Protection and security of information systems

Security in electronic business systems

prof. Ph.D. Boris Vrdoljak,
Ph.D. Luka Humski

University of Zagreb

Faculty of Electrical Engineering and Computing

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

- you are free to:
  - share —reproduce, distribute and communicate the work to the
  - public remix —rework the work
- under the following conditions:
  - appointment.You must acknowledge and attribute the authorship of the work in a manner specified by the author or licensor (but not in a manner that suggests that you or your use of their work has their direct endorsement).
  - non-commercial.You may not use this work for commercial purposes.
  - shares under the same conditions.If you modify, transform, or create using this work, you may distribute the adaptation only under a license that is the same or similar to this one.

In the case of further use or distribution, you must make clear to others the license terms of this work. The best way to do this is to link to this website.

Any of the above conditions may be waived with the permission of the copyright holder.

Nothing in this license infringes or limits the author's moral rights.

The text of the license was taken from http://creativecommons.org/.

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/.

Electronic business

Examples of electronic business

- electronic communication with other companies to order products and services and their electronic payment
  - business between companies - B2B (Business-to-Business)

- selling products and services through the Web site
  - e-commerce, business of the company with the final consumer - B2C (Business-to-Consumer)

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)

B2B electronic business - exchange of business documents

Basic business processes in the supply chain and electronic documents that are exchanged:

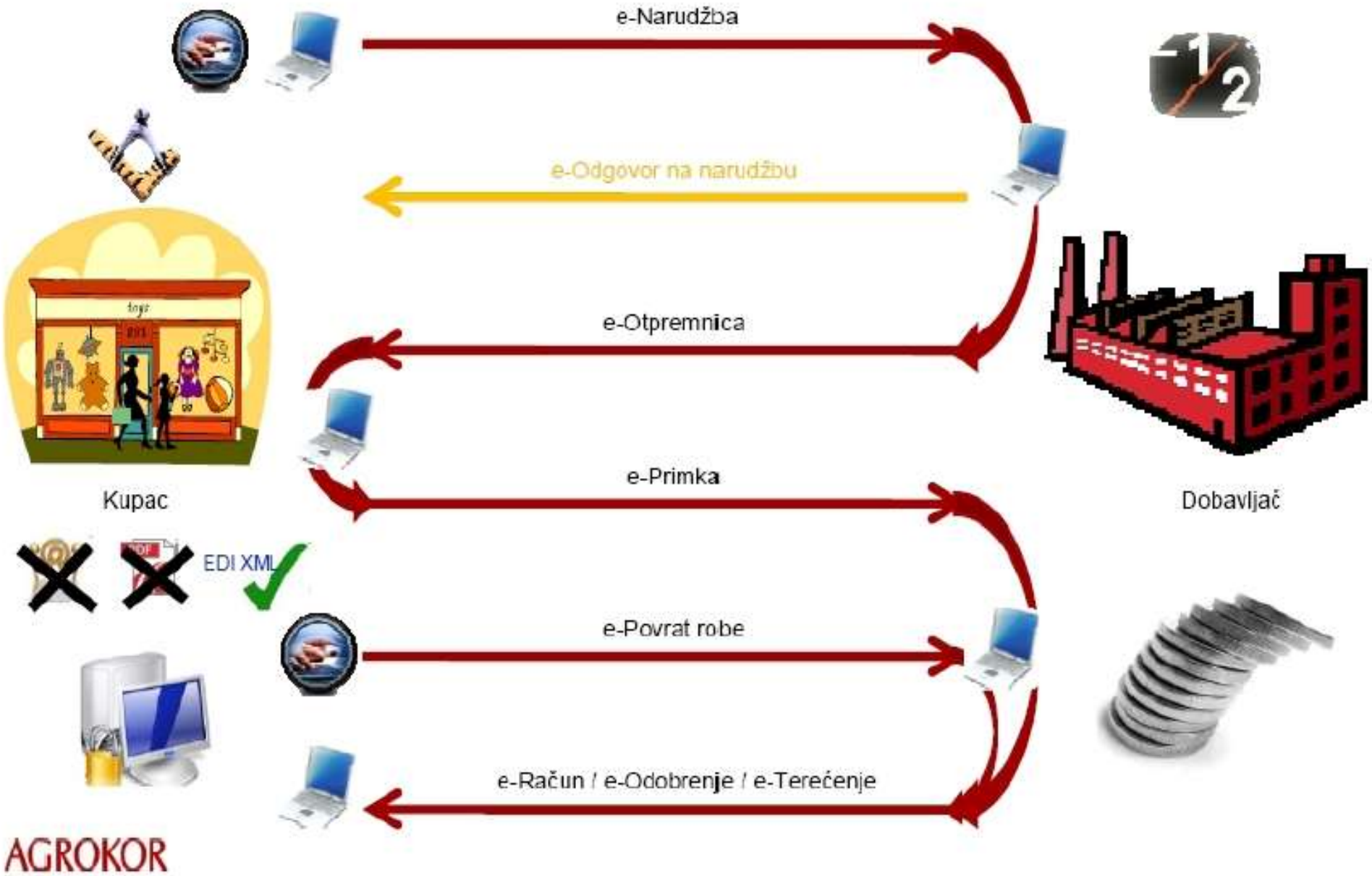
- Catalog	e-catalog
- Ordering	e-order form
- Shipping	e-shipping
- Receiving	e-receipt
- Invoicing	e-invoice
- Payment	e-order for payment

Elektroničko poslovanje B2B - razmjena poslovnih dokumenata

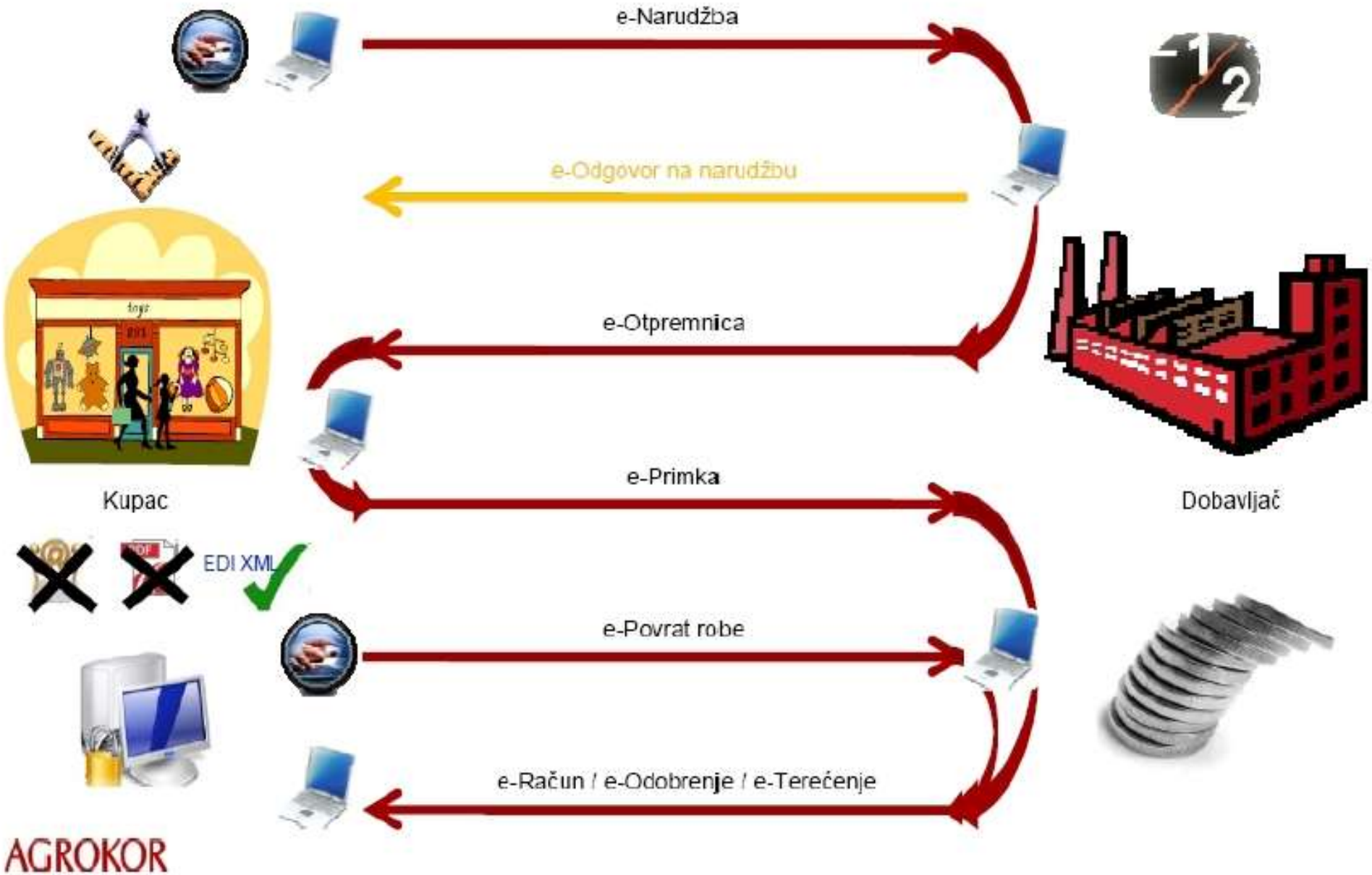
Osnovni poslovni procesi u dobavnom lancu i elektronički dokumenti koji se razmjenjuju:

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

Primjer razmjene e-dokumenata



Primjer razmjene e-dokumenata



Supply chain - basic business processes and documents

- Contemporary electronic documents which are exchanged in electronic business are mostly in XML format.

- There are also older norms EDDIE (Electronic Data Interchange), the most important of which is the norm EDIFACT (Electronic Data Interchange For Administration, Commerce and Transport).

- exchange of modern business electronic documents - technology: XML and Web services
- SECURITY?

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?

Security of electronic business

- B2B - exchange of XML documents and use of Web services

  - Ensuring authenticity (the declared sender is the real sender) and integrity (impossibility of changing the message)
    - E-signature
  - When the digital certificate expires, how do you prove that the certificate was valid at the time the document was signed?
    - Time verification, time stamp (timestamp)
  - Signing and encryption in XML format
    - XML Signature and XML Encryption
  - Security of Web services
    - Web Services Security (WSS) and other standards (WS-Extensions)
    - WS-I Basic Security Profile
    - Security of RESTful Web Services

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

Security when exchanging electronic documents

- e-invoiceis the most widespread electronic business document

- all EU member states should enable receivinge-Invoicefor tax purposes (VAT) if two conditions are met:

  1)recipient must agreewith receipt of invoices in electronic format;

  2)integrity (cannot be changed)and authenticity (the declared sender is the actual sender) must be secured during transmission and archiving.

This second requirement can be fulfilled eitheradvanced electronic signatureor through electronic data interchange (EDI) with agreed security measures.

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.

Electronic (digital) signature

- In the business and ICT world, we often encounter the term digital signature, electronic signature, e-signature or the English namee-signature.

- The Croatian encyclopedic dictionary says that a digital signature is "encryption that proves the authorship, i.e. the originality of the electronic document".

- The electronic signature is defined by the eIDAS regulation (adopted by the EU) as follows:data in electronic form which are associated or logically connected with other data in electronic form and which the signatory uses to sign".

- As part of this subject:
  - we will use the terms electronic signature and digital signature as synonyms,
  - the term electronic signature will not include the image of a handwritten signature (although it can also be considered a type of electronic signature in a broader sense).

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).

Asymmetric cryptography

It is used for digital signingasymmetric cryptography.

- one algorithm andpair of keys:one key for encryption, the other for decryption

- Encryption: transformsplaintext (plaintext)using a pre-arranged key

- The encryption result is calledcipher (ciphertext)orcryptogram

- the mathematical algorithm determines how to encrypt the plaintext complexity
- depends on the length of the key (number of bits)

- the strength of an encryption system rests on the key
  - an attacker can have ciphertexts and know the algorithms, the vulnerability of the system depends on the strength of the key
  - longer keys are harder to break (time, money)
  - key length: 128, 192 or 256 bits

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

Asymmetric cryptography

- in asymmetric cryptography, the keys are tied to each other
- knowing the algorithm and one key, it is impossible to discover another
- often: it doesn't matter which key is used to encrypt and decrypt
    - they work exclusively in pairs
- one of twothe key must remain secret

Each user has a pair of keys:

- private (secret) key
    - Available exclusively to the user, may not be distributed
- publickey
    - Available to all, must be distributed

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

Asymmetric cryptography

- what is encrypted with a public key can only be decrypted with a private key
- what is encrypted with a private key can only be decrypted with a public key

- knowing the public key, one cannot calculate the secret key in any reasonable time
- the time required to calculate the secret key from the known public key, i.e. breaking the code, is measured in millions of years on the most powerful computers available today

- Asymmetric cryptography is also calledpublic key cryptography.

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.**

Algorithms for asymmetric cryptography

- RSA (Rivest-Shamir-Adleman) - MIT
  - the most popular algorithm, developed in 1977.
- Diffie-Hellman
  - developed in 1976.
- Elliptic Curves Cryptosystem (ECC)
- others:

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

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 function and digital signature

- agodigital signatureshouldgenerate summary (hash, digest) messages hash
- functions
  - input: a string of characters of arbitrary length
  - output: string of characters of fixed length (eg 256 bits) basic
- properties of the hash function:
  - hashis a one-way function
    - it is not possible to regenerate the input message based on the output
    - it is not possible to specify an input message that would have a default hash
  - "application" and "change" will give a completely different summary (hash)
  - changing one bit of the input produces a completely different output

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-algorithms

- Secure Hash Algorithm (SHA-1) – not recommended to use
  - US Government Algorithm (NSA)
  - giveshasha value of length 160 bits from a character string of any length
  - collisiondiscovered in 2^{69}hasheva, 2005

- SHA-2 (variants SHA2-224, SHA2-256, SHA2-384, SHA2-512)

- SHA-3 (variants SHA3-224, SHA3-256, SHA3-384, SHA3-512)

- Message Digest Algorithm 5 (MD5) – not recommended to use
  - giveshashlength 128 bits
  - MD5 cracked in 2008

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

Digital signature procedure

is calculated

summary (hash)messages

sign the summary of the message

areown

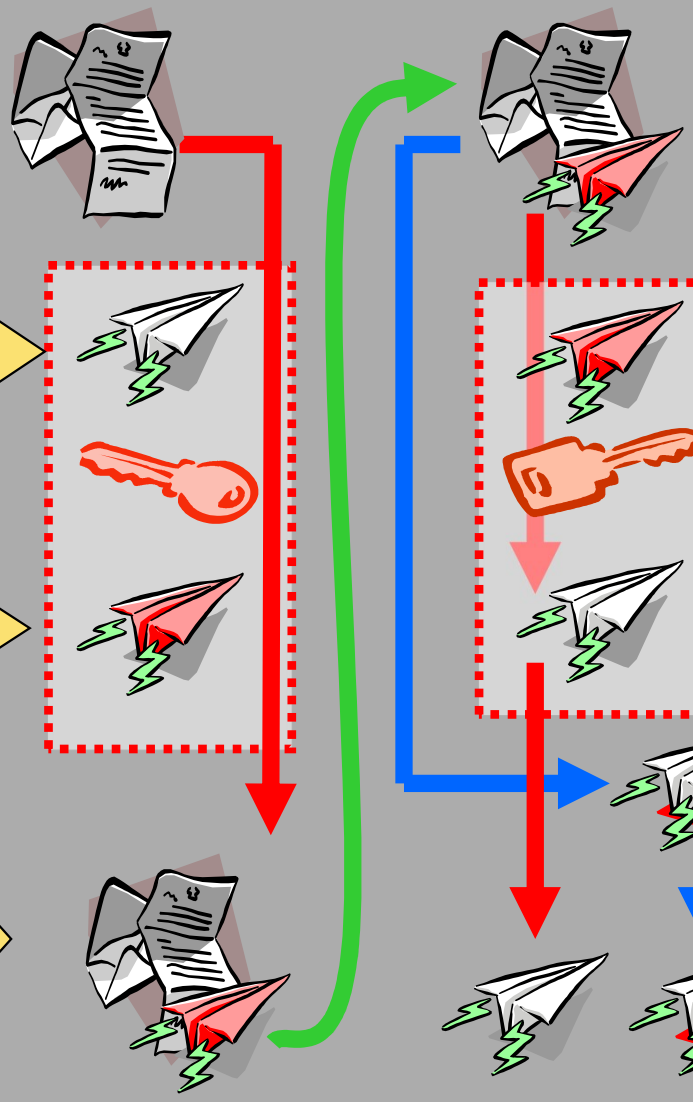
private key

to the original message

a signed summary is added and

everything is sent to the recipient as

text



an encrypted digest is

extracted from the message

the digest is decrypted

public key

sender

from the original message

a new summary is calculated

if the summaries are equal,

the identity of the sender is proven

and content integrity

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

Digital certificate

- It solves the problem of proving identity
- Connects user identity with his public key - confirms that a specific user is the owner of a specific public key
- A set of data that identifies the user and the certification service provider

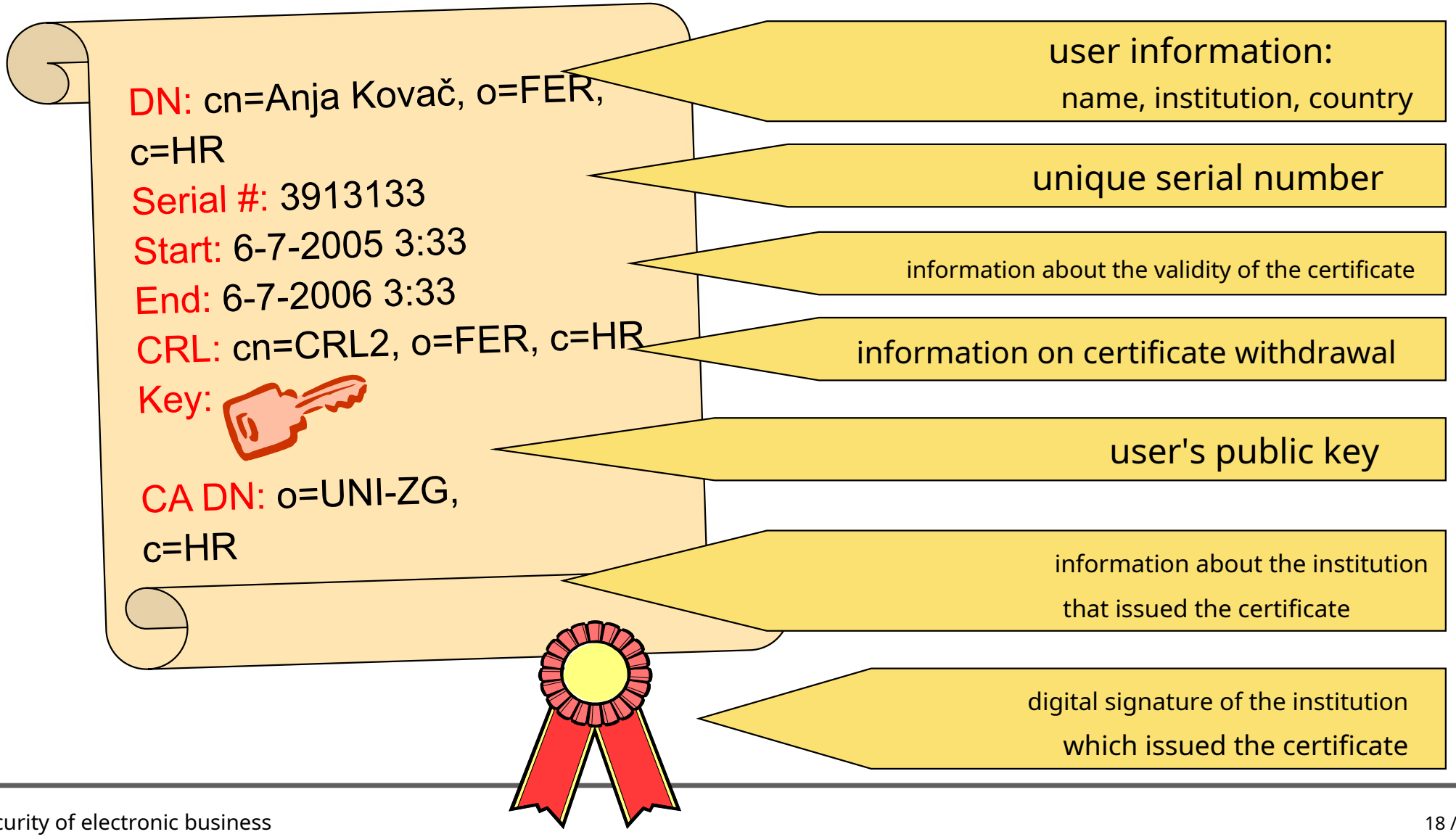
- Norm:
  - the norm is used for digital certificates X.509
  - names are displayed in certificates as pairs: name - value

Digitalni certifikat

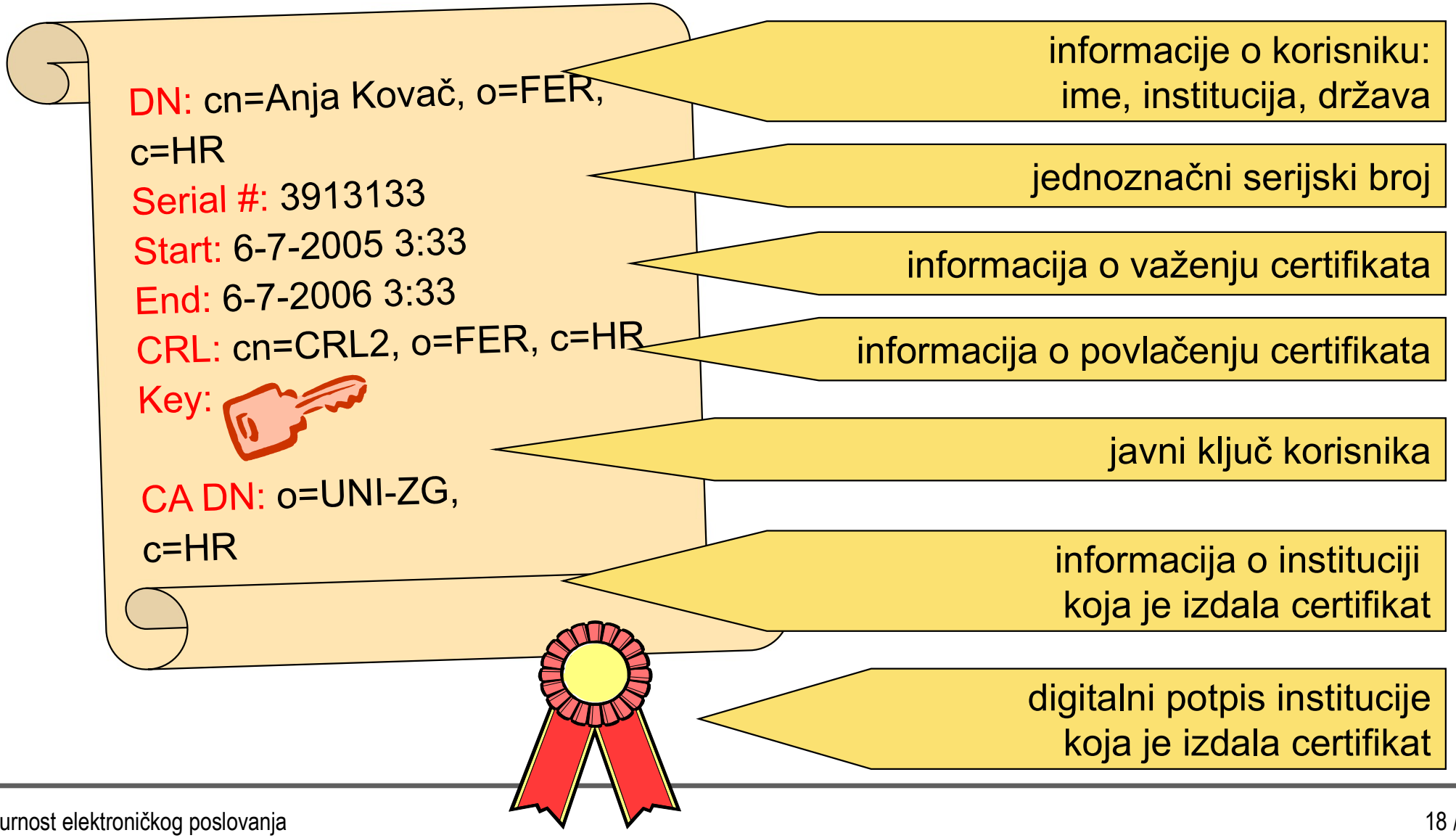
- Rješava problem dokazivanja identiteta
- Povezuje identitet korisnika s njegovim javnim ključem - **potvrđuje da je određeni korisnik vlasnik određenog javnog ključa**
- Skup podataka koji identificira korisnika i davatelja usluge certificiranja

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

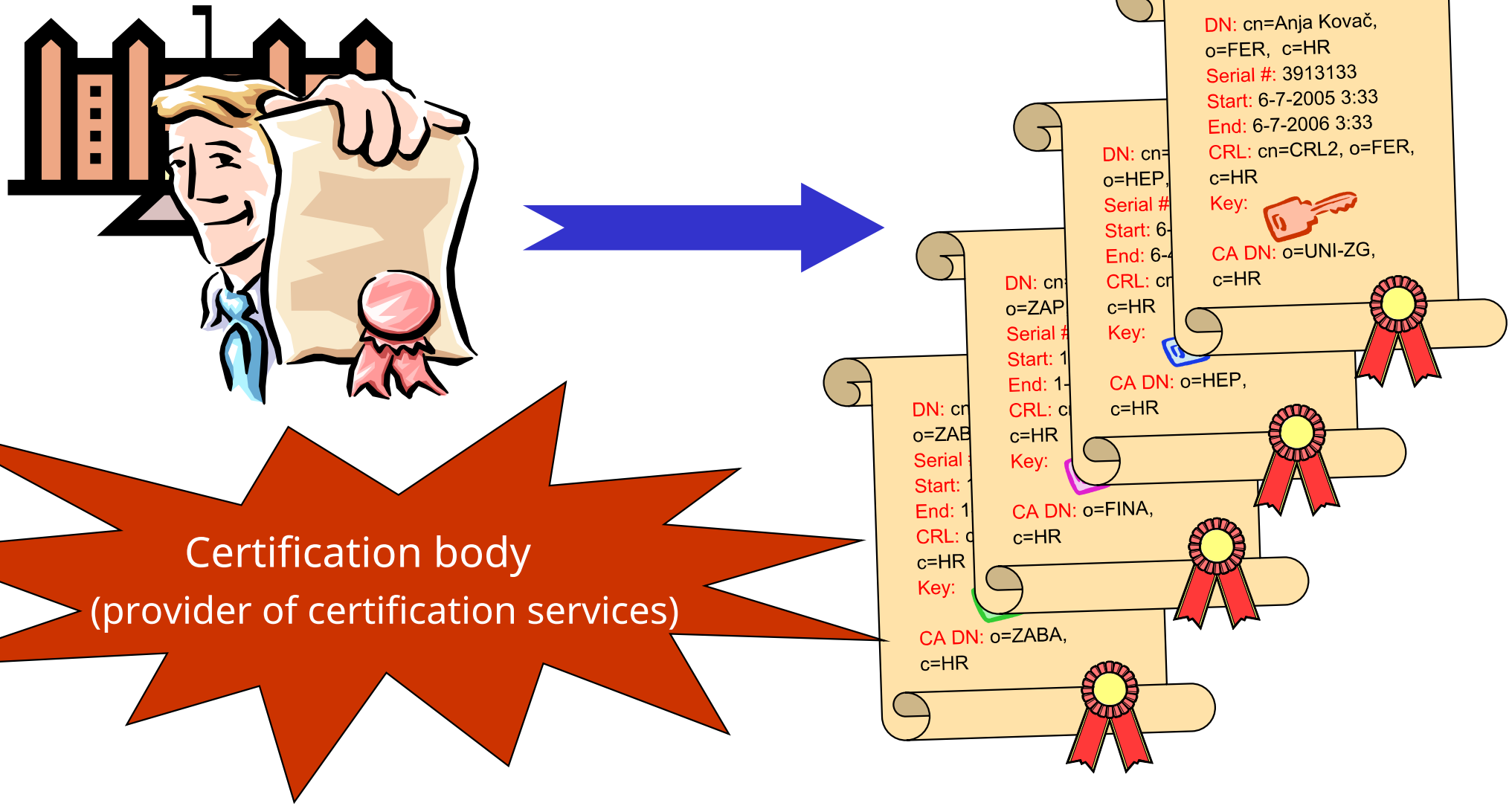
Content of the certificate



Sadržaj certifikata

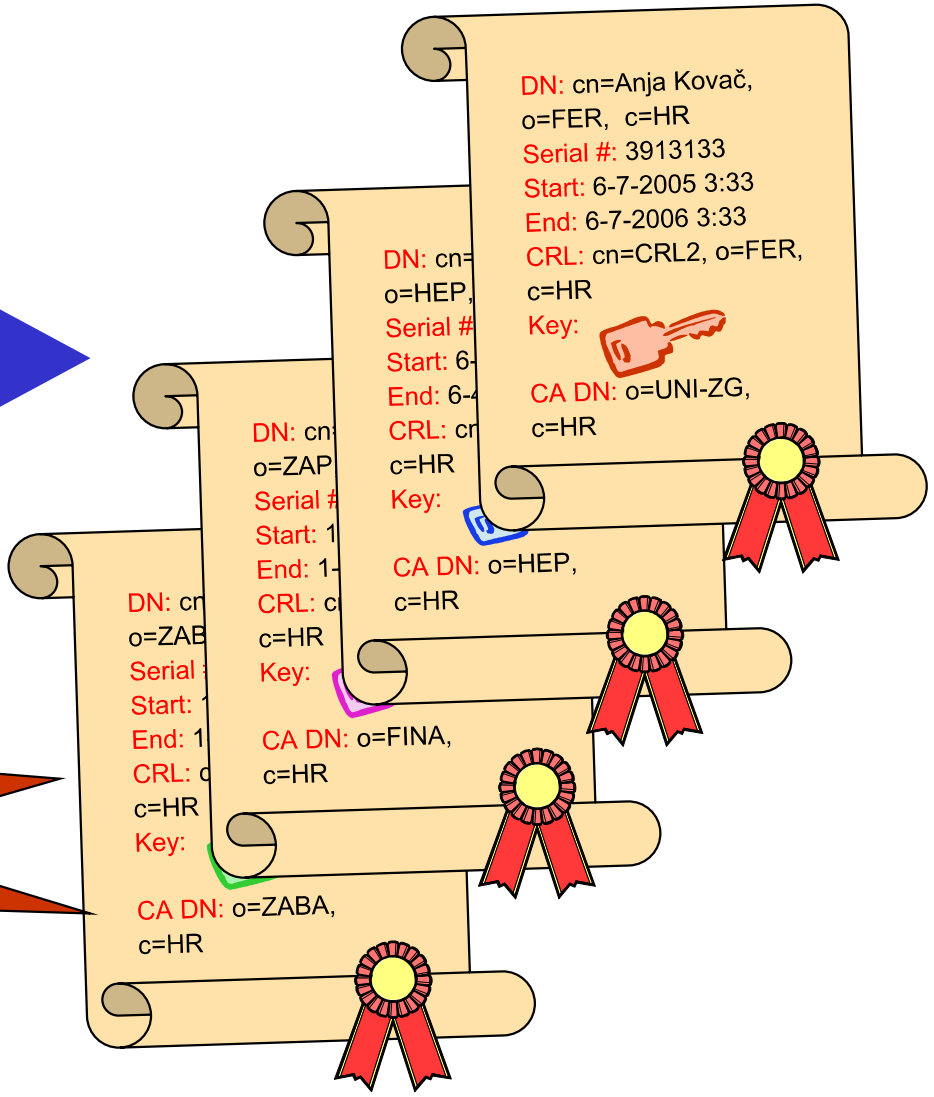


Certification Authority (CA –Certificate Authority)



Izdavanje certifikata

Certifikacijsko tijelo (CA – *Certificate Authority*)



Certifikacijsko tijelo
(davatelj usluga certificiranja)

Digital certificate

- If the sender signs the message with his private key, the receiver canto know that it is precisely this sender:
  - if possibledecipherdigital signatureby the sender's public key and
  - ifdigital certificate confirmsthat the public key used is exactlypublic key of that sender.
  - if a digital certificatenot expired or revoked

- The assumption for this procedure is that users havetrust in the certification body (i.e. the certification service provider) that issued the certificate and signed it with its private key or to the certification body that was certified by the certification body that issued the certificate.

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.

Public Key Infrastructure

- PKI - Public Key Infrastructure
  - a set of hardware, software support, people, policies and procedures necessary to create, manage, issue, use, store and revoke digital certificates
  - basis for creating safe and confidential data exchange between participants in the system
  - provides:
    - the integrity of electronic communication, making it impossible to change data during their transmission over the network
    - confirming the identity of the parties participating in the communication
    - non-denial of any party's participation in the communication

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

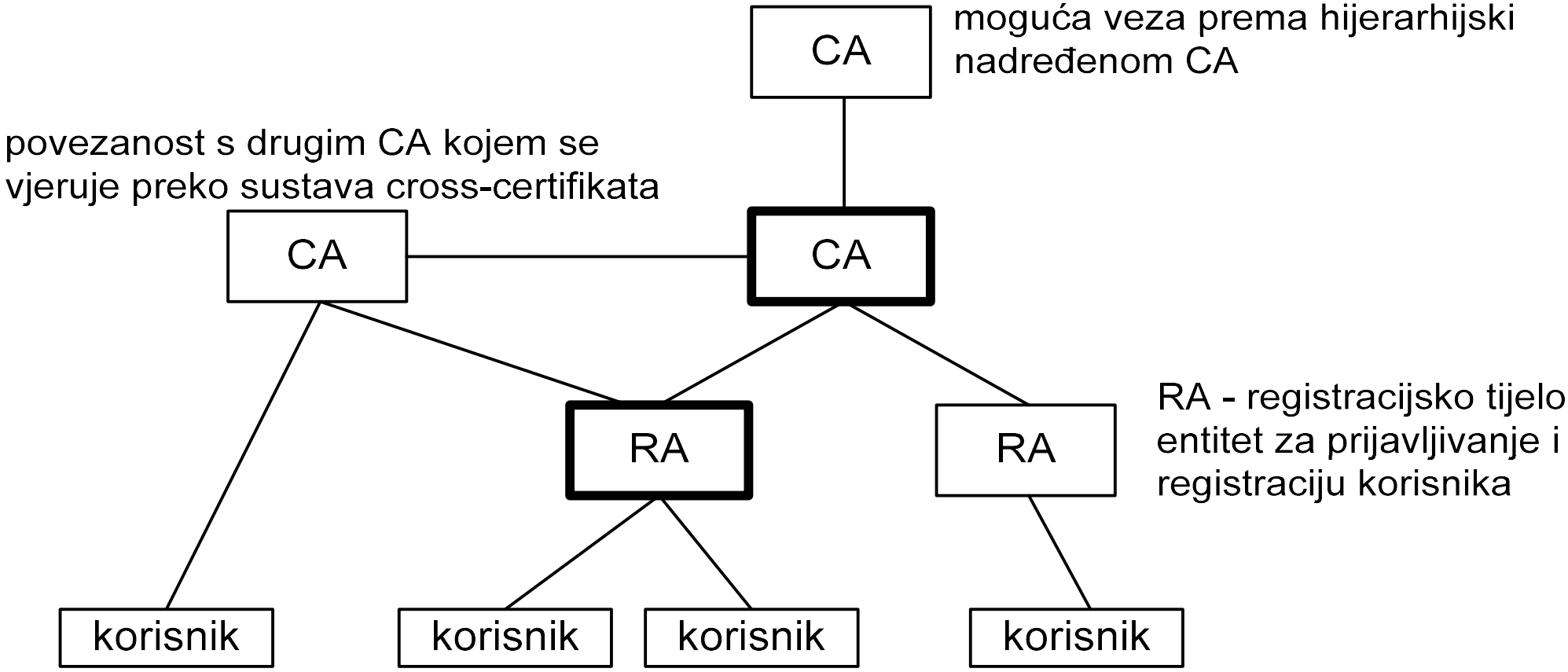
Parts of PKI

- certification authority (CA –Certificate Authority)
  - issues and withdraws certificates, maintains information on the status of certificates, publishes valid certificates...
- registration authority (RA –Registration Authority)
  - performs user registration (checks the content of certificates for CA, performs identification and authentication of parties applying for certificates)
- repository
  - contains a database of issued certificates and a database of revoked certificates (CRL - Engl. Certification Revocation List)
- clients (applications)
  - they verify digital signatures and certificates with a CA
- users of the PKI system
  - certificate holders
- Center for Trusted Time Stamping (TSA –EnglishTimestamp Authority)
  - creates timestamps

Dijelovi PKI

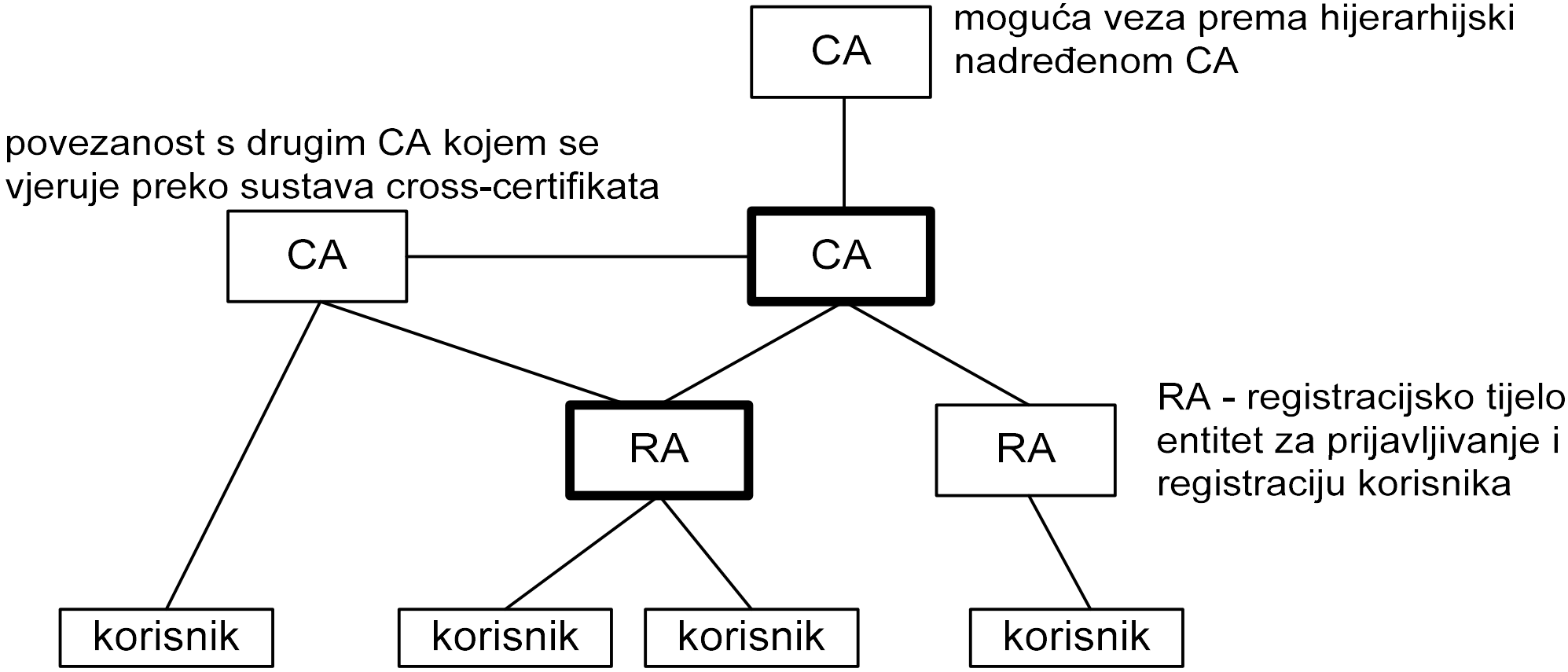
- **certifikacijsko tijelo** (**CA** – *Certificate Authority*)
  - obavlja izdavanje i povlačenje certifikata, održavanje informacija o stanju certifikata, objava važećih certifikata...
- **registracijsko tijelo** (**RA** – *Registration Authority*)
  - obavlja registraciju korisnika (provjerava sadržaj 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

- one CA can have multiple RAs for different groups of users, one RA
- can be associated with multiple CAs



Odnos RA i CA

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



Hierarchy of certification bodies

- One CA can sign another CA's certificate
- It can be donehierarchy of certification authorities (CA)
- If we don't trust a CA, we might trust a CA that is in the hierarchy above it. In this way, we also gain trust in the CA at a lower level of the hierarchy
- The CA at the highest level signs its own certificate – it is then a self-signed certificate. A CA with a self-signed certificate is a root 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

Trusted Time Stamp Center (TSA)

- It creates timestamps to prove that certain data existed before a certain time

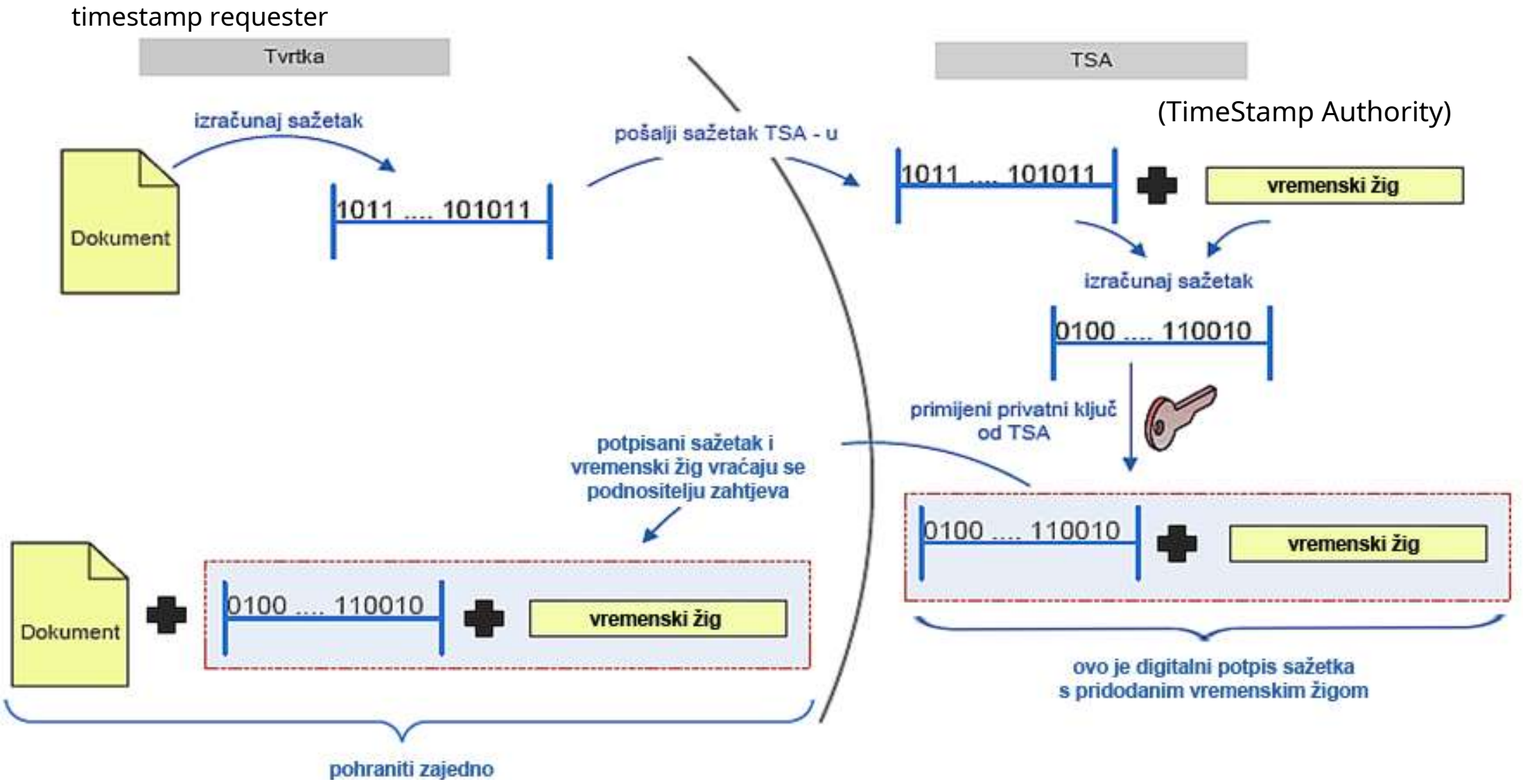
- TIME STAMP
  - Time stamp, time stamp, time stamp, time certification, Engl. timestamp
  - It ensures the reliability of the digital signature even after the expiration or revocation of the signer's certificate
    - Using a timestampit can be proven that the signature was made before the certificate expired

Centar za pouzdano vremensko označavanje (TSA)

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

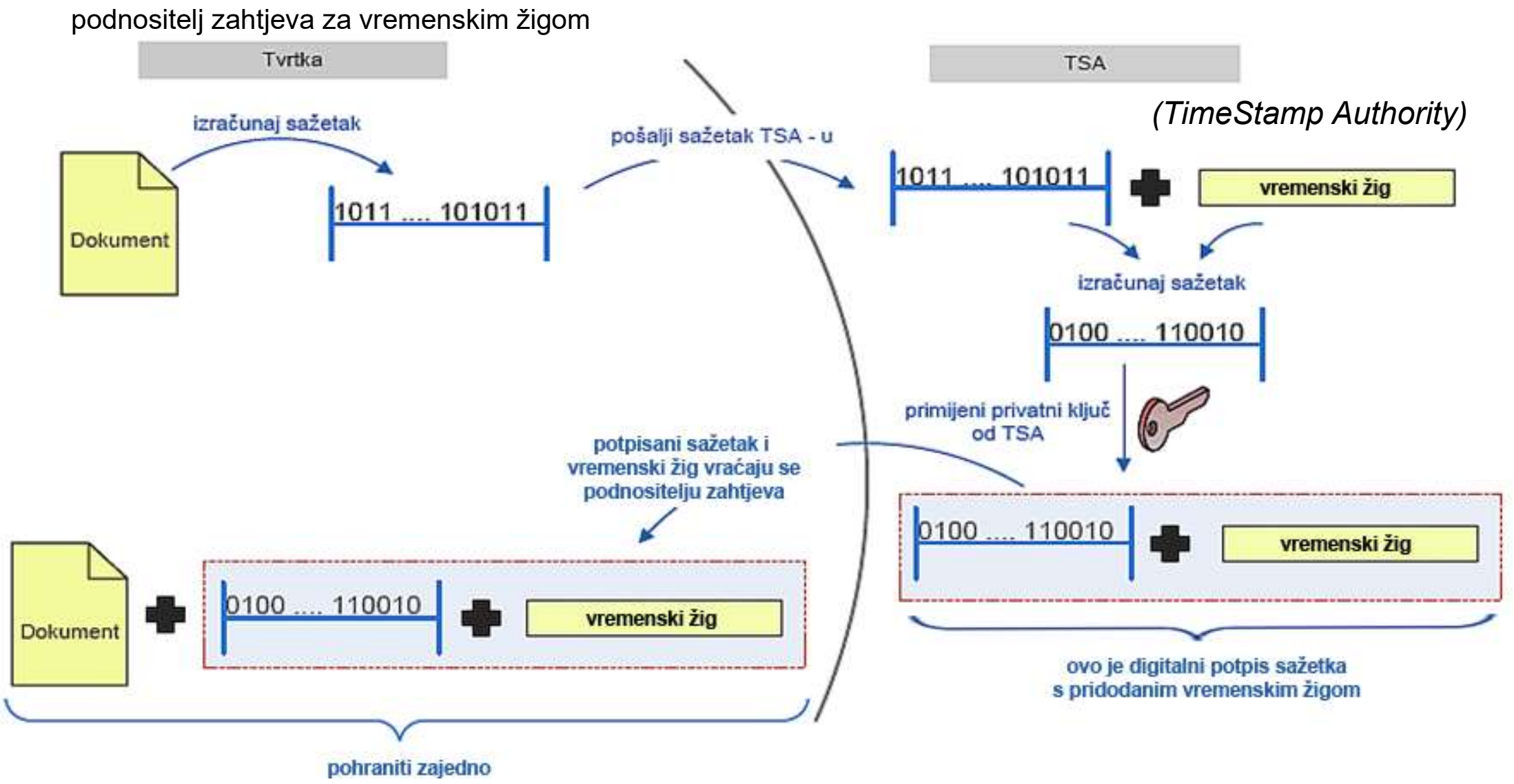
- **VREMENSKI ŽIG**
  - Vremenski žig, vremenski pečat, vremenska oznaka, vremenska ovjera, engl. ***timestamp***
  - **Osigurava pouzdanost digitalnog potpisa i poslije isteka valjanosti ili opoziva certifikata potpisnika**
    - Pomoću vremenskog žiga **može se dokazati da je potpis napravljen prije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

Timestamp assignment procedure



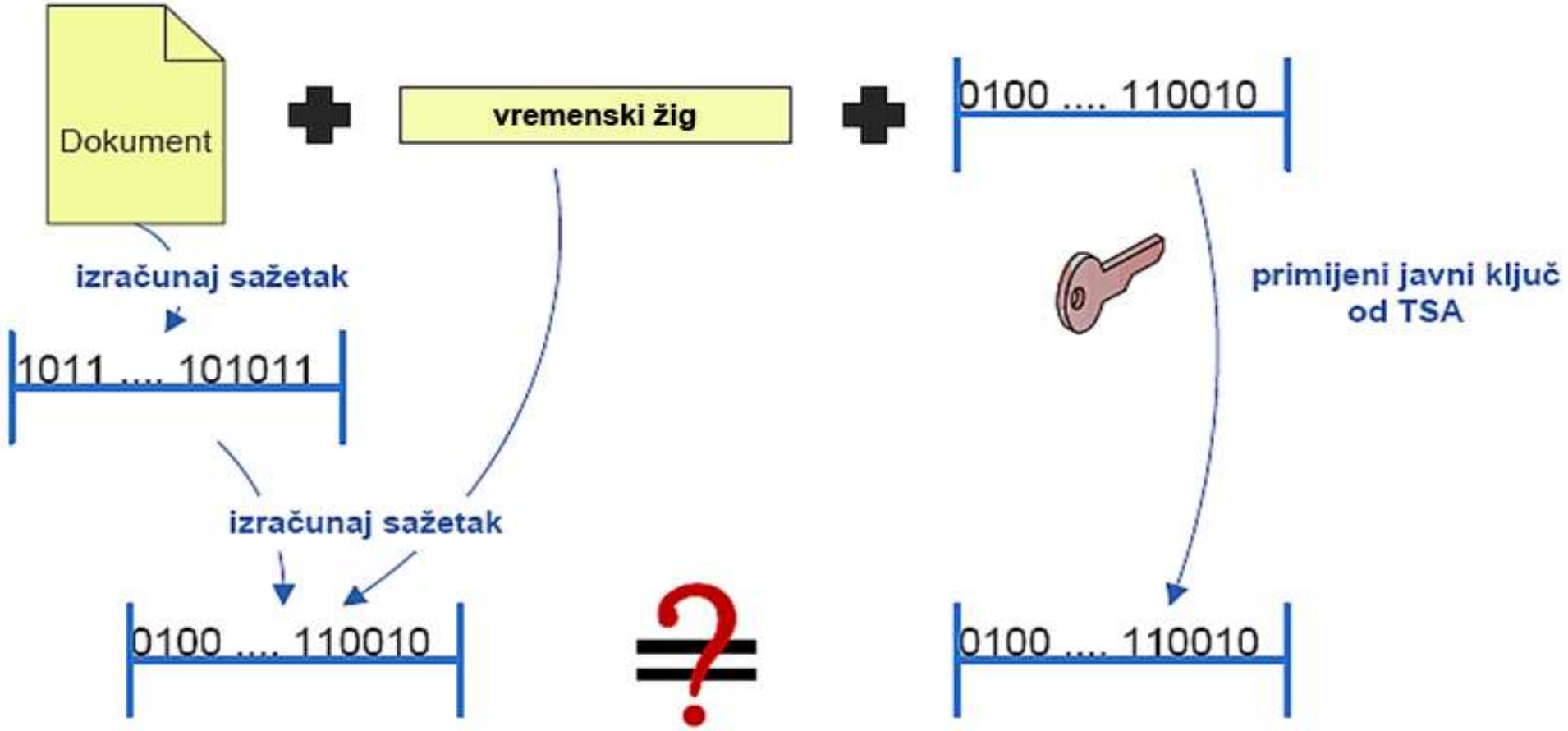
- TSA does not receive original data from applicants but always handles summaries

Postupak dodjeljivanja vremenskog žiga

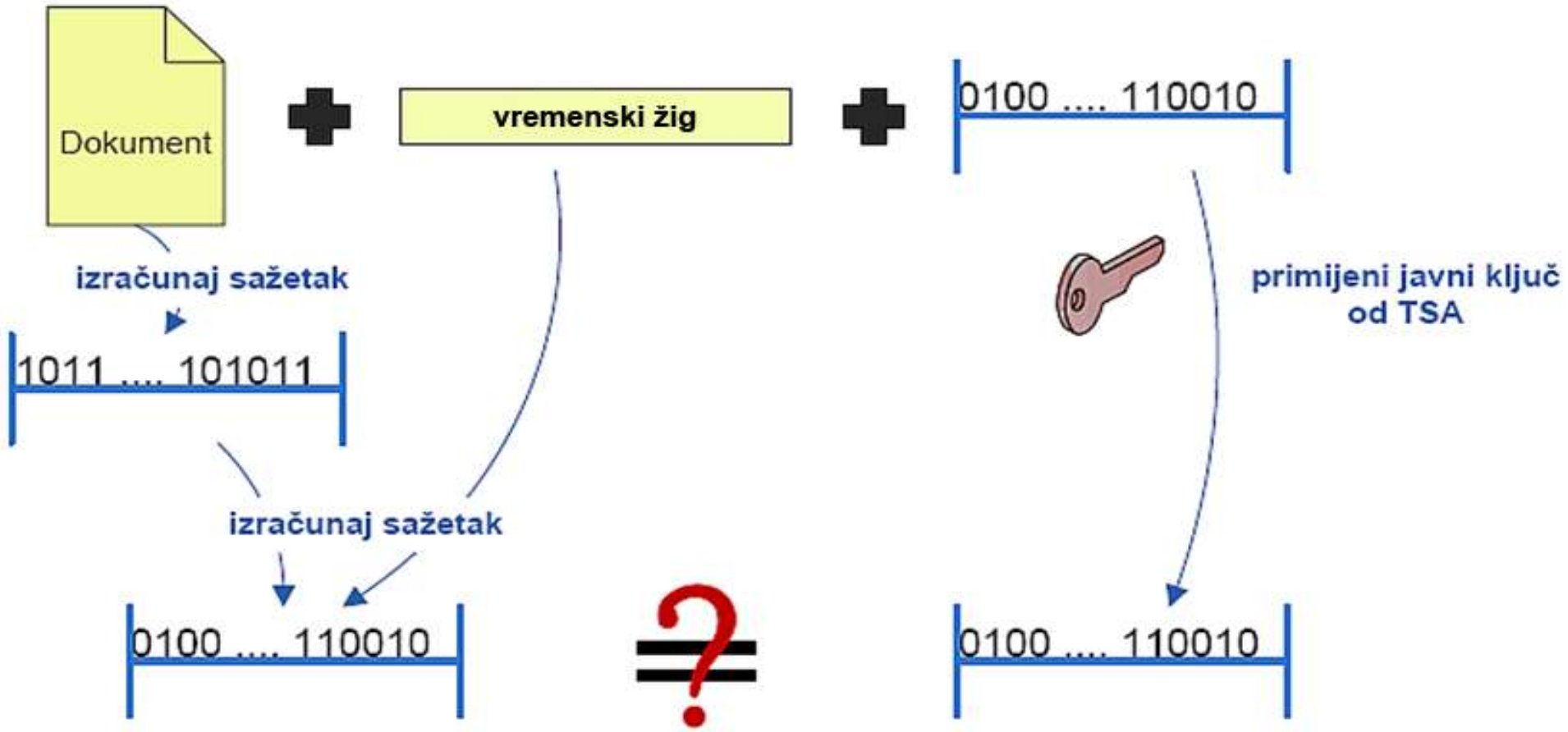


- TSA ne prima originalne podatke od podnositelja zahtjeva već uvijek barata sažetcima

Timestamp verification procedure



Postupak provjere vremenskog žiga



Timestamp verification procedure

- If the summaries are the same, it is proven that both the timestamp and the document are intact and that TSA issued the timestamp
  - It cannot be denied that the time stamp applicant was in possession of the original document at the time indicated by the time stamp.

- If the summaries are not equal, it means
  - that the timestamp or document has been changed
  - or that the time stamp was not issued by said TSA

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

1. Financial Agency (FINA)
   - Date of registration: 16 July 2008.
   - Services:qualified e-signature certificate, qualified e-seal certificate, qualified website authentication certificate, qualified time stamp, electronic signature certificate (nationally recognized
   - It issues certificates to individuals and legal entities for general purposes
2. Agency for Commercial Activity (AKD)
   - Date of registration: 29 May 2015.
   - Services:qualified e-signature certificate, qualified e-seal certificate, qualified time stamp
   - Certificates for eOI –smartID card
3. Zagrebačka banka (ZABA)
   - Date of registration: June 7, 2016.
   - Services:qualified e-signature certificate, qualified time stamp
   - Certificates primarily for banking services

The records of certification service providers in the Republic of Croatia are maintained by the Ministry of Economy and Sustainable Development

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

FINA TSA –public time verification service provider

-FINA (asTSA)is a service providercertification of electronic signature

- FINA TSA verifies the signatory's signature with a time stamp
- it is confirmed that they aredata and electronic signature existed before the time stamp was applied

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**

- Electronic signature
  - data in electronic form that are associated or logically connected with other data in electronic form and which the signer uses to sign
- Advanced electronic signaturemust meet the following requirements:
  - is undoubtedly related to the signatory
  - enables identification of the signatory
  - it is created using data for creating an electronic signature that the signer can, with a high level of confidence, use under his sole control
  - it is linked to the data signed by it in such a way that any subsequent modification of the data can be detected
- Qualified electronic signature
  - an advanced electronic signature that is created using qualified electronic signature creation tools and is based onqualified certificatefor electronic signatures

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

- member states have accepted qualified electronic signatures as legally equivalent to manual signatures and accept them as evidence in legal proceedings
  – the legal basis for the use of digital signatures exists
- some countries still have formal obstacles to the wider introduction of digital signatures (e.g. requirements for a written signature on two copies on a special form)
- the use of digital signatures in EU countries has not yet reached its peak, but there has been an increase in use over timelockdowncaused by the COVID pandemic
- legal uncertainty -the lack of a large number of previous court cases is a significant problem

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

Regulation eIDAS

- eIDAS – Electronic Identification and Signature (Croatian electronic identification and signature)
- Regulation of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market - adopted on 23 July 2014.
  - A binding legislative act for all member states
- Enacted due to inconsistency of national legislation
  - Differences in the implementation of norms and rules in practice
  - How to reliably validate the e-signature of a signatory from another country?
  - Lack of reliable information necessary for complete validation of the e-signature
- Goal: establishment of trust and mutual recognition of e-signatures and e-seals within the EU

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**

- To 7/7/2017 in the Republic of Croatia, the Law on Electronic Signature (from 2002)

- 23/07/2014 The European Parliament and the Council adopt the eIDAS regulation

- From 1 July 2016 The Law on Electronic Signature ceases to be valid in the part that contradicts the eIDAS regulation

- 19 June 2017 The Croatian Parliament passes the Law on the Implementation of the Regulation (...)

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 (…)

Electronic seal

- Three types of seals:
  - Electronic seal
    - data in electronic form that are associated with other data in electronic form or are logically connected to them in order to ensure the originality and integrity of that data
  - Advanced electronic sealmust meet the following requirements:
    - it is undoubtedly related to the author of the seal
    - enables identification of the author of the seal
    - it was created using data for creating an electronic seal that the author of the seal can, with a high level of confidence and under his control, use to create an electronic seal
    - is linked to the data to which it refers in such a way that any subsequent modification of the data can be detected
  - Qualified electronic seal
    - an advanced electronic seal that is created using a qualified electronic seal maker and is based on a qualified electronic seal certificate

Uvodi se uredbom eIDAS

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

Electronic signature and seal

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

taken from: Perinčić, M., eIDAS regulation – Trust and mutual recognition of e-signatures and e-seals in the EU, expert meeting e-biz 2015, Zagreb, April 2015.

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.

Electronic signature and seal (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.

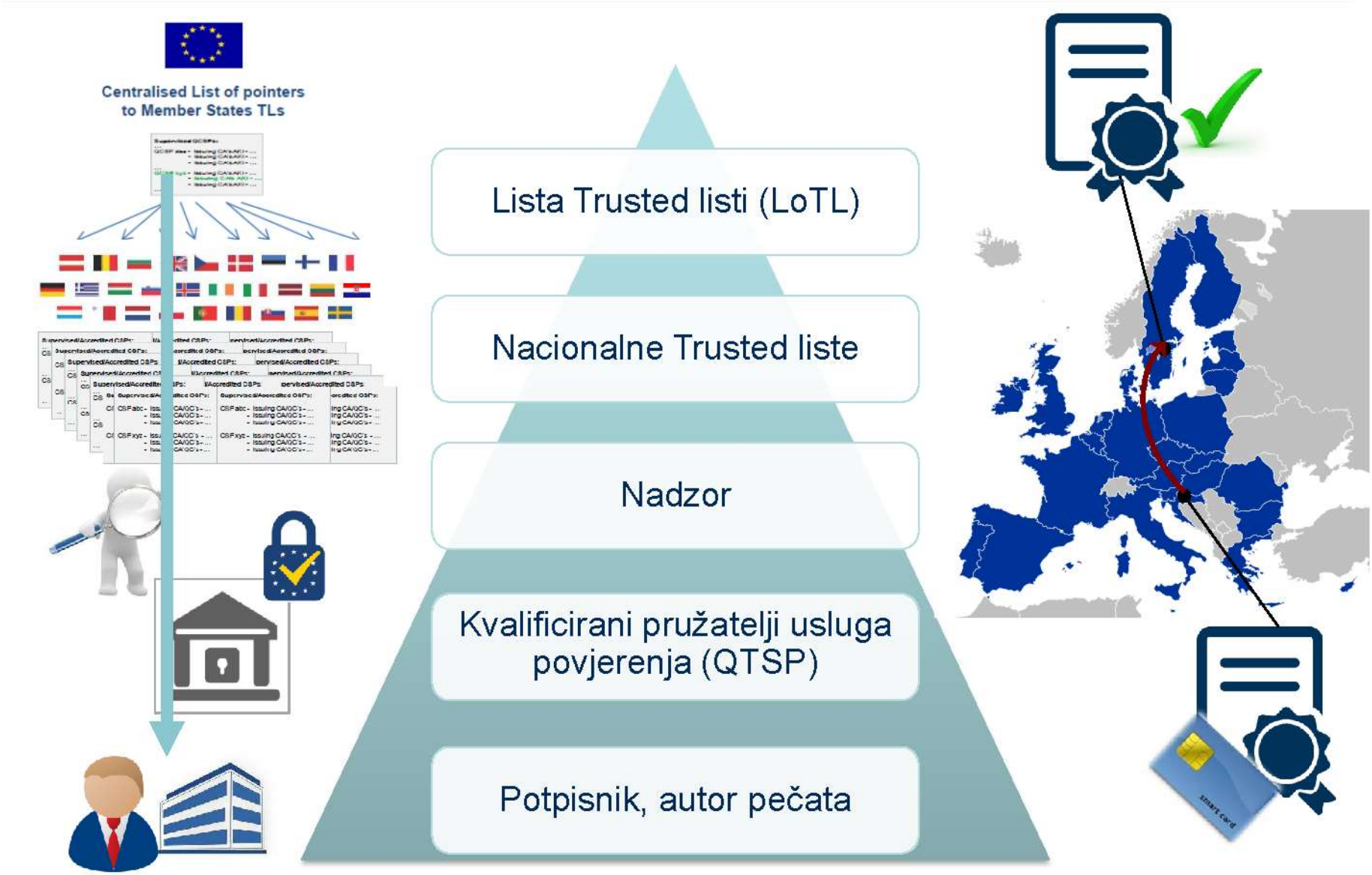
taken from: Perinčić, M., eIDAS regulation – Trust and mutual recognition of e-signatures and e-seals in the EU, expert meeting e-biz 2015, Zagreb, April 2015.

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.

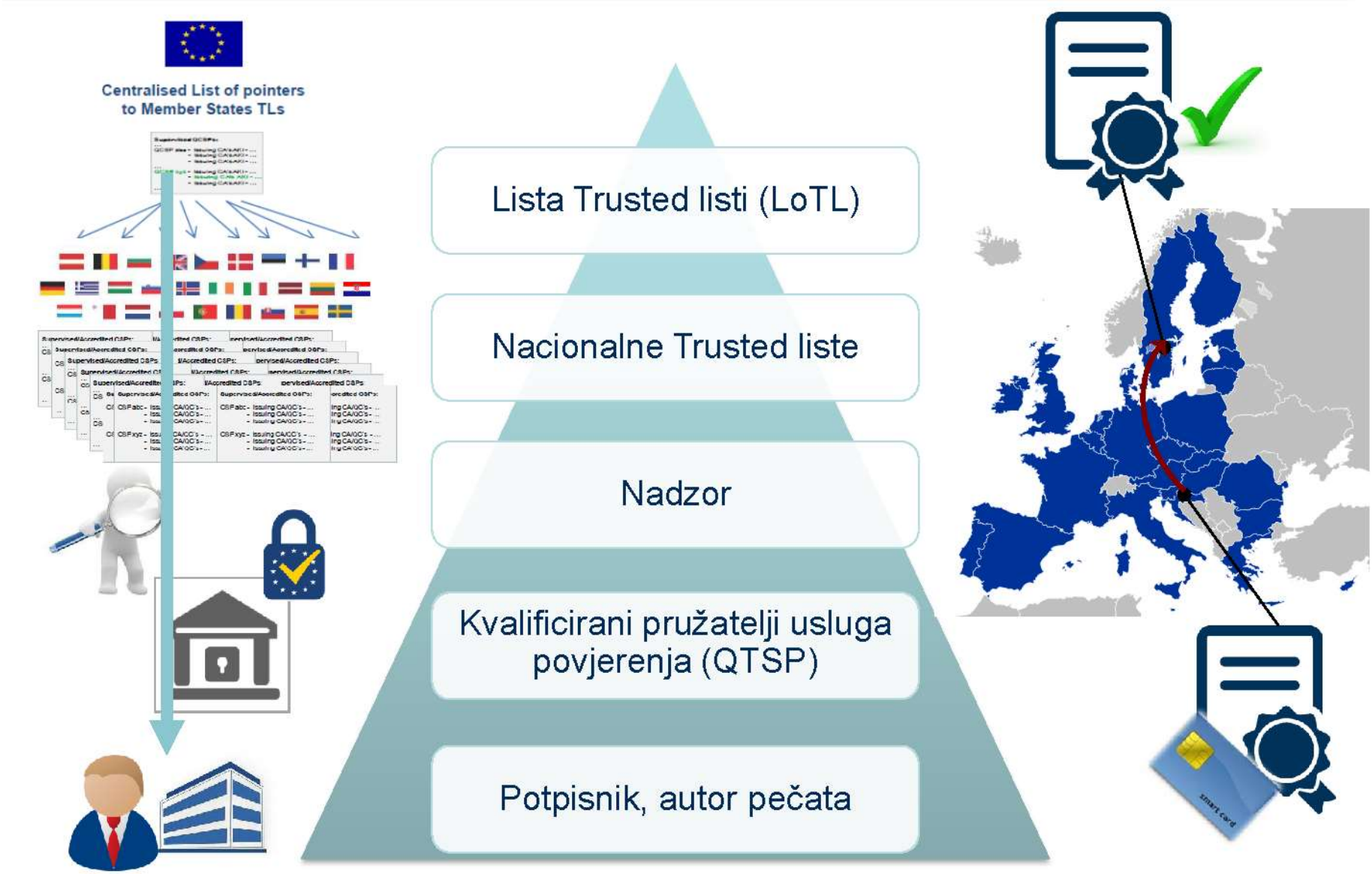
preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, travanj 2015.

Trust system according to the eIDAS regulation



taken from: Perinčić, M., eIDAS regulation – Trust and mutual recognition of e-signatures and e-seals in the EU, expert meeting e-biz 2015, Zagreb, 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.

Security of XML documents

- Electronic business is mainly based on exchangeXML documents.

- Security standards embedded in XML:
  - XML-EncryptionandXML-Signature
  - are added to the document without violating XML rules
  - such documents can be viewed using standard XML tools

- security of XML documents can be implemented using standard security protocols
  - these algorithms use binary files that can then only be interpreted using special tools

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

Security of XML documents

- TLS protocol can be used for secure transfer of documents through the network
  - that's itit only protects the transmissiondata through the network, anot storage
  - a document sent using only TLS ceases to be secure the moment it reaches its destination

- by applying security measures over the document itself using the XML security standard, the document is secured both in transmission and in later storage, because it is not the link that is secured, but the document itself

- normXML Digital Signatureis used to store a digital signature in an XML document
- normXML Encryptionis used to store encrypted content in XML format

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

Canonicalization

- two logically identical XML documents can be written differently,
- for example, one containsextra space or extra empty line

- two documents logically equal, but a summary of those two documents obtained hash-algorithm is not equal!

  → with digital signing it forresults in unsuccessful signature verification, although the document is logically not changed, i.e. it would be expected that the verification should succeed

- to avoid such problems,XML documents should be canonicalized i.e.reduce to the same (canonical) form (standardization of spacing, etc.)

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-DSigis a W3C standard
  - W3C =World Wide Web Consortium
- defines how to embed a digital signature in an XML document (so that XML rules are met)
- not an algorithmfor digital signing
- with one signature, it is possible to sign several documents, it is
- also possible to sign documents that are not in XML format
- it is possible to sign only part of an XML document (in this way it is possible for different parts of an XML document to be signed by different people)

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

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)

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

- An XML signature is implemented in an XML document via an elementsignatures

- ? -represents zero or one occurrence,

  \+ - one or more occurrences,

  * - zero or more occurrences

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>
```

- ElementSignedInfo–within its sub-elementsidentifies the data to be signed and different algorithmswhich will be used
- CanonicalizationMethod-contains a nameof the algorithm used to canonicalize the data

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-definessignature generation algorithm

- SignatureValue-contains the signature value of the elementSignedInfo

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

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)

- References-identifies the resources to be signed and all algorithmswhich will be usedfor preprocessingdata. These algorithms are written in the element Transformsand include operations such as encryption/decryption, compression/inflation orXPath transformation (XPath allows signing part of the document).

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

- ElementReferenceshas an attributeRUN which is optional butif the signature contains several elementsReferencesthen the URI is optional for only one element, and the others must have it.

- If the content of the URI"", i.e. an empty character string, it means that the document containing the element is being signed

```
<Signature ID?>
    <SignedInfo>
            <CanonicalizationMethod/>
            <SignatureMethod/>
            (<ReferencesURI?>
              (<Transforms>)?
            <DigestMethod>
              <DigestValue>
            </References>)+
        </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)

EachReferencesincludes :

- DigestMethod-contains information about the algorithm used to calculate the summary of the document
- DigestValue-contains a summary of the document calculated by the algorithm specified in DigestMethod

KeyInfo-contains information about the io key certificate

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

```
<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)

```
  <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)

- An XML signature can appear in three basic forms:
  - Wrapped signature (Enveloped) –the signature is inside the document.
  - Wrapping signature (Enveloping) –a signature delimits the document it signs.
  - Separate signature (Detached) –the signature is in a separate document, and the URI (Universal Resource Identifier)determines which document he signs.
  - it is possible to get new ones by combining these three forms
  - one of the possible combinations: insert the wrapping signature into the document so that it signs some precisely specified data

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>
```

- Example of a wrapped signature - a document containing <Signature> is signed

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)

- In the case of a wrapping signature, the content of the element is signedObject

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

- Example of a wrapping signature - the content of the <Object> element is signed

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>
```

- Example of a separate signature – the signature is in a separate XML file, and what is being signed is identified by a URI in the <Reference> elements

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

- An example of a hybrid signature – a combination of a wrapped and separate signature

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)

-XML-Dsig Recommendation Extension Set (only

reported for W3C recommendation)

ETSI (European Telecommunications Standards Institute)norm
TS 101 733

- It defines six profiles that differ in the level of protection they offer:
  - -XAdES - advanced electronic signature in accordance with Directive 1999/93/EC
  - -XAdES-T - includes a time stamp
  - -XAdES-C - adds to XAdES-T links to certificates and list of revoked certificates
  - -XAdES-X - adds to XAdES-C timestamps on introduced links
  - -XAdES-XL - adds certificates and a list of revoked certificates to the signed document
  - -XAdES-A - requires a sequence of timestamps for long-term archiving

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

XMLEncryption (XML-Enc)

- XML-Encdescribes how encrypted contentembed in XML
- It's notencryption algorithm

- Non-XML documents can also be encrypted
- It is possible to encrypt only part of the XML document
- Different parts of the XML document can be encrypted with different keys - access control

- XML Encryption Syntax and ProcessingVersion 1.1. (11.4.2013)

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

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/

XMLEncryption

Encryption can be performed in three ways:

- usingsymmetric cryptography -the data is encrypted with a symmetric key that was previously exchanged by the communication participants in some (secure) way

- usingasymmetric cryptography -the data is encrypted with the recipient's public key
- usinghybrid approach -data is encrypted with a symmetric key, and that symmetric key is encrypted with the receiver's public key; the encrypted symmetric key and the content encrypted with that symmetric key are embedded in the XML document; this approach is the most common

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

XMLEncryption –structure

```
<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* – 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)

- SpecificationXML Encryption Syntax and Processinghe betrayedW3CXML Encryption Working Groupwith the aim of establishing the encryption/decryption process of digital content (including XML documents as well as their parts) and syntax, in order to display:
  - encrypted contentand
  - enabling informationto a specific recipientdecoding received content.

- The result of encryption is a data element that contains (via one of its sub-elements) or identifies (via a URI reference)encrypted data.

- When we encrypt an XML element or element contentencrypted data (element EncryptedData)they replace the element or contentin an encrypted version of the XML document.

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.

XMLEncryption –example

```
<?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

- the content of the element is encrypted<position>
- a hybrid approach is used

- symmetrical key

is encrypted with public ones

key

recipient

(RSA algorithm)

and together with

encrypted

sends the content

to the destination

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

XMLEncryption –example

Example explanation:

- the content of the <position> element is encrypted
- hybrid approach - data is encrypted with a symmetric key, and then this symmetric key is encrypted with the receiver's public key, and it is sent to the destination together with the encrypted content
- in the picture, the algorithm that encrypts the symmetric key is marked in blue - the asymmetric RSA algorithm
- the encrypted key is shown in green
- the content of the XML document that needs to be hidden is encrypted with the symmetric AES algorithm, which is shown in orange in the picture. This is how the encrypted content is obtained, which is marked in gray in the picture.
- the <EncryptedData> element (red in the image) is located exactly where the element to be encrypted was previously located

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

Security in electronic commerce

Sigurnost u elektroničkoj trgovini

Security requirements codeonlinepayments

- Authentication -in an online payment transaction, it is known who is participating in the transaction and it is known that the person is exactly who he claims to be.
- Integrity -the data from the transaction will not be changed
- Uniqueness of payment requests -enables the merchant to recognize repeated requests for the same transaction
- Non-repudiation of the transaction -after executing the transaction, the buyer cannot deny that he executed the transaction, that is, the merchant cannot deny that he received the transaction
- Confidentiality –transaction data cannot be accessed without authorization
- Customer privacy and anonymity -the merchant can only see the buyer's pseudonym or username, but not his private information
- System reliability -preventive actions in the event of a system crash and in case of errors during the execution of the transaction

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

Card payment in the electronic store

- Example:PayPal –one of the most widespread and well-known online payment systems in the world

- to send money you only need to knowe-mail addressPayPalaccount of the person/company to whom the money is to be sent
- for paying money toPayPalthe account uses a credit or debit card
- onlinepayment: or sPayPalaccount or credit cards

- In October 2002eBayboughtPayPal (at the time of purchase more than 50% of users eBayhas already usedPayPal)

- He is in CroatiaPayPalcame in mid-2006.
  - initially only sending money, and since March 2011 users from Croatia have been able to receive money on their ownPayPalaccount

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

Card payment in the electronic store

SafetyPayPaltransaction

- the credit card number is not given to the merchant during the transaction
  - only the customer's e-mail address is forwarded to the merchant
  - the merchant receivesonlinepayment without being able to see the customer's financial data
  - after each transaction, the user receives an e-mail message to his e-mail address with information about the completed transaction

- all data (personal and financial) sent from the client computer toPayPalserver are encrypted.
  - when registering or logging in toPayPalwebsite uses TLS 1.2 (or higher)
  - the SHA-256 algorithm is used for SSL certificates
- servers with sensitive financial dataare not directly connected to the Internet

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**

Card payment in the electronic store

SafetyPayPaltransaction (continuation)

- Check:
- Address Verification Service (AVS)is the system used forverification of the person's address which claims to own a certain credit card. The system will compare the address provided by the credit card user when executing an online payment transaction (or when linking a credit card withPayPal account) with the address registered with the card issuer. AVS checks only the numerical part of the address (postal code, house number).
- Card Security Code (CSC)orCard Code Verification (CCV)- the three- or four-digit security code usually found on the back of the credit card written in reverse italics.
  - This code is used as a security check when it is not possible to use a PIN- And.
  - Merchants that require a CVV2 code on transactions of typecard-not-presentthey must notthat codeFeed.
  - This security measure is one of the security measures of the security standardPCI DSS (Payment Card Industry Data Security Standard).

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*).

Card payment in the electronic store

- About security...

  ... from websites

  provider of online billing services

- **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.

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

- -security standard for card business
- -defines minimum security measures and processes

- He defined itPayment Card Industry Security Standards Council
  - -Visa, MasterCard, American Express, Discover Card and JCBhave together created an industry standard for data security to protect their users.
  - -provides merchants, card houses, banks and other business entities that deal with card businesscardholder data protection
- The first version of the PCI DSS standard was issued in
- 2004. Version 3.2.1 was issued in May 2018.

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

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

- Banks and service providersthey have tocertify the codequalifiedauditor security, and merchants are obliged to comply with PCI DSS standards and conduct card transactions only with certified service providers.

- PCI DSS regulates requirements related to data security management, security procedures, network architecture, design of software support for data processing and other critical protective measures in card business.

- The core of PCI DSS consists of a group of principles and supporting requirements around which specific elements of data security in card business are organized.
  - 12 basic requirements and about 270 sub-requirements

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

Some of the requirements from PCI DSS:

Requirement 1:Install and maintain an appropriate firewall configuration (Eng.firewall)to protect cardholder information.

Request 2:Do not use passwords and other security parameters provided by the vendor of the software security solution

- Change initial passwordsset by the supplier

Request 3:All stored data about the cardholder must always and unconditionally be protected.

- card security codes (three- or four-digit number usually printed on the back of the card) used to confirm (verify) the transactionand PIN numbers must not be stored.

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**.

Some of the requirements from PCI DSS (continued):

Request 4:During transmission via open, public networks, all cardholder data must be protected by encryption.

- Use strong cryptographic methods and security protocols (eg SSL/TLS, IPSEC, SSH) to protection of sensitive card (user) data during transmissionthrough open, public networks (Internet, wireless transmission, GSM and GPRS).

Request 5:It is necessary to use and regularly update software to protect against malicious code, i.e. antivirus software

...

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**

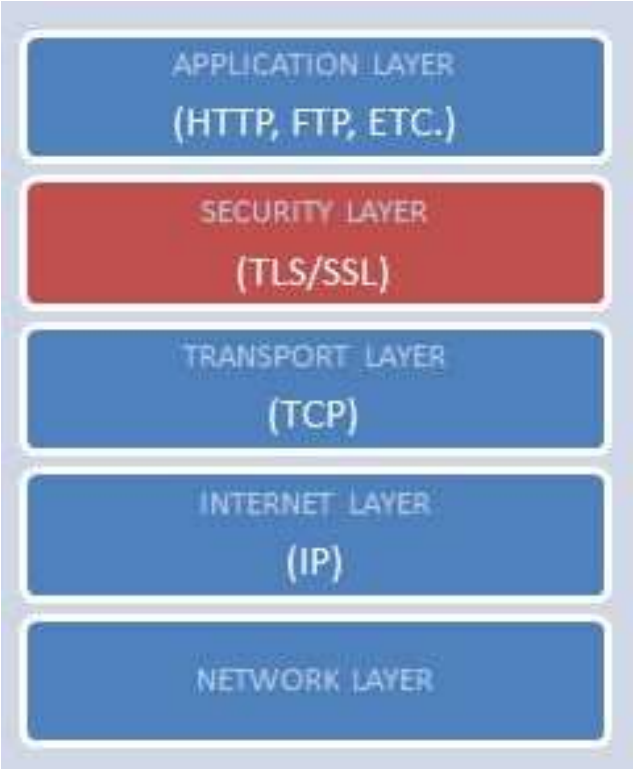
…

TLS / SSL

- The credit card number is entered via a web browser and travels to the online store's web server

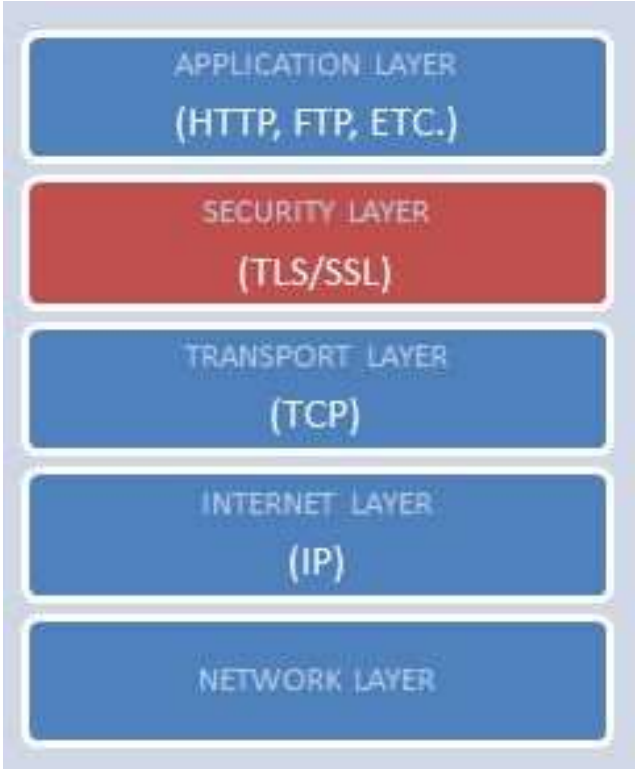
- with electronic paymentit is necessary between the transport protocol TCP and the application protocol HTTP to use isecurity protocol TLS / SSL

- TLS / SSLprovidescodingof all communications above the transport layer.



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

- SSL protocol (Eng.Secure Socket Layer)developed by Netscape Communications - version SSL 3.0 was released in 1996
- protocol TLS (Eng.Transport Layer Security)was released in 1999 - an upgrade to SSL 3.0
  - In 2006, TLS 1.1
  - in 2008TLS 1.2-useshash-functionSHA-256(from SHA-2)
  - in 2018TLS 1.3

- TLS / SSL
  - is used for more secure exchange of confidential data, such as username and password, credit card number, etc.
  - is based on the use of cryptography and public key infrastructure. Public key infrastructure -PKI)
    - private and public keys

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

- Forcard paymentover the network is recommended to useTLS 1.2 orTLS 1.3(published in August 2018)
- Do not use SSL.

- When using SSL/TLS
  - the address starts with a labelhttps://
  - all communication between the browser and the web server is encrypted

- HTTPS (Hypertext Transfer Protocol Secure) -a combination of HTTP and SSL/TLS protocols (Secure Sockets Layer / Transport Layer Security)

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

- It serves to protect against attacks:
  - eavesdropping (eng.eavesdropping)
  - man-in-the-middle (eng.man-in-the-middle)

- interception and unauthorized eavesdropping of communications and possible theft of credit card numbers are prevented

- however, it does not solve the problemstoragecredit card numbers on the server itself

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

- When a secure connection is established (certificate received and verified by CA), a padlock icon appears in the browser and the address begins with https://

- When entering confidential data on websites, check whether the website is currently protected (https://)
- The browser usually has built-in security mechanisms that alert if the web site is not secure

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

- some CAs have introduced "domain check only" type SSL certificates (domain validation only)for which it worksminimal checkdetails in the certificate
  - for each successful SSL connection – a padlock icon appears
- many browsers did not clearly distinguish certificates with lenient validation from those that do rigorous validation
  - users are not aware whether the web site is sufficiently verified or not
  - possibilityphishing -web sites built to serve forphishing they can use TLS/SSL to get extra credibility
- Extended Validation Certificate (EV) prescribesstricter criteriafor identity verification
  - The name of the CA that issued the EV certificate is displayed
  - The color (usually green) indicates that the EV certificate is valid
- Today's web browsers display the EV status.

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 -attackers try to find out confidential information (most often passwords, credit card information or PIN) by impersonating a credible subject in the communication.
- fake messagean attempt is made to lure the user by e-mail or by sending a message through the instant messaging systemto a fake website,in order to enter your username and password, PIN, credit card number, etc.
- For example "To verify that your account has not been used without authorization, please click on the link below and confirm your identity"
- fake websites of banks oronlinestores that visually look identical to real sites
- If the fake page mimics internet banking, when the user logs in to the system, a script in the background can automatically log him into the real bank page, while the generated OTP (one-time password) is still valid. After that, the script, hidden from the user, starts the money transfer...

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

- The company that developed a particular web browser decides which certification authorities (CA -certification authority)will believe.

- The user should trust the HTTPS connection only if:
  - The user trusts that the browser correctly implements HTTPS with correctly pre-installed certificate checks from known and trusted CAs
  - The web site has a valid certificate (signed by a CA)
  - The user trusts that CA

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 certificates
  - they confirm the identity of the website to website visitors,
  - guarantee safe and confidential data exchange As a
- result, the trust of visitors to the Web site grows.

- The most famous companies that issue SSL certificates:

  VeriSign, Thawte, GeoTrust, RapidSSL, GlobalSign, GoDaddy, Entrust, ...

- root CA – can authorize other CAs to sign and verify certificates on their behalf (CA hierarchy)

- Confidence in the certification system?
  - trust in CAs lower in the hierarchy who have received authority from root CAs?
  - adoption of standards for CA verification (like PCI standards in card business)?

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)?