CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

# SC servis
# (Server Certificate Service – SCS)

Albert Novak – CARNet

CUC 2006, 20.-22.11.2006.

# Sadržaj

- Što su to elektronički certifikati?
- Primjena elektroničkih certifikata
- Važno je biti priznati root CA (Certificate Authority)
- CARNetov SC servis (Server Certificate Service – SCS)
- Generiranje zahtjeva za certifikatom
- Podnošenje zahtjeva za certifikatom
- Odobravanje zahtjeva za certifikatom
- Instaliranje certifikata
- Što u slučaju kompromitiranja certifikata – opoziv certifikata

# Što su elektronički certifikati

- Elektronički certifikati predstavljaju skup atributa koji su na jednoznačan način povezani s parom ključeva i koji su ovjereni od certifikacijskog autoriteta
- Najviše korišteni certifikati su X.509v3
  - omogućavaju dodatne ekstenzije kojima se definira upotreba certifikata
- U zavisnosti o politici pod kojom se izdaju elektronički certifikati postoji mogućnost opoziva certifikata:
  - CRL – Certificate Revocation List
  - OCSP – Online Certificate Status Protocol

# Primjer elektroničkog certifikata (1)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:00:00:00:00:01:0e:bc:ac:0c:14
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BE, O=Cybertrust, OU=Educational CA, CN=Cybertrust Educational CA
        Validity
            Not Before: Nov  6 09:49:21 2006 GMT
            Not After : Nov  6 09:49:21 2007 GMT
        Subject: C=HR, L=Pula, O=CARNet, OU=RISS, CN=ulika.pu.carnet.hr/emailAddress=admin@pu.carnet.hr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:93:00:d7:75:0d:30:63:57:ae:63:54:12:76:0a:
                    81:57:3c:f7:d7:73:0f:8a:ef:74:87:a9:82:b3:a9:
                    ...
                    0e:75
                Exponent: 65537 (0x10001)
```

# Primjer elektroničkog certifikata (2)

X509v3 extensions:
X509v3 Certificate Policies:
Policy: 1.2.840.6334.1.0
CPS: http://www.globalsign.net/repository/cps.cfm

X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Authority Key Identifier:
keyid:65:65:A3:3D:D7:3B:11:A3:0A:07:25:37:C9:42:4A:5B:76:77:50:E1

X509v3 Subject Key Identifier:
BD:A8:24:E6:A3:02:70:80:E4:14:B5:45:CD:4A:BF:B5:79:7E:D5:F8
X509v3 CRL Distribution Points:
URI:http://crl.globalsign.net/educational.crl

Authority Information Access:
CA Issuers - URI:http://secure.globalsign.net/cacert/educational.crt

X509v3 Subject Alternative Name:
DNS:ulika.pu.carnet.hr, email:admin@pu.carnet.hr
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, E-mail Protection
Signature Algorithm: sha1WithRSAEncryption

# Primjena elektroničkih certifikata

- Elektronički certifikati nam omogućuju da s većom razinom sigurnosti možemo utvrditi da li smo pristupili pravom servisu, to jest da li je servis/poslužitelj onaj za kojega se izdaje
- Prilikom uspostave SSL ili TLS kanala
  - na osnovu poslužiteljskog certifikata klijent može ustvrditi da li je pristupio “pravom” servisu
  - na osnovu klijentskog certifikata poslužitelj može ustanoviti da li je klijent koji mu je pristupio onaj za kojega se izdaje
  - asimetrična kriptografija povezana s certifikatima omogućava nam sigurnu razmjenu podataka/ključeva

# Važno je biti priznati root CA

- Priznati root CA nalazi se popisu certifikata kojima vjeruje preglednik, ali i ostale aplikacije
  - Microsoft IE
  - Firefox
- Ukoliko se certifikat nije odobren od CA u kojega preglednik/aplikacija/mi imamo povjerenja pojavljuje se popup poruka koja nas upozorava da nije moguće provjeriti vjerodostojnost certifikata
- Povjerenje je skupa stvar:
  - postupci za stjecanje povjerenja u CA su vrlo skupe

# CARNetov SC servis

- Nastao je kao odgovor na potrebu da se akademskoj zajednici osigura neograničeni broj popup free poslužiteljskih certifikata
- SCS servis nastao je u okrilju TERENA-e
  - jedan od rezultata suradnje CARNeta i Srca na projektu AAI@EduHr
  - 8 NREN-ova:
    - ACOnet (Austria), CARNet (Croatia), CESNET (Czech Republic), RENATER/CRU (France), RedIRIS (Spain), SURFnet (the Netherlands), SWITCH (Switzerland) and UNI·C (Denmark)
  - Servis razvijen u suradnji s GlobalSignom
  - prva godina ugovora
  - pregovori za nastavak suradnje; uvođenje OCSP servisa
- Za korištenje servisa potrebna je predregistracija ustanove - proxy

# Generiranje zahtjeva za certifikatom

- Generira se par RSA ključeva određene dužine i zahtjev za izdavanjem certifikata – CSR (Certificate Request)
- U zahtjevu se definiraju osnovni podaci o certifikatu
- Želimo li da certifikat ima subject Alternative Name onda dodatne DNS zapise generiramo kao višestruka CN polja u Subjectu zathjeva za izdavanjem certifkata
- Predefinirane openssl konfiguracijske datoteke:
  - http://www.carnet.hr/crepozitorij/SCSreq.cnf
  - http://www.carnet.hr/crepozitorij/multiSCSreq.cnf

- *openssl req -new -config SCSreq.cnf -keyout server.key -out server.csr*

# Podnošenje zahtjeva za certifikatom

- Zahtjev se podnosi putem GlobalSign-ove web aplikacije:
  - URL: https://www.globalsign.net/ra/terena/carnet/edu.cfm
- Procedura podnošenja zahtjeva:
  - tehnička osoba podnosi zahtjev
  - kao administrativna osoba navodi se jedna od osoba koja je navedena kao ovlaštena osoba ustanove za ovjeravanje zahtjeva za izdavanjem certifikata
  - administrativna osoba po primitku e-mail poruke o zahtjevu za certifikatom istu osobnim potpisom autorizira i šalje je natrag SCS timu

# Odobravanje zahtjeva za certifikatom

- Svaki zahtjev za certifikatom mora proći provjeru:
  - statusa ovlaštenika ustanove za ovjeru zahtjeva za izdavanjem certifikata;
  - potpisa ovlaštenika ustanove na zahtjevu za izdavanjem certifikata
- Po izvršenim provjerama odobrava se ili odbija zahtjev za izdavanjem certifikata:
  - u praksi se zahtjevi odobravaju ili odbijaju u roku od 24 sata od primitka potpisanog zahtjeva za izdavanjem certifikata

# Instaliranje certifikata

- Tehnička osoba koja je podnijela zahtjev za izdavanjem certifikata dobiva e-mailom obavijest o načinu preuzimanja certifikata
- Instalacija zavisi od aplikacije koja će koristiti izdani certifikat – u principu radi se samo podešavanju konfiguracijskih datoteka
- Pošto su SureServerEdu certifikati potpisani od GlobalSignovog CA koji nije na vrhu hijerarhije potrebno je pravilno podesiti lanac povjerenja:
  - http://secure.globalsign.net/cacert/sureserverEDU.pem
- Konfiguracija mod_ssl na Apachu:
  - SSLCertificateFile mojserver.pem
  - SSLCertificateKeyFile mojserver.key
  - SSLCertificateChainFile sureserverEDU.pem

# Što u slučaju kompromitiranja certifikata – opoziv certifikata

- U slučaju da se ustanovi kompromitiranost certifikata isti je potrebno opozvati
- Opoziv certifikata može se izvršiti na dva načina:
  - korištenjem uputa i linka koji se nalaze u mailu obavijesti o izdavanju certifikata
  - slanjem zahtjeva za opozivom certifikata SCS timu. Zahtjev mora biti potpisan od ovlaštene osobe i ovjeren pečatom ustanove, te mora sadržavati točan Subject certifikata
- Radi provjere valjanosti certifikata potrebno je na klijentu imati CR liste, to jest OCSP servis.

# Zaključak

- Prilikom uspostave sigurnosnih kanala nemojte ignorirati popup poruke – postoji mogućnost da pristupate krivim stranicama
- Certifikati vam omogućavaju da korisnici vašeg servisa mogu biti sigurni da pristupaju pravom servisu – koristite ih tamo gdje je važna provjera autentičnosti servisa
- Iskoristite mogućnost dobivanja neograničenog broja poslužiteljskih certifika

- CARNet SCS - http://www.carnet.hr/scs

- Kontakt: scs-ra@carnet.hr