UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

DIPLOMSKO DELO

MITJA MAKOVEC

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

VLOGA JEZIKA XML V ELEKTRONSKEM POSLOVANJU

Ljubljana, november 2001 MITJA MAKOVEC

IZJAVA

Študent **Mitja Makovec** izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom **doc. dr. Mojce Indihar – Štemberger** in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 12.11.2001 Podpis:

Kazalo

Seznam slik

Seznam tabel

1. Uvod

Razvoj računalništva in informatike je tako velik, da je posegel na vsa področja življenja človeka. Prav tako je razvoj posegel na področje ekonomije ter korenito spremenil poslovanje gospodarskih subjektov. Tako je nastala nova besedna zveza, ki opisuje ta nov način poslovanja - elektronsko poslovanje.

Podjetja imajo na izbiro dve možnosti ali prevzamejo elektronski način poslovanja ali pa se odločijo, da bodo z elektronskim poslovanjem še malo počakala. Glede na konkurenco, ki je prisotna na trgu pa se moramo zavedati, da bodo podjetja, ki ne bodo šla v korak s časom ter sprejela izzivov elektronskega poslovanja, verjetno propadla, saj ne bodo mogla konkurirati drugim podjetjem.

V diplomski nalogi se bom dotaknil teme elektronskega poslovanja ter predvsem izmenjave podatkov v elektronski obliki med podjetji, kot načina za doseganje konkurenčnih prednosti s pomočjo računalniške tehnologije. Podjetja so se v preteklosti povezovala v zasebna omrežja ter si tako izmenjevala dokumente, vendar je bilo to dokaj drago, tako da je bila računalniška izmenjava podatkov (RIP) primerna samo za velike korporacije. S prihodom Interneta kot svetovnega omrežja ter predvsem jezika XML, pa je pričakovati, da se bodo stroški RIP-a zelo znižali, tako da bo le-ta na voljo tudi manjšim podjetjem.

Namen diplomskega dela je predstaviti jezik XML ter njegovo vlogo pri elektronskem poslovanju, predvsem kot jezik za standardizacijo elektronskih sporočil, ki se prenašajo med podjetji.

V drugem poglavju tega diplomskega dela je razlaga osnovnih pojmov povezanih z elektronskim poslovanjem, kot na primer razvoj elektronskega poslovanja skozi čas, vrste ter prednosti takega poslovanja. Poudarek je predvsem na poslovanju podjetje – podjetje (B2B), saj ta vrsta poslovanja obsega okoli 80 odstotkov vsega elektronskega poslovanja. V tretjem poglavju je podan pregled računalniške izmenjave podatkov, v četrtem poglavju pa opis značilnosti in lastnosti samega jezika XML ter vprašanj, ki so povezana z varnostjo. V šestem poglavju je opisana vloga in prednost uporabe jezika XML v elektronskem poslovanju, natančneje pri elektronski izmenjavi podatkov.

2. Elektronsko poslovanje

Elektronsko poslovanje je izraz, ki ga vedno večkrat zasledimo v vsakdanjem življenju. Mnogi ljudje si pod tem izrazom predstavljajo izmenjavo podatkov med računalniki (Jerman - Blažič, 2001, str. 11), ali pa mislijo na trgovanje – kupovanje in prodajo blaga preko svetovnega spleta[1] (Marusich, 2000, str. 7). Vendar pa sta ti dve definiciji preozki, da bi lahko opisali celoten obseg, ki ga zajema elektronsko poslovanje. Elektronsko poslovanje bi lahko opredelili kot vse, kar danes delamo v sklopu svoje poslovne dejavnosti s pomočjo programskih rešitev in računalniških omrežij (Jerman - Blažič, 2001, str. 11).

Elektronsko poslovanje obsega (Jerman - Blažič, 2001, str.11):

- elektronsko trgovanje (trading)
- elektronsko bančništvo (banking)
- elektronsko plačevanje
- elektronsko trženje
- elektronsko zavarovalništvo
- elektronsko založništvo
- delo na daljavo
- spletno trgovino
- pouk na daljavo
- avkcije na daljavo
- poprodajne storitve
- elektronsko borzno poslovanje
- elektronsko naročanje
- …

Pojem "elektronsko poslovanje" izhaja iz angleškega izraza "electronic commerce", ki je nastal v trgovini in industriji, oz. se je nanašal na vsa poslovna področja (Toplišek, 1998, str. 4). Vendar je ta izraz v današnjem času izpodrinil izraz "e-business", ker bolje odseva vsebino (Jerman - Blažič, 2001, str. 11).

V Sloveniji je državni zbor RS dne 13.6.2000 sprejel zakon o e-poslovanju in e-podpisu (ZEPEP), v katerem je opredeljena zakonska osnova za elektronsko poslovanje ter uporabo elektronskega podpisa in tudi kazenske določbe, v primeru kršitev ZEPEP.

[1] angl. WWW – World Wide Web

2.1. Kratka zgodovina

Elektronsko poslovanje spreminja način poslovanja modernih podjetij, saj se vse več podjetij odloča za poslovanje preko Interneta. Lahko bi rekli, da je elektronsko poslovanje v današnjem času nuja in ne samo trenutna modna muha. Kot primer lahko navedem ugotovitev podjetja Forrester Research[2], ki je v svoji raziskavi ugotovilo, da znaša vrednost trgovanja blaga in storitev med podjetji v letu 2000 preko 100 milijard ameriških dolarjev, predvidevajo pa, da bo vrednost v letu 2001 narasla preko 220 milijard ameriških dolarjev (iPier.com, 2001).

Vse se je začelo v letu 1968, ko se je začel razvoj računalniških omrežij ter standard za računalniško izmenjavo podatkov (RIP).[3] RIP je omogočila podjetjem, da so si lahko medsebojno izmenjavali podatke (Weisman, 2000).

V sedemdesetih letih se je s pojavom elektronskih finančnih prenosov med bankami prek varnih zasebnih omrežij[4] spremenil način poslovanja na finančnem trgu. V poznih sedemdesetih in zgodnjih osemdesetih letih se je elektronsko poslovanje razširilo v okviru podjetij, v obliki sistemov za prenos podatkov, računalniške izmenjave podatkov ter elektronske pošte. Prednost uporabe nove tehnologije se je odražala predvsem v zmanjšanju obsega papirnega dela in povečanju avtomatizacije pisarniškega poslovanja.

Sredi osemdesetih let so se pojavile elektronske konference, kot nova oblika družabne interakcije ter učenje na daljavo in prenosi datotek.[5] Še vedno pa je bilo računalništvo domena ozkega kroga zanesenjakov ter znanstvenikov. Devetdeseta leta so z razvojem in razširjenostjo Interneta ter s pojavom svetovnega spleta prinesla preobrat, ki je sprožil razvoj elektronskega poslovanja, ki smo mu priča danes. Nove tehnologije so zagotovile prijaznost do uporabnikov in enostavno uporabo. Tako je vse več ljudi začelo uporabljati svetovni splet, kar je s strani podjetij pomenilo vedno več potencialnih kupcev. Svetovni splet je poslovanje pocenil in tako zagotovil ekonomijo obsega ter omogočil raznovrstne poslovne aktivnosti (Jerman - Blažič, 2001, str. 14). Glavna prednost svetovnega spleta je, da je dostopen vsakomur, tako organizacijam kot fizičnim osebam.

---

[2] Forrester Research – http://www.forrester.com

[3] RIP – računalniška izmenjava podatkov, angl. EDI – electronic data interchange

[4] SWIFT – omrežje bančnih organizacij

[5] FTP – angl. File Transfer Protocol

2.2. Prednosti elektronskega poslovanja

Elektronsko poslovanje prinaša veliko prednosti pred običajnim poslovanjem. Prednosti elektronskega poslovanja lahko izrabljajo, tako velike multinacionalke kot tudi majhna podjetja. Velikost ni pomembna, važno je kako se podjetja lotijo elektronskega poslovanja.

Med prednosti elektronskega poslovanja lahko štejemo (Marusich, 1999, str. 8-14; Marshall, 2001):

- *Prihranek pri stroških:* Poslovanje preko svetovnega spleta je cenejše, saj so stroški povezani s poslovanjem manjši, kot so pri navadnem poslovanju(ni stroškov pošiljanja papirnatih dokumentov, poenostavitev poslovnih procesov).
- *Pot do novih kupcev:* Podjetja lahko s pomočjo svetovnega spleta oglašujejo svoje izdelke, s tem pa tudi privabljajo nove kupce, kateri lahko potem ali kupijo izdelke neposredno preko svetovnega spleta, ali pa se odpravijo v klasično trgovino ter kupijo izdelek, katerega so predhodno videli na svetovnem spletu.
- *Boljši odnosi s kupci:* Današnje Internetne tehnologije nam omogočajo, da lahko spremljamo obnašanje naših kupcev na svetovnem spletu, tako lahko zbiramo podatke o straneh, ki jih kupci obiskujejo, času, ki ga prebijejo na njih ter njihovih priljubljenih spletnih straneh. Tako lahko naredimo profile za posameznega kupca ter prilagajamo vsebino naše spletne strani prav njemu. S tem izboljšamo počutje kupca ter posredno vplivamo na njegove bodoče nakupe. Kot primer lahko podam podjetje Amazon,[6] pri katerem spremljajo nakupe svojih kupcev, ter kaj jim je všeč. Na podlagi zbranih podatkov svoje kupce obveščajo o novih naslovih, ki bi jih utegnili zanimati. Velja načelo: "Zadovoljen kupec bo verjetneje kupoval tudi druge izdelke v isti trgovini, kot nezadovoljen kupec." (Brain, 2001).
- *Hitrejši dostop do trga:* Svetovni splet prekaša vse običajne prodajne poti predvsem pri hitrosti in prilagodljivosti pri uvajanju novih izdelkov ter spreminjanju cen in posodabljanju prodajnega programa.
- *Večji, boljši prodajni program:* Če samo pomislimo, koliko različnih izdelkov naročajo trgovine, vendar ker je povpraševanje različno, ni nujno, da imajo trgovine vse izdelke na zalogi, ter da jih sploh prodajajo. Pri spletni trgovini lahko trgovina vpiše vse svoje prodajne izdelke, nato pa jih, če je zanimanje zadosti veliko, tudi naroči. Kot primer lahko spet vzamemo spletno knjigarno Amazon, katera ima v svojem

[6] Amazon – največja spletna knjigarna (http://www.amazon.com)

prodajnem programu preko 3 milijone knjig, kar je več kot jih ima katerakoli navadna trgovina.

- *Boljša povezanost s poslovnim ciklom podjetja:* Spletna stran podjetja mora biti čim bolje povezana s poslovnim ciklom podjetja. S tem prinaša prednosti, ki jih navadna trgovina ne more. Na primer, podjetje FedEx[7] je v svojem poslovanju uvedlo spremljanje paketnih pošiljk preko svetovnega spleta, tako da so njihovi naročniki točno vedeli, kje se trenutno nahaja njihov paket. Tako je podjetje dodalo dodatno vrednost svoji storitvi, s tem pa postalo bolj privlačno za svoje kupce.
- *Nabava:* Z uporabo svetovnega spleta, se poenostavi proces nabave podjetij ter tudi pospeši. Podjetjem ni potrebno več zadrževati ekonomskih dobrin v zalogah, saj lahko s pomočjo informacijske tehnologije spremljajo povpraševanje po dobrinah ter nabavljajo dobrine takrat, ko jih odjemalci potrebujejo.

Elektronsko poslovanje je prineslo spremembe na treh področjih (Istenič, 2000, str. 8):

- *Spremenjen način dela:* Elektronska pošta in programske rešitve za elektronsko sodelovanje postajajo že nepogrešljive pri poslovanju podjetij. Nove tehnologije omogočajo tudi večjo mobilnost.
- *Spremenjen način trgovanja:* Odnos s stranko se je spremenil. Podjetja s strankami gradijo dolgoročen odnos, ne gledajo samo na kratkoročne koristi. Na vsako stranko gledajo individualno, se ji želijo čim bolj približati s svojo ponudbo, tako da masovna proizvodnja izgublja pomen.
- *Spremenjene meje dejavnosti:* Podjetja se morajo čim bolj specializirati če želijo ostati konkurenčna. Izkoriščati mora svoje prednosti, ki jih ima pred svojo konkurenco ter jih čim bolj poudarjati.

2.3. Vrste elektronskega poslovanja

Elektronsko poslovanje lahko v grobem delimo na naslednje tri glavne vrste:

- Podjetje – potrošnik (B2C)[8]
- Podjetje – podjetje (B2B)[9]
- Javna in državna uprava – javnost in ljudstvo

[7] FedEx – http://www.fedex.com

[8] B2C – angl. Business to Consumer

[9] B2B – angl. Business to Business

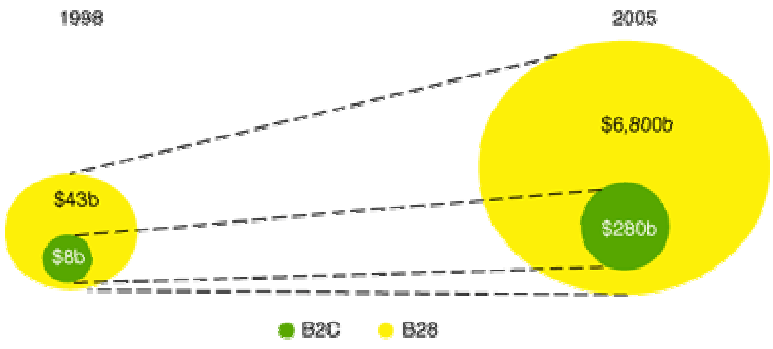
2.3.1. Podjetje – potrošnik (B2C)

Poslovanje Podjetje – potrošnik si lahko predstavljamo kot tradicionalno poslovanje, kjer kupec kupuje v trgovini s to razliko, da vse poteka elektronsko, preko svetovnega spleta (Berger, 2000). Elektronsko poslovanje s končnim potrošnikom zajema veliko področij, večinoma pa temelji celotno poslovanje na Internetnih spletnih straneh. Potrošniku omogočajo opravljanje raznovrstnih dejavnosti preko domačega računalnika, tako na primer elektronsko bančništvo, nakupovanje preko svetovnega spleta, izobraževanje na daljavo ter ne nazadnje tudi delo na daljavo (Jerman - Blažič, 2001, str. 17).

2.3.2. Podjetje – podjetje (B2B)

B2B je kratica, ki predstavlja poslovanje podjetja z drugim podjetjem, je tip poslovanja, ki vsebuje transakcije iz enega podjetja v drugega s pomočjo računalnikov, ter poteka preko elektronskih povezav.
Elektronsko poslovanje med podjetji (B2B) po ocenah različnih raziskav predstavlja največji del elektronskega poslovanja. Obstajajo ocene, da pomeni delež poslovanja B2B proti B2C kar osemdeset odstotkov vsega elektronskega poslovanja, v prihodnosti pa naj bi se ta odstotek še povečal. Napovedujejo, da naj bi do leta 2003 med 30 in 40 odstotki vseh podjetij prodajalo prek spleta, od 80 do 90 odstotkov podjetij pa bo v spletu tudi nabavljalo (Pavšič, 2001, str. 60).

Slika 1: Delež elektronskega poslovanja razdeljen med B2B in B2C



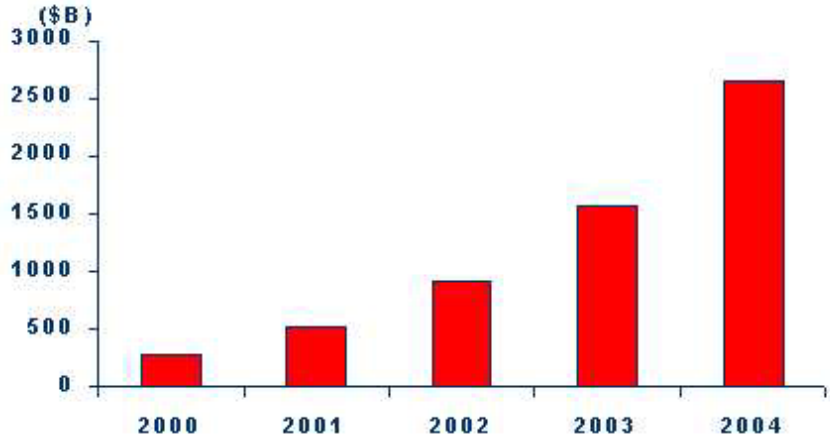
Vir: ERC Beximco, 2001.

Pričakuje se, da bodo prihodki iz B2B iz 185 milijard dolarjev v letu 2000, zrasli na 1,26 bilijona dolarjev letnega prometa v letu 2003. V Sloveniji je leta 1998 elektronsko

poslovalo samo 5 odstotkov podjetij, medtem ko je v Evropi 29 odstotkov podjetij že poslovalo elektronsko (Jerman - Blažič, 2001, str. 20).

Nekatere projekcije napovedujejo še višjo rast B2B, kot prikazuje slika 2. Vidimo, da so pričakovani prihodki iz B2B v letu 2003 okoli 1,6 bilijona ameriških dolarjev, v letu 2004 pa okoli 2,6 bilijona ameriških dolarjev.

Slika 2: Obseg svetovnega B2B e-poslovanja



Vir: Flisi, 2001.

Glavne prednosti elektronskega poslovanja podjetij (B2B) so (ERC Beximco, 2001):

- znižuje dobavne stroške in omogoča lažje iskanje najcenejšega dobavitelja, ter znižuje transakcijske stroške,
- omogoča boljšo povezanost z dobavitelji,
- omogoča boljše upravljanje z zalogami, oziroma celo odpravo zalog podjetij.

Čeprav je bil odstotek podjetij, ki poslujejo elektronsko, v Sloveniji dokaj majhen, kljub temu tudi pri nas najdemo veliko primerov uspešne uporabe elektronskega poslovanja. Med vidnejšimi so na primer Zavod za zdravstveno zavarovanje, Agencija za plačilni promet, Petrol, Carinska uprava RS, Luka Koper in drugi (Pucihar, 1999, str. 8).

Stanje na področju elektronskega poslovanja v Sloveniji se popravlja, kar je razvidno tudi v raziskavi, ki jo je opravil RIS[10], v kateri so prišli do naslednjih ugotovitev e-poslovanja slovenskih podjetij (RIS, 2001):

- Internet uporabljajo že praktično vsa večja podjetja in tudi večina manjših, najpogosteje za pridobivanje poslovnih informacij ter za komuniciranje.
- E-poslovanje uporablja polovica podjetij z dostopom do Interneta. Pri tem si večinoma dokumente izmenjujejo s petimi poslovnimi partnerji ali manj. Pri tem tuji partnerji predstavljajo več kot tretjino vseh partnerjev.
- Najpomembnejši razlogi uvajanja e-poslovanja so: večja kvaliteta storitev, fleksibilnost, konkurenčna prednost ter novi trgi. Nižanje stroškov in povečevanje prodaje sta nekoliko manj pomembna. Kot osnovna prednost e-poslovanja izstopa takojšna izvedba in vpogled v transakcije. Med ovirami večja podjetja najpogosteje navajajo pomanjkanje kadrov in tudi sredstev, manjša pa predvsem nepoznavanje.
- Ne-Internetni protokoli (X400, VAN[11]...), ki so prisotni v nekaj odstotkih podjetij (desetina pri velikih), bodo večinoma zamenjani z Internet sistemi.
- Podjetja, ki uporabljajo e-poslovanje – to pa je že večina slovenskih podjetij, menijo, da bo e-poslovanje v dveh do treh letih postalo standard poslovanja v njihovi panogi.
- V mednarodnih primerjavah e-poslovanja Slovenija ne zaostaja, nasprotno, visoka penetracija Interneta, predvsem pa uporaba elektronskega plačilnega prometa APP, jo v mnogih pogledih uvršča med razvitejše države.

Pomembni vidik podjetniške integracije in sodelovanja pa je tudi standardizacija elektronskega poslovanja, saj le-ta prinaša koristi z zmanjševanjem stroškov potrebnih za realizacijo elektronskega poslovanja. Eden izmed splošno priznanih in uporabljanih standardov je tudi standard UN/EDIFACT[12].

Vsako sporočilo v formatu UN/EDIFACT vsebuje edinstven podatek o ceni, izdelku ali zaporedni številki. Ponudniki želijo z uvedbo svojih tehnologij preseči možnosti za izmenjavo podatkov, ki jih ponuja RIP. Pri tem se opirajo predvsem na jezik XML[13], ki z leti pridobiva pravi pomen pri označevanju podatkov. Tako ima vedno več programskih

[10] RIS – Raba Interneta v Sloveniji (http://www.ris.org)

[11] VAN – angl. Value Added Network

[12] UN/EDIFACT – United Nations Electronic Data Interchange for Administration, Commerce and Transport

[13] XML – angl. eXtensible Markup Language

rešitev tudi vgrajeno podporo za jezik XML, obenem pa XML omogoča nadgradnjo UN/EDIFACT standarda, kar še olajša izmenjavo podatkov med podjetji oz. znotraj podjetja.

2.3.3. Javna in državna uprava – javnost in ljudstvo

Pri poslovanju z državno upravo ločimo njeno poslovanje s podjetji (na primer registracija vozil, oddaja davčnih napovedi, javne nabave…) in poslovanje s prebivalci (Jerman - Blažič, 2001, str. 171).

V raziskavi RIS so ugotovili, da slovenska podjetja najpogosteje izmenjujejo podatke z Agencijo za plačilni promet – to velja za tri četrtine velikih, slabi dve tretjini srednjih podjetij, pa tudi za vsako drugo majhno in vsako tretje mikro podjetje.

Izmenjava podatkov z drugimi institucijami je manj razširjena, nekoliko pogosteje podjetja sodelujejo še s Statističnim uradom RS ter Zavodom za pokojninsko in invalidsko zavarovanje. Z navedenimi institucijami najpogosteje sodelujejo velika podjetja: tako s Statističnim uradom RS sodeluje slaba tretjina, z Zavodom za pokojninsko in invalidsko zavarovanje dobra petina, s Carinsko upravo RS pa petina velikih podjetij. Velika podjetja pogosteje kot druga sodelujejo še z Zavodom za zdravstveno zavarovanje (17%) ter z Zavodom za zaposlovanje (16%) (RIS, 2001).

Pri poslovanju s prebivalci lahko omenimo Zavod za zdravstveno zavarovanje Slovenije[14], ki že omogoča nekatere dejavnosti preko svetovnega spleta, kot na primer elektronsko naročevanje konvencijskih potrdil.

3. Računalniško izmenjavanje podatkov – RIP

V literaturi se pojavlja veliko definicij računalniške izmenjave podatkov. Računalniško izmenjavo podatkov najlažje razumemo kot zamenjavo papirnih naročil z elektronskim nadomestkom (Škedelj, 1999, str. 34). Nekateri avtorji poudarjajo, da RIP za razliko od elektronske pošte pomeni izmenjavo podatkov v standardizirani obliki in tako omogoča avtomatizacijo postopkov njihove obdelave, oziroma računalniško komunikacijo brez človeškega vmešavanja (Bračko, 1997, str. 9). Ali na primer, RIP je izmenjava elektronskih dokumentov v standardnem formatu, ki je poznan obema stranema v

[14] ZZZS – http://www.zzzs.si

transakciji ter uporablja elektronski transakcijski medij, za prenos poslovnih dokumentov (Huemer, 2000, str. 680).

Razvoj elektronskega poslovanja je v zadnjih letih dosegel velik razmah, prav elektronsko poslovanje pa je posledica prave revolucije v poslovanju podjetij, saj se morajo podjetja začeti prilagajati elektronskemu poslovanju, če želijo ostati konkurenčna. Kot sem že omenil v prejšnjem poglavju, je velik del elektronskega poslovanja očem skrit – to je poslovanje podjetje s podjetjem oziroma B2B. Da pa bi lahko podjetja med seboj uspešno sodelovala ter si izmenjevala poslovne dokumente, morajo uporabljati enak standard izmenjave podatkov.

V začetku, v poznih šestdesetih letih, so podjetja uporabljala lastne standarde ter si dokumentacijo izmenjevala preko lastnih uporabniških programov. Vendar je tak način zahteval ogromna sredstva, zato so se začela podjetja iz iste panoge med seboj povezovati ter med seboj določila standarde, saj je samo na ta način bilo moč stroškovno opravičiti uvajanje RIP-a (Slana, 1999, str. 26).

V sedemdesetih letih so se začeli pojavljati razni standardi za RIP, ki so postopoma prerasli v nacionalne standarde. Vendar je kmalu postalo jasno, da se mora vzpostaviti mednarodni standard za RIP, saj je samo tako možna globalna izmenjava elektronskih dokumentov med podjetji. Eden od bolj znanih standardov, ki se uporablja danes, je standard UN/EDIFACT.

3.1. Elementi RIP-a

Poglavitni elementi računalniške izmenjave podatkov so (Škedelj, 1999, str. 34):

- Uporaba elektronskega prenosnega medija (normalno omrežja z dodano vrednostjo – VAN) in ne uporaba fizičnih podatkovnih medijev, kot na primer diskete in cd-romi.
- Uporaba strukturiranih, formatiranih sporočil, ki temeljijo na dogovorjenih standardih, kar daje možnost prevajanja, tolmačenja in kontrole skladnosti z obstoječim naborom pravil.
- Relativno hitra dostava elektronskih dokumentov od pošiljatelja do prejemnika.
- Direktna komunikacija med programskimi rešitvami in ne samo med računalniki.

3.2. Vzroki za uvedbo RIP-a

Najpogostejši razlogi za uvedbo RIP-a so naslednji (Bračko, 1997, str.10):

- konkurenčna prednost, ki jo prinaša RIP
- pritiski poslovnih partnerjev
- želja po vpeljavi poslovanja "ravno ob pravem času"[15]

3.3. Stroški in koristi RIP-a

Računalniška izmenjava podatkov prinaša podjetjem številne prednosti, njena uporaba pa prinaša tudi določene stroške. RIP podjetjem omogoča, da zmanjšajo administrativne stroške, odpravo nekaterih nepotrebnih aktivnosti oziroma večkratni vnos podatkov, ter s tem tudi zmanjša možnost napak pri vnosu. Administrativni stroški se zmanjšajo tudi zaradi elektronskega prenosa podatkov med partnerji. RIP omogoča tudi povečanje učinkovitosti ter racionalizacijo poslovanja, saj se tokovi med poslovnimi partnerji avtomatizirajo, kar podjetjem omogoča obvladovanje večjih količin podatkov, brez povečanja števila zaposlenih oziroma celo z njihovim zmanjšanjem. Med posredne učinke RIP-a lahko štejemo še skrajšanje časa od naročila do realizacije, skrajšanje dostavnih časov, zmanjšanje zalog in prihranek denarja (Bračko, 1997, str. 23). Mnogokrat pa je vzrok za uvedbo RIP-a predvsem nuja, da lahko podjetje sploh ostane konkurenčno.

Stroški Rip-a pa so (Bračko, 1997, str. 23-24):

- stroški analize obstoječega poslovanja
- stroški izobraževanja in usposabljanja
- stroški svetovanja
- stroški zaposlenih
- stroški programske in strojne opreme
- telekomunikacijski stroški
- stroški vzdrževanja sistema

Pri ocenjevanju koristi in stroškov RIP-a se je treba zavedati, da se koristi pojavijo na dolgi rok. Zato je analizo koristi in stroškov nujno izvajati na dolgi rok, saj so skoraj vsi stroški v zvezi z uvedbo RIP-a v podjetju enkratni, tako da jih je potrebno razdeliti na daljše obdobje.

[15] JIT – angl. Just in Time

3.4. Standard UN/EDIFACT

Leta 1986 se je v okviru Organizacije združenih narodov pričel razvoj mednarodno priznanega standarda računalniške izmenjave podatkov, imenovanega UN/EDIFACT. Standard podaja sintaktična pravila za pripravo sporočil, ki se izmenjujejo med partnerji po elektronski poti. Pomembna lastnost UN/EDIFACT standarda je v tem, da je oblikovan tako, da je v celoti neodvisen od strojne in programske opreme, sporočilo oziroma dokumenti pa so v celoti šifrirani. Slovnico tvorijo podatkovni elementi, ki so zapisani v standardu ISO 9735, besedni zaklad pa tvorijo podatkovni elementi, ki so predstavljeni v standardu ISO 7372.

Torej, UN/EDIFACT je standard, ki vsebuje skupek svetovno sprejetih standardov in navodil za računalniško izmenjavo podatkov, še posebej v panogah povezanih s trgovino med neodvisnimi z informacijsko tehnologijo podprtimi podjetji.

Prizadevanja UN/CEFACT-a potekajo v smeri, da bi vsaka posamezna država jasno opredelila vse potrebne papirne in elektronske postopke ter dokumente, objavila kriterije elektronskega poslovanja v državi ter oblikovala nacionalni standard elektronskih sporočil, ki bi bil v okviru celotnega standarda (nekakšen podstandard UN/EDIFACT).

3.5. Razvoj standardizacije v Sloveniji

V Sloveniji od leta 1994 obstaja priporočilo za predlog slovenskega standarda, ki predvideva uporabo standarda ISO 9735 in na njegovi podlagi oblikovanih elektronskih sporočil (UN/EDIFACT, SWIFT).

Ministrstvo za znanost in tehnologijo je leta 1991 ustanovilo tudi Urad za UN/EDIFACT, ki naj bi zagotavljal povezavo s standardom in omogočil vpliv na njegovo oblikovanje ter prilagajanje nacionalnim potrebam. Urad za UN/EDIFACT je potreben, saj je slovensko gospodarstvo še prešibko, da bi lahko posamezna podjetja sodelovala s svojimi strokovnjaki v delovnih skupinah pri Organizaciji združenih narodov (Damjan, 1990, str. 56).

Urad naj bi skrbel predvsem za (Bračko, 1997, str. 14):

- usklajevanje vladnih in branžnih delovnih skupin pri dopolnjevanju vsebine standarda in
- razširjanje vsebine standarda, ki bo posebej prilagojena našemu prostoru.

Tudi mnoga slovenska podjetja, ki že poslujejo elektronsko, zlasti tista, ki poslujejo s tujino, v medsebojnih poslovnih odnosih s svojimi poslovnimi partnerji, uporabljajo standard UN/EDIFACT, večinoma na pobudo tujih partnerjev (Slana, 1999, str. 27).

3.6. RIP in Internet

Velika podjetja in organizacije poslujejo elektronsko že nekaj desetletij. Ker so bili standardi za RIP sprejeti še pred komercialno uporabo Interneta, so tudi zahteve glede RIP-a bile drugačne, tako glede opreme kot tudi standardov. Najpogostejše omrežje za prenos podatkov, ki je bil v uporabi pri RIP, je bilo omrežje razvito v skladu s standardom ISO OSI X.400. Vendar pa je imelo to omrežje precej pomanjkljivosti, v primerjavi z omrežjem Internet (tabela 1).

Tabela 1: Primerjava prednosti in slabosti Interneta in omrežja ISO OSI X.400

Internet	ISO OSI X.400
+ poceni	- precej drag
+ široka razširjenost uporabe	- ni tako razširjen
+ poceni programska oprema	- draga programska oprema
+ hitrost	- precej počasen
+ ne zahteva predhodnih povezav	- zahteva predhodne povezave
+ malo standardov	- veliko standardov
- ni varnosti	+ relativna varnost
- ni sledljivosti	+ sledljivost je možna

Vir: Škedelj, 1999, str. 36.

Internet je globalno omrežje, na katerega je priključeno na stotine milijonov uporabnikov. Z razvojem Interneta, kot omrežja za prenos računalniških podatkov, se je pojavila tudi potreba po razvoju oziroma uvedbi standarda, ki bi deloval bolje kot standard EDIFACT. Tu pa se kot možnost pojavlja nov jezik XML. Jezik XML omogoča, da se RIP sporočila prenašajo zelo enostavno in poceni preko Interneta, direktno v programsko rešitev poslovnega partnerja.

4. XML – Razširljivi označevalni jezik

Jezik XML (eXtensible Markup Language) je preprosta tehnologija, ki je prevzela računalniški svet kot nevihta. Še preden je bil XML uradno specificiran, je predsednik družbe Microsoft, Bill Gates dejal, da je XML prelomna tehnologija, saj je v njem videl

prednosti, ki jih prinaša odprta ter od platforme neodvisna tehnologija kot je XML (Travis, 2000).

Jezik XML je izpeljanka jezika SGML (Standard Generalized Markup Language), ki se uporablja za označevanje in kreiranje vseh vrst dokumentacij. Iz jezika SGML so izpeljani tudi drugi jeziki kot: CML[16], VML[17], MathML[18] in še vrsta sorodnih jezikov (Mohorič, 2001, str. 55).

Jezik XML je nastal kot posledica slabosti in pomanjkljivosti svojih dveh predhodnikov:
- jezika SGML
- jezika HTML[19]

Glavne pomanjkljivosti obeh predhodnikov so bile, da je jezik SGML preveč kompleksen za vsakodnevno rabo v svetovnem spletu, medtem ko je jezik HTML sicer enostaven za uporabo, vendar ima dve glavni pomanjkljivosti:
- Podatki niso ločeni od oznak in drugih informacij za njihovo predstavitev,
- Jezik ni razširljiv, saj je slovar omejen na nabor oznak, ki jih določa specifikacija.

Druge prednosti XML pred SGML, pa so med drugim tudi (Pardi, 1999):
- Jezik XML je optimiziran za uporabo na svetovnem spletu.
- XML je manj obsežen jezik kot SGML: razvijalci jezika XML so poizkušali izločiti iz XML vse ukaze, ki niso potrebni za delo s svetovnim spletom, prednost je v preprostejši uporabi jezika XML.
- Specifikacija XML vsebuje tudi dodatne funkcije, kot na primer XLL[20] in XSL[21].

Zato se je oblikovala posebna skupina znotraj konzorcija W3C (World Wide Web Consortium), katera je leta 1995 predlagala razvoj jezika, ki bi bil tako enostaven za uporabo kot jezik HTML, obenem pa tako močan in razširljiv kot jezik SGML. Ta posebna skupina se je imenovala »delovna skupina za razvoj specifikacije XML«. Prvi osnutek je bil objavljen leta 1996, verzija 1.0 pa februarja leta 1998. Standard so podprla

[16] CML – angl. Chemical Markup Language
[17] VML – angl. Vector Markup Language
[18] MathML – angl. Mathematical Markup Language
[19] HTML – angl. Hiper Text Markup Language
[20] XLL – angl. Extensible Linking Language
[21] XSL – angl. Extensible Stylesheet Language

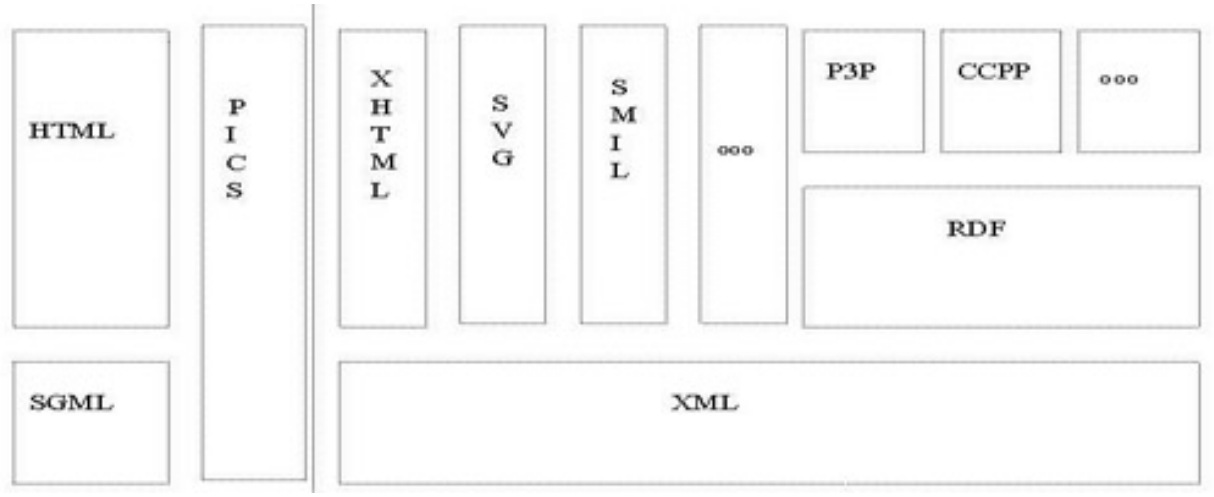
tudi vsa svetovno najbolj znana podjetja s področja informacijske tehnologije, kot so Microsoft, IBM, Oracle, Sun, SAP… (Dečman, 2000, str. 52).

W3C konzorcij je bil ustanovljen leta 1994 z namenom, da pomaga pripeljati svetovni splet na višjo raven uporabe, z razvijanjem splošnih protokolov, kateri naj bi omogočili njegovo evolucijo ter uporabnost. W3C ima več kot 500 članov iz celega sveta in je svetovno priznana organizacija, ki pomaga pri rasti svetovnega spleta. Osnovni cilji W3C konzorcija so:

- dostopnost do svetovnega spleta po celem svetu,
- uporabnost svetovnega spleta,
- zaupanje v svetovni splet.

Konzorcij W3C je izdal več kot 20 priporočil, katera se nadgrajujejo ter tako omogočajo tudi nadaljnji razvoj nekih standardov. Nekatere pomembnejše prikazuje tudi slika 3.

Slika 3: Izdana priporočila W3C konzorcija do danes



Vir: W3C konzorcij, 2001.

V prihodnosti W3C pripravlja predvsem naslednje specifikacije, ki naj bi spremenile svetovni splet:

- Možnost dostopa do svetovnega spleta preko mnogih drugih naprav, kot na primer televizija, mobilni telefoni, itd…
- Promocija najboljše prakse – W3C ne more obstajati sama zase, zato mora razvijalce prepričati o uporabnosti svojih specifikacij.

- Koordinacija z upravnimi telesi – zagotoviti je potrebno, da bo svetovni splet zakonit.
- Upoštevanje kulturnih razlik – potrebno je upoštevati kulturne in jezikovne razlike, če želimo, da bo čim več ljudi uporabljalo svetovni splet.
- Spodbujanje razvoja – če želimo, da se bo svetovni splet razvijal, je potrebno spodbujati razvoj ter nove raziskave na vseh področjih človekovega delovanja.

4.1. Osnovne tehnične značilnosti jezika XML

XML je programski jezik za opisovanje strukture in pomena podatkov. XML ne opisuje, kako naj se podatki prikazujejo na spletni strani, vendar je možno način izpisa definirati posebej s pomočjo ene od njegovih razširitev. To pomeni, da so v XML-u podatki ločeni od svoje predstavitve. V bistvu je XML zbirka pravil za definiranje pomenskih oznak (zaznamkov, angl. tag). Za razliko od HTML jezika, XML ne vsebuje vnaprej definirane množice oznak, ampak omogoča določanje lastnih oznak, ki morajo biti v dokumentu urejene glede na ustrezna pravila (Zupan, 2000).

Kot primer lahko predstavim enostaven primer zapisa dokumenta v HTML-ju ter enak primer dokumenta v jeziku XML, kot je prikazano na slikah 4 in 5.

Slika 4: Primer dokumenta v jeziku HTML

```
<HTML>
<BODY>
<TABLE>
<TR>
<TD> Osnove zaznamkovnih jezikov</TD>
<TD>AAA</TD>
<TD>Jože</TD>
<TD>Matej<BR>Ana<BR>Miha</TD>
</TR>
</TABLE>
</BODY>
</HTML>
```

V zgornjem primeru ne moremo točno razbrati iz zaznamkov ali gre za naslov knjige ali pa za seminar na fakulteti. Zaznamki in podatki nam tega ne povedo, toliko težje pa to ugotovi računalniški program. Iz zaznamkov lahko razberemo samo, da bodo podatki zapisani v eni vrstici in štirih celicah.

Dokument v jeziku XML, podatki so ekvivalentni prejšnjim, le zaznamki vsebujejo informacijo o tem, kaj podatki predstavljajo, primer je na sliki 5.

Slika 5: Primer dokumenta v jeziku XML

```
<?xml version="1.0">
<seminar>
<ime>osnove zaznamkovnih jezikov</ime>
<kratica>AAA</kratica>
<predavatelj>
<ime>Jože</ime>
</predavatelj>
<študenti>
<ime>Matej</ime>
<ime>Ana</ime>
<ime>Miha</ime>
</študenti>
</seminar>
```

Kot vidimo, je v drugem primeru bolj jasno, da gre za seminar s podatki o imenu predavatelja ter imena študentov, kateri se bodo udeležili seminarja. Vendar pa v tem primeru ne vemo nič o tem, kako bodo podatki prikazani.

Torej lahko vidimo, da XML in HTML opravljata vsak svojo nalogo: XML predstavlja informacije o vsebini, HTML pa način prikaza oziroma predstavitev vsebine.

Problem HTML-ja je v tem, da ni namenjen za hranjenje podatkov (Sturm, 2000). Tako moramo stalno popravljati HTML kodo, namesto da bi samo popravljali spremenjene podatke. V bistvu bi potrebovali tak jezik, ki bi znal ločiti podatke od predstavitve le teh. Prav ta problem, ki se pojavlja z uporabo jezika HTML, pa je v veliki meri privedel do tega, da prihaja jezik XML vedno bolj v ospredje, kot jezik za prenos podatkov preko omrežja.

4.1.1. Oznake XML

XML dokumenti so namenjeni shranjevanju podatkov. V tem smislu so podobni tabelam v relacijski bazi podatkov ali objektom v objektnih bazah podatkov. XML je samoopisni jezik, ki z uporabo oznak pojasnjuje pomen podatkov v dokumentu. Oznake so lahko poljubne, vendar je smiselno, da odražajo tudi pomen podatka, zato je razumljiv, tako človeku kot tudi računalniku oziroma programu.

Vrednost podatka, ki ga želimo zapisati v dokument se nahaja med dvema oznakama, to sta začetna in končna oznaka. Par oznak, med katerimi se nahaja vrednost imenujemo element (Mohorič, Krisper, 2001, str. 56).

Primer:

```
<Ime>Mitja</Ime>
<Priimek>Makovec</Priimek>
```

V zgornjem primeru predstavljata `<Ime>` in `</Ime>` začetno in končno oznako, Peter pa je vrednost elementa. XML pa razlikuje tudi med velikimi in malimi črkami, zato je potrebno biti pazljiv pri opredeljevanju oznak, saj `<Ime>` ni enako `<IME>`, zato morata biti začetna in končna oznaka zapisani na enak način.

4.1.2. Oblikovanje dokumentov XML

Podatki so lahko zapisani v XML-u na veliko različnih načinov. Nekateri načini so bolj pravilni nekateri manj. Čeprav XML dopušča definiranje lastnih oznak, pa mora dokument, ki jih uporablja, zadoščati nekaterim pravilom. Če dokument zadošča pravilom, lahko zanj rečemo da je dobro oblikovan (angl. well formed). Tako oblikovane dokumente lahko potem obdelujejo avtomatski razčlenjevalniki in berejo ter prikazujejo spletni brskalniki.

Dokument sodi med dobro oblikovane dokumente, če v njem ni sintaktičnih napak. Glavna pravila, katerim mora zadoščati dobro oblikovan dokument XML so (Harold, 1999, str. 143):

- *Dokument se mora pričeti z deklaracijo XML*
  Dokument se prične z deklaracijo XML, ki obsega verzijo dokumenta XML, podatek ali je dokument samostojen ali ne, ter način kodiranja:
  Primer: `<?xml version="1.0" encoding="UTF-8" standalone="yes"?>`
  Določili standalone in encoding sta praviloma opcijski, vendar ju je v nekaterih primerih potrebno uporabiti.
- *Elementu, ki vsebuje podatke, morata pripadati začetna in končna oznaka*
  Primer: `<Ime>Mitja</Ime>`
- *Elementi, ki ne vsebujejo podatkov pač pa le atribute, se morajo zaključiti z znakom /*
  Primer: `<naziv/>`
- *Dokument mora obsegati natanko en element, ki vsebuje vse ostale elemente*

Tak element imenujemo korenski element. Primer korenskega elementa `<pozdrav>` prikazuje slika 6.

Slika 6: Primer korenskega elementa `<pozdrav>`

```
<?xml version="1.0" standalone="yes"?>
<pozdrav>
Lep pozdrav XML!
</pozdrav>
```

- *Elemente lahko gnezdimo, vendar se ne smejo prekrivati*
  Elementi običajno vsebujejo druge elemente, kar pomeni, da morajo vsebovati, tako začetno kot tudi končno oznako gnezdenega elementa.
- *Vrednost atributa se mora nahajati v dvojnih narekovajih*
- *Znaka < in & se lahko uporabljata samo za začetek oznake oziroma reference na posebne znake*
- *Edine reference na posebne znake so: &, <, >, " in '*

Tabela 2: Znakovne entitete in njihov pomen

Entiteta	Simbol	Pomen
>	>	večji
<	<	Manjši
&	&	Konjukcija
'	'	Apostrof
"	"	dvojni narekovaj

Vir: Mohorič, Krisper, 2001, str. 56.

Ker imata začetna in končna oznaka < …> svoj rezervirani pomen, ki se uporablja pri zapisovanju oznak, je potrebno v primeru uporabe simbolov "večji" in "manjši" znotraj oznake nadomestiti z entiteto ">" ter "<". Podobna pravila veljajo tudi za druge posebne simbole predstavljene v tabeli 2 (Mohorič, Krisper, 2001, str. 56).

4.1.3. Veljavnost dokumentov XML

Dokument zapisan v jeziku XML je veljaven, če je dobro oblikovan dokument XML, ter če njegovi elementi ustrezajo določenim zahtevam glede strukture. V dokument se lahko zapisujejo le tisti podatki, ki so v skladu s shemo dokumentov. Dokumenti, ki so v skladu s shemo, so veljavni dokumenti.

Poznamo dve vrsti shem:

- DTD – definicija tipa dokumenta
- XML shema

4.1.3.1. DTD – definicija tipa dokumenta

Definicija tipa dokumentov opredeljuje seznam elementov, atributov, zaznamkov ter entitet, ki so v dokumentu, kot tudi relacije med njimi. DTD opredeljuje pravila za strukturo dokumenta. Z uporabo DTD, podatki v XML-u s seboj nosijo tudi informacijo o svoji strukturi. DTD lahko definiramo znotraj dokumenta XML ali pa se DTD nahaja v posebni datoteki in je vključen v dokument s pomočjo reference (Harold, 1999, str. 191).

Znotraj dokumenta XML definiramo DTD z naslednjo sintakso:

```
<!DOCTYPE korenski_element [deklaracije_elementov]>
```

Če pa se sklicujemo na DTD v drugem dokumentu, pa uporabimo:

```
<!DOCTYPE korenski_element SYSTEM "ime_datoteke">
```

Z vidika DTD je dokument XML sestavljen iz naslednjih tipov:

- elementi
- oznake
- atributi
- osebki
- znakovni podatki, ki se procesirajo (PCDATA)
- znakovni podatki, ki se ne procesirajo (CDATA)

Elemente definiramo na naslednji način:

```
<!ELEMENT ime_elementa kategorija>
<!ELEMENT ime_elementa (vsebina_elementa)>
```

Tabela 3: Primeri definicij elementov v DTD

<!ELEMENT ime_elementa EMPTY>	Prazen element
<!ELEMENT ime_elementa (#PCDATA)>	Element, ki vsebuje samo znakovne podatke
<!ELEMENT ime_elementa ANY>	Element, ki vsebuje poljubne podatke
<!ELEMENT ime_elementa (ime_sina1,ime_sina2, …)>	Element z enim ali več sinov
<!ELEMENT ime_elementa (ime_sina)>	Element vsebuje natanko eno pojavitev elementa sin
<!ELEMENT ime_elementa (ime_sina+)>	Element vsebuje eno ali več pojavitev elementa sin
<!ELEMENT ime_elementa (ime_sina*)>	Element vsebuje nič ali več pojavitev elementa sin
<!ELEMENT ime_elementa (ime_sina?)>	Element vsebuje nič ali eno pojavitev elementa sin
<!ELEMENT ime_elementa (ime_sina1, ime_sina2|ime_sina3, …)>	Element vsebuje natanko eno pojavitev prvega sina in pojavitev drugega ali tretjega sina

Vir: Jamnik, 2001, str. 8.

Zaporedje sinov, kot je definirano v DTD, določa zaporedje elementov v dokumentu XML. Atributi v DTD-ju so definirani:

```
<!ATTLIST ime_elementa ime_atributa tip_atributa privzeta_vrednost>
```

Tip atributa in privzeta vrednost lahko zavzameta eno od vrednosti, ki so podane v tabeli 4 ter 5.

Tabela 4: Vrednosti za tip atributa v DTD

CDATA	Vrednost je znakovni podatek
(vrednost1|vrednost2|…)	Vrednost lahko zavzame eno od naštetih možnosti
ID	Vrednost je unikatni identifikator
IDREF/IDREFS	Vrednost je identifikator drugega elementa oziroma seznam identifikatorjev drugih elementov
NMTOKEN/NMTOKENS	Vrednost je veljavno ime oziroma seznam veljavnih imen v XML
ENTITY/ENTITIES	Vrednost je osebek oziroma seznam osebkov
NOTATION	Vrednost je ime notacije
xml:	Vrednost je predefinirana vrednost XML

Vir: Pardi, 1999.

Tabela 5: Privzete vrednosti za atribute v DTD

#DEFAULT vrednost	Določena privzeta vrednost
#REQUIRED	Vrednost atributa je obvezna v elementu
#IMPLIED	Vrednost atributa v elementu ni obvezna
#FIXED Vrednost	Vrednost atributa je določena in nespremenljiva

Vir: Pardi, 1999.

Naslednji sestavni del DTD je osebek. Osebke definiramo z:

```
<!ENTITY ime_osebka "vrednost osebka">
```

oziroma

```
<!ENTITY ime_osebka SYSTEM "ime_datoteke">
```

Slabost uporabe DTD-ja je, da ne uporablja sintakse XML, zato so DTD-ji zapleteni in nepregledni ter omejeni na definirane elemente in pravila. Prav tako ni možno uporabljati rezčlenjevalnikov za avtomatsko obdelavo metapodatkov v DTD-ju in dinamično oblikovanje DTD-jev. Slabost DTD-ja je tudi v tem, da ne podpira imenskih prostorov, podatkovnih tipov in dedovanja. Večino teh težav rešuje novi standard – Shema XML, ki naj bi sčasoma nadomestil DTD.

4.1.3.2. Shema XML

Shema XML igra podobno vlogo kot DTD, uporablja se za opisovanje strukture podatkov. Shema XML uporablja sintakso XML in je zato preglednejša ter lažje berljiva, poleg tega, pa podpira več možnosti pri opredeljevanju strukture podatkov.

Ena od bistvenih prednosti sheme XML-a pred DTD-jem so podatkovni tipi, kar omogoča preverjanje vrednosti v elementih dokumenta XML in ustrezno konverzijo besedila v podatkovni tip znotraj programskega jezika, v katerem je napisan prevajalnik za XML.

4.1.4. Imenski prostor XML

Imenski prostor (XML Namespace) je zbirka imen tipov elementov in imen atributov. Namen imenskih prostorov je razreševanje problemov poimenovanja v dokumentih XML-a. Namreč imena oznak v XML-u niso v naprej definirana, zato lahko pride do konfliktov v poimenovanju posameznih elementov ali atributov, saj se v dveh različnih dokumentih lahko pojavijo oznake z enakim imenom, ki opisujejo različne elemente oziroma atribute.

Slika 7: Konflikt v poimenovanju elementov XML

Primer 1:

```
<?xml version="1.0">
<naslov>
<ulica>Dunajska 232</ulica>
<mesto>Ljubljana</mesto>
<posta>SI-1000</posta>
</naslov>
```

Primer 2:

```
<?xml version="1.0">
<streznik>
<ime>PC02</ime>
<naslov>300.00.00.23</naslov>
</streznik>
```

Pri obeh primerih na sliki 7 nastopa oznaka `<naslov>`, kot ime tipa elementa, vendar je pomen omenjenih oznak različen. Imenski prostor je potrebno identificirati s pomočjo identifikatorja URI[22]. Vsak tip elementa ali ime atributa, pa se v prostoru XML enolično identificira z dvodelnim imenom, s pomočjo URI in svojega lokalnega imena. Imenski prostori se potem deklarirajo z atributom xmlns, ki poveže poljuben prefiks z določenim imenskim prostorom (Mohorič, Krisper, 2001, str. 59).

```
<ime_elementa xmlns:predpona="imenski prostor">
```

Primera iz slike 7 lahko tako združimo v enega s pomočjo URI. Tako dobimo en dokument, v katerem je lepo ločen naslov podjetja `<nsl:naslov>` in naslov strežnika `<str:streznik>`.

Slika 8: Sestavljen dokument s pomočjo URI

```
<?xml version="1.0"?>
<podjetje>
<ime>PC</ime>
<nsl:naslov xmlns: nsl="http://www.podjetje.si">
<nsl:ulica>Dunajska 232</nsl:ulica>
<nsl:mesto>Ljubljana</nsl:mesto>
<nsl:pst>SI-1000</nsl:pst>
</nsl:naslov>
<str:streznik xmlns: str="http://www.podjetje.si/streznik">
<str:ime>PC02</str:ime>
<str:naslov>300.00.00.23</str:naslov>
</str:streznik>
</podjetje>
```

Na ta način se lahko izognemo nepregledni uporabi predpon, vendar pa lahko tak način uporabimo samo takrat, ko je možno posamezne dele dokumenta ločiti med seboj glede na imenski prostor.

[22] URI – angl. Universal Resource Identifier

4.2. Cilji jezika XML

Specifikacija jezika XML predpostavlja naslednje cilje za jezik XML (W3C, 2000, Walsh, 1998, Sturm, 2000.):

- *XML naj bi bil enostaven za uporabo preko Interneta:* Uporabnikom je potrebno omogočiti preprosto in hitro pregledovanje XML dokumentov, enako kot HTML dokumentov. V praksi bo to mogoče, ko bodo XML spletni brskalniki tako robustni in razširjeni kot HTML spletni brskalniki. Trenutno XML podpirajo naslednji spletni brskalniki: MS Internet Explorer, Netscape Navigator, Opera, Mozilla, itd…
- *XML naj bi podpiral široko uporabo dodatnih programskih rešitev:* XML naj bi podpiral široko paleto dodatnih programskih rešitev, čeprav je njegova začetna usmerjenost v izmenjavi strukturiranih dokumentov preko svetovnega spleta.
- *XML naj bi bil kompatibilen s SGML:* Veliko SGML programov ter SGML standardiziranih formatov že obstaja, zato je pomembno, da je XML kompatibilen s SGML, tako da lahko že narejene SGML programe še enkrat uporabimo z XML.
- *Pisanje programov, ki znajo procesirati XML dokumente, naj bi bilo preprosto:* Da bi jezik XML postal uporabljan po celem svetu, je pomembno, da je pisanje programov, kateri znajo procesirati XML dokumente enostavno. Tako bo uporaba XML-a tudi stroškovno smiselna.
- *Število pomožnih dodatkov v XML-u naj bi bilo kar najmanjše, v idealnem primeru nič:* Več kot je (opcijskih) pomožnih dodatkov, težja bo uporaba XML-a. Bolj kot je jezik kompliciran, večji bodo stroški z njegovim razvojem in manjša je verjetnost, da se bo kdorkoli (naključni uporabnik) odločil za uporabo. Standard XML je ta cilj izpolnil.
- *XML dokumenti naj bi bili čitljivi in pregledni:* Pomeni, da naj bi vsakdo z vsaj minimalnim znanjem XML-a znal razbrati dokument napisan v XML-u v kateremkoli tekstovnem urejevalniku (npr. MS Word).
- *Načrt XML-a naj bi se pripravil hitro:* Bistveno je namreč, da je standard hitro dokončan, tako da se lahko uporablja za reševanje tekočih problemov.
- *Načrt XML-a naj bo jedrnat in formalen:* Bistvenega pomena je, da so programske rešitve sposobne brati in razčleniti XML. Jezik, ki je oblikoven in zgoščen, bo računalniški program z lahkoto prevedel. XML je lahko izražen v obliki EBNF, kar je zapis, ki opisuje sintakso jezika. Računalniški program z lahkoto razčleni EBNF. V nasprotju z XML, SGML-a ni možno izraziti v EBNF.
- *XML dokumenti naj bi bili preprosti za izdelavo:* Dandanes je že nekaj XML urejevalnikov, ki omogočajo preprosto izdelavo XML dokumentov. Kot primer lahko

navedem XML Pro[23] in XML Spy[24], ki nam omogočata izdelavo in urejanje XML dokumentov s pomočjo menijev. Še veliko drugih programov za izdelavo in urejanje XML lahko najdemo na spletni strani XMLSoftware.[25]

- *Okrajšave v jeziku XML so minimalnega pomena:* SGML je imel veliko dodatkov v jeziku, ki so bili narejeni z namenom minimizacije velikosti ukazov. S tem se je kompleksnost jezika SGML zelo povečala. Zato je pomembno, da v specifikaciji jezika XML ni veliko okrajšav, saj se le-te lahko dodajo kot bližnjice v XML urejevalnikih.
- *Preciznost izboljšave XML-a je minimalnega pomena:* Narediti izboljšavo XML-a zgoščeno, je manj pomembno od zgoščenosti samega XML-a. Lahko bi vključili celo zbirko sprejemljivih bližnjic v standard (kot na primer SGML) in se izognili njihovi vključitvi v izboljšavo, s tem pa bi naredili XML mnogo bolj zapleten.

Specifikacije, ki jih je podal konzorcij W3C, težijo k temu, da naj bi bil jezik XML čim bolje definiran ter čimbolj preprost za uporabo, tako za strokovnjake kot tudi za druge uporabnike. Samo tako, bo le-ta jezik zaživel ter postal uporabljan v večjem številu. V nadaljevanju bom predstavil še prednosti, ki jih ima jezik XML.

4.3. Prednosti in pomen XML-a

Bistvene prednosti in pomen predstavitve podatkov v jeziku XML (Sturm, 2000.):

- *Razširljivost:* Lahko definiramo nove slovarje glede na potrebe konkretnih programov, gospodarske panoge ali načina komunikacije med poslovnimi partnerji.
- *Ločitev podatkov od njihove predstavitve:* Prednost se pokaže v neodvisnem spreminjanju predstavitve podatkov, ter v predstavitvi istih podatkov na več načinov.
- *Enostavna uporaba:* XML je samo malo bolj zahteven kot HTML. Vedno več je programov ter urejevalnikov, ki podpirajo XML, tako da je verjetno, da ga bo uporabljalo vedno več ljudi.
- *Neodvisnost podatkov:* Predstavitev v XML-u je neodvisna od programske in strojne opreme ter neobčutljiva za njihove nadgradnje.
- *Večja uporabnost podatkov:* Podatke v XML-u lahko uporabi katera koli programska rešitev, ki podpira jezik XML.

[23] XML Pro – http://www.vervet.com

[24] XML Spy – http://xmlspy.com

[25] XMLSoftware – http://www.xmlsoftware.com

- *Internacionalizacija XML-a:* XML bazira na Unicode[26] sistemu. Le-ta omogoča uporabo več znakov, kar pomeni, da lahko v XML-u uporabimo tudi druge tuje slovnice. SGML in HTML uporabljata ASCII[27] standard, kar predstavlja problem s tujimi slovnicami.
- *Podpora razvoju:* Dobra podpora razvijalcem ter veliko dostopnega gradiva za izobraževanje, predvsem na svetovnem spletu.

5. XML in varnost

Če želimo, da jezik XML postane standard za prenos podatkov preko svetovnega spleta, je zelo pomembno, da omogoča varne prenose podatkov. Namreč podjetja potrebujejo varne prenose, saj preko omrežja prenašajo dokumente, ki imajo določeno vrednost, zato ne želijo, da jih vidi nekdo, ki nima te pravice.

Elektronsko poslovanje se razlikuje od klasičnega poslovanja med drugim tudi po tem, da partnerja nimata direktnega kontakta med seboj. Pri klasičnem poslovanju, kot na primer pri izmenjavi pisnih dokumentov, partner lahko razbere naš podpis oziroma žig podjetja, ter tako ve, da smo to pismo poslali prav mi; pri elektronskem sporočilu pa ne more biti popolnoma prepričan, da smo to sporočilo poslali prav mi, ali pa da ga ni kdo med potjo prestregel ali ga celo spremenil.

Zato je potrebno sporočila, ki potujejo preko omrežja tudi primerno zaščititi. Zaščito elektronskih sporočil delimo na osnovno in razširjeno (Škedelj, 1999, str. 38). Osnovna zaščita se nanaša na samo sporočilo in je neodvisna od načina oddaje sporočila, prenosa in dostave. Sestavljena je iz:

- **Overovljenja izvora (angl. Mesage origin authentication):** zagotavlja naslovniku, da je sporočilo prišlo res od tistega avtorja, kateri je na sporočilu podpisan.
- **Neokrnjenosti vsebine (angl. Content integrity):** prepreči spreminjanje vsebine sporočila na poti med pošiljateljem in prejemnikom.
- **Zaupnosti vsebine (angl. Content confidentiality):** zavaruje vsebino sporočila pred prisluškovanjem tretje osebe na poti.
- **Nezavračanja izvora sporočila (angl. Non-repudiation of orgin):** avtorju sporočila je onemogočeno zavračanje avtorstva nekega sporočila.

[26] Unicode – 16-bitna koda, definirana s strani Unicode konzorcija

[27] ASCII – angl. American standard code for information interchange

Razširjena zaščita pa vsebuje še:

- **Dokazila o dostavi (angl. Proof of delivery):** zagotavlja prejemniku, da je bilo sporočilo oddano prejemniku brez spreminjanja na svoji poti.
- **Dokazila o predložitvi (angl. Proof of submission):** zagotavlja pošiljatelju, da je njegov lokalni MTA[28] prejel njegovo sporočilo ter ga poslal dalje.
- **Nezavračanje prejema sporočila (angl. Non-repudiation of delivery):** omogoča, da prejemnik ne more tajiti prejema sporočila.
- **Nezavračanje predložitve sporočila (angl. Non-repudiation of submission):** zagotavlja pošiljatelju, da je MTA prejel pošiljateljevo sporočilo v neokrnjeni obliki ter ga poslal dalje prejemniku.

Za zagotovitev varnosti imamo na voljo več možnih metod. Izbira metod je odvisna od zahtevanih varnostnih storitev, stopnje zaščite in oblike sistema. Varnost lokalnih sistemov lahko dosežemo že s fizičnim varovanjem. Vendar pa elektronsko poslovanje poteka prek meja organizacij, zato so za zaščito primernejši kriptografski mehanizmi (Jerman - Blažič, 2001, str. 101).

5.1. Varnost pri prenosu podatkov po svetovnem spletu

Svetovni splet je pomemben dejavnik pri elektronskem prenosu podatkov med subjekti, saj ima veliko prednosti pred drugimi omrežji, kot na primer X.400. (glej Tabela 1, str. 13). Vendar pa se pri prenosu pojavlja vprašanje varnosti podatkov, in ker je svetovni splet dostopen vsakomur, nudi tudi veliko možnosti zlorabe.

Skrb za varnost v svetovnem spletu delimo na dve osnovni kategoriji (Škedelj, 1999, str. 49):

- Prva se nanaša na nevarnost vdora v strežnik na svetovnem spletu, kjer lahko nepoklicana oseba pridobi dostop do informacij ali pa na strežniku izvaja škodljivo programsko opremo.
- Druga kategorija pa se nanaša na možnosti zlorabe uporabnikovih telekomunikacij, kot je na primer prisluškovanje prometu na mreži ali pa ponarejeni spletni strežniki, ki pretentajo uporabnike.

Ker se tudi v primeru prenosa dokumentov XML uporablja svetovni splet kot nosilec prenosa podatkov, lahko za zaščito in vzpostavitev varnosti uporabimo tehnologije in

[28] MTA – angl. Message Transfer Agent

standarde, ki so že dalj časa uveljavljeni na Internetu. V raziskavi Evropske unije iz leta 1998 v zvezi z varnostno tehnologijo, so ugotovili, da v 40 odstotkih podjetij niso vedeli kakšno tehnologijo uporabljajo, 52 odstotkov je odgovorilo, da uporabljajo SSL, 16 odstotkov pa jih je uporabljalo tehnologije, ki temeljijo na metodi SET, navidezna zasebna omrežja pa je uporabljalo 6 odstotkov (Jerman - Blažič, 2001, str. 117). Bistvo teh postopkov je, da med strežnikom in odjemalcem vzpostavijo varen kanal, po katerem poteka komunikacija med njimi. Na ta način onemogočajo prisluškovanje, spreminjanje in ponarejanje sporočil ter zagotavljajo avtentičnost njihovega izvora (Jerman - Blažič, 2001, str. 119).

V nadaljevanju bom na kratko predstavil oba pomembnejša protokola za varen prenos podatkov SSL in SET.

5.1.1. SSL – Secure Socket Layer

SSL je prvi implementiral in razvil Netscape Communications Corporation.[29] Protokol SSL zagotavlja zaščito podatkov pri prenosu s šifriranjem in podpira uporabo številnih kriptografskih algoritmov. Avtentifikacijo uporabnikov ponuja na transportnem nivoju, kar pomeni, da je uporaben tudi v programskih rešitvah, kot na primer elektronska pošta, HTTP, FTP, TELNET.
SSL je sestavljen iz dveh protokolov (Jerman – Blažič, 2001, str. 119):

- SSL Record Protocol – definira osnovni format izmenjanih podatkov, zagotavlja neokrnjenost in šifriranje;
- SSL Handshake protocol – omogoča usklajevanje algoritmov, overjanje strežnika in odjemalca, prenos digitalnih certifikatov in določitev skupnega ključa za simetrični kripto algoritem.

Slabost SSL-a je, da ne omogoča selektivnega obravnavanja podatkov, ampak procesira vse podatke, kar lahko pomeni precejšnjo obremenitev in časovno zahtevnost sistema. Kot druge slabosti SSL-a pa se omenjajo še luknje v implementaciji, prešibki ključi v ameriških produktih zaradi ameriških izvoznih omejitev[30], občutek lažne varnosti ter lažno predstavljanje, lažna digitalna potrdila (certifikati) (SSL(Secure Socket Layer), 2000).

[29] Netscape Communications Corporation – http://www.netscape.com

[30] Zdaj so te omejitve delno odpravljene, vendar je dobro preveriti, kakšne ključe podpira softver, ki ga nameravamo uporabljati

5.1.2. SET – Secure Electronic Transfer

SET protokol za varno plačevanje z bančnimi karticami v svetovnem spletu sta razvili skupaj dve največji izdajateljici bančnih kartic na svetu – Visa in MasterCard, ob pomoči IBM. SET je bil razvit z namenom, da bi vsem udeležencem v elektronskem poslovanju zagotovil visok nivo varnosti ter preprečil zlorabe pri plačilnih transakcijah s plačilnimi karticami. SET protokol zagotavlja predvsem zaupnost, integriteto podatkov, overovljenje identitete ter nezavračanje elektronskega nakupa.

SET protokol se od SSL protokola razlikuje predvsem v tem, da SET zavaruje vsebino podatkov, ki potujejo med sprejemnikom in oddajnikom, SSL protokol pa deluje kot nekakšen motilnik signala na telefonski liniji, ki onemogoči prisluškovalcu prestreči vsebino pogovora (Škedelj, 1999, str. 56).

5.2. Šifriranje

Transformacijo podatkov v obliko, ki onemogoča njihovo razumevanje, in tako ohranja tajnost, imenujemo šifriranje, nasprotni proces pa dešifriranje. Šifriranje sporočila zagotavlja zaupnost vsebine sporočila, ter tako onemogoči tretji osebi vpogled v sporočilo. Vsebina sporočila je dostopna samo tistemu, ki pozna ključ, s katerim je bilo sporočilo zašifrirano (Škedelj, 1999, str. 39).

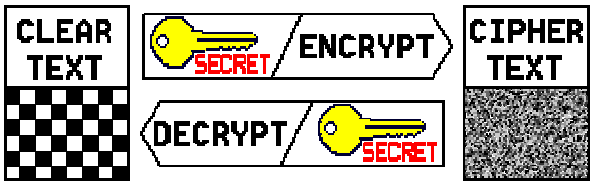
Poznamo dva sistema šifriranja:

- simetrično šifriranje in
- asimetrično šifriranje z javnim ključem

5.2.1. Simetrično šifriranje

Bistvo simetričnega šifriranja sporočil je v tem, da se uporablja isti tajni ključ, tako za šifriranje (angl. encryption) kot tudi za dešifriranje (angl. decryption).

Slika 9: Simetrično šifriranje



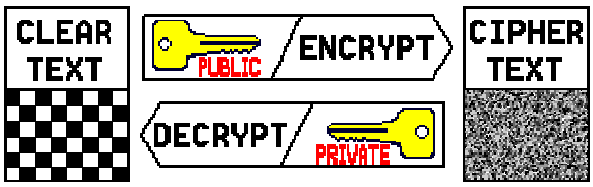
Vir: Bokler, 2001.

Problem simetričnega šifriranja je v tem, da mora vsak subjekt, ki želi dešifrirati sporočilo, imeti ta ključ, s katerim smo šifrirali sporočilo. To pomeni, da je potrebno ključ dostaviti vsakemu, to pa lahko prinaša varnostni riziko, saj se ključ prenaša preko javnih omrežij. Druga težava simetričnega šifriranja pa je veliko število ključev, saj potrebujemo po en ključ za vsak subjekt, s katerim komuniciramo.

5.2.2. Asimetrično šifriranje z javnim ključem

Drugi pristop je asimetrično šifriranje, pri katerem sta ključa za šifriranje in dešifriranje različna. Ključ za šifriranje je javni ključ (angl. public key), vendar je ta uporaben samo za šifriranje ne pa tudi za dešifriranje. Za dešifriranje je potreben drug ključ, imenovan privatni ključ (angl. private key), s katerim pretvorimo šifrirano sporočilo nazaj v berljiv tekst.

Slika 10: Asimetrično šifriranje z javnim ključem



Vir: Bokler, 2001.

Vendar pa je problem asimetričnega šifriranja v hitrosti šifriranja in dešifriranja ter overjanje javnih ključev. Simetrično šifriranje je tudi do 1000 krat hitrejše kot asimetrično šifriranje (Škedelj, 1999, str. 40). Zato je glavna uporaba asimetričnega šifriranja pri uporabi elektronskega podpisa, varnega prenosa ključev in zagotovitvi verodostojnosti. Za samo šifriranje sporočila pa se še vedno uporablja simetrično šifriranje.

Tabela 6: Najpogostejši simetrični in asimetrični šifrirni sistemi

Asimetrični sistemi	Simetrični sistemi
RSA (Rivest – Shamir – Adleman)[31]	DES (Data Encryption Standard)
ECC	SkipJack
ElGamal	IDEA
Rabin	RC2, RC4, RC5

Vir: Škedelj, 1999, str. 40.

V svetu deluje že precej organizacij, ki podeljujejo digitalna potrdila posameznikom in organizacijam z vsega sveta. Najbolj znana je Verisign[32], ki po nakupu druge največje take organizacije Thawte[33] obvladuje večino tega trga. Nastajajo pa tudi overitelji javnih ključev za neko omejeno področje – za državo, bančno združenje, zavarovalnice ipd. V Evropi že več let poteka projekt ICE-CAR[34] v katerem iz Slovenije sodeluje Laboratorij za odprte sisteme in mreže kot overitelj SI-CA.[35] SI-CA izdaja digitalna potrdila oziroma javne ključe predvsem agencijam za certificiranje javnih ključev (CA). SIGEN-CA[36] pa je eden od ponudnikov javnih certifikatov, kateri potem ponujajo le-te tudi fizičnim osebam (Certifikati javnih ključev, 2000). Certifikat, ki ga izda CA, je digitalni dokument, ki povezuje pravno ali fizično osebo z njenim javnim ključem. Le-ta se uporablja pri preverjanju javnih ključev. Certifikati otežujejo, da bi nekdo uporabil lažni ključ in se predstavljal kot nekdo drug.

Digitalni certifikat mora vsebovati: oznako različice formata, serijsko številko, identifikator podpisnega algoritma, naziv izdajatelja certifikata, rok veljavnosti, naziv lastnika certifikata, lastnikov javni ter digitalni podpis vseh polj. (Glej slika 11).

[31] RSA – RSA Security Inc. (http://www.rsa.com)

[32] Verisign – http://www.verisign.com

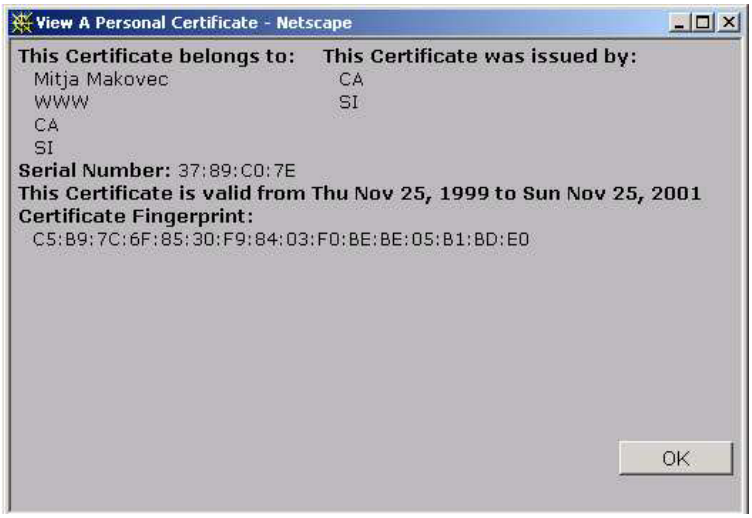
[33] Thawte – http://www.thawte.com

[34] ICE-CAR - http://ice-car.darmstadt.gmd.de/ICE-CAR-ProjectProgram.html

[35] SI-CA - http://www.e5.ijs.si/cert/sica.html

[36] SIGEN-CA - http://www.sigen-ca.si

Slika 11: Izgled uporabniškega certifikata v brskalniku Netscape Navigator



Spletna digitalna potrdila so uporabna predvsem za (SIGEN-CA, 2001):

- varno spletno komuniciranje po protokolih SSL (angl.Secure Sockets Layer) in TLS (angl. Transport Layer Security),
- varno pošiljanje elektronske pošte po protokolu S/MIME (angl. Secure Multipurpose Internet Mail Extensions),
- storitve oziroma aplikacije, za katere se zahteva uporaba spletnih kvalificiranih digitalnih potrdil overitelja na CVI[37].

Tudi za zaščito dokumentov XML lahko uporabljamo standardne metode šifriranja dokumentov, ki jih ponuja metoda javnih in zasebnih ključev, poleg tega pa obstajata pri konzorciju za svetovni splet (W3C) še dva standarda, ki naj bi poenostavila uporabo digitalnih podpisov in šifriranje podatkov v XML-u. To sta podpis XML[38] in šifriranje XML[39].

5.3. Podpis XML

Podpis XML je digitalni podpis, namenjen za uporabo v XML transakcijah. Podpis XML razvijata v sodelovanju W3C konzorcij in IETF.[40] Podpise XML lahko uporabljamo, tako na XML dokumentih kot tudi na poljubni drugi digitalni vsebini oziroma dokumentu.

[37] CVI – Center vlade za informatiko RS - http://www.gov.si/cvi/index_CVI.htm

[38] Podpis XML – angl. XML Signature

[39] Šifriranje XML – angl. XML Encryption

[40] IETF – angl. Internet Engineering Task Force

Bistvena lastnost podpisa XML je možnost, da z njim podpišemo samo del dokumenta ali pa cel dokument. Ta značilnost je uporabna predvsem takrat, ko imamo star dokument, ki je bil večkrat popravljen, tako da lahko vsak podpiše samo del, ki se nanaša nanj. Kot primer uporabe lahko navedem dokument, ki je poslan drugemu uporabniku, da ga dopolni s svojimi podatki. Ker je dokument samo delno podpisan in ne v celoti, lahko v trenutku ugotovimo, če je uporabnik spreminjal začetne vrednosti ali ne. Podpis XML je lahko v obliki ovojnice na podatkih znotraj istega dokumenta XML, lahko pa je podpis ločen od vsebine, ki ji pripada (Simon, 2001).

5.3.1. Zgradba podpisa XML

Podpis XML je zgrajen iz naslednjih atributov, katere prikazuje tudi slika 12.

Slika 12: Zgradba podpisa XML

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

Vir: Bartel, 2001.

Specifikacijo podpisa XML opredeljuje element `<Signature>`, ki vsebuje podatke digitalnega podpisa.

Podpis je povezan s podatki preko enoličnega identifikatorja vira URI, znotraj dokumenta XML pa preko spremenljivk, ki označujejo posamezne odstavke dokumenta. Podatki so lahko del podpisa, v tem primeru je podpis XML ovojnica oziroma oče v relaciji oče – sin, lahko pa podatki obdajajo podpis (v tem primeru je podpis XML sin) (XML-Signature Syntax and Processing, 2001). Naslednji element podpisa je `<SignedInfo>`, ki je obvezen element podpisa ter vsebuje podatke, ki jih podpisujemo in algoritme, ki jih uporabljamo za šifriranje in preverjanje podpisa. V elementu

<CanonicalizationMethod> je naveden algoritem, s katerim transformiramo podatke v tako imenovano kanonično obliko. Kanonična oblika je pomembna, saj morajo podatki ostati med postopkom podpisa nespremenjeni, zato mora biti predstavitev standardna (kanonična).

Element <SignatureMethod> uporabimo, da v njem napišemo algoritem, ki ga uporabimo, da lahko pretvorimo kanonično zapisane podatke v vrednost podpisa, ki jo zapišemo v element <SignatureValue>. Imena algoritmov so vsebovana v elementu <SignedInfo>. Podpisani podatki lahko vsebujejo enega ali več elementov <Reference>, v katerih zapišemo reference na podatke ali objekte, ki jih želimo podpisati. V elementu <DigestMethod> navedemo metodo za zgoščevanje, vrednost, ki jo pri tem zgoščevanju dobimo pa je zapisana v elementu <DigestValue>.

Slika 13: Primer podpisa XML

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo Id="foobar">
<CanonicalizationMethod
  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
<Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
<Reference
  URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-example.xml">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0E~LE=</SignatureValue>
<KeyInfo>
<X509Data>
<X509SubjectName>CN=Ed Simon,O=XMLSec Inc.,ST=OTTAWA,C=CA</X509SubjectName>
<X509Certificate>
MIID5jCCA0+gA...lVN
</X509Certificate>
</X509Data>
</KeyInfo>

</Signature>
```

Vir: Simon, 2001.

Za preverjanje podpisa XML potrebujemo informacije v elementu <KeyInfo>, ki vsebuje certifikate, ključe in postopke za dogovor glede ključev. Element <KeyInfo> ni obvezen, saj so lahko ti podatki že znani v sami programski rešitvi oziroma, oseba, katera podpisuje dokument, ne želi razkriti teh podatkov vsem strankam, ki imajo dokument na voljo.

5.3.2. Potek digitalnega podpisovanja XML

Potek digitalnega podpisovanja dokumentov XML je sestavljen iz naslednjih korakov. Najprej je potrebno definirati, katere dele oziroma cele dokumente bomo podpisali. Nato programska rešitev, ki jo predpisuje specifikacija podpisa XML transformira podatke po definirani metodi, opisana je v <DigestMethod> ter izračuna zgoščeno vrednost, ki je zapisana v <DigestValue>. Zgradi referenčni element <Reference> z vsemi potrebnimi informacijami in vanj zapiše vrednost, ki jo vrne zgoščevalna funkcija. V naslednjem koraku programska rešitev kreira element informacij podpisa <SignedInfo>, izvede transformacijo v kanonično obliko ter izračuna vrednost digitalnega podpisa <SignatureValue> s pomočjo navedenega algoritma. V končnem koraku kreira element podpisa XML v celoti.

Preverjanje podpisa XML sestavljata preverjanje referenc oziroma zgoščenih vrednosti v njih ter preverjanje šifriranega podpisa. Programska rešitev najprej poišče element <SignedInfo>, ga transformira in obdela z navedeno zgoščevalno funkcijo, ki je zapisana v <SignatureMethod>, nato pa le-to primerja z vrednostjo, ki je zapisana v referenčnem elementu. Če sta vrednosti enaki, prva faza preverjanja uspe. Za preverjanje digitalnega podpisa, programska rešitev prebere element s podatki o ključih in certifikatih, ali pa dobi te podatke iz kakšnega drugega vira. S pomočjo teh podatkov in algoritma preveri podpis in s tem integriteto podpisanih podatkov.

5.4. Šifriranje XML

Specifikacijo za šifriranje XML razvija konzorcij W3C, ki je trenutno v fazi priprave. Namen šifriranja XML je posebej opredeliti šifriranje dokumentov XML, ki bo omogočilo šifriranje samo tistih delov dokumentov, za katere bo to potrebno. Na primer, da imamo dokument XML, ki vsebuje podatke o zaposlenih, njihovih delovnih mestih ter plačah. Nekdo ima lahko na primer omogočen dostop do podatkov o zaposlenih, vendar ne more videti velikosti plače zaposlenih. Programska rešitev za zajem podatkov pa mora "vedeti", kateri elementi znotraj šifrirnega dokumenta so tisti, ki jih lahko dešifrira in

pokaže uporabniku. Specifikacija za šifriranje XML predvideva tudi šifriranje drugih poljubnih dokumentov, kot na primer, slike, celotne dokumente XML, stilne predloge (CSS[41]), dokumenti za tiskanje, itd.

Programske rešitve pogosto uporabljajo šifriranje dokumentov XML v kombinaciji s podpisom XML. Podatke namreč lahko šifriramo in nato podpišemo in obratno (Jamnik, 2001, str. 61).

6. XML in elektronsko poslovanje

Glavni problem računalniške izmenjave podatkov je v tem, da sporočila, ki se izmenjujejo niso standardizirana. V preteklosti so podjetja reševala te probleme s pomočjo dogovorov o pravilih za izmenjavo podatkov. Tako je nastala tudi RIP (Dečman, 2001, str. 54).

Ko je konzorcij W3C sprejel predlog o jeziku XML, je bil to prvi korak k oblikovanju skupnega formata za elektronsko izmenjavo dokumentov. Tako kot je HTML univerzalen jezik za pripravo spletnih strani, bo postal XML univerzalen jezik za izmenjavo podatkov na področju elektronskega poslovanja.

6.1. Bistvo uporabe XML v elektronskem poslovanju

V preteklosti je veliko podjetij uporabljajo standarde RIP-a za elektronsko izmenjevanje dokumentov, zdaj pa jih mnogo prehaja v nov jezik in sicer v XML. Jezik XML ponuja mnogo prednosti pred standardi RIP-a, vendar pa vseeno ni za pričakovati popolnega prehoda vseh podjetij na uporabo jezika XML. XML je v mnogih stvareh podoben RIP-u, na primer, z XML-o lahko definiramo formate za izmenjavo dokumentov, ter tudi DTD, ki so v bistvu enaki kot UN/EDIFACT tipi sporočila, tako da je XML več kot primeren za elektronsko izmenjavo informacij.

Slabost RIP-a je v tem, da avtomatizira izmenjavo podatkov med različnimi programskimi rešitvami na podlagi določenih standardov. Tako mora vsako podjetje pred začetkom elektronskega poslovanja preoblikovati vse svoje dokumente v ustrezno standardno obliko. Šele takrat lahko začnejo teči procesi tekoče in avtomatizirano. Za to pa je potrebna velika tehnična podkovanost ljudi v podjetju, kar je problem, ker manjša

[41] CSS – angl. Cascading Style Sheets

podjetja nimajo zadosti visoko izobraženega kadra. Velika slabost RIP je tudi v njeni visoki ceni, saj morajo podjetja zgraditi svoja privatna omrežja, kar pa zahteva velike stroške, kar pa si lahko privoščijo samo velika podjetja. Prednost XML-a pa je v njegovi fleksibilnosti. Na primer, tudi ljudje, ki niso ekstremno tehnično podkovani, lahko v zglednem času razvijejo svoj DTD, kar pa je težko trditi za razvijanje standardnih UN/EDIFACT tipov sporočil. Poleg tega pa so DTD-ji enostavni za distribucijo preko svetovnega spleta (Huemer, 2000, str. 686).

UN/EDIFACT je bil razvit z namenom, da lahko prenaša poslovne informacije, katere lahko predstavimo v tekstovnem formatu, problem pa se pojavlja pri netekstovnih informacijah, katerih prenos s standardom UN/EDIFACT ni možen. XML pa omogoča prenos netekstovnih informacij, kot so na primer slike.

Naslednja slabost standardov RIP je, da zahteva postavitev privatnih omrežij, katerih postavitev in vzdrževanje je zelo drago, tako da si taka omrežja lahko privoščijo samo zelo velika podjetja. XML uporablja že standardizirane protokole prenosov podatkov, predvsem je pomembna uporaba Interneta.

Možne prednosti XML-a so tudi v tem, da je koda XML veliko bolj berljiva, kot koda standardov RIP. Le-to pa pripomore k večji uporabi jezika XML, tako da bo v zglednem času na voljo dovolj XML programerjev, ki bodo pisali XML kodo za procesiranje podatkov. Za razliko od RIP-a, kjer je število programerjev, ki so sposobni napisati UN/EDIFACT tipe sporočil, še po desetih letih še zelo majhno.

Vendar pa tudi XML ni brez slabosti. Slabost XML-a je v pomanjkanju standardiziranih definicij zaznamkov. Tako se pojavljajo množice definicij zaznamkov s strani različnih podjetij, za podobne ali celo enake rešitve, v različnih ali istih panogah (Dečman, 2001, str. 54). XML poizkuša to slabost odpraviti z imenskim prostorom (angl. XML namespace) mehanizmom, kjer ima vsak element svoj imenski prostor, definiran z URI.

Prav tako se pojavljajo organizacije, ki poizkušajo standardizirati elektronske poslovne transakcije, na primer RosettaNet[42], Open Applications Group (OAG)[43], Microsoft BizTalk, Open Buying on the Internet (OBI)[44] ter Open Travel Alliance (OTA)[45]. Le-ti poizkušajo sestaviti XML specifikacije za posamezne poslovne sektorje, kar bi privedlo do standardizacije uporabe jezika XML, kar pa je tudi glavna prednost standarda RIP UN/EDIFACT (Huemer, 2000, str. 688).

V tabeli 7 so podane glavne značilnosti obeh standardov v elektronskem poslovanju.

Tabela 7: Primerjava značilnosti EDI in XML

EDI	XML
- Zapletena sintaksa - Nečitljiv - Dodajanje novih standardov je dolgotrajno in drago - Odvisen od strojne opreme in programske opreme - Dostopen samo velikim podjetjem in ustanovam - ozka uporaba - dolgotrajno in zapleteno nadgrajevanje - ozek krog strokovnjakov - različni vmesniki za komunikacijo s posameznimi partnerji	- enostavna sintaksa - večji nadzor nad programskimi rešitvami - enaka oblika predstavitve podatkov za interno uporabo in zunanjo komunikacijo - podpora v programskih rešitvah - široka uporaba - veliko programerjev - povezanost s Internetom - lahko berljiv - enostavno razširljiv - neodvisen od strojne in programske opreme - dostopen malim podjetjem

Vir: Jamnik, 2001, str. 69.

Čeprav ima XML veliko prednosti pred RIP-om, pa ima tudi svoje slabosti, tako da je malo verjetno, da bo XML v celoti nadomestil standarde RIP. Le-to pa verjetno tudi ni njegov cilj, temveč le določitev novih standardov in postopkov, ki v že avtomatiziranih poslovnih procesih dodatno podpirajo še XML. S tem namenom je bila formirana tudi skupina XML/EDI[46]. Njen cilj je uporabiti kombinacijo XML in standardov RIP za izdelavo novih močnih paradigem, ki izkoriščajo prednosti obeh jezikov (Dečman, 2001, str. 55).

[42] RosettaNet – http://www.rosettanet.org/

[43] Open Applications Group – http://www.openapplications.org

[44] Open Buying on the Internet – http://www.openbuy.org/

[45] Open Travel Alliance – http://www.opentravel.org/

[46] XML/EDI group – http://www.xmledi-group.org

6.2. Prihodnost XML-a v elektronskem poslovanju

Razlogi za razširjenost jezika XML so v njegovi funkcionalnosti, široki dostopnosti ter predvsem enostavnosti uporabe. Čeprav je namen ohraniti jezik XML preprost, se pojavljajo težnje po dodajanju novih značilnosti in funkcij v XML-u, z namenom povečanja njegove uporabnosti in prilagodljivosti. Če pa bi XML in njegove razširitve postali preveč kompleksni, bi se število razvijalcev in programerjev, ki bi implementirali rešitve elektronskega poslovanja v jeziku XML zelo zmanjšalo, kar bi posledično pomenilo tudi manj rešitev, torej manjšo razširjenost in dostopnost. Verjetno se bo v prihodnosti razvila okleščena verzija XML-a, za razvijalce zunanjih sistemov in reševanje problemov elektronskega poslovanja ter kompleksna verzija XML, za razvijalce internih sistemov, ki bodo uporabljali XML z vsemi nadgradnjami in razširitvami (Jamnik, 2001, str. 69).

Prihodnost uporabe XML v elektronskem poslovanju bo odvisna tudi od dobre definicije standardnih sporočil. Če želimo, da bo jezik XML uporaben globalno, je potrebno zaznamke definirati tako, da jih bodo "razumele" različne programske rešitve, ki te zaznamke berejo. Torej je problem XML-a enak kot pri RIP-u – potreba po definiranju standardnih sporočil. Ker je rešitev podobna za oba standarda, sta se združila tudi dva glavna igralca UN/EDIFACT in OASIS[47] ter začela izvajati projekt Electronic Business XML (ebXML), katerega namen je standardizacija XML-a za elektronsko poslovanje (Huemer, 2000, str. 690).

6.2.1. ebXML

Začetki ebXML segajo v leto 1999, ko sta UN/CEFACT in OASIS podala mednarodno iniciativo za izdelavo standarda ebXML.

Trenutno ebXML še ni standard, vendar se pričakuje, da bo postal v prihodnosti. Še prej pa bo postal "de facto" standard pri elektronskem poslovanju, saj naj bi ga sprejela večina industrijskih skupin, podjetij ter ponudnikov elektronskega poslovanja (ebXML.org, 2001).

Problem XML-a je tudi v pomanjkanju standardizacije zaznamkov. Zato se pojavljajo težnje po organiziranju in standardizaciji jezika. Za uporabo XML-a v elektronskem

[47] OASIS – angl. Organization for the Advancement of Structured Information Standards

poslovanju, se pojavlja kot možnost nek podjezik XML, in sicer ebXML. Le-ta naj bi prinesel standardizirane zaznamke, ki bi bili uporabni v ekonomski sferi, torej pri elektronskem poslovanju. EbXML naj bi definiral zaznamke za elektronsko poslovanje med podjetji, kar bi omogočilo podjetjem, da bi elektronsko sodelovala s pomočjo XML-a (Imani, 2001).

Ali kot so zapisali pri OASIS, cilj ebXML-a naj bi bil poenostavitev elektronskega poslovanja med podjetji ne glede na velikost ali programsko opremo ter uporaba jezika XML za elektronsko izmenjavo podatkov med subjekti (Mahoney, 2001).

7. Sklep

Elektronsko poslovanje se je v zadnjih nekaj letih razširilo na vsa področja človekovega delovanja. Na svetu skorajda ni več kotička oziroma človeka, ki ne bi poznal besede Internet. Tako je tudi v poslovni sferi vedno manj podjetij, ki zavračajo uporabo informacijske tehnologije pri svojem poslovanju. Če je včasih veljalo, da prinaša uporaba računalnikov konkurenčno prednost podjetju, danes velja, da podjetje brez računalniške podpore poslovanju ne more obstajati, saj ne more poslovati konkurenčno.

Čeprav so bili mnogi skeptični glede pomena in prednosti, ki jih prinaša jezik XML, postaja jasno, da bo XML pomenil eno od prelomnic v razvoju elektronskega poslovanja, kot tudi samega svetovnega spleta. Da bo XML pomenil veliko prelomnico v elektronskem poslovanju, nakazuje tudi podzvrst jezika XML – ebXML, za katerega se pričakuje, da bo postal standard na področju elektronskega poslovanja ter računalniške izmenjave podatkov.

XML utegne prinesti pravo revolucijo v elektronsko poslovanje z poenostavitvijo načina zapisa podatkov in sporočil, ki se pošiljajo preko svetovnega spleta. Prednost pa je tudi v tem, da je možna komunikacija med najrazličnejšimi sistemi. S pojavom XML-a povezovanje med podjetji in računalniška izmenjava podatkov ni več domena samo največjih podjetij, ampak tudi srednjih in majhnih, s tem pa le-ta postajajo tudi bolj konkurenčna, ter tako lažje konkurirajo velikim podjetjem.

Seveda pa prinaša uporaba XML-a tudi slabe strani. Z vidika uporabnika je slabost predvsem v sledenju novosti, ki jih s seboj prinaša jezik XML ter nedosledno upoštevanje standardov. Z vidika razvijalcev pa predstavlja XML novo tehnologijo, ki

zahteva nova znanja, pogosto pa tudi dodatno delo, saj je potrebno že razvite programske rešitve napisati na novo, saj stare niso kompatibilne z novim jezikom XML. Prav tako pa se pojavlja tudi problem varnosti prenosa podatkov, saj vemo, da XML uporablja svetovni splet za prenos podatkov, vendar pa mislim, da bo z uporabo opisanih metod varovanja dokumentov, (opisane so v petem poglavju tega dela), prenos podatkov varnejši.

Uvedba e-poslovanja mora biti povezana s prenovo poslovnih procesov, katerih rezultat je drugačen način dela in posledično tudi uporaba novih programskih rešitev. Podjetja bodo v vedno večji meri uporabljala jezik XML pri izmenjavi dokumentov, vendar pa naj bi se jezik, ki je trenutno šele v prvi verziji skozi čas razvijal in pridobival na svoji standardizaciji. Pričakovati je, da bo prihodnost jezika XML temeljila na nekaterih osnovah, ki so že postavljene, in sicer na osnovah standardov RIP.

8. Literatura

1. Bartel Mark, Boyer John, Fox Barb, LaMacchia Brian, Simon Ed: XML – Signature Syntax and Processing. [URL: http://www.w3.org/TR/2001/CR-xmldsig-core-20010419/], W3C, 19.4.2001.
2. Berger Sandy: B2B, B2C, and C2B. Who Needs a Translation?. [URL: http://www.compukiss.com/np/2000/b2bb2c/b2bb2c.html], Compu-KISS, 2000.
3. Bračko Andrej: Ocena priložnosti računalniškega izmenjavanja podatkov in elektronskega poslovanja v medorganizacijskih povezavah ministrstva za notranje zadeve. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 1997. 83 str.
4. Brain Marshall: How E-commerce works. [URL: http://www.howstuffworks.com/ecommerce.htm], 20.7.2001.
5. Damjan Maruša: Vloga urada za UN/EDIFACT pri uvajanju svetovnega standarda za RIP. Informatika v državnih organih, zbornik referatov, 1993, Brdo pri Kranju, str. 55 – 59.
6. Dečman Mitja: Elektronsko poslovanje in XML. Uporabna informatika, Ljubljana, 8(2000), 1, str. 51 – 56.
7. Dillaway Blair, Fox Barbara, Imamura Takeshi, LaMacchia Brian, Maruyama Hiroshi, Schaad Jim, Simon Ed: XML Encryption Syntax and Processing. [URL: http://lists.w3.org/Archives/Public/xml-encryption/2000Dec/att-0024/01-XMLEncryption_v01.html], W3C, 15.12.2000.
8. Flisi Maximilian: E-distributors poised to lead B2B. [URL: http://www.itworld.com/Tech/3478/CIO010415newsletter], 15.4.2001.
9. Harold Elliotte Rusty: XML Bible. Foster City, CA : IDG Books Worldwide, 1999. 974 str.
10. Huemer Christian: XML vs. UN/EDIFACT or Flexibility vs. Standardisation. Bled : 13th International Electronic Commerce Conference, 2000, str. 680 – 692.
11. Irani Romin: An introduction to ebXML. [URL: http://www.webservicesarchitect.com/content/articles/irani02.asp], Web Services Architect, Julij 2001.
12. Istenič Irena: Elektronsko poslovanje in poslovni modeli. Diplomsko delo. Ljubljana : Ekonomska fakulteta, 2000. 51 str.
13. Jamnik Anka: Razširljivi označevalni jezik XML in njegove razširitve ter pomen pri razvoju poslovnih Internetnih storitev. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 2001. 98 str.
14. Jerman Blažič Borka et al.: Elektronsko poslovanje na Internetu. Ljubljana : GV Založba, 2001. 206 str.
15. Mahoney Michael: Global E-Commerce Standard Proposed. [URL: http://ecommercetimes.com/perl/story/9722.html], E-commerce Times, Maj 2001.
16. Marusich Carmen, Blackthorn Sandy: Elektronsko poslovanje za telebane. Drugi natis. Ljubljana : Pasadena, 1999. 80 str.

17. Mohorič Tomaž, Krisper Marjan: O razširljivem označevalnem jeziku XML in njegovi uporabi. Uporabna informatika, Ljubljana, 9(2001), 2, str. 55 – 59.
18. Pardi J. William: XML in Action. Redmond, Washington : Microsoft Press, 1999. 329 str.
19. Pavšič Robert: Simfonija E-poslovanja. Moj Mikro, Ljubljana, 2(2001), str. 60 – 62.
20. Pucihar Andreja: Priložnosti in težave elektronskega poslovanja med organizacijami v Sloveniji. Uporabna informatika, Ljubljana, 7(1999), 4, str. 7 – 13.
21. Simon Ed, Madsen Paul, Adams Carlisle: An Introduction to XML Digital Signatures. [URL: http://www.xml.com/pub/a/2001/08/08/xmldsig.html], XML.com, 8.8.2001.
22. Slana Lidija: Elektronsko poslovanje – uvajanje mednarodnega standarda UN/EDIFACT v poslovno in bančno okolje. Uporabna informatika, Ljubljana, 7(1999), 4, str. 25 – 31.
23. Sturm Jake: Developing XML Solutions. Redmond, Washington : Microsoft Press, 2000. 415 str.
24. Škedelj Miran: Uporaba sodobnih telekomunikacijskih storitev v poslovanju veledrogerije. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 1999. 97 str.
25. Toplišek Janez: Elektronsko poslovanje. Prva izdaja. Ljubljana : Atlantis, 1998. 336 str.
26. Travis E. Brian: XML and SOAP programming for Biztalk servers. Redmond, Washington : Microsoft Press, 2000. 428 str.
27. Walsh Norman: What is XML?. [URL: http://www.xml.com/pub/a/98/10/guide1.html#AEN58], 3.10.1998.
28. Weisman Jon: The Making of E-Commerce: 10 Key Moments. [URL: http://www.ecommercetimes.com/perl/story/4085.html], 22.8.2000.
29. Zupan Neja, Gričar Jože: Priložnosti in težave izmenjavanja podatkov preko Interneta med večjimi in manjšimi podjetji v Sloveniji. Zbornik posvetovanja, DSI 1999, Portorož, str. 278 –286.

9. Viri

1. A Dictionary of Computing. Četrta izdaja. Oxford : Oxford University Press, 1997. 550 str.
2. A Proposal for XSL: [URL: http://www.w3.org/TR/NOTE-XSL.html], W3C, august 1997.
3. Bokler: Bokler Software's Cryptographic Resources Page. [URL: http://spider.bokler.com/bokler/resrcs_1.html], Bokler Software Corp., 2001.
4. Certifikati javnih ključev. [URL: http://www.gov.si/tecaj/kripto/kr-cert.htm], Center vlade RS za informatiko, december 2000.
5. ebXML – Enabling A Global Electronic Market –Specifications. [URL: http://www.ebxml.org/specs/index.htm], oktober 2001.
6. ebXML FAQ. [URL: http://www.ebxml.org/faq.htm], ebXML.org, oktober 2001.

7. ERC Beximco: Rising star of E-commerce. [URL: http://www.beximco.org/economic-research/rising.html], ERC Beximco, 2001.
8. Gooogle: [URL: http://www.google.com], junij – august 2001.
9. Hornby A. S.: Oxford Advanced Learner's Dictionary of Current English. Šesta izdaja. Oxford : Oxford University Press, 2000. 1600 str.
10. iPier.com: E-Commerce 101: E-Commerce Overview. [URL: http://www.ipier.com/ecom101/ecom1.html], 20.7.2001.
11. Kubler Jean: Electronic commerce on the Web – background information: From paper to EDI to electronic forms using XML?. [URL: http://www.unece.org/cefact/xml/press/eforms.pdf], United Nations Centre for Trade Facilitation and Electronic Business, 7.12.1999. 23 str.
12. Netscape Communications Corporation: Introduction to SSL. [URL: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm], 10.9.1998.
13. Protokol SET. [URL: http://www.gov.si/tecaj/kripto/kr-set.htm], Center vlade RS za informatiko, 26.3.1998.
14. RIS: Anketa podjetij, Elektronsko poslovanje RIS 2000/2001. [URL: http://www.ris.org/publikacije/j_eposlovnj.htm], julij 2001.
15. RIS: Anketa podjetij, Elektronsko poslovanje z državo RIS 2000/2001. [URL: http://www.ris.org/id/elekt_posl_drzava.htm], julij 2001.
16. Rosenberg M. Jerry: Dictionary of Computers, Information Processing & Telecommunications. Druga izdaja. New York : John Wiley & Sons, 1987. 734 str.
17. SET Secure Electronic Transaction LLC. [URL: http://www.setco.org/set.html], 2001.
18. SIGEN-CA: Splošno o potrdilo za fizične osebe. [URL: http://www.sigen-ca.si/faq-spletna-fo.htm], SIGEN-CA, oktober 2001.
19. SSL(Secure Socket Layer). [URL: http://www.gov.si/tecaj/kripto/kr-ssl.htm], Center vlade RS za informatiko, december 2000.
20. Šalamon Brane: Internet pojmovnik. Druga izdaja. Izola : Desk d.o.o., 1998. 287 str.
21. Škerlj Ružena: Angleško – slovenski slovar. Četrta izdaja. Ljubljana : Državna založba Slovenije, 1957. 773 str.
22. W3C: Extensible Markup Language (XML) 1.0 (second edition). [URL: http://www.w3.org/TR/REC-xml], W3C, 6.10.2000.
23. World Wide Web Consortium (W3C). [URL: http://www.w3.org], W3C, august 2001.
24. XML Linking Language (XLink) Version 1.0. [URL: http://www.w3.org/TR/WD-xlink], W3C, junij 2001.
25. XML-Signature Syntax and Processing. [URL: http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/], W3C, 20.8.2001.
26. Zakon o elektronskem poslovanju in elektronskem podpisu. [URL: http://www2.gov.si/zak/Zak_vel.nsf/4c1d8c547755fffac1256616002dd5e1/c12563a400338836c12568fd00505349?OpenDocument], www.gov.si,13.6.2000.

10. Priloge

Pojasnila kratic in slovar angleških izrazov

	Electronic Commerce	Elektronsko poslovanje
	Encryption	Šifriranje
	Web Browser	Brskalnik za svetovni splet
	XML Namespace	Imenski prostor XML
ASCII	American standard code for information interchange	
B2B	Business to Customer	Poslovanje med podjetji in strankami
B2C	Business to Business	Poslovanje med podjetji
CA	Certificate Authority	Agencija za certificiranje javnih ključev
DES	Data Encryption Standard	Najpogostejši sistem simetričnega šifriranja
DTD	Document Type Definition	Definicija tipa dokumentov
EBNF	Extended Backus-Naur Form	Razširjena Backus-Naur forma, ki opisuje sintakso programskega jezika
ECC	Elliptic Curve Criptografy	Sistem asimetričnega šifriranja
EDI	Electronic Data Interchange	Računalniška izmenjava podatkov
FTP	File Transfer Protocol	Protokol za prenos datotek
HTML	Hyper Text Markup Language	Jezik za označevanje hiperteksta
HTTP	Hyper Text Transfer Protocol	Protokol, ki se uporablja na svetovnem spletu za prenos hiperteksta
IDEA	International Data Encryption Algorithm	Sistem simetričnega šifriranja
JIT	Just in Time	Poslovanje brez zalog, poslovanje "ravno ob pravem času"
MTA	Message Transfer Agent	Agent, ki sprejme pošiljateljev e-mail ter ga pošlje prejemnikovemu agentu
RC2	Rivest's Cypher	Sistem simetričnega šifriranja
RSA	Rivest – Shamir – Adleman	Najpogostejši sistem asimetričnega šifriranja
S/MIME	Secure Multipurpose Internet Mail Extensions	
SET	Secure Electronic Transfer	Varni elektronski prenos
SGML	Standard Generalized Markup Language	Standardni splošni označevalni jezik
SSL	Secure Socket Layer	Sloj varnih vtičnic

SWIFT	Society for Worldwide Interbank Financal Transmissions	Omrežje bančnih organizacij
TELNET	Teletype Network	Internet protokol, ki omogoča uporabniku priključitev na druge računalniške sisteme
TLS	Transport Layer Security	Transportni nivo varnosti
UN/CEFACT	United Nations Centre for the Facilitation of Procedures and Practices for Administration, Commerce and Transport	Organizacija združenih narodov za poenostavitev mednarodnega poslovanja
UN/EDIFACT	United Nations Electronic Data Interchange for Administration, Commerce and Transport	Standard združenih narodov za računalniško izmenjavo podatkov za področje administracije, trgovine in transporta
UNICODE		16-bitna koda, definirana s strani Unicode konzorcija
URI	Universal Resource Identifier	Enolični identifikator vira
VAN	Value Added Network	Omrežje z dodano vrednostjo
W3C	World Wide Web Consortium	Konzorcij za svetovni splet
WWW	World Wide Web	Svetovni splet
XLL	Extensible Linking Language	Dodatek XML za povezovanje dokumentov med seboj
XML	Extensible Markup Language	Razširljivi označevalni jezik
XSL	Extensible Stylesheet Language	Dodatek XML za besedilne sloge