Popis tehnologija

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.

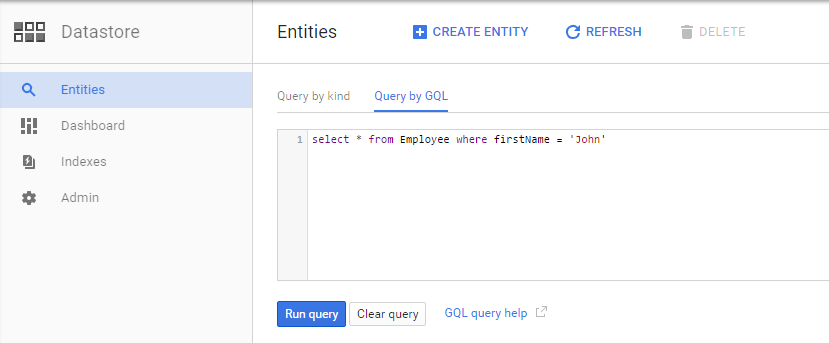
Cloud Datastore je u potpunosti vođen, što znači da Google automatski obrađuje replikaciju kako bi pružio vrlo dosljednu i dostupnu bazu podataka.

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) (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) 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) 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) ) ili računovodstveni sustav. Usmjeravanje i pravila moraju se uspostaviti u specifikaciji projekta. To obično uključuje članove platnih obveza, IT, a ponekad i nabavu.

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.

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.