SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

Digitalni certifikati

Creative Commons

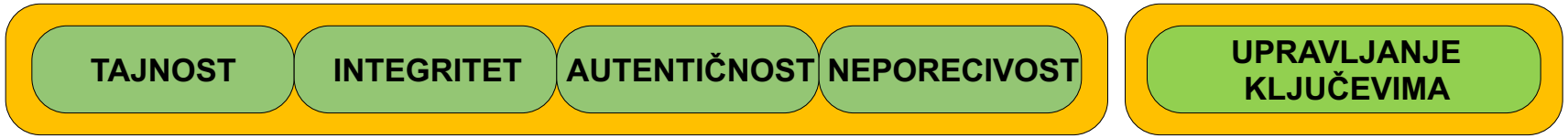
- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način 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/.

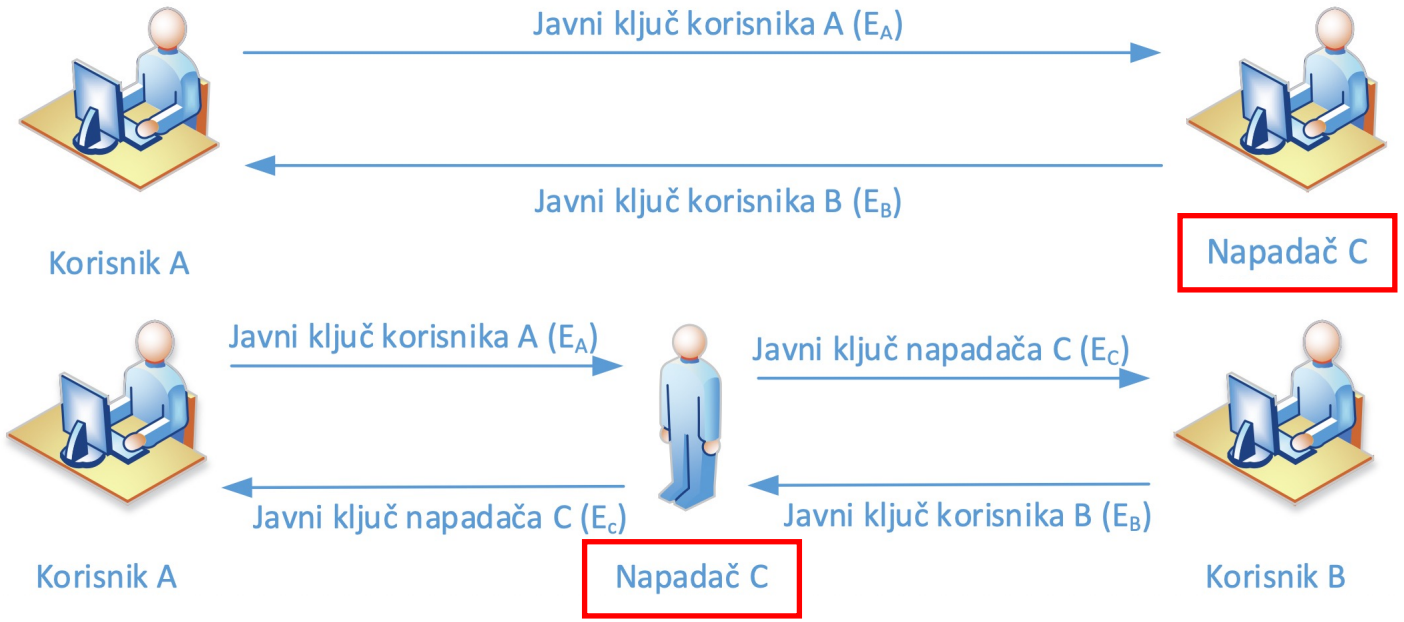
Ponovimo …

- simetrični algoritmi
  - jedan tajni ključ (za šifriranje i dešifriranje koristi se isti ključ)
- asimetrični algoritmi:
  - par ključeve
  - javni ključ dostupan svima
  - privatni ključ dostupan samo vlasniku
- upravljanje ključevima



Problem sigurne distribucije javnih ključeva

- Kad primimo nečiji javni ključ kako znamo da nam netko nije podmetnuo svoj javni ključ?
  - Kako znamo da nije u tijeku MITM napad ili lažno predstavljanje? Javni ključ je samo jedan veliki broj...
  - Prva slika prikazuje lažno predstavljanje, a druga MITM napad



Problem sigurne distribucije javnih ključeva

- temelj rješenja čini certifikacijsko tijelo (engl. certificate authority, CA)
  - treća strana kojoj svi vjeruju (engl. trusted third party)
- javnim ključevima dodaju se informacije o identitetu vlasnika koje potom potpisuje certifikacijskog tijelo
  - korisnik (osoba, Web stranica, poslužitelj elektroničke pošte) koji želi certifikat generira javni i tajni ključ, javnom ključu dodaje identifikacijske podatke i potpisuje ih te šalje certifikacijskom tijelu na potpis
    - Certificate Signing Request, CSR
  - CA prije potpisivanja mora provjeriti da javni ključ doista pripada onome čiji identitet je dan uz javni ključ (telefonski, direktno, ...)
  - javni ključ, podaci o identitetu i potpis CA čine certifikat

Problem sigurne distribucije javnih ključeva

- certifikacijsko tijelo također ima svoj certifikat
  - njega potpisuje samo certifikacijsko tijelo
    - samopotpisani certifikat (engl. self-signed certificate)
  - moraju ga imati svi na Internetu i tada će biti u mogućnosti provjeriti svaki certifikat koji je CA potpisao te na taj način spriječiti MITM napade i lažno predstavljanje
- tako povezani javni ključevi čine infrastrukturu javnog ključa (engl. Public Key Infrastructure, PKI)

Upravljanje ključevima

- upravljanje ključevima (engl. key management)
  - kriptografski algoritmi su opisani standardima
  - upravljanje ključevima je složeniji dio kriptografskog sustava; skup ljudi, hardvera, softvera, procedura, standarda i politika koji treba riješiti sljedeće probleme:
    - kreiranje
    - distribucija
    - korištenje
    - arhiviranje
    - automatizacija životnog ciklusa ključa
- 20% tehnologija : 80% procedure
- PKI (Public Key Infrastructure) - infrastruktura javnog ključa

PKI

- Ima li privatni ključ samo odgovarajuća osoba?
  - kriptografski uređaj
- Kako povezati javni ključ sa osobom?
  - certifikat
- Vrijedi li nečiji javni ključ? Da li je opozvan?
  - lista opozvanih certifikata - CRL
- Tko će izdati i jamčiti za certifikat?
  - certifikacijsko tijelo – certification authority – CA
- Tko će jamčiti identifikaciju i autentifikaciju osobe?
  - registracijsko tijelo – RA
- Kako dobiti / distribuirati javni ključ ?
  - javni imenik
- U koju svrhu mogu koristiti ovaj certifikat?
  - certificate policy - CP

Javni ključ

- javni ključ / Public-Key: (1024 bit)

```
Modulus:
      00:ca:a4:05:83:6f:0c:1d:a0:3e:2d:93:89:d2:76:
      2d:25:9e:b4:c4:81:09:e9:f3:e4:c5:0f:12:88:91:
      a7:f0:ac:21:3a:e6:f1:22:5d:f7:9e:84:e0:94:23:
      b2:02:00:61:40:fb:ac:5f:e3:25:dc:7a:3f:94:e9:
      b4:82:ac:88:da:20:6f:a8:42:d3:bd:2e:bc:b4:ef:
      ce:0b:22:06:22:84:51:74:ac:15:62:d0:dd:78:f7:
      7e:71:86:32:35:2c:07:3e:97:7e:f1:8f:13:2b:78:
      36:eb:9a:9e:ee:a4:0a:cb:23:b5:05:96:e6:c8:ce:
      b8:1e:18:1e:df:62:6d:74:89
Exponent: 65537 (0x10001)
```

- kako povezati javni ključ s korisnikom (subjektom)?
  - javni ključ nema podatke o osobi kojoj pripada
- zahtjev: prepoznatljivost i jednostavno korištenje javnog ključa
  - digitalni certifikat

Digitalni certifikati

- Certifikat – digitalni objekt
  - Sadrži javni ključ i ostale informacije o subjektu, izdavatelju i valjanosti
  - Subjekt certifikata je naziv računala ili osobe kojoj certifikat pripada
  - Certifikat izdaje i digitalno potpisuje izdavatelj certifikata (CA, Certificate Authority)
- Standardi:
  - format X.509 - ISO, ITU-T
  - RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Sadržaj osobnog certifikata

DN: cn=Anja Kovač, o=FER, c=HR

Serial #: 3913133

Start: 6-7-2009 3:33

End: 6-7-2010 3:33

CRL: cn=CRL2, o=FER, c=HR

Key:

CA DN: o=UNI-ZG, c=HR

informacije o korisniku: ime, institucija, država (ili naziv poslužitelja)

jednoznačni serijski broj

informacija o važenju certifikata

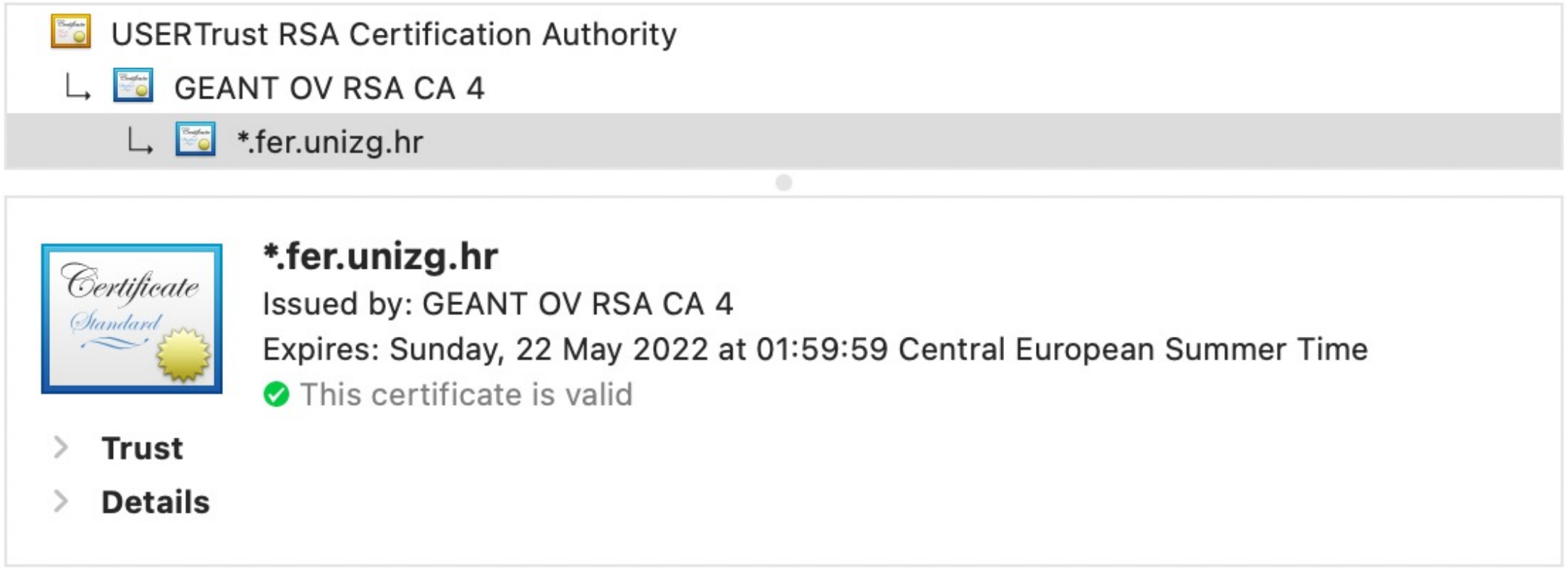
informacija o povlačenju certifikata

javni ključ korisnika

informacija o instituciji koja je izdala certifikat

digitalni potpis institucije koja je izdala certifikat

Sadržaj certifikata za web poslužitelj



Sadržaj certifikata

Subject Name	
Country or Region	HR
Postcode	10000
County	Grad Zagreb
Locality	Zagreb
Street Address	Unska 3
Organisation	Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva
Organisational Unit	CIP
Common Name	*.fer.unizg.hr
Issuer Name	
Country or Region	NL
Organisation	GEANT Vereniging
Common Name	GEANT OV RSA CA 4
Serial Number	00 9F 6E AB 25 65 BB F2 CC 7D 8C E0 15 6F 1A FC 4F
Version	3
Signature Algorithm	SHA-384 with RSA Encryption (1.2.840.113549.1.1.12)
Parameters	None
Not Valid Before	Thursday, 21 May 2020 at 02:00:00 Central European Summer Time
Not Valid After	Sunday, 22 May 2022 at 01:59:59 Central European Summer Time

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes: A6 05 99 6E EE 6E 2A F6 …
Exponent	65537
Key Size	2.048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	512 bytes: 5E 5A 3B 65 A1 53 11 20 …
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature, Key Encipherment
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)

Sadržaj certifikata

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	*.fer.unizg.hr
DNS Name	fer.unizg.hr
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.6449.1.2.2.79)
Qualifier ID #1	Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI	https://sectigo.com/CPS
Policy ID #2	(2.23.140.1.2.2)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl
Extension	Embedded Signed Certificate Timestamp List (1.3.6.1.4.1.11129.2.4.2)
Critical	NO
SCT Version	1
Log Operator	Google
Log Key ID	46 A5 55 EB 75 FA 91 20 30 B5 A2 89 69 F4 F3 7D 11 2C 41 74 BE FD 49 B8 85 AB F2 FC 70 FE 6D 47
Timestamp	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	72 bytes: 30 46 02 21 00 98 A1 CF ...

Log Operator	Let's Encrypt
Log Key ID	DF A5 5E AB 68 82 4F 1F 6C AD EE B8 5F 4E 3E 5A EA CD A2 12 A4 6A 5E 8E 3B 12 C0 20 44 5C 2A 73
Timestamp	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	72 bytes: 30 46 02 21 00 E8 15 0D ...
SCT Version	1
Log Operator	Sectigo
Log Key ID	6F 53 76 AC 31 F0 31 19 D8 99 00 A4 51 15 FF 77 15 1C 11 D9 02 C1 00 29 06 8D B2 08 9A 37 D9 13
Timestamp	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	71 bytes: 30 45 02 21 00 D9 F5 21 ...
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
Method #2	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://GEANT.ocsp.sectigo.com
Fingerprints	
SHA-256	6C B5 C9 D6 65 CF 7F 87 74 8B 8B D0 84 69 D0 01 C9 41 11 93 F7 FD 7D B5 F2 3A 75 B7 87 E5 28 D0
SHA-1	DF 5E 53 9B CC BB 7F 4F A9 FC EC BD 40 08 D3 C2 C6 78 F7 0C

Datoteke

- .CER/.CRT/.DER – binarni, DER kodirani certifikat (ili niz certifikata)
- .PEM – dodatno kodiran po Base64
  - počinje retkom “`-----BEGIN CERTIFICATE-----`”
- .PFX – PKCS#12, javni i privatni ključ (zaštićen lozinkom)

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Certifikat X.509 - .CRT

```
$ hexdump -C mycert.crt

00000000  30 82 05 30 30 82 04 18  a0 03 02 01 02 02 10 08  |0..00...........|
00000010  a3 71 e3 32 95 57 63 54  96 58 82 75 b3 95 12 30  |.q.2.WcT.X.u...0|
00000020  0d 06 09 2a 86 48 86 f7  0d 01 01 0b 05 00 30 69  |...*.H........0i|
00000030  31 0b 30 09 06 03 55 04  06 13 02 4e 4c 31 16 30  |1.0...U....NL1.0|
00000040  14 06 03 55 04 08 13 0d  4e 6f 6f 72 64 2d 48 6f  |...U....Noord-Ho|
00000050  6c 6c 61 6e 64 31 12 30  10 06 03 55 04 07 13 09  |lland1.0...U....|
00000060  41 6d 73 74 65 72 64 61  6d 31 0f 30 0d 06 03 55  |Amsterdam1.0...U|
00000070  04 0a 13 06 54 45 52 45  4e 41 31 1d 30 1b 06 03  |....TERENA1.0...|
00000080  55 04 03 13 14 54 45 52  45 4e 41 20 50 65 72 73  |U....TERENA Pers|
00000090  6f 6e 61 6c 20 43 41 20  33 30 1e 17 0d 31 35 30  |onal CA 30...150|
000000a0  39 31 37 30 30 30 30 30  30 5a 17 0d 31 38 30 39  |917000000Z..1809|
000000b0  31 37 31 32 30 30 30 30  5a 30 67 31 0b 30 09 06  |17120000Z0g1.0..|
000000c0  03 55 04 06 13 02 48 52  31 0f 30 0d 06 03 55 04  |.U....HR1.0...U.|
000000d0  07 13 06 5a 61 67 72 65  62 31 2e 30 2c 06 03 55  |...Zagreb1.0,..U|
000000e0  04 0a 13 25 46 61 6b 75  6c 74 65 74 20 65 6c 65  |...%Fakultet ele|
000000f0  6b 74 72 6f 74 65 68 6e  69 6b 65 20 69 20 72 61  |ktrotehnike i ra |
00000100  63 75 6e 61 72 73 74 76  61 31 17 30 15 06 03 55  |cunarstva1.0...U|
00000110  04 03 13 0e 4d 69 6c 6a  65 6e 6b 6f 20 4d 69 6b  |....Miljenko Mik|
00000120  75 63 30 82 01 22 30 0d  06 09 2a 86 48 86 f7 0d  |uc0.."0...*.H...|
. . .
```

Certifikat X.509 - .PEM

```
$ cat mycert.pem

-----BEGIN CERTIFICATE-----
MIIFMDCCBBigAwIBAgIQCKNx4zKVV2NUlliCdbOVEjANBgkqhkiG9w0BAQsFADBp
MQswCQYDVQQGEwJOTDEWMBQGA1UECBMNTm9vcmQtSG9sbGFuZDESMBAGA1UEBxMJ
QW1zdGVyZGFtMQ8wDQYDVQQKEwZURVJFTkExHTAbBgNVBAMTFFRFUkVOQSBQZXJz
b25hbCBDQSAzMB4XDTE1MDkxNzAwMDAwMFoXDTE4MDkxNzEyMDAwMFowZzELMAkG
A1UEBhMCSFIxDzANBgNVBAcTBlphZ3JlYjEuMCwGA1UEChMlRmFrdWx0ZXQgZWxl
. . .
tM8DqHDMa6RhNmrxJlldokQIVh94RLfQESnm0UHNEXSStDa7nSAcdMasDnH3avvh
yIeC9dS1H9wT4Hiu7t48vw04jeUgCbbRGmglYhg5Dpekj244
-----END CERTIFICATE-----
```

Certifikat X.509 (1/3)

```
$ openssl x509 -in mycert.pem -text –noout

Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        08:a3:71:e3:32:95:57:63:54:96:58:82:75:b3:95:12
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Personal CA 3
Validity
        Not Before: Sep 17 00:00:00 2015 GMT
        Not After : Sep 17 12:00:00 2018 GMT
Subject: C=HR,L=Zagreb,O=Fakultet elektrotehnike i racunarstva,CN=Miljenko Mikuc
Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:9d:44:b8:ed:f6:a1:4a:1b:31:dd:8d:aa:d4:a2:
            . . .
```

Certifikat X.509 (2/3)

```
X509v3 extensions:
    X509v3 Authority Key Identifier:
        keyid:F0:21:E9:49:77:73:9F:85:AE:18:3B:E8:52:70:14:06:ED:42:EE:CA

    X509v3 Subject Key Identifier:
        BA:12:55:BC:2B:D4:08:C2:0A:BC:90:E4:B7:C5:75:82:DD:AA:BF:E7
    X509v3 Basic Constraints: critical
        CA:FALSE
    X509v3 Subject Alternative Name:
        email:miljenko.mikuc@fer.hr
     X509v3 Key Usage: critical
         Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication, E-mail Protection
    X509v3 Certificate Policies:
         Policy: 2.16.840.1.114412.4.1.2
         CPS: https://www.digicert.com/CPS
```

Certifikat X.509 (3/3)

```
X509v3 CRL Distribution Points:
    Full Name:
        URI:http://crl3.digicert.com/TERENAPersonalCA3.crl
    Full Name:
        URI:http://crl4.digicert.com/TERENAPersonalCA3.crl
    Authority Information Access:
        OCSP - URI:http://ocsp.digicert.com
        CA Issuers - URI:http://cacerts.digicert.com/TERENAPersonalCA3.crt

Signature Algorithm: sha256WithRSAEncryption
     04:ce:64:89:c6:f2:5d:ee:dd:67:75:8a:ea:d0:98:41:09:4e:
     a4:f3:1d:27:91:47:18:c9:1f:af:fd:ae:80:8c:e6:14:4d:a4:
     26:29:91:e4:38:5b:8a:52:5d:82:e6:d4:58:7a:b5:4c:a7:bd:
     . . .
     e6:d1:41:cd:11:74:92:b4:36:bb:9d:20:1c:74:c6:ac:0e:71:
     f7:6a:fb:e1:c8:87:82:f5:d4:b5:1f:dc:13:e0:78:ae:ee:de:
     3c:bf:0d:38:8d:e5:20:09:b6:d1:1a:68:25:62:18:39:0e:97:
     a4:8f:6e:38
```

Standardi i preporuke

- ASN.1: Abstract Syntax Notation One (ASN.1)
  - opis struktura podataka koje se mogu serijalizirati na jedinstven način, neovisno o korištenoj platformi
- ITU-T X.690
  - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- BER - Basic Encoding Rules
  - Format kodiranja apstraktnih informacija u tok podataka. Specificira slijed okteta. Sintaksa definira elemente za prikaz osnovnih tipova podataka, strukturu informacija o dužini i način definiranja složenih ili miješanih tipova podataka.
    - CER - Canonical Encoding Rules
    - DER - Distinguished Encoding Rules

Standardi i preporuke

- DER - Distinguished Encoding Rules
  - osigurava točno jedan način kodiranja ASN.1 vrijednosti
  - namijenjen situacijama kad je potrebno jedinstveno kodiranje
    - npr. u kriptografiji - osigurava da digitalno potpisana podatkovna struktura rezultira jedinstvenim serijaliziranim prikazom
  - kanonski oblik BER
    - npr. BER kodira logičku vrijednost za laž s vrijednošću 0, a vrijednost logičke istine se može prikazati na 255 načina.
    - DER kodira logičke vrijednosti istine i laži na točno jedan način
- CER - Canonical Encoding Rules (CER)
  - razlikuje se od DER u načinu prikaza duljine podataka
  - DER uvijek ima oznaku duljine podataka na početku, a CER koristi oktet za oznaku kraja konteksta
  - CER zahtijeva manje meta podataka za velike kodirane vrijednosti

Standardi i preporuke

- PKCS - Public-Key Cryptography Standards (RSA Laboratories)
  - PKCS #12 – definira format datoteke za pohranu privatnog X.509 ključa uz javni X.509 certifikat (zaštićene lozinkom temeljenom na simetričnom ključu)
  - PKCS #7 – definira sintaksu šifriranih poruka
    - za potpisivanje ili šifriranje poruka u PKI te za dostavu informacija o certifikatu (kao odgovor na poruku PKCS#10)
    - temelj standardu S/MIME
  - PKCS #10 - definira format poruke koja se šalje CA kao zahtjev za certificiranjem javnog ključa

Standardi i preporuke

- CMS - Cryptographic Message Syntax
  - IETF-ov standard (RFC 5652) za kriptografski zaštićene poruke
  - može se koristiti za digitalno potpisivanje, sažimanje, autentifikaciju ili šifriranje bilo kojeg oblika digitalnih podataka
  - izveden iz standarda PKCS #7
  - osnovna kriptografska komponenta mnogih standarda
    - npr. S/MIME, PKCS #12 i RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

Važenje certifikata

- javni ključevi
  - mogu se koristiti kroz dugi vremenski period (desetljeća)
    - zbog provjere potpisa
- privatni ključevi
  - trebaju imati što kraće vrijeme važenja
- opoziv ključa
  - ako je ključ kompromitiran treba ga opozvati
  - ako je ključ opozvan, potpisani dokument ne vrijedi (osim kada ima vremensku oznaku, „timestamp”)
  - ako je ključ opozvan, svi dokumenti koji su njime šifrirani su kompromitirani
- provjera certifikata
  - obavezna! (pošiljatelj / primatelj)
  - treba uključivati provjeru važenja certifikata i provjeru potpisa certifikata
  - ako je potrebno arhivirati potpisani dokument: „timestamp”

Valjanost certifikata

- Polja u certifikatu: „not valid before” i „not valid after”
- Za vrijeme roka valjanosti certifikat može biti opozvan
  - Gubitak ili kompromitacija privatnog ključa, promjena naziva ili imena, …
- *Certificate Revocation List* (CRL) – lista opozvanih certifikata
  - CRL je digitalni objekt s rokom valjanosti koji sadrži listu opozvanih certifikata te vrijeme i razlog opoziva (digitalno potpisan od strane CA)
  - u certifikatu su navedene adrese i načini pristupa CRL (https, ldap)
- OCSP - Online Certificate Status Protocol
  - OCSP stapling: poslužitelj, uz certifikat, dostavlja klijentu i vremenski ovjeren rezultat OCSP provjere od strane CA

Dohvaćanje CRL

- objava CRL
  - u certifikatu piše gdje je CRL
  - Directory Address: CN=CRL58, OU=RDC, O=FINA, C=HR
  - URI:ldap://rdc-ldap.fina.hr/ou=RDC, o=FINA,c=HR?certificateRevocationList%3Bbinary
  - URI: http://rdc.fina.hr/crls/rdc.crl
  - URI: http://srl3.digicert.com/TERENAPersonalCA34.crl
- javni imenik i HTTP

- OCSP - Online Certificate Status Protocol
  - RFC 6960
    - OCSP - URI: http://ocsp.digicert.com

Dohvaćanje CRL

```
$ wget http://crl3.digicert.com/TERENAPersonalCA3.crl

$ openssl crl -inform DER -outform PEM \
    -in TERENAPersonalCA3.crl -out TERENAPersonalCA3.pem

$ openssl crl -in TERENAPersonalCA3.pem -text -noout
Certificate Revocation List (CRL):
...
Issuer: /C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA Personal CA 3
Last Update: Oct 27 18:00:22 2015 GMT
Next Update: Nov  3 17:00:00 2015 GMT
...
Revoked Certificates:
    Serial Number: 0E085BF033E3E00C05454B91CDE4C0ED
        Revocation Date: Feb  3 12:47:53 2015 GMT
    . . .
    Serial Number: 095819C43C84DEA4B14875B765DA18E4
        Revocation Date: Oct 26 15:04:50 2015 GMT
    Signature Algorithm: sha256WithRSAEncryption
         b1:67:df:f6:a3:0f:43:42:cd:cc:af:5e:ae:f1:13:32:53:82:
         . . .
         4d:a0:7f:95
```

Dohvaćanje CRL

```
$ openssl ocsp  \
    -text \
    -issuer TERENA\ Personal\ CA\ 3.pem \
    -cert GordanGledecDigiCertCertifikat.pem \
    -VAfile TERENA\ Personal\ CA\ 3.pem \
    -url http://ocsp.digicert.com
```

Dohvaćanje CRL

```
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: F021E94977739F85AE183BE852701406ED42EECA
    Produced At: Oct 28 09:37:00 2015 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: BD3B9EE18745EFF24C919C59BDECACA670A50828
      Issuer Key Hash: F021E94977739F85AE183BE852701406ED42EECA
      Serial Number: 0E1A6B4B1FC6D9EFD036FD82E7164138
    Cert Status: good
    This Update: Oct 28 09:37:00 2015 GMT
    Next Update: Nov  4 08:52:00 2015 GMT

    Signature Algorithm: sha256WithRSAEncryption
         ab:d0:fd:d2:81:e2:96:d1:9f:2b:62:5c:fb:e1:56:18:1a:fc:
         . . .
```

Korisnici PKI

- organizacije i pojedinci koji koriste PKI

- nositelj certifikata (Certificate holder)
  - subjekt certifikata koji raspolaže s privatnim ključem
    - zahtjeva certifikat od CA kontaktirajući RA
    - dobiva certifikat od CA i koristi ga
    - autentificira se, izrađuje elektronički potpis, dešifrira podatke i sl.

- pouzdajuće strane (Relying parties)
  - korisnici koji raspolažu s javnim ključem
    - identificiraju CA kao početnu točku kojoj vjeruju
    - koriste repozitorij
    - provjeravaju potpis, šifriraju podatke i sl.

Certifikacijsko tijelo

- Certificate Authority (CA) - povjerljiva treća strana
  - središnji i odgovorni servis sustava PKI
  - izdaje i potpisuje certifikate i jamči vezu subjekta s javnim ključem
  - izdaje CRL i upravlja informacijama o statusu certifikata
  - nužna adekvatna zaštita privatnog ključa certifikacijskog tijela
  - u tehničkom smislu: hardver i softver koji potpisuje certifikate i CRL
  - u tehnološkom smislu: skup ljudi, procedura, standarda i politika
- certifikati svih poznatih izdavatelja ugrađeni su u preglednike ili operacijski sustav (certificate store, keychain,…)
  - unutar organizacije je moguće kreirati i vlastito certifikacijsko tijelo koje izdaje samopotpisani certifikat („self-signed certificate”)

Odgovornosti CA

- zaštita svog privatnog ključa
- provjera točnosti informacija u certifikatu (prije izdavanja)
- zaštita profila
  - certifikati i CRL se izdaju sukladno svom profilu
- održavanje ažurnosti CRL
- distribuirati (objavljivati) certifikate i CRL
- održavati arhivu za provjeru certifikata i nakon njenog isteka
- moguće je delegiranje odgovornosti trećim stranama
  - registracijsko tijelo („Registration Authority”, RA) - zbog rasprostranjenosti ureda
  - javni imenik - zbog povećanja dostupnosti
  - arhiva - zbog sigurnijeg i dugotrajnijeg čuvanja arhivskih podataka

Certificate Policy - CP

- u koju svrhu mogu koristiti ovaj certikat?
- politika, “policy”
  - skup implementiranih procedura
  - primjena: sve komponente PKI - CA, RA, javni imenik
- Certificate Policy (CP)
  - skup pravila koja ukazuju na prikladnost certifikata za određenu zajednicu ili skupinu sa zajedničkim sigurnosnim zahtjevima
  - opisuje pravila rada CA i odgovornosti svih strana
  - javno se objavljuje
- Certification Practice Statements (CPS)
  - detaljno opisuje kako CA implementira CP
  - ne treba biti javno objavljen

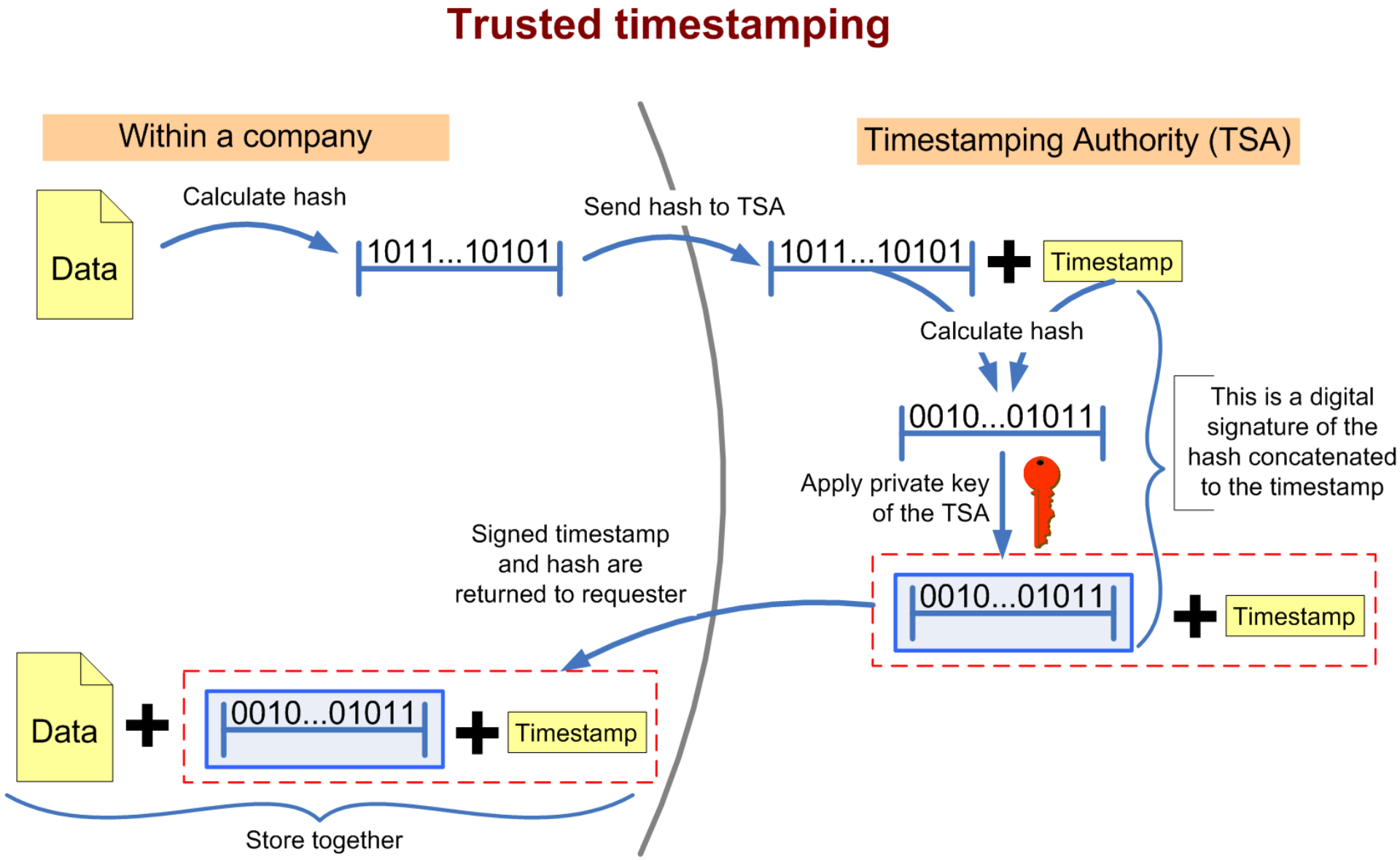
Dodatni servisi

- Timestamp Authority (TSA) - usluga vremenske ovjere
  - podatak je postojao u trenutku izrade potpisa
  - certifikat je bio valjan u trenutku izrade potpisa
  - potpis je izrađen prije datuma i vremena TS
  - nužno za izradu kvalificiranog potpisa
  - poslovni modeli
    - besplatne informacije – bez autentifikacije
    - plaćanje po zahtjevu – s autentifikacijom

Arhitektura TS

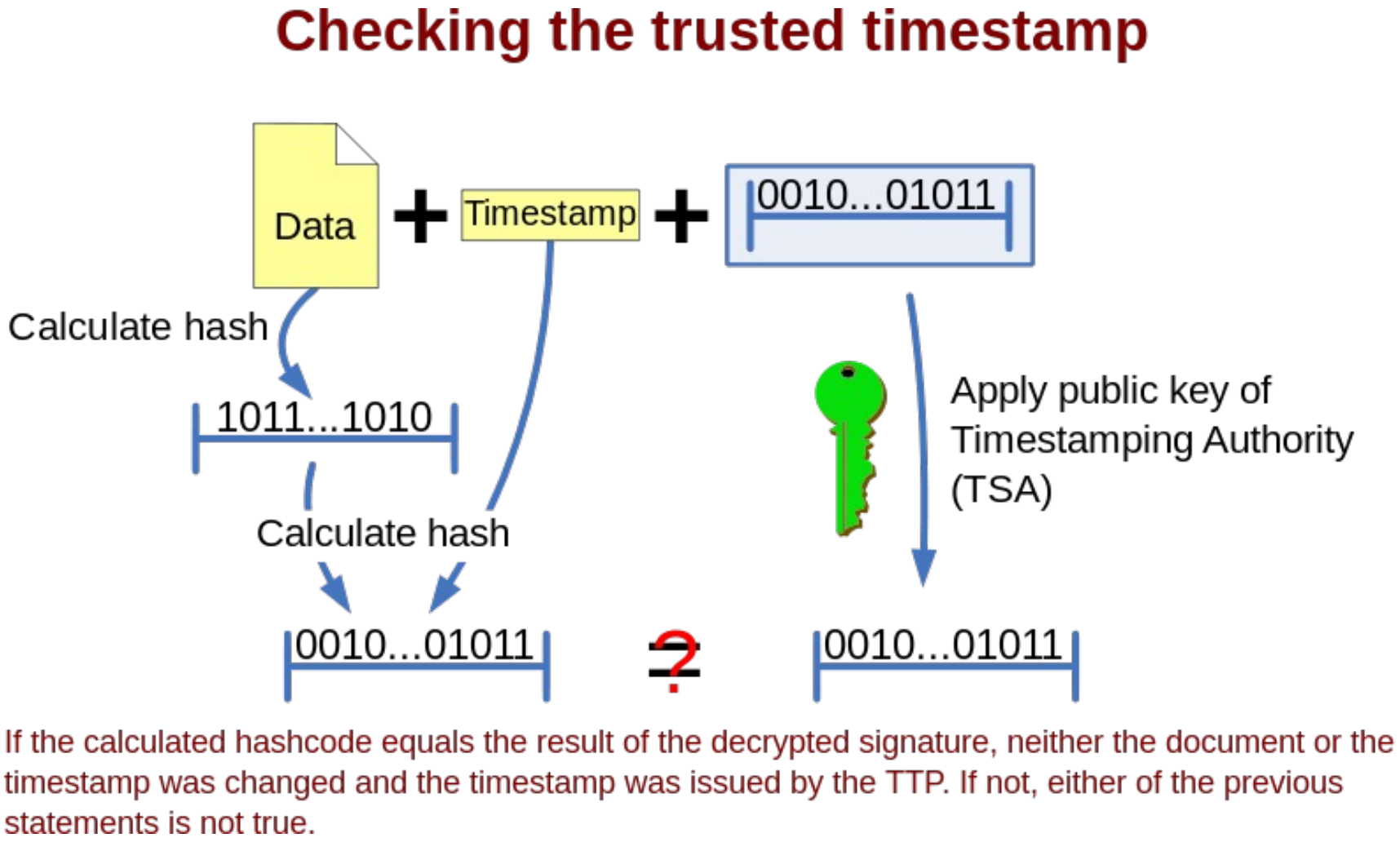
- TS (Timestamp) – servis vremenske ovjere
  - NTP server, GPS
  - HSM (Hardware security module) za čuvanje privatnog ključa TS
- tijek:
  - potpisani hash dokumenta se šalje TS poslužitelju u obliku zahtjeva
  - TS poslužitelj vraća odgovor potpisan njegovim certifikatom

Arhitektura TS



https://commons.wikimedia.org/wiki/File:Trusted_timestamping.gif

Arhitektura TS



https://en.wikipedia.org/wiki/File:Checking_timestamp.svg

Problemi sa sustavom PKI (1)

- certifikacijska tijela su vrlo primamljiv cilj napadačima
  - ima ih mnoštvo koje priznaju proizvođači Web preglednika i ako je bilo koji kompromitiran, cijeli sustav je u opasnosti
  - ne postoji općeprihvaćeni mehanizam provjere koji CA smije izdavati koje certifikate
- primjer velikog napada na CA/incidenta
  - DigiNotar – U rujnu 2011. otkrivena provala u Danski CA te izdavanje lažnih certifikata za Google koji su se koristili za špijuniranje građana Irana. DigiNotar je bankrotirao 2011. godine
- pojedina certifikacijska tijela ne provjeravaju identitet korisnika dobro
- prodaja certifikata s mogućnošću izdavanja certifikata

Problemi sa sustavom PKI (2)

- sustav je zbunjujući za prosječnog korisnika Interneta
  - pa čak i za ICT profesionalce
- problemi zbog kojih su korisnici zbunjeni
  - samopotpisani certifikati se ne bi smjeli pojavljivati jer se onda ljudi priučavaju na njih i smatraju ih normalnim/očekivanim
  - Web preglednici variraju način označavanja da se radi o zaštićenoj koneciji čak i između verzija (sa/bez https, različiti lokoti)
    - napadači to zloupotrebljavaju tako što lokote stavljaju na razna mjesta pokušavajući iskoristiti zbunjenost korisnika
- postojanje različitih vrsta certifikata (Extended/Organization/Domain Validation)
- problem s listama opozvanih certifikata i OCSP-om

Problemi sa sustavom PKI (3)

- certifikati koštaju te se izbjegava kupovina
  - pridonosi zbunjenosti korisnika Interneta, Web preglednici sa svojim porukama ne pridonose tome
  - cijena ovisi o trajanju i tipu certifikata
  - Let’s Encrypt omogućava besplatne certifikate trajanja cca. 6 mjeseci
- Let’s Encrypt
  - temelji se na dokazivanju vlasništva domene izmjenama u DNS-u
  - ako netko preuzme kontrolu nad DNS-om omogućeno je izdavanje lažiranih certifikata
- problem s obnavljanjem certifikata na vrijeme
  - certifikati koji su istekli također zbunjuju korisnike
- PKI sustav se smatra nedovoljno dobrim
  - ali boljeg rješenja trenutno nema

Primjeri izdavatelja certifikata

- elektronička osobna iskaznica, eOI (izdavatelj certifikata: AKD)
  - http://eid.hr
- FINA – CA za pravne osobe
  - “Registar digitalnih certifikata”, http://rdc.fina.hr/
- u suradnji s organizacijom GÉANT, CARNET nudi uslugu izdavanja elektroničkih certifikata tvrtke Sectigo Limited
  - OV certifikati (Organization Validation), EV certifikati (Extended Validation),
  - poslužiteljski, klijentski, „document signing”, …
- poslužiteljski TLS certifikati „Let's Encrypt”
  - https://letsencrypt.org
  - DV (Domain Validation)
  - RFC 8555: ACME (Automatic Certificate Management Environment)