Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Obrazovni materijali

Verzija 2.2

U Zagrebu, 2009.

Izradili:

Dr.sc. Zoran Bohaček
Mario Brčić, dipl.ing.
Prof. dr.sc. Krešimir Fertalj
Prof.dr.sc. Nikola Hadjina
Prof.dr.sc. Damir Kalpić
Prof.dr.sc. Mario Kovač
Dr.sc. Ivan Magdalenić
Tomislav Rajnović, dipl.ing.
Prof.dr.sc. Zoran Skočir
Ranko Smokvina, dipl.oec.
Nikša Stanović, dipl.ing.
Doc.dr.sc. Boris Vrdoljak

Voditelj Projekta:

Prof.dr.sc. Damir Kalpić

Odgovorna osoba:

Dekan Fakulteta elektrotehnike
i računarstva

Prof.dr.sc. Vedran Mornar

Dozvola uporabe:

creative commons

COMMONS DEED

Imenovanje-Nekomercijalno-Bez prerada 3.0 Hrvatska

Slobodno smijete:

- **dijeliti** (umnožavati, distribuirati i javnosti priopćavati 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).

Bez prerada (ne smijete mijenjati, preoblikovati ili prerađivati ovo djelo).

- U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela.
- 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.

Cjelovit tekst dozvole nalazi se na :

http://creativecommons.org/licenses/by-nc-nd/3.0/hr/legalcode

Sadržaj

0. Kratice

API	*Application Programming Interface*
BPEL4WS	*Business Process Execution Language for Web Services*
BPML	*Business Process Modelling Language*
ERP	*Enterprise Resource Planning*
HTML	*Hypertext Markup Language*
HTTP	*Hypertext Transfer Protocol*
MIME	*Multipurpose Internet Mail Extensions*
OASIS	*Organization for the Advancement of Structured Information Standards*
TCP/IP	*Transfer Control Protocol/Internet Protocol*
SAML	*Security Assertion Markup Language*
SMTP	*Simple Mail Transfer Protocol*
SOAP	*Simple Object Access Protocol*
UDDI	*Universal Description, Discovery and Integration*
URI	*Uniform Resource Identifier*
UUID	*Universally Unique Identifier*
W3C	*World Wide Web Consortium*
WS-I	*Web Service Interoperability*
WSDL	*Web Service Description Language / Web Service Definition Language*
X-KISS	*XML Key Information Service Specification*
X-KRSS	*XML Key Registration Service Specification*
XACML	*XML Access Control Markup Language*
XKMS	*XML Key Management Specification*
XML	*Extensible Markup Language*

1. Uvod

Čitatelja se prvo upoznaje s Web servisima kao čimbenikom e-Poslovanja. U najvećoj mjeri je korišten tekst iz [7]. Slijedi jedan prijedlog za potporu i uspješno širenje e-Poslovanja.

Priređene su prezentacije koje služe za informiranje gospodarstvenika o ulozi norma u elektroničkom poslovanju, dani su sažeti pregled svrhe i sadržaja norme, prikazani tipični slučajevi implementacije i primjeri najbolje prakse. Prezentacija norma se može koristiti na konferencijama i seminarima za diseminaciju znanja o normama, te za predstavljanje ovog projekta i njegovih rezultata putem Portala elektroničkog poslovanja.

Uz odobrenje autora preuzeti su edukativni materijali GS1 Croatia.

Uz odobrenje autora preuzeti su edukativni materijali

eBusiness Community Model-Vocational Education and Training, eBCM-VET, Leonardo da Vinci Project 2005 - 2007

2. Web servisi

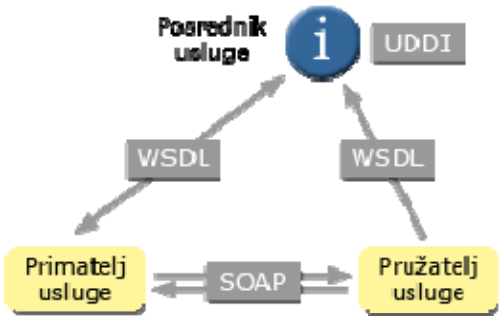
Tehnologija Web servisa se još uvijek razvija i u e-Poslovanju se počela primjenjivati pojavom prvih sigurnosnih protokola nad Web servisima. Velika prednost norma jest podrška od većine velikih proizvođača softvera i podrška za osnovne norme u različitim programskim jezicima.

Web servisi se smatraju obećavajućim i ključnim dijelom u realizaciji učinkovitih poslovnih rješenja. Koristeći standardne internetske protokole i norme, cilj im je pružiti aplikacije jednostavne za korištenje, koje omogućuju tvrtkama integraciju i automatizaciju poslovnih procesa unutar svojih tvrtki, a posebno sa svojim poslovnim partnerima. Web servisi su namijenjeni poboljšanju interoperabilnosti poslovnih procesa između različitih organizacijskih jedinica i osnovnih aplikacijskih sustava. Također se smatraju jednim od glavnih građevnih elemenata za pouzdani okvir elektroničkog poslovanja.

2.1. Opis tehnologije

2.1.1. WS-I *Basic Profile*

Specifikacija koja dolazi od organizacije WS-I (*Web Service Interoperability*) definira interoperabilnost osnovnih (*core*) specifikacija za Web servise kao što su SOAP, WSDL i UDDI.



Slika 1. Slika 1 - Arhitektura Web servisa

2.1.1.1. Universal Description, Discovery and Integration *(UDDI)*

Universal Description, Discovery and Integration je repozitorij usluga koji omogućava pronalazak informacija o specifičnim Web servisima. UDDI pruža mogućnost pretrage za Web servisima ovisno o zadanim kriterijima. UDDI je tehnološka specifikacija, ali i stvarna, postojeća usluga koja se nalazi na Internetu i pružaju je korporacije kao što je IBM ili Microsoft.

Način na koji UDDI radi, pomalo podsjeća na način rada Internet *Domain Name Service* (DNS). Pružatelji Web servisa (usluga na Webu) mogu registrirati svoje servise na nekom UDDI registru. Tada se važne informacije o specifičnom Web servisu sačuvaju u toj UDDI bazi podataka. Nije važno koji se UDDI registar odabere jer se oni redovito međusobno sinkroniziraju. UDDI također obuhvaća mehanizme koji bi trebali omogućiti sigurnost i kvalitetu podataka. Na primjer, organizacije koje žele objaviti informacije preko UDDI registra, prvo se moraju registrirati. Registracija se odvija putem kodirane veze (SSL). A kao rezultat registracije svaka novo registrirana organizacija dobije svoj jedinstveni broj (UUID). Takav broj dobije i svaki Web servis koji se objavi preko UDDI registra. Nakon što se podaci integriraju u bazu podataka postaju dostupni putem svakog UDDI registra. Također, UDDI registar ne mora biti samo na Internetu, već ga kompanije mogu posebno prilagoditi i koristiti unutar svoje mreže.

UDDI pruža tri kategorije informacija:

- *White pages* – sadrži osnovne informacije o pružatelju Web servisa kao što je ime kompanije, adresa, web stranica itd.
- *Yellow pages* – sadrži informacije o proizvodima i uslugama koje pruža ta kompanija, lokacijama itd. Koristi se klasifikacijski sistem.
- *Green pages* – pruža tehničke informacije o tipu i funkcionalnosti svakog Web servisa. Te se upravo te informacije proslijede primatelju usluge kad ih zatraži putem WSDL poruke.

UDDI može spremiti bilo kakve opise Web servisa, te se mogu koristiti različiti formati. WSDL nije obavezan.

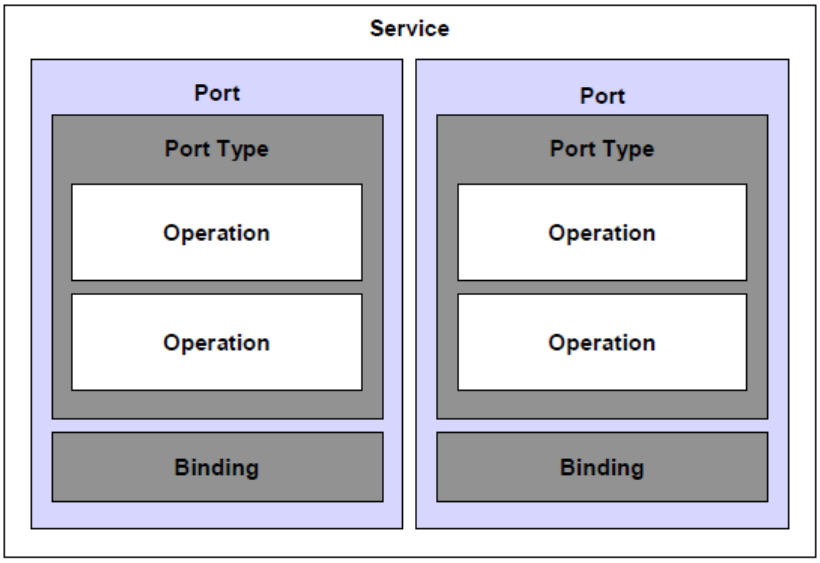
Za korištenje UDDI registra postoje tri aplikacijsko programska sučelja (API). "*Publisher* API" se koristi za objavljivanje informacija o Web servisima, "*Inquiry* API" služi za pretraživanje i dohvaćanje informacija o Web servisima, a "*Subscriber* API" se može koristiti za obavještavanje korisnika u slučaju promjene u registru.

UDDI pruža jednostavan, fleksibilan i moćan mehanizam za pohranu, lociranje i pozivanje informacija o Web servisima i njihovim pružateljima na normiziran način. Ali UDDI ne rješava sve probleme vezane za pretragu Web servisa. Nedostatak univerzalnog i jedinstvenog sistema za klasifikaciju organizacija, proizvoda i usluga, te probleme koji nastaju zbog te činjenice je nemoguće riješiti pomoću UDDI registra.

2.1.2. *Web Services Definition Language* (WSDL)

Na UDDI-u postoji usluga za pronalazak Web servisa, ali uspješan pronalazak nekog servisa ne znači da je taj Web servis spreman za korištenje. Sučelja, veze na protokole (*bindings*) i formati podataka korišteni za specifični Web servis su opisani pomoću WSDL-a (*Web Service Description Language*). Da bi se iskoristila funkcionalnost Web servisa, primatelj usluge mora samo imati pristup WSDL opisu traženog Web servisa, iz kojeg se mogu izvući sve relevantne informacije. Sam WSDL je neovisan o specifičnim formatima podataka i mrežnim protokolima, ali se uglavnom koristi sa SOAP, MIME i HTTP GET/POST.

WSDL definira servis kao set apstraktnih, krajnjih točaka mreže (*network end-points*), tj. portova. Poruke su apstraktni opisi podataka koji se izmjenjuju. Nadalje, WSDL uključuje operacije koje opisuju pod-akcije Web servisa. Apstraktna definicija portova, poruka i operacija je odvojena od konkretnog korištenja u instanci, što omogućuje ponovnu upotrebu tih definicija. Tek se u posljednjoj fazi procedure izvršavanja tim definicijama dodijele konkretne vrijednosti.



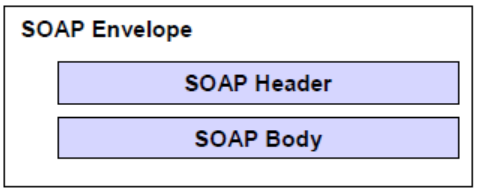
Slika 2. Slika 2 - Struktura WSDL-a

Može se reći da WSDL pruža razrađen mehanizam za definiranje Web servisa. Zbog njihove kompleksnosti, čovjeku je WSDL dokumente teško čitati i shvatiti. Ali to nije problem budući da se pri stvaranju WSDL dokumenata većinom koriste programski alati.

2.1.3. SOAP

SOAP je vjerojatno najvažniji dio Web servis tehnologije. SOAP predstavlja apstraktan sloj za prijenos stvarnih podataka. Točnije, specificira neutralnu reprezentaciju podataka koji se izmjenjuju sakrivajući komunikacijske protokole koji stoje iza, kao što je HTTP ili SMTP.

Kao i WSDL, SOAP je također temeljen na XML-u. SOAP poruke se sastoje od tri glavna elementa: omotnica (*envelope*), zaglavlje (*header*) i tijelo (*body*). Omotnica je korijenski element koji definira početak i kraj SOAP poruke. Zaglavlje nije obavezan element, a može sadržavati jedan ili više blokova metapodataka o samoj poruci. Tijelo sadrži stvarnu poruku.



Slika 3. Slika 3 - Struktura SOAP dokumenta

SOAP pruža tehnologiju za prijenos i razmjenu bilo kakve vrste podataka neovisno o komunikacijskom protokolu. Najvažnije prednosti SOAP-a su jednostavnost i proširljivost. Još jedna značajka SOAP-a je da se može koristiti sa sinkronim protokolima, kao što je HTTP, ali i sa asinkronim kao što je SMTP. Negativne strane su da SOAP ne podržava sigurnosne mehanizme kao što je kriptiranje, autentifikacija, ili digitalni potpis, što bi moglo biti od interesa u poslovnim aplikacijama, no takve specifikacije postoje na XML razini. Nadalje, ne pruža kontrolu procesa i transakcija, već se ta kontrola odvija na višim razinama.

2.2. Ostale važnije Web servis specifikacije

2.2.1. WS-*Addressing*

WS-*Addressing* je norma koja osigurava transportno neutralne mehanizme koji omogućavaju izmjenu informacija o adresama. WS-*Addressing* je standardiziran način koji u SOAP zaglavlja uključuje podatke o usmjeravanju poruke. Umjesto da odluke o usmjeravanju poruke donosi transportni sloj mreže, poruka koja koristi WS-*Addressing* u SOAP zaglavlju može sadržavati metapodatke o putu usmjeravanja.

2.2.2. WS-*Reliability*/WS-*ReliableMessaging*

WS-*Reliability* i WS-*ReliableMessaging* su norme namijenjene za ispunjavanje pouzdane dostave poruka. Omogućavaju da SOAP poruke budu pouzdano dostavljene između distribuiranih aplikacija u slučaju grešaka na softverskim komponentama, sustavu ili mreži.

2.2.3. WS-Coordination/WS-Atomic Transaction

WS-*Coordination* je norma koja opisuje programski okvir koji osigurava protokole namijenjene koordinaciji akcija distribuiranih aplikacija. Međutim, ta norma nije dovoljna da bi se koordinirale transakcije između Web servisa. WS-*Coordination* pruža potreban programski okvir, a druge norme poput WS-*Atomic Transaction* su potrebni za tu svrhu.

2.2.4. Poslovni procesi i Web servisi

Web servisi su primarno tehnologija za implementaciju komunikacije jedne aplikacije s drugom. Tj. jedna aplikacija može direktno koristiti funkcionalnosti i usluge druge aplikacije, uz pretpostavku da obje podržavaju Web servis tehnologiju. Web servisi dobiju još veću važnost kada se koriste na razini poslovnih procesa. Poslovni proces se sastoji od pod-procesa koji su međusobno povezani. Neki pod-procesi se mogu samo izvršavati sekvencijalno, a neki se mogu izvršavati i paralelno, što zahtijeva nekakav oblik sinkronizacije. Procesi povezuju Web servise jedne s drugim, pozivaju Web servise i vrše prijenos podataka.

2.3. *Business Process Modelling Language* (BPML)

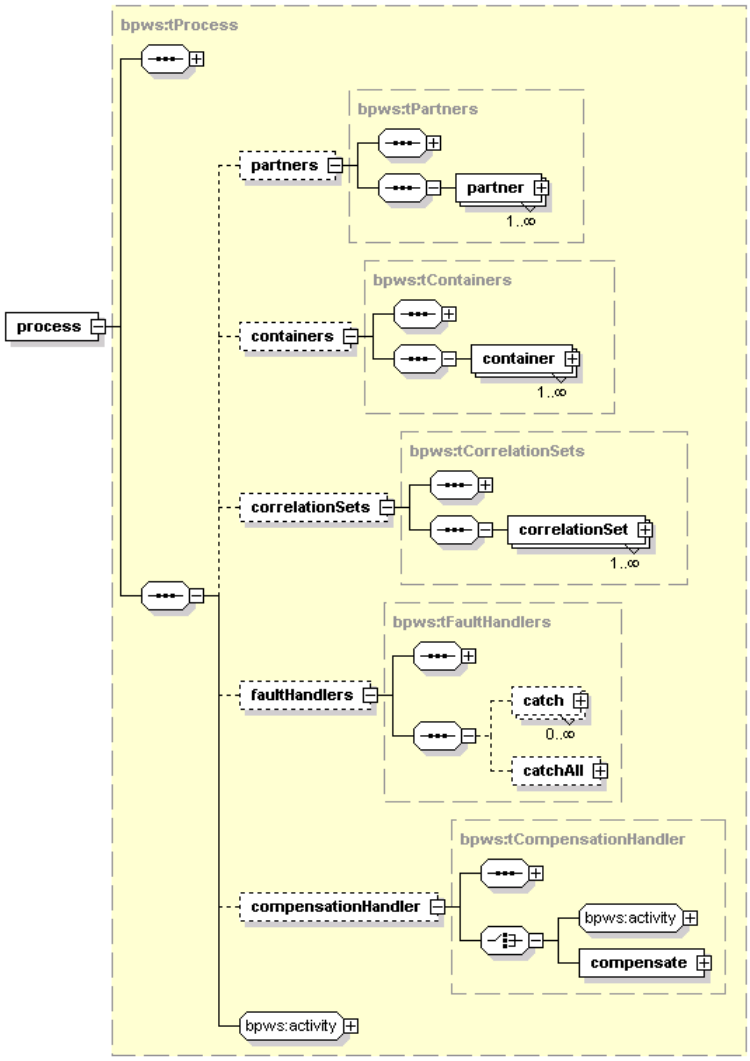
The Business Process Modelling Language (BPML) je metajezik za modeliranje poslovnih procesa, isto kao što je XML metajezik za modeliranje poslovnih podataka. BPML pruža apstraktnu provedbu modela za skupne i transakcijske poslovne procese temeljene na konceptima transakcijskog automata s konačnim brojem stanja. BPML pruža građevne elemente koji omogućavaju definiranje i manipulaciju toka podataka, ali i definiranje svakog koraka procesa posebno, te kontrolu toka tog koraka. S obzirom na kontrolu toka razlikuju se četiri tipa:

- *value based* – ovisnost nekog koraka procesa se određuje prema vrijednostima procesnih podataka tijekom izvođenja.
- *state based* – stanje procesa određuje ovisnosti.
- *time based* – kontrola toka je određene brojem izvođenja ili je podvrgnuta nekom vremenskom rasporedu
- *cycle based* – tok se kontrolira ponavljanjem jedne ili više aktivnosti.

BPML također omogućuje upotrebu ugnježđenih aktivnosti i definiranje da li će se grupa aktivnosti izvršavati sekvencijalno ili paralelno. Također ima podršku za transakcije, te građevne elemente i metode za upravljanje iznimkama.

2.4. *Business Process Execution Language* (BPEL)

BPEL je jezik baziran na XML jeziku, koji služi za opisivanje ponašanja poslovnih procesa temeljenih na Web servisima. BPEL omogućuje *top-down* realizaciju servisno orijentirane arhitekture kroz kompoziciju, orkestraciju i koordinaciju Web servisa. Pruža relativno jednostavan način za sastavljanje nekoliko Web servisa u kompozitne usluge nazvane poslovni procesi. BPEL se može koristiti za modeliranje ponašanja izvršnih, ali i apstraktnih procesa.



Slika 4. Slika 4 - XML shema BPEL procesa

Shema BPEL procesa je prikazana na slici 4. Najprije se definiraju različite uloge poslovnih partnera uključenih u proces. Zatim spremnici koji uključuju podatke koji se izmjenjuju između pojedinih koraka procesa. Definiraju se i elementi za upravljanje iznimkama tijekom procesa (*faultHandlers*, *compesationHandlers*). *correlationSets* element pruža mogućnost povezivanja i identificiranja prenesenih podataka. Nadalje se definiraju aktivnosti, koje mogu biti sljedeće:

- *Receive*
- *Reply*

- *Invoke*
- *Assign*
- *Throw*
- *Terminate*
- *Wait*
- *Empty*
- *Sequence*
- *Switch*
- *While*
- *Pick*
- *Flow*
- *Scope*
- *Compensate*

Značenje pojedinih aktivnosti se može zaključiti iz njihovog imena. *Scope* aktivnost omoguće korištenje svojih funkcija za upravljanje iznimkama. Unutar *Flow* aktivnosti procesi se mogu izvršavati paralelno, dok se unutar *Sequence* aktivnosti izvršavaju sekvencijalno.

2.5. Sigurnost Web servisa

2.5.1. Utjecaj

U radu s podacima pitanje sigurnosti uvijek mora biti razmotreno. Vezano uz e-poslovanje, ispunjavanje sigurnosnih zahtjeva uz privatnost, integritet i tajnost je ključna. Bez sigurnosti nema povjerenja, a bez povjerenja nema ni posla. Sa Web servisima je situacija ista. Ako tehnologija želi biti prihvatljiva za poslovne primjene, sigurnosni problemi moraju biti prepoznati kao i u bilo kojoj drugoj tehnologiji. Dok se Web servisi mogu razlikovati od alternativnih tehnologija, sigurnosni zahtjevi ne mogu.

Pojam IT sigurnosti se često poistovjećuje sa kontrolom pristupa (u obliku mehanizama dozvoljavanja pristupa informacijama ili sistemima samo autoriziranim korisnicima). U stvarnosti taj pojam obuhvaća puno više aspekata koje treba razmotriti. Npr. ostale dimenzije IT sigurnosti su tajnost, integritet, virusna zaštita, detekcija upada u sustav, zaštita intelektualnog vlasništva. Ove dimenzije nisu uvijek od jednake važnosti u svim aplikacijama IT-a. Identificiranjem važnih dimenzija sigurnosti za Web servise dobije se lista koja je u principu identična onoj koja vrijedi i u svijetu tradicionalnih klijent/server aplikacija.

2.5.2. Dimenzije sigurnosti

Vezano uz Web servise najvažnije dimenzije sigurnosti koje treba pokriti su obuhvaćene sljedećim poglavljima.

2.5.2.1. Autentikacija/Autorizacija

Kontrola pristupa dozvoljava pristup sustavu samo autoriziranim korisnicima. Autentikacija znači da sustav mora biti sposoban prepoznati korisnika. Uljezi ne bi trebali imati mogućnost maskirati se kao netko drugi. Autorizacija regulira što autenticirani korisnik u sustavu može (npr. pročitati neke specifične podatke).

Mehanizam kontrole pristupa mora se moći nositi sa eksternim ili internim tipovima napada na sustav. Eksterni napadi izvode se izvana od osoba koje uopće ne bi trebale imati pristup sustavu. Interne napade izvode osobe koje u principu imaju pristup sustavu, ali se namjeravaju predstaviti kao netko drugi.

Kontrola pristupa za Web servise može biti implementirana na različite načine koji su usporedivi sa mehanizmima koji se koriste na standardnim web stranicama. Najčešće se koristi antentikacija preko korisničkog imena i lozinke. Drugi način je ograničavanje pristupa svima osim autoriziranim sustavima koji se npr. mogu identificirati preko IP adrese. Ovaj pristup se najčešće koristi u privatnim mrežama.

2.5.2.2. Integritet podataka/poruka

Integritet podataka označava mogućnost verifikacije podataka (ili poruka). Sistem bi trebao uključivati mehanizme za prepoznavanje i falsificiranih ili neispravno prenesenih podataka. Jedna moguća implementacija koja bi osigurala integritet podataka uključivala bi korištenje digitalnog potpisa.

2.5.2.3. Tajnost

Tajnost je zahtjev da podatke mogu vidjeti samo legitimni korisnici, čak i ako su mehanizmi kontrole pristupa zaobiđeni. Tajnost prije svega znači osigurati podatke od prisluškivanja. Za napadača bi trebalo biti nemoguće presresti i pročitati podatke tijekom prijenosa. Ovo je posebno važno za servise koji prenose povjerljive podatke preko nesigurne mreže (npr. Interneta). U elektroničkom poslovanju obično je potreban prijenos osjetljivih podataka pa je tajnost najčešće implementirana upotrebom kriptografskih algoritama kao što je npr. AES. Međutim, postoje i druge opcije osiguranja podataka od prisluškivanja. Tako je moguće kriptirati cijelu sesiju (SSL npr.) ili samo sadržaj (u slučajevima kada je dodatak zbog SSL nepoželjan).

2.5.2.4. Integritet transakcija

Ovaj zahtjev svoje korijene vuče iz svijeta sustava za upravljanje bazama podataka. Mora biti osigurano da su podaci mijenjani dosljedno, npr. da dva korisnika ne mijenjaju podatke istovremeno ili da jedan čita dok drugi mijenja. Ako integritet transakcija ne može biti osiguran kroz odgovarajuće mehanizme, pojavit će se greške u podacima. Za Web servise to znači da pozivi funkcija koji ne mogu biti ispravno izvršeni unutar pripadajuće transakcije, na neki način moraju biti obrađeni (npr. poruka korisniku, ili kroz mehanizam obrade pogrešaka). Poželjno je uključiti ove značajke u sam protokol. Integritet transakcija se obično osigurava unutar *workflow* protokola.

2.5.2.5. Privatnost

Privatnost je ljudsko pravo. Opisuje pravo osobe na limitiranje pristupa i upotrebe osobnih informacija. Osobne informacije su najčešće potrebne pojedincima ili kompanijama za pružanje usluga (npr. liječnik treba medicinske informacije o svojim pacijentima). Privatnost regulira što se može s tim informacijama, posebno kada su ti podaci redistribuirani trećim stranama bez znanja osobe na koju se odnose. Privatnost može biti osigurana kombinacijom tehničkih i zakonskih sredstava. Tehnologija može zaštititi privatnost, ali ne može spriječiti širenje informacija.

2.5.3. Sigurnosni rizici

Smisao Web servisa je omogućiti komunikaciju između sustava koja se jednostavno implementira i koristi široko rasprostranjene protokole. Međutim, s tim mogućnostima dolazi cijeli set sigurnosnih rizika koji moraju biti razmotreni. Tehnologija Web servisa koristi se u visoko decentraliziranom okruženju kako arhitekturno tako i administrativno. Također to je i izrazito heterogena okolina u smislu primijenjenih tehnologija. Naposljetku, okruženje Web servisa je takvo da su usluge obično otvorene na javno dostupnom Internetu. Provođenje sigurnosne politike preko visoko decentralizirane i heterogene okoline može biti vrlo složeno.

Nekoliko glavnih sigurnosnih rizika koji se tiču Web servisa je opisano u sljedećim poglavljima.

2.5.3.1. DoS napadi

DoS (*Denial of Service*) napadi pokušavaju onemogućiti sustav velikom navalom zahtjeva, više nego ih sustav može obraditi. Kod običnih web stranica, DoS napade je relativno lako detektirati. Međutim, kod Web servisa detekcija takvih napada može biti teža. Posebno kada Web servis zahtijeva relativno puno vremena za obradu. Tada čak i mali broj zahtjeva može onemogućiti sustav u daljnjem radu, a da pri tome automatizirani sustav detekcije upada ni ne detektira napad.

2.5.3.2. Zlonamjerni napadi

Tehnologija Web servisa se u grubo odnosi na pozivanje funkcija na udaljenim sustavima. To je omogućeno slanjem SOAP zahtjeva preko standardnog HTTP protokola (ili nekog drugog Internet protokola). Standardni HTTP port je otvoren na većini vatrozida, što znači da SOAP promet može nesmetano proći do interne mreže (ili najmanje do demilitarizirane zone). Jasno je da mogućnost izvršavanja funkcija na udaljenom sustavu otvara taj sustav hakerskim napadima koji bi mogli iskoristiti sučelje Web servisa za dobivanje ulazne točke u sustav. Vrlo je bitno pažljivo dizajnirati Web servis s obzirom da bi hakeri mogli iskoristit slabosti i kompromitirati cijeli sustav. Također, svi SOAP zahtjevi bi trebali biti parsirani i evaluirani prije prosljeđivanja.

2.5.3.3. Napadi reprodukcijom

Napadi reprodukcijom odnose se na napade u kojoj napadač kopira ispravan zahtjev i naknadno ga više puta šalje u sustav. Primjer takvog napada bi mogao biti višestruko slanje kopije zahtjeva za prijenos novca u banci što bi rezultiralo višestrukom sumom novca na računu napadača. Napadi reprodukcijom većinom mogu biti spriječeni uključivanjem vremenske oznake i digitalnim potpisivanjem zahtjeva.

2.5.3.4. Man-in-the-Middle *napad*

Odnose se na napade kada je zlonamjerni napadač presreo komunikaciju prometa (kao što su SOAP poruke) između dvije strane i pri tome mijenja, briše ili u potpunosti zamjenjuje poruke. Radeći to, napadač krivotvori poruke čime strane A i B u komunikaciji misle da komuniciraju jedna sa drugom. Infrastruktura javnog ključa sa centrom za pouzdanu raspodjelu ključeva može pomoći u obrani od ovakvih napada.

2.5.3.5. Buffer Overflow *napadi*

Buffer overflow napadi pokušavaju promijeniti stog funkcije prilikom izvršavanja funkcije što može rezultirati rušenjem sustava ili izvršavanjem određenog koda. To se može učiniti prosljeđivanjem dužih vrijednosti parametara od onih koje funkcija može obraditi (npr. lozinka od 200000 znakova). Ponekad je moguće da napadač uključi vlastiti kod koji će se izvršiti upotrebom *buffer overflow* napada.

2.5.3.6. Napadi lozinkama

Kao i drugim sustavima, Web servisi mogu biti ranjivi na tip napada u kojem napadač pokušava upasti zaštićenim servisima pogađanjem ispravnog korisničkog imena i pripadajuće lozinke. Ovaj tip napada se može izvršavati čistom silom ili uz upotrebu rječnika koji sadrži listu popularnih lozinki.

2.5.4. XML sigurnost

Web servis je tehnologija temeljena na XML-u, i na nju se kao takvu, odnose pravila XML sigurnosti. Nadalje, neke opće norme XML sigurnosti su ukomponirane u specifične sigurnosne norme Web servisa.

Jezici koji su temeljeni na XML-u, kao SOAP, su također bazirani na tekstu i proširljivi. Dakle, moguće je dodati mjere sigurnosti kao što je tajnost, integritet i kontrola pristupa na cijeli XML dokument ili na dijelove tog dokumenta bez da se prekrše pravila XML dokumenta. Kao rezultat toga, razvijena je specifična arhitektura za XML dokumente. Osnovne norme XML sigurnosti su:

- XML *Encryption* (XML-Enc)
- XML *Digital Signature* (XML-DSig)
- XML *Access Control Markup Language* (XACML)
- *Security Assertion Markup Language* (SAML)
- XML *Key Management* (XKMS)

2.5.4.1. XML Encryption *(XML-Enc)*

Kriptiranjem XML dokumenata se postiže tajnost podataka. XML dokument se prilikom prijenosa može zaštititi i sigurnom vezom (SSL), ali ne i kad se pohrani. Kriptiranjem se osigurava tajnost podataka i prilikom prijenosa i kad se dokument pohrani na server. Kriptirati se može i samo dio XML dokumenta, ako se želi da različiti ljudi vide različite dijelove.

XML dokument se može kriptirati i sa standardnim kriptografskim alatima, ali onda će se dokument pretvoriti u binarni oblik i neće ga biti moguće otvoriti sa XML preglednicima i drugim alatima. XML-Enc prepoznaje i eliminira taj problem.

XML-Enc kao i ostali kriptografski alati koristi kriptografske algoritme koji pretvaraju podatke iz nekriptiranog u kriptirani oblik i obratno koristeći ključ. Općenito gledajući, kriptirati se može na dva različita načina:

- simetrično kriptiranje (koristi jedan ključ)
- asimetrično kriptiranje (koristi dva ključa: javni i tajni)

XML-Enc podržava obje tehnologije. Također je moguće kriptirati dio dokumenta ili čak samo jedan jedini element. Nakon upotrebe XML-Enc-a na XML dokumentu, rezultat je također XML dokument koji se i dalje može procesirati sa standardnim XML alatima.

2.5.5. XML *Digital Signature* (XML-DSig)

XML potpis je u stvari digitalni potpis, ali prilagođen upotrebi u XML dokumentima. Digitalni potpis funkcionira na principu asimetrične kriptografije i koristi dva algoritma. Jedan za potpisivanje, koji koristi korisnikov tajni ili privatni ključ (*Private key*), a drugi za provjeravanje potpisa, koji koristi javni ključ (*Public key*).

XML potpis u XML dokumentu je realiziran preko elementa signature koji ima sljedeću strukturu ("?" predstavlja nula ili jedno pojavljivanje, "+" jedno ili više, a "*" nula ili više pojavljivanja) :

```
<Signature ID?>
    <SignedInfo>
     <CanonicalizationMethod/>
     <SignatureMethod/>
     (<Reference URI?>
       (<Transforms>)?
       <DigestMethod>
       <DigestValue>
     </Reference>)+
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
</Signature>
```

SignedInfo element je informacija koja je zapravo potpisana. Te informacije sekvencijalno prolaze kroz nekoliko koraka na putu da budu potpisane.

Slika 5. Slika 5 - Koraci u stvaranju XML potpisa

CanonicalizationMethod element sadrži algoritam s kojim se kanoniziraju podaci ili strukturiraju podaci na način koji je prihvatljiv uglavnom svima. Reference element identificira resurse koji će biti potpisani i sve algoritme koji će se koristiti za pretprocesiranje podataka. Ti algoritmi su ispisani u *Transforms* elementu i uključuju operacije kao što su kanonizacija, kodiranje/dekodiranje, kompresija/inflacija ili XPath transformacija. *SignatureMethod* element sadrži algoritam koji se koristi za konvertiranje kanoniziranog elementa *SignedInfo* u *SignatureValue*. Svaki Reference element uključuje *DigestMethod* i rezultirajući *DigestValue* koji je izračunat nad identificiranim podacima. Reference element može sadržavati više *Transforms* elemenata. Reference element ima URI atribut koji je opcionalan, ali ako potpis sadrži više Reference elemenata onda je URI opcionalan samo za jedan element, a ostali ga moraju imati. *KeyInfo* element definira koji se ključ koristi pri ovjeravanju potpisa. *Object* je opcionalni element koji služi za uključivanje podatkovnih objekata unutar potpisa.

XML potpis može se pojaviti u tri različita oblika:

- Omotani potpis (*Enveloped*) – potpis se nalazi unutar dokumenta.
- Omotavajući potpis (*Enveloping*) – potpis omeđuje dokument koji potpisuje.
- Odvojeni potpis (*Detached*) – potpis se nalazi zasebnom dokumentu, a URI (*Universal Resource Identifier*) određuje koji dokument potpisuje.

No to su samo nominalni slučajevi XML potpisa. XML potpis je jako fleksibilan i moguće je kombinacijama ta tri oblika dobiti nove. Primjera radi, jedna od mogućih kombinacija bi bila: Omotavajući potpis umetnuti u dokument tako da on potpisuje neke točno određene podatke. Što znači da je moguće potpisivati samo dio podataka. XML potpis omogućuje čak i potpisivanje više dokumenata jednim potpisom itd.

2.5.6. XML *Access Control Markup Language* (XACML)

XACML je jezik koji se može koristiti za kontrolu pristupa XML dokumentu. Obično, modeli kontrole pristupa uključuju to, da korisnik zatraži pristup XML dokumentu, a sustav mu to dozvoli ili odbije. Moguće je kontrolirati pristup cijelom XML dokumentu ili samo dijelovima, sve do pojedinačnog elementa.Također se mogu definirati akcije koje su dozvoljene i one koje nisu.

Kad se XACML primjeni na neki dokument, onda se svaki zahtjev korisnika procesira i ocjenjuje, te se donosi odluka o pristupu temeljena na pravilima zapisanim u XACML-u.

2.5.6.1. Security Assertion Markup Language *(SAML)*

Općeniti zahtjev distribuiranog računarstva danas je "*single sign-on*" autentifikacija. Što znači da se korisnik mora prijaviti samo jedanput, a onda se ta informacija proširi po cijelom sustavu da bi se izbjegla ponovna autentifikacija.

SAML omogućuje "*single sign-on*" autentifikaciju, proširujući XML na način da se mogu dijeliti sigurnosna pravila. SAML također uključuje zahtjev/odgovor (*request/response*) protokol i vezu na SOAP protokol. SAML ne određuje neki posebni mehanizam autentifikacije, već se mogu koristiti razni mehanizmi. Od jednostavnih kao što je lozinka, pa do složenih biometrijskih mehanizama autentifikacije.

2.5.7. XML *Key Management* (XKMS)

XKMS pruža protokole za upravljanje javnim ključevima. Javni ključevi su kritičan dio digitalnog potpisa i igraju važnu ulogu kod pružanja tajnosti u distribuiranim sustavima.

Važni koraci u korištenju kriptografije s javnim ključem uključuju stvaranje para javni/privatni ključ i povezivanju javnog ključa s informacijama o identitetu vlasnika. U slučaju da se ugrozi tajnost privatnog ključa, onda je potreban mehanizam za povlačenje i javnog ključa.

XKMS definira XML poruke za zahtjev, odgovor, registraciju ključa, povlačenje ključa i promjene ključa. Primarni cilj je omogućiti korisniku aplikacije s javnim ključem jednostavno lociranje potrebnih ključeva i informacije o tim ključevima. XKMS se sastoji od dva dijela, XML Key Information Service Specification (X-KISS) i XML Key Registration Service Specification (X-KRSS). X-KISS definira protokole za procesiranje informacija o ključu, kao što je lokacija ključa ili podaci o vlasniku ključa. X-KRSS pruža potporu za servise zadužene za registraciju ključa. Registracijski proces se uglavnom sastoji od slanja javnog ključa i informacija o vlasniku ključa na pouzdani registracijski server. Nakon registracije, informacije o ključu se mogu dohvatiti sa servera slanjem zahtjeva na server koristeći X-KISS poruke.

2.5.8. WS-*Security*

SOAP, jezgra specifikacije Web servisa, ne sadrži sigurnosne mehanizme. Međutim, XML sigurnosni mehanizmi mogu biti korišteni nad SOAP-om. Osim XML sigurnosnih mehanizama, postoji set SOAP ekstenzija koje olakšavaju implementaciju tajnosti i autentičnost poruka za SOAP dokumente. Te ekstenzije sadržane su pod imenom "WS-*Security*“ i prvotno su razvijene od kompanija IBM, *Microsoft* i *VeriSgin*, ali je daljnji razvoj prepušten *Oasis-Open* organizaciji (*Organization for the Advancement of Structured Information Standards).*

WS-*Security* baziran je na ranije postojećim tehnologijama (npr. XML-Enc, XML-DSig) čime je izbjegnut razvoj rješenja za probleme za koje IT industrija od ranije ima dobra rješenja. Primjerice *Kerberos* i X.509 rješavaju problem autentikacije.

X.509 također koristi postojeću PKI za manipuliranje ključevima. XML-Enc i XML-DSig opisuju načine kriptiranja i potpisivanja sadržaja XML poruka. XML *Canonicalization* opisuje načine pripremanja XML sadržaja za digitalno potpisivanje i enkripciju. Ono što WS-*Security* dodaje postojećim specifikacijama je okosnicu za ugradnju tih mehanizama u SOAP poruke. To je načinjeno na način neovisan o transportnom sloju.

WS-*Security* definira element SOAP zaglavlja koji nosi podatke vezane uz sigurnost. Ako je npr. XML-Sig korišten, zaglavlje može sadržavati informacije definirane XML-Sig-om koje opisuju kako je poruka potpisana, ključ koji je korišten i rezultat potpisa. Slična situacija je i kod kriptiranja elemenata unutar poruke. Tada WS-*Security* zaglavlje sadrži informacije o enkripciji. WS-*Security* ne definira format potpisa ili enkripcije. Umjesto toga, specificira način kako bi se format, definiran drugom specifikacijom, ugradio u SOAP poruku.

Prva verzija WS-*Security* protokola izdana je 2004 pod nazivom oznakom 1.0. Protokol je nadopunjen 2006. i izdan pod oznakom 1.1. Međutim, razvijatelji nastavljaju sa razvojem i rade na upotpunjavanju sigurnosne arhitekture pa je nad WS-*Security* protokolom razvijeno ili se još razvijaju sljedeći protokoli:

2.5.8.1. *WS*-Policy

Definira okosnicu koji omogućava opis zahtjeva i ograničenja Web servisa koji se odnose na posrednike i krajnje točke (npr. zahtijeva se korištenje sigurnosnih znački, pravila vezana uz privatnost, korišteni enkripcijski algoritmi).

2.5.9. WS-*Trust*

Definira okosnicu za trust modele koji omogućavaju Web servisima sigurnu interoperabilnost. Trenutno je aktualna verzija 1.3 iz 2007. godine.

2.5.9.1. WS-Privacy

Opisuje model kako organizacije mogu uskladiti svoje politike privatnosti i provjeriti da li korisnici ispunjavaju te zahtjeve politike. WS-*Privacy* radi u spoju sa WS-*Policy* i WS-*Trust*.

2.5.9.2. *WS*-SecureConversation

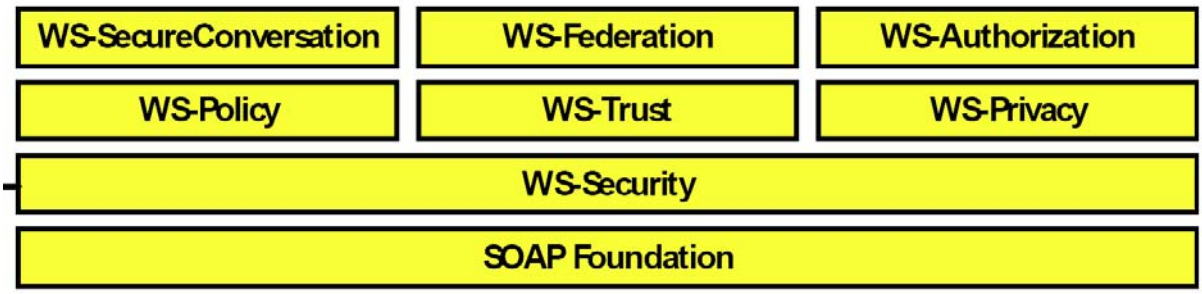
Opisuje standardne mehanizme za izmjenu sigurnosnih informacija između Web servisa. Pruža formalne definicije za kreiranje i razmjenu sigurnosnog konteksta i pripadajućih sesijskih ključeva.

2.5.9.3. WS-Federation

Pruža seriju norma i sigurnosnih modela za uspostavu federacije, tj. okoline gdje je dostignuta željena razina povjerenja između različitih trust domena.

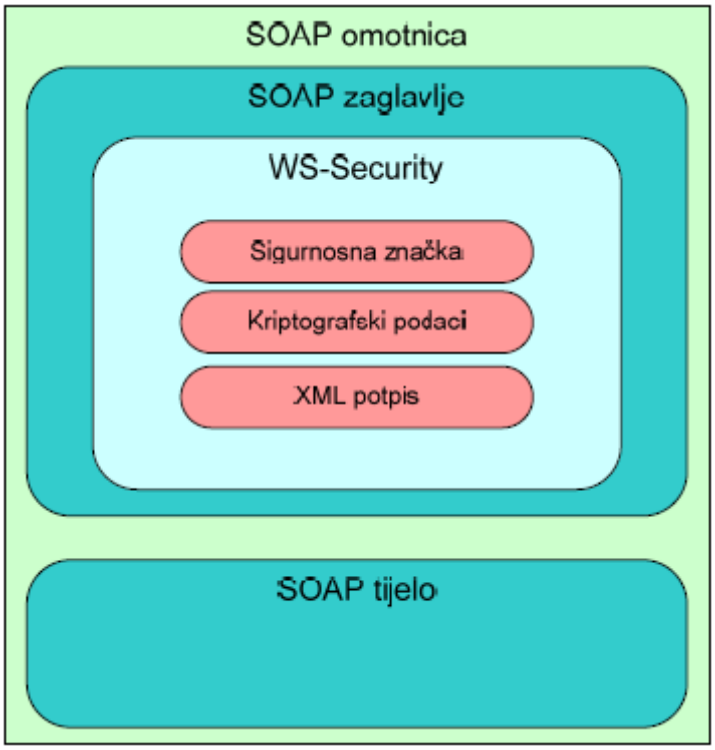
2.5.9.4. WS-Authorization

Opisuje normu za upravljanje informacijama koje se koriste za autorizaciju i kontrolu pristupa. Kao dio norme sadržan je i način na koji se zahtjevi prezentiraju unutar sigurnosnih znački.



Slika 6. Slika 6 - WS-*Security* i nadogradnje

Shematski bi se struktura sigurnosnih informacija u SOAP poruci prema WS-*Security* protokolu mogla prikazati na sljedeći način:



Slika 7. Struktura sigurnosnih informacija u SOAP poruci prema WS-*Security* protokolu

```
<SOAP:Envelope xmlns:SOAP="...">
  <SOAP:Header>
    <wsse:Security SOAP:role="..." SOAP:mustUnderstand="...">
      <wsse:UsernameToken>
        ..
      </wsse:UsernameToken>
      ...
    </wsse:Security>
  </SOAP:Header>
  <SOAP:Body Id="MsgBody">
  <!-- SOAP Body data -->
  </SOAP:Body>
</SOAP:Envelope>
```

Slika 8. Primjer WS-*Security* zaglavlja:

2.6. Primjer scenarija upotrebe WS

Sljedeći primjer ilustrira scenarij kompleksne *online* narudžbe sa provjerom kreditne sposobnosti i PKI infrastrukturom. Takav scenarij upotrebe Web servisa prikazuje značajne sigurnosne mehanizme. Bit će opisano kako različite specifikacije mogu biti implementirane po pojedinim pitanjima sigurnosti.

'*Smith Company*' planira kupiti nekoliko novih strojeva od '*Machine Company*', prodavača opreme koji prodaje skupe strojeve preko Interneta. Stoga, '*Machine Company*' zahtjeva provjeru kreditne sposobnosti prije nego transakcija može biti izvršena. Naravno, kreditni podaci kompanije '*Smith Company*' su osjetljivi pa provjera mora biti obavljena tajno. '*Smith Company*' ima otvoren bankovni račun u banci '*The Bank*'. Četvrti igrač u scenariju je '*Trust Company*' koja osigurava PKI infrastrukturu. Osim toga, 'Trust kompanija' upravlja i XKMS serverom za registraciju ključeva.

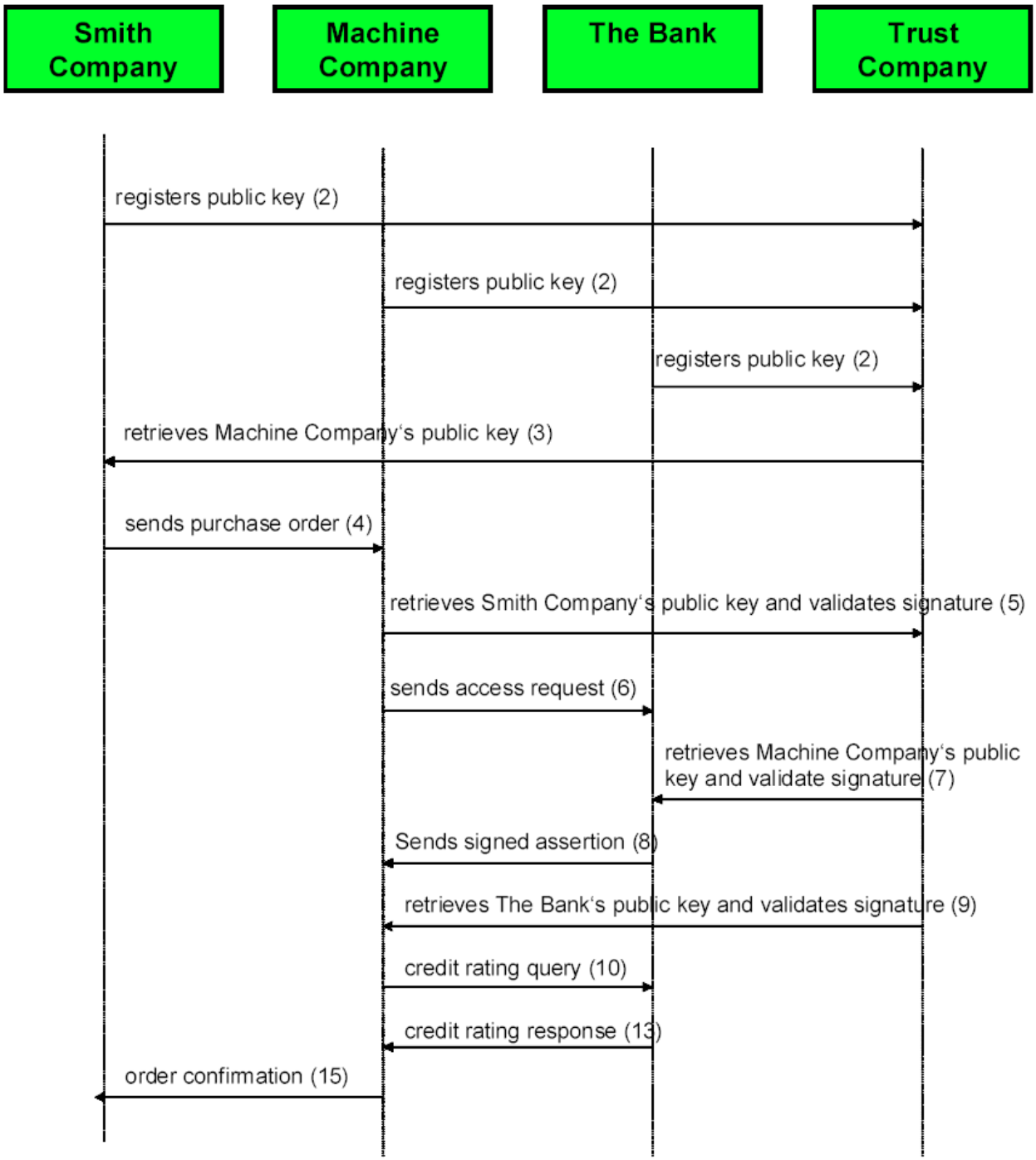
Način na koji opisani scenarij može biti implementiran:

- IT odjeli u '*Machine Company*', '*Smith Company*' i '*The Bank*' svaki za sebe kreiraju svoj par privatnih i javnih ključeva koji mogu biti korišteni za digitalno potpisivanje ili kriptografiju.
- Sva tri odjela registriraju svoje javne ključeve u XKMS serveru tvrtke '*Trust Company*' putem X-KISS protokola.
- '*Smith Company*' kreira SOAP dokument koji sadrži detalje narudžbe i digitalno ga potpisuje sa javnim ključem tvrtke '*Machine Company*'. Informacija o potpisu se uključuje o SOAP zaglavlje prema WS-*Security*/XML-DSig specifikacijama. Nakon toga, narudžba se šalje u '*Machine Company*'.
- U '*Machine Company*', sustav za procesiranje narudžbi zaprima javni ključ tvrtke 'Smith Company' od '*Trust Company*' putem X-KISS i validira digitalni potpis *narudžbe da se uvjeri u autentičnost.*
- Sustav za procesiranje narudžbi u '*Machine Company*' šalje digitalno potpisani zahtjev za pristup kreditnim podacima u 'The Bank' banku.
- Kreditni sustav banke '*The Bank*' zaprima od '*Trust Company*' javni ključ tvrtke '*Machine Company*' putem X-KISS i verificira digitalni potpis na zahtjevu za pristup da utvrdi autentičnost.
- Banka '*The Bank*' naplaćuje tvrtki '*Machine Company*' pristup bazi s kreditnim podacima i šalje SOAP dokument koji sadrži SAML potvrdu nazad u tvrtku *'Machine Company*'.
- *'Machine Company*' zaprima javni ključ banke od '*Trust Company*' putem X-KISS.
- Sustav za procesiranje narudžbi u '*Machine Company*' kreira SOAP zahtjev prema banci, kriptira sadržaj koji sadrži podatke tvrtke '*Smith Company*' korištenjem WS-*Security*/XML-Enc i javnim ključem banke. Nakon toga se dodaje SAML potvrda u SOAP zaglavlje i digitalno se potpisuje digitalnim potpisom tvrtke '*Machine Company*'.
- Kreditni sustav banke verificira digitalni potpis tvrtke '*Machine Company*' i SAML sigurnosnu potvrdu.
- Kreditni sustav banke dekriptira SOAP sadržaj koristeći svoj vlastiti privatni ključ.
- Kreditni sustav banke, zadovoljan potpisom i SAML potvrdom, kreira SOAP dokument koji sadrži kreditne podatke tvrtke *'Smith Company*'. Naravno,

dokument se kriptira korištenjem WS-*Security*/XML-Enc i javnog ključa tvrtke '*Machine Company*' te digitalno potpisuje i takav šalje u '*Machine Company*'

- Sustav za procesiranje narudžbi u '*Machine Company*' verificira digitalni potpis i dekriptira SOAP sadržaj koji sadrži zahtijevane informacije.
- Zadovoljan kreditnim rejtingom tvrtke '*Smith Company*', sustav za procesiranje u 'MC' šalje SOAP dokument koji sadrži digitalno potpisanu potvrdu narudžbe u sustav 'SC'.

Slikovni prikaz opisanog procesa:



Slika 9. Primjer scenarija upotrebe WS

2.7. Zaključak

Web servisi su tehnologija koja omogućava jednostavnu razmjenu podataka i inetroperabilnost između poslovnih subjekata. Kao takva vrlo je zanimljiva za primjenu u elektroničkom poslovanju. Međutim, prve implementacije nisu se pojavile odmah nakon nastanka tehnologije već se čekalo da se riješi problem sigurnosti.

Sigurnost nije karakteristika kvalitete koja se može optimirati i unaprijediti tijekom vremena. Sigurnost je čvrsti zahtjev koji tehnologija Web servisa mora implementirati u poslovnoj okolini. Činjenica da svi poslovni scenariji ne zahtijevaju jednako snažne sigurnosne mehanizme ne mijenja činjenicu da svaki sigurnosni zahtjev scenarija mora biti pokriven, ili Web servisi kao tehnologija uopće neće moći biti primijenjeni za scenarij. Ne postoji sigurnost koju bi mogli ocijeniti kao polu dobru. Ili je aplikacija dovoljno sigurna ili nije. Između ne postoji.

Sigurnosne potrebe za Web servise su adresirane velikim brojem XML i WS-*Security* specifikacija.

SAML i XACML rješavaju problem autentikacije i autorizacije. Ove dvije specifikacije su u potpunosti kompatibilne i vjerojatno mogu riješiti svaki slučaj u praksi.

XML-DSig i XKMS preko mehanizama digitalnih potpisa i upravljanja javnih ključevima rješavaju pitanje integritet podataka.

Tajnost je pokrivena preko XM-Enc koji omogućuje korištenje dokazanih kriptografskih aplikacija u Web servisima.

3. Smjernice za efikasno uvođenje elektroničkog poslovanja u Republici Hrvatskoj

3.1. Polazne pretpostavke

Elektroničko poslovanje se koristi u Republici Hrvatskoj na jedan nesustavan način u kojem su pojedine tvrtke primorane na korištenje elektroničkog poslovanja ako žele poslovati s određenim tvrtkama, često iz inozemstva. Naravno, u tehničkoj izvedbi to zahtijeva dosta financijskih sredstava. Uočava se potreba da se na razini Republike Hrvatske dogovore postupci koji će omogućiti efikasan i nadasve financijski prihvatljiv način uvođenja elektroničkog poslovanja.

Pri tome potrebno je uvažavati sljedeće činjenice:

- Zahvaljujući razvoju Interneta, širokopojasnih mreža i usluga, inovacijom u nova tehnološka rješenja moguće je sustavnim uvođenjem elektroničkog poslovanja

značajno povećati konkurentnost domaćih tvrtki na sve zahtjevnijem tržištu roba, usluga i informacija.

- Odabir norma i odgovarajućih aplikacija je vrlo ozbiljan zadatak.

- Republika Hrvatska je premala zemlja da bi podržavala sve postojeće norme jer to zahtijeva veliki broj eksperata za njihovu implementaciju i ne mala financijska sredstva.

- Potrebno je predložiti skup norma primjerenih za korištenje u Republici Hrvatskoj i oko njih graditi globalnu arhitekturu sustava elektroničkog poslovanja i razviti (primijeniti) odgovarajuće aplikacije, gdje bi većina malih, srednjih i velikih tvrtki pronašla rješenje za svoje potrebe.

- Potrebno je analizirati potrebu implementacije referentnih instalacija i razvoja pilotskih aplikacija.

- Kod implementacije sustava elektroničkog poslovanja za male i srednje tvrtke odabir norma nije jedini problem – potrebno je motivirati tvrtke za uključenje u sustav konkretnim rješenjima.

- Tvrtke moraju odmah uvidjeti korist implementiranih rješenja, a same aplikacije moraju istovremeno predstavljati i izgradbene blokove većeg sustava elektroničkog poslovanja.

- Uvođenje sustava elektroničkog poslovanja za male i srednje tvrtke zahtijeva značajna financijska sredstva.

- Velike tvrtke bi trebale omogućiti malim i srednjim tvrtkama kao poslovnim partnerima da na jednostavan način ponude proizvode i usluge kroz široko poznate tehnologije (elektronička pošta, Internet pretraživači, mobilni uređaji). Razvoj odgovarajućih Web aplikacija i portala osiguralo bi malim i srednjim tvrtkama jeftiniji način uključivanja u elektroničko poslovanje i na odgovarajući način nametnulo korištenje predloženih norma.

Svi prethodno navedeni problemi moraju se sustavno rješavati jer samo na taj način moguće je efikasno, uz minimalna financijska sredstva uvesti globalno elektroničko poslovanje u svim segmentima gospodarstva Republike Hrvatske. Dakle, prva faza efikasnog uvođenja elektroničkog poslovanja je normizacija i njeno široko prihvaćanje, koja značajno pojeftinjuje njegovo uvođenje. Softverski proizvodi trebaju podržavati predložene norme, a sve novo što se radi (bez obzira radi li se o domaćim ili stranim proizvođačima) treba biti usklađeno s tim normama. Pošto normizacija ne može biti propisana nego samo preporučena (osim kada država strogo inzistira na normi i to stavi u zakon), treba posebno naglašavati ekonomski aspekt korištenja predloženih norma (uštede itd.).

Uz prezentaciju na e-biz 2009 i razgovorima s kompetentnim stručnjacima iz područja elektroničkog poslovanja nametnuo se sljedeći prijedlog za efikasno uvođenje elektroničkog poslovanja u Republici Hrvatskoj:

- **Potrebno je organizirati operativni informacijski poslovni centar (*ebProvider*) koji će se brinuti o sustavnom korištenju predloženih norma, pružati servise potpore i aplikacije za elektroničko poslovanje i uključivati eksperte za pojedina područja.**

3.2. Uloga *ebProvidera*

Nositelji elektroničkog poslovanja u Republici Hrvatskoj su uglavnom velike organizacije, međusobno povezane partnerskim odnosom. Međutim, ponavljamo da 95% privrednih subjekata u Hrvatskoj su mala i srednja poduzeća. Bez organizirane pomoći, a napose pomoći koja će se nuditi preko informacijskih usluga, većina ovih organizacija neće biti u stanju koristiti pogodnosti elektroničkog poslovanja. Rješenja, odnosno poslovne aplikacije moraju biti isplative (niska početna ulaganja, profit u kratkom roku), modularne, skalabilne te međusobno kompatibilne (s gledišta norma koje koriste). Tvrtke moraju odmah uvidjeti korist implementiranih rješenja, a same aplikacije moraju istovremeno predstavljati i gradbene blokove većeg sustava elektroničkog poslovanja. Upravo se na tim spoznajama temelji i uloga *ebProvidera.* Napominjemo da je uloga *ebProvidera* isključivo u strategiji implementacije tehnoloških rješenja za elektroničko poslovanje, a ne na zakonskoj regulativi.

Uloga *ebProvidera*:

- Odabire tehnologije i norme (preporuke) kojima će se tvrtke koje se uključe u sustav elektroničkog poslovanja morati prilagoditi. Pri tome proces prilagodbe mora biti što jednostavniji. Hrvatska ne može ni financijski ni kadrovski podržavati sve postojeće norme. Zbog toga je zadaća ebProvidera da predloži skup norma primjerenih za korištenje u Hrvatskoj i oko njih gradi globalnu arhitekturu sustava elektroničkog poslovanja i razvija (primjenjuje) odgovarajuće aplikacije, gdje bi većina malih, srednjih i velikih tvrtki pronašla rješenje za svoje potrebe. Pri tome mora voditi računa o već korištenim normama u Republici Hrvatskoj i svjetskim trendovima.

- Odabire organizacije u kojima će ispitati referentne modele i pilotske aplikacije. Na taj način moguće je puno efikasnije uvesti u proces elektroničkog poslovanja pojedine postupke i aplikacije.

- Osmišljava inicijalne poslovne aplikacije/rješenja koju će ponuditi tvrtkama. Implementira aplikacije koje moraju biti isplative i privlačne malim i srednjim tvrtkama, prilagodljive njihovim potrebama, a dovoljno generička kako bi služila kao gradbeni blok sustava elektroničkog poslovanja. Kupoprodaja roba, usluga i informacija preko Interneta bila bi omogućena svima, kako velikim poslovnim sustavima tako i srednje velikim odnosno malim tvrtkama. Premještanjem složenosti ovakva sustava, a kroz navedene usluge aplikacija i servisa potpore, tvrtke s malim ili nedovoljno aktivnim ljudskim i drugim resursima mogle bi se na

relativno jednostavan način uključiti u B2B ili B2C poslovanje. Bitno je da takva primjena u malim i srednjim tvrtkama bude ekonomski isplativa.

- Osigurava potrebnu hardversku i softversku potporu sustavu elektroničkog poslovanja.

- Osigurava dostupnost kataloga za hrvatske tvrtke. Naime, postoji čitav niz različitih kataloga po vrstama i dosegu (svjetski, europski, regionalni, nacionalni, granski, lokalni). Za svakoga već ima puno organizacija koje ih kvalitetno i kompetentno vode. Istaknimo vrlo uspješan hrvatski elektronički katalog trgovačkih jedinica i partnera eCROKAT [8]. Uloga ebProvidera je da daje informacije i smjernice u korištenju kataloga, upućuje na organizacije koje mogu pružati adekvatne usluge, te osigurava mogući razvoj registra i repozitorija za potrebe tvrtki u Republici Hrvatskoj. Isto tako, brine se za jedinstveni sustav popisa šifarnika potrebnih kod izrade elektroničkih dokumenata kao npr. šifarnici za jedinice mjere, jezike, valute, države, načine plaćanja, vrste dokumenata (račun, terećenje, storno, odobrenje), šifre PDV-a (izvoz, 22%, 0%, 10%, ne podliježe oporezivanju, ...), trošarine (povratna naknada, akciza, razne trošarine za duhan i alkohol) s posebnim naglaskom na lokalne šifarnike.

- Održava sustav te ga proširuje i razvija ovisno o zahtjevima i potrebama sudionika elektroničkog poslovanja.

ebProvider bi također morao imati ključnu ulogu u sljedećem:

- Turizam, kao jedan od najatraktivnijih hrvatskih "proizvoda", poslovno je povezan s lancem aktivnosti u proizvodnji, preradi i distribuciji hrane. Istovremeno, on djeluje poticajno i na prodaju roba i usluga u nizu drugih područja. Zato je važno da i turistička djelatnost bude uključena u djelatnost *ebProvidera*. Naglasimo da u Republici Hrvatskoj u okviru Adriatica.net Group (vodeći turistički operatori i agencije u Hrvatskoj i jadranskoj regiji) djeluje vrlo uspješni portal *www.adriatica.net* [9] koji pruža usluge informiranja, rezerviranja i korištenja čitavog niza turističkih usluga. Naravno, uloga *ebProvidera* bi samo nadopunjavala djelovanja ovakvih uspješnih tvrtki na onim segmentima koji su nepokriveni, što ne isključuje mogućnost da i ovakve tvrtke ne preuzmu dio uloge *ebProvidera* u području turizmu.

- Elektronička burza roba i usluga za poslovanja tipa B2B i B2G. Cilj je uspostaviti elektroničku burzu (*electronic exchange*) roba i usluga za poslovanja tipa B2B (*business-to-business*) i B2G (*business-to-government*). Kupovanje i prodaja na načelu samoposluživanja (uz razmjenu digitalno potpisanih dokumenata), aukcije (prodavača ili kupaca) i elektroničko plaćanje, osnovne su funkcije elektroničke burze. Preko nje će se otvoriti i dodatni prostor za informacijsko povezivanje cijelih proizvodno-distribucijskih lanaca i za radikalnu modernizaciju poslovnih procesa u svim uključenim organizacijama. Inicijalno bi se uspostavila tzv. "vertikalna" burza, namijenjena jednom tipu djelatnosti, u ovom slučaju proizvodnji i distribuciji hrane i turizmu. Da bi se resursi burze što efikasnije koristili, u kasnijoj fazi obuhvatit će se i druga područja. Nadalje, kako je

Hrvatska mala zemlja, racionalnost nalaže da se s istim rješenjima obuhvate potrebe privrednih organizacija i države kao velikog kupca raznih roba i usluga. Nadležnim organima će se stoga predložiti da i država postane sudionikom ovoga projekta. On će joj omogućiti da sve svoje nabave u budućnosti obavlja elektroničkim putem. Pored velikih ušteda, takav postupak donijet će još jedan značajan dobitak. Cijeli sustav postat će potpuno transparentan, što znači da će se bitno suziti prostor mogućim neregularnostima tijekom državnih nabavki.

- Potpora elektroničkom poslovanju tipa B2C kroz uslugu elektroničkog trgovačkog centra. U okviru *ebProvider*a može se uspostaviti usluga elektroničkog trgovačkog centra s kojom će se na sustavan način podržavati poslovanje tipa B2C (*business-to-consumer*). Elektronički trgovački centar treba omogućiti svakom zainteresiranom poduzeću ili pojedincu da vrlo lako, na principu samoposluživanja, otvori, strukturira i vodi vlastiti elektronički dućan u okviru elektroničkog trgovačkog centra. Svu brigu oko informacijsko-komunikacijske infrastrukture dućana preuzet će pritom *ebProvider*. S ovom uslugom zadovoljit će se potrebe široke populacije potrošača i velikog broja organizacija i pojedinaca koji će prodavati robe i usluge fizičkim osobama. Iako su efekti poslovanja tipa B2C mnogo manji od onih koje donosi B2B, ovaj način rada, dopunjen s elementima B2B, može biti vrlo zanimljiv hrvatskom turizmu. Elektroničkim povezivanjem ponuđača turističkih usluga (pa i onih najmanjih, tipa *"Zimmer frei"*) s jedne strane i elektroničkog trgovačkog centra s druge, omogućila bi se i razmjena poslovno obvezujućih (digitalno potpisanih) poruka o prijavi ili prihvatu gostiju. Očekivani rezultat je viša kvaliteta turističke usluge i bolje korištenje raspoloživih kapaciteta.

3.3. Tko može biti *ebProvider*

Ključni je problem tko će preuzeti odgovornost za sustavno uvođenje elektroničkog poslovanja i razvoj odgovarajućih aplikacija, dakle biti *ebProvider*.

Jedno od rješenja je da odgovornost za dizajn i implementaciju sustava preuzme neka neprofitna organizacija koju financira gospodarstvo ili državno tijelo. Takvo rješenje moglo bi se pokazati neučinkovito, upravo zbog toga što je potrebno realizirati konkretno rješenje uporabljivo u stvarnim poslovnim uvjetima.

Potencijalno je bolje rješenje da odgovornost preuzmu velike tvrtke koje posjeduje dovoljno ljudskih i financijskih sredstava za razvoj sustava i koje su ključni tržišni sudionici. Razvijeni sustav bi se zatim ponudio ograničenom skupu malih i srednjih tvrtki koje su poslovni partneri velike tvrtke. Ovakav pristup osigurao bi visoku razinu prilagodljivosti i kontrolirani rast sustava.

Ipak, uvažavajući naše specifičnosti zbog međusobne konkurencije velikih tvrtki mišljenja smo da bi *ebProvider* trebala biti neprofitna organizacija koju financira gospodarstvo ili državno tijelo. Međutim, ona bi trebala imati dovoljni broj eksperata (ne nužno zaposlenih u *ebProvideru*) koji bi bili kritična masa za efikasno uvođenja elektroničnog poslovanja. Jedanput kad elektroničko poslovanje saživi u većini malih i srednjih tvrtki, tada će i ostale tvrtke morati uvesti elektroničko poslovanje ako žele

ostati na tržištu. Zbog toga je bitno da uz koncept *ebProvider* ulazak srednjih i malih tvrtki bude financijski isplativ.

3.4. Zaključak

Za sustavno uvođenje elektroničkog poslovanja u hrvatsko gospodarstvo bitni su preduvjeti:

- **Tvrtke moraju definirati vlastitu strategiju uvođenja elektroničkog poslovanja, odnosno potrebno je pomoći s adekvatnim rješenjima onim malim i srednjim tvrtkama u Republici Hrvatskoj koje zbog nedostatka kadrovskih i financijskih resursa nisu u mogućnosti definirati vlastitu strategiju uvođenje elektroničkog poslovanja, a još manje je i realizirati.**

- **Republika Hrvatska ne može podržavati sve postojeće norme jer to zahtijeva veliki broj eksperata za njihovu implementaciju i prevelika financijska sredstva. Potrebno je prihvatiti skup norma primjerenih za korištenje u Republici Hrvatskoj i oko njih graditi globalnu arhitekturu sustava elektroničkog poslovanja i razviti (primijeniti) odgovarajuće aplikacije, gdje bi većina malih, srednjih i velikih tvrtki pronašla rješenje za svoje potrebe i u tome pronašle ekonomski efekt (ušteda, konkurentnost).**

- **Potrebno je organizirati operativni informacijski poslovni centar (*ebProvider*) koji će se brinuti o sustavnom korištenju predloženih norma, pružati servise potpore i aplikacije za elektroničko poslovanje i uključivati eksperte za pojedina područja. Za tu namjenu može se osnovati Agencija za elektroničko poslovanje koja bi se financirala iz proračuna ili iz gospodarstva. Bitna je pretpostavka da dugoročno ekonomske uštede kroz djelovanje Agencije za elektroničko poslovanje (*ebProvidera*) višestruko nadmaše ulaganja.**

4. Prezentacija norma

Prezentacija izrađena u *PowerPoint*-u je koncipirana tako da omogućuje zainteresiranima i samostalno upoznavanje s materijalima, koristeći mogućnosti koje nudi Portal projekta.

Sastoji se od sljedećih cjelina:

4.1. Pregled problematike

`Isporuka6Faza01_5_01_PregledProblematikePPT.ppt`

4.2. Pregled sadržaja isporuka

`Isporuka6Faza01_5_02_SadržajiIsporuka.ppt`

4.3. Tematski detalji

`Isporuka6Faza01_5_03_TematskiDetalji.ppt`

4.4. Materijali GS1 Croatia (autor: Damir Šegović)

4.4.1. eCROKAT – Kako krenuti

`Isporuka6Faza01_5_05_GS1_1_eCROKAT_Kako_krenuti_2008.pdf`

4.4.2. Opis sustava GS1

`Isporuka6Faza01_5_05_GS1_2_opis_sustava_2006.pdf`

4.4.3. e-Poslovanje

`Isporuka6Faza01_5_5_GS1_3_ePoslovanje_2008.pdf`

4.5. Nastavni materijali za stručno obrazovanje (eBCM-VET, *Leonardo da Vinci Project* 2005 – 2007)

Rezultati projekta financiranog od EU su preuzeti privolom autora s Islanda [10], te su prevedeni na hrvatski. Nalaze se u datoteci:

`Isporuka6Faza01_5_05_01_Gen_Intro_eBiz-ppt.ppt`

Podijeljeni su na 11 tematskih cjelina, navedenih u sljedećim poglavljima.

4.5.1. Opći uvod u e-Poslovanje

4.5.2. Upravljanje promjenama, motivacija zaposlenika, upravljanje ljudskim odnosima, upravljanje performansama

4.5.3. Odabir trenutka ulaska u e-Poslovanje

4.5.4. Infrastruktura e-Poslovanja

4.5.5. Zakoni i regulativa

4.5.6. Potreba za sinkronizacijom

4.5.7. e-Poslovni ugovori

4.5.8. Sigurnost kao osnova povjerenja i pouzdanja u e-Poslovanju

4.5.9. Vrijednost i upravljanje dobrim podacima

4.5.10. Implementacija e-Poslovanja

4.5.11. ICT znanja za upravljanje vlastitim sustavima

5. Zaključak

Obrazovni materijali u tekstualnom obliku imaju za cilj upoznati čitatelje s relativno novom tehnologijom Web servisa u kojoj se javljaju mnogi aspekti e-Poslovanja.

Slijedilo je poglavlje koje predlaže jedan mogući način za uspješno širenje e-Poslovanja u Republici Hrvatskoj.

Obrazovni materijali u obliku *PowerPoint* prezentacija daju:

- Pregled problematike e-Poslovanja
- Pregled sadržaja elaborata isporučenih temeljem ovog Projekta
- Detaljnija razmatranja nekih aspekata e-Poslovanja
- Materijali GS1 Croatia, preuzeto po odobrenju autora Damira Šegovića
- Nastavni materijali za stručno obrazovanje, preuzeto po odobrenju autora, Rúnar Már Sverrisson i Gudbjorg Bjornsdottir, eBCM-VET, *Leonardo da Vinci Project* 2005 – 2007 i prevedeno na hrvatski.

6. Reference

[1] Amir Hartman & John Sifonius with John Kador: *Net Ready,* McGraw-Hill, 2000

[2] CWA 14921: *Web Services: Technology and Standardization Aspects; 2004 WS-Security Policy* 1.2 OASIS Standard; OASIS; 2007

[3] Basic Profile Version 1.0; The Web Services-Interoperability Organization; 2004

[4] *Web Services Security: SOAP Message Security* 1.1; OASIS; 2006

[5] *WS-Trust* 1.3 OASIS Standard; OASIS; 2007

[6] Miroslav Popović: Nadziranje pristupa računalnim sustavima zasnovanim na uslugama, Magistarski rad, FER, 2006

[7] Tomislav Rajnović, Nikša Stanović: Tehnologija Web servisa u elektroničkom poslovanju, Seminarski rad, FER/ZPR,Zagreb, 2009.

[8] Damir Šegović, GS1 Croatia, eCROCAT – 3 *PowerPoint* prezentacije

[9] Adriatica.net, Početna stranica: http://www.adriatica.net/home/home_hr.htm (17. travnja 2009.)

[10] Rúnar Már Sverrisson i Gudbjorg Bjornsdottir: *eBusiness Community Model – Vocational Education and Training project*, http://www.ebcm-vet.net/, svibnja 2009, *PowerPoint* prezentacija