

Računarstvo zasnovano na uslugama

<http://www.fer.hr/predmeti/rznu>

Doc.dr.sc. Dejan Škvorc

Doc.dr.sc. Ante Đerek

Prof.dr.sc Siniša Srbljić

**Fakultet elektrotehnike i računarstva
Sveučilište u Zagrebu**

Sigurnost

Dr.sc. Miroslav Popovi

Plan predavanja

- “ Motivacija
- “ Osnove sigurnosti
- “ REST
- “ WS-Security

Motivacija

ˇ Domena primjene usluga

- . Financijski sektor (banke, osiguravajuće)
- . Zdravstveni sektor (ordinacije opće medicine, bolnice, zavod za zdravstvo)
- . Državni sektor (razna ministarstva, policijska uprava, Oupanije, katastri, izborne jedinice)
- . Promet (zračne i pomorske luke, cestovni promet)
- . Vojni sektor (mornarica, kopnene i zračne snage)

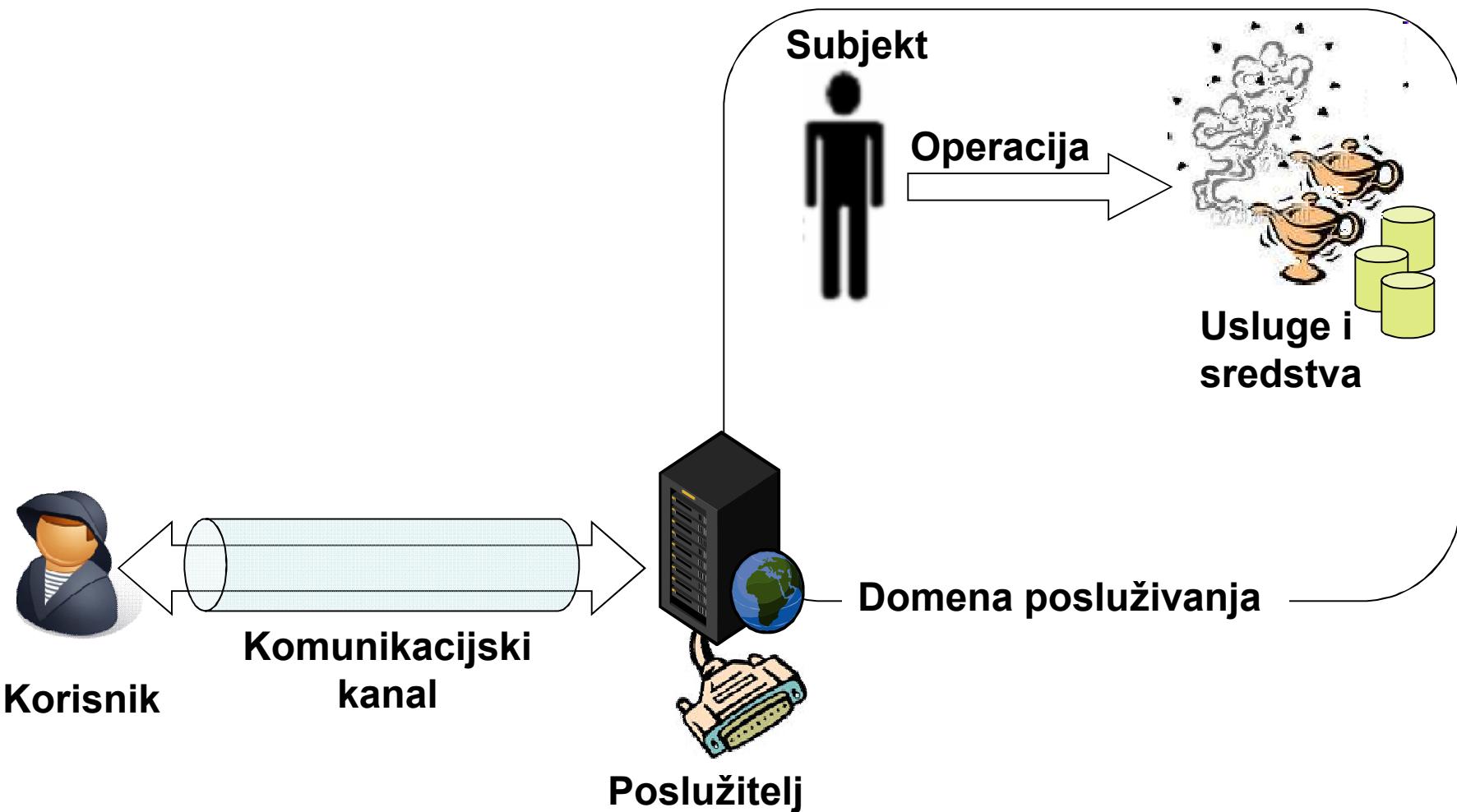
Svojstva sigurnosti

- “ Sigurnosna pitanja
 - . **Tko je poslao zahtjev?**
 - . **Da li korisnik smije koristiti uslugu?**
 - . **Tko, kada i koliko je koristio uslugu?**
 - . **Što ako se prisluškuje?**
 - . **Korisnik tvrdi da nije koristio uslugu?**

Svojstva sigurnosti

- “ Sigurnosna pitanja
 - . **Tko je poslao zahtjev?**
 - “ Autentičnost ili izvornost
 - . **Da li korisnik smije koristiti uslugu?**
 - “ Nepovredivost
 - . **Tko, kada i koliko je koristio uslugu?**
 - “ Pribilježenost
 - . **Što ako se prisluškuje?**
 - “ Tajnost ili povjerljivost
 - . **Korisnik tvrdi da nije koristio uslugu?**
 - “ Neporecivost

Dva problema sigurnosti usluga

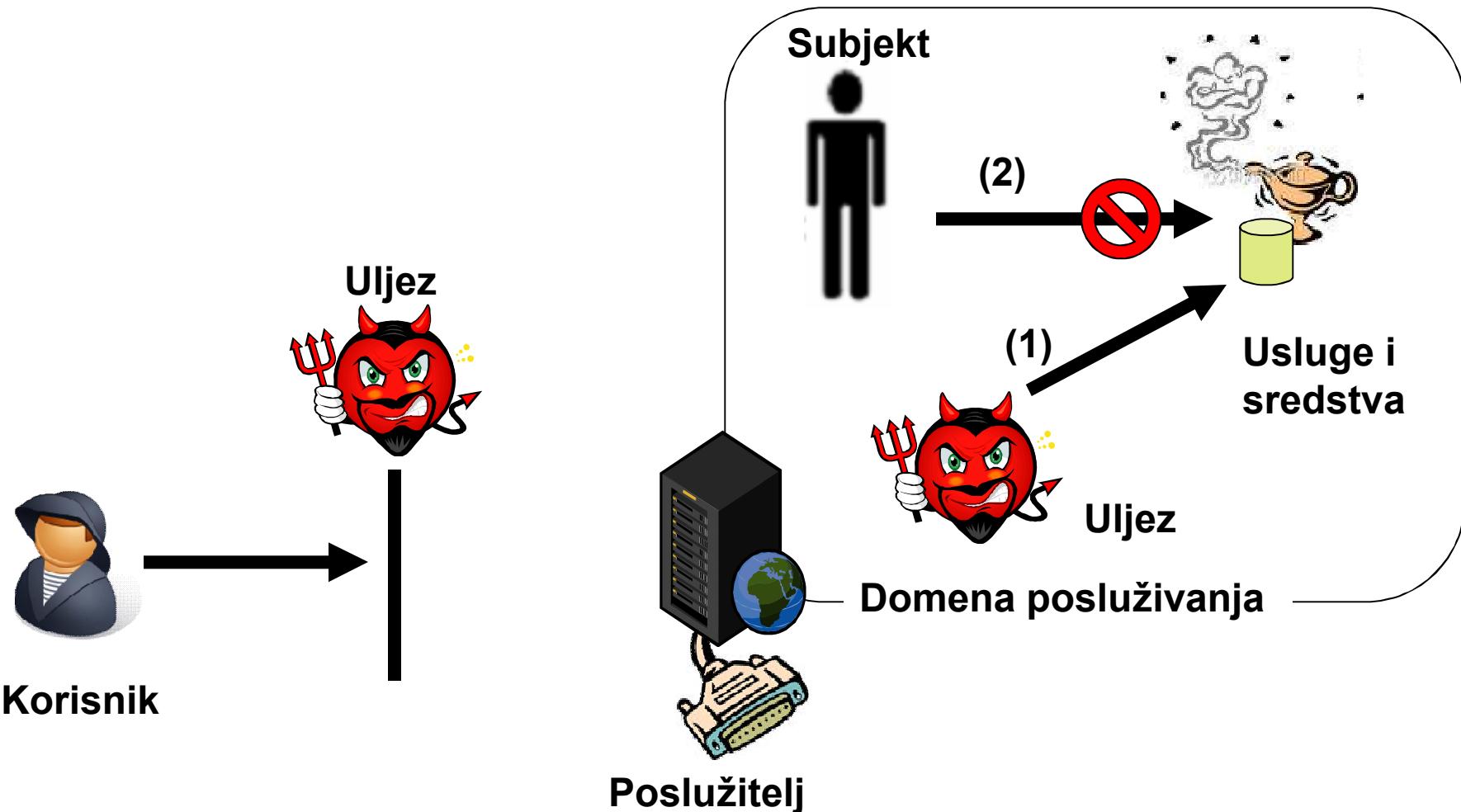


Vrste ugrođavanja sigurnosti

- “ Prekid
- “ Prisluzkivanje
- “ Izmjena
- “ Izmisljanje

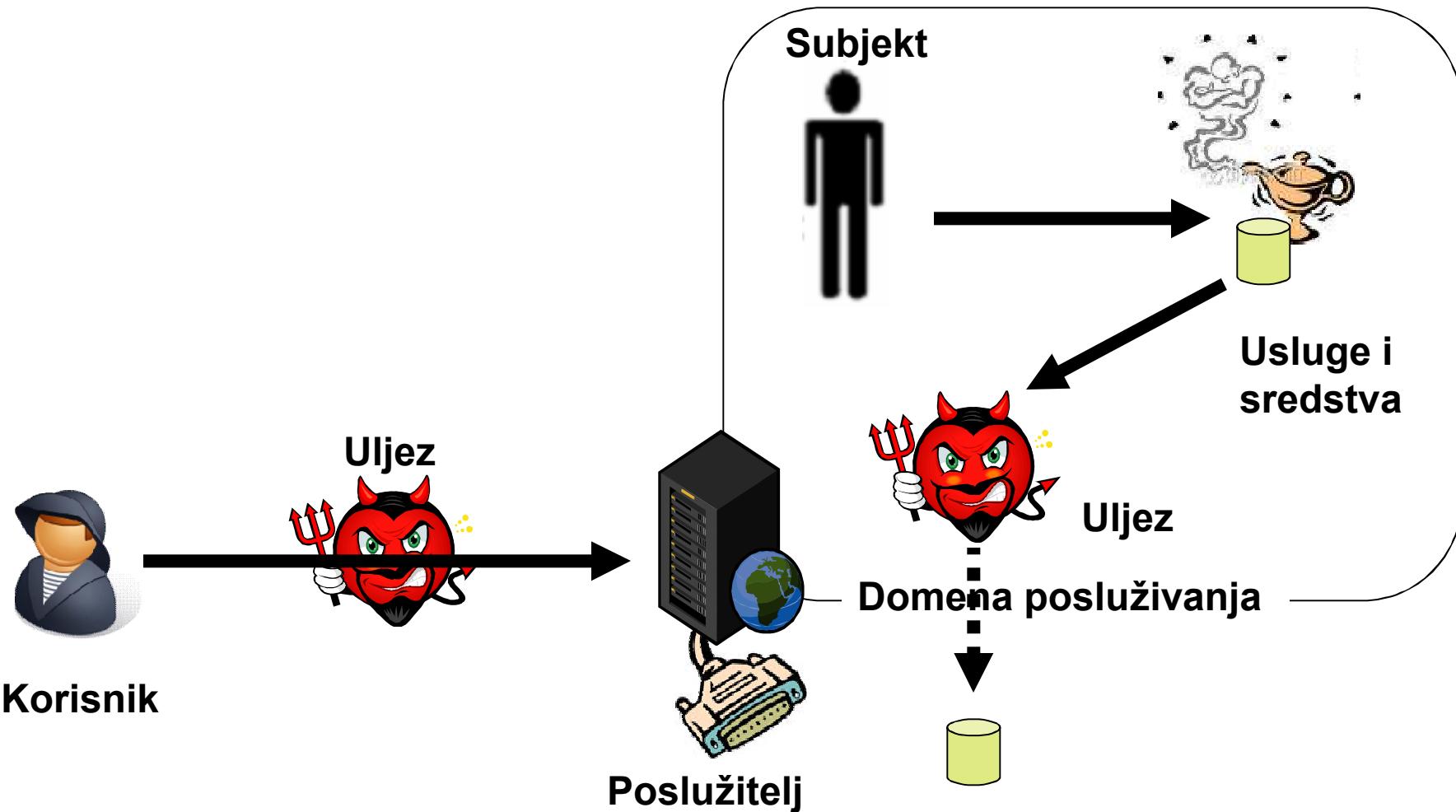
Ugrođavanje sigurnosti prekidom

- „ Svojstvo dostupnosti



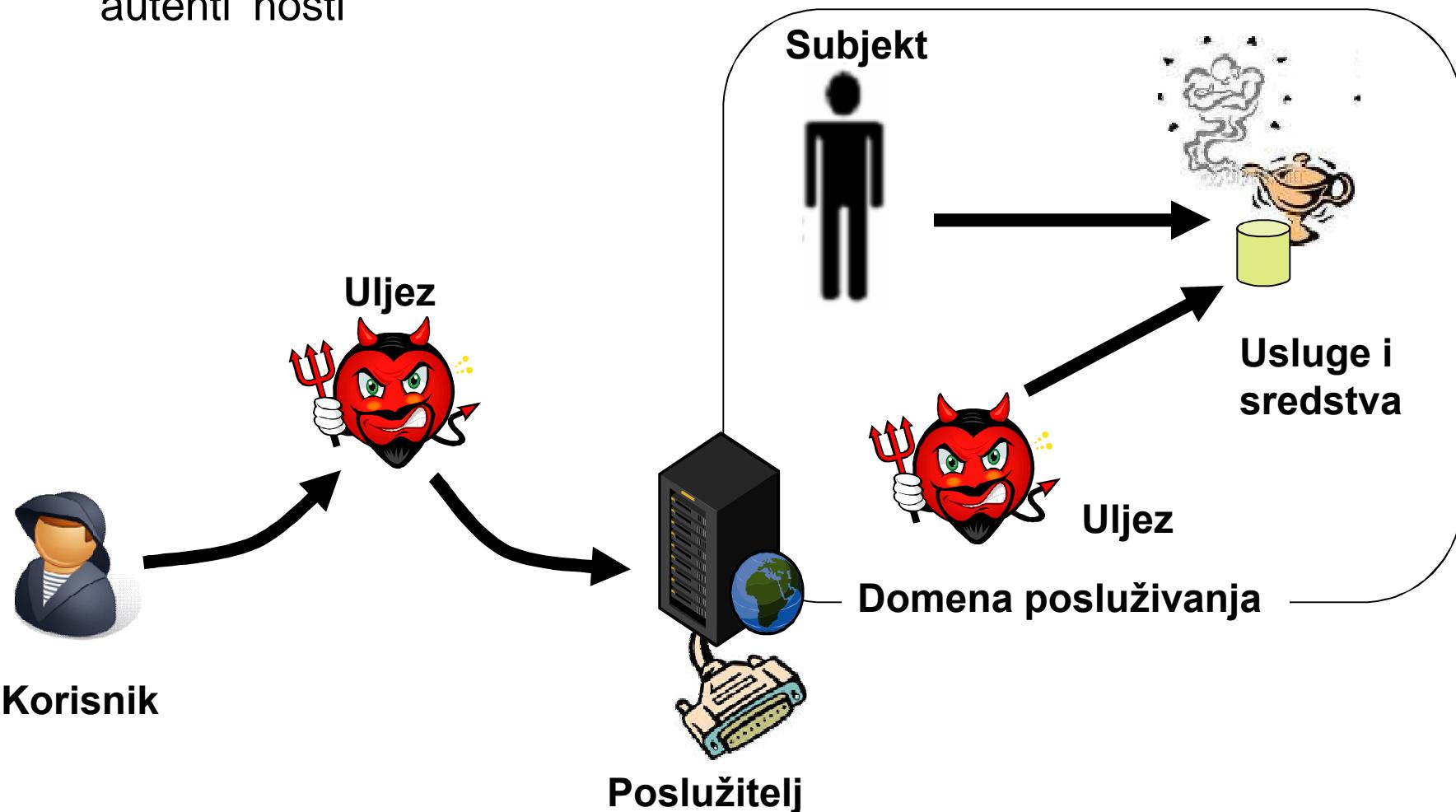
Ugrođavanje sigurnosti prisluzkivanjem

- „ Svojstvo tajnosti



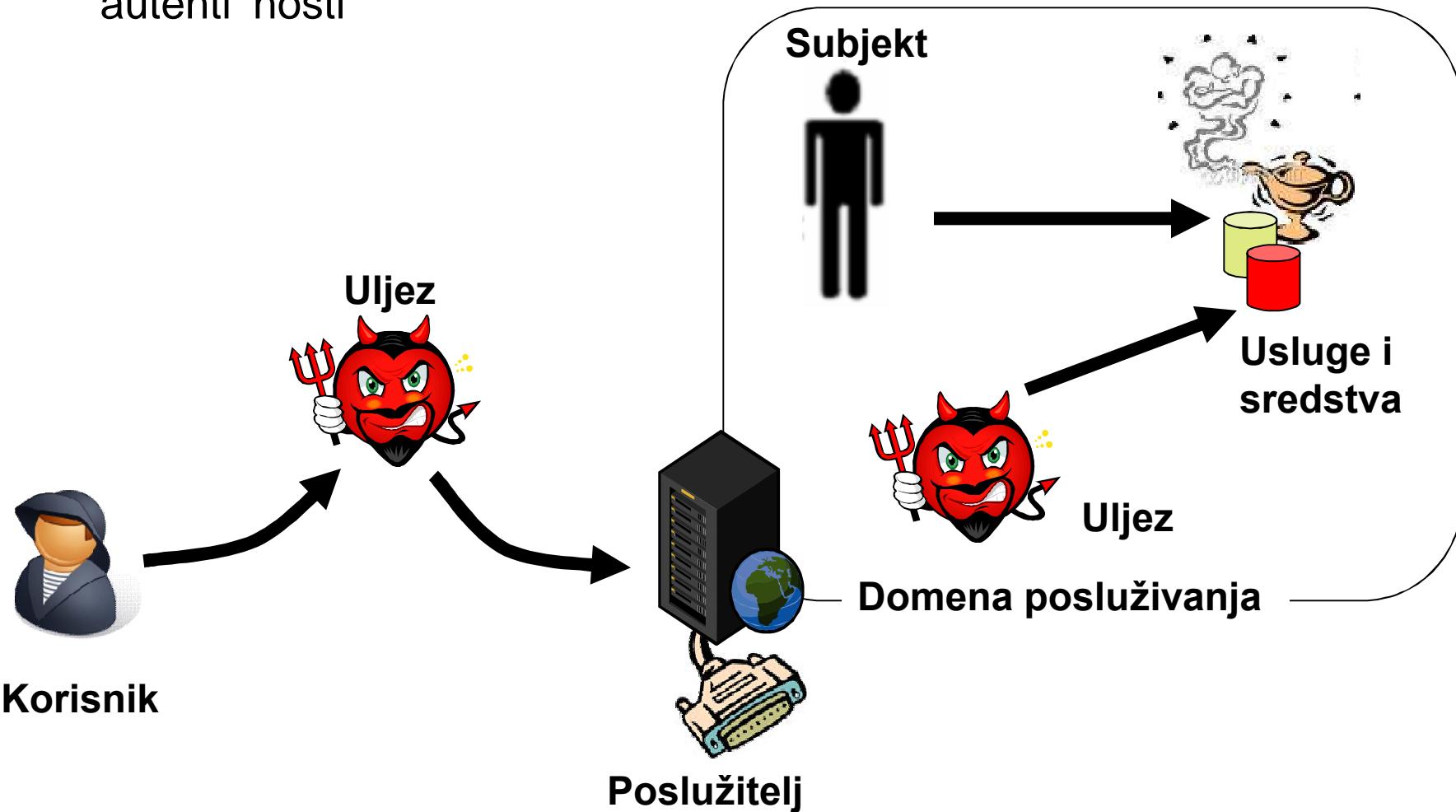
Ugrođavanje sigurnosti izmjenom

- ~ Svojstvo nepovredivosti i autenti nosti



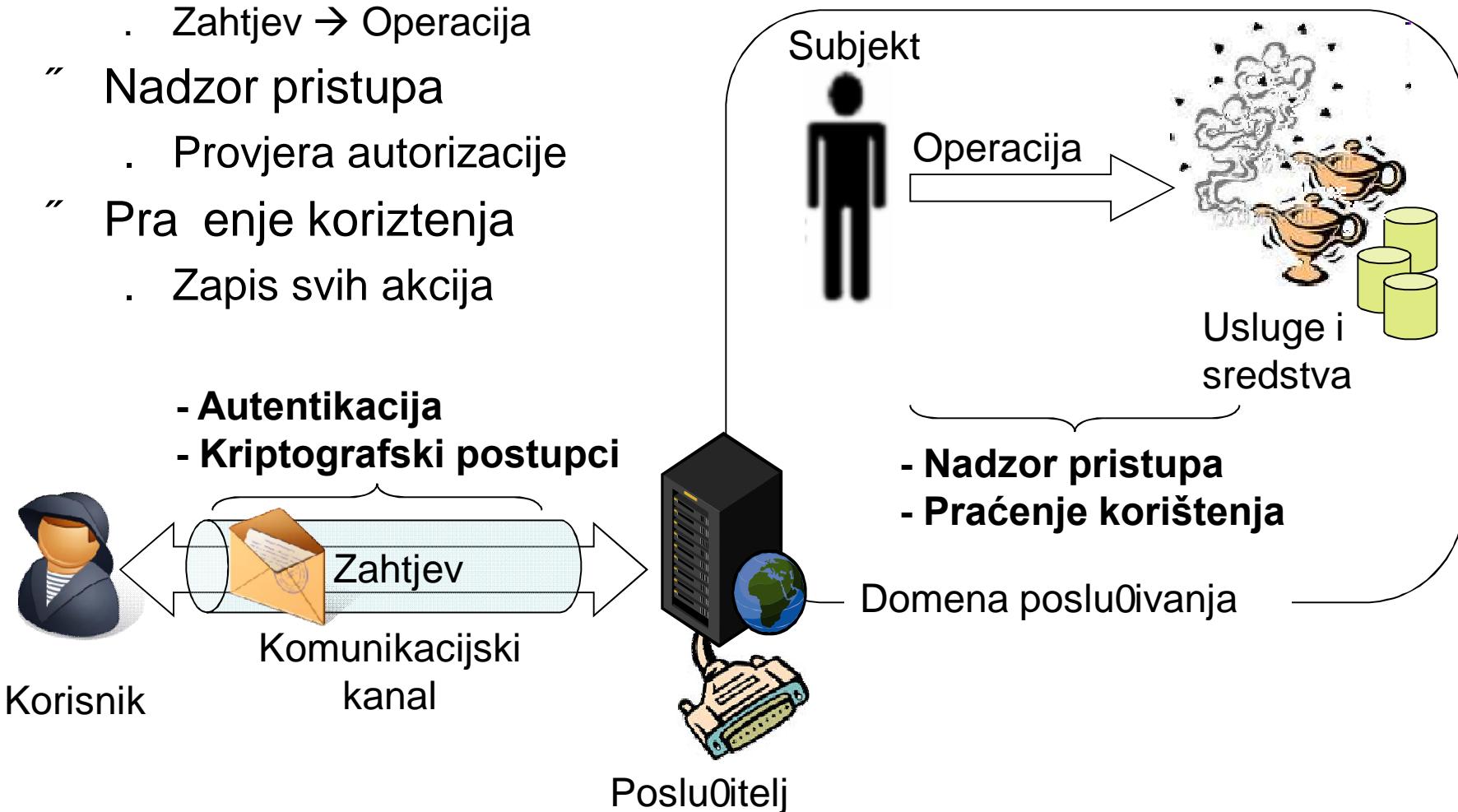
Ugrođavanje sigurnosti izmisljajem

- ~ Svojstvo nepovredivosti i autenti nosti



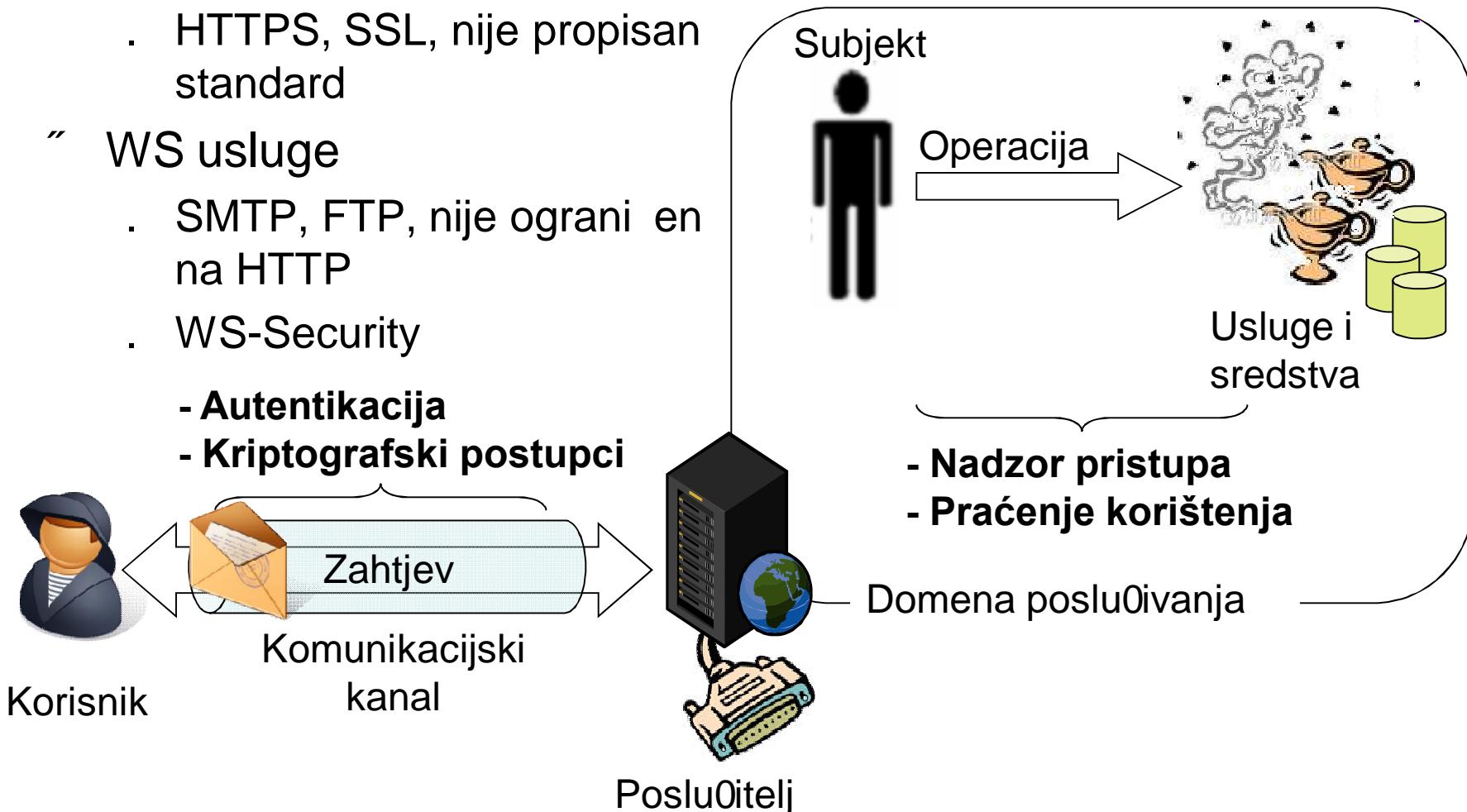
Postupci uspostave sigurnosti

- Autentikacija i kripto-postupci
 - . Korisnik → Subjekt
 - . Zahtjev → Operacija
- Nadzor pristupa
- Praćenje koriztenja
 - . Zapis svih akcija



Postupci uspostave sigurnosti

- „ REST usluge
 - . Prijenos zahtjeva HTTP-om
 - . HTTPS, SSL, nije propisan standard
- „ WS usluge
 - . SMTP, FTP, nije ograničen na HTTP
 - . WS-Security



Kriptografski postupci uspostave sigurnosti

- ~ Simetri na kriptografija
 - . Razmjena ključa je problem



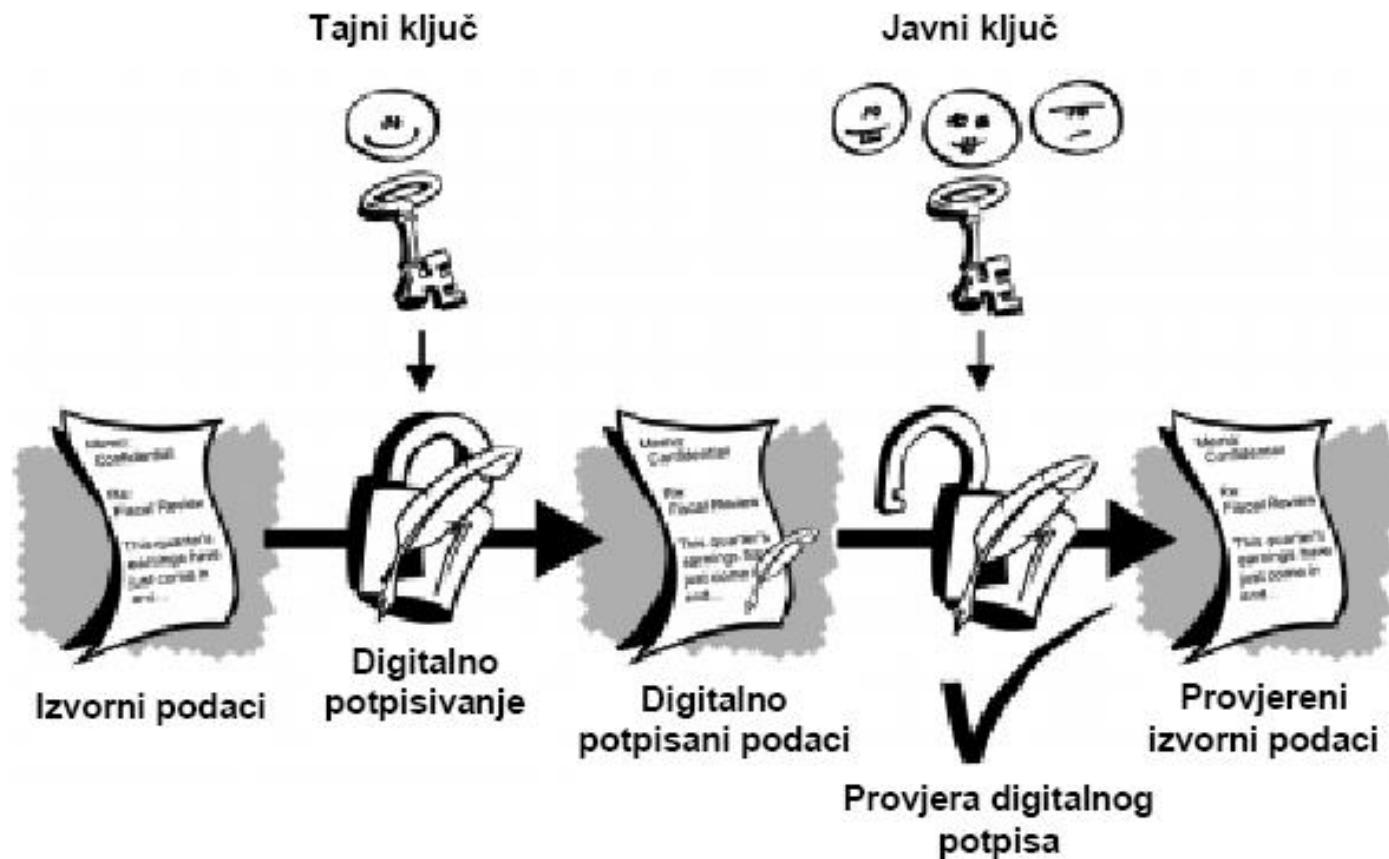
Kriptografski postupci uspostave sigurnosti

- Asimetri na kriptografija
 - Računski zahtjevno



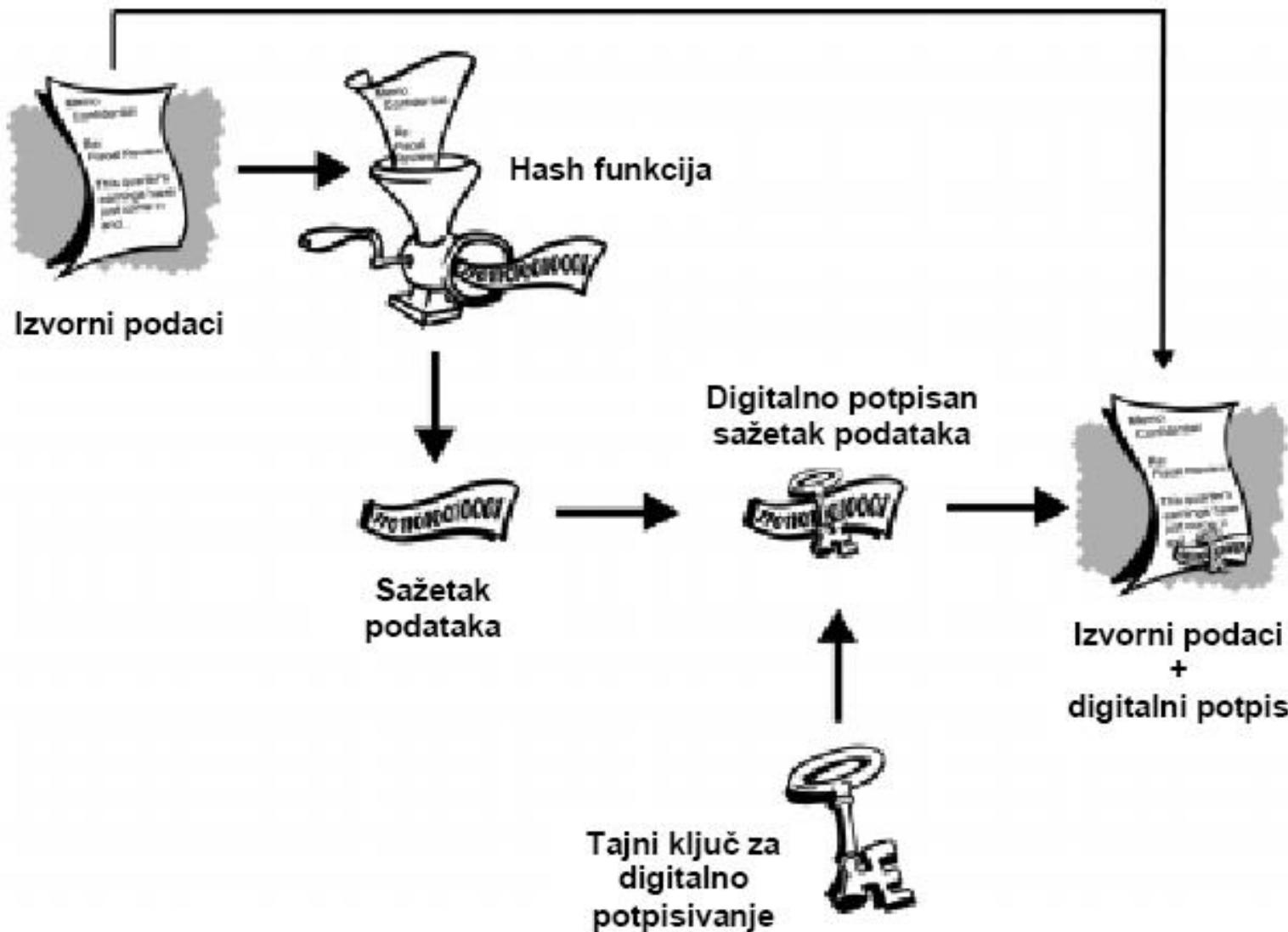
Kriptografski postupci uspostave sigurnosti

- ~ Digitalno potpisivanje
 - . Računski zahtjevno



Kriptografski postupci uspostave sigurnosti

„ Digitalno potpisivanje



Sigurnost REST usluga

Sigurnost REST usluga

- „ Postoje i mehanizmi za sigurnost Web aplikacija
- „ Autentikacija, kriptiranje povjerljivih informacija
 - . **HTTPS, SSL/TLS**
- „ Ispitivanje ispravnosti zahtjeva
 - . **Provjera ulaznih parametara**
 - . **QueryString ili XML**
- „ Nadzor pristupa
 - . **ACL**
 - . **Sredstva URI**
 - . **operacije GET, POST, PUT, DELETE**
- „ Pra enje koriztenja
 - . **Dnevniici korištenja**

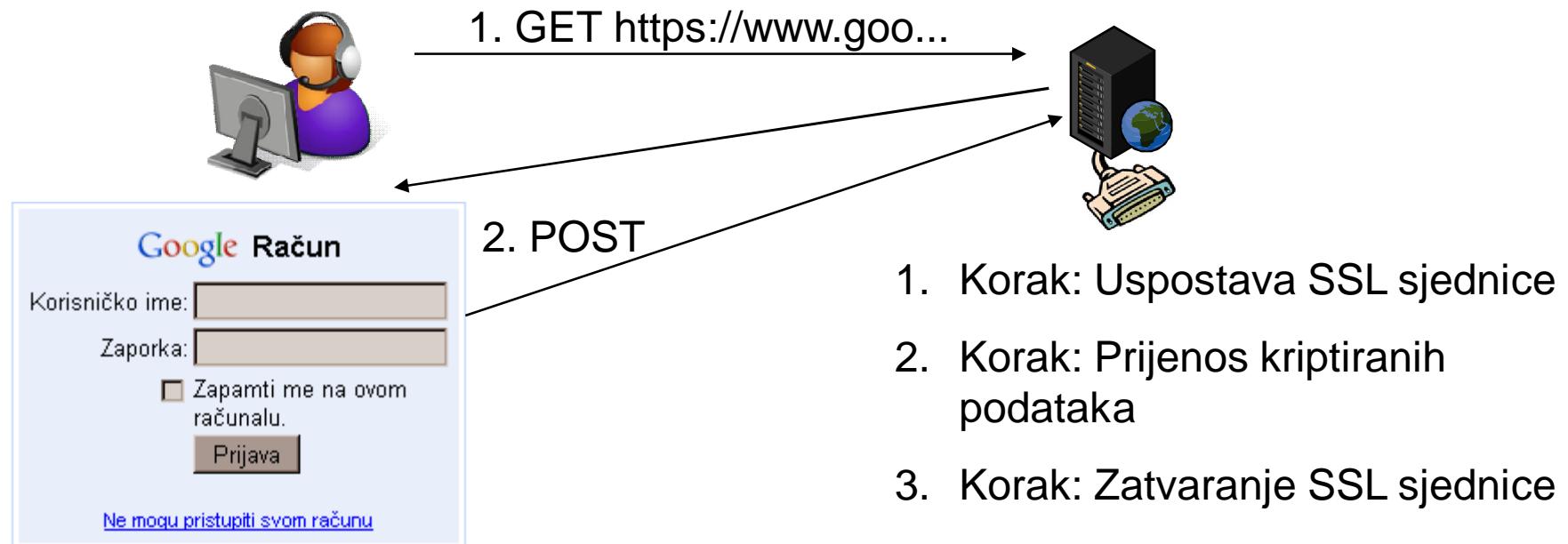
Primjer: REST autentikacija i kriptiranje

- ~ Koristi se REST obrazac GET i POST

- <http://mail.google.com>

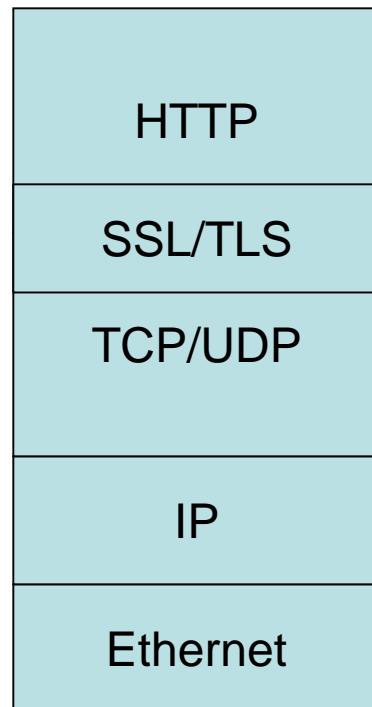
- Redirection to

<https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3DI&bsv=1k96igf4806cy<mpl=default<mplcache=2...>



Uspostava SSL sjednice

- “ HTTPS = HTTP + SSL
- “ Prvo se izvodi SSL protokol uspostave sjednice
- “ Zatim se izvodi HTTP protokol



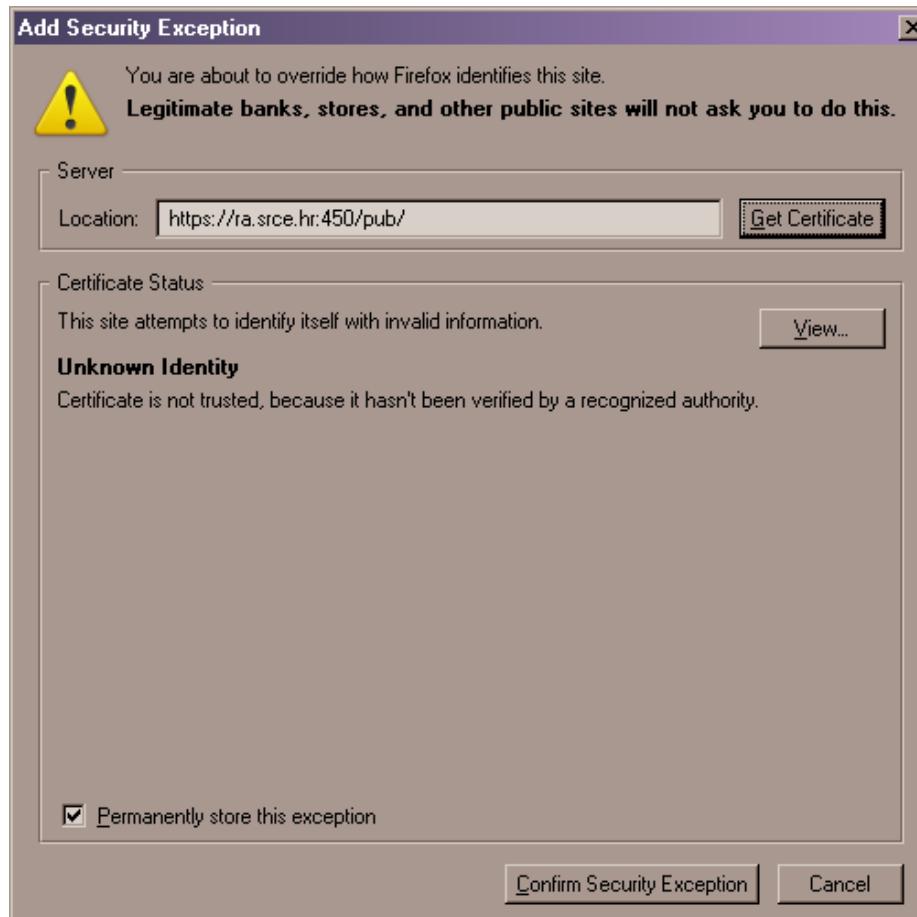
Primjer: Uspostava SSL sjednice

- ~ SRCE, CRO NGI
 - . Registracija na <http://ra.srce.hr/pub/>
 - . Redirection na <https://ra.srce.hr:450/cgi-bin/pub/>
- ~ Uspostava SSL sjednice
 - . Firefox javio da mu certifikat nije povjerljiv
 - . Stranica se ne iscrtava dok se ne završi uspostava sjednice



Primjer: Uspostava SSL sjednice

- “ Zato Firefox nije automatski prihvatio certifikat?
 - **Nije izdan od povjerljivog izvora**
 - **Može se dohvatiti, pogledati i prihvatiti certifikat**



Primjer: Uspostava SSL sjednice

- ~ Certifikat sadrži javni ključ SRCA
 - . Vidi se da nije potписан od povjerljivog izdavača certifikata

Certificate Viewer: "ra.srce.hr"

General | **Details**

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN) ra.srce.hr
Organization (O) edu
Organizational Unit (OU) srce
Serial Number 00:B3

Issued By

Common Name (CN) SRCE CA
Organization (O) edu
Organizational Unit (OU) srce

Validity

Issued On 16.7.2008
Expires On 15.8.2009

Fingerprints

SHA1 Fingerprint BB:63:60:74:E9:C3:12:E3:50:D2:EF:99:C5:6D:91:D6:9E:2F:D6:F5
MD5 Fingerprint E4:65:42:8F:66:66:03:DF:4C:E7:9D:49:83:94:6A:B1

Certificate Viewer: "ra.srce.hr"

General | **Details**

Certificate Hierarchy

SRCE CA
ra.srce.hr

Certificate Fields

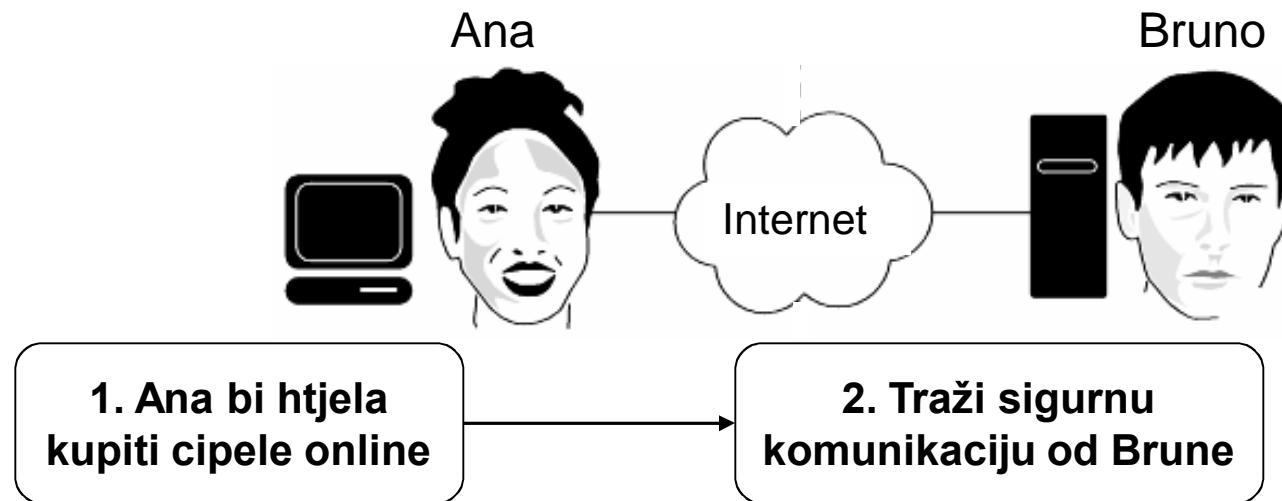
ra.srce.hr

- Certificate
- Version
- Serial Number
- Certificate Signature Algorithm
- Issuer
- Validity
 - Not Before
 - Not After

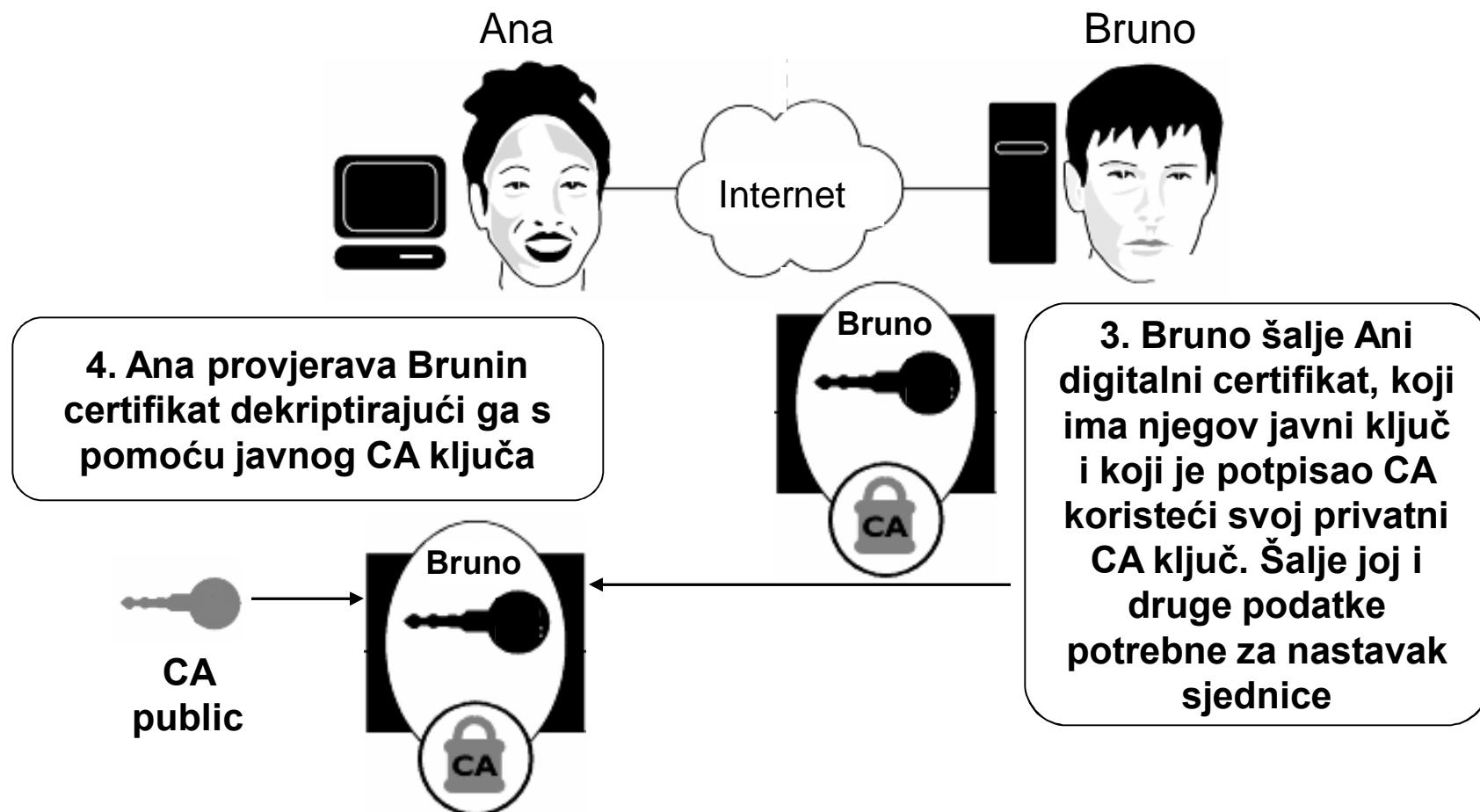
Field Value

Export...

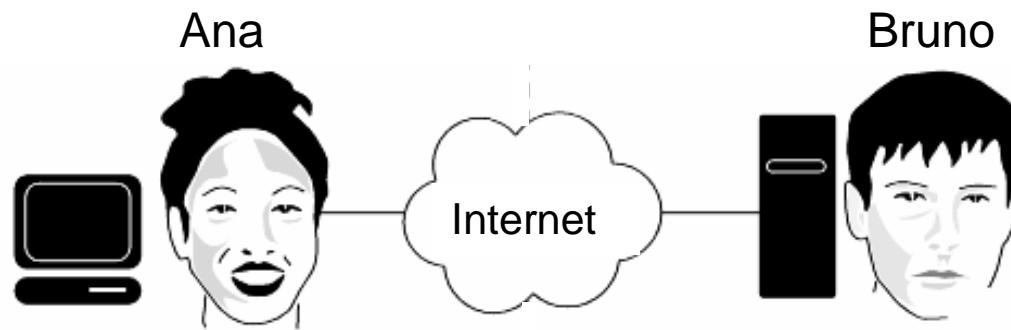
SSL uspostava sjednice: Detalji



SSL uspostava sjednice: Detalji

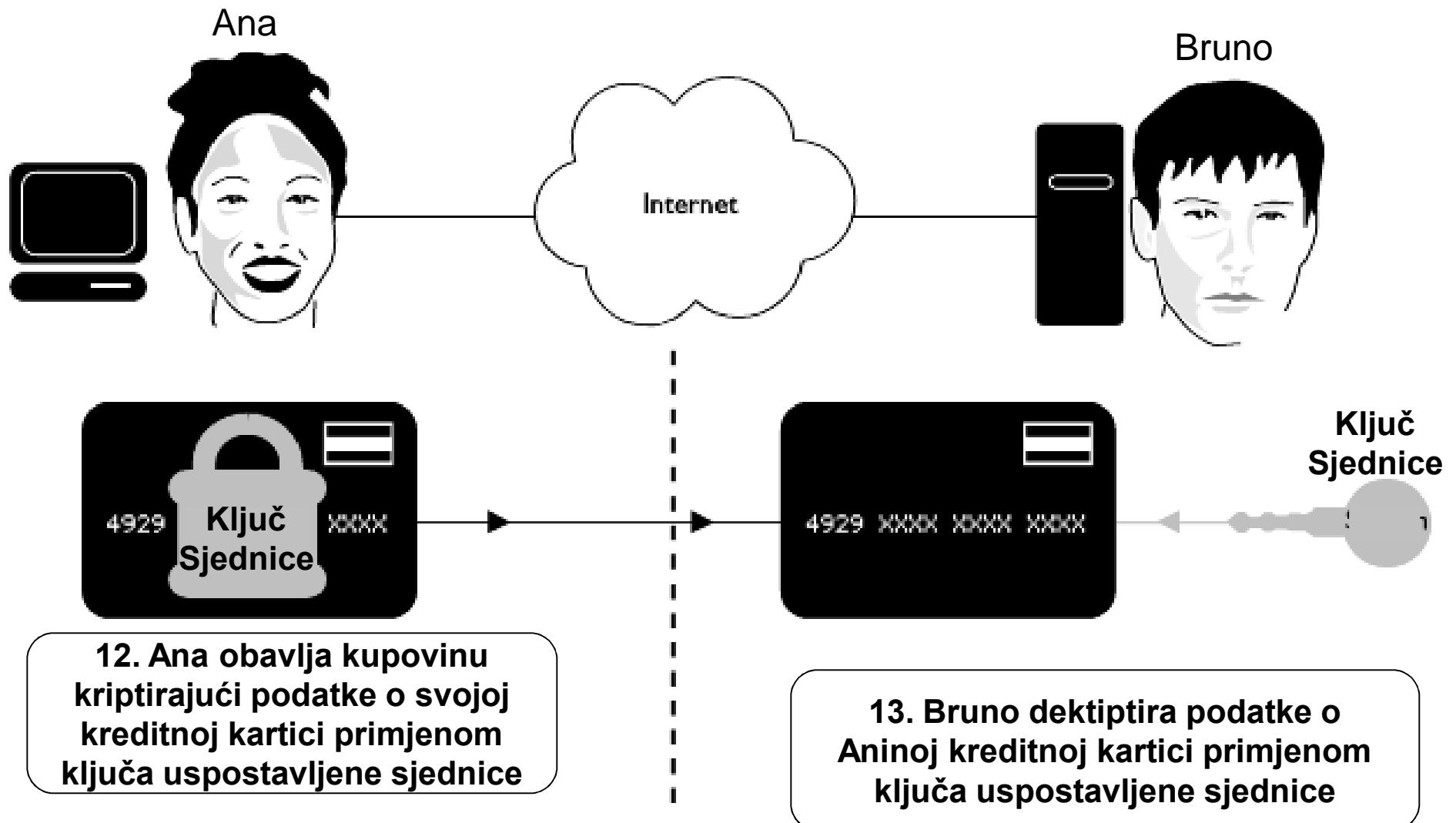


SSL uspostava sjednice: Detalji

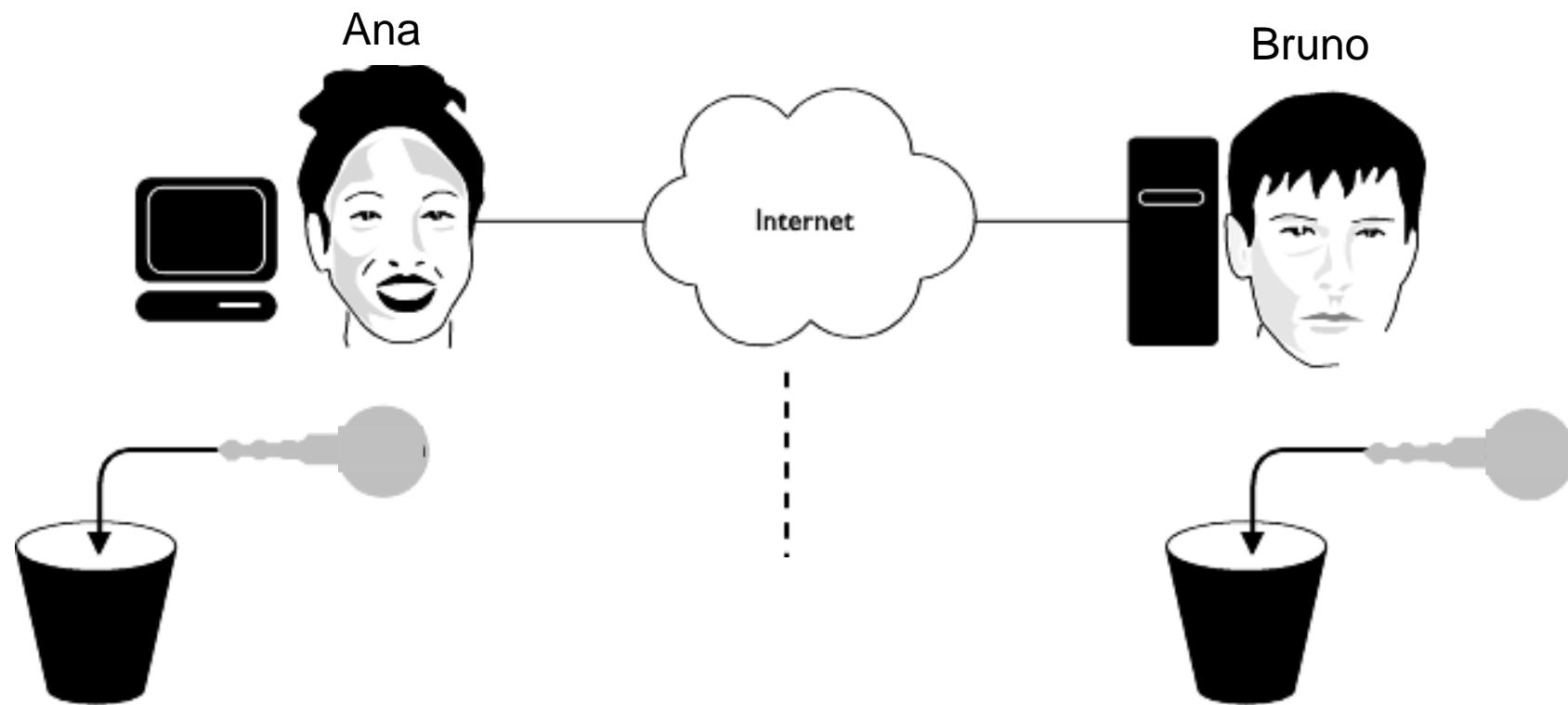


5,6...11. Ana šalje tajni kod na temelju kojeg oboje zasebno računaju novi kod. Zatim uspoređuju izračunate kodove i ako se poklapaju, uspostavljaju sjednicu

SSL prijenos kriptiranih podataka



Zatvaranje SSL sjednice



REST usluge: Nadzor pristupa i pravene koriztenja

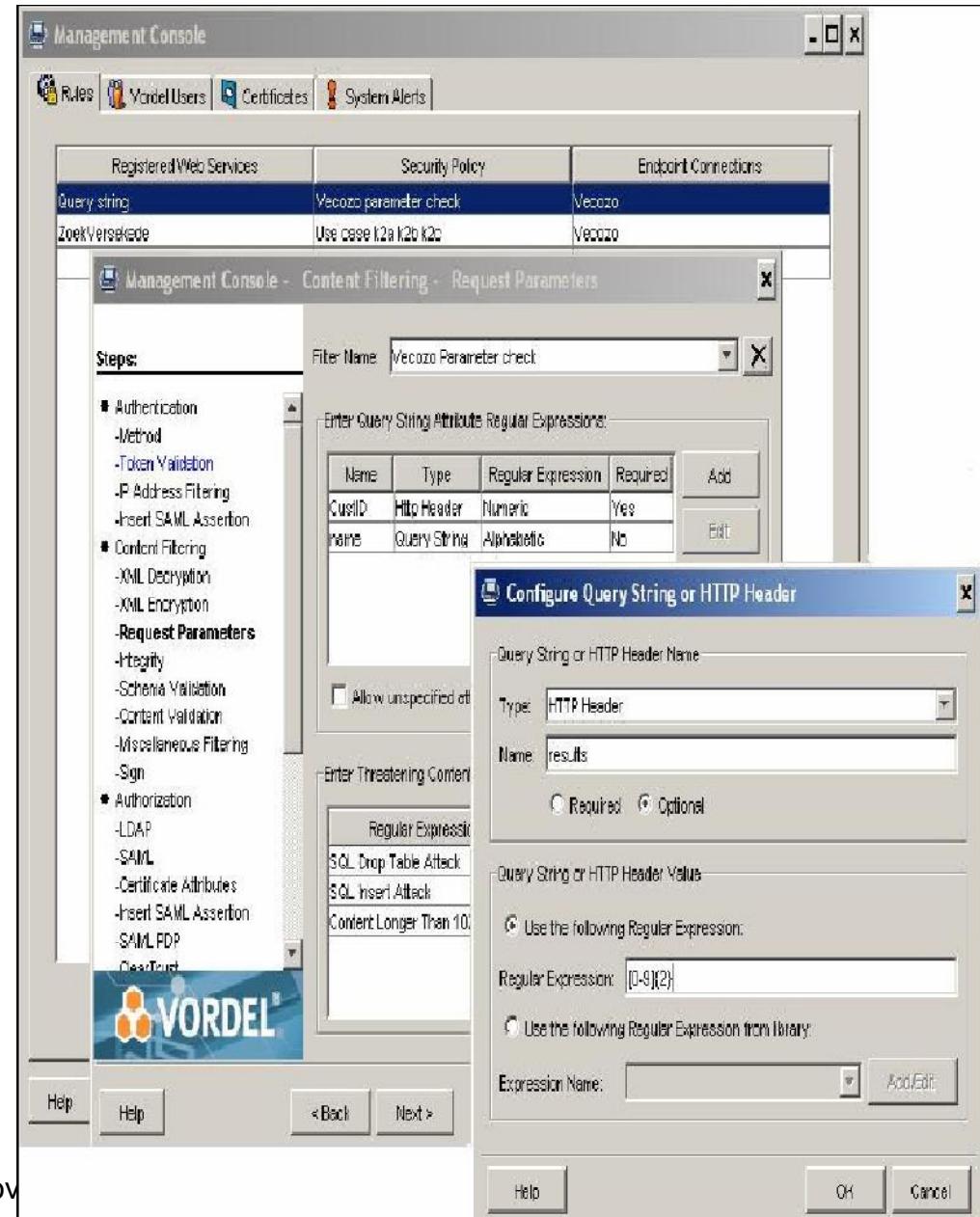
- “ REST ideologija
 - . “**Sve je sredstvo”**
 - . **Sredstva imaju URI**
 - . **operacije GET, POST, PUT, DELETE**
 - . **Operacija i sredstvo navedeni u HTTP zahtjevu**
- Primjeniti postojeće alate i mehanizme za sigurnost Web aplikacija
 - . **Aplikacijska sigurnosna prepreka (firewall)**
 - . **Propušta HTTP promet**
 - . **Provodi nametnuta pravila nad zahtjevima i odgovorima**
 - . **Potrebno definirati pravila**

REST Primjer: Sigurnosna prepreka

„VORDEL“

- Potpora filtriranja QueryStringa
- RegEx za otkrivanje nedozvoljenih vrijednosti parametara
- Sprije ava SQL injekciju

„Pogledajte IIS“



Nadzor pristupa REST uslugama

- “ Nadzor pristupa
 - . Primjeniti ACL (Access Control List)

ACL	Sredstvo1	Sredstvo2	...	SredstvoN
Korisnik1	GET, POST, PUT, DEL	GET	...	GET
Korisnik2	GET	GET, POST, PUT, DEL	...	GET
...
KorisnikM	GET	GET	...	GET

- “ Praćenje koriztenja bilježi
 - . Koje URI sredstvo je korizteno
 - . Kad je korizteno
 - . HTTP zaglavlja
 - . ostali dostupni podaci iz zahtjeva

Primjer: Nadzor pristupa REST uslugama

The screenshot shows a Google Docs interface. At the top, the URL is http://docs.google.com/Doc?id=d92gpw3_35c96rt4hq. Below the address bar, there's a toolbar with icons for back, forward, refresh, and home, followed by a search bar and a link to "Latest Headlines". The main navigation bar includes links for "Most Visited", "Getting Started", "Latest Headlines", "Gmail - Inbox (1) - popovic.miroslav@gm...", "Google Docs - Owned by me", and "Bez naslova -". On the left, the "Google Docs" logo is visible with the word "BETA" underneath. The document title is "Bez naslova" and it was saved by "popovic.miroslav@gmail.com" on "19. studenoga 2008. 23:17". Below the title, there are two buttons: "[« Natrag na uređivanje dokumenta](#)" and "[Dijeli ovaj dokument](#)". The main content area has a section titled "Pozovi osobe" with two radio buttons: "kao suradnici" (selected) and "kao pregledavatelji". A text input field is shown below, with the placeholder "Adrese e-pošte odvojite zarezom." and a link "Izaberi iz kontakata". A button "[Pozovi suradnike](#)" is present. A horizontal line separates this from the "Napredna dopuštenja" section. Under "Napredna dopuštenja", there are two checked checkboxes: "Suradnici mogu pozvati druge" (with a note "Ovo može promijeniti samo vlasnik") and "Svatko može koristiti pozivnice" (with a note "Omogućava popise za slanje" and a link "[Saznajte više](#)"). A large black arrow points from the text "Isključeno – znači primjenjivat će sa ACL za osobe koje pozovemo" to the second checkbox.

Isključeno – znači primjenjivat će sa ACL za osobe koje pozovemo

Potencijalni problem REST sigurnosti

- “ Koje prepostavke ne prepostavljati
 - . Sve REST usluge ispravno implementiraju na elu REST-a
- “ Flickr je kontraprimjer
 - . *Dare Obasanjo from Microsoft has pointed out that Flickr has a “delete” operation that is invoked by a HTTP GET*
 - . GET je operacija koja ne bi smjela mijenjati/brisati podatke
 - . Proizvo a sigurnosne prepreke to ne može predvidjeti i unaprijed ugraditi
- “ REST usluga prima XML parametre
 - . Definirano WADL specifikacijom
 - . Sigurnosne prepreke za Web aplikacije ne provjeravaju XML

Sigurnost WS usluga

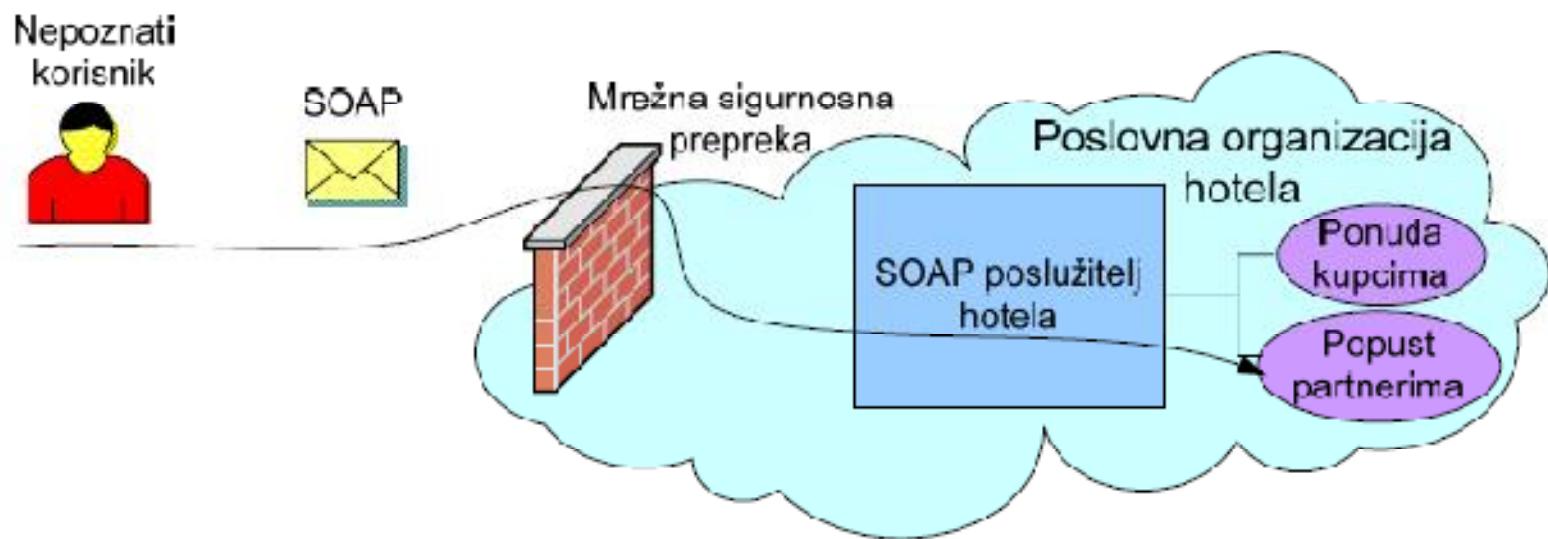
Sigurnost WS usluga

- “ **Prijenosni protokol nije predodređen**
 - . FTP, SMTP, HTTP
- “ **Cjelokupna informacija sadržana u SOAP poruci**
 - . Svi podaci zahtjeva su XML (operacija, parametri poziva)
 - . Svi podaci odgovora su XML
 - . Propisani oblik poruka prema WSDL-u
- “ **SOAP se najčešće prenosi HTTP-om**
 - . Sve sigurnosne stijene propuztaju HTTP promet
 - . SOAP se uvijek zaliže HTTP POST-om

Sigurnost WS usluga

“ Klasična sigurnosna prepreka

- Ne razumije podatke iz SOAP zahtjeva/odgovora
- Nepoznati korisnik nema dozvolu za korištenje popusta



“ Potrebno ostvariti SOAP sigurnost

- Potrebna autentikacija, kriptografija, nadzor pristupa, pravne koriztenja na razini SOAP-a

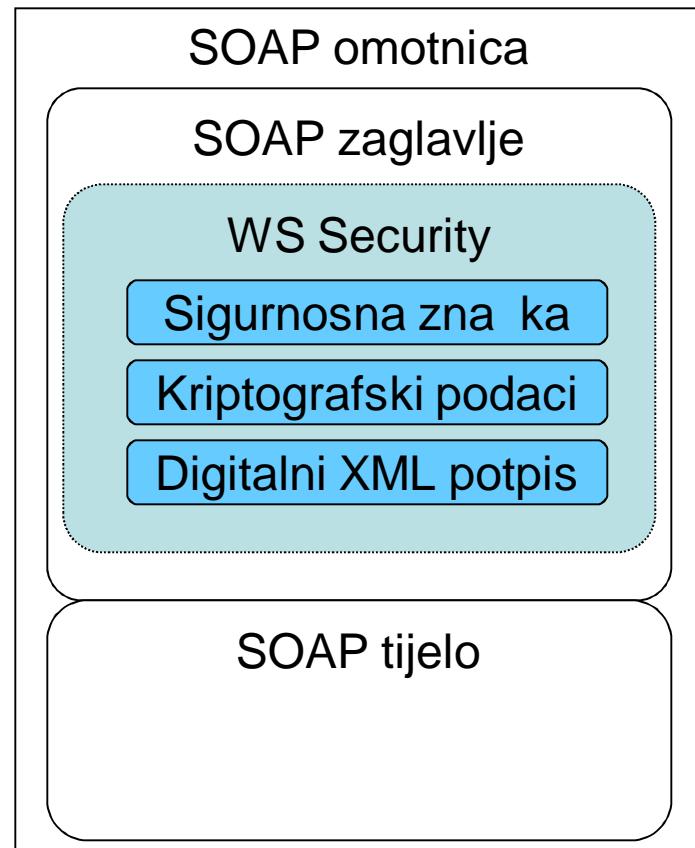
Povjerljivost SOAP komunikacije

„Propisana WS-Security standardom“

- . Dodaje podatke u zaglavje SOAP poruka

„Sigurnosna značka“

- . Tekstualni ime-zaporka (vidljivo svima)
- . Binarni X.509 certifikat (autentikacija slično SSLu)



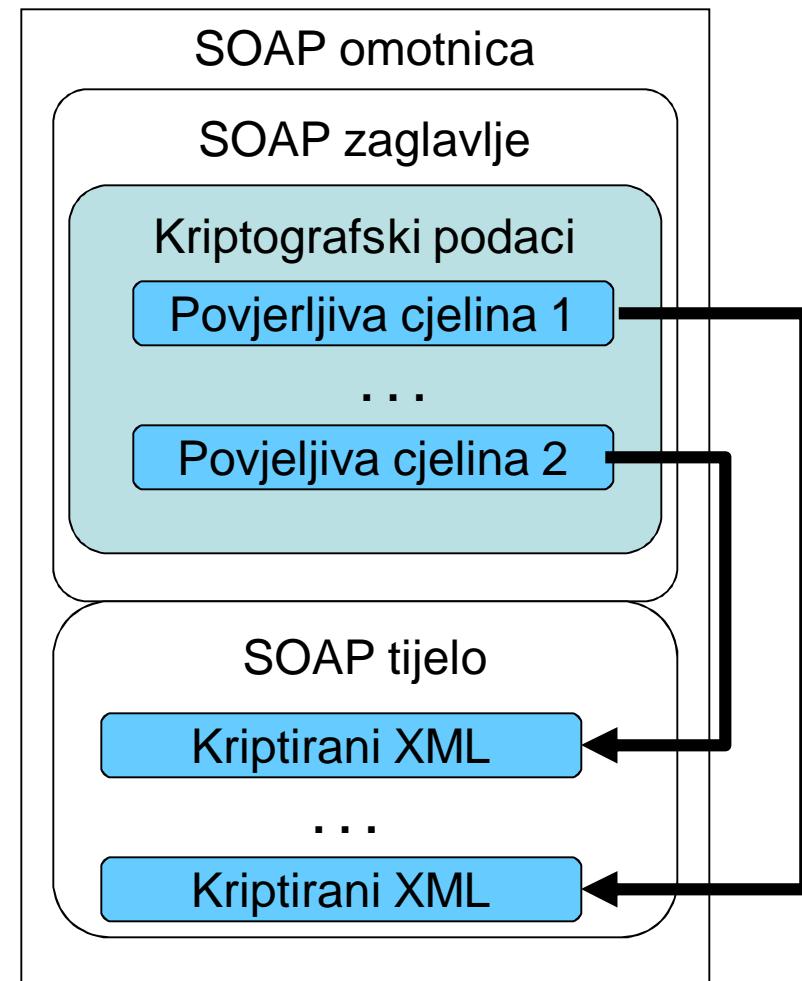
WS-Security: Kriptografski podaci

„Kriptograski podaci sadrže“

- Listu referenci
- Reference pokazuju na cjelinu koja je kriptirana

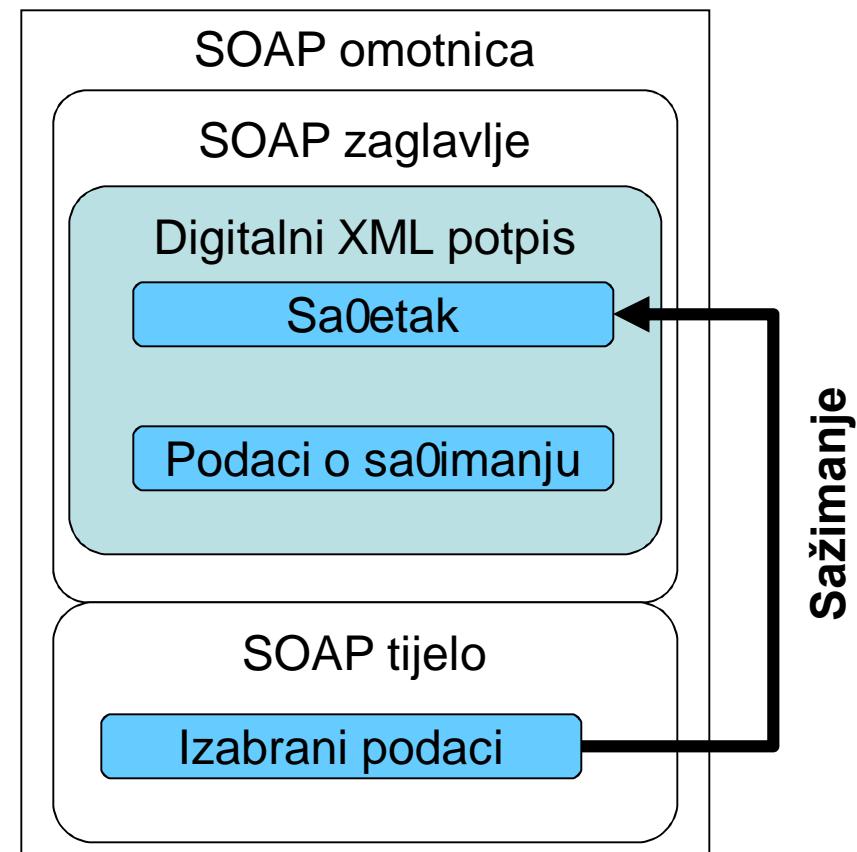
„Moguće kriptirati“

- Korijenski element, tj cijeli XMLdokument
- Cjelokupni XML element
- Unutražnjost XML elementa



WS-Security: Digitalno potpisivanje

- Elementi propisani WS-Security standardom
 - Pojednostavljena slika, nisu prikazani svi elementi



Digitalno potpisivanje: Ujednačavanje XML-a

Ujednačavanje XML-a

- . Semantički isti XML
- . Sačeci različiti
- . Prazni znakovi, prazni elementi, itd.

```
<podaci>
    <osoba ime=%Marko+
        prezime=%Markic+/>
    <osoba ime=%Rero+prezime=%Reric+/>
    <osoba ime=%Iozo+prezime=%Iozic+/>
</podaci>
```

Ujednačavanje

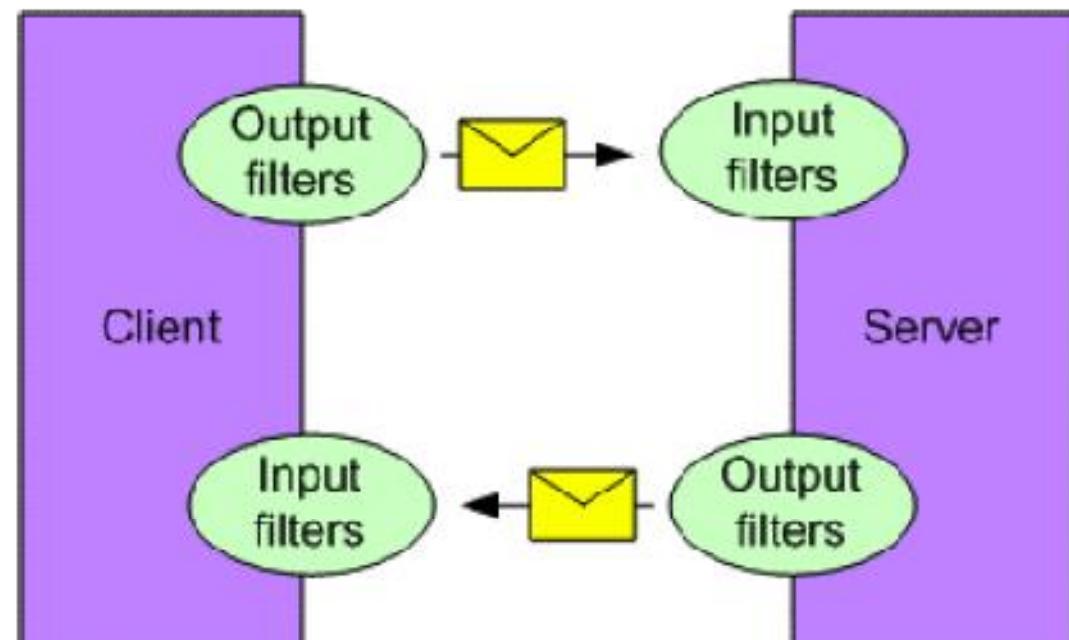


```
<podaci>
    <osoba prezime=%Markic+ime=%Marko+></osoba>
    <osoba prezime=%Reric+ime=%Rero+></osoba>
    <osoba prezime=%Iozic+ime=%Iozo+></osoba>
</podaci>
```

Uspostava SOAP sigurnosti

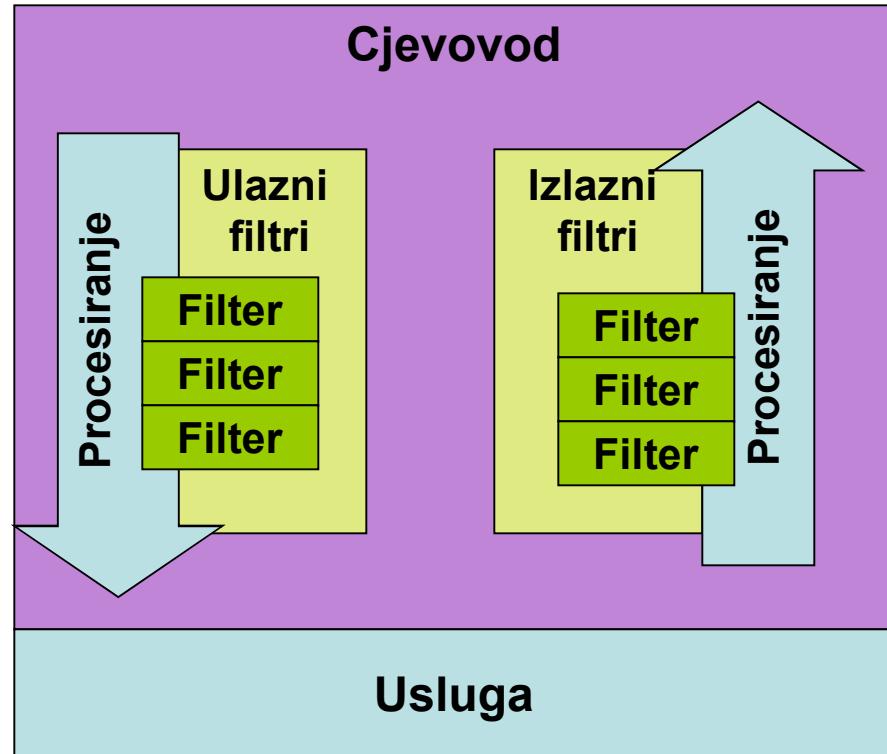
„Razvijeni SOAP dodaci poslužitelju“

- . Npr. Microsoft WS Enhancements
- . Potpora WS-Security dodataka na korisni koj strani
- . Proizvoljni dodaci za obradu SOAP poruka na poslužitelju



WS Security sigurnost

- “ Cjevovod filtera
 - . Ulazni cjevovod
 - . Obrada zahtjeva
 - . Izlazni cjevovod
- “ Ne moraju djelovati simetrično
- “ Zadaci jedinica obrade
 - . Bilježiti koriztenje, vrijeme ulaska i izlaska
 - . Obaviti dekripciju, enkripciju,
 - . Pogledati ACL za operaciju
 - . Provjeriti ulazne parametre



Napredna sigurnost

- “ Složene usluge
 - . **Usluga, postaje korisnik druge usluge**
- “ Primjeri složenih usluga
 - . **Mashups**
 - . **WS kompozicija**
- “ Hijerarhija koriztenja postaje složenija i nastaju problemi
 - . **Ispod 18, ne smije pristupiti**
 - . **Netko tko je iznad 18, proxy prema ljudima ispod 18**
- “ Kako se to riješava
 - . **Ugovorima (contracts, licence agreement)**
 - . **Svi preko istog posredničkog sustava**

Literatura

- “ Dejan Škvorc, %Sigurni prijenos podataka u mrežama s posredničkim sustavima+, diplomski rad, Zagreb, 2003.
- “ Miroslav Popović, %Nadziranje pristupa računalnim sustavima zasnovanim na uslugama+, magisterski rad, Zagreb, 2006.
- “ Tomislav Ohar, %Sigurnosni mehanizmi u logičkim komunikacijskim mrežama s ravnopravnim sudionicima+, diplomski rad, Zagreb, 2005.
- “ Mark O'Neill, %Security for REST Web Services+, http://www.vordel.com/downloads/rsa_conf_2006.pdf, RSA Conference, 2006.