalificirani certifikat za elektronički pečat** Izdaje ga kvalificirani pružatelj usluga povjerenja i ispunjava posebne uvjete
Kvalificirano sredstvo za izradu elektroničkog potpisa Dodatno ispunjava zahtjeve za povjerljivost i sigurnost podataka za izradu e-potpisa, zaštićuju e-potpis od krivotvorenja i sl.	**Kvalificirano sredstvo za izradu elektroničkog pečata** Dodatno ispunjava zahtjeve za povjerljivost i sigurnost podataka za izradu e-pečata, zaštićuju e-pečat od krivotvorenja i sl.

preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, travanj 2015.

Sustav povjerenja prema uredbi eIDAS



preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, 2015.

Sigurnost XML-dokumenata

- Elektroničko poslovanje uglavnom se temelji na razmjeni **XML dokumenata**.

- Sigurnosne norme ugrađene u XML:
  - ***XML-Encryption*** i ***XML-Signature***
  - dodaju se dokumentu bez kršenja pravila XML-a
  - takvi dokumenti mogu se pregledavati korištenjem standardnih alata za XML

- sigurnost XML-dokumenata može biti implementirana i korištenjem standardnih sigurnosnih protokola
  - ti algoritmi koriste binarne datoteke koje onda mogu biti interpretirane samo korištenjem posebnih alata

Sigurnost XML-dokumenata

- za siguran prijenos dokumenata kroz mrežu može se koristiti protokol TLS
  - time se **štiti samo prijenos** podataka kroz mrežu, a **ne i pohrana**
  - dokument poslan korištenjem isključivo TLS-a prestaje biti siguran onog trenutka kada stigne na odredište

- primjenom sigurnosnih mjera nad samim dokumentom korištenjem standarda za sigurnost XML-a, dokument se osigurava i u prijenosu i u kasnijoj pohrani jer se ne osigurava veza nego sami dokument

- norma ***XML Digital Signature*** koristi se za pohranu digitalnog potpisa u XML-dokument
- norma ***XML Encryption*** koristi se za pohranu kriptiranog sadržaja u formatu XML

Kanonikalizacija

- dva logički jednaka XML-dokumenta mogu biti različito zapisana
- primjerice, u jednom se nalazi **razmak viška ili prazan red viška**

- dva dokumenta logički jednaka, ali sažetak ta dva dokumenta dobiven *hash*-algoritmom nije jednak!

  → kod digitalnog potpisivanja to za **posljedicu ima neuspješnu verifikaciju potpisa**, iako dokument logički nije promijenjen, tj. očekivalo bi se da bi verifikacija trebala biti uspješna

- kako bi se takvi problemi izbjegli, **XML-dokumente treba kanonikalizirati** tj. **svesti se na jednak (kanonički) oblik** (normiranje razmaka i sl.)

XML-Signature (XML-DSig)

- **XML-DSig** je W3C norma
  - W3C = World Wide Web Consortium
- **definira kako ugraditi digitalni potpis u XML dokument (tako da su zadovoljena pravila XML-a)**
- **nije algoritam** za digitalno potpisivanje
- jednim potpisom moguće je potpisati više dokumenata
- moguće je potpisati i dokumente koji nisu u formatu XML
- moguće je potpisati samo dio XML dokumenta (na taj se način omogućuje da različite dijelove jednog XML-dokumenta potpisuju različiti ljudi)

XML Signature Syntax and Processing Version 1.1
(W3C preporuka, 11.4.2013.)
http://www.w3.org/TR/xmldsig-core/

XML-Signature (XML-DSig)

```
<Signature ID?>
    <SignedInfo>
        <CanonicalizationMethod/>
        <SignatureMethod/>
        (<Reference URI?>
          (<Transforms>)?
        <DigestMethod>
         <DigestValue>
        </Reference>)+
    </SignedInfo>
    <SignatureValue>
     (<KeyInfo>)?
     (<Object ID?>)*
</Signature>
```

- XML potpis se u XML dokumentu realizira preko elementa ***signature***
- **?** - predstavlja nula ili jedno pojavljivanje,
  + - jedno ili više pojavljivanja,
  * - nula ili više pojavljivanja

XML-Signature (XML-DSig)

```
<Signature ID?>
    <SignedInfo>
        <CanonicalizationMethod/>
            …
     </SignedInfo>
            …
 </Signature>
```

- Element *SignedInfo* – unutar svojih podelemenata **identificira podatke koji se potpisuju te različite algoritme** koji će se koristiti
- *CanonicalizationMethod* **-** sadrži ime **algoritma kojim se radi kanonikalizacija podataka**

XML-Signature (XML-DSig)

- *SignatureMethod* - definira **algoritam za generiranje potpisa**
- *SignatureValue* - sadrži vrijednost potpisa elementa *SignedInfo*

```
<Signature ID?>
   <SignedInfo>
          <CanonicalizationMethod/>
          <SignatureMethod/>
          (<Reference URI?>
            (<Transforms>)?
          <DigestMethod>
           <DigestValue>
          </Reference>)+
      </SignedInfo>
    <SignatureValue>
...
</Signature>
```

XML-Signature (XML-DSig)

- ***Reference*** **- identificira resurse koji će biti potpisani i sve algoritme** koji će se koristiti **za pretprocesiranje** podataka. Ti algoritmi su ispisani u elementu ***Transforms*** i uključuju operacije kao što su šifriranje/dešifriranje, kompresija/inflacija ili **XPath** transformacija (XPath omogućuje potpisivanje dijela dokumenta).

```
<Signature ID?>
   <SignedInfo>
          <CanonicalizationMethod/>
          <SignatureMethod/>
          (<Reference URI?>
            (<Transforms>)?
          <DigestMethod>
           <DigestValue>
          </Reference>)+
      </SignedInfo>
    <SignatureValue>
...
</Signature>
```

XML-Signature (XML-DSig)

- Element *Reference* ima atribut ***URI*** koji je neobavezan, ali **ako potpis sadrži više elemenata *Reference*** onda je URI neobavezan samo za jedan element, a ostali ga moraju imati.

- Ako je sadržaj URI-ja **“”**, tj. prazan znakovni niz, to znači da se potpisuje dokument u kojem se nalazi element

```
<Signature ID?>
   <SignedInfo>
          <CanonicalizationMethod/>
          <SignatureMethod/>
          (<Reference URI?>
            (<Transforms>)?
          <DigestMethod>
           <DigestValue>
          </Reference>)+
      </SignedInfo>
    <SignatureValue>
...
</Signature>
```

XML-Signature (XML-DSig)

Svaki *Reference* uključuje :

- ***DigestMethod*** - sadrži informaciju o algoritmu koji se koristi za računanje sažetka dokumenta
- ***DigestValue*** - sadrži sažetak dokumenta izračunat algoritmom navedenim u *DigestMethod*

KeyInfo - sadrži informacije o ključu i o certifikatu

```
<Signature ID?>
   <SignedInfo>
          <CanonicalizationMethod/>
          <SignatureMethod/>
          (<Reference URI?>
            (<Transforms>)?
           <DigestMethod>
           <DigestValue>
          </Reference>)+
      </SignedInfo>
    <SignatureValue>
    (<KeyInfo>)?
...
</Signature>
```

XML-Signature (XML-DSig)

```
<SignedInfo>
 <CanonicalizationMethod
  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
 <SignatureMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
 <Reference URI="">
  <Transforms>
   <Transform
    Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>tVicGh6V+8cHbVYFIU91o5+L3OQ=</DigestValue>
 </Reference>
</SignedInfo>
```

XML-Signature (XML-DSig)

```
  <SignatureValue>
   dJDHiGQMaKN8iPuWApAL57eVnxz2BQtyujwfPSgE7HyKoxYtoRB97ocxZ
   8ZU440wHtE39ZwRGIjvwor3WfURxnIgnI1CChMXXwoGpHH//Zc0z4ejaz
   DuCNEq4Mm4OUVTiEVuwcWAOMkfDHaM82awYQiOGcwMbZe38UX0oPJ2DOE=
  </SignatureValue>
  <KeyInfo>
   <X509Data>
    <X509SubjectName>
     CN=My Name,O=Test Certificates Inc.,C=US
    </X509SubjectName>
    <X509Certificate>
     MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhkiG9w0BAQUFADBAMQswCQYD
     VQQGEwJVUzEfMB0GA1UEChMWVGVzdCBDZXJ0aWZpY2F0ZXMgSW5jLjEQ
     MA4GA1UEAxMHTXkgTmFtZTAeFw0wNzAxMDMyMTE4MTFaFw0zMTA4MjUy
     ...
    </X509Certificate>
   </X509Data>
  </KeyInfo>
 </Signature>
</PurchaseOrder>
```

XML-Signature (XML-DSig)

- XML potpis može se pojaviti u tri osnovna oblika:
  - Omotani potpis (***Enveloped***) – potpis se nalazi unutar dokumenta.
  - Omotavajući potpis (***Enveloping***) – potpis omeđuje dokument koji potpisuje.
  - Odvojeni potpis (***Detached***) – potpis se nalazi u zasebnom dokumentu, a URI (*Universal Resource Identifier*) određuje koji dokument potpisuje.
  - moguće je kombinacijama ta tri oblika dobiti nove
  - jedna od mogućih kombinacija: omotavajući potpis umetnuti u dokument tako da on potpisuje neke točno određene podatke

XML-Signature (XML-DSig)

```
<Igrac xmlns="http://www.hou.hr/">
  <Ime>Antea</Ime>
  <Prezime>Tadic</Prezime>
  <Pozicija>Tehnicar</Pozicija>


  <Signature xmlns='http://www.w3.org/2000/09/xmldsig#'>

    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/07/xmldsig#rsa-sha1" />
      <Reference URI="">
        <Transforms Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710" />
        <DigestMethod Algorithm="http://www.w3.org/2000/07/xmldsig#sha1" />
        <DigestValue>jkhKJHHIhkklADKHj=dsfs34'FDE'?sdsa</DigestValue>
      </Reference>
    </SignedInfo>

    <SignatureValue>DFSLK89sdf?sdasHK</SignatureValue>

    <KeyInfo>
      <X509Data>
```

- Primjer omotanog potpisa - potpisuje se dokument u kojem se nalazi <Signature>

XML-Signature (XML-DSig)

- U slučaju omotavajućeg potpisa, potpisuje se sadržaj elementa *Object*

```
<Signature ID?>
    <SignedInfo>
        …
    </SignedInfo>
    <SignatureValue>
     (<KeyInfo>)?
     (<Object ID?>)*
</Signature>
```

XML-Signature (XML-DSig)

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
         Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod
         Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#obj">
      <ds:DigestMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue/>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue/>
  <ds:Object Id="obj">Hello, World!</ds:Object>
</ds:Signature>
```

- Primjer omotavajućeg potpisa - potpisuje se sadržaj elementa <Object>

XML-Signature (XML-DSig)

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
         Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod
         Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="http://www.w3.org/TR/xml-stylesheet">
      <ds:DigestMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue/>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue/>
</ds:Signature>
```

- Primjer odvojenog potpisa – potpis se nalazi u zasebnoj XML-datoteci, a ono što se potpisuje identificira se URI-jem u elementima <Reference>

XML-Signature (XML-DSig)

```
<Igrac xmlns="http://www.hou.hr/">
  <Ime>Antea</Ime>
  <Prezime>Tadic</Prezime>
  <Pozicija>Tehnicar</Pozicija>
  <Signature xmlns='http://www.w3.org/2000/09/xmldsig#'>
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/07/xmldsig#rsa-sha1" />
      <Reference URI="">
        <Transforms Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710" />
        <DigestMethod Algorithm="http://www.w3.org/2000/07/xmldsig#sha1" />
        <DigestValue>jkhKJHHIhkklADKHj=dsfs34'FDE'?sdsa</DigestValue>
      </Reference>
      <Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>DFSLK89sdf?sdasHK</SignatureValue>
    <KeyInfo>...</KeyInfo>
    <Object>...</Object>
  </Signature>
</Igrac>
```

ovaj dokument

neki drugi dokument identificiran URI-jem

- Primjer hibridnog potpisa – kombinacija omotanog i odvojenog potpisa

XAdES

XAdES (*XML Advanced Electronic Signatures*)

- **Skup proširenja preporuke XML-Dsig**

(samo prijavljen za W3C preporuku)

ETSI (*European Telecommunications Standards Institute)* norma TS 101 733

- Definira šest profila koji se razlikuju po razini zaštite koju nude:
  - XAdES - napredni el. potpis u skladu s Direktivom 1999/93/EC
  - XAdES-T - uključuje i vremensku oznaku
  - XAdES-C - dodaje na XAdES-T poveznice na certifikate i listu opozvanih certifikata
  - XAdES-X - dodaje na XAdES-C vremenske oznake na uvedene poveznice
  - XAdES-X-L - u potpisani dokument dodaje certifikate i listu opozvanih certifikata
  - XAdES-A - zahtijeva slijed vremenskih oznaka za dugoročno arhiviranje

XML *Encryption (XML-Enc)*

- **XML-Enc** opisuje kako šifrirani sadržaj **ugraditi u XML**
- **Nije** algoritam šifriranja

- Mogu se šifrirati i neXML-ovski dokumenti
- Moguće je šifrirati samo dio XML-dokumenta
- Različite dijelove XML-dokumenta moguće je šifrirati različitim ključevima – kontrola pristupa

- **XML Encryption Syntax and Processing** Version 1.1. (11.4.2013.)

  http://www.w3.org/TR/xmlenc-core/

XML *Encryption*

Šifriranje se može izvesti na tri načina:

- korištenjem **simetrične kriptografije** – podatci se šifriraju simetričnim ključem koji su ranije sudionici komunikacije na neki (siguran) način razmijenili
- korištenjem **asimetrične kriptografije** – podatci se šifriraju javnim ključem primatelja
- korištenjem **hibridnog pristupa** – podatci se šifriraju simetričnim ključem, a taj simetrični ključ šifrira se javnim ključem primatelja; šifrirani simetrični ključ i sadržaj šifriran tim simetričnim ključem ugrađuju se u XML-dokument; ovaj je pristup najučestaliji

XML *Encryption* – struktura

```
<EncryptedData Id? Type? MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
  <CipherData>
    <CipherValue>?
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties>?
</EncryptedData>
```

Algoritam kojim se podatci šifriraju

Informacije o ključu kojim je sadržaj šifriran

Šifrirani podatci

Dodatne informacije

XML-*Encryption* (XML-Enc)

- Specifikaciju ***XML Encryption Syntax and Processing*** izdao je **W3C** XML *Encryption Working Group* s ciljem da uspostavi proces šifriranja/dešifiranja digitalnih sadržaja (uključujući XML dokumente kao i njihove dijelove) i sintaksu, kako bi se prikazali:
  - **šifrirani sadržaj** i
  - **informacija koja omogućava** određenom primatelju **dešifriranje** primljenog sadržaja.

- Rezultat šifriranja je podatkovni element koji sadrži (preko jednog od svojih podelemenata) ili identificira (preko URI reference) **šifrirane podatke**.

- Kad šifriramo XML element ili sadržaj elementa **šifrirani podaci** (element *EncryptedData*) **zamjenjuju element odnosno sadržaj** u šifriranoj verziji XML dokumenta.

XML *Encryption* – primjer

```
<?xml version="1.0" standalone="no"?>
<igrac>
    <ime>Antea</ime>
    <prezime>Tadic</prezime>
    <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
        xmlns="http://www.w3.org/2001/04/xmlenc#">
      <EncryptionMethod
          Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
          <EncryptionMethod
              Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <KeyName>session</KeyName>
          </KeyInfo>
          <CipherData>
            <CipherValue>r4f7SI1aZKSvibbfsd5345</CipherData>
        </EncryptedKey>
      </KeyInfo>
      <CipherData>
        <CipherValue>sGNhKqcSovipJdOFCFKYEEMRFsdaZIUh</CipherValue>
      </CipherData>
    </EncryptedData>
</igrac>
```

šifrirani sadržaj

algoritam za šifriranje saržaja

algoritam šifriranja simetričnog ključa

šifrirani simetrični ključ

podatci šifrirani simetričnim ključem

- šifrira se sadržaj elementa <pozicija>
- koristi se hibridni pristup

- simetrični ključ šifrira se javnim ključem primatelja (algoritam RSA) i zajedno sa šifriranim sadržajem šalje na odredište

XML *Encryption* – primjer

Objašnjenje primjera:

- šifriran je sadržaj elementa <pozicija>
- hibridni pristup - podatci se šifriraju simetričnim ključem, a onda se taj simetrični ključ šifrira javnim ključem primatelja i takav se zajedno sa šifriranim sadržajem šalje na odredište
- na slici je plavom bojom označen algoritam kojim se šifrira simetrični ključ - asimetrični algoritam RSA
- zelenom je bojom prikazan šifrirani ključ
- sadržaj XML-dokumenta koji je potrebno sakriti šifrira se simetričnim algoritmom AES što je na slici prikazano narančastom bojom. Tako se dobije šifrirani sadržaj koji je na slici označen sivom bojom.
- element <EncryptedData> (crveno na slici) nalazi upravo na mjestu na kojem se prethodno nalazio element koji se šifrira

Sigurnost u elektroničkoj trgovini

Sigurnosni zahtjevi kod *online* plaćanja

- **Autentifikacija -** u transakciji online plaćanja se zna tko sudjeluje u transakciji i zna se da je osoba upravo ta za koju tvrdi da jest.
- **Integritet -** podaci iz transakcije se neće mijenjati
- **Jedinstvenost zahtjeva za plaćanjem -** omogućava trgovcu da prepozna ponovni zahtjev za istom transakcijom
- **Neporecivost transakcije -** nakon izvršavanja transakcije kupac ne može poreći da je izvršio transakciju, odnosno trgovac ne može poreći da je primio transakciju
- **Povjerljivost** – podacima o transakciji se ne može neovlašteno pristupiti
- **Privatnost i anonimnost kupca -** trgovac može vidjeti samo pseudonim ili korisničko ime kupca, ali ne i njegove privatne podatke
- **Pouzdanost sustava -** preventivne radnje u slučaju pada sustava te kod greški prilikom izvršavanja transakcije

Kartična naplata u elektroničkoj trgovini

- Primjer: ***PayPal*** **–** jedan od najraširenijih i najpoznatijih sustava za online plaćanje na svijetu

- za slanje novca potrebno je znati samo **e-mail adresu** *PayPal* računa osobe/tvrtke kojoj se želi poslati novac
- za uplaćivanje novca na *PayPal* račun koristi se kreditna ili debitna kartica
- *online* plaćanje: ili s *PayPal* računa ili kreditnim karticama

- U listopadu 2002. godine *eBay* je kupio *PayPal* (u trenutku kupnje više od 50% korisnika *eBaya* je već koristilo *PayPal*)

- U Hrvatsku je *PayPal* došao sredinom 2006. godine.
  - u početku samo slanje novca, a od ožujka 2011. godine korisnicima iz Hrvatske je omogućeno i primanje novca na vlastiti *PayPal* račun

Kartična naplata u elektroničkoj trgovini

Sigurnost *PayPal* transakcija

- pri transakciji se trgovcu ne daje broj kreditne kartice
  - trgovcu se prosljeđuje samo e-mail adresa kupca
  - trgovac prima *online* uplatu bez mogućnosti da vidi financijske podatke kupca
  - nakon svake transakcije korisnik na svoju e-mail adresu dobiva e-mail poruku s informacijama o izvršenoj transakciji

- svi podaci (osobni i financijski) koji se šalju s klijentskog računala na *PayPal* poslužitelj su šifrirani.
  - prilikom registracije ili prijave na *PayPal* web stranice koristi se TLS 1.2 (ili viši)
  - za SSL certifikate koristi se algoritam SHA-256
- poslužitelji s osjetljivim financijskim podacima **nisu direktno povezani na Internet**

Kartična naplata u elektroničkoj trgovini

Sigurnost *PayPal* transakcija (nastavak)

- Provjera:
- *Address Verification Service* (AVS) je sustav koji se koristi za **verifikaciju adrese osobe** koja tvrdi da posjeduje određenu kreditnu karticu. Sustav će usporediti adresu koju daje korisnik kreditne kartice kod izvršavanja transakcije online plaćanja (ili kod povezivanja kreditne kartice s *PayPal* računom) s adresom koja je zapisana kod izdavatelja kartice. AVS provjerava samo brojčani dio adrese (poštanski broj, kućni broj).
- *Card Security Code (CSC)* ili *Card Code Verification* (CCV) - troznamenkasti ili četveroznamenkasti sigurnosni kod koji se obično nalazi na stražnjoj strani kreditne kartice napisan obrnuto nakošeno.
  - Taj kod koristi se kao sigurnosna provjera kad ne postoji mogućnost korištenja PIN-a.
  - Trgovci koji zahtijevaju CVV2 kod pri transakcijama tipa ***card-not-present*** **ne smiju** taj kod **pohraniti**.
  - Ta sigurnosna mjera je jedna od sigurnosnih mjera sigurnosnog standarda **PCI DSS** (*Payment Card Industry Data Security Standard*).

Kartična naplata u elektroničkoj trgovini

- O sigurnosti…

  … s web-stranica pružatelja usluga online naplate

- **3D Secure zaštita za sve trgovce i kupce**
  - WSpay™ sustav koristi najviše standarde zaštite i privatnosti podataka.
  - Svi trgovci koji koriste WSpay™ su uključeni u 3D secure zaštitu, čime se jamči korisnicima shopa da je kupnja sigurna.
  - Brojevi kreditnih kartica kupaca se ne čuvaju na sustavu a sami upis se štiti SSL enkripcijom podataka

Jamstvo sigurne online kupnje Klikni ovdje

MasterCard SecureCode learn more

Verified by VISA learn more

- **Certifikacija po PCI DSS standardima**
  - WSpay™ sustav radi kontinuirano na povećanju sigurnosti i potvrđivanju toga. Od ove godine će biti potvrđeno da posluje po najvišim standardima koji kartičar propisuje.
  - PCI Data Security Standard (PCI DSS) je norma koja definira sigurnosne mjere za obradu, spremanje i prenošenja (komunikaciju) kartičnih podataka.

Sigurnost

Od 1.siječnja 2008. godine počeo se primjenjivati novi sigurnosni standard (PCI DSS) u CEMEA regiji. Sigurnosni standard vrijedi za sve trgovce, procesore i banke koji sudjeluju u kartičnom poslovanju. PCI DSS vrijedi i za proizvođače opreme, aplikacija kako i na tvrtke koje nude hosting usluge.

VISA, MasterCard, American Express, Diners, Discover Card i JCB su zajedno stvorili industrijski standard za sigurnost podataka kako bi zaštitili svoje korisnike. Ovaj standard za industriju kartičnog poslovanja osigurava svim trgovcima, bankama i pružateljima usluga zaštitu podataka vlasnika kartica.

Svi pružatelji usluga moraju se certificirati od strane kvalificiranih revizora sigurnosti za VISA-u i akreditiranog pružatelja usluga skeniranja za MasterCard kako bi zadržali pravo procesiranja kartičnog plaćanja.

PCI DSS

PCI DSS - *Payment Card Industry Data Security Standard*

- sigurnosni standard za kartično poslovanje
- definira minimalne sigurnosne mjere i procese

- Definirao ga je *Payment Card Industry Security Standards Council*
  - **Visa, MasterCard, American Express, Discover Card i JCB** su zajedno stvorili industrijski standard za sigurnost podataka kako bi zaštitili svoje korisnike.
  - osigurava trgovcima, kartičnim kućama, bankama i ostalim poslovnim subjektima koji se bave kartičnim poslovanjem **zaštitu podataka vlasnika kartica**
- Prva verzija standarda PCI DSS izdana je 2004. godine
- Verzija 3.2.1 izdana je u svibnju 2018. godine

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

PCI DSS

- **Banke i pružatelji usluga** moraju se **certificirati kod** kvalificiranih **revizora** sigurnosti, a trgovci su dužni se pridržavati PCI DSS standarda i obavljati kartično poslovanje samo s certificiranim pružateljima usluga.

- PCI DSS regulira zahtjeve koji se odnose na upravljanje sigurnošću podataka, sigurnosne procedure, mrežnu arhitekturu, oblikovanje programske potpore za obradu podataka te ostale kritične zaštitne mjere u kartičnom poslovanju.

- Jezgru PCI DSS-a čini skupina načela i pratećih zahtjeva oko kojih su organizirani specifični elementi sigurnosti podataka u kartičnom poslovanju.
  - 12 osnovnih zahtjeva i oko 270 podzahtjeva

PCI DSS – načela i zahtjevi

Neki od zahtjeva iz PCI DSS:

Zahtjev 1: **Instalirati i održavati odgovarajuću konfiguraciju vatrozida** (eng. *firewall*) **radi zaštite podataka o vlasnicima kartica.**

Zahtjev 2: **Ne koristiti lozinke i druge sigurnosne parametre dobivene od dobavljača softverskog sigurnosnog rješenja**

- **Promijeniti početne zaporke** postavljene od strane dobavljača

Zahtjev 3: **Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štititi.**

- **sigurnosni kodovi kartica** (troznamenkasti ili četveroznamenkasti broj obično ispisan na stražnjoj strani kartice) koji se koriste za potvrđivanje (verifikaciju) transakcije **i PIN brojevi ne smiju se pohranjivati**.

PCI DSS – načela i zahtjevi

Neki od zahtjeva iz PCI DSS (nastavak):

Zahtjev 4: **Tijekom prijenosa putem otvorenih, javnih mreža svi podatci o vlasniku kartice moraju se štititi šifriranjem (enkripcijom).**

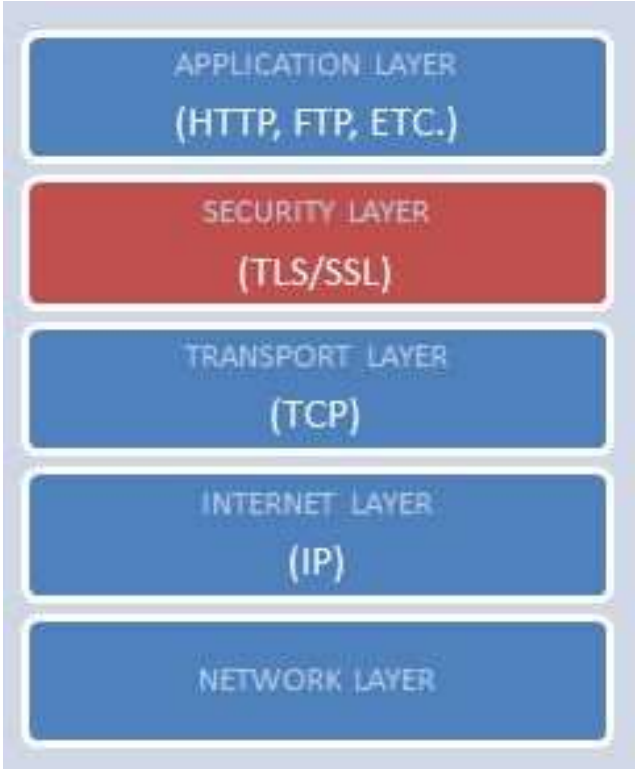
- Koristiti snažne kriptografske metode i sigurnosne protokole (primjerice SSL/TLS, IPSEC, SSH) za **zaštitu osjetljivih kartičnih (korisničkih) podataka tijekom prijenosa** kroz otvorene, javne mreže (Internet, bežični prijenos, GSM i GPRS).

Zahtjev 5: **Nužno je koristiti i redovito osvježavati softver za zaštitu od zlonamjernog koda, odnosno antivirusni softver**

…

TLS / SSL

- Broj kreditne kartice upisuje se preko web preglednika i putuje do web poslužitelja on-line trgovine
- **kod elektroničkog plaćanja** potrebno je između transportnog protokola TCP i aplikacijskog protokola HTTP koristiti i **sigurnosni protokol TLS / SSL**
- **TLS / SSL** osigurava **šifriranje** cjelokupne komunikacije iznad transportnog sloja.



TLS / SSL

- **protokol SSL** (eng. *Secure Socket Layer*) razvila je tvrtke Netscape Communications – verzija SSL 3.0 izašla je 1996. godine
- **protokol TLS** (eng. *Transport Layer Security*) objavljen je 1999. godine - nadogradnja na SSL 3.0
  - 2006. godine TLS 1.1
  - 2008. godine **TLS 1.2** - koristi *hash*-funkciju SHA-256 (iz SHA-2)
  - 2018. godine **TLS 1.3**
- **TLS / SSL**
  - koristi se za ostvarivanje sigurnije razmjene povjerljivih podataka, poput korisničkog imena i zaporke, broja kreditne kartice i sl.
  - temelji se na upotrebi kriptografije te infrastrukture javnih ključeva (engl. *Public key infrastructure* - PKI)
    - privatni i javni ključevi

TLS / SSL

- Za **kartično plaćanje** preko mreže preporučuje se korištenje TLS 1.2 ili TLS 1.3 (objavljen u kolovozu 2018. godine)
- Ne koristiti SSL.

- Pri korištenju SSL/TLS-a
  - adresa počinje oznakom **`https://`**
  - sva komunikacija između preglednika i web poslužitelja se šifrira

- **HTTPS** (*Hypertext Transfer Protocol Secure)* - kombinacija protokola HTTP i SSL/TLS (*Secure Sockets Layer / Transport Layer Security)*

TLS / SSL

- Služi za zaštitu od napada:
  - prisluškivanje (eng. *eavesdropping*)
  - čovjek-u-sredini (eng. *man-in-the-middle*)
- onemogućuje se presretanje i neovlašteno prisluškivanje komunikacije te eventualna krađa broja kreditne kartice
- međutim, ne rješava se problem **pohrane** brojeva kreditne kartice na samom poslužitelju

TLS / SSL

- Kad je uspostavljena sigurna veza (certifikat zaprimljen i provjeren od strane CA), pojavljuje se ikona lokota u pregledniku i adresa počinje oznakom `https://`

- Prilikom unosa povjerljivih podataka na web stranice provjeriti je li web stranica trenutno zaštićena (`https://`)
- preglednik obično ima ugrađene sigurnosne mehanizme koji javljaju ako web sjedište nije sigurno

TLS / SSL

- neki CA su uveli SSL certifikate tipa “samo provjera domene” (*domain validation only)* za koje se radi **minimalna provjera** detalja u certifikatu
  - za svaku uspješnu SSL konekciju – pojavljuje se ikona lokota
- **mnogi preglednici nisu jasno razlikovali certifikate s blažom validacijom od onih koji rade rigoroznu provjeru**
  - korisnici nisu svjesni je li web sjedište dovoljno provjereno ili nije
  - mogućnost *phishinga* – web sjedišta napravljena da bi služila za *phishing* mogu koristiti TLS/SSL da bi dobili dodatni kredibilitet

- **Extended Validation Certificate** (EV) propisuje **strože kriterije** za provjeru identiteta
  - Prikazuje se ime CA koji je izdao EV certifikat
  - Boja (obično zelena) ukazuje na to na je EV certifikat valjan
- Današnji web-preglednici prikazuju status EV.

Phishing

- ***Phishing*** - napadači pokušavaju saznati povjerljive podatke (najčešće zaporke, podatke o kreditnoj kartici ili PIN) lažno se predstavljajući kao vjerodostojan subjekt u komunikaciji.
- **lažnom porukom** elektroničke pošte ili porukom preko sustava za trenutno poručivanje korisnika se pokušava namamiti **na lažnu web stranicu**, kako bi na njoj upisao svoje korisničko ime i zaporku, PIN, broj kreditne kartice i sl.
- Npr. "*Radi provjere da Vaš račun nije neovlašteno korišten, molimo kliknite na poveznicu dolje i potvrdite svoj identitet*"
- lažne Web stranice banaka ili *online* trgovina koje vizualno izgledaju identično stvarnim stranicama
- Ako lažna stranica mimicira internetsko bankarstvo, u trenutku kada se korisnik prijavi na sustav, u pozadini ga skripta može automatski prijaviti na pravu stranicu banke, dok još vrijedi generirani OTP (one-time password). Nakon toga skripta, skriveno od korisnika, započinje prijenos novca…

TLS / SSL

- Tvrtka koje je razvila određeni web preglednik odlučuje kojim certifikacijskim tijelima (CA – *certification authority*) će vjerovati.

- **Korisnik treba vjerovati HTTPS konekciji samo ako:**
  - Korisnik vjeruje da preglednik ispravno implementira HTTPS s ispravno unaprijed instaliranim provjerama certifikata poznatih i pouzdanih CA
  - Sjedište weba ima valjani certifikat (kojeg je potpisao CA)
  - Korisnik ima povjerenje u tog CA

TLS / SSL

- **TLS/SSL certifikati**
  - posjetiteljima Web sjedišta potvrđuju identitet web sjedišta,
  - garantiraju sigurnu i povjerljivu razmjenu podataka
- Kao rezultat raste povjerenje posjetitelja Web sjedišta.

- Najpoznatije tvrtke koje izdaju SSL certifikate:
  VeriSign, Thawte, GeoTrust, RapidSSL, GlobalSign, GoDaddy, Entrust, ...
- korijenski CA – može ovlastiti druga certifikacijska tijela da potpisuju i provjeravaju certifikate u njihovo ime (hijerarhija CA)
- **Povjerenje u sustav certificiranja?**
  - povjerenje u CA niže u hijerarhiji koji su dobili ovlasti od korijenskih CA?
  - donošenje normi za provjeru CA (kao PCI norme u kartičnom poslovanju)?