Sveučilište u Splitu  
Sveučilišni odjel   
za stručne studije

**Tim Korisnici**

Seminar u sklopu kolegija  
SIT125: Programiranje u Javi

**Nositelj kolegija:** **Studenti:**  
Josip Vrlić, dipl. ing. rač. Bikić Filip  
 Burić Marin  
 Galac Šime  
 Vrdoljak Karlo

**Sadržaj:**

1. Tjedna izvješća po studentu
2. Opis tehnologija

**1. Tjedna izvješća po studentu**

- *Bilješke rada svakog člana grupe za svaki tjedan*

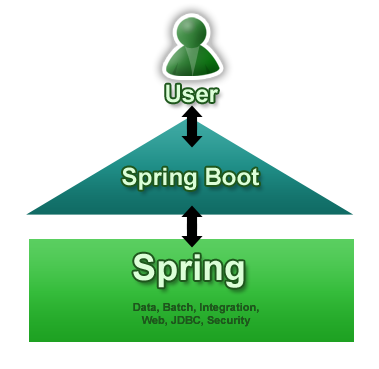
* 1. Tjedan 31.10. – 07.11. 2018.  
     **Vrdoljak Karlo** – Otvorio zajednički repozitorij na GitHubu,  
     napisao dokumentaciju za tehnologije **Spring Boot**, **Spring Tool** **Suite** i **GitHub**.  
      **Bikić Filip** – Pridružio se u repozitorij na GitHubu, napisao dokumentaciju za **Google Compute Engine**, **Google Cloud Shell** i   
     **Web Service Security** (WSS).  
      **Burić Marin** - Pridružio se u repozitorij na GitHubu, napisao dokumentaciju za **Google Cloud Datastore** (NoSQL database), **UBL OASIS** Standard i **E-invoice**.  
       
     **Galac Šime** - Pridružio se u repozitorij na GitHubu, napisao dokumentaciju za **Soap web service**, **WSDL** i **XML**.
  2. Tjedan 07.11 – 14.11. 2018.  
     **Vrdoljak Karlo** – Nastavio izdradu dokumentacije potrebnih tehnologija, obradio **Google Cloud Platform**.  
       
     **Bikić Filip** – Nastavio izdradu dokumentacije potrebnih tehnologija, obradio **XML Digital Signature**.  
       
     **Burić Marin**  – Nastavio izdradu dokumentacije potrebnih tehnologija, obradio tehnologiju **Digitalni certifikati** (CA-Certificate Authority).  
       
      **Galac Šime**  – Nastavio izdradu dokumentacije potrebnih tehnologija, obradio **XSD** i **Rest web service**.
  3. Tjedan 14.11 – 21.11. 2018.  
       
     **Vrdoljak Karlo** – Zaršio svoj dio izdrade dokumentacije potrebnih tehnologija, obradio **Google App Engine**.  
       
     **Bikić Filip** – Zaršio svoj dio izdrade dokumentacije potrebnih tehnologija, obradio **XPATH**.  
       
     **Burić Marin** – Zaršio svoj dio izdrade dokumentacije potrebnih tehnologija, obradio **SSL** (HTTPS).  
       
     **Galac Šime** – Zaršio svoj dio izdrade dokumentacije potrebnih tehnologija, obradio **JSON**.

1. **Opis tehnologija**

*- Dokumentacija svih potrebnih tehnologija za razvoj seminara*

**Spring Boot**

**Spring Boot** je organziran na način da pojednostavni stvaranje, preko platforme **Spring**, aplikacije i servise na stručnoj razini s minimalnom razinom složenosti. Spring Boot također omogućuje da postojeći i novi korisnici vrlo lako koriste segmente Spring-a koji su im potrebni. Može se koristiti u svrhu stvaranja samostalnih (stand-alone) Java aplikacija. SB pruža i 'command line tool' preko kojeg se vrlo lako pokreću Spring skripte.



Spring Boot ne generira nikakav dodatni kod. Nije postoji niti potreba za XML postavkama za rad! Spring skrpite se pišu jezikom **Groovy**, sintaksa vrlo nalik na Javu, ali je pojednostavnjena s obzirom na Javu. Groovy je vrlo intuitivan pri pisanju, stoga je moguće logički deducirati što tuđi kod znači s vrlo malo razmišljanja. Primjer jednostavne skripte:

@Controller

class ThisWillActuallyRun {

@RequestMapping("/")

@ResponseBody

String home() {return "Hello World!"}

}

Preko Spring Boot CLI-a s komandom **‘spring run webapp.groovy’** se pokreće ova jednostavna skripta  
Vise informacija se nalazi na [spring.io](https://spring.io/blog/2013/08/06/spring-boot-simplifying-spring-for-everyone/)

**Spring Tool Suite**

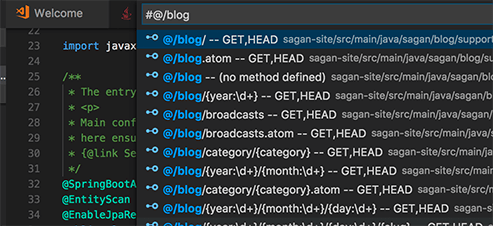
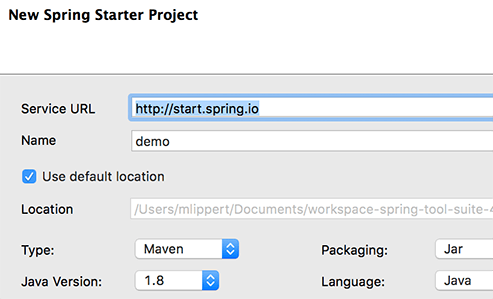
**Spring Tool Suite (STS)** pruža među najboljim okruženjenjima za stvaranje i razvoj aplikacija koje rade preko **Spring platforme**. **STS** pruza mnogo alata za rad s najnovijim izdanjima Jave i Springa te je najčešće na vrhu liste Eclipse-ovih alata. STS podržava razvojni tip **Pivotal tc Server**-a, dogovorena zamjena za Apache Tomcat, vrlo dobro optimiziran za rad u Spring-u.

**Pivotal Tc Server** pruža graficki (real-time) prikaz od performansi aplikacija, što omogućuje softver programerima lakše uočavanje problema u aplikaciji te ubrzava cijeli razvojni proces projekta.

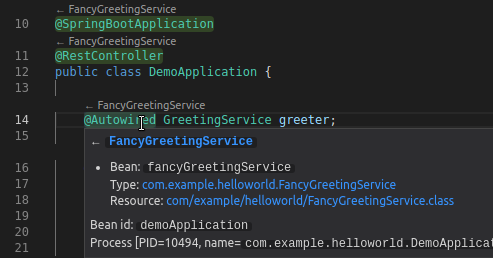
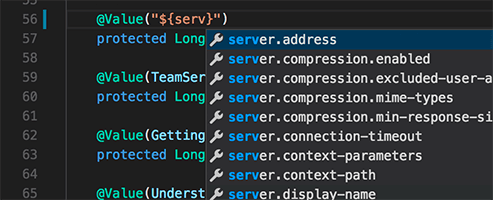
Aktualni STS je **Spring Tool Suite 4**:  
 **-** Najnovija generacija Spring alata za svoje radno okruženje  
 **-** STS4 je većinski napravljen ispočetka  
 **-** Pruža svjetsku razinu podrške za rad nad Spring aplikacijama  
 **-** STS4 se može koristiti u više razvojnih okruženja: **Eclipse, Visual Studio Code, Atom IDE**

**Spring aware**Stvoren za rad sa Spring platformomi Spring Boot-om**,** vrlo lako detektira bilo kakvu Spring aplikaciju i pruža mnoštvo alata i preporuka za pisanje koda.

**IDE diagnostic**Koristi se u svim inačicama STS-a kroz sva razvojna okruženja koja imaju njegovu podršku.  
Služi za dodavanje dodatnih sučelja i uključivanje različitih inačica alata iz STS-a koje bi programeru omogućile lakši razvoj aplikacije.



Intuitivno stvaranje **Spring** podržane aplikacije Olakšane pretrage svih izvornih kodova   
kroz par jednostavnih koraka. za 'importanje' u svoju aplikaciju.



IDE automatski prati što pišete u kodu te odmah  
traži sve moguće nadopune tako da se izbjegnu Uz to pruža dijagnostiku svih djelova vaše  
pogreške na razini tipkanja samog aplikacije čak dok je u pogonu, u svrhu koda. pronalaženja mogućih grešaka

**GitHub**

**GitHub** je distribuirani sustav za upravljenje izvornim kodom nastao 2005. godine iz nezadovoljstva razvijatelja Linux operacijskoga sustava karakteristikama postojećeg sustava za upravljanje izvornim kôdom ("BitKeeper").

**Svojstva GitHuba:**

* **Distribuiranost**, za razliku od ranijih sustava za upravljanje izvornim kôdom (CVS,SVN) GitHub je distribuiran, dakle nakon inicijalnog "kloniranja" spremišta/repozitorija nije nužno za svaki *commit* odnosno inačicu softvera spajati se na središnje spremište, moguće je pohraniti inačicu u lokalno spremište i sinkronizirati spremišta izvornog kôda onda kad je to prikladno
* **Usklađenost s postojećim protokolima**, GitHub podržava HTTP, FTP, rsync, git ili ssh internetske protokole
* **Efikasnost u radu s velikim projektima**, npr. Linux Kernel

Jednostavnost stvaranja repozitorija se jasno vidi na primjeru:

**moj-prvi-projekt** i stvoriti novi repozitorij u njemu:

$ mkdir moj-prvi-projekt // stvara se direktorij na računalu **moj-prvi-projekt**

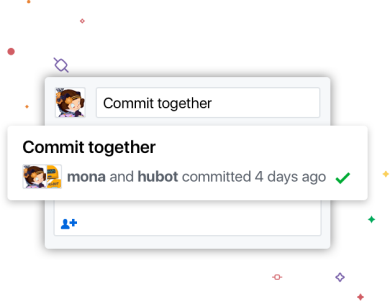
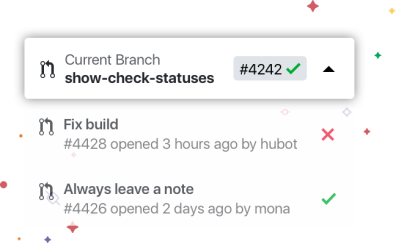
$ cd moj-prvi-projekt // lokaliziramo terminal na novostvoreni direktorij

$ git init // git init stvara repozitorij s imenom izvorne mape

Initialized empty Git repository in /home/user/moj-prvi-projekt/.git/

$

Git naredbe imaju strog tip formatiranja: $ git <naredba> <opcija1> <opcija2> ...  
  
 **GitHub Desktop**

Stvoren u svrhu brzog i jednostavnog pristupa  
GitHubu i korištenja većina njegovih funkcija   
bez potrebe korištenja Git naredbi preko CLI-a.

Vrlo lako se vidi tko je kada napravio 'commit'  
na GitHub.   
Također je vrlo fleksibilan za   
preuzimanje podataka iz jedne ili više grana.

Vrlo lako se primjete izmjene nad kodom  
sa obojanim **'diff'**-ovima.  
GitHub desktop kao i GitHub podržava   
razlikovanje vrsta jezika kojim je bilo koji  
**'push'**-an kod napisan.

* GOOGLE COMPUTE ENGINE

Google compute engine (GCE) je infrastruktura kao usluga (IaaS) komponenta Google cloud platforme koja je građena kao globalna infrastruktura koja pokreće Google search engine, Gmail,Youtube i ostale servise.

GCE omogučava klijentima keiranje i pokretanje vlastitih programa na Google fizičkom hardveru.

GCE nam pruža veći broj skalabilnih virtualnih mašina(VMs) koje služe kao računalni cluster za navedenu svrhu.

GCE-om se može upravljati preko RESTful API-a, CLI-a(Command line interface) ili preko Web konzole.

VMs se mogu pokreniti preko standardne slike (system images) ili prilagođene slike kreirane od strane korisnika.

GCE omogučava administratoru da izabere regiju i zonu gdje će podatkovni resursi biti pohranjeni i korišteni. Do sada na raspolganju stoji United States, Europa i Azija.

GCE također pruža paket alata koji omogučava administratorima izgradnju napredne mreže na regionalnom nivou.

Podržava Linux i windows slike (system images) koje su nužne za pokretanje VMs.

Uporaba GCE virtualnih mašina nije besplatna, već se nakon 10-minutnog rada naplačuje po minuti.

* GOOGLE CLOUD SHELL

Google cloud shell nam pruža Command-line pristup našim cloud resursima iz samog browsera.

Omogučava nam da upravljamo našim projektima i resursima bez instaliranja Google Cloud SDK-a ili drugih alata. Uz pomoć Cloud shell-a, Cloud SDK gcloud command-line alati su nam uvijek dostupni i ažurirani.

Cloud shell pruža command-line pristup instanci virtualne mašine (VM) u terminalskom prozori koji se otvara u web konzoli.

Cloud shell tako pruža sigurnost pristupa projektima i resursima korištenjem autorizacije.

Cloud shell također pruža široki izbor već instaliranih i ažuriranih command-line alata iz basha,sh-a,emacs-a,vim-a, kao i administrativnih alata kao što su mysql client i kubernetes.

Osim command-line alata Cloud shell također pruža široki izbor razvojnih alata kao što su Java,Python,Go,node.js, PHP i uby.

Cloud shell pruža 5GB memorije na persistent disku za pohranu podataka koji je mountan kao $HOME direktorij na Cloud shell instanci.

* WEB SERVICE SECURITY (WSS)

WSS je SOAP ekstenzija koja uvodi sigurnosni sloj kod web usluga.

U 2002, Microsoft, IBM, i Verisign su izdali WS-Security specifikaciju jer SSL/TLS nije bio dovoljan kada SOAP poruka prolazi kroz posredne točke.

U 2003, WS-Security je predložen kao OASIS norma, i u 2004 je izdan kao OASIS norma.

WS-Security specificira SOAP sigurnosne ekstenzije koje omogućavaju tajnost uporabom XML Encryption i integritet podataka uporabom XML Signature.

WS-Security također uključuje profil koji specificira kako umetnuti različite tipove binarnih i XML sigurnosnih tokena u WS-Security zaglavljima za provjeru autentičnosti i autorizacijske namjere:

* Korisničko ime s opcionalnim pregledom lozinke (definira kako korisnik Web usluge može dostaviti korisničko ime kao ovlaštenje za provjeru autentičnosti; uz korisničko ime može biti priložen *hashed* lozinka).
* X.509 certifikat (potpisana struktura podataka dizajnirana za slanje javnog ključa stranki koja prima).
* Kerberos etiketa (token za provjeru autentičnosti i sesiju).
* Security Assertion Markup Language (SAML) sigurnosni tokeni (više detalja o SAML kasnije u ovom dokumentu).
* REL dokument (*rights expression language* (REL) odobreni tokeni umetnuti u WS-Security zaglavlja se rabe za autorizaciju).
* XCBF dokument (definira kako uporabiti XML Common Biometric Format (XCBF) jezik za provjeru autentičnosti s WS-Security specifikacijom).

**Google Cloud Datastore (NoSQL database)**

Cloud Datastore je „highly-scalable“ NoSQL baza podataka za aplikacije.

Automatski obavlja brisanje i replikaciju.

Pruža mnoštvo mogućnosti kao što su ACID transakcije,upite slične SQL,indekse i još mnogo toga.

Nesmetano i automatski mijenja podatke, omogućujući aplikacijama održavanje visokih performansi.

Podržava različite vrste podataka, uključujući integer,float,stringove,datume,binarne podatke.

Omogućuje prikaz entitetskih statistika, upita baze podataka, pregled indeksa i sigurnosno kopiranje / vraćanje podataka.

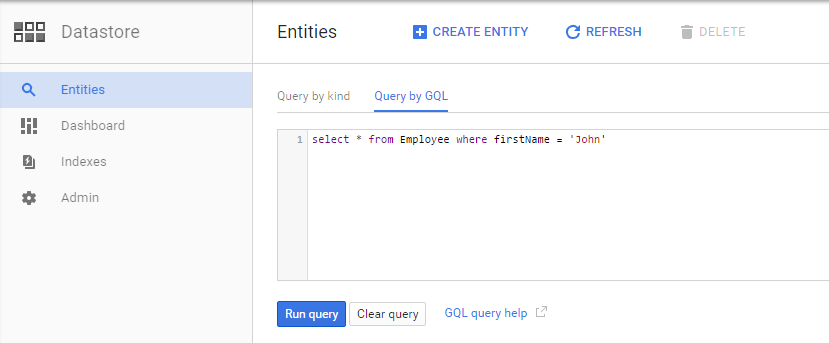
Cloud Datastore je u potpunosti vođen, što znači da Google automatski obrađuje replikaciju kako bi pružio vrlo dosljednu i dostupnu bazu podataka.

Podržani su upiti djeteta roditelja,transakcije i indeksi.

**Jezici** : JAVA, NODE.JS, PYTHON, GO, PHP

**Cijena**

* 1 GB Free
* 50k Daily read/write operation
* Upit za konzolu



**UBL OASIS Standard**

UBL, Univerzalni poslovni jezik, definira besplatnu knjižnicu standardnih XML poslovnih dokumenata koji podržavaju digitalizaciju komercijalnih i logističkih procesa za domaće i međunarodne opskrbne lance kao što su nabava,transport, logistika, intermodalni teretni promet i drugi.

UBL se može smatrati *lingua-francima* - formatom (formatom podataka) koji omogućuje različitim poslovnim aplikacijama i trgovinskim zajednicama razmjenu informacija duž lanaca opskrbe pomoću uobičajenog formata.

UBL je dizajniran da se priključi izravno u postojeće poslove, računovodstvene, pravne, revizijske,eliminirajući tradicionalni faksove, skeniranja, i time osigura ulaznu točku u elektronički posao za male i srednje tvrtke.

Iako je dizajniran za uporabu u poslovnim lancima opskrbe, može biti (i bio) prilagođen za druge kontekste uporabe.

Dizajn UBL-a temeljen na knjižnici ima nekoliko dubokih praktičnih implikacija.To znači da zajedničke strukture podataka kao što su adresa i stavka retka implementiraju se točno s istim XML strukturama u svakoj vrsti dokumenta koji ih koristi.

Kako bi odgovaralo zahtjevima specifičnih trgovinskih odnosa, podatkovne strukture proizvoljne složenosti mogu se dodati (uzajamnim dogovorom) UBL dokumentima bez prekidanja XML validacije prema standardnim shemama.

Počevši od usvajanja UBL-a iz 2005. godine za sve fakturiranje u javnom sektoru u Danskoj (OIOUBL), UBL je postao temelj za niz uspješnih europskih okvira javne nabave, uključujući EHF (Norveška), Svefaktura (Švedska), ePrior (Europska komisija DIGIT), Nacionalna zdravstvena služba (UK) i PEPPOL, paneuropska platforma javne nabave. PEPPOL zajednica (OpenPEPPOL) služi državnim agencijama i njihovim dobavljačima iz Austrije, Danske, Francuske, Irske, Italije, Norveške, Poljske i Švedske putem mreže od preko 100 pristupnih točaka, a sve razmjenjujući dokumente sukladne UBL.

UBL je također utemeljen na nizu napora u području transporta i logistike, uključujući Europski zajednički okvir (Europska komisija), DTTN (Luka Hong Kong), TradeNet (Luka Singapur), Electronic Freight Management (SAD) i Freightgate (globalno).

**E-invoice**

**Electronic invoicing** (**e-invoicing**) je oblik elektroničke naplate.

Koriste ga trgovinski partneri, kao što su kupci i njihovi dobavljači, kako bi prezentirali i pratili transakcijske dokumente jedni s drugima i osigurali uvjete njihovih dogovora o trgovanju.

Ovi dokumenti uključuju fakture, narudžbenice, debitne note, bilješke o kreditnim karticama, uvjete plaćanja i upute te dozvole za doznaku.

E-invoice uključuje niz različitih tehnologija i mogućnosti unosa, a koristi se kao krovni izraz za opisivanje bilo kojeg načina na koji se faktura elektronički prikazuje kupcu za plaćanje.

E-račun se može definirati kao strukturirani podaci o fakturi koji su izdani u [elektronskoj razmjeni podataka](https://translate.googleusercontent.com/translate_c?depth=1&hl=hr&prev=search&rurl=translate.google.hr&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Electronic_data_interchange&xid=17259,15700021,15700124,15700149,15700186,15700191,15700201,15700214,15700230&usg=ALkJrhhRAcepKSASTf4I48TZ8rD90ofNGQ" \o "Elektronska razmjena podataka) (EDI) ili [XML](https://translate.googleusercontent.com/translate_c?depth=1&hl=hr&prev=search&rurl=translate.google.hr&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/XML&xid=17259,15700021,15700124,15700149,15700186,15700191,15700201,15700214,15700230&usg=ALkJrhibU6GzLYEmhgjR1oClpTsP5GmqAw" \o "XML) formata, a možda i putem internetskih obrazaca.Ovi se dokumenti mogu razmjenjivati ​​na brojne načine, uključujući EDI, XML ili [CSV](https://translate.googleusercontent.com/translate_c?depth=1&hl=hr&prev=search&rurl=translate.google.hr&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Comma-separated_values&xid=17259,15700021,15700124,15700149,15700186,15700191,15700201,15700214,15700230&usg=ALkJrhgjUSd5p08Iqyg67YBGNnX7-nKb4Q" \o "Vrijednosti odvojenih zarezima) datoteke. Može ih se prenijeti putem e-pošte, virtualnih pisača, web aplikacija ili FTP mjesta. Tvrtka može koristiti softver za slikanje kako bi prikupila podatke iz PDF ili papirnatih faktura i unijela ih u svoj sustav fakturiranja

Raznolikost formata i kanala za isporuku komplicira korištenje e-računa. Da bi se to pojednostavilo, moguće je koristiti .INV ekstenziju, što ih računovodstvenim softverima čini lakim za otvorit. INV datoteka može biti u standardu koji zadovoljava XML format.

Da biste omogućili e-fakturiranje, mora postojati način za gledanje transakcija, obično ERP ( [Enterprise Resource Planning](https://translate.googleusercontent.com/translate_c?depth=1&hl=hr&prev=search&rurl=translate.google.hr&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Enterprise_Resource_Planning&xid=17259,15700021,15700124,15700149,15700186,15700191,15700201,15700214,15700230&usg=ALkJrhjM-bxkk5ZpSvgHA8o-l65-ztseqw" \o "Planiranje resursa poduzeća) ) ili računovodstveni sustav. Usmjeravanje i pravila moraju se uspostaviti u specifikaciji projekta. To obično uključuje članove platnih obveza, IT, a ponekad i nabavu.

**Soap web service – Simple Object Access Protocol**

* Protokol za slanje poruka za izmjenu informacija u implementaciji web servisa i računalnih mreža
* Koristit XML
* Oslanja se na protokole aplikacijskog sloja – HTTP ili SMTP
* Envelope(omotnica), definira strukturu poruke I kako ju koristit
* Skup pravila za izražavanje instanci aplikacijskog sloja
* Konvencija za prikaz procedura poziva I odgovora

Pravila za sintaksu

* A SOAP poruka MORA biti kodirana u XML-u
* A SOAP poruka MORA koristiti SOAP Envelope namespace
* A SOAP poruka MORA koristit SOAP Encoding namespace
* A SOAP poruka NE SMIJE sadržavati DTD reference
* A SOAP poruka NE SMIJE sadržavati XML Processing Instructions

ELEMENTI

Envelope(required) –korijenski element koji enkapsulira cijelu informaciju

Header(Optional) − sadržava određene attribute koji pomažu u obradi poruke

Body(required) − sadržava XML kod koji nas zanima

Fault(optional) – sadrži informacije o pogreškama

<https://www.w3schools.com/xml/xml_soap.asp>

**WSDL**

* WSDL - Web Services Description Language
* WSDL se koristi za opisivanje web servisa
* Koristi XML

|  |  |
| --- | --- |
| Element | Opis |
| <types> | Definira tipove koje koristi web servis |
| <message> | Definira podatkovne elemente za svaku operaciju |
| <portType> | Opisuje operacije koje mogu biti izvršene I poruke koje su uključene |
| <binding> | Definiria protocol I tip podataka za svaki port |

## WSDL Binding to SOAP

 binding element ima 2 atributa – ime I tip.

Ime (bilo koje se može koristiti) definira ime binding-a, I tip atributa koji pokazuje na port za bindanje

soap:binding element ima 2 atributa - style i transport.

Style atribut može biti "rpc" or "document". Transport atribut definira SOAP protocol koji se koristi(HTTP ili SMTP)

operation element definira svaku operaciju koju portType otkriva

Za svaku operaciju odgovarajuća SOAP akcija moa biti definirana. Također, potrebno je navesti ulaz I izlaz koji su kodirani

<https://www.w3schools.com/xml/xml_wsdl.asp>

**XML**

XML - eXtensible Markup Language.

XML se koristi za pohranjivanje I transport podataka

XML je dizajniran da bude čitljiv I čovjeku I stroju

XML ne radi ništa, on je samo informacija zapakirana u tagove

XML I HTML su dizajnirani s različitim ciljevima

* XML je dizajniran da prenosi podatke – s fokusom na ono što podaci jesu
* HTML je dizajniran da pokazuje podatke – s fokusom kako podaci izgledaju
* XML tagovi nisu predefinirani kao u HTML-u

Kada se prikazuju podaci u HTML-u, ne treba uređivati HTML datoteke kad se podaci promijene, s XML-om se podaci mogu spremiti u odvojene XML datoteke

Čitanje I uređivanje XML datoteke se može jednostavno napraviti s JavaScipt-om.

<https://www.w3schools.com/xml/xml_usedfor.asp>

**Google Cloud Platform**

**Google Cloud Platforma** je pružana od strane Googlea, sadrži skupinu servisa za programiranje na cloudu. Neki od pruženih servisa ubrajaju i podršku za spremanje podataka, analizu podataka, strojno učenje i slično. Za registraciju na GCP je potrebna **kreditna kartica** ili **bankovni račun**.  
  
**Sadržaj GCP**

**Compute**App Engine – Platforma za pokretanje Java, PHP, Python, C#, .NET, Ruby, Node.js i Go aplikacija  
Compute Engine – Infrastruktura za pokretanje MS Windows i Linux virtualnih mašina  
Cloud Functions – Funkicje kao servis za pokretanje 'event-driven' kod baziranog nad Node.js

**Pohrana i Baze Podataka**Cloud Spremište – Objektno spremište za nestrukturirane podatke.  
Cloud SQL – Baza podataka kao servis baziran nad MySQL i PostgreSQL.  
Cloud BigTable – Rukovođen NoSQL servis za baze podataka  
Cloud Spanner – Horizontalno skalabilan, snažno konzistentna, Relacijska Baza Podataka  
Persistent Disk – Block spremište za Compute Engine virtualne mašine

**Networking**VPC – Virtualni privatni cloud za upravljanje nad softver definiranim networkom cloud resursa  
Cloud Load Balancing – Softverski definirani servis za upravljanje stresom nad prometom podataka  
Cloud Armor – pruža sigurnost protiv napada 'hakera' npr. DDos napadi.

**Alati za Upravljanje**Stackdriver – promatranje, zabilježavanje te dijagnostika za aplikacije na GCP i AWS  
Cloud Deployment Manager – Alat za pokretanje GCP resursa koji su definirani na gotovim platformama  
Cloud Console – Web konzola za upravljanje GCP resursima  
Cloud Shell – Preko browsera (Firefox i slični) CLI za pristupanje GCP resursima.  
Cloud Console Mobile App – Android i iOS aplikacija za pristup GCP resursima.

**Identitet i Sigurnost**Cloud Identity – Single sign on (SSO) servis baziran na SAML 2.0 i OpenID.  
Cloud IAM – Identitiy & Access Managment (IAM) servis za definiranje postavki baziranih na   
role-based access control  
Cloud Identity-Aware Proxy – Servis za kontrolni pristup cloud aplikacijama koje rade na GCP bez korištenja VPN-a  
Cloud Data Loss Prevention API – Servis za automatizirano otkrivanje, klasificiranje, i raščlanjenje osjetljivih podataka  
Security Key Enforcement – Two-Step verification servis baziran na sigurnosnom ključu.

**IoT**Cloud IoT Core – Sigurna konekcija nad uređajem i upravljanje servisa za IoT  
Cloud IoT Edge – Dovodi AI (artifitial inteligence) u sloj za 'edge computing'.

* **XML DIGITAL SIGNATURE**

Definira sintaksu i pravila za kreiranje digitalnog potpis XML sadržaja.

XML (Extensible Markup Language) je vrlo jednostavan, fleksibilan tekstualni format razvijen iz SGML (Standard Generalized Markup Language) jezika.

SGML je ISO (International Organization for Standardization) standard za definiranje markup jezika za dokumente.

Digitalni potpis je elektronička zamjena za rukom pisani potpis, a služi istoj funkciji. Uz to pruža i potvrdu autentikacije, integriteta, te povjerljivosti izvora i podataka koji se prenose.

digitalni potpis nije kopija ručno pisanog potpisa.

U tehničkom smislu, digitalni potpis stvara i provjerava posebna aplikacija koja generira kriptografske poruke. Kako bi digitalni potpis funkcionirao, stvaraju se dva različita ključa. Prvi, zvan javni ključ, kreira digitalni potpis transformacijom podataka u nerazumljiv kod. Drugi, zvan privatni ključ, provjerava digitalni potpis te dešifrira transformiranu poruku u izvorni oblik. Ovaj sustav je siguran dok je privatni ključ zadržan tajnim.

XML digitalni potpis je u principu digitalni potpis dizajniran za uporabu u XML transakcijama, a može se koristiti za potpisivanje bilo kojeg tipa podataka.

Dobra strana XML digitalnih potpisa je bolja fleksibilnost od digitalnih potpisa kao što su PGP (Pretty Good Privacy) i CMS12 (Cryptographic Message Syntax), jer ne radi na binarnim podacima nego na XML informacijskom skupu.

XML digitalni potpie koristi koncept kanonizacije što omogućuje potpisivanje samo važnog dijela, te uklanjanje manje važnih podataka poput praznih razmaka i završetka retka.

Nepravilno rukovanje XML digitalnim potpisima može dovesti do pojave sigurnosnih ranjivosti. Jedno od važnih obilježja ovih potpisa je da se potpisani XML elementi, zajedno s potpisom, mogu kopirati iz jednog dokumenta u drugi uz zadržavanje mogućnosti za provjeru potpisa.

**Digitalni certifikati (CA-Certificate Authority)**

Digitalni certifikat je potvrda u elektroničkom obliku koja predstavlja elektronički identitet u elektroničkim transakcijama te omogućuje sigurnu i povjerljivu komunikaciju internetom. Digitalnim certifikatom dokazujete svojim poslovnim partnerima, suradnicima i prijateljima te elektroničkim servisima da je informacija koju su zaprimili od Vas autentična. Certifikat zapravo predstavlja elektroničku identifikacijsku iskaznicu koja sadrži ključ i informacije o imatelju, svom vijeku trajanja, izdavatelju, te ovjeru, odnosno potpis izdavatelja, a ujedno povezuje imatelja certifikata s njegovim javnim ključem.

**Certifikati prema namjeni** mogu biti:

**1.** **Kvalificirani certifikati za elektronički potpis**, koji se koriste za izradu elektroničkih potpisa. Na nedvojben su način povezani s potpisnikom te omogućavaju njegovu identifikaciju.

**2. Certifikati za autentikaciju**, koji se koristi za izradu elektroničkog potpisa, za jaku autentikaciju i enkripciju ključa

**3. Certifikat za elektronički pečat**, koji se koristi za povezivanje podataka za validaciju elektroničkog pečata s pravnom osobom i potvrđuje naziv te osobe, a osigurava cjelovitost dokumenta.

**4. Certifikat za aplikacije**, odnosno poslovni certifikati za IT opremu izdaju se za IT sustave, aplikacije ili servise  povezane s poslovnim subjektom. Koristi se za izradu e-potpisa, za jaku autentikaciju i enkripciju ključa u poslovne svrhe.  
  
 **5. Certifikat za autentikaciju mrežnih stranica (SSL certifikati)** upotrebljavaju se samo za autentikaciju mrežnih stranica, tj. za autentikaciju web poslužitelja kojima se pristupa putem TLS ili SSL protokola te povezuje web site s pravnom osobom kojoj je izdan.

**Certifikati prema subjektu certificiranja** mogu biti:

[1. CERTIFIKATI ZA POSLOVNE SUBJEKTE](https://www.fina.hr/lgs.axd?t=13&id=10752)- poslovni certifikati,

[2. CERTIFIKATI ZA FIZIČKE OSOBE/GRAĐANE](https://www.fina.hr/lgs.axd?t=13&id=10753)- osobni certifikati,

[3. CERTIFIKATI ZA TIJELA DRŽAVNE UPRAVE (TDU)](https://www.fina.hr/lgs.axd?t=13&id=10754)- certifikati za državne dužnosnike i zaposlenike u tijelima državne uprave.

**XSD**

XML Schema language se često zove I XML Schema Definition (XSD)

## XML sheme podržavaju tipove podataka

## XML sheme koriste XML sintaksu

## Ukratko, XML, samo što postoje tipovi podataka i onda definiramo u toj shemi što je koji tip podatka.. To se u zaglavlju određuje

## https://www.w3schools.com/xml/schema\_schema.asp

**Rest web service - REpresentational State Transfer**

REST je web-standard arhitektura I koristi HTTP Protocol. Svaka komoponenta je nekakav resurs I svakom resursu se pristupa preko njegovog sučelja koristeći standardne HTTP metode.

HTTP methods:

* GET − omogućava read-only određenog resursa
* POST – koristi se za kreiranje novog resursa
* DELETE – za brisanje resursa
* PUT – za kreiranje novog resursa ili update postojećeg

REST web servis koristi JSON iako može i XML-om dok SOAP koristi isklučivo XML.

https://en.wikipedia.org/wiki/Representational\_state\_transfer

**Google App Engine**

**Google App Engine** je web framework platforma za razvoj i pružanje web aplikacija u Google-upravljanim podatkovnim centrima. Aplikacije su prilagođene za rad preko mnoštvo servera.

App engine pruža automatsku skalabilnost podatkovnih resursa za aplikaciju. Što je potražnja za aplikacijom veća, to će se više resursa memorije pridodijeliti aplikaciji kako bi mogla brzo i neometano raditi na svakom klijentu bez kompromisa.

Google App Engine je besplatna platforma do određenih granica korištenja. Cijena za korištenje je diktirana potrebom za više memorije spremišta podataka, brzine konekcije, ili sati neometanog rada aplikacije.

Podržani pogramski jezici uključuju sve standardne razvojne programske jezike današnjeg svijeta. A to su uglavnom :

* Python
* Java
* JRuby
* Go
* PHP
* Node.js
* C#

Google App Engine sadrži mnoštvo Java i Python standarda i frameworkova,što uključuje  
Pyramid, Flask, web2py za Python i za Javine standarde je ključan servlet 2.5 tehnologija.

Preko integrirane baze podataka, Google Cloud Datastore, možda nepoznata mnoštvu programera, njoj se pristupa preko jednostavne Low-level API te ima podršku od JPA i JDO.

Spring platforma također može raditi preko Google App Engine.

**Pouzdanost i Podrška**App engine je dizajniran na način da može podnijeti više podatkovnih čvorova bez padova ili smetnja. Ova otpornost na gubljenje informacija je pokazana statistički da GAE ima 'down time' od 0%!  
Plaćena podrška je omogućena za motrenje aplikacija na dubljoj i sigurnijoj razini nego besplatna varijanta korištenja GAE.  
Besplatna podrška omogućuje sve standarne načine potražnje pomoći, Stack Overflow,GitHub, Server Fault itd.

* **XPATH**

Xpath je jezik za specifkaciju upita nad XML podacima (kao sql za upite nad relacijskim bazama).

Služi za lociranje dijela XML dokumenta, pronalaženje elemenata I atributa koji odgovaraju određenom kriteriju I omogučava traženje u bilo kojem smjeru (unaprijed, unatrag, u oba smjera).

Rezultat XPath izraza može bit skup čvorova ili atomarnih vrijednost (sadržaj), odnosno bilo koji slijed u podatkovnom modelu.

Zadnja verzija Xpatha je Xpath 3.1(W3C preporuka 21.03.2017) i u usporedbi s Xpathom 1.0(prvom verzijom, W3C preporuka 16.11.1999) podržava bogatiji skup podatkovnih tipova, mapa i nizova, iskorištava tip informacije kod validacije putem XML Scheme i uvodi podršku za JSON.

**SSL (https)**

Secure Sockets Layer (SSL) je standardna sigurnosna tehnologija za uspostavljanje šifrirane veze između poslužitelja i klijenta - obično web poslužitelja (web stranice) i preglednika ili poslužitelja e-pošte i klijenta e-pošte (npr. Outlook).

SSL omogućuje sigurno prenošenje osjetljivih informacija kao što su brojevi kreditnih kartica, brojevi socijalnog osiguranja i vjerodajnice za prijavu.

Točnije, SSL je sigurnosni protokol. Protokoli opisuju kako se algoritmi trebaju koristiti. U tom slučaju, SSL protokol određuje varijable šifriranja za vezu i podatke koji se prenose.

Svi su preglednici sposobni za interakciju s osiguranim web-poslužiteljima pomoću SSL protokola. Međutim, preglednik i poslužitelj trebaju ono što se naziva SSL certifikat kako bi se uspostavila sigurna veza.

SSL-sigurne web stranice također počinju s https, a ne http.

Kada preglednik pokušava pristupiti web stranici koja je osigurana SSL-om, preglednik i web-poslužitelj uspostavljaju SSL vezu pomoću postupka nazvanog "SSL Handshake".

U osnovi se koriste tri tipke za postavljanje SSL veze: javne, privatne i sesije. Sve šifrirane pomoću javnog ključa mogu se dešifrirati samo privatnim ključem i obrnuto.

Budući da šifriranje i dešifriranje s privatnim i javnim ključem ima puno snage obrade, upotrebljavaju se samo tijekom SSL Handshake za stvaranje simetričnog ključa sesije. Nakon uspostavljanja sigurne veze, ključ za sesije koristi se za šifriranje svih prenesenih podataka.

1. **Preglednik se** povezuje s web poslužiteljem (web stranicom) osiguranim SSL-om (https). Preglednik traži da se poslužitelj identificira.
2. **Poslužitelj** šalje kopiju SSL certifikata, uključujući javni ključ poslužitelja.
3. **Preglednik** provjerava root potvrde prema popisu pouzdanih CA i da je certifikat nestančan, neopozvan i da njegovo uobičajeno ime vrijedi za web stranicu na koju se povezuje. Ako preglednik vjeruje certifikatu, on stvara, šifrira i šalje simetrični ključ za sesije pomoću javnog ključa poslužitelja.
4. **Poslužitelj** dešifrira simetrični ključ sesije pomoću svog privatnog ključa i šalje dekodiranu šifru ključa sesije za pokretanje šifrirane sesije.
5. **Poslužitelj** i **preglednik** sada šifriraju sve prenesene podatke s ključem sesije

**JSON**

JSON: JavaScript Object Notation.

JSON je sintaksa za pohranu I izmjenu podataka.

JSON je tekst, pisan sa JavaScript objektnom notacijom.

JSON is text, and we can convert any JavaScript object into JSON, and send JSON to the server.

Budući je JSON text, možemo kovertati bilo koji JavaScript object u JSON I poslati ga na server.

JavaScript ima ugrađene funkcije za pretvorbu stringa iz JSON-a u JS objekt

JSON.parse()

JSON vrijednosti moraju biti neki od ovih tipova

* a string
* a number
* an object (JSON object)
* an array
* a boolean
* null

## JSON koristi JavaScript sintaksu

I JSON I XML se mogu koristit za primanje podataka sa web server.

**JSON i XML sličnosti**

* oboje su “self describing" (čitljivi ljudima)
* imaju istu hijerarhiju
* oboje mogu biti parsirani I korišteni od više programskih jezika
* oboje mogu biti dohvaćeni sa XMLHttpRequest

**JSON i XML razlike**

* JSON ne koristi završni tag
* JSON je kraći
* JSON je brži za čitanje I pisanje
* JSON can use arrays

Najveća razlika:

 XML mora biti parsiran sa XML parserom. JSON može biti parsran sa standardnom JS funkcijom

**Zašto je JSON bolji**

XML je teže parsirati nego JSON.  
JSON je parsiran u JavaScript objekt.

Using XML

* dohvati XML document
* koristi XML DOM za proći kroz dokument
* izvuci vrijednosti I spremi u varijable

Using JSON

* dohvari JSON string
* JSON.Parse se koristi za izvlačenj podataka

https://www.w3schools.com/js/js\_json\_intro.asp