UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

TOMAŽ PERNOVŠEK

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VARNA IZMENJAVA ELEKTRONSKIH SPOROČIL NA OSNOVI PODPISA XML V PODJETNIŠKEM POSLOVANJU

LJUBLJANA, SEPTEMBER 2004 **TOMAŽ PERNOVŠEK**

IZJAVA

Študent Tomaž Pernovšek izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Borke Jerman Blažič in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, 1.9.2004

Podpis: _____

KAZALO

1 UVOD

Sodobna storitvena podjetja se želijo vse bolj približati uporabnikom, hkrati pa čim bolj izrabiti sodobne tehnologije in prijeme, s katerimi lahko učinkovito spremenijo obstoječe poslovne procese z namenom racionalizacije in večje stroškovne učinkovitosti. Na drugi strani želijo naročniki pri poslovanju vse bolj vzeti nadzor dogajanj v svoje roke, kar pomeni, da vmesni koraki niso več zaželeni. Splet se je pokazal kot idealno orodje za postavitev stičišča, kjer lahko uporabniki storitev prihajajo in si ogledujejo, kako uporabljajo svoje naročene storitve, kaj jim je novega na voljo, kakšna je kakovost storitve, česa ne morejo uporabljati več in podobno (Kalakota, 2000, str. 20). Portali, ki so prilagojeni posameznim uporabnikom, so tako postali samoumevni, njihova moč pa se kaže predvsem v možnosti dvostranskega komuniciranja. Osnovne aplikacije, kot so prikaz opravljenega prometa, naročenih storitev, arhiva uporabljenih storitev in izdanih računov, podatkov o uporabniku ipd., so nujne, vendar ne več zadostne. Potrebna je torej komunikacija tudi v smeri od naročnika do ponudnika storitev. Vendar je za to treba zagotoviti identifikacijo pošiljatelja, neokrnjenost poslanih podatkov na komunikacijski poti in predvsem preprečevanje zanikanja sodelovanja v elektronski transakciji. Podpora za to pa (za zdaj) v spletnih brskalnikih oziroma bolj splošno na operacijskih sistemih ni zagotovljena.

Problem, ki zahteva ustrezno rešitev, je zagotoviti varne izmenjave elektronskih sporočil (dokumentov, pogodb, aneksov k pogodbam, naročil ipd.) in sklepanje pogodb prek interneta. Problem je treba reševati s treh zornih kotov – tehnološkega, organizacijskega in pravnega (Makarovič et. al., 2001, str. 41). Osnovna zahteva pri teh dejavnostih je zagotovljena varnost, natančneje avtentičnost in nespremenljivost elektronskih podatkov in preverjena identiteta subjektov, s katerimi se komunicira. S takšnim problemom se je srečevala tudi družba SiOL, d. o. o., ki ponuja internetne storitve na slovenskem in tudi širšem trgu. Problem, ki se je postavljal pred družbo, je bila avtomatizacija dela v kontaktnem centru, ki bi naročnikom (tudi bodočim) omogočila dvostransko komunikacijo in hitrejši odziv na posredovane zahteve po spremembah naročenih storitev. Vse delo, ki je zahtevalo odprtje novih storitev oziroma spremembe na obstoječih priključkih, je potekalo v papirnati obliki. Uporabnike je motilo, da ne morejo s ponudnikom komunicirati v elektronski obliki.

1.1 Namen dela s temeljno hipotezo

Namen pričujočega dela je bilo raziskati tehnološke in pravne možnosti izmenjave elektronskih sporočil, določiti potrebne tehnologije in organizacijske postopke ter vzpostaviti okvirni sistem za njihovo varno izmenjavo v naročniškem sistemu podjetja SiOL. Za ta namen sem:

- pripravil ustrezno predstavitev koncepta elektronskega poslovanja v gospodarstvu, predvsem na področju ponujanja internetnih storitev,
- analiziral infrastrukturo za zagotavljanje varne izmenjave elektronskih sporočil,
- analiziral tehnologije za potrebe v infrastrukturi, predvsem metajezika XML (razširljiv označevalni jezik, angl. Extensible Markup Language), varnostnih mehanizmov, ki se delijo na tri sklope (elektronska komunikacija, elektronska oblika in elektronski podpis), infrastrukturo javnih ključev (PKI), podpisovanje dokumentov, zapisanih v XML, načine preverjanja podpisov, elektronskega arhiviranja ipd.,
- oblikoval model storitve v konkretnem podjetniškem okolju podjetja SIOL, d. o. o.,
- izdelal projekt vpeljave storitve za varno izmenjavo elektronskih dokumentov v produkcijsko okolje omrežja SiOL, ki omogoča elektronsko sklenitev naročniškega razmerja na podlagi elektronske priprave in podpisa naročniške pogodbe, ter
- izdelal kritično analizo sistema in predstavil prednosti ter slabosti modela s ciljem nakazati smernice nadaljnjega razvoja.

Pri izdelavi magistrskega dela sem izhajal iz naslednje hipoteze: izdelati sistem, ki bo pokazal, da je možno vzpostaviti varen sistem za elektronsko izmenjavo sporočil na osnovi podpisa dokumentov, zapisanih v XML, v podjetniškem okolju v skladu s slovensko zakonodajo, predvsem z Zakonom o elektronskem poslovanju in elektronskem podpisu, v nadaljevanju **ZEPEP**.

Pri tem sem uporabil pristop prehajanja od splošnega k podrobnemu, saj sem želel predstaviti opisano problematiko čim bolj celovito. Zaradi kompleksnosti sem uporabil več metod dela. Pri opisu elektronskega poslovanja s poudarkom na izmenjavi elektronskih sporočil sem uporabil analizo preteklih rešitev (pregled možnosti izmenjav v preteklosti). Zatem sem analiziral domačo zakonodajo z vidika možnosti uvajanja elektronskega poslovanja s poudarkom na izmenjavi elektronskih sporočil v omrežju SiOL. V nadaljevanju sem uporabil metodo vodenja projektov, ki se uporablja v podjetju SiOL. Njene ključne prednosti so orientacija k poslovni upravičenosti in prilagodljiv pristop, predvsem pa upoštevanje izkušnje izvajanja dosedanjih projektov. Na koncu sem dodal še kritično analizo celotnega sistema, predvsem v luči ekonomske upravičenosti, prednosti in slabosti uporabe sistema ter identifikacije kritičnih dejavnikov nadaljnjega razvoja uporabe/uveljavljanja.

2 VARNOST V ELEKTRONSKEM POSLOVANJU

2.1 Zagotavljanje varnosti pri izmenjavi elektronskih sporočil

Zagotavljanje varnosti sloni na storitvah zaupnosti (zagotavljanje tajnosti sporočil), celovitosti (neokrnjenost podatkov, še posebno z zagotavljanjem nespremenljivosti sporočil na poti od oddajnika do prejemnika), razpoložljivosti (upravičenim uporabnikom se ne prepreči dostopa do sporočila) in overjanja uporabe (preprečevanje dostopa do informacij neavtoriziranim osebam). Storitve uporabljajo tako komunikacijski kot računalniški sistemi (Warwick, 2001, str. 93–97). Komunikacijski sistemi se ukvarjajo predvsem s prenosom podatkov od oddajnika do prejemnika, medtem ko se računalniški ukvarjajo z zagotavljanjem varnosti znotraj sistema, npr. znotraj operacijskih sistemov, podatkovnih baz, aplikacij itn. Za zagotovitev resnične varnosti je nujno, da informacijska varnost dopolnjuje ostale tipe varnosti, kot so fizična (varovanje prostorov, ključavnice...), osebna, administrativna in medijska varnost (uničevanje dokumentov in medijev na zanesljiv način).

Na elektronsko poslovanje preži veliko nevarnosti. Lahko jih razdelimo v več kategorij.

- Pretvarjanje (uporaba legitimnih dejanj na nelegalen način). Sem sodi cela vrsta napadov, od vohljanja na lokalnem omrežju ali prehajajočem prometu do razbijanja gesel.
- Zanikanje sodelovanja pri določenih aktivnostih (avtor sporočila pozneje taji svoje avtorstvo).
- Spreminjanje podatkov (z vdorom v sistem lahko napadalec namerno spremeni izvorno sporočilo, npr. znesek na finančni transakciji).
- Vdor v sistem.
- Kršitev nadzora dostopa (napadalec sicer ima pravice za dostop do nekaterih informacij v napadenem sistemu, vendar pride tudi do tistih, za katere ni avtoriziran).
- Sejanje (napadalec pri avtoriziranem dostopu pusti za sabo aplikacijo, po navadi zamaskirano, ki mu služi pozneje za vdor v sistem). V to kategorijo sodijo virusi in trojanski konji.

Informacijska varnost se ukvarja s preprečevanjem vseh nevarnosti, ki prežijo na elektronsko poslovanje. Kot je znano, je varnost le tolikšna, kot je varen najšibkejši člen znotraj opazovanega sistema, zato je nujno, da se prijemi za preprečevanje prežečih nevarnosti uporabljajo skupaj in ne posamezno za vsako obliko groženj. Nič ne pomaga najsodobnejša tehnološka zaščita, če v organizaciji ni prisotne ustrezne varnostne kulture oziroma če lahko

napadalec izve za geslo le s klicem na tehnično pomoč podjetja ali s krajšim sprehodom po pisarnah v času malice. Med osnovne prijeme za zagotavljanje informacijske varnosti se prištevajo storitve overjanja (po navadi s kombinacijo nečesa, kar legitimen uporabnik ima, in nečesa, kar ve), storitve dostopne kontrole do različnih virov znotraj sistema, storitve zaupnosti (po navadi s šifriranjem), storitve skladnosti podatkov in storitve preprečevanja tajenja avtorstva podatkov. Veda, ki se ukvarja z zagotavljanjem tehnik, potrebnih za učinkovito in predvsem varno elektronsko poslovanje, se imenuje kriptografija, temelji pa predvsem na kompleksnih matematičnih funkcijah (Nash et. al., 2001, str. 67). Beseda »cryptography« pomeni pretvorbo čistopisa v tajnopis.

2.2 Kriptografija

Temelj kriptografije so kriptosistemi oziroma šifrirni algoritmi, ki jih sestavljata dve podatkovni transformaciji (šifriranje in dešifriranje), ki se umestita na sporočilo, v kriptografiji imenovano čistopis (angl. plaintext). Rezultat šifriranja je neberljiv tekst, imenovan tajnopis (angl. ciphertext). Vrnitev v prvotno stanje se lahko izvede le z ustreznim dešifriranjem. Transformacija šifriranja ima tipično dva vložka – čistopis in šifrirni ključ. Slednji je navidezno naključen niz znakov, ki ima točno določeno dolžino, odvisno od šifrirnega sistema. Z uporabo ustreznega ključa s primerno dolžino se lahko zagotovi tajnost podatkov tudi pri prenašanju skozi javne, nevarovane sisteme, saj ga napadalec brez pravega dešifrirnega ključa praktično ne more zlomiti.

2.2.1 Simetrični in asimetrični algoritmi

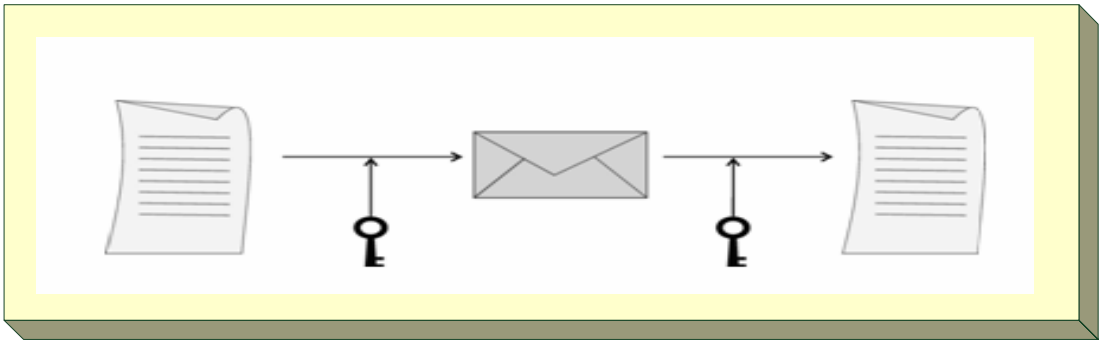
Kriptosisteme ločimo na dva osnovna tipa, simetrične in asimetrične. Simetričnemu ponekod pravijo sistem zasebnega ključa, asimetričnemu sistem javnega ključa, obstajajo pa še druga poimenovanja.

Simetrični algoritmi so poznani že precej časa, saj so v svoji osnovi enostavnejši za uporabo in razumevanje. Osnovni gradnik je poleg šifrirnega algoritma ključ, poimenovan simetrični ključ, ki ga za šifriranje čistopisa oziroma dešifriranje tajnopisa uporabljata oba, tako oddajnik (v nadaljevanju **Metka**) kot prejemnik (v nadaljevanju **Janko**[1]),. Ključ morata oba skrbno varovati, saj bi bila zasebnost sporočila v primeru, da je poznan še komu drugemu, ogrožena. Za razpošiljanje ključa je na voljo več metod, ki bodo opisane v nadaljevanju. Za uspešno preneseno tajno informacijo se morata Metka in Janko vnaprej dogovoriti, kakšen simetrični algoritem bosta uporabila, kateri in kako dolgi ključ bo dostopen obema in prek kakšnega komunikacijskega medija bosta prenesla tajno informacijo. Oba se seveda zavedata, da na tem komunikacijskem mediju preži Čarli, ki želi prestreči tajnopis in simetrični ključ, na voljo pa mu še vedno ostane, da skuša s

[1] Imeni Metka in Janko se po navadi uporabljata v knjigah, povezanih z varnostjo, tako da bralec vedno ve, za koga gre. Pogosto se uporablja še ime Čarli, ki ponazarja napadalca.

preizkušanjem velikega števila različnih ključev[2] uganiti izbranega. To je najbolj enostavna, vendar z večanjem števila bitov v izbranem simetričnem ključu vedno težja naloga.

Slika 1 - Simetrična kriptografija



Vir: Jerman Blažič, 2001, str. 103

Poznanih je veliko simetričnih algoritmov, ki jih v splošnem delimo v dva tipa, pretočni in blokovni tajnopis. Razlikujeta se v številu bitov čistopisa, ki se naenkrat šifrira. Pretočni algoritmi šifrirajo vsak bit posebej in zaporedoma, medtem ko blokovni vzamejo blok bitov (tipično n-krat 64 bitov) in jih šifrirajo v skladu s šifrirnim algoritmom. Najbolj znan blokovni algoritem je DES (Data Encryption Standard), ki je bil sprejet kot standard ameriške administracije že leta 1977[3] in kot standard finančne industrije leta 1981[4]. Uporabljal se je vrsto let, dokler procesorska moč računalnikov ni postala tako močna (tudi v obliki porazdeljenega delovanja prek interneta), da je postal neuporaben, ker se da v doglednem času razkriti uporabljeni ključ. Od leta 1997 je ameriška administracija v okviru razpisanega natečaja začela pospešeno iskati nov algoritem, ki bi nadomestil DES in postal nov uporabljan standard. Poimenovali so ga AES (Advanced Encryption Standard), avtorja pa sta Belgijca Daemen in Riijmen. Temelji na šifriranju 128-bitnih blokov čistopisa z uporabo 128-, 198- ali 256-bitnih simetričnih ključev. Kot standard je bil sprejet novembra 2001[5]. Ostali pogosto uporabljani simetrični algoritmi so Triple-DES (trikratno šifriran blok podatkov z DES, pri čemer sta prvi in tretji ključ po navadi enaka), Rivestovi algoritmi (RC2, RC4, RC5, RC6), IDEA, Blowfish in drugi (Warwick, 2001, str. 102–103).

[2] Napad s surovo silo (Brute Force Attack).

[3] U. S. Department of Commerce, Data Encryption Standard, Federal Information Processing Standards Publication FIPS PUB 46 (1977; ponovno izdan leta 1994 kot FIPS PUB 46-2), na voljo na spletnih straneh http://cscr.nist.gov).

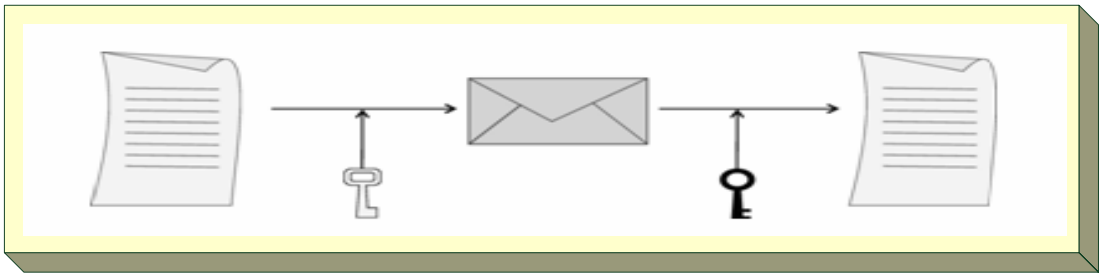
[4] American National Standards Institute, ANSI X3.92: American National Standard, Data Encryption Algotithm (1981).

[5] U. S. Department of Commerce, Advanced Encryption Standard, Federal Information Processing Standards Publication FIPS PUB 197, na voljo na straneh http://csrc.nist.gov/CryptoToolkit/aes/.

Osnovna težava pri simetričnih kriptosistemih je v tem, da ni ustrezne podpore za zagotavljanje neokrnjenosti poslanega sporočila, torej da se sporočilo na svoji prenosni poti ni spremenilo. Zato se pri teh sistemih uporablja koda za overitev sporočila (Message Authentication Code), tako da lahko prejemnik (Janko) preveri, ali je sporočilo ostalo nespremenjeno. MAC je dodatno sporočilo, ki se naredi z uporabo zgoščevalne funkcije nad originalnim sporočilom. Če je MAC, ki ga z zgoščevanjem in svojim simetričnim ključem pridobi tudi Janko, enak tistemu, ki ga je naredila Metka in dodala k tajnopisu, se sporočilo na poti ni spremenilo. Najbolj znane enostranske zgoščevalne funkcije so SHA-1 (Secure Hash Algorithm 1), SHA-256, SHA-384 in SHA-512 [6].

Leta 1976, nekaj let za pojavom simetričnih kriptosistemov, sta Diffie in Hellman (Ford et. al., 1997, str. 50), oba z ameriške univerze v Stanfordu, predstavila nove smeri v kriptografiji z novim kriptografskim sistemom, imenovanim asimetrični sistem oziroma sistem javnih ključev. Lotila sta se predvsem slabosti pri širši uporabi simetrične kriptografije, to je upravljanje s simetričnimi ključi, kamor sodi izdelava, razpošiljanje, uporaba, arhiviranje in uničenje. **Asimetrična kriptografija** sloni na dveh različnih ključih, zasebnem in javnem. Pri tem je treba skrbeti za skritost le enega ključa, zasebnega, medtem ko je drugi javni, kar pomeni, da za njegovo skritost ni treba skrbeti.

Slika 2 - Asimetrična kriptografija



Vir: Jerman Blažič, 2001, str. 104

Kako asimetrična kriptografija deluje? V prvem koraku mora Janko narediti par ključev. Zasebnega varno shrani (npr. na pametno kartico), javnega pa pošlje Metki na popolnoma nezavarovan način ali ga objavi v kakšnem javnem imeniku, vendar mora v tem primeru Metko obvestiti, kje ga lahko dobi. Le-ta nato šifrira čistopis z Jankovim javnim ključem in mu pošlje pripravljen tajnopis. Dešifrira ga lahko le imetnik drugega ključa, torej Janko. V primeru, da nekdo želi dešifrirati z istim ključem, kot se je uporabil za šifriranje čistopisa, ne more priti do želenega rezultata, saj je osnova delovanja asimetrične kriptografije skrita ravno v asimetriji – v uporabi obeh ključev.

[6] Standard je na voljo na spletnem naslovu http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (maj 2004).

Omenjeno je že bilo, da asimetrična kriptografija rešuje problem simetrične v smislu varne izmenjave ključa, simetrična kriptografija pa rešuje problem prevelike zahtevnosti po zmogljivostih računalniških sistemov sicer zelo močne asimetrične kriptografije. Janko in Metka morata izmenjati simetrični ključ, vendar le na takšen način, da se Čarli do njega nikakor ne more dokopati. Zaradi hitrosti simetričnega šifriranja se takšen pristop kombiniranja asimetrične in simetrične kriptografije v praksi največkrat uporablja. Kombinacija obeh metod šifriranja povzema najboljše lastnosti iz posameznih algoritmov. Janko mora najprej narediti par ključev in objaviti javni ključ, zasebnega pa varno shraniti. Metka, ki želi poslati zaupne podatke Janku, najprej pridobi Jankov javni ključ in naredi simetrični ključ, ki ga mora poslati Janku. Z njegovim javnim ključem šifrira simetrični ključ in mu ga pošlje prek javnega omrežja. Ker je imetnik drugega ključa (zasebnega) le Janko, lahko le on dešifrira poslano sporočilo, ki je v bistvu simetrični ključ, s katerim bosta kasneje šifrirala zaupna sporočila. Sedaj ko sta varno izmenjala simetrični ključ, ne potrebujeta več asimetrične kriptografije, temveč le še zelo hitro simetrično, kar znatno zmanjša stroške in čas procesiranja za uporabo kriptografije za izmenjavo zaupnih sporočil.

Asimetrični algoritmi izkoriščajo dejstvo, da je iskanje velikih praštevil relativno enostavno, zelo težko pa je razstavljanje zmnožka dveh velikih praštevil. Če sta praštevili zadovoljivo veliki, zahteva razstavljanje njunega zmnožka ogromno procesorske moči računalnika in predstavlja praktično nerešljiv problem. Vprašanje, ki si ga stalno zastavlja množica znanstvenikov in raziskovalcev ob neprestanem naraščanju procesorske zmogljivosti, pa je, kakšna je potrebna velikost praštevila, da bo asimetrična kriptografija zadovoljivo močna in nezlomljiva? Pred nekaj časa se je v komercialne namene uporabljala velikost 512 bitov za asimetrične ključe, danes je to premalo. Za naslednja leta obstaja priporočilo uporabe 1024-bitne velikosti ključev, ob primerni opremi pa je 2048-bitni ključ velika prednost.

2.2.2 Elektronski podpisi

Pri uporabi simetrične kriptografije so se pokazale tri osnovne pomanjkljivosti:

- problem razpošiljanja simetričnih ključev,
- problem preprečevanja zanikanja in
- problem neokrnjenosti podatkov.

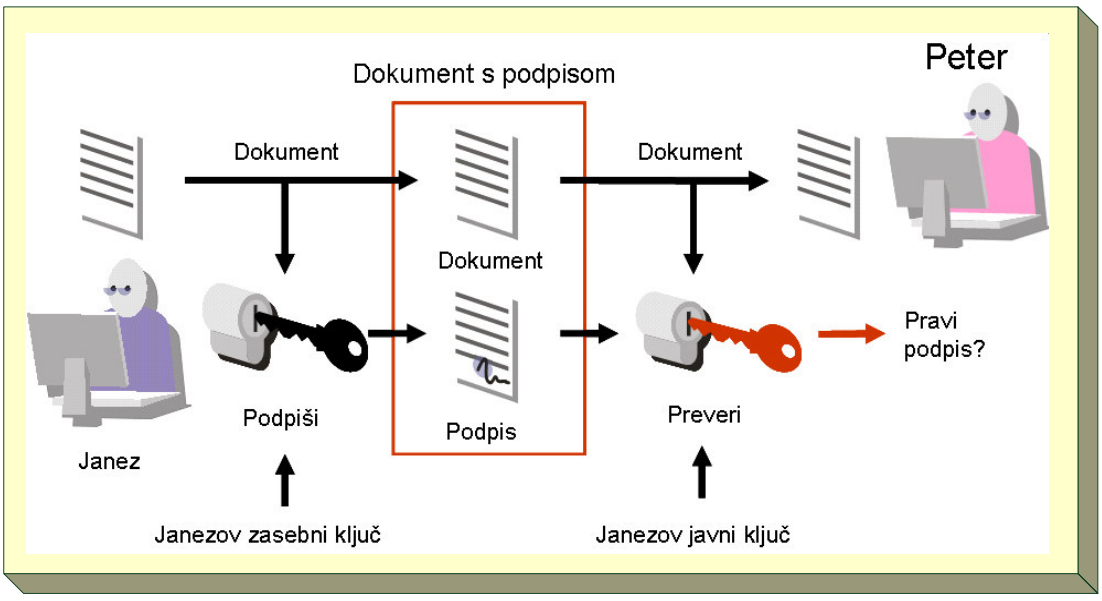
S sistemom javne kriptografije se rešuje prvi problem, ostala dva pa z uporabo **elektronskega podpisa**. Elektronski podpis je nadomestek lastnoročnega v elektronskem poslovanju in je namenjen pristnosti podatkov in identifikaciji podpisnika (Jerman-Blažič, 2001, str. 106). Pri podpisovanju obstajajo enostavne (dodajanje slike podpisa, uporaba svetlobnega peresa ipd.) in napredne metode, ki uporabljajo asimetrično kriptografijo. Slednje omogočajo **digitalno podpisovanje**. Za vsako metodo digitalnega podpisovanja stoji matematična funkcija, ki zgoščuje osnovno sporočilo, po navadi na točno določeno število

znakov, ne glede na dolžino sporočila. Ena izmed najbolj uporabljenih zgoščevalnih funkcij v sodobni kriptografiji je funkcija SHA-1. Le-ta daje za poljubno sporočilo izhodni blok podatkov stalne dolžine, poimenovan tudi »prstni odtis«, v velikosti 20 zlogov. Danes so že na voljo naprednejše verzije omenjene funkcije (SHA-256, SHA-512), ki dajejo daljši izhodni rezultat, seveda pa s tem izdatno zmanjšujejo možnost kolizije.

Digitalno podpisovanje elektronskega sporočila poteka v dveh korakih. Najprej se izvede skrčenje dokumenta z uporabo ene izmed enosmernih zgoščevalnih funkcij. Za razliko od običajnega krčenja dokumentov z namenom prihranka prostora se pri tem izgubi informacija o načinu povrnitve dokumenta v prvotno obliko. Sledi šifriranje prstnega odtisa s podpisnikovim zasebnim ključem.

Preverjanje digitalnega podpisa, ki ga po navadi izvede prejemnik digitalno podpisanega elektronskega sporočila, poteka v obratni smeri. Najprej se podpisano sporočilo dešifrira z javnim ključem podpisnika. Sledi ponovni izračun prstnega odtisa dokumenta in primerjanje z dešifriranim prejetim odtisom. Če se ujemata, je digitalni podpis veljaven, v nasprotnem primeru je sporočilo podpisal nekdo drug ali pa je bil spremenjen.

Slika 3 - digitalno podpisovanje



Vir: Jerman Blažič, 2001, str. 108

2.2.3 Digitalna potrdila

Overjanje javnega ključa pri uporabi asimetrične kriptografije za elektronsko podpisovanje je zelo pomembna. Janko, prejemnik podpisanega sporočila, mora biti prepričan, da je pošiljatelj sporočila in njegov avtor dejansko Metka. Janko sicer ima neizpodbiten dokaz, da

se sporočilo na svoji komunikacijski poti ni spremenilo, vendar ne ve, ali ga je Metka dejansko podpisala. Podobno kot je problematično prenesti ključ k prejemniku v simetrični kriptografiji (ki ga rešuje asimetrična kriptografija), je potreben dodaten mehanizem za preverjanje identitete podpisnika. Takšen mehanizem mora neločljivo povezovati javni ključ z uporabnikom, ki ima pri sebi odgovarjajoči zasebni ključ. Rešitev je uporaba infrastrukture za overjanje javnih ključev (PKI). Temelj PKI je digitalno potrdilo.

Idealno potrdilo mora vsebovati vse značilnosti, ki jih vsebujejo potrdila iz vsakdanje uporabe v fizičnem svetu (poslovne vizitke ali kreditne kartice), poleg pa še nekaj zelo pomembnih dodatkov, ki morajo biti overjeni s strani zaupanja vredne inštitucije. Po (Housley, Polk, 2001, str. 21) mora idealno potrdilo imeti naslednjih devet značilnosti:

- to je digitalna datoteka, ki se lahko razpošilja prek svetovnega spleta in samodejno obdeluje,
- vsebuje ime imetnika zasebnega ključa, identifikacijo imetnikovo organizacijo in kontaktne podatke,
- vsebuje možnost enostavnega preverjanja časa izdaje potrdila,
- kreiran je s strani zaupanja vrednega podjetja in ne s strani imetnika samega,
- vsebuje enkratni podatek, s katerim se razlikuje od ostalih izdanih potrdil s strani izdajatelja, tudi za istega imetnika,
- vsebuje možnost enostavnega preverjanja, ali je original ali ponaredek,
- je varen pred nepooblaščenim spreminjanjem podatkov,
- omogoča enostavno in hitro preverjanje ažurnosti podatkov ter
- vsebuje seznam aplikacij, za katere je namenjen.

Najboljši približek danes znanemu idealnemu potrdilu je digitalno potrdilo, torej elektronsko potrdilo, ki temelji na asimetrični (javni) kriptografiji. Je popolnoma digitalen objekt, ki vsebuje podatke o imetniku, kontaktni podatki vsebujejo še njegovo elektronsko pošto, ima vnesen datum veljavnosti potrdila, izda ga zaupanja vredna organizacija[7], ki ga tudi podpiše s svojim potrdilom, in vsebuje naslov, kje se lahko preveri zadnje ažurirano stanje veljavnosti potrdila. Organizacijo imenujemo overitelj javnih ključev. Danes uporabljamo potrdila po standardu X.509 v3. Njihov zapis je opredeljen v dokumentu standardizacijskega telesa ITU-T pod številko X.509 / ISO/IEC 9594-8[8]. Potrdilo vsebuje vsa zgoraj našteta polja z

[7] Slovenski zakon v okviru ZEPEP določa izraz overitelj, to je oseba, ki izdaja potrdila ali izvaja druge storitve v zvezi z elektronskim podpisovanjem.

[8] ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate

zahtevanimi funkcionalnostmi. Polja vsebujejo oznako verzije (1, 2 ali 3, možna tudi morebitna višja verzija), serijsko številko, identifikacijo uporabljenega algoritma za podpisovanje s strani overitelja, ime overitelja v formatu X.500[9], veljavnost, ime imetnika v formatu X.500, informacijo o namenu uporabe, unikatno identifikacijo overitelja in opcijski opis imetnika. Najpomembnejši člen v opisovanju imetnika je razločevalno ime, označeno s kratico DN (angl. Distinguished Name), vsebuje pa imena, naslove, telefone in ostale informacije, s katerim se imetniki potrdil enega overitelja razlikujejo med sabo. Primer razločevalnega imena je naslednji: Country = SI, Organization = SiOL, Common Name = Janez Novak, Employee Number = 023245.

Verzija 3 vsebuje še dodatne informacije, kot so opis politik overitelja, omejitve uporabe, dodatna polja za identifikacijo imetnika ipd. Najpomembnejši dodatek formata v zadnji različici so razširljiva polja za dodatne informacije. Nekatere razširitve so standardne in so že vsebovane v priporočilih in standardih X.509, možnost pa obstaja tudi za lastno kreiranje razširljivih polj. Osnovni namen razširitve standarda je bil zadostiti dodatnim zahtevam po funkcionalnosti, ki so se pokazale sredi devetdesetih let pri prvih večjih sistemih z uporabo asimetrične kriptografije:

- možnost izdajanja več potrdil istemu osebku za uporabo v različnih aplikacijah in za različne namene (npr. glede pooblastil ali funkcij, ki jih ima v podjetju),
- možnost identificiranja uporabnikov po še nekaterih drugih imenih, ne samo imenih, zapisanih v formatu X.500 (npr. naslov elektronske pošte), in
- možnost izdajanja potrdil pod različnimi politikami izdajanja – npr. za varno pošto overitelj preveri le to, da je imetnik potrdila tudi imetnik podanega poštnega predala, medtem ko za uporabo potrdila v poslovnih aplikacijah overitelj dejansko fizično preveri imetnika.

Identifikacija imen se lahko vrši na podlagi poimenovanj, standardiziranih po X.509 v3, poleg tega lahko nastopa informacija o spletnem poštnem naslovu, ime spletne domene, poštni naslov po standardu X.400, ime imenika X.500, ime EDI (angl. Electronic Data Interchange)[10], URI (standardni način naslavljanja virov na svetovnem spletu, angl. Uniform Resource Identifier), spletni naslov IP ipd. Standardne razširitve potrdila se lahko razdelijo v naslednje skupine:

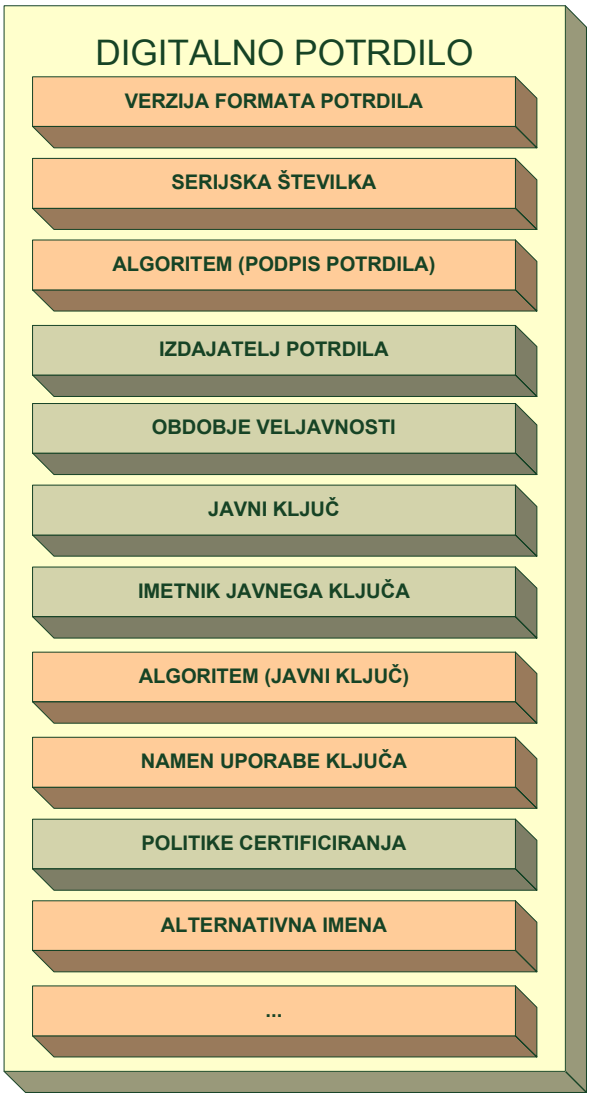
Frameworks, 2001. Prva različica je nastala v letu 1988, druga 1993, zadnja, označena z v3, pa leta 1997, ko so bile dodane nekatere neobvezne razširitve.

[9] Format za imena X.500 se uporablja predvsem za imenike X.500 in za digitalna potrdila verzije X.509 v1 in v2, v precej ohlapnem merilu pa tudi za digitalna potrdila X.509v3. Zadnja verzija ni več strogo povezana s pravili X.500, temveč lahko vsebuje celo vrsto dodatnih poimenovanj.

[10] Starejša verzija elektronskega poslovanja predvsem med kupci in dobavitelji, ki se uporablja že nekaj desetletij. Omejen je bil na zaprta okolja, danes pa obstaja že cela vrsta orodij in ponudnikov storitev, ki znajo pretvarjati formate med datotekami, zapisanimi v XML, in tistimi, ki se uporabljajo v okoljih EDI.

- informacije o ključih (imetnikovih in overiteljevih, kot je npr. predvidena uporaba ključa),
- informacije o politiki (označuje, katera politika overitelja se uporablja),
- vzdevki imetnika in izdajatelja (dodatna imena za identifikacijo, npr. polje Subject Alternative Name, ki je namenjeno vpisu poštnega naslova imetnika),
- omejenost poti potrdil (uporablja se za navzkrižno priznavanje digitalnih potrdil, izdanih s strani različnih overiteljev) in
- dodatki za sezname preklicanih potrdil CRL (angl. Certification Revocation List).

Slika 4 - digitalno potrdilo po standardu X.509v3



Vir: Jerman Blažič, 2001, str. 110

Digitalno potrdilo vsebuje polje, ki označuje datume veljavnosti, pri tem pa overitelj domneva, da se bo potrdilo v tem času dejansko uporabljalo. Vendar je včasih nujno, da pod določenimi pogoji (nepooblaščena odkritost zasebnega ključa pred potekom veljavnosti) overitelj izdano potrdilo prekliče. Samo preklic še ni dovolj, da se izdano potrdilo ne bo uporabljalo še naprej, saj je tehnično še povsem pravilno in uporabno. Treba ga je postaviti na javni seznam. Overitelj mora ob vsakem času vsem uporabnikom omogočiti vpogled v seznam preklicanih potrdil. Najbolj uporabljana metoda za obveščanje o preklicanih potrdilih je periodično izdajanje seznama preklicanih potrdil CRL. Takšen seznam mora biti tudi digitalno podpisan in časovno ožigosan s strani overitelja. Dostop do teh seznamov je omogočen prek spleta na podlagi različnih protokolov (HTTPS, FTP, LDAP in drugih)[11], z uporabo protokola OCSP (angl. On Line Certificate Status) pa se lahko ugotovi status izdanega potrdila tudi v realnem času.

Poleg najbolj razširjenih potrdil v formatu X.509 v3 obstaja še nekaj drugih formatov, ki se uporabljajo za digitalno podpisovanje. Za mobilno podpisovanje se uporabljajo potrdila v formatu WAP WTLS (angl. Wireless Transport Layer Security), že precej časa se uporabljajo potrdila PGP (angl. Pritty Good Privacy), obstajajo še DNSSEC za varnost v DNS, SPKI (angl. Simple PKI) in drugi (Warwick, 2001, str. 238).

Digitalni podpisi temeljijo na asimetrični kriptografiji, kar pomeni, da je za njihovo delovanje potreben par ključev – zasebni in javni. Prvi se uporablja za podpisovanje, drugi za preverjanje podpisov. Nujno je, da imetnik zasebnega ključa poskrbi za njegovo varno hranjenje, tako da nikomur ne uspe priti do njega. Zato je treba biti previden že od samega začetka, torej od trenutka, ko se par ključev šele oblikuje. Priporočljivo je, da je par izdelan na varnem, z varnim programom in za varen algoritem (Klobučar, 2002, str.10). Ker je slabost ključev v tem, da se lahko enostavno kopirajo in je s tem kopija povsem enaka izvirniku, je našteta priporočila vedno treba upoštevati, saj se v nasprotnem primeru lahko zgodi veliko škode. Sredstva, ki se uporabljajo v elektronskem poslovanju danes, v splošnem znajo ustvarjati pare ključev, še vedno pa je na voljo uporaba storitev izdelave parov ključev zunanjih izvajalcev. Slednje ne bi bilo možno, če ne bi obstajal splošni format za zapis ključev in njihovo prenašanje med aplikacijami. Definiran je v dokumentu PKCS#12 (Public Key Cryptography Standard številka 12), ki sodi med splošno uveljavljene standarde podjetja RSA[12], ki so na voljo tudi kot priporočila IETF.

Za shranjevanje zasebnega ključa še dandanes ni razjasnjeno, ali je njegova uporaba na trdem disku računalnika varna ali ne, vsekakor pa je bolje, če se uporabi pametna kartica, strojni kriptografski modul ali pametni ključ. Pri uporabi takšnih varnih medijev zasebni ključ nikoli ne zapusti svojega nahajališča, tako da se ne more kopirati in uporabiti drugje,

[11] Opis se nahaja v slovarčku na koncu magistrskega dela

[12] PKCS #12: Personal Information Exchange Syntax Standard, version 1.0(http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/)

saj poteka podpisovanje vedno na mediju in nikoli ne pride v računalniški spomin, kjer bi se z uporabo posebnih metod lahko napadalec dokopal do njega. Strojni kriptografski moduli (angl. Hardware Security Module, HSM) imajo po navadi vgrajeno najvišjo stopnjo zaščite ključa, namenjeni pa so podpisovanju večjega števila sporočil, ki se generirajo aplikativno in ne zahtevajo ročnega posredovanja. Pametne kartice so namenjene osebni uporabi varnostnih aplikacij. Velike so tako kot kreditne kartice in imajo vgrajen čip, pred vsako uporabo zahtevajo vnos gesla, napredne pa vsebujejo še dodatno varnost na osnovi preverjanja prstnega odtisa imetnika. Še uporabnejši so pametni ključki, ki se priklopijo na računalnik prek vrat USB, njihova zmogljivost pa je primerljiva s pametnimi karticami. Trenutna slabost pri skoraj vseh varnih medijih je v tem, da jih sodobni operacijski sistemi ne prepoznavajo samodejno.

2.2.4 Infrastruktura javnih ključev

Asimetrična (javna) kriptografija je orodje, ki omogoča varnostne operacije, kot so digitalno podpisovanje, šifriranje, razpošiljanje ključev itn. Na voljo je že skoraj 30 let, vendar je pravi razcvet doživela šele v zadnjem času. Razlog je infrastruktura za overjanje javnih ključev (**v nadaljevanju PKI**, angl. Public Key Infrastructure), ki je skupen izraz za niz storitev, programskih vmesnikov, administrativnih orodij in uporabniških aplikacij (Nash et. al, 2001, str. 63). Standardi in priporočila v okviru PKI se stalno nadgrajujejo in izboljšujejo, vendar sami osnovni principi in formati ostajajo nespremenjeni.

Osnovna naloga PKI je vzpostavitev digitalnega subjekta, ki se mu lahko zaupa. To je lahko najboljši prijatelj, zdravnik, sodnik ali zaupanja vredna organizacija , pomembno je, da uporabniki znotraj PKI zaupajo tistemu, ki pooseblja zaupanje. Takšne subjekte se lahko uporablja tako, da skupaj s kriptografskimi in poslovno-operativnimi metodami zagotavljajo varnostne storitve, kot so overjanje, nadzor dostopa, neokrnjenost ipd. Pomembno je, da uporabniki zaupajo subjektu, seveda pa njegova vzpostavitev s tako mero zaupanja ni enostavna naloga. V PKI se takšen subjekt imenuje agencija za overjanje javnih ključev (**v nadaljevanju AC**), včasih poimenovan tudi CA (angl. Certification Authority). AC je tako le eden izmed subjektov, ki so v zakonu določeni kot overitelji. AC ni le programska oprema, ki izdaja potrdila, temveč veliko več.

Standard X.509 definira format potrdil, polja znotraj njih in postopek razpošiljanja javnih ključev. Je zelo splošen in pušča mnogo odprtih vrat pri vsakdanji uporabi. Zato so že leta 1995 znotraj delovne skupine za internetsko inženirstvo, **v nadaljevanju IETF**, ustanovili delovno skupino, ki se ukvarja z definiranjem niza profilov potrdil, ki bi bili primerni za uporabo v svetovnem spletu. Skupina se je poimenovala PKIX (angl. Public Key Infrastructure X.509)[13]. Izdali so standarde, ki opisujejo standard X.509: oblika potrdila in seznama preklicanih potrdil (RFC 2459), protokol za dostop do seznama LDAP v2 za

[13] Rezultat dela delovne skupine PKIX se nahaja na spletnem naslovu http://www.ietf.org/html.charters/pkix-charter.html.

shranjevanje potrdil in seznamov CRL (RFC 2587), oblika kvalificiranega potrdila (RFC 3039) in okvirni program za politike in prakse izdajanja potrdil (RFC 2527). Že na začetku svojega delovanja so se začeli ukvarjati tudi z izdelavo popolnoma novih standardov, ki so potrebni za vzpostavitev in delovanje PKI na internetu: protokol za upravljanje s potrdili CMP (RFC 2510), protokol za preverjanje statusa potrdila v realnem času OCSP (RFC 2560), format za poizvedbo po upravljanju potrdil CRMF (RFC 2511), protokol za časovno žigosanje (RFC 3161), sporočanje o upravljanju potrdil (RFC 2797), protokol za časovno žigosanje infrastrukture javnih ključev (RFC 3161) in uporaba protokola za prenos datoteke prek svetovnega spleta FTP in HTTP za prenašanje aktivnosti na PKI (RFC 2585). Trenutno se ukvarjajo z razširitvijo svojega dela tudi na druga področja.

Elementi, ki sestavljajo infrastrukturo javnih ključev, so natančno določeni v standardih PKIX, s katerimi lahko organizacije postavijo lokalno infrastrukturo javnih ključev ali razširijo obstoječe. PKIX jih opisuje na naslednji način:

- Agencija za overjanje AC je odgovorna je za izdajanje in upravljanje digitalnih potrdil končnim uporabnikom (imetnikom). Potrdila povezujejo identiteto imetnika potrdila, ki je prikazana znotraj imenskih polj, javni ključi (ki je tudi del potrdila) in zasebni ključ, ki ga ima imetnik varno shranjenega pri sebi. AC je odgovorna tudi za celotni življenjski ciklus potrdil, kar pomeni, da mora imeti na voljo podatke o statusu vseh izdanih potrdil. Agencij je več vrst, od korenskih (vrhovnih,t. i. Root CA) do vmesnih, končnih ipd.

- Agencija za registracijo AR je ponekod del AC, priporočljivo pa je, da je samostojna enota. Ukvarja se z administrativnimi opravili, povezanimi z registracijo bodočega imetnika potrdila v AC. Delo je v zelo tesni povezavi s politiko certificiranja AC, v splošnem pa je to naslednje: osebno overjanje imetnika, verifikacija pravilnosti vnesenih podatkov, preverjanje dejanskega lastništva zasebnega ključa imetnika, dodelitev imen v skladu s politiko, izdelava para ključev ipd.

- Skladišče podatkov se uporablja za javno shranjevanje potrdil in seznamov CRL. V začetku uporabe PKI se je uporabljal za dostop do imenika X.500 protokol DAP (angl. Directory Access Protocol), sedaj pa predvsem imenik LDAP (angl. Light Directory Access Protocol).

- Imetniki potrdil so lahko končni uporabniki ali strežniki.

PKIX v svojih dokumentih identificira osnovne funkcije infrastrukture javnih ključev:

- Registracija – bodoči imetnik potrdila se mora najprej registrirati pri overitelju. To lahko stori prek agencije za registracijo AR ali kar neposredno pri AC, če le-ta sočasno izvaja tudi dela AR. Imena in vsi ostali atributi, ki so del potrdila in jih ostali upoštevajo, morajo biti preverjeni s strani AR v skladu s politiko certificiranja AC.

- Začetek – sem je všteto definiranje začetnih vrednosti, preden se komunikacija med bodočim imetnikom potrdila in AC oziroma AR začne.

- Overjanje – AC izda potrdilo imetnikovim javnim ključem in ga vrne imetniku oziroma ga objavi v javnem imeniku.

- Obnovitev para ključev – ključi, ki so namenjeni šifriranju oziroma prenosu ostalih ključev, so lahko arhivirani, tako da se ob ustreznem postopku tudi pozneje ponovno izdajo. Takšna funkcija mora biti usklajena s politiko AC, ki mora obnovitev dovoljevati.

- Izgradnja para ključev – AC lahko omogoča izgradnjo zasebnega ključa na strani bodočega imetnika potrdila ali na strani overitelja. V slednjem primeru mora AC zagotoviti tudi varen prenos k imetniku.

- Osveževanje ključa – PKIX pričakuje redno osveževanje potrdil, naj si bo po preteku veljavnosti (vsako potrdilo je izdano za določen čas) ali v primeru predčasnega razkritja zasebnega ključa. Vsi postopki, potrebni za ponovno izdajo potrdil, sodijo v to kategorijo, podobno tudi lastna potrdila AC.

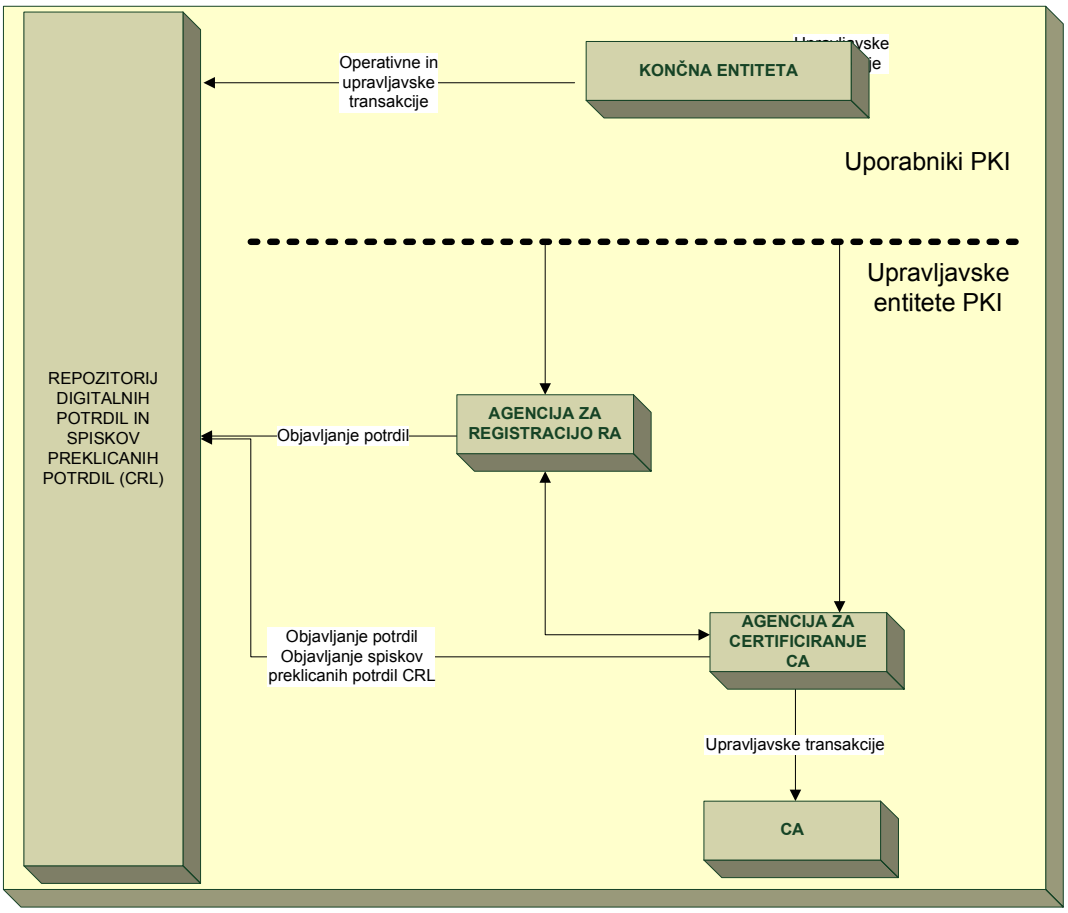
- Navzkrižno certificiranje – AC lahko izda drugi AC navzkrižno potrdilo, s katerim priznava vsa njena potrdila.

- Preklic potrdila – AC je dolžna vzdrževati statuse izdanih potrdil, kar povzema periodično izdelavo in objavo seznama preklicanih potrdil CRL in podporo za obstoječe (OCSP) in prihajajoče standarde za izmenjavo informacij o statusu izdanih potrdil.

- Razpošiljanje oziroma objavljanje potrdil in preklicev – AC je dolžna razpošiljati izdana potrdila in sezname CRL.

Delovna skupina PKIX je pripravila specifikacije, ki opisujejo arhitekturni model PKI, prikazan na sliki Slika 5, in se lahko razvrstijo v več področij, ki jih pokrivajo. Najpomembnejši del je opis potrdila v formatu X.509, predvsem njegova razširljiva polja. Zaradi ustreznega medsebojnega delovanja različnih proizvajalcev opreme so ta polja natančno določena in omejena, vsako je opisano kot »obvezno«, »opcijsko« ali »prepovedano«. Poleg opisa potrdila specifikacije zavzemajo področje operativnih protokolov (kako se izdana potrdila in seznami CRL dostavljajo končnim uporabnikom ali aplikacijam), upravljavskih protokolov (kako različne entitete PKI komunicirajo med sabo), osnutkov politik in storitev za časovno žigosanje in preverjanje podatkov (okvirni program za bodoče zaupanja vredne ponudnike storitev).

Slika 5 - Arhitekturni model PKI



Vir: IETF, 2004

Standardizacija protokolov in specifikacij, ki jih izdaja delovna skupina PKIX, skupaj z dodanimi priporočili in osnutki, omogoča proizvajalcem opreme razvoj različnih strojnih in programskih rešitev, ki lahko delujejo znotraj obstoječih infrastruktur javnih ključev, kjer so vključene entitete, delujoče na osnovi opreme drugih proizvajalcev. Brez tega to ne bi bilo mogoče.

2.2.5 Arhiviranje

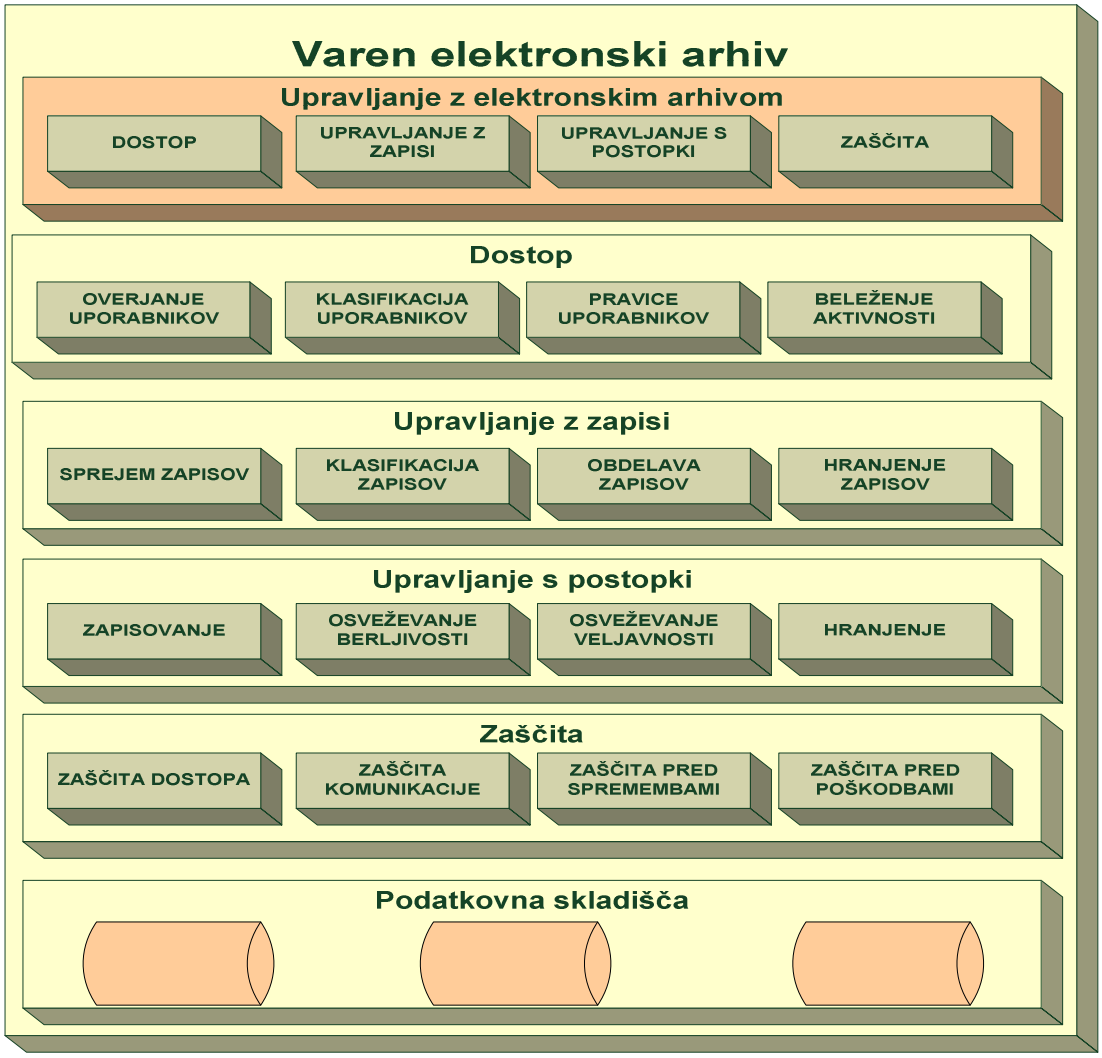
ZEPEP določa, da je treba hraniti dokumente v takšni obliki, kot so bili prejeti. To pomeni, da vsi napori, ki spremljajo podjetja pri njihovi težnji k preslikavi procesov v elektronsko obliko, prinesejo tudi zahtevo po vzpostavitvi elektronskega arhiva oziroma po uporabi storitve pri ponudnikih elektronskega arhiviranja, ko bodo le-ti sploh začeli to sploh ponujati. Poslovni subjekti so zavezani k hranjenju poslovnih zapisov, ki so lahko evidentni ali dokazni material za določeno obdobje v skladu z zakonodajo. Problem pa ni samo uporaba, temveč spremenjen način arhiviranja in postopkov, povezanih s tem. Logika arhiviranja ne temelji več na vzdrževanju in ohranjanju nosilcev z zapisanimi sporočili, temveč na

vzpostavljanju, vzdrževanju in razumevanju kontekstov, v katerih so zapisi nastali ali bili uporabljeni (e-Slog, 2004, str. 7).

Arhiviranje je postopek, s katerim se dokumentarno in arhivsko gradivo prevzema, hrani, vzdržuje, obdeluje in uporablja v arhivu poslovnega subjekta ali posameznika. Ker zapisi niso več le papirni, temveč tudi digitalni (pisna oblika predstavljena v elektronski obliki) oziroma elektronski, so se začeli vzpostavljati tudi elektronski arhivi. Elektronske in digitalne zapise namreč spremljajo tudi številni opisni elementi in atributi (t. i. metapodatki), spremenile pa so se tudi možnosti nepooblaščenega spreminjanja, brisanja in drugih dejanj, ki brišejo revizijsko varne sledi v arhivih.

Elektronski arhivi so zelo kompleksni sistemi, namenjeni dolgoročnemu hranjenju elektronskih zapisov. Na eni strani se ukvarjajo s problemom ohranjanja berljivosti (10 let je dolga doba v računalništvu, kar pomeni, da se lahko v tem času format sporočila spremeni oziroma ni kompatibilen za nazaj), na drugi pa z upravljanjem arhiviranih zapisov. Funkcionalna zgradba, ki natančno opredeljuje elektronski arhiv, je prikazana na sliki:

Slika 6 - Funkcionalna zgradba varnega elektronskega arhiva



Vir: e-Slog, 2004, str. 4

Priporočil in standardov, ki bi v celoti opredeljevali vzpostavitev in upravljanje z elektronskimi arhivi, trenutno še ni na voljo, obstaja pa nekaj specializiranih priporočil, od katerih vsako opredeljuje svoj del. Delimo jih lahko na standarde za elektronske arhive (ISO 15489, AS 4390, OAIS, TAP), za hranjenje vsebine (XML, PDF), za zaščito elektronskih dokumentov (ES, SSL, TS, CRL, OCSP) in na standarde za ohranjanje veljavnosti digitalnih podpisov (DVCS, TSP, ES-X). Podrobnejši opis vseh omenjenih protokolov se nahaja v Tehničnih priporočilih za varno arhiviranje elektronskih dokumentov (e-Slog, 2004, str. 11–13). V omenjenem dokumentu se nahaja tudi kontrolni seznam, namenjen praktičnemu preverjanju zahtev, ki jih mora izpolnjevati elektronski arhiv.

2.3 Elektronsko poslovanje v slovenski in evropski pravni ureditvi

2.3.1 Izmenjava elektronskih sporočil

V informacijski družbi je vse več legalnih dejanj izvedenih v elektronski obliki. Jasno je, da nima smisla uporabljati elektronskega podpisovanja, če lokalna zakonodaja ne prepoznava elektronskih podpisov. S prepoznanjem je mišljeno predvsem to, da zakonodaja pripisuje neki pravno-formalni učinek elektronskemu podpisu, npr. da pod določenimi pogoji izenačuje elektronski in lastnoročni podpis ali da je elektronski podpis dokaz pristnosti v zakonskih procedurah. V preteklosti večina zakonodaj ni pripisovala elektronskim podpisom nobene veljave, vendar je z naraščanjem elektronskega trgovanja in poslovanja kot posledice podjetniške uporabe interneta postalo vse bolj očitno, da informacijska družba potrebuje ustrezno zakonodajo na področju elektronskega podpisovanja, ki bi sledila razvoju elektronskega poslovanja.

2.3.2 Varen elektronski podpis, potrdila in kvalificirana potrdila

Pravna veljavnost digitalnih podpisov in elektronskega poslovanja se razlikuje od države do države. Prvi zakon je bil sprejet v Združenih državah Amerike, v zvezni državi Utah leta 1995, potem pa so do danes že skoraj vse razvite države sprejele zakonodajo na področju elektronskega poslovanja in podpisa. Ustrezno z velikansko hitrostjo širjenja interneta so se praviloma sprejemale tudi nacionalne zakonodaje, ki so bile narejene in sprejete precej hitreje kot drugi pomembni zakoni. Prva ustanova, ki se je na mednarodni ravni spopadla z elektronskim poslovanjem in posledično tudi z elektronskim podpisom, je Komisija Združenih narodov za mednarodno gospodarsko pravo UNCITRAL (United Nations Commision on International Trade Law). Leta 1996 je izdala vzorčni model zakona s področja elektronskega poslovanja s priporočilom o njegovi uzakonitvi[14]. Namenjen je olajšanju uporabe modernih tehnik pri komunikaciji in shranjevanju podatkov, kot je komunikacija na podlagi protokola EDI (Electronic Data Interchange), elektronske pošte ali daljinskega kopiranja, z ali brez uporabe interneta. Temelji na želji po vzpostavitvi funkcionalnega ekvivalenta papirnih konceptov – podpis, original, pisni format. Poleg tega vsebuje še pravila za specifična področja elektronskega poslovanja, kot je npr. dostava blaga. Leta 2001 je UNCITRAL izdal še en vzorčni zakon[15], imenovan UNCITRAL-ov vzorčni model elektronskih podpisov, ki je na podlagi predhodnega, predvsem njegovega 7. člena, podal dodatna pravna zagotovila, s katerimi se lahko elektronski podpisi izenačujejo z ročnimi, seveda le če so izpolnjeni določeni pogoji. Vzročni model sledi tehnološko nevtralnemu pristopu in se strogo izogiba priporočanju uporabe specifičnega tehničnega izdelka ali tehnologije. Definira še osnovna pravila glede elektronskega poslovanja z uporabo elektronskih podpisov in obveznosti ter odgovornosti vseh udeležencev –

[14] UNCITRAL Model Law on Electronic Commerce with Guide to Enacment (1996) z dodatkom, sprejetim leta 1998, dosegljiv na naslovu http://www.uncitral.org/en-index.htm.

[15] UNCITRAL Model Law on Electronic Sigantures (2001), dosegljiv na naslovu http://www.uncitral.org/en-index.htm.

podpisnika, prejemnika in zaupanja vrednih tretjih oseb, ki lahko pozneje po potrebi posredujejo v procesu podpisovanja.

Najvažnejši predpis, ki je bil sprejet v Evropski uniji na področju elektronskega podpisa, je smernica EU 1999/93/EC Evropskega parlamenta, sprejeta 13. decembra 1999, poimenovana Okvirni program skupnosti za elektronsko podpisovanje[16] (v nadaljevanju **Smernica**). Nastala je na podlagi predhodnega dokumenta Evropske komisije[17], ki je poudarjal pomen združljive infrastrukture za nadaljnji razvoj elektronskega poslovanja v regiji in potrebo po ureditvi pogojev ter pravno-formalnih zahtev na tem področju. Pred tem je bilo sprejetih že nekaj zakonov na državnih ravneh (Nemčija leta 1997, Italija, Avstrija itd.), zato je bilo sprejetje Smernice nujno, saj se je le s tem postavila osnova za sprejemanje čim bolj usklajenih zakonov na nacionalnih ravneh. Smernica je članicam Evropske unije podala tudi rok, do katerega so morale sprejeti nacionalno zakonodajo z omenjenega področja, to je 19. julij 2001, bolj ali manj pa so temu roku in navodilom sledile tudi ostale države (kandidatke za EU, neodvisne države, ostale zainteresirane države).

Namena Smernice sta dva:

- pospešiti uporabo elektronskih podpisov in prispevati k njihovemu legalnemu prepoznanju ter
- vzpostavitev legalnega okvirnega programa za elektronske podpise in nekatere overiteljske storitve z namenom zagotovitve pravilnega funkcioniranja internega trga.

Smernica vsebuje še štiri anekse. **Aneks 1** definira kvalificirano potrdilo, **Aneks 2** pogoje za delovanje agencije za certificiranje AC, ki izdaja kvalificirana potrdila, **Aneks 3** definira pogoje za napravo, s katero se izdelujejo kvalificirani podpisi, **Aneks 4** pa predpisuje načine za preverjanje kvalificiranega podpisa.

Smernica je napisana zelo preudarno, saj ne predpisuje celovito regulativo elektronskih podpisov, temveč se ukvarja predvsem s pospeševanjem njihove uporabe in ne želi predpisati njihove zakonske prepoznavnosti v nacionalnih zakonih, temveč želi pri tem le »prispevati« in urediti področje. Pomembna je še njena vloga pri vzpostavitvi enovitega evropskega legalnega okvirnega programa na področju elektronskega podpisa, saj se je le tako dalo izogniti nasprotovanjem med različnimi nacionalnimi zakoni s tega področja. Ukvarja se z izdajatelji digitalnih potrdil in njihovo vsebino, precej manj pa z ostalimi storitvami, ki sodijo v delovne naloge zaupanja vrednih tretjih oseb, kot so npr. agencije za časovni žig,

[16] Directive 1999/93/EC of the Eurpoean Parliament and the Council of 13th december 1999 on a Community Framework for Electronic Signatures.

[17] Towards an European Framework for Digital Signatures and Encryption of 1. december 1997.

elektronski notarji itn. Smernica ne določa navodil za spreminjanje obstoječih nacionalnih zakonov na področju pogodbenega prava. Prav tako daje izrazito prednost tistim zakonom, ki predpisujejo uporabo točno določenih obrazcev, hkrati pa ne predvidevajo in zato ne dovolijo uporabe elektronskih obrazcev ali arhiviranja elektronskih obrazcev – v takšnih primerih se elektronski podpisi ne morejo uporabljati. Smernica tudi ločuje uporabo elektronskih podpisov glede na okolje. V določenih primerih, predvsem tam, kjer se pogodbene stranke same dogovorijo o načinu poslovanja, regulativni okvirni program ni potreben in se ne uporablja. To se nanaša predvsem na zaprta okolja, kot je npr. bančno okolje, intranet, navidezna zasebna omrežja itn.

Osnovna načela, na katerih sloni Smernica, so:

- pravno-formalna prepoznavnost elektronskih podpisov,
- tehnološka neodvisnost,
- prosti pretok izdelkov in storitev,
- prepoved predhodnega nadzora dostopa ali sheme licenciranja za ponudnike storitev overjanja oziroma agencij za certificiranje (AC),
- določanje sheme nadzorovanja za AC in
- priporočanje nadzorovanja prostovoljne sheme pooblaščanja.

Smernica prinaša nove definicije, ki se uporabljajo v evropskem prostoru:

- elektronski podpis (podatki v elektronskem formatu, ki so dodani in logično povezani z drugimi elektronskimi podatki in služijo kot metoda za overjanje; to je zelo splošen opis in zavzema vse vrste tehnologij za kreiranje podpisov),
- overitelj AC,
- podpisnik (oseba, ki ima v rokah napravo za izdelavo podpisa in deluje v svojem ali drugem imenu),
- napredni elektronski podpis (elektronski podpis z nekaterimi dodatnimi pogoji),
- podatki za kreiranje in preverjanje podpisov,
- naprava za kreiranje in preverjanje podpisov,
- kvalificirano potrdilo (potrdilo, ki ustreza zahtevam v Aneksu 1 Smernice, in je bilo izdano s strani AC, ki deluje ustrezno z zahtevami Aneksa 2 Smernice) in
- kvalificiran podpis.

V tretjem in delno četrtem poglavju Smernice se nahajajo navodila za trg storitev overjanja, natančneje z opredelitvijo agencij za overjanje AC. Predstavljeno je načelo državnega porekla, ki pravi, da se mora AC držati zakonodaje tiste države, v kateri je ustanovljena. Če svoje storitve ponuja tudi zainteresiranim na zunanjem trgu, ji ni treba upoštevati lokalne zakonodaje vsake države. Smernica prepoveduje državno licenciranje za izvajanje overiteljskih storitev, priporoča pa prostovoljno akrediticijsko shemo z namenom povečanja kakovosti delovanja AC. Vsaka država mora na svojem ozemlju vpeljati in vzdrževati sistem za nadzor AC, ki izdajajo kvalificirana potrdila javnosti, torej takšna potrdila, ki ustrezajo zahtevam Aneksa 1 Smernice in so izdana s strani AC, kar ustreza zahtevam Aneksa 2. Smernica v 4. poglavju definira še princip svobodnega pretoka izdelkov s področja elektronskega podpisovanja. Izdelki, ki ustrezajo Smernici, se lahko prosto uporabljajo znotraj internega trga, takšen primer pa je pametna kartica, ki vsebuje zasebni ključ in algoritem za digitalno podpisovanje.

Najpomembnejše poglavje Smernice je 5. poglavje, ki se ukvarja z legalnimi posledicami elektronskih podpisov. Dolgo časa je bilo nejasno, kako bodo sodišča znotraj članic Evropske unije in ostalih zainteresiranih držav upoštevala veljavnost elektronskih podpisov. Vprašanj o tem, ali bo sodišče upoštevalo ovrgljivo domnevo, da je bil elektronski dokument, na katerega je določena oseba dodala svoj elektronski podpis, podpisan s strani te osebe, dokler se ne dokaže drugače, ali kakšno dokazno vrednost bodo dajali elektronskim podpisom, je bilo veliko. S tem poglavjem Smernice se je deloma preprečilo, da bi sodišča vsake države odgovarjala na takšna vprašanja različno. Tako obstajata dve kategoriji elektronskih podpisov:

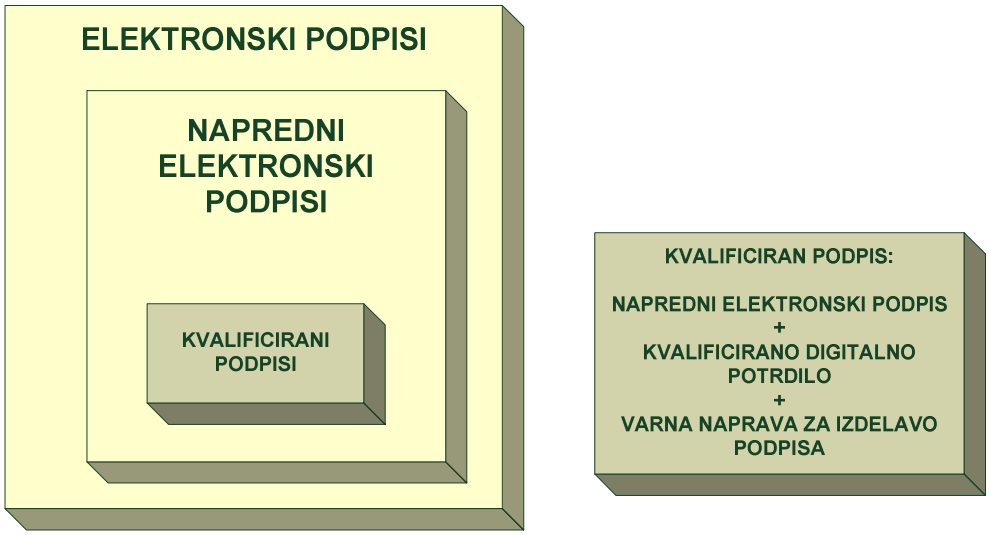
- napredni elektronski podpisi, ki so osnovani na kvalificiranih potrdilih in narejeni z varnimi napravami za izdelavo podpisa, skladnimi z Aneksom 3 Smernice in
- ostali elektronski podpisi.

Napredni elektronski podpisi se lahko poimenujejo tudi digitalni podpisi, saj asimetrična kriptografija tehnično ustreza zahtevam Smernice. Ostale lastnosti digitalnega podpisa so:

- prejemnik lahko preveri identiteto avtorja podpisanega sporočila,
- digitalni podpis je vedno kreiran s sredstvom, ki ohranja podpisovanje sporočila pod kontrolo podpisnika,
- povezan je s podpisanim sporočilom, saj se naredi prstni odtis sporočila na osnovi zgoščevalne funkcije,
- vsaka sprememba podpisanega sporočila se takoj opazi in
- digitalni podpis je nedvoumno povezan z zasebnim ključem, na katerem je osnovan.

Na osnovi Smernice so morale vse članice in ostale zainteresirane države zagotoviti, da vsi napredni elektronski podpisi v relaciji s podatki v elektronski obliki ustrezajo pravno-formalnim zahtevam na enak način kot lastnoročni podpisi v relaciji s podatki na papirju in da so sprejemljivi kot dokaz v pravnih postopkih.

Slika 7 - vrste podpisov



Osnovni pravno-formalni predpis Smernice je, da imajo pravne posledice vsi elektronski podpisi. Pravno-formalno vprašanje je tudi odgovornost izdajatelja digitalnih potrdil (AC). Na tem področju je Smernica dala nekaj usmeritev.

Kvalificirana potrdila, ki jih izda AC znotraj Evropske unije, so po navodilih Smernice prepoznavna v vseh državah članicah, pod določenimi pogoji pa tudi tista, ki so izdana v drugih državah. Možnosti so prostovoljna akreditacija AC v kateri od članic, garancija za potrdila s strani AC v Evropski uniji ali izdaja AC, ki je nastala na osnovi bilateralnega sporazuma med državo članico in drugo državo.

Posebno vprašanje je še zagotavljanje zasebnosti pri digitalnih potrdilih. Na njih so lahko osebni in ostali podatki imetnika, vidni ali shranjeni pri AC. V določenih primerih mora AC shranjevati še zasebni ključ vseh imetnikov ... Smernica na tem področju zahteva zbiranje le tistih podatkov, ki so nujno potrebni za izdajanje in upravljanje s potrdili.

2.3.3 Implementacija Smernice v Evropi

Članice EU in nekatere ostale zainteresirane države (kandidatke, Švica, tudi ostale države) so bolj ali manj zvesto prenesle navodila Smernice v nacionalne zakonodaje, s tehničnega vidika pa je jasno, da je Smernica vplivala na ne samo evropska, ampak tudi mednarodna standardizacijska telesa, predvsem z določanjem terminov, ki se uporabljajo v pravno-

formalnem in tehničnem jeziku. Tudi vsebina se je v grobem pravilno prenesla, resnica pa je, da so si države različno interpretirale nekatere vsebinske usmeritve, predvsem v praktični uporabi pravil.

Poročilo o zakonskih in tržnih vidikih aplikacije Smernice in praktičnih aplikacij elektronskih podpisov v članicah in ostalih zainteresiranih državah, ki je bilo pripravljeno po naročilu Evropske komisije, je ugotovilo naslednje (Dumortier et.al, 2003, str. 4–8):

- Princip nediskriminacije elektronskih podpisov je bil prevzet s strani večine nacionalnih zakonodajnih teles, v nekaterih državah zelo natančno, v nekaterih pa malo nejasno oziroma nenatančno. Uporaba principa se bo zaradi majhne dejanske prakse pokazala šele v prihodnosti, tako da se priporoča nadaljnje nadziranje.

- Pravni učinek kvalificiranih elektronskih podpisov je vsepovsod izenačen (razen v nekaterih izjemah) z lastnoročnimi podpisi.

- Nadzorne sheme za AC, ki izdajajo kvalificirana potrdila, so uveljavljene v vseh opazovanih državah, njihova vloga in razvitost pa je precej odvisna od števila lokalnih AC in izdanih potrdil, torej dejanske uporabe digitalnih podpisov.

- Pogoj za izvedbo kvalificiranega elektronskega podpisa je upoštevanje Aneksov 1–3. Implementacija prvega aneksa je zelo podobna v vseh državah, drugi pa precej niha od države do države. Pogoji za AC so nekje strožji kot drugje, kar lahko v prihodnosti prinese težave tistim AC, ki se bodo želeli akreditirati v različnih državah, proizvajalcem opreme in implemenatorjem. Poročilo priporoča Komisiji, da identificira takšne nepotrebne zahteve in priporoča njihovo izločitev. Tretji aneks je prav tako različno implementiran, saj obstajajo po državah različni kriteriji glede naprav za varno kreiranje in preverjanje podpisov.

- Glede odgovornosti AC so se v nacionalne zakonodaje vnesle usmeritve, podane v Smernici, ponekod so uvedli le še nekaj dodatnih, strožjih predpisov.

- Kvalificirana potrdila, ki so izdana v tujih AC, se lahko uporabljajo v skladu s Smernico tudi v vseh opazovanih državah, nekatere države pa sploh ne ločujejo med domačimi in tujimi potrdili.

Število nadzirajočih in akreditiranih AC v Evropi se zelo razlikuje, v nekaterih državah ni nobenega ali eden, ponekod, npr. v Sloveniji, jih je več. Število izdanih kvalificiranih potrdil je zelo povezano z nekaterimi državnimi zahtevami, saj naravnih zahtev po njih dejansko še ni. Največ takšnih potrdil se danes uporablja v elektronskem bančništvu, a je takšna aplikacija digitalnih potrdil zunaj področja delovanja Smernice (zaprto uporabniško okolje). Dejanska uporaba kvalificiranih potrdil je še vedno zelo majhna in omejena predvsem na storitve javnih uprav. Prav tako je zelo zanimivo, da veliko upraviteljev spletnih aplikacij razume narobe, da so edina potrdila in z njimi narejeni elektronski podpisi, ki imajo pravno

veljavo, kvalificirana potrdila, kar vodi v velike stroške in kompleksnost pri izgradnji aplikacij in njihovi uporabi.

Trenutno predstavlja poseben problem pomanjkanje medsebojnega delovanja različnih storitev z uporabo potrdil, izdanih s strani različnih ponudnikov opreme, kar je povzročilo, da zdaj obstaja cela vrsta okolij, v katerih druga potrdila tehnično ne delujejo. Del krivde je treba zapisati tudi raznim standardizacijskim telesom, ki so počasneje pripravljala standarde, kot jim je naročila Evropska komisija. Več o tem se nahaja v poglavju 3.1.4, kjer so standardizacijska telesa (npr. EESSI) opisana skupaj z njihovim opravljenim delom na tem področju.

2.3.4 Elektronsko poslovanje in elektronski podpis v slovenski pravni ureditvi

Republika Slovenija je leta 2000 sprejela Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/00), ki je začel veljati 22. 7. 2000. Pozneje je bil sprejet še podzakonski predpis, ki ureja tehnične pogoje za delovanje AC, za elektronsko podpisovanje in pogoje za elektronsko poslovanje v javni upravi[18]. Zakon je bil narejen tako, da je večina določb usklajena s smernicama Evropske unije, ki urejata elektronski podpis (Smernica) in elektronsko poslovanje [19] (v nadaljevanju **Smernica o elektronskem poslovanju**), upoštevan pa je tudi že omenjeni UNCITRAL-ov Vzorčni zakon o elektronskem poslovanju. Prvo osvežitev je zakon doživel leta 2004, ko je vlada RS potrdila Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu (Ur. l. RS, št. 25/2004), v nadaljevanju **ZEPEP-A**.

Za varstvo veljavnosti pravnega posla in uporabo nepravilne oblike, ki ima rezultat v ničnosti pravnega posla ali vsaj izpodbojnost, številne zakonske določbe v Sloveniji vsebujejo zahtevo po določeni obliki dokumenta, kjer prevladuje papirna oblika (Ilešič et. al., 2001). To področje ureja ZEPEP, vendar za zdaj le za nezahtevne oblike dokumentov, zahtevnejše, kot so notarski zapis ali prisotnost prič, pa ne. Vsaka **elektronska oblika dokumenta** ni vedno enakovredna dokumentu na papirju, ker ni možno vedno v elektronski obliki zagotoviti vseh lastnosti, ki jih ima zapis podatkov na papir. ZEPEP določa dva pogoja, po katerih je možno ob njunem izpolnjevanju pravnoveljavno enačiti papirno z elektronsko obliko dokumenta:

- podatki morajo biti dosegljivi tudi po preteku daljšega obdobja od njihovega zapisa, kar vključuje zagotavljanje mehanizmov za njihovo varno shranjevanje, in

[18] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS št. 77/00 in 2/2001).

[19] Directive 2000/31/EC of the European Parliament and the Council of 8th June 2000 on certain aspects on Information Society Services, in particular Elektronic Commerce, in the Internal Market.

- podatki morajo biti primerni tudi za kasnejšo uporabo, pri čemer se morajo upoštevati mogoče bistvene spremembe pri strojni in programski opremi po določenem času.

Tako je zagotovljeno, da tudi v elektronskem svetu veljajo enaka pravila obligacijskega prava kot pri papirni obliki. Pri tem se upošteva še dejstvo, prav tako opisano v ZEPEP, da se v elektronskem svetu ne ločuje med izvirnikom in kopijami, ker jih preprosto ni mogoče ločevati.

Poleg oblike je zelo pomembno tudi področje elektronskega sporočanja[20], pri čemer je v ospredju predvsem dvoje: podvajanje elektronskih sporočil in potrjevanje prejema sporočila. Pri podvajanju zakonodaja ločuje več enakih sporočil, ki se morajo obravnavati ločeno in več enakih sporočil, ki so nastala kot posledica napake v informacijskem sistemu. Prejemnik je dolžan šteti vsako prejeto sporočilo, tudi enake, razen če ve ali bi moral vedeti (če bi ravnal kot skrben gospodar), da je po pomoti prejel več enakih. Zakon določa, da se podobno kot pri klasičnem tudi pri elektronskem pošiljanju lahko zahteva potrditev prejema sporočila.

Osnovna načela, ki jih ZEPEP prinaša, so:

- načelo nediskriminacije elektronske oblike,
- načelo odprtosti oziroma tehnološke nevtralnosti,
- načelo dvojnega pristopa,
- načelo pogodbene svobode (avtonomije) strank,
- načelo varstva podatkov,
- načelo mednarodnega priznavanja in
- načelo varstva potrošnikov.

Celoten zakon je sestavljen iz pet poglavij. V **prvem poglavju** se nahajajo splošne določbe zakona in področje urejanja. Pri tem je predlagatelj zakona veliko pozornost namenil uporabi slovenskih izrazov, kjer se je kar najbolj držal usklajene slovenske informacijske terminologije. Na samem začetku je nakazana razlika med podatki v elektronski obliki in med elektronskimi sporočili; slednja so ločena na sprejeta ali poslana. Med pomeni izrazov se nahajajo še opisi elektronskih podpisov, varnih elektronskih podpisov, časovnih žigov in subjektov pri prometu z elektronskimi sporočili: pošiljatelja, naslovnika, prejemnika, posrednika in podpisnika. Definirani so še informacijski sistem, sredstva in podatki za elektronsko podpisovanje ter preverjanje elektronskega podpisa, potrdilo, kvalificirano

[20] Sporočanje v elektronski obliki (elektronska pošta, računalniška izmenjava podatkov...).

potrdilo in na koncu overitelj, ki takšna potrdila izdaja. V istem poglavju je podana še svoboda strank pri urejanju medsebojnih razmerij, obenem pa zakon določa, da ne velja za obstoječe in prihodnje zaprte informacijske sisteme, ki delujejo (ali bodo delovali) med znanimi udeleženci. S 4. členom želi zakon preprečiti, da bi se podatkom v elektronski obliki odrekel pravni učinek oziroma da bi se jim v pravu zmanjšala teža kot drugim oblikam podatkov, npr. pisnim virom, izpovedim prič ipd.

Drugo poglavje ima naslov Elektronsko poslovanje. Navkljub zelo splošnemu naslovu se zakon ne ukvarja z vsemi pravnimi vprašanji, povezanimi z elektronskim poslovanjem, saj se jih precej že ureja ali se jih še bo z drugimi področnimi zakoni (npr. Zakon o upravnem postopku ZUP s celovitimi rešitvami za elektronsko poslovanje v upravnih zadevah). Poglavje je ločeno na dva dela: prvi govori o elektronskem sporočilu, drugi pa o elektronskih podatkih. Definirani so pošiljatelji, prejemniki, elektronske povratnice ter pravne (ali ni bolje: domneve) glede časa in kraja pošiljanja ter prejema elektronskega sporočila. Osnova za prvi del je UNCITRAL-ov Vzorčni zakon o elektronski trgovini (UNCITRAL, 1996), zakonodajalec pa se je pri tem želel čim bolj distancirati urejanju obligacijskih in drugih zasebnopravnih razmerij in ustvariti predvsem most med dosedanjimi pravnimi instrumenti in novimi tehnologijami. Vseeno je ZEPEP precej posegel v civilnopravne oziroma pogodbene odnose strank. Na svetovnem spletu sta danes poznana predvsem dva načina sklepanja e-pogodb:z izmenjavo elektronske pošte in z uporabo pogodb na zaslonu. Primer prvega sklepanja je pošiljanje ponudbe po elektronski pošti, ki jo kupec sprejme z odgovorom na poslano elektronsko pošto. Drugi način se sklene s klikom na gumb v brskalniku, poimenovan »strinjam se«.

Elektronski podpis je v marsikateri evropski državi opredeljen z zakonom, saj je bila leta 1999 izdana že opisana Smernica, na podlagi katere so države sprejemale lokalno zakonodajo. Slovenija je to vključila v ZEPEP kot eno zaključeno celoto, ki se nahaja v **tretjem poglavju**. Najprej je definirana nediskriminacija in pravna teža elektronskega podpisa, v celoti usklajena s Smernico. Če je elektronski podpis varen in overjen s kvalificiranim potrdilom, je enakovreden lastnoročnemu podpisu, vsem drugim elektronskim podpisom pa lahko sodišče ali drug organ prizna enako ali manjšo težo (ali sploh ne prizna pravnega učinka), vendar nikoli na podlagi diskriminacijskih podlag, definiranih v 14. členu zakona. V nadaljevanju zakon podrobneje ureja delovanje overiteljev, ki so prvi pogoj za uporabo infrastrukture elektronskih podpisov. Uveden je tako imenovan dvojni pristop, ki dovoljuje delovanje overiteljev na podlagi priglasitve. Omogočeno jim je delovanje pod različnimi pogoji in s tem so jim dani različni pravni učinki njihovih izdanih digitalnih potrdil. Nekaj členov se ukvarja še z obveznim nadzorom in prostovoljno akreditacijo. Za samo delovanje overiteljev je tako dovolj le priglasitev pristojnemu inšpekcijskem organu o pričetku delovanja. Storitve lahko ponujajo različni ponudniki (overitelji) z različnimi stopnjami varnosti, uporabnik pa se odloči, katere storitve bo uporabljal. Hkrati z obveznim nadzorom overiteljev zakon predvideva tudi prostovoljni nadzor (akreditacijo), katere namen je zagotoviti še višjo raven kakovosti in s tem večje zaupanje strank.

V zadnjih dveh poglavjih so definirane kazenske določbe za overitelje in imetnike potrdil ter prehodne in končne določbe.

Po štirih letih izvajanja zakona je na podlagi komentarjev zakona ZEPEP in novih Smernic v evropskem prostoru vlada RS sprejela novelo ZEPEP-a, kjer lahko razloge za spremembe razdelimo v tri skupine:

- uskladitev slovenskega pravnega reda s pravnim redom EU,
- odprava nekaterih sistemskih in tehničnih pomanjkljivosti in
- določitev pravne podlage za vzpostavitev oziroma vključitev digitalnih potrdil na osebne in druge identifikacijske dokumente.

Nekaj usmeritev Smernice Evropskega parlamenta in Sveta 2000/31/ES o nekaterih pravnih vidikih informacijske družbe, zlasti elektronskega poslovanja v notranjem trgu, je že bilo upoštevanih v ZEPEP. Nekatere uredbe so bile naknadno sprejete v slovensko pravno ureditev s sprejetjem Zakona o spremembah in dopolnitvah Zakona o varstvu potrošnikov (ZVPot-a), vendar ne vse, tako da je v celoti prevzeta Smernica o elektronskem poslovanju šele leta 2004. Smernica o elektronskem poslovanju se na splošno ukvarja s pravilnim delovanjem notranjega trga Evropske unije z zagotavljanjem prostega pretoka storitev informacijske družbe[21] med državami članicami in zavezuje ponudnike teh storitev s sedežem v EU.

Na načelni ravni se zakon ZEPEP ne spreminja veliko, spreminja se le določitev posebnih pogojev za odgovornost posredniških storitev informacijske družbe. Ker je podatkov, ki se preko posredniškega sistema pretakajo, ogromno, je odgovornost za škodo, ki izvira iz takšnih podatkov nemogoče naložiti na posrednike. Implementacijo kompleksnega sistema pogojev in domnev za podajanje odgovornosti ponudnikov posredniških storitev v skladu s Smernico o elektronskem poslovanju predvideva ZEPEP-A.

Osnovni cilj Smernice o elektronskem poslovanju je nedvomno varstvo potrošnikov pri sklepanju pogodb na daljavo, pri čemer ločuje sklepanje pogodb na daljavo na splošno in na svetovnem spletu. Določene sistemske ureditve so že urejene z ZVPot-a, nekatere pa tja

[21] Pojem Storitev informacijske družbe je na novo definiran v 2. členu, povzema pa definicijo direktive 98/48/ES (Transparency Directive), na katero se sklicuje Smerica o elektronski trgovini. Le-ta definira storitev informacijske družbe kot storitev, ki se po navadi zagotavlja za plačilo na daljavo, z elektronskimi sredstvi in na posamezno zahtevo prejemnika storitev, pri čemer pomeni:

- da se »na daljavo« zagotavlja tako, da nikoli nista obe strani sočasno prisotni,
- »z elektronskimi sredstvi«, da se najprej pošlje in v namembnem kraju sprejme z elektronsko opremo za obdelavo in stiskanje ter v celoti pošlje, prenese in sprejme po žici, radiu, optičnih sredstvih in drugih elektromagnetnih sredstvih,
- »na posamezno zahtevo prejemnika storitev«, da se storitev zagotavlja s prenosom podatkov na posamezno zahtevo.

V to kategorijo sodijo zlasti storitve prodaje blaga in storitev, dostopa do podatkov in oglaševanje na svetovnem spletu, poleg tega pa še storitve dostopa do komunikacijskega omrežja, prenosa podatkov ali shranjevanja podatkov v komunikacijskem omrežju.

nikakor ne sodijo. To so posamezne specifične oblike zagotavljanja storitev informacijske družbe, kot so izključni prenos, gostiteljstvo in shranjevanje v predpomnilniku.

Sprememba, ki se nanaša na veljavnost potrdil za elektronsko podpisovanje, je prenos obveznosti obveščanja o vzrokih za preklic potrdila na imetnika, tako da je overitelj le tedaj dolžan preklicati potrdilo, ko je obveščen. Dodane so tudi določbe glede vsebine kvalificiranega potrdila. Pomembna sprememba je popolna uskladitev z Aneksom 1 Smernice pri določanju imena oziroma psevdonima (izločitev naziva oziroma psevdonima informacijskega sistema, saj se lahko zasebni ključ prenese na drug informacijski sistem, zaradi česar ne obstaja nikakršno jamstvo, da je sporočilo poslano iz navedenega informacijskega sistema) in pri določanju dodatnih podatkov, ki jih kvalificirano potrdilo vsebuje. Na tem mestu je dodan še en odstavek, ki se nanaša na določitev pravne podlage za vključitev digitalnih potrdil na osebne identifikacijske dokumente. V prvi vrsti je ta dodaten odstavek 28. členu namenjen povezovanju podatkov v Centralnem registru prebivalstva kot matična evidenca imetnika in evidenca identifikacijske oznake potrdila. Ker se bo s tem uvedla serijska številka, ki bo povezovala podatke na kvalificiranem potrdilu in podatke v Centralnem registru, sprememba zakona omogoča vpis te serijske številke tudi v Centralni register.

2.3.5 Ostali zakoni in predpisi s področja elektronskega poslovanja v Sloveniji

Dva meseca po sprejetju ZEPEP je Državni zbor potrdil še Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje, ki jo je dopolnil z dodatnimi pravili glede registracije kvalificiranih overiteljev v letu 2001. V njej so določena merila za presojanje izpolnjevanja zahtev za delovanje overiteljev in vsebina notranjih pravil overiteljev, ki izdajajo kvalificirana potrdila, podrobnejše tehnične predloge za elektronsko podpisovanje in preverjanje varnih elektronskih podpisov, časovno veljavnost kvalificiranih potrdil, pogoje glede uporabe varnih časovnih žigov, vrsto in uporabo označb akreditiranih overiteljev in pogoje za elektronsko poslovanje v javni upravi. V poročilu o pravnih in tržnih perspektivah elektronskih podpisov (Dumortier et al, 2003, str. 121) je navedeno, da je Slovenija edina država, ki je v nacionalno zakonodajo uvrstila ameriški standard za kriptografske module (FIPS 140-1), poleg tega pa še obvezno ovrednotenje programske opreme za overitelje po splošnih kriterijih (angl. Common Criteria).

Drug podzakonski akt je Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji, ki je bil objavljen v Uradnem listu 99/2001. Z njim se urejajo postopki za prijavo in vpis overiteljev v sodni register in postopki za samo vodenje registra. Le-ta se je prej nahajal na TradePointu (http://www.tradepoint.si), v letu 2003 pa se je prenesel na Ministrstvo za informacijsko družbo[22].

[22] Register overiteljev se nahaja na spletnih straneh Ministrstva za informacijsko družbo na naslovu http://mid.gov.si (1. 3. 2004).

Elektronsko poslovanje v Sloveniji je podvrženo številnim ostalim zakonom. V **obligacijskem zakonu** je določena veljavnost ponudbe, ki je lahko ponujena tudi v elektronski obliki, načini sprejema ponudbe, postopki sestavitve listine (57. člen) ... **Zakon o splošnem upravnem postopku** že daje pravno veljavo tudi dokumentom v elektronski obliki. V 63. členu je tako določeno, da se vloga lahko pošlje po elektronskem mediju, vendar le če pri organu obstajajo tehnične možnosti za sprejem. Organ lahko v skladu s 67. členom zahteva od stranke, da po elektronskem mediju poslano vlogo papirno potrdi. Takšno potrjevanje postane nepotrebno, če stranka uporabi elektronsko podpisovanje in elektronskemu dokumentu priloži kvalificiran podpis, saj je namen papirnega potrjevanja zagotovitev identitete stranke. ZUP tudi določa, da se lahko uradni spisi, kot so vabila, odločbe in sklepi, vročijo po elektronski pošti, in hkrati nalaga, da Vlada Republike Slovenije s posebno uredbo določi postopek za takšno vročenje. 216. člen se nanaša neposredno na elektronske podpise, saj omogoča izdajanje odločbe v obliki računalniškega izpisa, ki ima lahko tudi elektronski podpis. Kot javna listina je pod določenimi pogoji računalniški zapis, dejansko stanje pa se lahko ugotavlja na podlagi podatkov v računalniških bazah. Tudi **Zakon o pravdnem postopku** omogoča uporabo telekomunikacijskih storitev za pošiljanje vlog (tožbe, odgovori na tožbo, pravna sredstva in druge izjave, predlogi in sporočila, ki se vlagajo zunaj obravnave). Pri tem se za podpisnika šteje oseba, ki je v vlogi navedena kot podpisnik. Po ZPP-ju se lahko v nujnih primerih sodišče poslužuje telekomunikacijskih sredstev. Podobno **Zakon o dostopu do informacij javnega značaja** omogoča vlaganje zahtev v elektronski obliki. **Zakon o varstvu osebnih podatkov** določa zbiranje, hrambo in posredovanje osebnih podatkov. Ker so to zelo občutljivi podatki, zakon pa je bil sprejet pred ZEPEP, se vse bolj kaže potreba po njegovi dopolnitvi v smislu hrambe podatkov v šifrirani obliki, posredovanja v elektronski obliki z obojestransko varno identifikacijo ipd. Zelo vpliven bo tudi prenovljen Zakon o arhivskem gradivu in arhivih, ki se bo imenoval Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZDAGA). Trenutno je v fazi nastajanja. Zadnja novela **Zakona o gospodarskih družbah** prinaša možnost oddajanja letnih izkazov družb v elektronski obliki, medtem ko se druge oblike elektronskega poslovanje ne obravnavajo, tako da bo potrebno precej sprememb in dopolnitev zakona, da bo elektronsko poslovanje resnično zaživelo.

Elektronsko poslovanje poleg vseh prednosti prinaša tudi slabosti, med katerimi je na prvem mestu cela vrsta novih možnosti goljufij in kaznivih dejanj, skratka računalniški kriminal. Zato bo treba posodobiti **Kazenski zakonik RS** in **Zakon o kazenskem postopku** v skladu s konvencijo Sveta Evrope o računalniškem kriminalu[23].

2.3.6 Sporazum o elektronskem poslovanju in ostali dokumenti

Določbe v veljavni zakonodaji, ki urejajo elektronsko poslovanje, so tako splošne, da poslovni partnerji marsikdaj vidijo potrebo po sklenitvi dodatnega sporazuma, s katerim

[23] Council of Europe: Convention on Cybercrime, poročilo se nahaja na spletnih straneh http://conventions.coe.int.

podrobneje določijo načine medsebojnega komuniciranja. Med strankami se sprejemajo dodatni sporazumi, vsaj okvirni, ki specificirajo določene zakonske določbe, druge določbe zakona pa normalno veljajo naprej. Po navadi so ti sporazumi okvirni, mednje sodijo bolj specializirani sporazumi, kot so politike elektronskega podpisa, politike potrdil ipd. Pravna pravila, ki urejajo posamezen elektronski posel, so lahko v najširšem pomenu vsebovana v naslednjih sporazumih:

- Zakon o elektronskem poslovanju in elektronskem podpisu ZEPEP,
- sporazum o elektronskem poslovanju (podrobneje razčlenjuje določene načine komuniciranja med podpisniki, določijo ga podpisniki sami),
- politika elektronskega podpisa (natančneje opredeljuje poslovne procese in vloge podpisnikov) in
- konkreten elektronski pravni posel (ponudba, pogodba, račun ipd).

Vsebina sporazuma se velikokrat pokriva s vsebino politike elektronskega podpisovanja, ki je bolj specializiran pravni akt, kar pomeni, da v primeru nesoglasij med akti prevlada določitev v sporazumu. Idealno sporazum določa splošne oblike elektronskega komuniciranja, za posamezne tipe elektronskega sporočila pa se sklicuje na posamezne politike elektronskega podpisovanja. Ponekod se poslovni partnerji dogovorijo tako za način poslovanja kot tudi za politike podpisovanja kar s sporazumom.

Sporazum o elektronskem poslovanju natančneje določa načine elektronske komunikacije, tako tehnične načine (elektronska pošta, uporaba elektronskih podpisov, digitalna potrdila ipd.) kot tudi njihovo pravno vsebino (dokumenti). Tipični členi sporazuma so omenjeni načini komuniciranja, ki jih poslovni partnerji uporabljajo pri svojem elektronskem poslovanju, kraj in čas oddaje elektronskega sporočila (kraj je po navadi stalno prebivališče fizične osebe oziroma sedež podjetja ne glede na dejanski kraj oddaje, čas pa je takrat, ko elektronski dokument zapusti informacijski sistem pošiljatelja), kraj in čas prejema sporočila (kraj je enako definiran kot pri oddaji, čas prejema je najpomembnejši čas v slovenski zakonodaji, saj je po sprejemni teoriji to čas, ko nastanejo pravni učinki), potrditev prejema (opcijski člen, ki po navadi definira 24-urni čas potrditve prejemnika pošiljatelju), razveljavitev sporočila, nastop pravnih učinkov, obdobje veljavnosti (čas veljavnosti ponudbe 15 dni in podobno), obdobje za sprejetje (tipično 24 ur), omejitev odgovornosti za elektronske pravne posle, politike elektronskih podpisov, kvalificirana digitalna potrdila, ki se lahko uporabljajo, verifikacija in arhiviranje sporočil, v primeru mednarodnih poslov še izbira prava, prekinitev pogodbe (pomembno je, da sporazum določa tudi ohranjanje pravne veljave, kar pomeni, da morata podpisnika poskrbeti za določbe o shranjevanju in dolgoročnem arhiviranju navkljub prekinitvi pogodbe) in na koncu razreševanje sporov.

Politika elektronskega podpisa je množica pravil za ustvarjanje in preverjanje elektronskega podpisa, ki opredeljujejo njegovo veljavnost. Določa tako pravne kot tehnične pogoje in hkrati tudi področja njegove uporabe. Namenjena je še bolj natančnemu določanju elektronskega poslovanja med podpisniki, kjer se določa elektronsko poslovanje za določene poslovne procese. Poslovni partnerji lahko podpišejo en sporazum o elektronskem poslovanju in več politik elektronskega podpisovanja.

Vsebina politike se deli na pravni (pogoji, ki opredeljujejo pravno veljavnost podpisane vsebine in pravne omejitve, kot so pooblastila, omejitve podpisnika, tipi zaveze ipd.), tehnični (tehnični pogoji za kreiranje in preverjanje elektronskega podpisa) in splošni del (naziv izdajatelja politike, enolični identifikator, čas veljavnosti, datum izdaje in področje uporabe politike). Politika poleg tega vsebuje še vrsto pravil, ki so lahko splošna, posebna, lahko se nanašajo na podpisnika ali na nasprotno stranko, lahko pa opredeljujejo varnostne zahteve, na primer v zvezi z izdajatelji digitalnih potrdil ali s časovnim žigosanjem. Na dokumentu je lahko eden ali več podpisov, ki so lahko hkratni ali zaporedni, tako da je število potrebnih podpisov tudi pomemben del politike.

Politika se lahko nahaja znotraj samega podpisanega dokumenta, vendar je predvsem zaradi prevelike obsežnosti po navadi zunaj njega. Dokument vsebuje samo sklic na politiko, ki je objavljena na neki spletni strani.

Vzorčni primer politike elektronskega podpisa za elektronski račun je pripravila Delovna skupina za elektronski podpis znotraj projekta e-SLOG[24]. V njem se nahajajo določila o podpisnikih (lahko so navedeni po svojih poslovnih vlogah ali poimensko), o pooblastilu podpisnikov (kako se omenjene osebe identificirajo kot nosilci pooblastil), o vrstah zaveze oz. odgovornosti (ker je elektronski podpis možno uporabiti za različne namene, od gole identifikacije do izražanja pravne volje oz. pravnega zavezovanja, je nujno, da se s politiko določi, za kaj se podpis uporablja[25]), časovne omejitve, varovanje zaupnih podatkov, reševanje sporov, vsebina računa, dovoljenje DURS za izdajo računov v nematerializirani obliki (po novem zakonu o DDV, ki velja od 1. 5. 2004, je potrebna le še priglasitev), prehodno obdobje (ker od preklica digitalnega potrdila do objave v seznamu preklicanih potrdil mine nekaj časa, je prehodno obdobje za ugotavljanje veljavnosti dokumenta nujno),

[24] Projekt e-SLOG teče od leta 2001 na Gospodarski zbornici Slovenije, vanj pa so vključena nekatera večja slovenska podjetja in drugi zainteresirani gospodarski subjekti. Namenjen je pospeševanju slovenskega elektronskega poslovanja s pripravo in uveljavitvijo standardov na tem področju. Do junija 2004 so pripravili priporočila za elektronski račun in njegovo enostavno različico, za elektronsko naročilo, potrditev naročila in povratnico, v pripravi pa so še ostali pomembni dokumenti, ki se uporabljajo pri vsakodnevnem poslovanju slovenskih podjetij. Več informacij o projektu in priporočila ter uporabniška dokumentacija se nahaja na spletnem naslovu http://www.gzs.si/e-poslovanje.

[25] Tipi zavez so overitev, potrditev sprejema dokumenta, avtorstvo, nadzor dostopa, pregled dokumenta ipd.

potrdila (katera potrdila se uporabljajo), kreiranje elektronskega računa, verifikacija in arhiviranje.

3 JEZIK XML, SPLETNE STORITVE IN DIGITALNI PODPIS DOKUMENTOV, ZAPISANIH V XML

3.1 Standardizacijska telesa za protokole XML

Standardizacijska telesa so osnovni organi, ki gradijo nove protokole in priporočila ter s tem usmerjajo razvoj interneta in elektronskega poslovanja. Na področju metajezika XML in varnostnih protokolov, ki so nastali na njegovi podlagi, so najpomembnejša standardizacijska telesa Konzorcij svetovnega spleta (W3C), Mednarodna organizacija za standardizacijo (ISO), Delovna skupina za internetno inženirstvo (IETF), Organizacija za napredek na strukturnih informacijskih standardih (OASIS) in ostali.

3.1.1 Konzorcij svetovnega spleta W3C

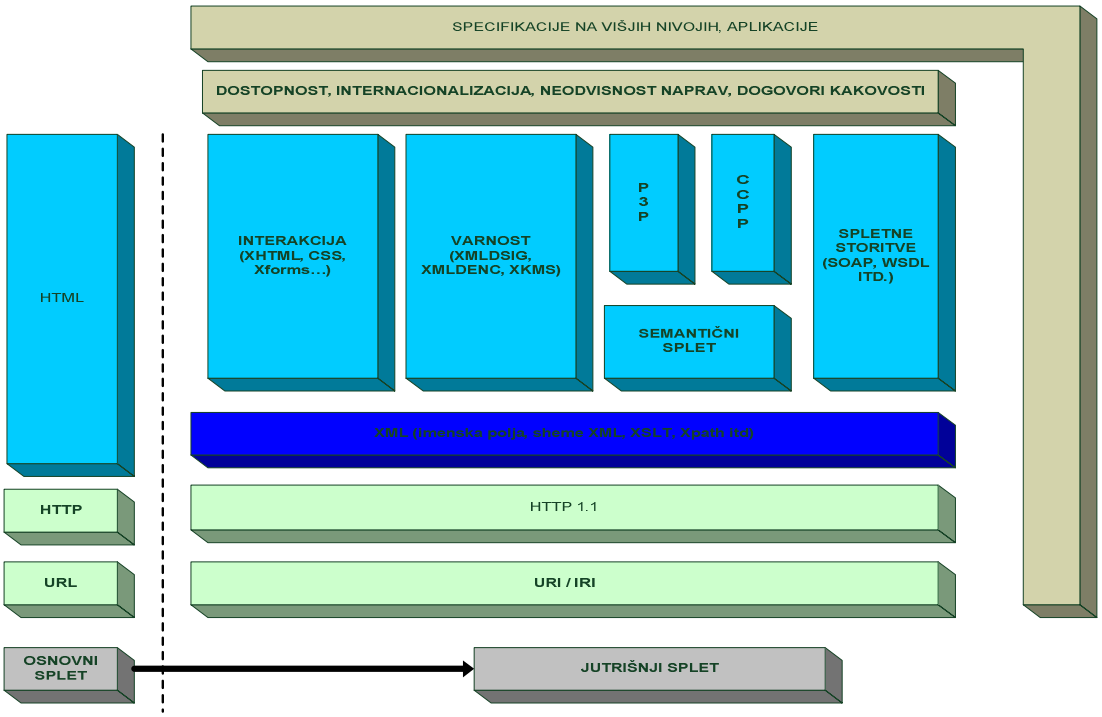
Konzorcij svetovnega spleta je bil vzpostavljen oktobra 1994 za vodenje razvoja svetovnega spleta na podlagi razvijanja splošnih protokolov, ki bi promovirali njegovo evolucijo in zagotavljali medsebojno sodelovanje različnih aplikacij in naprav. Njegov ustanovitelj in trenutni direktor je Tim Berners-Lee, izumitelj svetovnega spleta[26]. Danes v konzorciju sodeluje prek 450 organizacij.

Dolgoročni cilji W3C so skrčeni na tri sklope. Prvi je zagotavljanje univerzalnega dostopa za vse, ne glede na različnosti v kulturi, jeziku, izobrazbi, dostopnosti naprav, materialnih sredstvih, fizičnih omejitvah ipd. Druga dva cilja sta povezana z izgradnjo semantičnega in zaupanja vrednega spleta. Svetovni splet je kot aplikacija, zgrajena na internetu, podedoval temeljna razvojna načela, to je medsebojno delovanje programske in strojne opreme, ki uporabljata spletne jezike, upoštevanje evolucije v drugih prihajajočih tehnologijah in decentralizacija zmogljivosti in virov. Od svojega nastanka do danes se je konzorcij vseskozi oziral na omenjena razvojna načela in na svoje cilje ter v tem času objavil prek 40 priporočil. Vsako od teh ne upošteva samo predhodnih, temveč je že v svoji osnovi zgrajeno tako, da predvideva prihodnje specifikacije. W3C načrtuje nadgradnjo vzpostavljene arhitekture današnjega spleta, ki se trenutno ukvarja predvsem s HTML (jezik, s katerim se ustvarjajo dokumenti na svetovnem spletu, angl. Hypertext Markup Language), URI in HTTP (protokol za premikanje dokumentov prek svetovnega spleta, angl. Hypertext Transfer Protocol). V prihodnosti bodo vsa priporočila temeljila na metajeziku XML.

[26] Več na spletnih straneh http://www.w3.org/People/Berners-Lee/.

Priporočila, ki jih je izdal W3C, so razvrščena v več kategorij. Dotikajo se jezika (X)HTML, stilov v obliki datotek CSS (angl. Cascading Style Sheets), metajezika XML in ostalih gradnikov (XSLT, XPath ipd.), dokumentnega objektnega modela DOM, matematičnega označevanja XML, grafičnega formata PNG, vektorskega formata SVG, multimedijskega jezika SMIL, semantičnega označevanja z RDF, jezika za pridobivanje informacij o spletnih straneh za uporabnika in zagotavljanje njegove zasebnosti (P3P), priporočil za dostopanje do strani za invalide in varnosti dokumentov, zapisanih v XML, kar bo natančneje predstavljeno v nadaljevanju. Opis vseh se nahaja na spletnih straneh http://www.w3c.org.

Slika 8 - Področja delovanja W3C



Vir: W3C, 2004

W3C formalno izdaja priporočila, ki so tehnično le priporočila za nadaljnjo standardizacijo, v praksi pa so postala de facto standardi na svojih področjih. Dokument pridobi najprej status »delovni osnutek«, nato »kandidat za priporočilo«, po testiranju »priporočeno priporočilo« in končno, po sprejetju znotraj W3C, **»priporočilo W3C«**.

3.1.2 Delovna skupina za internetsko inženirstvo - IETF (Internet Engineering Task Force)

IETF je skupina znotraj internetnega združenja ISOC (angl. Internet Society), ki razvija in sprejema tehnične standarde, na katerih temelji internet. Glavne pristojnosti skupine so:

- odkrivanje in iskanje rešitev za pomembna operacijska in tehnična vprašanja interneta,
- določanje smeri razvoja, uporabe protokolov in kratkoročnih sprememb zgradbe z namenom reševanja tehničnih težav,
- dajanje priporočil skupine IESG glede standardizacije in uporabe protokolov v internetu ter
- skrb za prenos tehnologij iz skupine IRTF do internetne skupnosti.

Udeležba na strokovnih srečanjih IETF je odprta, pogoj je plačilo minimalne kotizacije. Sodelujejo lahko vsi zainteresirani, od strokovnjakov, inovatorjev do uporabnikov. Omogočen je tudi neposreden prenos sestankov na avdio- in videokanalih delovnih postaj, povezanih v internet. Pomembno je, da lahko vsak sodeluje pri ustvarjanju in izdelavi standardov ter pozneje pri izdelavi programske opreme, ki gradi internet. Po izdelavi delujoče programske opreme je ta po navadi dosegljiva v omrežju brezplačno (za osebno uporabo). Testiranje spremljajo organi ISOC-a in skrbijo za uspešen zaključek procesa. Delovne skupine nastajajo hitro in ob koncu procesa hitro ugasnejo. Standarde odobrijo odbori ISOC-a .

Postopek nastajanja standarda je poenoten. Začne se s »predlogom« in nadaljuje z »osnovo standarda«. Sledi razvoj, testiranje in zbiranje povratnih informacij od uporabnikov Končni predlog se poda v obliki **»zahtevka za komentar RFC«** (Request For Comment). Prvi je bil objavljen leta 1969 (RFC 1 Network Control Program), do zdaj se jih je nabralo prek 3600.

3.1.3 OASIS - Organisation for the Advancement of Structured Information Standards

Organizacija za napredek na strukturnih informacijskih standardih je neprofitni globalni konzorcij, ki vodi razvoj, zbliževanje in sprejemanje standardov za e-poslovanje. Ustanovljen je bil leta 1993. Ima več kot 2000 članov, ki predstavljajo 600 organizacij z vsega sveta, namenjen pa je predvsem vzpostavitvi mednarodnega industrijskega soglasja že pred razvojem novega standarda.. Standardi, ki jih OASIS objavi, se nanašajo na varnost, spletne storitve (Web Services), poslovne transakcije, elektronsko objavljanje in na medsebojno delovanje znotraj enega in med različnimi elektronskimi trgi.

OASIS je najprej deloval pod imenom »SGML Open«, kjer je bil osnova metajezik SGML (angl. Standard Generalized markup Language),. V letu 1998 so se preimenovali in z novim imenom poudarili zelo razširjeno delo le na enem področju SGML-ja, to je na razširljivem označevalnem jeziku XML. Informacijski kanal, s katerim OASIS komunicira s svetom, sta dve spletni mesti: Cover Pages (http://xml.coverpages.org) in XML.org (http://xml.org).

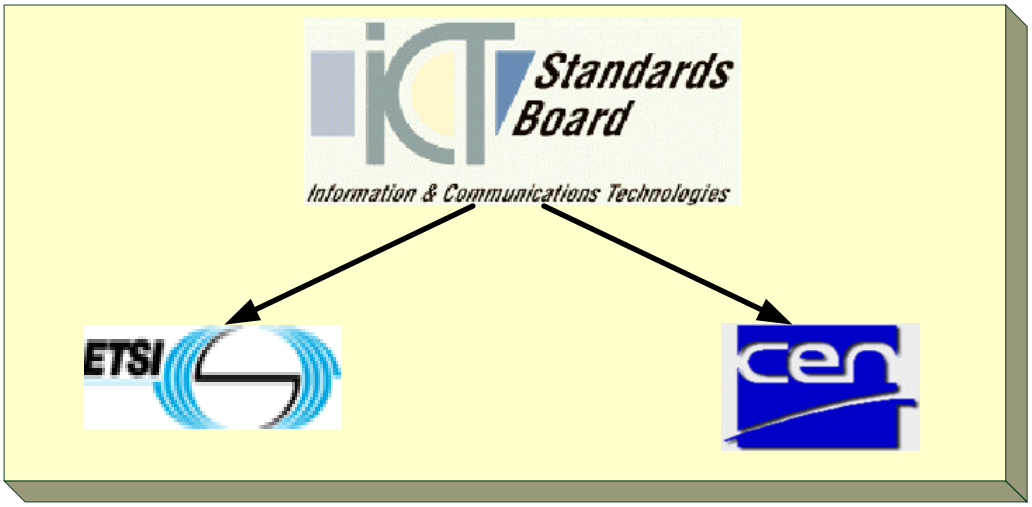
Na področju varnosti deluje več tehničnih komitejev znotraj OASIS. To so Web Services Security, Digital Signature Services (izgradnja tehnik za podporo procesiranju digitalnih podpisov, skupaj z definiranjem vmesnika za podporo spletnim storitvam, ki naredijo in/ali preverjajo podpise), Security Services (delo na okvirnem programu XML za podporo kreiranja in izmenjave overjanja ter overjenih informacij - SAML), UDDI ipd.

Najvišji status v OASIS imajo dokumenti, označeni kot **»standard OASIS«**, kar pomeni, da ga je po izvedenem glasovanju odobrilo celotno članstvo OASIS. Predhodni status se imenuje »osnutek komisije« (nekdaj tehnična resolucija), kar označuje odobritev specifikacije od enega izmed tehničnih komisij znotraj OASIS.

3.1.4 EESSI – Evropska iniciativa za standardizacijo elektronskih podpisov

Smernica za elektronsko podpisovanje v Evropski uniji določa zahteve za kvalificirana potrdila, za izdajatelje takšnih potrdil in naprave, ki varno podpisujejo elektronska sporočila. Komisija Evropske unije izdaja standarde in podaja navodila za uporabo (reference) globalno priznanih standardov, ki ustrezajo Smernici, članicam EU in ostalim zainteresiranim državam pa priporoča, da se jim čim bolj približajo v lokalnih zakonodajah za izvajanje e-poslovanja. Da ne bi čas prehitel rokov za sprejetje lokalnih zakonodaj, je Komisija zaprosila evropska standardizacijska telesa in industrijo, da skupaj pod okriljem novonastale organizacije EESSI (angl. The European Electronic Signature Standardization Iniciative) pridejo do zahtevanih standardov in priporočil. Delo se je tako razporedilo predvsem na Evropski komite za standardizacijo CEN/ISSS in Evropski inštitut za telekomunikacijske standarde ETSI, koordinacijo pa je prevzel Odbor za standardizacijo informacijskih in telekomunikacijskih tehnologij ICTSB (glej sliko Slika 9).

Slika 9 - EESSI

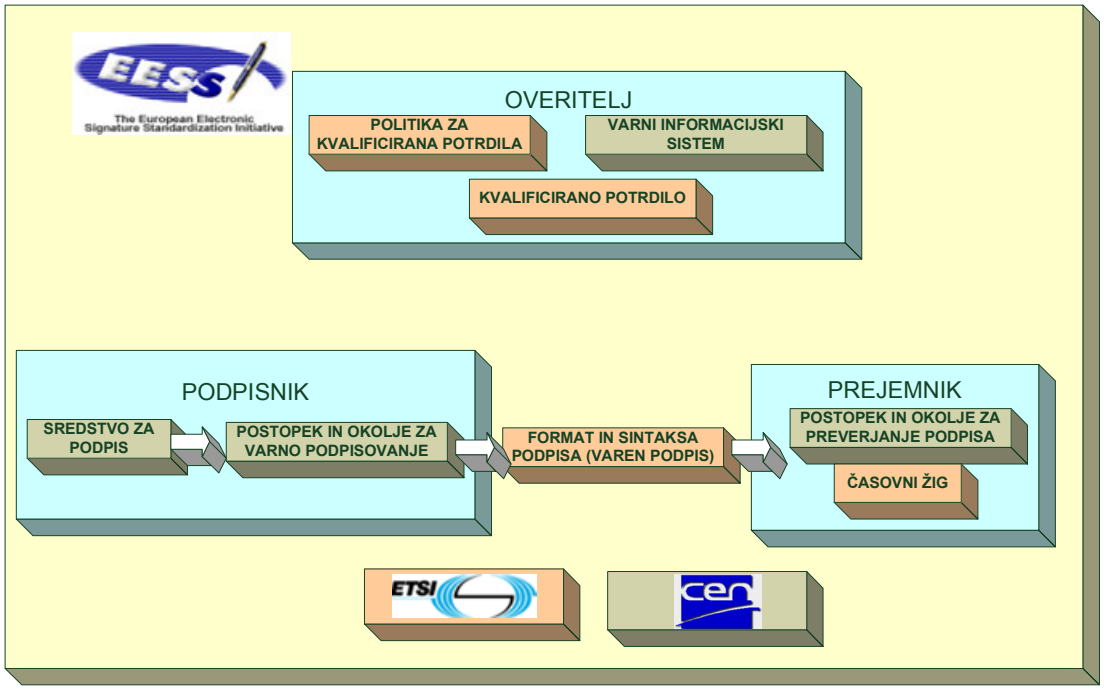


Znotraj EESSI so se identificirala tri kritična področja dela:

- standardi kakovosti in funkcionalnosti za overitelje,
- standardi kakovosti in funkcionalnosti za izdelke, s katerimi se izvaja kreiranje podpisov in preverjanje, ter
- standardi za navzkrižno delovanje elektronskih podpisov.

Delo se je začelo leta 2000, do sedaj pa sta omenjeni organizaciji izdali že veliko standardov, bolj znanih pod imeni CWA (CEN Workshop Agreements) in TS (ETSI Technical Specifications). Vsi so javno dostopni na njihovih spletnih straneh.

Slika 10 - Področja standardizacije znotraj EESSI



Vir: EESSI, 2004

Standardizacija EESSI je bila na začetku na razpotju. Ali naj se aktivnosti znotraj EESSI izvajajo le v okviru Smernice in njenih aneksov ali naj se razširijo tudi na področje medsebojnega delovanja različnih sistemov za izvajanje e-poslovanja? Po burnih debatah se je delo nadaljevalo tudi v slednji smeri, kar se je pozneje izkazalo kot zelo potrebna in dobrodošla naloga EESSI.

Standardi, ki jih je izdal CEN/ISSS[27], so:

- CWA14365 – Vodič za uporabo elektronskih podpisov,
- CWA 14355 – Usmeritve za implementacijo naprav za varno izdelavo podpisov,
- CWA 14172 – Usmeritev za ocenjevanje ustreznosti,
- CWA 14171 – Postopki za preverjanje elektronskih podpisov,
- CWA 14170 – Varnostne zahteve za sisteme, ki izdelujejo podpise,
- CWA 14169 – Varne naprave za izdelavo podpisov 'EAL 4+',
- CWA 14168 – Varne naprave za izdelavo podpisov 'EAL 4',
- CWA 14167 – Varnostne zahteve za zaupanja vredne sisteme, ki upravljajo z digitalnimi potrdili.

ETSI je izdal več standardov, ki se nanašajo na področja upravljanja infrastruktur javnih potrdil, digitalnega podpisa in digitalnega arhiva. Vsi so doživeli že več revizij, ki so jasno označene z verzijami za oznako standarda. Najpomembnejši med njimi so:

- TS 101 733 v1.5.1 (december 2003) – Format elektronskih podpisov,
- TR 102 038 (april 2002) – Format XML za politike podpisovanja,
- TS 102 023 (april 2002) –Zahteve za politiko izdajateljev časovnih žigov,
- TS 101 456 v1.2.1 (april 2002) – Zahteve za politiko overiteljev, ki izdajajo kvalificirana digitalna potrdila,
- TS 101 861 v1.2.1 (marec 2002) – Profil časovnega žiga,
- TS 101 903 (februar 2002) – Napredni elektronski podpisi v formatu XML (XAdES),
- TS 101 862 v 1.2.1 (junij 2001) – Profil kvalificiranega potrdila.

Na področju podpisovanja dokumentov, zapisanih v XML, je treba upoštevati predvsem dva, to sta TS 101 733 in TS 101 903. Prvi definira format za napredne elektronske podpise, ki ostanejo veljavni tudi po daljšem časovnem obdobju, so skladni s Smernico in imajo vključene uporabne dodatne informacije, potrebne za kasnejšo verifikacijo podpisov in

[27] Celoten pregled izdanih standardov CEN / ISS se nahaja na internetnem naslovu http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/published+cwas/cwa+download+area.asp .

arhiviranje. TS 101 903 je **standard za napredne elektronske podpise**, poznan tudi pod kratico **XAdES**. Z njim se razširja priporočilo XMLDSIG v področje preprečevanja zanikanja sodelovanja v elektronskem poslovanju z definiranjem formatov XML za napredne elektronske podpise, ki ostanejo veljavni še dolgo po podpisu.

3.2 Razširljivi označevalni jezik XML

Svet XML je neskončen svet standardov in tehnologij, ki predstavljajo živ, neprestano spreminjajoč in razvijajoč se organizem. Nemogoče je predstaviti celoten XML v enem poglavju, zato bomo tu pregledali osnovne koncepte XML, predvsem v povezavi z varnostnimi koncepti, potrebnimi za varno izmenjavo dokumentov. Ta predstavitev se lahko deli na osnovno sintakso in na načine procesiranja dokumentov in sporočil XML.

Razširljivi označevalni jezik in njegovo še bolj popularno okrajšavo XML je iznašel James Clark[28]. Mnogokrat je bila citirana njegova izjava, s katero je poudarjal enostavnost XML: »XML ne bo nikoli dobil kakšne nagrade za tehnično eleganco. Vendar je dovolj enostaven, da so ga ljudje sprejeli, in ima v sebi ravno dovolj standardiziranega splošnega označevalnega jezika, da ga je skupnost SGML sprejela med svoje standarde.« Označevalni jezik je mehanizem za opisovanje zgradbe dokumenta, XML pa specificira način strukture, shranjevanja in pošiljanja dokumenta. Nič ne govori o predstavitvi informacij uporabniku – temu se XML namerno izogne in s tem pridobi nevtralnost in preglednost. Pomembno je še dejstvo, da XML ni jezik, temveč metajezik. Kaj to pomeni? Z metajezikom se opisujejo drugi jeziki oziroma, kot pravijo nekateri, to je pravi jezik. Predpona »meta« se uporablja v analitični filozofiji in ohlapno pomeni eno stopnjo nad nečim. Jeziki, ki nastanejo z uporabo XML, se pogostokrat imenujejo tudi aplikacije XML. O nekaterih bo v tem delu še govora, večina pa se navezuje na pojem varnosti. Osnovni aplikaciji XML na področju magistrske naloge sta podpisovanje in šifriranje dokumentov zapisanih v XML.

Osnovni standard oziroma priporočilo W3C je »XML 1.0 Recommendation«, ki pa ne definira samo sintakse in gramatike. Sintaksa se nanaša na vrsto omejitev o tem, kako in kje so lahko oznake postavljene, nanaša se na prikaz sprejemljivih znakov in predvsem na pravila, s katerimi se lahko označevanje izvaja na splošno. Ker je filozofija XML tudi enostavnost, lahko uporabnik omenjeni standard usvoji zelo hitro. XML-priporočilo skupaj s celim nizom drugih priporočil tvori načine, kako izdelovati in procesirati XML. Ta priporočila so Namespaces in XML (januar 1999), XML Base (junij 2001), XML Path Language oziroma Xpath (oktober 1999), XSL Transformations oziroma XSLT (november 1999), XML Pointer Language oziroma Xpointer (januar 2001), XML Linking Language

[28] James Clark je bil tehnični vodja aktivnosti znotraj W3C, ki je leta 1998 objavila Priporočilo XML 1.0. Več o tem na spletnih straneh http://www.w3.org/XML/Activity.

oziroma Xlink (juni 2001), Extensible Style Language oziroma XSL (avgust 2001) in XML Inclusions oziroma Xinclude (maj 2001)[29].

Varnost dokumentov zapisanih v XML zahteva gledanje na XML z malce drugačnega zornega kota kot na druge tovrstne aplikacije, saj je to predvsem predstavitvena semantika. Trenutne specifikacije varnosti dokumentov zapisanih v XML se ne osredotočajo na podpisovanje ali šifriranje, temveč se pri tem naslanjajo na obstoječe varnostne tehnologije, definirane predvsem s standardi PKCS (Public Key Criptography Standards)[30], ukvarjajo pa se z njihovo apliciranje na dokumente zapisane v XML.

3.3 Spletni protokol SOAP

Protokol za enostaven dostop do objektov SOAP (angl. Simple Object Access Protocol), ki v skladu z zadnjo verzijo 1.2 ni več akronim, ampak ime, je osnovan na metajeziku XML, uporablja pa se za podajanje informacij v eno smer. Sporočila SOAP se lahko kombinirajo za implementacijo različnih procesov v obliki »zahteva–odgovor« oziroma drugačnih, še bolj zapletenih procesov. Informacije, ki se prenašajo v sporočilu SOAP, so lahko v obliki dokumenta ali klica za sprožitev oddaljenega postopka RPC (angl. Remote Procedure Call), s katerim se izvede določena procedura pri ponudniku storitev. Dokument je lahko naročilnica za nakup blaga, s klicem RPC pa se izvede postopek za obračun tega blaga naročniku. Točno določene ločnice med dokumenti in RPC-ji ni.

SOAP, ki je bil prvič predstavljen leta 1998[31], je rezultat skupnega dela več podjetij (Develop-Mentor, Microsoft, IBM in mnogo drugih) pod okriljem W3C, kjer so leta 2003 sprejeli več dokumentov kot priporočila protokola SOAP (verzija 1.2) Slednji je tako kot drugi v okviru metajezika XML opisan z natančnim popisom sporočil in z zaporedjem izmenjave sporočil. Eden izmed ključnih razlogov za današnjo razširjenost uporabe protokola je v minimalističnem pristopu, ki so ga uporabili avtorji za njegov opis. Namesto da bi predvideli in natančno specificirali vse mogoče scenarije, so definirali le ogrodje in tako omogočili prilagajanje uporabe SOAP-a za specifične namene. Poleg specifikacije sporočila so definirali še povezave, najbolj uporabna pa je vsekakor tista prek protokola HTTP.

V protokolu SOAP obstaja več vrst vozlišč, ki si podajajo sporočila. Glavna sta vsekakor prvi pošiljatelj in zadnji prejemnik sporočila, na poti med njima pa se lahko nahaja cela vrsta vmesnih vozlišč. Telo sporočila je namenjeno samo zadnjemu prejemniku, tako da ga

[29] Vsa priporočila se nahajajo na straneh Konzorcija svetovnega spleta http://www.w3.org.

[30] Standardi PKCS so osnovni standardi v varnostnem svetu. Njihov pregled je na voljo na več spletnih straneh, tudi na http://www.rsa.com.

[31] Koncept SOAP kot XML RPC je bil narejen leta 1998 v podjetju Userland Software, njegov avtor pa je David Winer.

vmesni prejemniki ne smejo spremeniti, lahko pa ga preberejo ali osvežijo navodila v glavi. Zelo pomembno je, da vsi prejemniki poznajo sintakso in uporabljena poimenovanja, drugače se vrne pošiljatelju sporočilo o neuspešnem prejemu.

Osnovna, minimalna oblika sporočila SOAP je prikazana na sliki 11.

Slika 11 - Osnovna oblika sporočila SOAP

```
<? Xml version='1.0' ?>
<env:Envelope xmlns:env="http://www.w3.org/2002/06/soap-envelope">
    <env:Header>
            Glava sporočila SOAP
    </env:Header>
    <env:Body>
            Vsebina sporočila SOAP
    </env:Body>
</env:Envelope>
```

Ker je SOAP izrazito enostranski protokol za sporočanje, se sporočila razlikujejo glede na to, ali so zahteve oziroma odgovori nanje. Poleg informativnih sporočil so lahko sporočila tudi napake pri sporočanju. Napaka je edina oznaka znotraj vsebine sporočila, ki jo protokol natančno določa. Iz vsega napisanega se zelo hitro ugotovi, da je protokol lahko enostavno zlorabljen, če načrtovalci aplikacij ne uporabijo ostalih funkcionalnosti, ki razširjajo specifikacijo. Uporaba le-teh je seveda na izbiro, vendar zaradi vseh nevarnosti, ki prežijo na svetovnem spletu, zelo dobrodošla in priporočljiva.

SOAP je zelo enostaven protokol, osnovan na XML in shemi XML z zelo malo zahtevanimi elementi. Lahko se prenaša prek protokola »http« ali z drugimi internetnimi protokoli. Na strežaj pušča odprta vrata za druge, komplementarne standarde, zato so se le-ti v zadnjem času zelo množično pojavili, pri čemer vsak bolj ali manj pokriva svoje področje. Dva izmed najbolj uporabljenih sta UDDI, ki definira imenike specifičnih spletnih storitev (več o tem je zapisano v poglavju 3.3.1) in s tem razširja njihovo uporabo, ter WSDL (angl. Web Services Description Language) kot formalen način opisa vmesnika za spletno storitev. Na eni strani je SOAP poskrbel za enostavno medsebojno delovanje med aplikacijami, na drugi pa prinesel celo vrsto novih nevarnosti in izzivov na področju zagotavljanja varnosti, kar je temeljni razlog za še vedno dokaj počasno širitev sporočanja na način, kot ga določa SOAP, saj so standardi na področju varnosti zelo zapleteni in predvsem šele dobro nastali.

3.3.1 Spletne storitve (Web Services)

Spletne storitve (Web Services) so tehnologija, ki omogoča aplikacijam komunicirati med seboj, in to neodvisno od uporabljene platforme ali programskega jezika. Natančneje je to

programerski vmesnik, ki opisuje zbirko operacij, dostopnih tudi prek spleta z uporabo standardiziranih sporočil v XML-formatu. Skupina vzajemno delujočih spletnih storitev definira aplikacijo spletnih storitev v storitveno orientirani arhitekturi (angl. Service-Oriented Architecture – SOA).

Na višji, konceptualni ravni se lahko spletne storitve opisujejo kot moduli, ki izvajajo samostojno, točno določeno nalogo. Po navadi se izenačujejo s poslovnimi nalogami, tako da lahko njihovo medsebojno delovanje načrtujejo tudi drugi, ne le tehnično usposobljeni ljudje. Pomembna lastnost je predvsem odprtost in povezljivost. To omogoča, da se določen poslovni proces odvija na modulih različnih proizvajalcev in ponudnikov. Hitrejše povračilo naložbe v aplikacijo, osnovano na spletnih storitvah, se doseže tudi s ponovljivostjo, saj lahko isti modul v obliki spletne storitve uporabljajo različni procesi znotraj podjetja ali celo v odprtem podjetniškem okolju.

V preteklosti je bila osnovna miselnost pri programiranju aplikacij zasnovana na funkcijah in postopkih, ki so na podlagi podanih vhodnih parametrov izvedli določeno aplikacijo in vrnili rezultat. Pozneje se je prvi koncept nadgradil z objekti, ki so vsebovali celo vrsto funkcij in internih spremenljivk. S prehodom na komuniciranje med aplikacijami se je pokazala potreba po definiranju univerzalnih vmesnikov za te objekte, ki niso odvisni niti od operacijskih sistemov niti od uporabljenih programskih jezikov. Počasi se je začel uporabljati metajezik XML za izvedbo takšnih vmesnikov, saj se lahko le z njegovo uporabo naredi ločitev gramatične strukture (sintakse) od gramatičnega pomena (semantike). Tako zasnovane omogočajo:

- medsebojno delovanje aplikacij, delujočih na kateri koli platformi in napisanih v katerem koli programskem jeziku,
- izdelavo konceptualnih procesnih diagramov,
- prilagajanje obstoječih aplikacij vedno spremenljivemu poslovnemu okolju,
- ohlapno povezovanje aplikacij, kar pomeni, da v primeru manjših sprememb na delovanju ene aplikacije ni rezultat prekinitev delovanja celotne aplikacije,
- zagotavljanje delovanja tudi obstoječim aplikacijam z izdelavo ustreznih vmesnikov in
- ločevanje administrativnih in operativnih funkcij (varnost, zanesljivost …) od osnovne funkcije spletne aplikacije.

Spletne storitve se danes razvijajo z uporabo družine povezanih standardov, ki opisujejo, prinašajo in medsebojno sodelujejo. Standarde lahko razvrščamo v več skupin glede na njihovo vlogo. Prvo skupino, ki se ukvarja s sporočanjem, opisom vmesnikov, naslavljanjem in dostavljanjem, predstavlja predvsem protokol SOAP, s pomočjo katerega se lahko

kodirajo sporočila tako, da se prenašajo prek omrežja z uporabo transportnih protokolov, kot so HTTP, SMTP in drugi. V drugo skupino, ki se ukvarja z oglaševanjem spletnih storitev, sodi protokol UDDI, ki definira imenik in pridružene protokole za iskanje in dostopanje do spletnih storitev. Podoben protokol, ki deluje brez imenika, je WSIL (angl. Web Services Inspection Language). Tretjo skupino tvorijo varnostni protokoli za spletne storitve (WS-Security, WS – Policy, WS – Trust, WS – Privacy, WS – Secure Conversation, WS – Federation in WS – Authorization). Specifikacije in standardi so bolj ali manj še v fazi nastajanja. Največ dela poteka v okviru standardizacijskih teles OASIS, W3C in IETF [32].

Vendar uporaba standardov za spletne storitve prinaša nekaj zadržkov: spletne storitve (še) niso preizkušena tehnologija; njihova tesna povezanost z metajezikom XML in protokolom SOAP povzroča dodatne podatke in s tem poveča velikost sporočil. Vprašanje se tako nanaša na to, ali prednosti XML prekašajo zahteve po dodatnih zmogljivostih, prostoru in procesiranju.

3.3.2 Zgodovina spletnih storitev

Ozadje, ki je pripeljalo do spletnih storitev, je povezano najprej s tehnologijami in koncepti, ki so se prvič pojavili v drugi polovici zadnjega desetletja prejšnjega stoletja, vsi pa so imeli skupen medij, to je svetovni splet. To so programi v obliki odjemalskih programčkov, ki so znali komunicirati s spletnim strežnikom.. Danes le-ti tvorijo spletne strani na veliko strežnikih, namenjeni pa so predvsem povezovanju z zalednimi sistemi. Sočasno se je začela tudi »revolucija« z uporabo metajezika XML in vseh protokolov, ki so se gradili na njem. Na začetku so bili to lastniški protokoli, ki so bili predani v uporabo na zahtevo standardizacijskih teles[33] ali kot protokoli neformalnih združenj zainteresiranih podjetij[34]. Kmalu je nastalo formalno združenje za standardizacijo, imenovano OASIS. Nadaljevalo se je s predstavitvijo modela ponudnikov aplikacij (ASP – angl. Application Service Provider), ki so ga zelo podpirali največji svetovni proizvajalci programske opreme, vendar je preživelo le nekaj podjetij, ki so se tedaj osnovale na takšnem poslovnem modelu. Naslednja tehnologija, ki je tudi zelo pomembna pri razvoju spletnih storitev, je J2EE (Java 2 Enterprise Edition), ki se uporablja v trinivojskih arhitekturah kot sredinska raven. Takrat se je pokazalo, da Java ne bo tako zelo uspešna na uporabniških namizjih, zelo dobra pa bi lahko bila kot dostavna platforma v odprtih, programsko neodvisnih okoljih. Tudi podjetje Microsoft je kmalu odgovorilo z novo tehnologijo, poznano kot Microsoft.NET. Nekaj rešitev in konceptov so spletne storitve pobrale tudi s področja porazdeljenih sistemov (DCE,

---

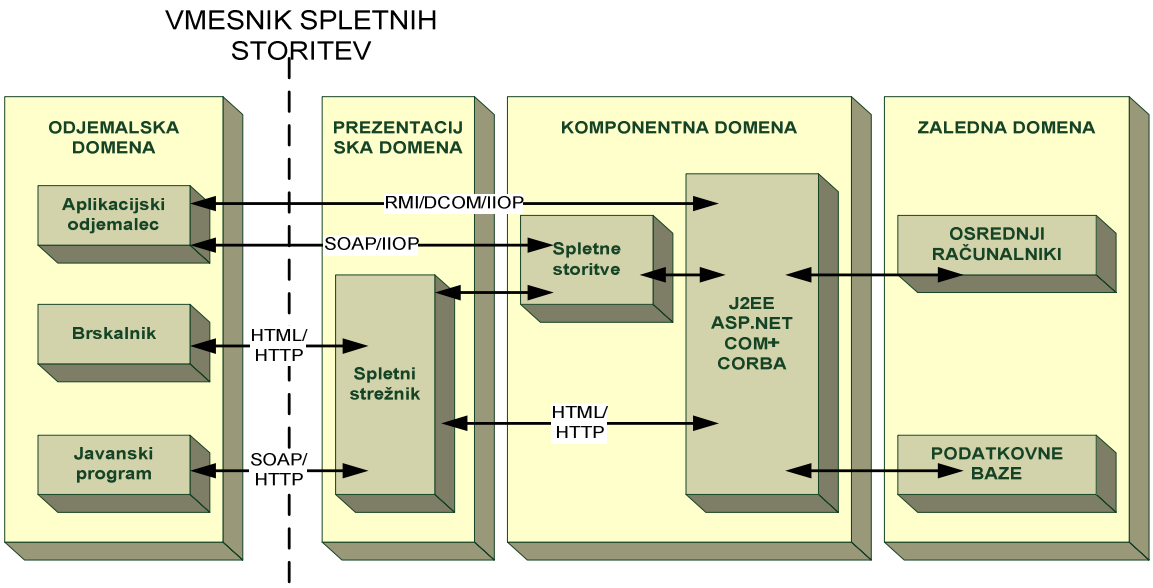
[32] Natančnejše obrazložitve in nove oziroma spremenjene objave protokolov se nahajajo na straneh omenjenih teles, celoten opis vseh protokolov iz okolja spletnih storitev pa se nahaja na spletnih straneh http://www-136.ibm.com/developerworks/webservices/ (27. 3. 2004).

[33] Podjetje CommerceOne (http://www.commerceone.com) je naredilo protokol CBL, ki se je pozneje vključil v ebXML, ki je sedaj standard OASIS.

[34] Večje število RosettaNet, ki je sedaj prav tako obravnavan kot predhodnik ebXML.

CORBA. DCOM) in protokolov za sporočanje na srednji ravni ((Hartman et.al, 2003, str. 100).

Slika 12 - Tipično okolje spletnih storitev



Vir: Hartman et.al., 2003, str. 100)

3.3.3 Vodniki za izdelavo varnih spletnih aplikacij

Osnovni vodniki, ki v današnjem svetu poganjajo vse širšo razpredenost spletnih storitev v svetovnem spletu, intranetih, ekstranetih in drugje, so (Baltimore, 2003, str. 6–9) naslednji:

- Programska oprema kot storitev. To je ideja večine velikih ponudnikov programske opreme, integratorjev in drugih zainteresiranih, ki zori že dolgo časa, vendar je šele s spletnimi storitvami postala realnost.
- Integracija aplikacij, sistemov in poslovanja med podjetji. Podatkovna integracija in sinhronizacija prek omrežij postaja enostavnejša in hitrejša, vzdrževanje enostavnejše, prav tako ponovljivost uporabe napisanih vmesnikov.
- Zmanjšanje stroškov. Statistike kažejo, da vzdrževanje programske opreme lahko predstavlja 80 % stroškov sistema, enak odstotek se pojavlja tudi pri integraciji novega izdelka v obstoječe okolje. Spletne storitve so osredotočene predvsem na zmanjšanje teh dveh stroškovnih nosilcev.
- Ena platforma in odprtost. Po nekaj letih opazovanja vojne med različnimi operacijskimi sistemi (Unix proti Windows) imajo informatiki raje platformo, ki omogoča kreiranje in nameščanje aplikacij ne glede na uporabljeno nižje ležečo

tehnologijo. Spletne storitve v bistvu prinašajo novo platformo – »internetni operacijski sistem«. Omogočajo podjetjem, da ne zavržejo obstoječih rešitev, temveč da izgradijo vmesnike, s katerimi lahko dostopajo do drugih starejših aplikacij.

- Široka uporaba profesionalnih računalniških idej. Končno se lahko uporabljajo preizkušene ideje, kot je CORBA, ki so dozorele v zadnjih 20 letih v računalniških laboratorijih in tehnoloških podjetjih.

- Mrežna uporaba računalnikov. Osnovni tehnični cilj je zmožnost porazdeljevanja računalniških zmogljivosti neposredno med podjetji.

- Poslovni objekti in programiranje poslovnih procesov. Osnovna ideja je, da se lahko z uporabo poslovnega programiranja spletnih storitev omogoči hitro prilagajanje novim spremembam v poslovnem svetu in hitro integriranje v druga podjetja.

- Mobilnost človeških, finančnih in informacijskih zmogljivosti. Vse večja globalnost današnjega poslovanja se podpira s spletnimi storitvami. Delo na domu, prodaja na terenu, integrirana nabavna veriga, uporabniške strani in podobno postaja resničnost.

Vsi porazdeljeni modeli v preteklosti, prav tako marsikatere ostale tehnologije, so bili narejeni na način »najprej je treba izdelati delujoče stanje, nato pa se bomo lotili še varnosti« in spletne storitve niso nobena izjema. Rezultat je slabo delovanje in zelo težavna uporaba varnostnih mehanizmov. Varnost je sedaj postavljena na prvo mesto med zaviralci večje uporabe spletnih storitev (Hartman et.al, 2003, stran 20). Porazdeljena varnost je namreč popolnoma nov koncept v informatiki. Varnost spletnih storitev (v nadaljevanju **WSS**[35]) uporablja približno enake varnostne pristope in mehanizme, kot so jih uporabljali pred razvojem spletnih storitev, s to razliko, da upošteva temeljno filozofijo razpršenosti storitev vsepovsod po internetu, kar pomeni velik poudarek na zagotavljanju fleksibilnosti uporabljenih varnostnih modelov.

Osnovne varnostne zahteve in mehanizmi se rešujejo z uporabo specifikacij spletnih storitev, povezanih z varnostjo, ki v zadnjem času zelo hitro nastajajo in se dopolnjujejo. Vse imajo skupno tehnološko osnovo, sporočanje v obliki kombinacije XML in SOAP. Pri sprejemu sporočila mora biti aplikacija prepričana v njegov izvor in skladnost, kar se zagotavlja z digitalnimi podpisi, zajetimi v sporočilo. Pošiljatelj mora digitalno podpisati sporočilo pred pošiljanjem, prejemnik pa ga najprej preveriti. Ker je format spletnih storitev XML, se za digitalno podpisovanje uporablja **standard za digitalno podpisovanje dokumentov, zapisanih v XML**, ki je natančneje opisan v poglavju 3.4. Zagotoviti je treba tudi zaupnost, zasebnost in tajnost sporočila, ko je le-to na poti. Zato se uporablja **standard za digitalno šifriranje dokumentov, zapisanih v XML** (poglavje 3.4.2). Oba standarda, skupaj z opisi glave sporočila SOAP, sodita med osnovne elemente standarda WSS.

[35] WSS – Web Services Security.

Trenutne aplikacije spletnih storitev se izvajajo večinoma znotraj podjetij, pričakuje pa se, da se bodo počasi začele vpletati/vključevati tudi zunanje aplikacije. To je zelo velik korak naprej, saj se zahteva premik k storitveno orientiranim arhitekturam. Nekateri se z njim ukvarjajo že od leta 1998 (Banking Technology, nov.2003, stran 21), saj se zavedajo tovrstnih potencialov. Ena najpomembnejših zahtev pri porazdeljeni varnosti je enkratna prijava za celotno storitveno domeno. S tem se arhitekti izogibajo zahtevam po stalno ponavljajočem se posredovanju uporabniških imen in gesel. Specifikacija, ki se ukvarja s tem, je **jezik za označevanje z izjavo o varnosti SAML** (Security Assertions Markup Language). Njegova uporaba je pregledna za uporabnika, saj deluje v ozadju, prenaša pa tri vrste informacij, ki se imenujejo izjave:

- izjave o overitvi (informacije o overjenih uporabnikih in času overitve),
- atributne izjave (informacije o uporabnikih in njihovih atributih) in
- izjave o nadzoru dostopa (informacije o uporabnikovih dovoljenjih, pravicah in privilegijih).

Z omenjeno porazdeljeno varnostjo se ukvarja več podjetij, skupin in standardizacijskih teles. Začelo se je z namenom programerskega giganta Microsoft, da uvede dejanski standard za enkraten vpis[36]. Na odgovor industrije ni bilo treba čakati dolgo, saj se je konec leta ustanovila zveza Liberty Alliance[37], katere glavni zagovornik je bilo konkurenčno podjetje Sun Microsystems. Danes je v zvezi prek 160 organizacij iz različnih sfer (programska podjetja, storitvena, industrija …). Specifikacije, ki so jih izdali, temeljijo na SAML, SOAP, XML in WSS. Zelo podobna specifikacija, ki je v nastajanju, njeni avtorji pa so iz podjetij IBM, Microsoft, BEA in RSA Security, se imenuje WS-Federation. Med napredne varnostne arhitekture za spletne storitve sodijo tudi nove storitve za digitalno podpisovanje (Digital Signature Services DSS). Na podlagi DSS se bodo lahko spletne storitve same pogovarjale o preverjanjih in izdelavi digitalnih podpisov, kar je tudi začetni pogoj za uvedbo neodvisnih storitev za spletno varnost, kamor sodijo preverjanja, časovni žigi itn.

3.4 S-XML: Rešitev varnostnih vprašanj pri uporabi XML

Metajezik XML določa predvsem sporočila za izmenjavo med sistemi, posledično pa se z njimi ukvarja tudi rešitev varnostnih vprašanj dokumentov, zapisanih v XML, ki je nastala pod okriljem W3C, imenuje pa se S-XML (angl. Secure XML). Osnovni standardi, ki so uporabljeni, so podpisovanje dokumentov, zapisanih v XML (W3C, 2002a), v nadaljevanju

[36] Podjetje Microsoft je leta 1998 kupilo podjetje Firefly Network in kmalu za tem predstavilo storitev Microsoft Password. Z agresivno kampanjo je želelo pridobiti vse velike spletne strani, da vgradijo njihovo tehnologijo, vendar se je nekaj let pozneje pokazalo, da se uporablja le na Microsoftovih straneh in na največji avkcijski strani eBay (http://www.ebay.com).

[37] Glej: http://www.projectliberty.org/.

XMLDSIG, in šifriranje dokumentov, zapisanih v XML (W3C, 2002b), v nadaljevanju **XMLENC**. Z XMLDSIG se lahko obdelujejo dokumenti in sporočila v poljubnem formatu, namenjen pa je predvsem dokumentom XML, kjer se lahko podpisujejo ali šifrirajo celotni dokumenti ali samo poljubni deli. Prav v tem se pokaže njegova prava moč. Ker so bili omenjeni standardi zasnovani zelo na široko, je rezultat viden že danes, saj je na tej osnovi nastala cela vrsta novih specifikacij in specifičnih standardov, ki se uspešno uporabljajo na številnih področjih in v industrijskih panogah.

Poleg dveh že omenjenih, najvažnejših standardov tvori S-XML še nekaj drugih, ki pokrivajo vsak svoje področje. V poglavju 3.3.1 sta bila omenjena tretji gradnik, ki je namenjen upravljanju s ključi, to je XKMS, in četrti, ki je namenjen overjanju in nadzoru dostopa, to je SAML. V to skupino sodijo še standard XACML (angl. XML Access Control Markup Language) in številne aplikacije, kot so WSS, platforma za zasebnost P3P (angl. Platform for Privacy Preferences), upravljanje z digitalnimi pravicami XrML (angl. eXtensible Rights Markup Language). S-XML prinaša celo vrsto tehničnih standardov, ki zagotavljajo varnostne zahteve v svetu sporočil XML. Ukvarjajo se z definicijo slovarjev za predstavitev varnostnih informacij, z uporabo ostalih že narejenih standardov XML, kjer je možno, z zagotavljanjem varnosti od začetka do konca, z uvrstitvijo obstoječih standardov in tehnik na področju varnosti v svet XML, s prožnostjo jezika XML in njegovo uporabo za poenostavitev robustne strukture PKI ipd. Čeprav XML ne prinaša nič izrazito novega, pa učinkovito rešuje probleme predstavitve varnostnih atributov. Vsak standard tako definira **slovar XML**, ki je potreben za opis varnostnih informacij, kot tudi **pravila za procesiranje**, potrebna za razumevanje pred implementacijo standarda v aplikacije.

3.4.1 Podpisovanje dokumentov, zapisanih v XML

Priporočilo za digitalno podpisovanje dokumentov, zapisanih v XML, definira mehanizme za izdelavo digitalnih podpisov in preverjanje le-teh, prav tako podpira druge mehanizme, ki so namenjeni digitalnim podpisom. Definira, kako se digitalni podatki podpisujejo in kako se naj izdelan podpis vključi v dokument XML. Dovoljeno je podpisovati:

- celotne dokumente XML ali le njihove dele,
- poljubne dokumente, lahko tudi v binarni obliki,
- sestavljene dokumente, tudi več naenkrat,
- podpise, kar vodi do dvojnih podpisov (podpis znotraj podpisa), in
- lastnosti dokumenta.

Uporabljajo se obstoječi algoritmi za podpisovanje, izdelavo prstnih odtisov sporočil in za simetrične podpise. Podpisovanje dokumentov, zapisanih v XML, se lahko izvaja celo brez digitalnih potrdil, npr. z overiteljskim mehanizmom Kerberos (Ford, 2001, str. 124–126),

uporabnim v operacijskem sistemu Microsoft Windows. Znotraj izdelave podpisanih dokumentov, zapisanih v XML, se uporabljajo še druge nujno potrebne metode. Normalizacija dokumenta XML je zaradi robustnosti metajezika XML nujna, saj odstrani nepotrebne znake (presledki, prelomi strani ipd.). Pomembne so tudi metode procesiranja. Zaradi teh lastnosti je digitalno podpisovanje XMLDSIG bolj kompleksno od digitalnega šifriranja XMLENC, saj je med drugim treba poskrbeti za konsistentnost podatkov.

Proces izdelave digitalnega podpisa v dokumentih XML in njegovega preverjanja poteka v sedmih korakih:

1. Najprej je treba izvesti vse zahtevane transformacije na dokumentu XML v določenem vrstnem redu. Izvajajo se z namenom pripravljanja ustreznih podatkov za podpisovanje, npr. uporaba transformacije base64[38].
2. Izvede se zgoščevanje (prstni odtis) rezultata transformacij.
3. Pripravi se referenčni element, ki vsebuje informacijo o lokaciji podatkovnega objekta, ki se podpisuje, uporabljene transformacije, algoritem za kreiranje prstnega odtisa in vrednost prstnega odtisa. Lahko se pripravijo elementi z več referencami, saj se lahko naenkrat podpiše več objektov.
4. Nadaljuje se kreiranje elementa, ki specificira metodo za podpisovanje, normalizacijsko metodo in vsebuje vse reference, narejene v prejšnjem koraku.
5. Na vrsti je normalizacija z izbrano metodo.
6. Sledi podpisovanje dokumenta XML ali dela dokumenta z uporabo določenega algoritma. Po navadi je to izdelava prstnega odtisa nad normaliziranim elementom in zatem njegovo podpisovanje.
7. Na koncu je treba zgraditi še element »Signature«, ki je sestavljen iz elementov »SignedInfo«, »SignatureValue« in po želji še »KeyInfo« in »Object«.

V procesu digitalnega podpisovanja dokumenta XML se tvorijo dodatne značke, ki vsebujejo informacije o podpisu (element <SignedInfo>), informacije o uporabljenem ključu, kar ni obvezno (element <KeyInfo>), in druge podatke, ki se podajo v elementu <Object>. Korenski element se imenuje <Signature>.

Primer dokumenta XML z vsemi potrebnimi elementi za zagotavljanje digitalnega podpisa dokumenta, zapisanega v XML na osnovi XMLDSIG,je prikazan na sliki:

[38] Base64 predstavlja kodiranje binarnih podatkov v enostaven tekst, zapisan v formatu ASCII, natančneje samo s 64 znaki (A-Z, a-z, 0-9,+ in /). Uporablja se v elektronski pošti.

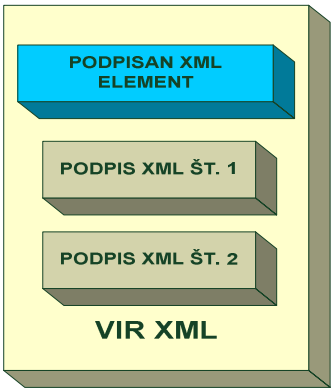
Slika 13 - Primer podpisa v dokumentu XML

```
<Document>
  <Content Id="digital_contract">
    <Contract><html></html></Contract>
  </Content>
 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="provider">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"></CanonicalizationMethod>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></
SignatureMethod>
    <Reference URI="#digital_contract">
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
    <DigestValue>LXZhUbr/kptL1rRgB7sfcjxt6bA=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
        rezultat digitalnega podpisa
  </SignatureValue>
  <KeyInfo>
    <X509Data>
     <X509Certificate>
        digitalno potrdilo v berljivem formatu
      </X509Certificate>
    </X509Data>
  </KeyInfo>
 </Signature>
</Document>
```

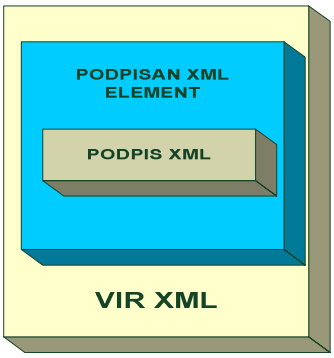
Informacije o podpisu, ki se nahajajo pod elementom <SignedInfo>, so najkompleksnejši del podpisa, saj so po priporočilu W3C vedno zahtevan element, vsebujejo pa informacije o uporabljeni normalizacijski metodi, kar se označuje s <ChanonicalizationMethod>, uporabljen algoritem za podpis <SignatureMethod> in eno ali več referenc na podpisane podatke. Tisti elementi, ki opisujejo uporabljene metode in algoritme, vsebujejo zgolj kazalce na sredstva in nimajo nobene povezave s podpisljivimi podatki. Referenca oziroma kazalnik na podpisane podatkepa dejansko nakazuje, kaj se podpisuje. Ali so znotraj dokumenta XML ali zunaj, je odvisno od uporabljene vrste podpisa XML. Element <Reference> poleg kazalca na podpisovane podatke vsebuje tudi njihov prstni odtis. **Informacija o ključu** je element, imenovan <KeyInfo>, ki dejansko ni zahtevan, je pa priporočljiv. Zajema namreč podatke, potrebne za preverjanje podpisa, ki so lahko neposredni (digitalno potrdilo, tudi kakšen drug standard) ali posredni (kazalec na imenik, kjer se nahaja digitalno potrdilo). Največjo podporo imajo (trenutno) digitalna potrdila, saj sodi v ta sklop cela vrsta elementov, kot so serijske številke, ime pošiljatelja ipd. Informacija o ključu aplikaciji olajša delo pri preverjanju podpisa, saj ni potrebno iskanje potrdila po spletu, vsekakor pa obstaja dejstvo, da navkljub veljavnosti potrdila v dokumentu XML to ne pomeni, da je uporabljeno potrdilo še dejansko veljavno – pregled seznama preklicanih potrdil ali uporaba spletne storitve na osnovi XKMS je še vedno zelo priporočljiva. Za vse **druge informacije**, kot so vrsta podpisanih podatkov ali časovni žigi, se uporablja element <Object>, kjer so zaradi izogibanja navzkrižjem vsi uporabljeni objekti enolično identificirani.

Standard XMLDSIG predvideva tri vrste podpisov dokumentov, zapisanih v XML. Katera vrsta podpisovanja se uporablja, je odvisno od aplikacije in njenih zahtev. Nekatere želijo podpisati celoten dokument XML, tako da je podpis del podpisanega dokumenta (**vsebovani** podpis – enveloping), ponekod je bolj primerna uporaba dodanega podpisa k dokumentu XML, kar se označuje kot **dodani** podpis (enveloped), če se pa podpisuje zunanji dokument, se imenuje **ločeni** podpis (detached). Element <Signature> v prvem primeru vsebuje element, ki ga podpisuje, v drugem primeru je njegov podrejeni element, v zadnjem pa je ločen od elementa, ki ga podpisuje.

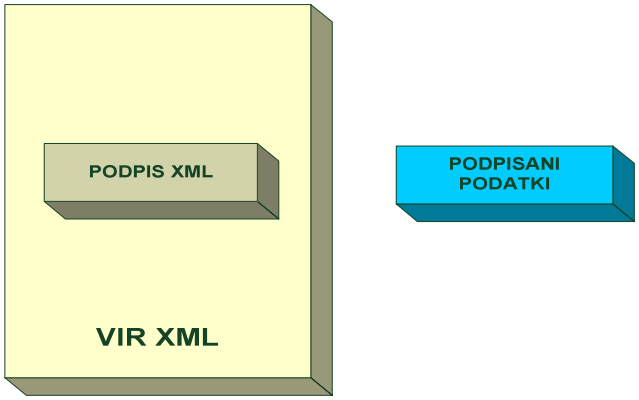
Slika 14 - Dodan podpis – Enveloped



Slika 15 – Vsebovan podpis - Enveloping



Slika 16 - Dodan podpis –Detached



Pomemben del podpisovanja XML je **preverjanje podpisa**, ki ga izvaja prejemnik dokumenta. Tudi preverjanje vsebuje več faz, ki se morajo izvesti zaporedno, da lahko prejemnik pride do odgovora na zastavljeno vprašanje – ali podpis potrjuje pristnost poslanega dokumenta ali ne. Na začetku se izvede normalizacija elementa <SignedInfo> po definirani metodi. Za to je treba pridobiti podatke, na katere kažejo kazalci, in jih ustrezno procesirati, rezultat pa se normalizira. Z matematično transformacijo sledi priprava prstnega odtisa. Na tem mestu se že lahko izvede primerjanje pridobljenih odtisov z vsebovanimi v dokumentu, če sta odtisa različna, preverjanje dokumenta spodleti. Ob ustreznosti je treba preveriti še identiteto pošiljatelja. V veliko pomoč je izpolnjen element <KeyInfo> in javni ključ pošiljatelja, če ga ni, ga mora aplikacija pridobiti drugje.

3.4.2 Šifriranje dokumentov, zapisanih v XML

S priporočilom W3C s konca leta 2002 o sintaksi za šifriranje in procesiranje so definirani **procesi za šifriranje digitalnih podatkov** in **načini vstavljanja** dobljenih rezultatov šifriranja v dokument XML. Le-ti podpirajo šifriranje celotnega dokumenta XML ali samo njegovih delov, pri čemer predpostavljajo, da je najmanjši del, ki se lahko šifrira samostojno, element. Dopuščena je tudi možnost »superšifriranja«, kar pomeni dodatno šifriranje že procesiranih podatkov. Podobno kot podpisovanje XML tudi to priporočilo ne želi definirati novih algoritmov šifriranja, saj uporablja že narejene simetrične in asimetrične algoritme za šifriranje/dešifriranje, izmenjavo ključev, zgoščevanje, overjanje in druge, razen algoritmov za podpisovanje, logično pa definira tudi način dešifriranja dokumenta XML.

Zgradba dokumenta XML, v katerem se nahajajo šifrirani podatki, se razlikuje od navadnih dokumentov XML po elementu <EncriptedData>. Le-ta vsebuje šifrirane podatke in ostale elemente o načinu šifriranja. Sami podatki, ki so rezultat šifriranja, se nahajajo v elementu <CipherData>. Način šifriranja in velikost šifrirnega ključa je zapisan v <EncryptionMethod>, dodan pa je lahko še ključ, uporabljen za šifriranje. Priporočilo predpisuje uporabo vseh načinov zapisovanja uporabljenih ključev, tako kot to definira priporočilo za podpisovanje dokumentov. Pri tem je treba upoštevati dejstvo, da v primeru

uporabe simetričnih algoritmov zapis ključa ni smiseln in takrat se zapiše le ime ključa, aplikacija za dešifriranje pa seveda mora poznati vrednost ključa. Primer uporabe šifriranja XML za dokument XML, ki vsebuje občutljive informacije, kot je npr. številka kreditne kartice za izvedbo plačila, se nahaja na sliki 17. Pri tem je pomembno to, da dokument ne skriva elementa <CreditCard>, temveč le dela, ki vsebuje kritične informacije (številko kartice).

Slika 17 - Dokument XML z občutljivimi informacijami in njihova enkripcija z uporabo šifriranja XML

Procedura za šifriranje elementov XML se začne z določitvijo algoritmov in parametrov za šifriranje. Sledi pridobivanje ključev in šifriranje podatkov. Rezultat je niz znakov, ki se ga mora v naslednjem koraku zamenjati z nešifriranim delom.

Uporaba šifriranja XML je zelo raznolika, saj priporočilo dopušča šifriranje dela ali celotnega dokumenta XML, izpuščanje določenih elementov, kot je npr. <KeyInfo>, izbiro algoritmov in dolžin uporabljenih ključev, nikjer pa ne zapisuje, kako naj se uporablja v aplikacijah, npr. v SOAP.

3.5 Praktična uporaba S-XML

Elektronsko poslovanje, zakoni s tega področja, digitalna potrdila, infrastruktura javnih ključev in ostala tehnološka oziroma pravna področja postanejo uporabni šele tedaj, ko se vzpostavijo razmere za izvajanje elektronskega poslovanja v skladu s pravno-formalnimi in varnostnimi razmerami. Osrednjo vlogo imajo tako aplikacije – nekatere pridobijo veliko prednost z integracijo digitalnih potrdil oziroma brez njih sploh ne morejo delovati, druge pa lahko dopolnijo svojo celovitost z dodatno funkcijo uporabe potrdil. Glede na funkcionalnost se delijo na naslednja področja:

- varna elektronska pošta: z uporabo varnostnih mehanizmov se zagotavlja skladnost, zasebnost in overjanje pošiljatelja elektronske pošte;
- varne komunikacije: SSL z overjanjem strežnika, SSL z overjanjem strežnika in uporabnika, navidezna zasebna omrežja (Virtual Private Network, VPN) z uporabo varnostnega protokola IP (IP Security, IPSec);
- varne transakcije v e-poslovanju: digitalno podpisane transakcije (izpolnjeni obrazci na spletnem strežniku), ki zagotavljajo izvor transakcije s strani lastnika digitalnega potrdila;
- podpisane programske datoteke: Programski izdajatelji lahko podpišejo programsko kodo in končnim uporabnikom zagotavljajo, da je programska koda njihova in nespremenjena.

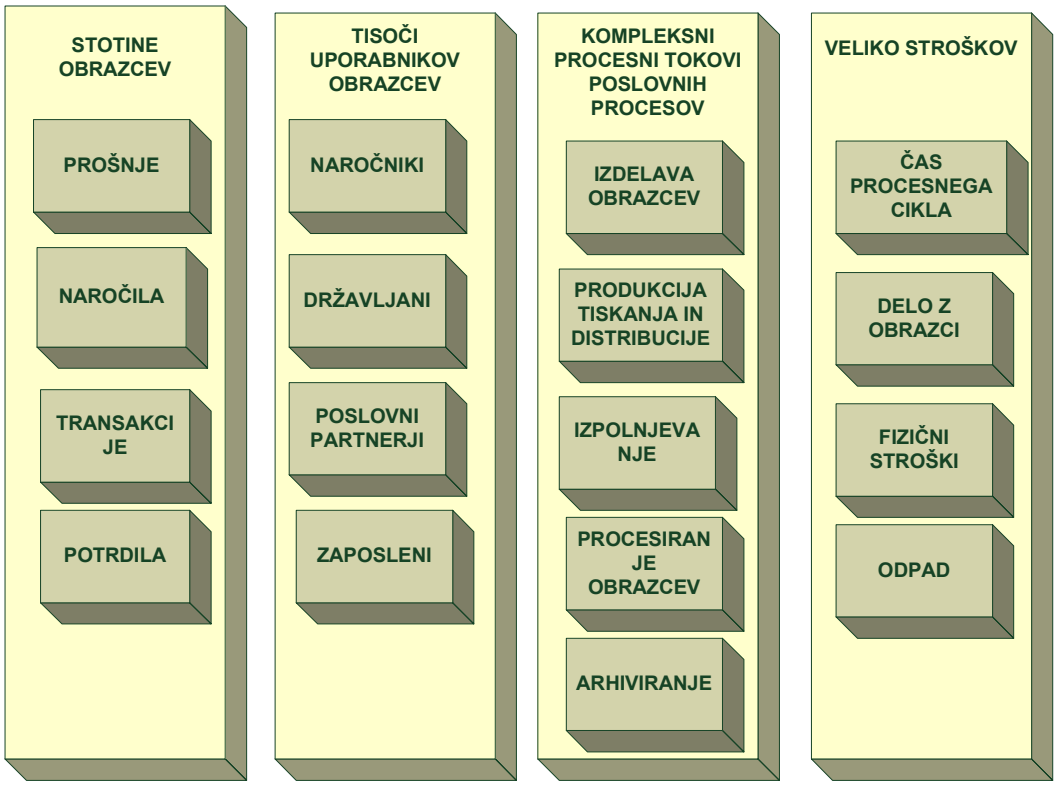
Uvedba PKI in overitelja brez storitev, ki uporabljajo njegovo funkcionalnost in doda le dodano vrednost uporabniku, je nesmiselna. To je tudi razlog za počasno napredovanje uvajanja in implementacij ne samo v domačem merilu, temveč tudi v svetovnem. V tem času je varnostna tehnologija dozorela, začetne napake in težave (predvsem na funkcionalnosti in povezljivosti različnih programskih oprem) so odpravljene, tako da so postale aplikacije najvažnejši del nadaljnjega uspeha PKI. Vendar je zmotno razmišljanje marsikaterih načrtovalcev, da je z implementacijo asimetrične kriptografije in digitalnih potrdil v njihove aplikacije dovolj le zahteva po njihovi uporabi oziroma še skrajnejši primer, da bodo uporabniki sami spoznali uporabnost potrdil in jih začeli uporabljati. V nadaljevanju so prikazani nekateri primeri, kako se v svetovni praksi uporablja infrastruktura javnih ključev, predvsem v navezi z digitalnim podpisovanjem dokumentov, zapisanih v XML.

3.5.1 Avtomatizacija poslovanja z obrazci (e-obrazci)

Vsakodnevno poslovanje storitvenih podjetij se ukvarja z nepreglednim številom papirnih obrazcev, ki jih izpolnjujejo naročniki, administrativni delavci, pogodbena podjetja itd. S tem se ne srečujejo le velika podjetja, temveč tudi manjša, skratka vsi. Z ročnim izpolnjevanjem obrazcev, tudi prek spleta, se začnejo in upravljajo veliki kompleksni poslovni procesi.

Podjetja se ukvarjajo z izdelavo, razvrščanjem, ažuriranjem in razpošiljanjem obrazcev, ki so praviloma v papirni obliki.

Slika 18 - Poslovni obrazci v papirni obliki



Vir: Moon, 2004, str. 5

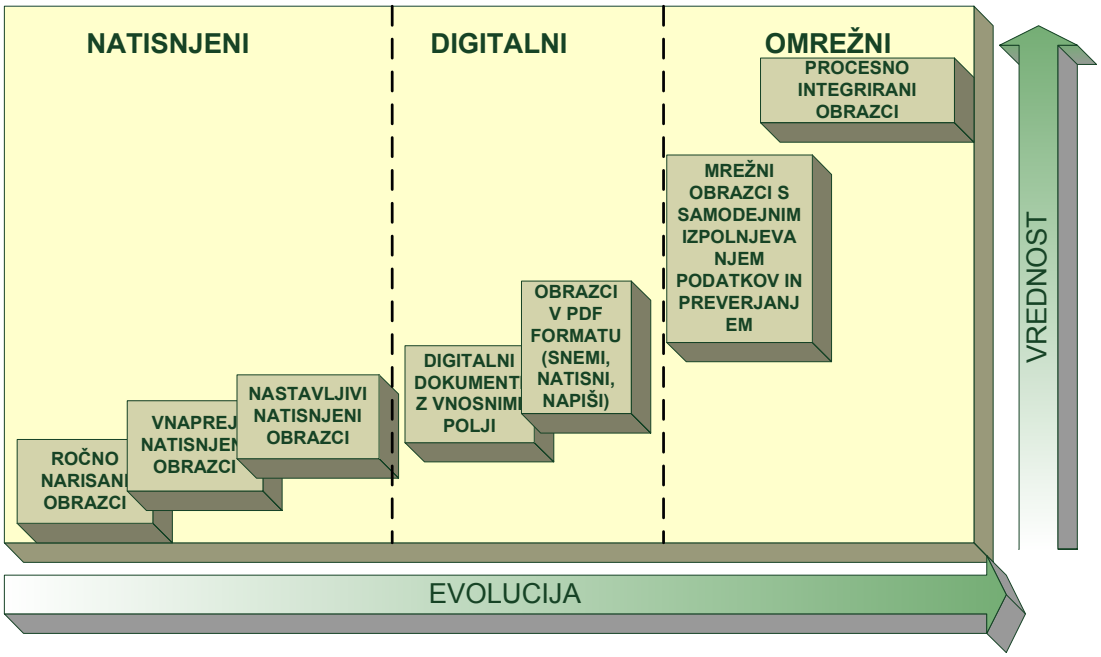
V večjem podjetju je v obtoku na stotine obrazcev (različne prošnje, sporazumi, naročila, materialno poslovanje, podaljšanje ...), ki jih izpolnjuje na tisoče uporabnikov. To so lahko naročniki, državljani, javni uslužbenci, poslovni partnerji, tudi zaposleni znotraj organizacije. Poslovni procesi pri obvladovanju dela z obrazci v papirni obliki so zelo zapleteni in dolgotrajni. Začne se pri oblikovanju obrazcev (raziskovanje namena, izdelava, oblikovanje podatkovnega modela, oblikovanje videza, pridobitev potrditve), naslednja faza pa je tiskanje (dostava tiskarju, izdelava matrice, potrditev testnih primerov, tiskanje in skladiščenje). Tretja faza je razpošiljanje obrazcev na vsa mesta, kjer so njihovi uporabniki (pobiranje naročil, pakiranje, dostava, shranjevanje in izdelave vse spremne dokumentacije). Šele po zaključeni tretji fazi je na voljo poslovni proces izpolnjevanja obrazcev, ki zajema pridobitev obrazca, izpolnjevanje, pojasnjevanje vprašanj, pošiljanje ali oddajo obrazca .... V podjetju se začne faza procesiranja obrazcev (pridobitev obrazcev, sortiranje, vstavljanje dodatnih podatkov, preverjanje pravilnosti vstavljenih podatkov, zavračanje obrazcev oziroma zahtevanje dopolnitve, pošiljanje obrazložitev zavrnitve, pošiljanje potrdila o prejemu ...). Končni proces je arhiviranje prejetih in obdelanih obrazcev. Pri tem nastaja veliko nepotrebnih stroškov, ki so posledica:

- tiskanja papirnih obrazcev, skladiščenja praznih, razpošiljanja, arhiviranja obdelanih obrazcev,
- izmeta neuporabljenih obrazcev, ki so zastareli,
- podaljšanja izvajanja celotnega cikla pridobitve in procesiranja obrazcev kot posledica fizične logistike ter
- dodatnega dela.

Poslovni proces z obrazci v papirni obliki je tog, neučinkovit, zelo drag, obdan s številnimi napakami kot posledica ročnega dela in se upira izboljšavam oziroma jih onemogoča.

Evolucija poslovnih obrazcev se je začela z ročno napisanimi obrazci. Le-te so sčasoma začeli zamenjavati vnaprej natisnjeni, ki so se pozneje začeli pojavljati tudi v poosebljenih oblikah, vsi pa so tvorili ero papirnih obrazcev. Sledila je digitalna era, kamor sodijo digitalni obrazci z vnosnimi polji, in spletni obrazci, ki jih uporabniki izpolnijo in končane natisnejo ter pošljejo v podjetje. Evolucija obrazcev se na tej točki ni ustavila, saj je sedaj obdobje mrežnih, elektronskih obrazcev. Obrazci so postali »pametni«, saj spletne aplikacije že same izpolnjujejo zahtevane podatke (npr. na osnovi overjanja uporabnika in njegovih shranjenih podatkov v zbirki) in opravljajo potrebne verifikacije vnesenih podatkov. Takšni obrazci so praviloma že vpeti v poslovne procese podjetja, s katerimi se lahko začne obdelava poslanih obrazcev takoj po njihovi oddaji. Njihova evolucija je prikazana na 19.

Slika 19 - Evolucija poslovnih obrazcev



Vir: Moon, 2004, str. 7

Celoten cikel pametnih obrazcev je sestavljen iz naslednjih faz:

- izdelava obrazca (aktivnosti raziskovanja, izdelava podatkovnega modela, pisanje teksta in izdelava skript, dopolnjevanje ...),
- oblikovanje (obrazec se oblikuje na novo ali na podlagi pripravljene predloge, oblikovanje teksta, vnosnih polj in grafike, usklajevanje),
- izdelava (izbira medija(ev), kopiranje na prave lokacije, priprava ustreznih elektronskih formatov),
- razpošiljanje (izvajanje vseh potrebnih logističnih aktivnosti, povezanih s poslovnim procesom),
- izpolnitev (uporabniki morajo najprej najti ustrezen obrazec, ga prenesti na svoj računalnik, izpolniti vnosna polja, po potrebi uporabiti pomoč kontaktnih centrov podjetja, podpisati in poslati podjetju prek elektronske pošte oziroma drugih ustreznih spletnih protokolov),
- procesiranje izpolnjenega obrazca (pridobitev izpolnjenih obrazcev, razvrščanje v ustrezne razrede, usmerjanje na ustrezne naslove, sprejetje oziroma zavrnitev, obveščanje uporabnikov o (ne)uspešnem sprejetju obrazca, dopolnjevanje s podatki, izločanje podatkov za nadaljnjo procesiranje ...) in

- arhiviranje (razvrstitev, priprava na arhiviranje, transport v e-skladišče, vnos v arhiv, priprava na dostop do obrazca na zahtevo in izločitev obrazcev iz poslovnega procesa).

Integriran sistem elektronskega procesiranja obrazcev prinaša precejšnjo dodano vrednost poslovnim procesom, vendar z različno utežjo glede na navedene faze celotnega cikla pametnih obrazcev. Osnovne funkcije lahko razvrstimo na štiri razrede – integracija z vsebinskim procesom, avtomatizirano pridobivanje podatkov, enostavnost uporabe in zagotavljanje varnosti podatkov. Procesna integracija vsebine prinaša veliko dodano vrednost na skoraj celotnem ciklu, medtem ko avtomatizirano pridobivanje podatkov pokaže svojo moč v fazah izpolnjevanja obrazcev in kasnejšem procesiranju. Enostavnost uporabe je izrazita pri izdelavi obrazcev, razpošiljanju in predvsem pri izpolnjevanju obrazcev, varno pridobivanje podatkov pa je zelo pomembno pri prenašanju, procesiranju in arhiviranju izpolnjenih obrazcev.

Avtomatizacija zajema in procesiranja podatkov je realnost, brez česar sodobno podjetje v vse bolj konkurenčnem okolju ne more več poslovati. Prenos papirnih obrazcev v elektronsko obliko naj se začne z enostavnimi obrazci, uporabniško orientiranimi, ki dopuščajo možnost napak, saj že v papirni obliki niso povsem natančni oziroma potrebujejo preverjanje in popravljanje. Takšni obrazci so po navadi na začetku poslovnega procesa, ki jih izpolnjujejo novi ali potencialni naročniki in s tem sprožijo izpolnitev naročenega s strani podjetja. Naslednja vrsta obrazcev, transakcijski obrazci, že na podlagi vnesenih podatkov računa in dopolnjuje obrazec s svojimi podatki, vsekakor pa ne dopušča več veliko svobode pri vnašanju. Rezultat je večja hitrost poslovnega procesa in zmanjševanje napak. Obstajata še dve vrsti obrazcev, ki sodijo v višjo skupino glede zahtevnosti svoje vpeljave v elektronsko obliko. Zahtevajo zaupno in tajno obravnavo ali sodijo pod regulativni nadzor (npr. e-dohodnina in ostali obrazci Davčnega urada Republike Slovenije[39]). Integriran sistem procesiranja elektronskih obrazcev je po navadi sestavljen iz vseh naštetih vrst obrazcev in ponuja elektronsko obdelavo podatkov, pridobljenih za pridobivanje informacij in procesiranje transakcij ob ustreznem upoštevanju regulativnih predpisov v lokalnem in globalnem okolju.

Svetovalno podjetje Gistics[40] je tehnične funkcionalnosti integriranega sistema za procesiranje elektronskih obrazcev, ki zagotavljajo pomembne performančne rezultate, razdelilo na naslednje skupine, ki so po pomembnosti navedene v padajočem vrstnem redu (Moon, 2004, str.14):

[39] Več na spletnem naslovu http://edavki.durs.si.

[40] Glej: http://www.gistics.com.

- integracija vsebinskih procesov (globalni repozitorij, ponovna uporaba vsebine, prožilci v delovnih potekih, kontrola nad obrazci, globalizacija z vzorci obrazcev in transportnih shem, virtualizacija upravljanja obrazcev z ostalimi tipi vsebin),

- avtomatizirano pridobivanje podatkov (univerzalen odjemalec – spletni brskalnik, mobilnik, kioski, dlančniki, interaktivnost obrazcev, eleganca, validacija vnesenih podatkov, vnos podatkov s strani uporabnikov in s tem zmanjšanje dela v administraciji, digitalni podpisi),

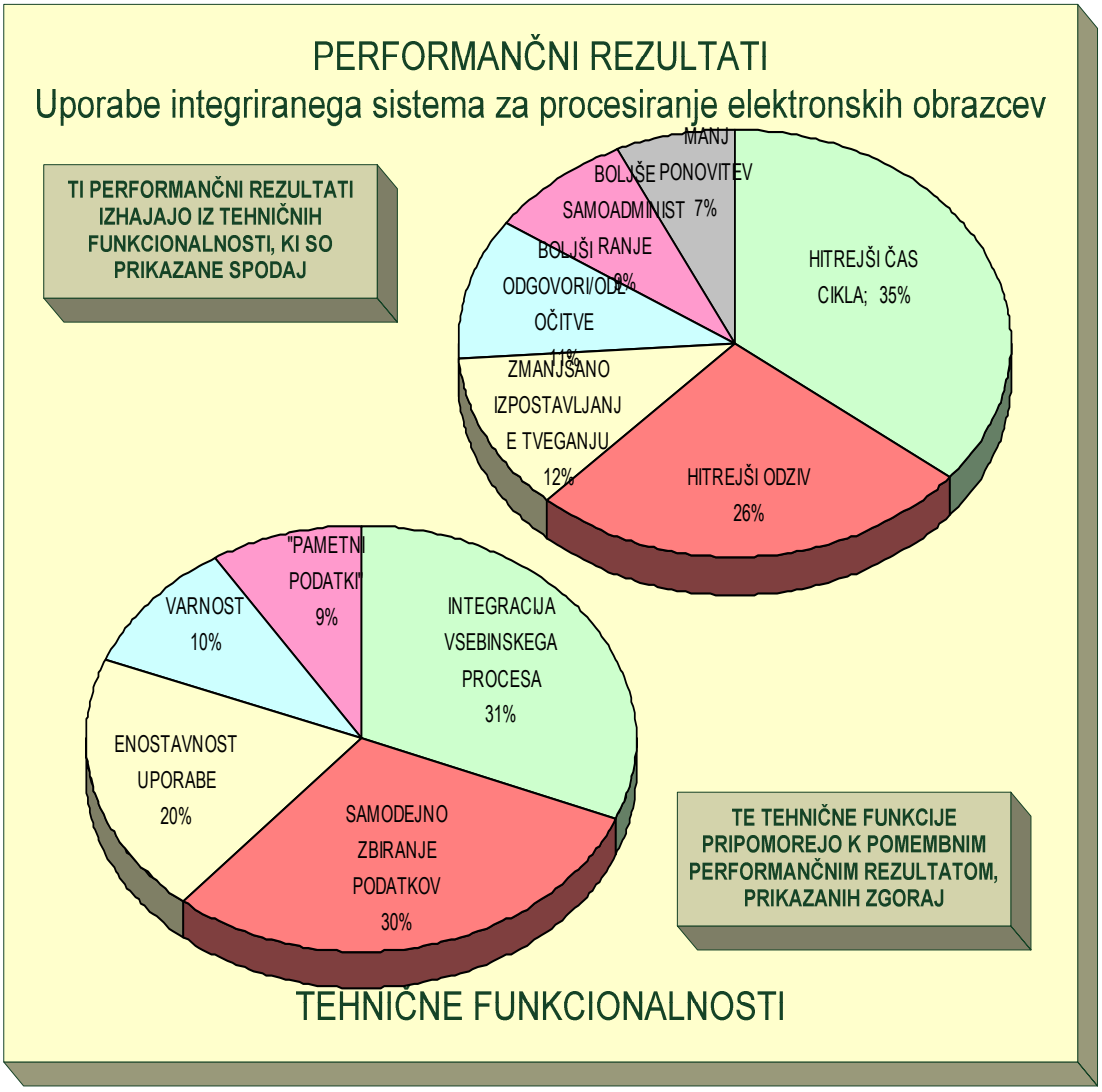
- enostavnost uporabe (povezava na največkrat zastavljena vprašanja, povečava podatkov in slik ter enostavnejše branje, konsistenca blagovne znamke in celostne grafične podobe, spletna pomoč),

- varnost (prednost glede na uporabnika, kontrola vpogleda/tiskanja, dinamična dovoljenja, varen in šifriran transport v zaledne sisteme podjetja, zaklenjen in nespremenljiv tekst, digitalno podpisovanje izpolnjenih obrazcev) in

- »pametni« podatki (vgrajeni metapodatki, transportni podatki za enostavni prenos, ovoj XML, standardni podatkovni modeli za razširjanje na vse vrste odjemalcev, časovni žig).

Rezultati in učinkovitost poslovanja so posledica zgoraj navedenih tehničnih funkcionalnosti in se kažejo na prenovljenih poslovnih procesih. Lahko jih povzamemo kot: hitrejši čas poslovnega cikla, večje sodelovanje, zmanjšano izpostavljanje tveganju, boljši odgovori in odločitve, večja samostojna administracija uporabnikov in zmanjšano ponovno opravljanje istega dela.

Slika 20 - Performančni rezultati tehničnih funkcionalnosti integriranega sistema za procesiranje elektronskih obrazcev



Vir: Moon, 2004, str. 14

Tako pripravljeni elektronski obrazci se lahko pošljejo uporabnikom, vendar če se želi zadostiti na eni strani pravno-formalnim in na drugi strani tehničnim zahtevam z oziroma na varnost, je treba pri izdelavi končne oblike, torej izpolnjenih obrazcev poskrbeti še za ustrezen digitalni podpis dokumentov. Ena izmed možnosti je uporaba digitalnega podpisovanja dokumentov, zapisanih v XML, ki je najbolj priporočljiva, saj omogoča podpisovanje tistega, kar podpisnik dejansko vidi, torej ima v skladu z zakonodajo pod kontrolo sredstvo podpisovanja. Drugi najbolj razširjen format za obrazce je PDF[41], vendar

[41] Obrazci v obliki standarda Portable Document Format, ki je izdelek podjetja Adobe (http://www.adobe.com) in je zelo razširjen na internetu, saj zelo verodostojno preslikava pisno verzijo teksta in slik. Uporablja model jezika postscript.

zaradi njegove zaprtosti in neznanega vpogleda v izvorni format (protokol je last podjetja) ni priporočljiv za izmenjavo dokumentov. Dokument za podpis namreč ne sme vsebovati kakršnih koli skritih podatkov, saj le-ti predstavljajo resno grožnjo, ker so lahko odvisni od nepodpisane vsebine, ki se jih po navadi podpisnik ali tisti, ki preverja, ne zavedata. Kako se je implementacije integriranega sistema za procesiranje elektronskih obrazcev lotil SiOL, je prikazano v 4. poglavju.

3.5.2 Elektronska predstavitev in plačevanje računov

Elektronska predstavitev in plačilo računov (EBPP, angl. Electronic Bill Presentment and Payment) omogoča podjetjem pošiljanje mesečnih računov svojim uporabnikom v elektronski obliki in procesiranje plačil teh računov prek interneta. Z aplikacijami EBPP se ne omogoča le plačevanje, saj je to sočasno tudi orodje za izvajanje odlične spletne naročniške podpore, za utrjevanje vezi med uporabniki in ponudnikom storitev, za izvajanje usmerjenih marketinških aktivnosti s poosebljenimi sporočili in akcijami ter nenazadnje tudi za obveščanje svojih uporabnikov o novostih in ostalih novicah oziroma spremembah, ki se jih tičejo.

Tradicionalna metoda dostave računov je tiskanje papirnatih računov in njihovo razpošiljanje z uporabo nacionalne poštne službe. Takšen proces zahteva čas, hkrati pa je predrago tako za podjetje kot za uporabnike. Elektronska metoda dostave je v zadnjem času vse bolj priljubljena, saj omogoča uporabnikom vpogled v svoje stanje še pred dejanskim pošiljanjem računa, pregled računa prek brskalnika, enostavno plačilo v vnaprej določenem časovnem roku in hkrati tudi enostavnejše zavračanje (ne)opravljenih storitev. Dostop do takšnih računov je lahko omogočen neposredno na straneh ponudnika storitev, lahko pa se tudi nahaja na straneh agregatorjev računov, ki so tipično veliki spletni portali in ponudniki internetnih storitev.

V svetu je bilo narejenih že precej poskusov uvedbe aplikacij EBPP, izkazalo pa se je, da je odstotek uporabljanja precej manjši, kot je bilo najprej pričakovano. Razlogov je več, največji med njimi je vsekakor nepravilna izbira tehnologije za pridobitev pozornosti uporabnika. Namesto metode »pull«, torej pričakovanje od uporabnika, da se registrira in obišče spletno stran, je boljša metoda »push«, s katero ponudnik storitev pošilja račune neposredno v naročnikov poštni predal, registracija pa tudi ni potrebna, saj so že vsi uporabniki registrirani v sistemu (uporabniško ime in geslo).

Vsekakor je treba poskrbeti za določeno raven varnosti, saj računi za opravljene storitve niso dostopni vsakomur, torej morajo biti ustrezno zaščiteni. Najboljši način je uporaba PKI in digitalnih potrdil, tako za strežnike, ki izdelujejo račune (podpis računa v obliki elektronske pošte s strežnikovim zasebnim ključem), kot tudi za uporabnike, ki so jim računi namenjeni (šifriranje računa z uporabnikovim javnim ključem). Če se uporabnik odloči, da bo potrdil

plačilo kar takoj, lahko to naredi s klikom na gumb plačaj, sočasno pa se njegova odločitev tudi podpiše z njegovim zasebnim ključem.

Prednosti uvedbe takšne aplikacije je več. Poleg zmanjšanja stroškov (le če se preseže kritična masa uporabnikov, ki plačujejo na takšen način) se lahko bolj učinkovito opozarja neplačnike, zmanjšajo se klici na podporo uporabnikom, izdatno pa se lahko podpre tudi dodatne marketinške akcije in prodajne aktivnosti. Ker je celotna aplikacija namenjena finančnim transakcijam, je nujno potrebna podpora infrastrukture PKI za zagotavljanje zasebnosti in avtentičnosti posredovanih podatkov.

3.5.3 Plačilne transakcije prek interneta: 3-D Secure

V svetu elektronskih plačil veliko vlogo zajema plačevanje najrazličnejših storitev in blaga prek svetovnega spleta. Največkrat uporabljen plačilni mehanizem je kreditna kartica, vendar že od samega začetka prihaja do najrazličnejših prevar, saj je to plačevanje brez prisotnosti kartice (angl. Card Not Present Transactions), poleg tega je internet idealno mesto za zakrivanje sledi. Zato se že nekaj let uporabljajo različni sistemi za zagotavljanje varnega zajema plačila prek interneta z neposrednimi povezavami do plačilnih procesorjev, ki poskrbijo za takojšnjo avtorizacijo plačila. Pri tem se plačilo izvede na podlagi posredovane številke kartice in njene veljavnosti (seveda poleg ostalih podatkov, ki opisujejo transakcijo – znesek, valuta, številka trgovca, številka terminala ipd.), v zadnjem času pa še z uporabo dodatnih varnostnih mehanizmov. Ti so kontrola naslova[42], CVN (angl. Card Verification Numbers), preverjanje vnesene številke in njene kontrolne kode (angl. Check Digit Algorithm), ročni pregled naročil (klicanje naročnika, stop liste, e-pismo naročniku, zgodovina naročil ipd.), interne kontrole, sistemi za nadzor nad goljufijami) ipd. Vendar se je izkazalo, da tudi to ni dovolj. Nujno je trena vnesti še overjanje plačnika. S tem se je najprej ukvarjal protokol SET (angl. Secure Electronic Transaction)[43] konec prejšnjega tisočletja, vendar je zaradi prevelike kompleksnosti, zahtevane uporabe digitalnih potrdil, velikih stroškov tako za trgovce kot tudi za uporabnike neslavno propadel. Njegov naslednik je 3-D Secure, ki ga podpirata obe največji svetovni omrežji plačevanja s kreditnimi karticami – Visa International in Mastercard.

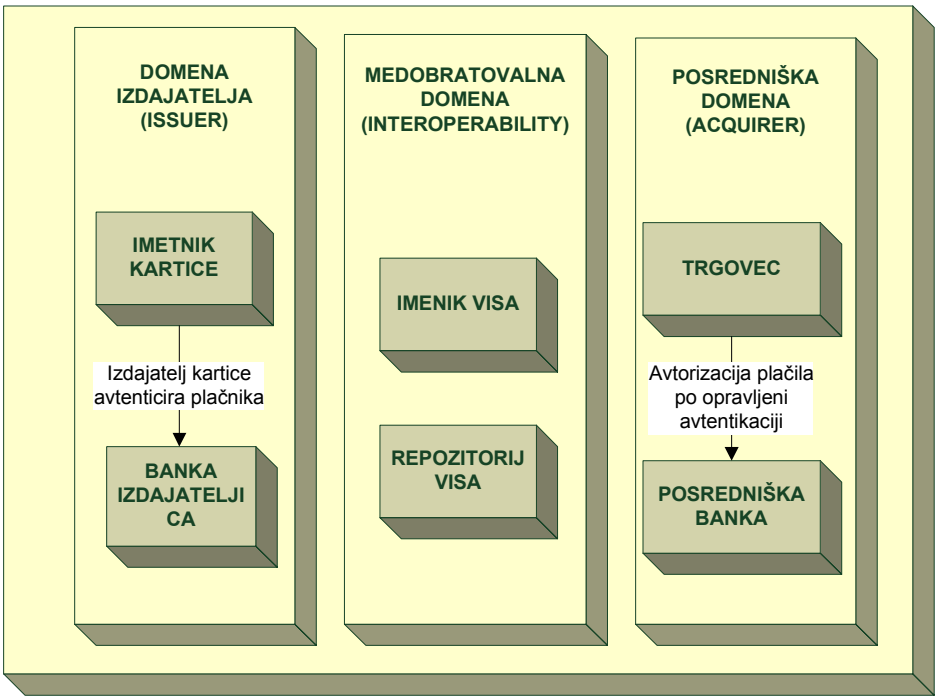
3-D Secure ni samo metoda za overjanje, je tudi zelo natančno definiran poslovni model, ki izolira odgovornosti različnih strank, vpletenih v celoten cikel plačilne transakcije. Osnovan je na predpostavki, da imajo banke izdajateljice (torej tiste, ki izdajajo kreditne kartice svojim komitentom) pogodben odnos s svojimi strankami, na drugi strani pa imajo

[42] Mehanizem je poznan pod kratico AVS – Adress Verification Check. Plačilni procesor sam odloči, kakšno stopnjo varnosti bo uporabljal – ali se preverja le ulica, ali mesto, poštna številka, hišna številka ipd. Uporablja se predvsem v ZDA.

[43] Več na naslovu http://www.setco.org.

posredniške banke pogodben odnos s trgovci, ki sprejemajo plačila s kreditnimi karticami v svojih trgovinah.

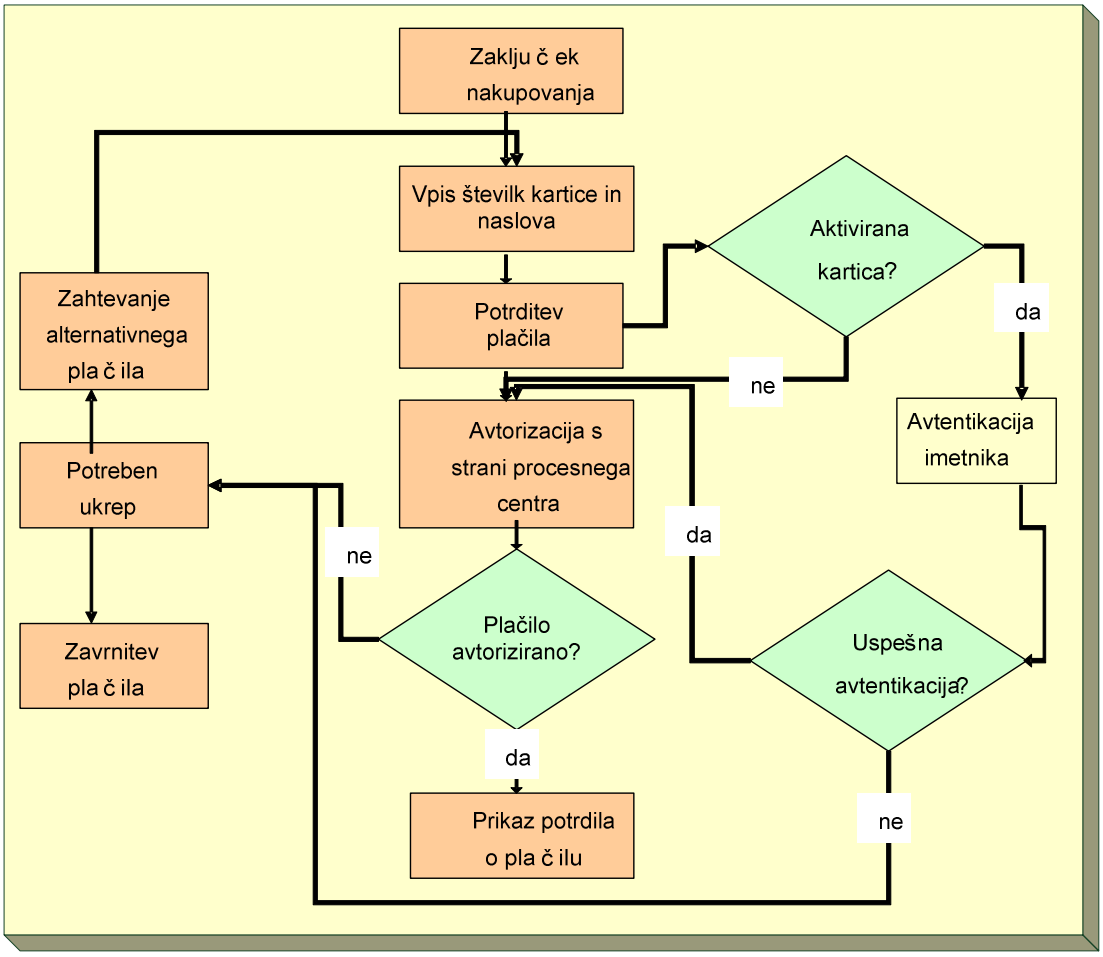
Slika 21 - Funkcionalna shema 3-D Secure



Poleg omenjenih domen (izdajateljska in posredniška) je definirana še tretja, imenovana medobratovalna domena, ki je namenjena povezovanju vseh vpletenih pri procesiranju transakcij, torej posredniške banke, trgovca, imetnika kartice, banke izdajateljice in kartičnih omrežij. Da se izvedejo plačilne transakcije v skladu s 3-D Secure, morajo biti vključeni trgovci prek posebnega modula, imenovanega MPI (angl. Merchant Plug-in), banke izdajateljice morajo omogočati overjanje plačnikov, sami imetniki kartice pa morajo pred prvim nakupom aktivirati svojo kartico za spletne nakupe. Na sliki je prikazan proces internetnega nakupa, ki upošteva model 3-D Secure.

Osnovna prednost 3-D Secure za trgovca je zmanjšanje goljufivih transakcij ter posledično reklamacij in z njimi povezanih stroškov. Predvideva se, da se bo s tem zmanjšalo število reklamiranih spletnih plačil za 80 %. Trgovci lahko poleg zmanjšanja reklamacij pričakujejo povečanje spletne prodaje, saj naj bi imetniki kartic zaradi prenosa odgovornosti imeli večje zaupanje v kartično plačevanje prek interneta in večjo preglednost nad plačevanjem. Imetnik lahko, ob ustrezni predhodni aktivaciji kartice, brezskrbno nakupuje po internetu, posredniška banka lahko zagotavlja storitev prodaje s kreditnimi karticami z manjšo stopnjo tveganja, banke izdajateljice pa si lahko povečujejo svojo prepoznavnost in uporabnost bančnih aplikacij, saj so vključene v vsak nakup.

Slika 22 - Tipičen spletni nakupovalni proces



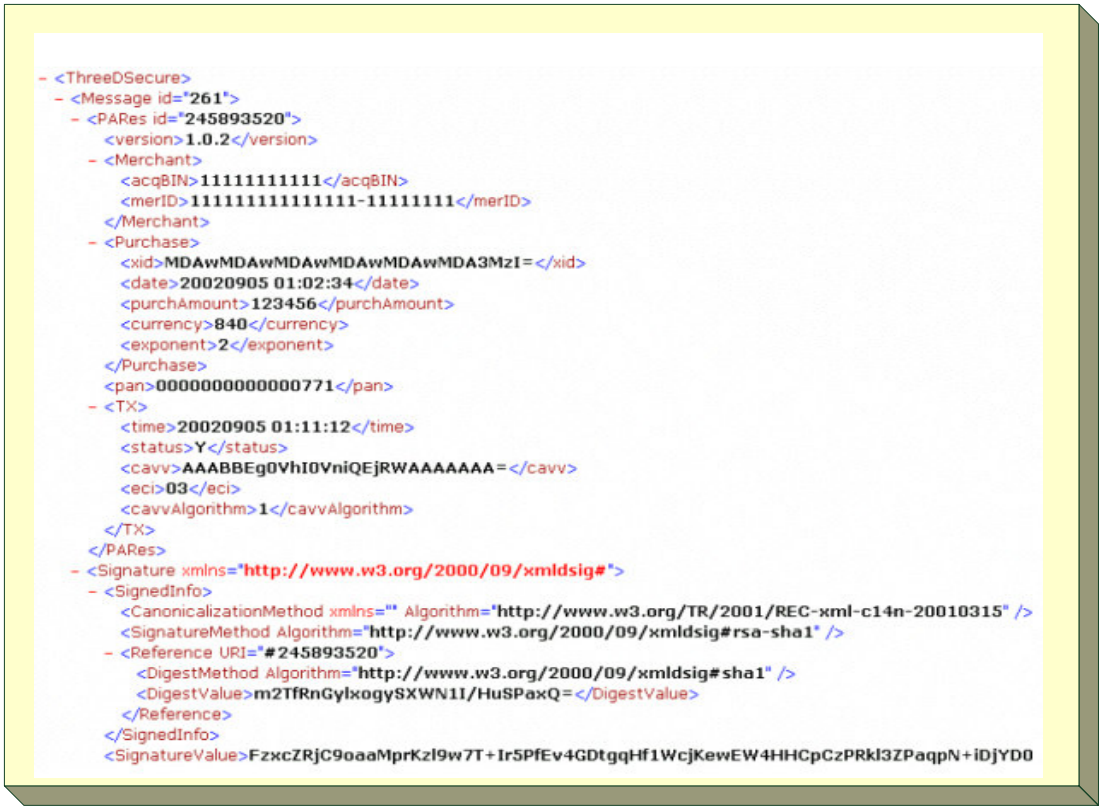
Ker je model namenjen natančnemu definiranju odgovornosti, je treba definirati še različne scenarije pri uporabi 3-D Secure v spletnih nakupih in brez njega. Reklamacija plačila nastopi takoj, ko imetnik kartice ali banka izdajateljica poda zahtevo za preverjanje plačila. Brez modela 3-D Secure mora trgovec takoj povrniti reklamirani znesek nakupa, ki ga pridobi nazaj po predložitvi dokaza o izvršenem plačilu. Z uporabo 3-D Secure se odgovornost razporedi v odvisnosti od tega, kdo od vpletenih omogoča izvedbo plačilne transakcije v skladu s specifikacijami modela. Odgovornost je prikazana na tabeli.

Sodelovanje trgovca?	Sodelovanje banke izdajateljice?	Ali je imetnik aktiviral kartico?	Za reklamacijo je odgovoren:
Ne	Da	Da	Trgovec
Da	Da	Da	Imetnik kartice
Da	Da	Ne	Imetnik kartice
Da	Ne	Ne	Banka izdajateljica
Ne	Ne	Ne	Brez sprememb, odgovornost ostane enaka kot sedaj

Tabela 1 - Odgovornost za reklamacijo

3-D mehanizem je sestavljen iz dveh osnovnih funkcij. Z **aktivacijo** se imetnik kreditne kartice prijavi v sistem 3-D Secure, seveda le ob predpostavki, da njegova banka izdajateljica to omogoča. Pri prijavi, ki se izvaja na registracijskem strežniku banke, se poleg preverjanja njegove identitete zapišejo še dodatni podatki, ki jih bo imetnik uporabljal pri spletnih nakupih. Izbor identifikacijske metode (uporabniško ime in geslo, digitalno potrdilo, enkratna gesla ipd.) je prepuščen banki ali imetniku, odvisno od izbranega poslovnega modela banke. Druga funkcija je **overjanje plačnika** pri spletnem nakupu. Za overjanje uporabnika prek varnega kanala komunicirajo vsi vpleteni v nakup – spletni trgovec, imetnik kartice, njegova banka izdajateljica, plačilni procesor in kartično omrežje. Uporabljajo se dokumenti, ki so varno podpisani z digitalnimi potrdili v skladu s priporočili W3C (XMLDSIG in XMLENC). Primer takšnega sporočila je prikazan na sliki.

Slika 23 - Primer podpisanega sporočila v 3-D Secure



3.5.4 ebXML

Skupna aktivnost združenja OASIS in Centra za elektronsko poslovanje v Združenih narodih (UN/CEFACT) je ebXML, katerega cilj je definiranje standardov za formiranje in prenašanje podatkov za elektronsko poslovanje, opis poslovnih procesov in pogajanje poslovnih zahtev in odgovornosti. Gradi na predpostavki, da se da z uporabo metajezika XML in internetnih protokolov bolj znižati stroške implementacije in operativnega delovanja kot če bi se

uporabil standard za enake namene, ki je že dolgo v uporabi, EDI (Electronic Data Interchange)[44].

EbXML uporablja SOAP kot format za sporočila in specifikacije W3C za podpisovanje in šifriranje dokumentov, zapisanih v XML, za zagotavljanje varnosti. Kot dodatno možnost se omogoča tudi uporaba varne elektronske pošte po standardu S/MIME (Nash, 2001, str. 119) in PGP MIME[45]. Za zagotavljanje varnosti se uporablja še SAML, ki prinaša orodje za avtorizacijske odločitve znotraj različnih delov celotnega sistema. Zanimivo je, da ebXML poleg natančnega definiranja elementov SOAP (za usmerjanje sporočil, izmenjavo informacij o poslovnih subjektih, definicijo ravni kakovosti storitev …) uporablja tudi imenik poslovnih partnerjev, vendar le-ta ne temelji na standardnem protokolu za spletne imenike UDDI, temveč na lastni specifikaciji. Poleg tega je zelo velik poudarek na načinih modeliranja poslovnih procesov, kjer se zahteva uporaba univerzalnega jezika za modeliranje, imenovanega UML. Vse skupaj podjetjem omogoča zelo globoko integracijo poslovnih procesov, a na koncu se morajo podjetja sama odločiti, kako globoko integracijo ebXML-ja bodo vpeljala v svoje poslovno okolje.

4 AVTOMATIZACIJA POSLOVANJA Z OBRAZCI V PODJETJU SIOL: VARNA IZMENJAVA E-SPOROČIL V POSLOVNIH OKOLJIH

Podpis in šifriranje dokumentov, zapisanih v XML, se uporablja na vedno več področjih, saj je metajezik XML postal de facto standard za formuliranje elektronskih sporočil na internetu, ki mu je manjkalo le še učinkovito zagotavljanje celovitosti in zaupnosti. Konzorcij W3C s specifikacijami za podpisovanje in šifriranje dokumentov, zapisanih v XML, rešuje natanko to. V nadaljevanju je predstavljena praktična uporaba varnosti v poslovnem okolju, s katerim je omogočena varna izmenjava elektronskih dokumentov podjetja SiOL, d. o. o., z naročniki in poslovnimi partnerji. V začetku, za samo vzpostavitev okvirne infrastrukture za kreiranje, predstavitev in izmenjavo elektronskih dokumentov, se je vzpostavil projekt, zasnovan na **avtomatizaciji poslovanja z obrazci**, a kot se je v praksi pokazalo pozneje, se je brez večjih težav lahko razširil tudi na druge poslovne procese podjetja.

Snovalec in odgovorni vodja projekta sem bil avtor tega magistrskega dela.

4.1 Vzpostavitev projekta (predprodukcija)

[44] Electronic Data Interchange (EDI) se uporablja za izmenjavo standardiziranih dokumentov med računalniškimi sistemi za poslovno uporabo v zaprtem okolju.

[45] Več o enkripciji PGP se nahaja na spletnem naslovu http://www.pgp.org.

4.1.1 Opisi postopkov pri varni izmenjavi e-dokumentov (funkcionalne zahteve projekta)

Servisne strani SiOL so dosegljive vsem naročnikom storitev SiOL. Pred zaključkom projekta so bile narejene v obliki »samo beri« oziroma so ponujale le osnovno dvosmerno komunikacijo (npr. vpis telefonske številke). Osnovni razlog, zakaj je bilo tako, je bila pravno-formalna zadostitev sklepanja in spreminjanja naročniških razmerij. V primeru uporabe PKI in digitalnih potrdil vsa komunikacija postane dvosmerna, saj lahko uporabnik vsako oddano naročilo digitalno podpiše, seveda ob predhodnem overjanju. Aplikacija še dodatno poglobi uporabo PKI, saj se vsa sporočila med obema stranema dodatno šifrira in s tem izdatneje poveča zasebnost in neokrnjenost vseh izmenjanih sporočil.

Z uporabo PKI se poveča stopnja varnosti iz osnovne na t. i. razširjeno (angl. Enhanced Security). Osnovna stopnja varnosti zajema celo vrsto pomanjkljivosti, zatorej je njena nadgradnja prvi pogoj za učinkovito elektronsko poslovanje vsakega podjetja. Pomanjkljivosti so v identifikaciji uporabnikov (uporablja se le varna povezava SSL, strežniško digitalno potrdilo predstavlja spletni strežnik, odjemalec pa se predstavi le z uporabniškim imenom in geslom, kar še ne pomeni, da to res je), zasebnosti podatkov (pošiljanje podatkov po elektronski pošti lahko prestreže vsak), nekontroliranim obnašanjem uporabnikov (uporabniki ne puščajo sledi za seboj), nadzorom zanikanja (ni formalnega dokaza o izvedbi transakcije), upravljanjem z varnostjo (ni centralne administracije identifikacije in dostopne kontrole) ipd.

Z razširjeno varnostjo se zagotovijo naslednje informacije:

- s kom spletna aplikacija komunicira (identifikacija),
- kdo je pooblaščen za dostop do kakšnih informacij,
- formalen zapisnik vseh operacij, narejenih v okviru spletne aplikacije, vključno z vsemi opravljenimi transakcijami in naknadno revizijo ter
- zasebnost – dostop do uporabniških podatkov, naročenih storitev, izdanih računov, uporabe storitev, arhiva ipd. imajo samo pooblaščene osebe.

Ostale prednosti razširitve varnosti na uporabniški strani z omogočanjem izpolnjevanja aneksov k pogodbam so naslednje:

- zmanjšanje stroškov s povečanjem avtomatizacije procesiranja novih in obstoječih naročil na internetne storitve, s poslovanjem v digitalni obliki (tiskanje in poštni stroški) in z arhiviranjem dokumentov v elektronski obliki,
- zmanjšanje napak, ki nastajajo ob pretipkavanju pisno izpolnjenih podatkov o naročenih storitvah v obstoječi zaledni sistem, in

- zmanjšanje časa procesiranja, saj se z odpravo počasne pošte in s samodejnim vklopom (izklopom) storitev prek elektronskega toka dogodkov zmanjša čas iz nekaj dni na nekaj minut.

Poslovni scenarij, iz katerega so izhajale funkcionalne zahteve projekta, se lahko opiše z natančnim definiranjem korakov elektronskega poslovanja med uporabniki (naročniki) in podjetjem SiOL.

1. korak

Uporabnik storitev SiOL pride na SiOL-ove spletne strani na naslovu http://www.siol.net, kjer se nahaja ogromno informacij v statični ali dinamični obliki. Prva stran (naslovnica) vsebuje osnovne informacije o storitvah SiOL-a in vsebinski del portala skupaj s povezavami na vse osnovne podportale (novice, avtomobilski del, nakupovalni del, oglaševanje, stiki, spletna pošta, uporabniške strani, servisne strani, registracija ipd.). Uporabnik, ki želi elektronsko poslovati s SiOL-om, ima na izbiro dve možnosti: ali **želi postati nov naročnik storitev SiOL-a** ali želi dostopiti do **podatkov o svojem naročniškem priključku**, jih pregledovati, spreminjati oziroma naročati (preklicevati) nove naročniške storitve. V slednjem primeru se nadaljuje proces na 3. koraku.

2. korak

V prvem primeru se naročniku po kliku na gumb »prijavi se« prikaže možnost izbire med različnimi dostopnimi storitvami SiOL-a. Nekatere zahtevajo posebne pogoje za sklenitev naročniškega razmerja, tako da je na voljo samo tradicionalen (papirni) način podpisovanja pogodbe, marsikdaj s potrebnim usklajevanjem z referentom v prodajno-administrativni službi. Večina storitev, namenjena masovnemu trgu, pa ima poslovni proces tako standardiziran, da se lahko podpisuje pogodba tudi v elektronski obliki. Potencialni naročnik lahko izbira med papirnim in elektronskim podpisovanjem pogodbe. Zanimiva je predvsem nova oblika, torej elektronska, tako da bo le-ta v nadaljevanju podrobno prikazana. Naročnik se mora najprej identificirati s pravno veljavno metodo, nato še vpisati vse podatke, na podlagi katerih se lahko preveri možnost izpolnitve storitve in pripravi osnutek elektronske pogodbe. Obvestilo o prejeti zahtevi se samodejno pošlje uporabniku po elektronski pošti.

3. korak

Referent v prodajno-administrativni službi dnevno pregleduje zahtevke za nove storitve. Najprej preveri možnost izpolnitve naročila, ki ga je vpisal naročnik in mu zatem odgovori. Če je storitev možna, je na vrsti postopek kreiranja novega naročnika oziroma dodajanje storitve k obstoječemu naročniku. Zaledna aplikacija pripravi vse potrebno za obveščanje

uporabnika o možnosti podpisa pogodbe. Ta korak je opcijski, saj nekatere storitve ne zahtevajo predhodnega preverjanja možnosti izpolnitve.

4. korak

Uporabnik vnese uporabniško ime in geslo za vstop v aplikacijo ter v primeru naprednega overjanja še digitalno potrdilo, aplikacija pa poskrbi za predstavitev njemu relevantnih podatkov (uporabniški podatki, arhiv, izdani računi, poraba ipd.). Spletna aplikacija za delovanje uporabniških strani pridobi podatke o uporabniku iz imenika (LDAP) in iz podatkovne baze. Če uporabnika v imeniku naročnikov še ni (nov naročnik), aplikacija pridobi podatke iz vmesne tabele potencialnih naročnikov.

5. korak

Če uporabnik želi naročiti kakšno novo ali spremeniti/preklicati obstoječe storitve, se informira o novih cenah, vnese dodatne (zahtevane) podatke in na koncu vrne popravljen osnutek dokumenta oziroma pogodbo na SiOL, kjer sistem pripravi končno obliko dokumenta. Aplikacija vrne uporabniku končni dokument skupaj s klicem posebnega programa za podpisovanje (ker ga obstoječi brskalniki in operacijski sistemi nimajo), ki ne sme dostopiti do nobenih drugih podatkov pri uporabniku, naloži in izvede pa se ob prvi uporabi oziroma ob spremembi verzije. Uporabniku se ponudi izbira digitalnega potrdila, ki jih ima na voljo in ustrezajo politiki SiOL-a, za podpis poslanega dokumenta.

6. korak

Uporabnik pošlje tako izpolnjen in elektronsko podpisan obrazec na SiOL-ov spletni strežnik v samodejno obdelavo takoj po podpisu.

7. korak

Referent v naročniški službi samo pregleda izpolnjene podatke v pogodbi in preveri njihovo pravilnost ter neokrnjenost, preveri izpolnjevanje v zalednem sistemu in, če je storitev pripravljena za uporabo, pošlje uporabniku digitalno podpisano in šifrirano obvestilo o odprtju zahtevane storitve in začetku njenega obračuna.

Predstavljeni primer je namenjen točno določeni storitvi. Mehanizmi, ki potekajo v ozadju, so splošni, kar pomeni, da je možno scenarij razširiti na različna področja obdelave podatkov o uporabnikih in drugih poslovnih procesih. Podobno se torej lahko izvede marsikatera dodatna interakcija z uporabniki, ki je doslej potekala papirno.

Cilj projekta je bil usmerjen v podpisovanje dinamično zgrajenih dokumentov v formatu XML z uporabo spletnega odjemalca, varne izmenjave v poslovnem okolju in avtomatske obdelave v zalednih sistemih. Obstoječi spletni odjemalci že omogočajo upravljanje z uporabniškimi certifikati in izvajanje določenih varnostnih funkcij, kot je overjanje uporabnika, vzpostavitev varnega kanala SSL ipd. S stališča dokumentov spletni odjemalci omogočajo le prikaz strani oziroma interpretacijo dokumentov v formatu HTML ali XHTML. Da bi omogočili tudi podpisovanje dokumentov različnih formatov, je treba pri uporabniku zagotoviti izvajanje kriptografskih funkcij oziroma namestiti primernega odjemalca za izvajanje kriptoalgoritmov za podpisovanje in šifriranje. Rešitve za to že obstajajo, vendar niso del operacijskih sistemov in zahtevajo namestitev dodatnega odjemalca. Ker se je predvidevalo, da bodo aplikacije za podpisovanje in šifriranje dokumentov še nekaj časa omejene na manjšo skupino uporabnikov, je bilo treba ponuditi alternativo, ki sicer rešuje le specifične probleme. Aplikacija za podpisovanje dokumentov znotraj oziroma kot del spletnega odjemalca je namenjena zgolj določenim, a še vedno praktično zelo razširjenim scenarijem. Osnovni koncept je zasnovan na razmerju odjemalec–strežnik, kjer se na strežniku sproti izdelujejo dokumenti glede na uporabniški ali strežniški vnos. Ko je takšen dokument (npr. pogodba) ustvarjena, jo lahko uporabnik podpiše s pomočjo funkcij spletnega odjemalca in operacijskega sistema ter shrani lokalno za potrebe lastnega arhiva. Podpisano pogodbo v elektronski obliki prejme strežnik in jo varno shrani oziroma posreduje poslovnemu informacijskemu sistemu.

Naslednji štirje koraki opisujejo osnovni koncept izvajanja scenarija, ki je že upoštevan v predhodno prikazanem poslovnem scenariju oziroma natančneje določa potek njegovega 5. koraka:

1. korak

Uporabnik se registrira v sistem (način prijavljanja je nepomemben za delovanje sistema, vendar je priporočljiva uporaba digitalnih potrdil za overjanje uporabnikov, ki potrdila v vsakem primeru potrebujejo za podpisovanje). Sledi izbira želene storitve (urejanje naročniškega razmerja[46]). Urejanje razmerji med ponudnikom in odjemalcem temelji na pogodbah, ki so pravno-formalna osnova za vzpostavitev ali spreminjanje naročniških razmerij. Pogodbe za urejanje naročniških razmerij so vnaprej pripravljene po vzorcih, kar pomeni, da je treba le vnesti podatke v določena polja. Te podatke prestreže strežnik na osnovi spletnih form, ki jih izpolni uporabnik, in protokola HTTP. Ko so podatki zajeti, to pomeni, da jih uporabnik vnese, strežnik generira pogodbo, ki ureja novo ali spreminja obstoječe naročniško razmerje.

2. korak

[46] Izhajamo iz osnovnega scenarija, tj. urejanje naročniških razmerij, čeravno je scenarij vedno enak, kadar je treba dinamično zgraditi dokument in pridobiti podpis uporabnika.

Na novo ustvarjeno pogodbo strežnik sočasno podpiše z zasebnim ključem, s čimer zagotovimo neokrnjenost pogodbe na poti do uporabnika in njeno verodostojnost. Pogodbo prek varnega kanala pošlje uporabniku.

3. korak

Pogodba je varno dostavljena uporabniku in predložena na vpogled. Hkrati uporabniški odjemalec preveri veljavnost strežniškega podpisa. Nato pogodbo podpiše s svojim zasebnim ključem, s čimer potrdi zahtevo po novem ali spremenjenem naročniškem razmerju. Podpisano pogodbo pošlje strežniku.

4. korak

Strežnik prestreže podpisano pogodbo, preveri uporabniški podpis in jo varno shrani oziroma posreduje informacijskemu sistemu. Kot potrdilo o prejemu pogodbe, strežnik pogodbo ponovno podpiše[47] in vrne uporabniku. Uporabnik shrani kopijo prejete pogodbe.

S četrtim korakom je celoten proces končan. V zadnji fazi ima strežnik podpisano pogodbo s strani uporabnika, uporabnik pa potrditev oziroma *ožigosano kopijo* podpisane pogodbe.

4.1.2 Definiranje varnostnih in nefunkcionalnih zahtev

Funkcionalne zahteve projekta so se nanašale na delovanje aplikacij, ki so vključene v procese varne izmenjave dokumentov preko interneta in so bile opisane v prejšnjem poglavju. Infrastruktura se deli na dve osnovni strežniški skupini, ki delujeta okoli Servisnega in Varnostnega strežnika[48], obe pa delujeta v javanskem okolju in arhitekturi J2EE. Širšo sliko celotne infrastrukture sestavljajo še zaledni sistemi in uporabniško okolje naročnikov oziroma uporabnikov. Poleg aplikacij, ki zadovoljujejo funkcionalne zahteve, je bilo treba poskrbeti tudi za varnostne in nefunkcionalne zahteve projekta.

Varnostne zahteve Servisnega strežnika, katerega osnovna odgovornost je zagotavljanje informacij o uporabnikih, kdo so, kakšne naloge lahko izvajajo, kako bodo overjeni ipd., ter povezovanje na eni strani z Varnostnim strežnikom in na drugi strani z zalednimi sistemi, so:

- **Omejevanje dostopa uporabnikov**. Servisni strežnik mora biti postavljen v demilitariziran sloj (DMZ), tako da osnovno filtriranje zahtevkov opravlja že požarni zid skupaj s sistemom za odkrivanje vsiljivcev. Neavtoriziranim uporabnikom je omogočen dostop do osnovnih podatkov o sistemu, ostalo pa je namenjeno le tistim, ki se uspešno overijo v sistem. Takoj se deli naslednja stopnja uporabnikov na tiste,

[47] Tukaj gre predvsem za potrditev prejema. Podobno je pri pogodbah v pisni obliki, kjer je prejem potrjen z žigom oziroma kopijo pogodbe.

[48] Strežnika sta v resnici poimenovana drugače, njihova dejanska imena pa naj zaradi varnostnih razlogov ostanejo skrivnost. Ker sta to resnična strežnika, sta zapisana z veliko začetnico.

ki uporabljajo digitalna potrdila, in na tiste, ki uporabljajo le osnovni način overjanja, to je uporabniško ime in geslo.

- **Dodeljevanje pravic naročnikom**. Overjanje uporabnikov se lahko izvede na več načinov, na drugi strani pa imajo naročniki različne pravice. Sistem mora na osnovi overitve uporabnika zagotoviti različne stopnje pravic in s tem dostopa do več ali manj informacij.

- **Varna izmenjava sporočil** z Varnostnim strežnikom in zalednimi sistemi. Ker je cilj zagotovitev varnosti od začetka do konca poti sporočil ob predpostavki, da se overjanje oddajnika sporočila ne izvaja na vsakem strežniku, je nujno, da se zagotovi način prenašanja teh sporočil in varnostnih informacij.

- **Samostojna administracija naročnikov.** Administrativne naloge so veliko breme za podjetja, tako da je nujno, da se prenesejo na naročnike same, vendar se mora upoštevati dejstvo, da nepazljivo sestavljena aplikacija lahko povzroči hude probleme.

- **Varovanje podatkov posameznih naročnikov.** Pomembno je, da overjeni naročnik ne vidi podatkov drugih, razen v primeru ustreznih pooblastil.

Tudi **Varnostni strežnik ima svoje varnostne zahteve**, ki so še bolj strogo določene kot zgoraj naštete, vsekakor pa so tudi v veliki meri komplementarne z njimi:

- **Varna izmenjava sporočil**. Varnostni strežnik je namenjen izdelavi varnih sporočil v obliki digitalno podpisanih dokumentov XML in pošiljanju teh sporočil na predhodno dogovorjene naslove tako v formatu SOAP prek HTTPS ali v obliki podpisane elektronske pošte. Ker pridobiva zahtevke prek spletnih storitev, mora iz njih poleg osnovnih funkcionalnih podatkov znati razbrati tudi dodatno zapisane varnostne parametre in jih preslikati v skladu s predhodno dogovorjeno shemo s pošiljateljem.

- **Omejevanje dostopa uporabnikom**. Varnostni strežnik komunicira le s strežniki iz notranjega omrežja SiOL, poleg tega pa sprejema zahtevke le za predhodno overjene uporabnike. Če Servisni strežnik pošlje zahtevek, ki ga je predhodno naredil gost, mora Varnostni strežnik takšno zahtevo takoj zavrniti.

- **Administratorjeve (ne)zmožnosti**. V določenih kritičnih funkcijah, kot je ponovno pošiljanje dokumenta v elektronsko podpisovanje v primeru napak, je potrebno administratorjevo posredovanje, v nekaterih primerih pa to posredovanje nikakor ne sme biti dovoljeno, npr. podpisovanje dokumentov v naročnikovem imenu.

- **Transformacija dokumentov** v druge oblike na osnovi transformacijskih shem. V poslovnem okolju se velikokrat zahteva, da se podatki preslikujejo iz ene oblike v drugo, tako da se zagotovi ustrezna komunikacija med sistemi.

Ključne zahteve **odjemalca na strani uporabnika** so:

- **Enostavna namestitev in preprosta uporaba.** Enostavna namestitev zahteva hitro in uporabniku prijazno nadgradnjo spletnega odjemalca s funkcijami za šifriranje in podpisovanje elektronskih dokumentov. To omogoča uporaba primerne tehnologije, na osnovi katere je zagotovljena enkratna namestitev razširitve spletnega odjemalca z dodatnimi funkcijami in kontrolami. Komponenta na strani odjemalca temelji na osnovi tehnologije ActiveX, ki zagotavlja preprosto in hitro namestitev ter popolno integracijo v okolje Windows.

- **Podpora najpogosteje uporabljenih spletnih odjemalcev** (vsaj 95 %). Zaradi različnosti operacijskih sistemov in spletnih odjemalcev je skoraj nemogoče zadostiti potrebam po prenosu tehnologije med različnimi sistemi in preprosti uporabi. Ker je najpogosteje uporabljeni operacijski sistem ena izmed različic Windows podjetja Microsoft, je sistem odjemalec–strežnik zasnovan na spletnem odjemalcu Internet Explorer (del operacijskega sistema Windows).

- **Hitra odzivnost, hitro delovanje.**

- **Visoka stopnja zaščite**. To pomeni zaščito razširitvene kode (ActiveX), ki jo uporabnik namesti v svojem okolju, zaščito prenosa kode, varno namestitev kode, varno izmenjavo podatkov, varno izmenjavo dokumentov, preverjanje veljavnosti dokumentov, varno hranjenje dokumentov, varno podpisovanje in zanesljivo overjanje digitalno podpisanih dokumentov.

Ključna zahteva poleg varne izmenjave podatkov je pravilnost podpisovanja dokumentov. Tako uporabniku kot strežniku je treba zagotoviti verodostojnost oziroma pravilno interpretacijo vsebine pogodbe. Koncept »kar si videl, si podpisal« (angl. What You See Is What You Sign – WYSIWS) zagotavlja enolično interpretacijo vsebine elektronske pogodbe. Vsaj dva formata zagotavljata delovanje v konceptu WYSIWS: slikovni zapis GIF ali JPEG oziroma zapis XML[49]. Ko uporabnik podpiše pogodbo v enemu izmed formatov, je sočasno zagotovljena enakost vsebine pogodbe z vsebino, prikazano v prikazovalniku (odjemalcu).

Poleg funkcionalnih in varnostnih je treba upoštevati še **nefunkcionalne zahteve**, ki so nujne za uspešno delovanje sistema sedaj in v bližnji oziroma daljni prihodnosti. To so zmožnost upravljanja (nadzor, ponovni zagon ob napaki, nameščanje programskih nadgradenj, administracija in revizija), razširljivost (podpora različnih varnostnih politik in procedur ob poslovnih spremembah, prihajajoči novi varnostni standardi …), zanesljivost (ki se meri v povprečnem času med napakami in povprečnem času za odpravo napak), razpoložljivost (odprava vseh možnosti napak in povečanje zanesljivosti z vpeljavo podvojene programske in strojne opreme, replikacije, arhiviranja, uravnoteževanja

[49] V formatu XML lahko določimo, katera polja so dovoljena in katera prepovedana.

obremenitve ipd.) in razširljivost (ker se od vsake storitve pričakuje rast, je treba takoj razmišljati o nadgradnjah sistema zaradi povečanja zahtev).

4.1.3 Analiza stanja obstoječih informacijskih sistemov in pravnih ter formalnih podlag

Podjetje SiOL se je srečevalo s podobnimi težavami, kot so opisani v poglavju 3.5.1, ki so posledica izvajanja poslovnih procesov z obrazci v papirni obliki. Trenutno se operira z več kot 50 različnimi obrazci (poleg standardnih obrazcev še naročniške pogodbe, aneksi k pogodbam, zahteve za spremembe naročniških paketov, pooblastila, preklici in prekinitve razmerij ...). Njihovi uporabniki so skoraj vsi zgoraj našteti, saj nudenje internetnih storitev ni namenjeno točno določenim ciljnim skupinam, temveč vsem, ki jih potrebujejo. Ker je takšno poslovanje postajalo vse bolj pereč problem, se je vodstvo SiOL-a začelo ozirati po rešitvah, ki bi zmanjšale stroške ob povečanju kakovosti in hitrosti izvajanja poslovnih procesov. Obrazci v elektronski obliki so bili rešitev, ki bi ustrezala tem pogojem.

Informacijski sistemi v omrežju SiOL temeljijo na javanski tehnologiji in predvsem okolju J2EE, tako da je bila navkljub vse večjemu prepletanju tehnologij in odprtih standardov, ki omogočajo medsebojno delovanje različnih pristopov k enakim tehnologijam, najbolj smiselna izvedba projekta na tej tehnologiji in predvsem odprtih standardih, s čimer so ostala odprta vrata za nadaljnje nadgradnje sistema.

Formalne podlage so natančno specificirane in opisane v poglavju 2.3. Najbolj smiselna je bila uporaba digitalnih potrdil in infrastrukture javnih ključev ob upoštevanju vseh veljavnih zakonov, ki urejajo to področje v slovenskem prostoru in širše.

4.1.4 Načrtovanje aktivnosti

Projektna specifikacija je najpomembnejši dokument v fazi pred in med izgradnjo sistema. Navkljub temu da jo lahko sestavi večja skupina ljudi, je projektni vodja tisti, ki mora prevzeti vso odgovornost za njegovo izgradnjo. Izvajajo se natančno specificirane naloge, s strani točno določenih izvajalcev s točno določenim časovnim okvirjem. Če je specifikacija dobro narejena, je vodenje projekta precej enostavnejše, prav tako pa se izdatno poveča skupinska morala in pripadnost delu. Vsak natančno vidi, kaj mora narediti in zakaj je tako pomembno, da opravi svoje delo v določenem času, saj je zelo jasno predstavljeno, da je del cele skupina.

Osnovna aktivnost pred izgradnjo sistema je bila dana projektnemu vodji, ki je moral skupaj z ostalimi v določeni projektni skupini narediti specifikacijo projekta. Vsebina dokumenta je določala potrebno delo, predvidene stroške projekta in pogodbe z izvajalci, poglavja pa so, kot je opisano v (Friedlein, 2001, 102), naslednja:

- kontrola verzije,

- distribucijski seznam,
- vsebina,
- uvod,
- cilji projekta,
- kriteriji uspešnosti,
- funkcionalna specifikacija,
- tehnična specifikacija,
- vsebinski načrt,
- marketinške pobude,
- načrt testiranja,
- nadgradnje in vzdrževanje,
- kritični dejavniki,
- proračun projekta in
- priloge.

Najpomembnejši dokument, ki je nastal v predprodukciji, je bila Projektna dokumentacija, ki je last podjetja SiOL, d. o. o., in je zaupne narave. Vsa nadaljnja dela so se izvajala izključno po predpisanem vsebinskem načrtu in v dogovorjenih rokih.

4.1.5 Analiza kriterijev uspeha, kritičnih dejavnikov in tveganosti projekta

Pri izdelavi projektne specifikacije je treba upoštevati na eni strani kriterije uspeha, s katerimi merimo zastavljene cilje, in na drugi strani nepredvidene situacije, ki lahko zavrejo projektno izvedbo ali, v najslabšem primeru, celo onemogočijo njegov zaključek in predvidene cilje.

Pomembna je čim bolj natančna definicija **kriterijev uspeha projekta**, s katerimi se lahko med izvedbo meri uspešnost. Seveda je nujna zmernost pri vzpostavljanju meril, saj poznejše doseganje kriterijev oziroma njihovo preseganje zelo dobro vpliva na projektno skupino in poveča možnosti za uspešen konec projekta. Nekatere kriterije uspeha se ponekod veže tudi v pogodbena določila z izvajalci in se s tem zagotovi maksimalna privrženost izvajalcev k dobremu zaključku. V primeru spletnih projektov, ki so precej nov način poslovanja, je kriterije uspeha težje določiti, razvrstimo pa jih lahko v dve skupini:

- neposredni kriteriji uspeha: število izmenjanih e-dokumentov, novi naročniki, tržni delež, število posledičnih akcij (npr. plačila elektronskega računa), delovanje storitve (čas neprekinjenega delovanja strežnikov, čas neprekinjenega delovanja storitve), ogledi spletnih strani, zmanjšanje stroškov (tiskanje, razpošiljanje, telekomunikacijski stroški …);

- posredne koristi: izboljšana povezava z naročniki, povečanje znanja in izkušenj v podjetju za delo z elektronskimi dokumenti, gradnja povezav z drugimi podjetji v elektronski obliki, 7dni/24-urna prisotnost, navzočnost v medijih, konkurenčna prednost, zadržanje talentiranega osebja, povečana morala zaposlenih …

Poleg natančne definicije kriterijev uspeha je nujna tudi analiza kritičnih dejavnikov in skupnega tveganja projekta. Pri analizi kritičnih dejavnikov in odpravljanju njihovega negativnega učinka je priporočljivo upoštevati štiri korake (Stutely, 2002, str. 223). To so razmišljanje (identifikacija tveganj), ocenjevanje škode, ki jo lahko povzročijo, načrtovanje s pozicioniranjem (njihovo vključevanje v strategijo) in nadziranje (obdržanje neprestanega nadziranja za pričakovane in nepričakovane ovire ter takojšnje reagiranje). Bolj natančno kot se identificira kritične dejavnike, boljše je celotno načrtovanje projekta. V fazi predprodukcije je tako možno identificirati kritične dejavnike in izdelati alternativne možnosti ravnanja, če kateri od njih tudi postane resničnost. Nekateri kritični dejavniki, ki so bili identificirani pred projektom in ki jim je dodana tudi možna rešitev, so bili:

- **Pomanjkanje ali prezasedenost predvidenih strokovnjakov** in programerjev. Tveganje se je zmanjšalo z vnaprejšnjim pregledom možnih zamenjav pri zunanjih izvajalcih.

- Premajhna **prodaja** lahko povzroči vzpostavitev novih, nujno potrebnih projektov in akcij za povečanje prodaje, medtem ko prevelika prodaja povzroči več dela na obstoječih poslovnih procesih. Tveganje se zmanjša s preusmeritvijo dela tudi na druge zunanje izvajalce, ki morajo biti v pripravljenosti.

- **Problemi v informatiki**. Poleg razvoja in drugega dela na projektu je treba neprestano nadzorovati vsakodnevna informacijska dela, ki jih morajo izvajati drugi strokovnjaki, ki niso del projektne ekipe in so zato neobremenjeni s projektnimi roki.

- **Težave pri koordinaciji** dela strokovnjakov, ki prihajajo z različnih področij SiOL-a in zunanjih izvajalcev. Tveganje se zmanjša z organiziranjem rednih koordinacijskih sestankov, rednim spremljanjem opravljenega dela, obveščanjem opravljenega dela med ekipami in z uporabo skupne spletne aplikacije za upravljanje s projektom.

- **Spreminjanje zakonodaje** in tehničnih standardov na področju elektronskega poslovanja. Rešitev je v neprestanem spremljanju razvoja zakonodaje in tehničnih priporočil in manjše prilagajanje novim dognanjem na tem področju.

- **Naravne katastrofe**, kot so potresi, poplave, požari ipd. S pripravo načrta za okrevanje po nesrečah se lahko pripravijo procesi ob naravni katastrofi.

Tveganje projekta se je presodilo na podlagi zgoraj naštetih kritičnih dejavnikov in z upoštevanjem priprave ob njihovem morebitnem nastopu. Največja verjetnost nastopa kritičnega dejavnika je bila dana sami spremembi zakonodaje in z njo povezanim nepričakovanim potrebnim spremembam projekta.

4.2 Izgradnja sistema (produkcija)

4.2.1 Funkcionalna izvedba

Celotna infrastruktura za varno komuniciranje na osnovi podpisa XML temelji na sodobnih tehnologijah ob maksimalni izrabi splošno dostopnih orodij na strani uporabnika, medtem ko so bile ostale funkcionalnosti, ki jih obstoječa orodja ne podpirajo, razvite v okviru projekta. Na splošno se deli na štiri celovite domene – uporabniško okolje, Servisni strežnik, Varnostni strežnik in zaledne aplikacije (obračunsko aplikacijo, finančno-računovodsko aplikacijo, podatkovni strežnik ipd.). Ker so to samostojno delujoči sistemi, je treba opisati funkcionalnosti za vsako domeno posebej. Celotna infrastruktura je bila v fazi definiranja projekta poimenovana **SiOL WebSign**, kar je bilo pozneje uporabljeno tudi v produkcijski fazi. V nadaljevanju se bo to poimenovanje uporabljalo za opis celotnega sistema, kar pomeni tako strežniškega dela kot tudi samega odjemalca.

Funkcionalnosti odjemalca, ki omogočajo varno komunikacijo uporabnika oziroma naročnika s SiOL-om, so naslednje[50]:

- vzpostavitev varnega kanala za izmenjavo podatkov,
- prejem dokumenta,
- preverjanje veljavnosti dokumenta,
- preverjanje podpisa dokumenta,
- podpis dokumenta,
- hranjenje dokumenta in
- pošiljanje dokumenta.

Uporabniki ob prvem obisku na spletni strani sprožijo namestitev komponente na operacijski sistem. Pred namestitvijo se pojavi okno, kjer je prikazana identiteta avtorja komponente, ki

[50] Vnos v obrazce, prikaz strani in ostalo so funkcije, ki jih izvaja že osnovna različica spletnega odjemalca

se bo namestila v sistem. Uporabnik lahko zaupa prikazani informaciji na osnovi digitalno podpisane programske kode. Z ročno potrditvijo sproži dejansko namestitev komponente.

Slika 24 - Opozorilni napis pred prvo namestitvijo odjemalca

Vir: SiOL, d.o.o., 2004

Ob naslednjem obisku spletne strani sistem zazna, ali ima uporabnik zahtevano komponento že nameščeno in mu je zato ne namešča ponovno. Velikost komponente ni večja od 700 K, tako da je tudi pri uporabniku z modemsko povezavo namestitev končana v manj kot treh minutah.

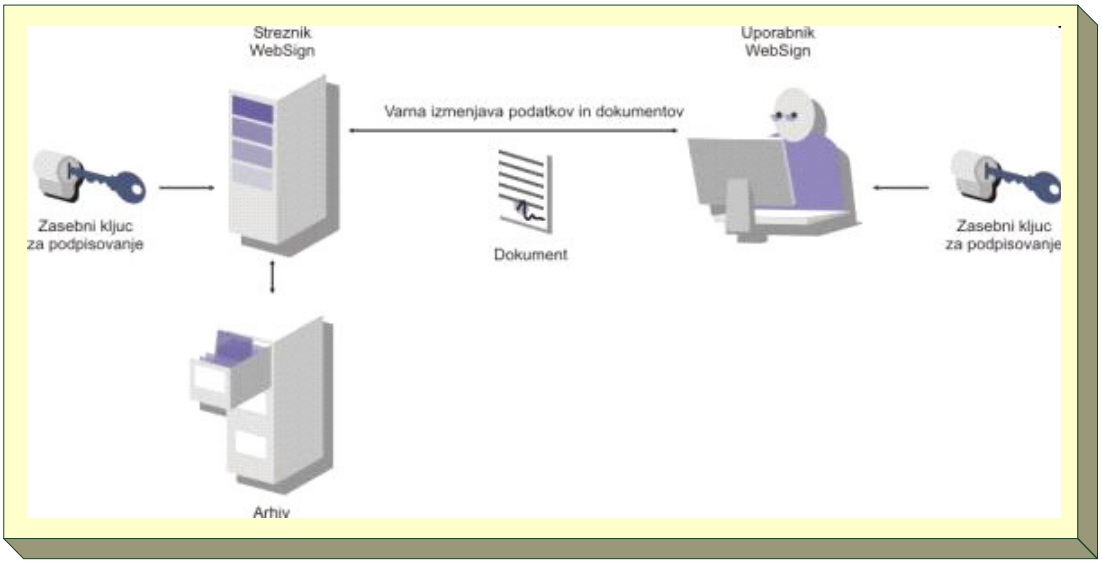
Varnost je zagotovljena s tem, da je šifrirana vsa komunikacija med ponudnikom storitev in uporabnikom, avtentičnost podatkov pa z uporabo digitalnega podpisa. S temi postopki lahko zagotovimo visoko stopnjo varnosti, a le ob predpostavki, da uporabnik lahko zaupa svojemu računalniku (torej, da v svojem računalniku nima nameščenega trojanskega konja).

Funkcionalnosti specifične za Varnostni strežnik so naslednje[51]:

- vzpostavitev varnega okolja za izmenjavo podatkov,
- varna izmenjava dokumentov s Servisnim strežnikom in zalednimi aplikacijami,
- podpis dokumenta,
- pošiljanje dokumenta,
- prejem dokumenta,
- preverjanje podpisa dokumenta in
- varno hranjenje dokumenta oziroma posredovanje informacijskemu sistemu.

[51] Zajem podatkov za generiranje pogodbe se izvaja prek standardiziranih obrazcev.

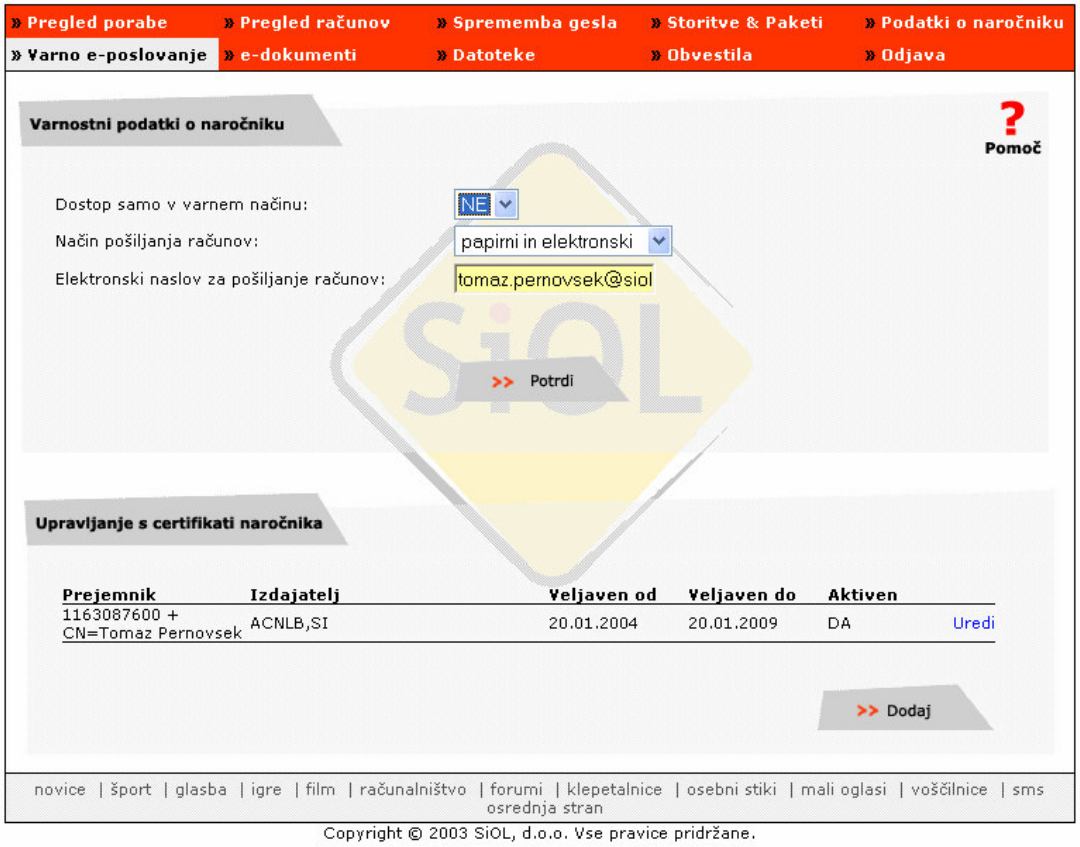
Slika 25 – Varna izmenjava podatkov in dokumentov



Že obstoječa aplikacija Servisnega strežnika je nadgrajena z naslednjimi funkcionalnostmi, ki so odgovor na funkcionalne, varnostne in nefunkcionalne zahteve iz prejšnjega poglavja:

- vzpostavitev varnega okolja za izmenjavo podatkov,
- izdelava dokumenta na osnovi pridobljenih podatkov s strani uporabnika in zalednih sistemov,
- registracija digitalnih potrdil uporabnikov in ostalih podatkov za elektronsko poslovanje, kot so želeni elektronski naslov za komunikacijo s SiOL-om, način prejemanja elektronskih računov itn.,
- dva načina overjanja uporabnika – osnovno z uporabniškim imenom in geslom in napredno, ki dodatno zahteva še ustrezno digitalno potrdilo,
- pošiljanje dokumentov z ustreznimi varnostnimi podatki in pravicami na Varnostni strežnik,
- prejemanje podpisanih dokumentov s strani Varnostnega strežnika in hranjenje v zaledne sisteme,
- omejevanje dostopa uporabnikom in dodajanje/odvzemanje pravic,
- samostojna administracija naročnikov na osnovi dvonivojskega uporabniškega načina (temeljni priključki in ostali) in
- varovanje podatkov naročnikov.

Slika 26 - Registracija kvalificiranega potrdila na servisnih straneh

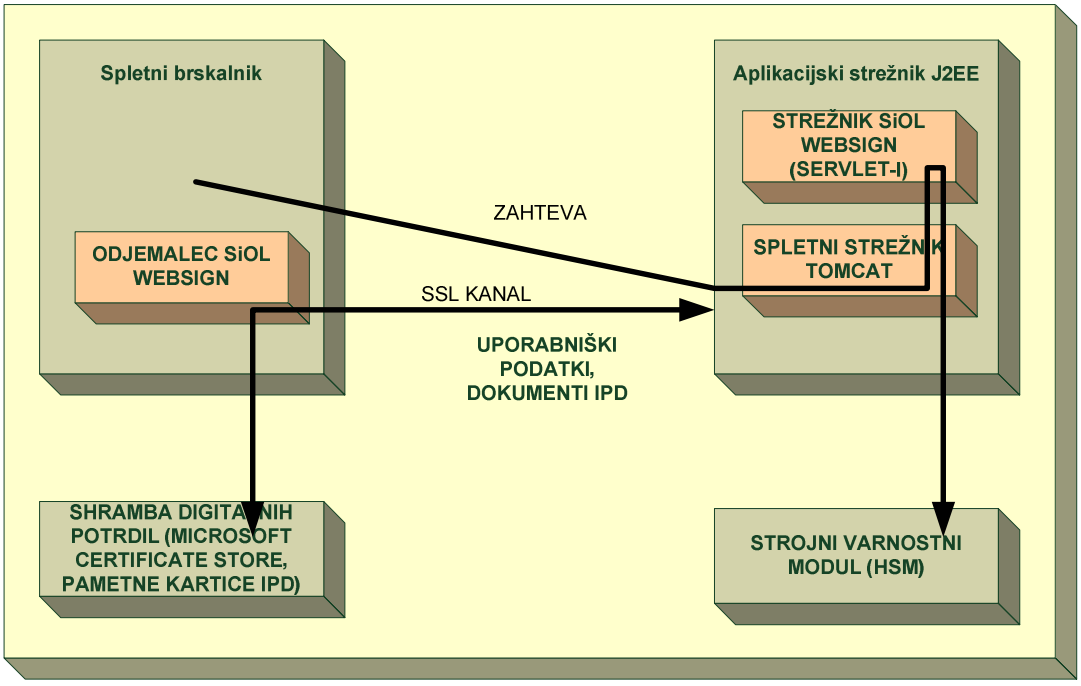


Slika 27 - Varnostne nastavitve za registrirano digitalno potrdilo

Zaledne aplikacije so nadgrajene tako, da omogočajo učinkovito elektronsko poslovanje z uporabniki ob predpostavki, da se bo določeno delo opravljalo tudi s strani referentov in administratorjev na SiOL-u:

- Podatkovne zbirke so razširjene z novimi in predelanimi obstoječimi tabelami.
- Zaledni sistemi so razširjeni tako, da poslovni procesi prepoznajo nov način upravljanja z dokumenti in izkoriščajo njihove prednosti ter odpravljajo slabosti drugih ob predpostavki, da se osnovna vodila ne spreminjajo.
- Aplikacije, ki jih uporabljajo referenti in administratorji, so dodelani tako, da je oblika dokumenta prepoznavna in da se način komuniciranja ohranja čez ves proces (v primeru sklepanja pogodb na elektronski način se celotno nadaljnje komuniciranje izvaja elektronsko, vključno s pozneje izstavljenimi računi za opravljene storitve v preteklem mesecu).
- Arhiviranje dokumentov se izvaja v skladu z zakonom ZEPEP, ki določa, da se morajo hraniti v izvorni obliki.

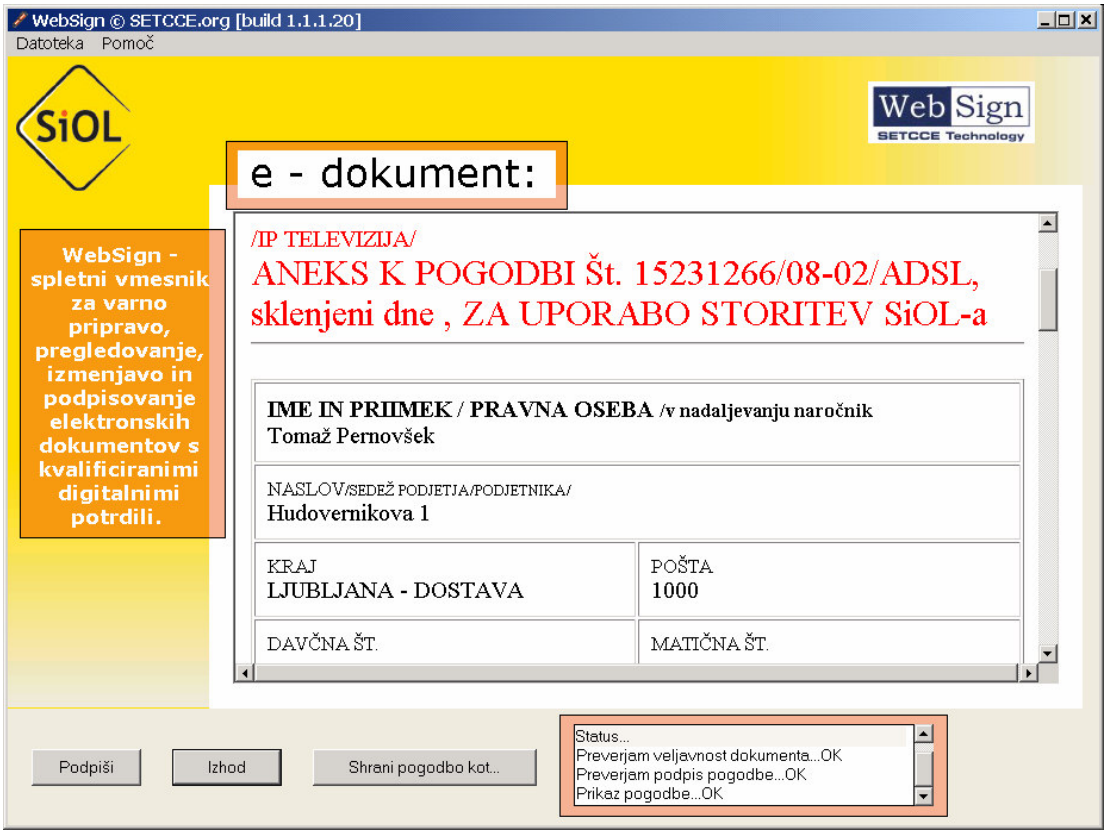
Slika 28 - Zgradba SiOL WebSign na osnovi javanske tehnologije in activeX



Sistem SiOL WebSign, ki ozko gledano ponazarja samo surovo infrastrukturo za varno izmenjavo dokumentov prek interneta brez njegove implementacije v omrežje SiOL, je razdeljen na več funkcijskih elementov, ki so se razvili v okviru projekta:

- Komunikacijski modul. Pošiljanje in sprejem sporočil SOAP (angl. request/reply) s pripetimi datotekami (angl. SOAP with attachments).
- Modul za generiranje dokumentov. Zajame vnose iz tabel HTML in generira dokument XML (pogodbo).
- Modul za podpisovanje. Podpis dokumentov z uporabo podpisa XML.
- Modul za preverjanje. Preverjanje veljavnosti oznak v dokumentu in pogodbi.
- Modul za prikaz. Prikaz HTML dela dokumenta.
- Modul za preverjanje komunikacije.

Slika 29 - Odjemalec SiOL WebSign z vstavljenim e-dokumentom



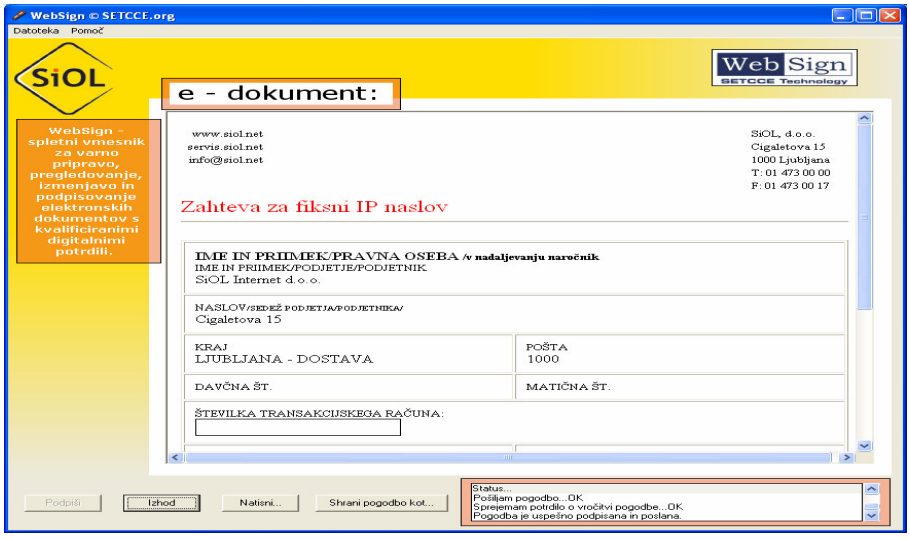
4.2.2 Tehnična izvedba

Tehnična izvedba je bila razdeljena na več faz, ki so se izvajale tudi sočasno, saj je bilo vpletenih več razvojnih ekip različnih izvajalcev. Največji razvoj je naredila ekipa, ki se je ukvarjala s sistemom SiOL WebSign. Izdelala je prototip infrastrukture za varno komuniciranje na osnovi dokumentov XML. Druga ekipa se je ukvarjala z nadgradnjo obstoječih sistemov na SiOL-u, tako da sedaj delujejo tudi dvosmerno z uporabo PKI in spletnih storitev.

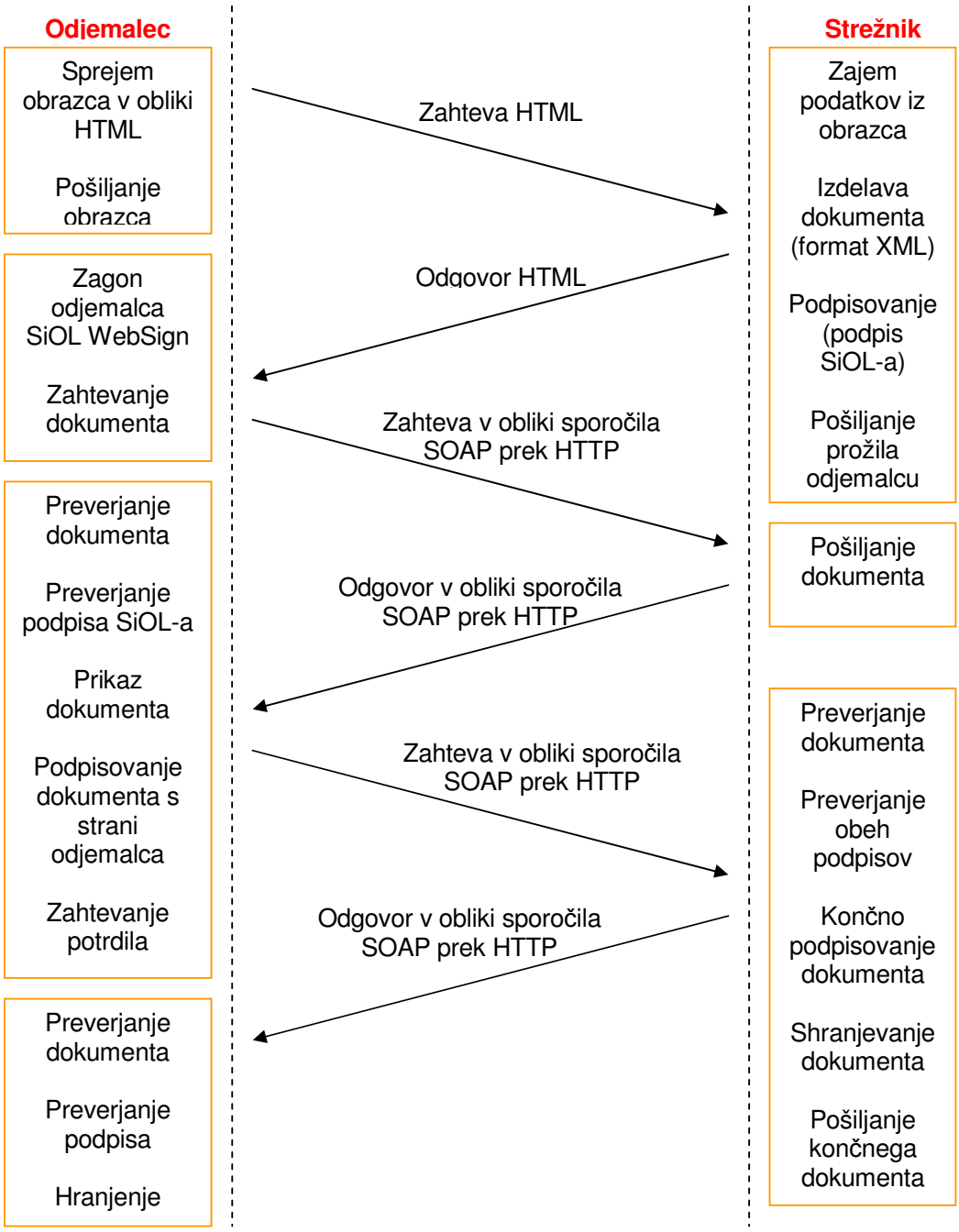
S tehničnega stališča potek oblikovanja pogodbe in njenega podpisovanja delimo na dva osnovna dela (ne glede na vrsto odjemalca oziroma skupino uporabnikov). V prvem delu (ko se uporabnik prijavi prek spletnega odjemalca in izbere storitev) gre za vnos podatkov v pogodbo. Izvedba temelji na preprostih obrazcih HTML. Uporabnik vnese podatke, ki so relevantni v pogodbi (ime, priimek, davčna številka itd.) in jih s funkcijo »pošlji« posreduje strežniku. Temu sledi drugi korak, ki obsega oblikovanje pogodbe v formatu XML, podpis na obeh straneh in varno hranjenje pogodbe ter njeno posredovanje v informacijski sistem. Drugi korak je zasnovan na načelu zahtevek–odgovor (angl. request-response), ki ga sproži uporabnik. Slika 31 prikazuje postopek delovanja drugega koraka. Uporabnik s funkcijo »pošlji« prvega koraka sproži postopek na strežniku. Strežnik prejema in pošilja strežnike na osnovi strežniških programčkov (angl. Servlet) ali strežniških zrn (angl. Enterprise Java Beans) in na osnovi vhodnih podatkov (prejetih podatkov prek obrazca) oblikuje pogodbo v formatu XML ter jo sočasno podpiše. Hkrati prek nove strani HTML sproži zagon odjemalca SiOL WebSign na uporabniški strani. Odjemalec tako zahteva od strežnika prenos podpisane pogodbe.

Odjemalec pogodbo skupaj s podpisom preveri in jo prikaže na zaslonu v formatu HTML. Uporabnik nato pogodbo podpiše in odjemalec ponovno s funkcijo »request« zahteva potrditev prejema pogodbe. Kot potrditev strežnik pošlje ponovno podpisano pogodbo, ki jo uporabnik shrani.

Slika 30 - Zaključek podpisovanja in varne izmenjave e-dokumenta



Slika 31 - Potek delovanja SiOL WebSign



Tehnično je celoten poslovni scenarij, opisan v poglavju 4.1.1, rešen na naslednji način:

1. korak

Na spletnem strežniku se dodajo statične strani, ki omogočajo uporabnikom, da se prek brskalnika odločijo, ali želijo skleniti novo naročniško razmerje ali upravljati z obstoječim.

2. korak

Če uporabnik izbere elektronski način, se izvede prva funkcija znotraj infrastrukture novih Servisnih strani – preverjanje identifikacije uporabnika na podlagi kvalificiranega digitalnega potrdila (angl. client-side authetication). To overjanje izvede spletni strežnik, ki na osnovi vpisanega naslova URL vidi, da je zahtevana varna povezava prek HTTPS. Uporabnik izbere digitalno potrdilo iz nabora svojih potrdil, ki jih ima varno spravljene na pametni kartici, varnem ključu ali na trdem disku svojega računalnika. Spletni strežnik ima nastavljeno omejitev na le tista potrdila, ki so izdana s strani kvalificiranih overiteljev. Aplikacija v podatkovno bazo zapiše poleg podatkov, ki jih uporabnik vpiše v spletni obrazec, še podatke iz digitalnega potrdila (ime, priimek, elektronski naslov) in javni del potrdila. Pred vpisom se še preveri pravilnost vnesenih podatkov (npr. če telefonska številka še nikoli ni bila vnesena v aplikacijo) s povezavo v zaledni sistem z zahtevkom SOAP prek HTTPS v zaledni sistem in enako se pošlje še uspešno vnesena zahteva za storitev. Aplikacija poskrbi za samodejno pošiljanje potrdila o prejeti zahtevi prek elektronske pošte in za vnos nove naloge med opravila za referente SiOL-a.

3. korak

Če je potrebno predhodno preverjanje razpoložljivosti storitve, mora referent preveriti, ali je storitev možno izpolniti in na podlagi odgovora nadalje ukrepati. Preverjanje se vrši prek spletne storitve v drug informacijski sistem (ponudnika omrežja). Ko je odgovor znan, se morajo ob pozitivnem odgovoru pripraviti podatki za pogodbo s klici v zaledni sistem in vmesno tabelo potencialnih uporabnikov in poslati uporabniku prek poštnega strežnika v obliki elektronskega sporočila s povezavami na dokončanje pogodbe.

4. korak

Uporabnik se mora najprej overiti v sistem Servisnih strani z istim digitalnim potrdilom, ki ga je uporabil za izdelavo zahtevka s klikom na povezavo, ki mu je bila poslana prek elektronske pošte. Spletni strežnik na osnovi naslova URL spet ugotovi, da mora vzpostaviti varno povezavo in da se mora uporabnik identificirati z digitalnim potrdilom, takoj zatem pa se opravi še preverjanje pravilnosti izbranega potrdila glede na poslani zahtevek. Na osnovi uspešnega overjanja SiOL WebSign podeli ustrezne pravice uporabniku z izvedbo vnosa SAML. Če je uporabnik že obstoječi naročnik SiOL-ovih storitev, aplikacija dopušča overjanje na dva načina (samo uporabniško ime in geslo oziroma kombinacija uporabniškega imena, gesla in digitalnega potrdila), ki ju izbere uporabnik sam. Aplikacija omogoča elektronsko poslovanje le uporabnikom, ki so uporabili slednji način.

5. korak

Po uspešni overitvi in podelitvi pravic na osnovi vnosa SAML se uporabniku predstavijo dokumenti, ki jih lahko elektronsko izmenja prek sistema. Če je uporabnik šele potencialni naročnik, se mu takoj prikaže osnutek pogodbe, ki je sestavljena na osnovi podatkov, pridobljenih v poizvedbi. Na tem mestu je osnutek spletni obrazec, ki ima že nekatere

vnaprej izpolnjene podatke, ki jih lahko ali pa ne sme spreminjati, odvisno od poslovnega modela. Ko je spletni obrazec popravljen in vsebuje vse podatke za podpis pogodbe, ga uporabnik s potrditvijo pošlje nazaj na spletni strežnik Servisnih strani (shema POST). Servisni strežnik pripravi dokument XML, zahtevek SOAP (ki vsebuje dokument in varnostne informacije) ter pošlje vse skupaj na Varnostni strežnik z uporabo SOAP prek HTTPS znotraj območja DMZ v lokalnem omrežju SiOL-a, sporočilo SOAP pa nosi vse varnostne informacije o pošiljatelju (WS-Security) in njegove pravice prek vnosa SAML. Varnostni strežnik prejme zahtevek SOAP iz Servisnega strežnika in preveri dokument WS-Security/SAML v glavi sporočila SOAP (če je resnično pošiljatelj Servisni strežnik, če je zahtevek še veljaven in če se na poti ni spremenil), kar pomeni, da je s tem pridobil vse informacije o avtorju dokumenta in njegovih pravicah, ne da to ponovno preverja, saj zaupa Servisnemu strežniku in njegovim ugotovitvam. Spletni strežnik pošlje zahtevek naprej na aplikacijski strežnik J2EE, ki izlušči uporabniško ime ter njegove pravice iz vnosa SAML in pripravi vsebino JAAS (opisano v poglavju 4.2.4). Vse nadaljnje operacije se izvajajo na javanskih zrnih, ki komunicirajo s podatkovno bazo in strojnim varnostnim modulom, kjer se vrši podpisovanje dokumenta, saj so digitalna potrdila podjetja SiOL shranjena samo tam. Izvede se prvi podpis v formatu podpisa XML in takšen dokument se pošlje po isti metodi nazaj na Servisni strežnik, ta pa pripravi stran HTML, ki po izvedbi pri uporabniku pokliče odjemalca activeX, s katerim lahko uporabnik še enkrat pregleda pogodbo in jo s klikom na gumb »podpiši« tudi elektronsko podpiše s svojim digitalnim potrdilom. Celoten proces se dogaja za varnim kanalom SSL med odjemalcem in Servisnim strežnikom, ta pa nadalje z že opisano metodo zagotovi varnost na celotni poti.

6. korak

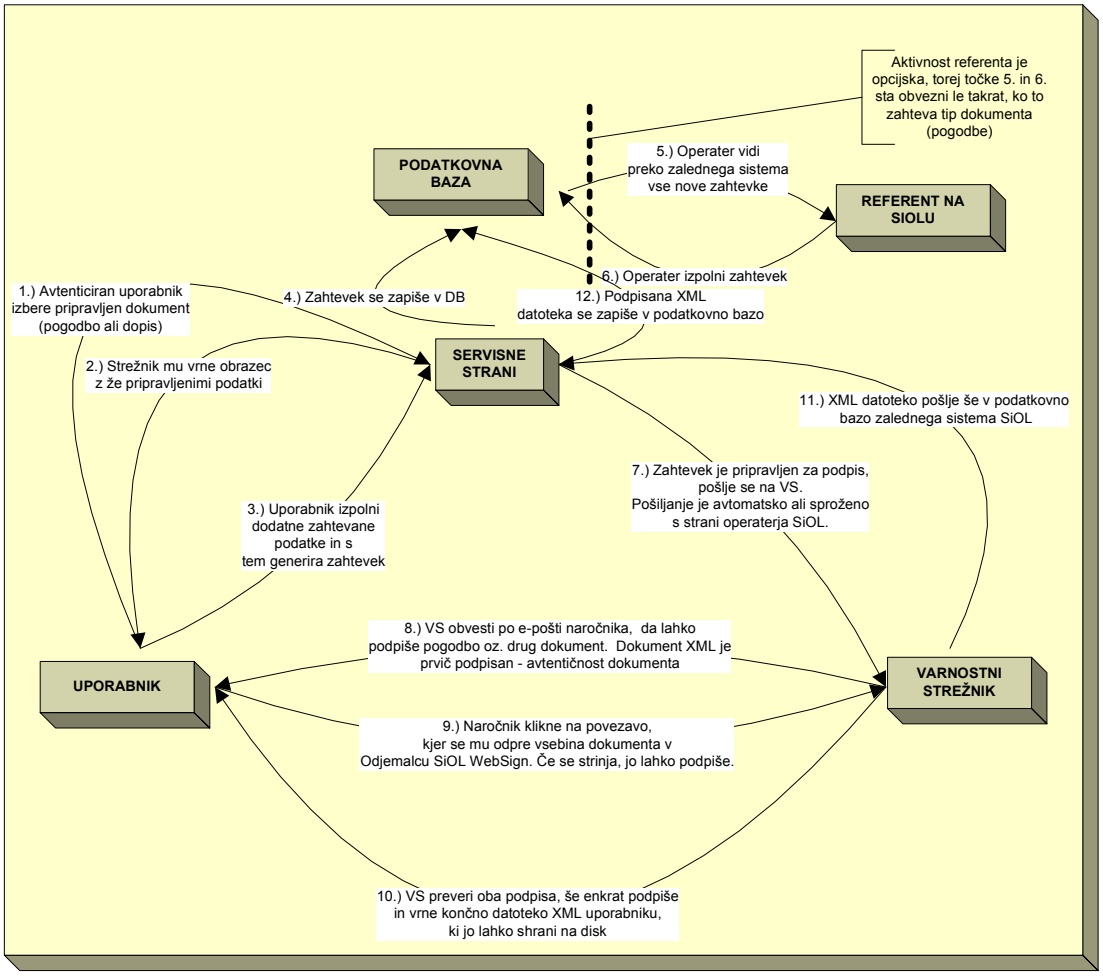
Odjemalec uporabniku zagotovi možnost, da preveri v predstavljenem dokumentu, kdo je njegov avtor (ali je resnično strežnik SiOL-a) s preverjanjem podpisa znotraj dokumenta, omogoči podpisovanje dokumenta in njegovo samodejno pošiljanje nazaj na SiOL oziroma natančneje na Servisni strežnik. Le-ta se v tem trenutku obnaša kot posredovalni strežnik (angl. Proxy), saj dobljen dokument spet preoblikuje v zahtevek SOAP in ga pošlje na Varnostni strežnik, ki dokončno preveri podpisnike in doda svoj končni podpis, kar zagotavlja, da sta v danem trenutku oba podpisa veljavna. Po isti poti potuje končna oblika dokumenta nazaj do Servisnega strežnika, ki ga potem razpošlje na dva naslova – proti uporabniku, da lahko shrani zadnjo kopijo na lokalni disk, in proti zalednemu sistemu, ki poskrbi za njegovo arhiviranje v izvorni obliki.

7. korak

Referent mora naknadno spremljati izpolnitev pogodbe in po potrebi posredovati prek odjemalca za zaledne sisteme. Vsa nadaljnja komunikacija z naročnikom mora potekati v elektronskem načinu, kar zahteva uporabo podpisane in po možnosti tudi šifrirane elektronske pošte v formatu S/MIME.

Na sliki 22 je prikazana tehnična izvedba generiranja, podpisovanja in varne izmenjave elektronskih dokumentov, ki je integrirana v omrežje SiOL. Celoten potek je prikazan od tistega trenutka dalje, ko se že opravi overjanje naročnika.

Slika 32 - Shematski prikaz generiranja in izmenjave dokumentov



Vir: SiOL, d.o.o., 2004

4.2.3 Format, podpisovanje in preverjanje dokumentov

Za format pogodb (dokumentov) je uporabljen XML-standard, ki omogoča preverjanje vsebovanih polj. Zaradi enolične interpretacije razčlenjevalnik XML na strani odjemalca in na strani strežnika sproti preverja veljavnost dokumenta. Če dokument vsebuje neveljavna polja, se zavrže kot neveljaven.

Za prikaz vsebine dokumenta XML poskrbi ločen del, ki je sestavljen v skladu s formatom HTML 4.0. Da bi zagotovili verodostojnost prikaza pogodbe, uporabniški odjemalec vizualizira zgolj del dokumenta v zapisu HTML. S pomočjo podpisa XML uporabnik

podpiše zgolj tisti del, ki je namenjen vizualizaciji. S tem je zadoščeno WYSIWYS[52]. Del dokumenta, ki je podpisan v formatu HTML, odjemalec preveri z namenom, da ne vsebuje nedovoljenih polj, ki bi omogočila napačno vizualizacijo besedila (bele črke na beli podlagi).

Celoten dokument vsebuje tudi dodatna polja za potrebe procesiranja pogodb v informacijskem sistemu. Ta polja določajo nekatere vsebinske dele pogodbe, kot so na primer ime, priimek, davčna številka, predmet pogodbe. Spodnja slika predstavlja primer enostavnega dokumenta XML, ki se uporablja v sistemu SiOL WebSign, vendar nima dodanih oznak, povezanih z digitalnim podpisovanjem.

Slika 33 - Primer dokumenta XML, ki vsebuje besedilo pogodbe

```
<?xml version="1.0" encoding="UTF-8" ?>
 <pogodba>
   <text_pogodbe>
      <html>
        <body>
         vsebina
        </body>
      </html>
   </text_pogodbe>
 <elementi_pogodbe>
  <ime>Janez</ime>
  <priimek>Novak</priimek>
  <predmet>pogodba </predmet>
  <cena>123456789</cena>
 </elementi_pogodbe>
</pogodba>
```

Podpisovanje poteka po standardu za podpisovanje dokumentov, zapisanih v XML (opis je v poglavju 3.4.1), ki omogoča uporabo enotnega zapisa za pogodbo in sam podpis. Podpis je dodan v dokument, ki vsebuje pogodbeno besedilo. Pred podpisom sistem preveri, da dokument XML vsebuje le varnostno nesporne elemente. Tako dokument ne sme vsebovati dinamične vsebine, na primer animacij, skript in drugih interaktivnih delov. Pregledovanje pogodbe se izvaja v posebnem oknu, ki ni del brskalnika. Ko se uporabnik odloči, da bo podpisal pogodbo, sproži proces podpisa na osnovi digitalnega potrdila. Sistem nato

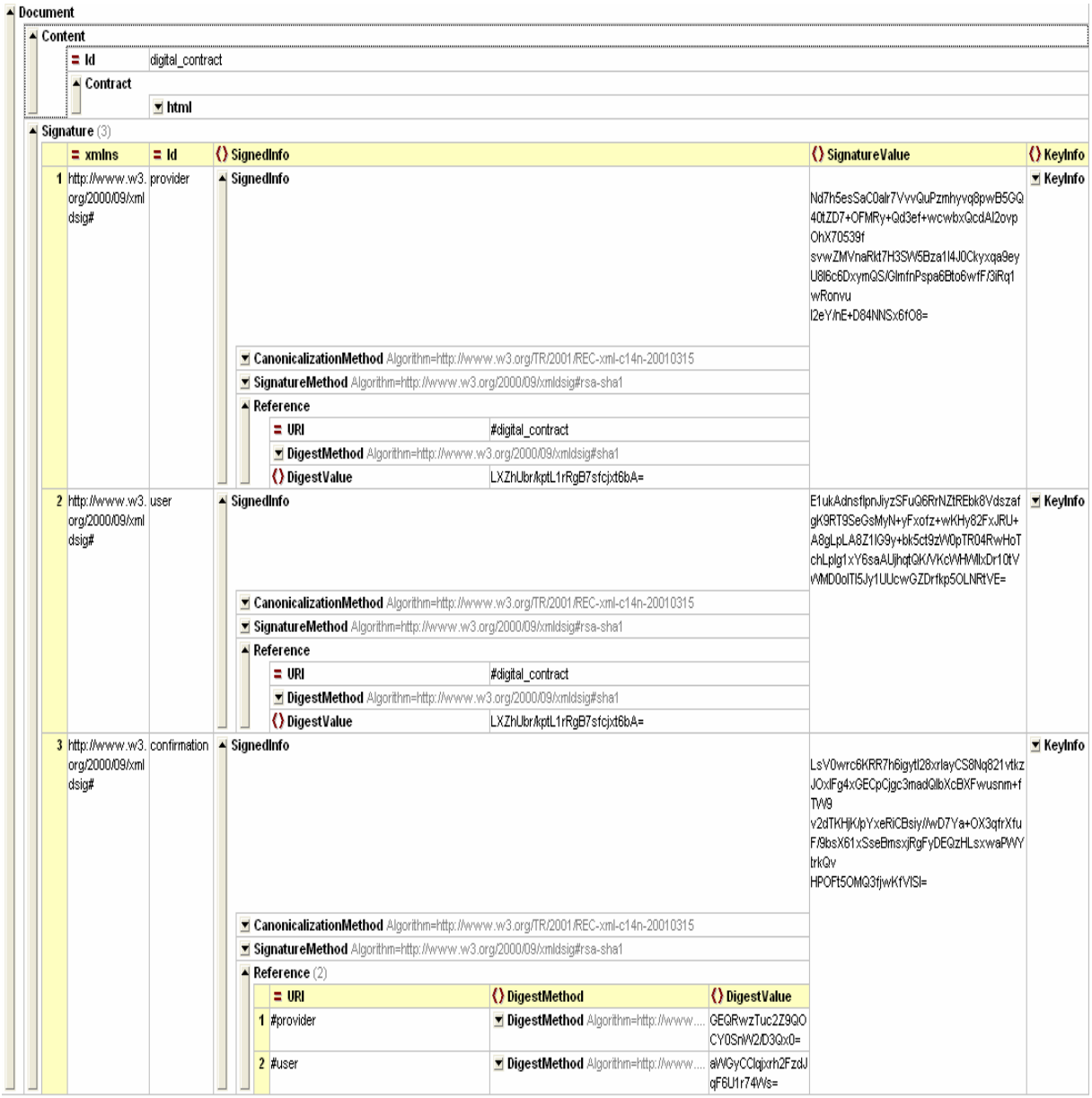
[52] Podpisujem tisto, kar vidim (What You See Is What You Sign).

samodejno pošlje podpisano pogodbo na strežnik in tam preveri veljavnost polj in podpisa. Tudi tu se, tako kot pri vsakem prenosu podatkov, podatki prenesejo v šifrirani obliki.

Dokument, ki je rezultat izdelave, podpisovanja in varne izmenjave dokumentov prek sistema SiOL WebSign, je strukturno prikazan na sliki 34, kjer je bilo uporabljeno orodje za delo z dokumenti XML podjetja Altova, imenovano XML SPY[53]. Osnovni dokument je pripravljen v obliki HTML oziroma izpolnjenega obrazca za spletni prikaz pogodbe, kar hkrati predstavlja tudi vsebino dokumenta. Na tem mestu bi se lahko uporabili tudi dodatni zapisi, na podlagi katerih bi se izvajalo neposredno izpolnjevanje v zalednih sistemih. Vse skupaj je označeno z identifikacijo »digital_contract«. V naslednjem sklopu se nahajajo trije digitalni podpisi v skladu s tehničnimi funkcionalnostmi sistema. Prvi podpis je bil narejen s strani ponudnika internetnih storitev SiOL-a, kar je označeno z identifikacijo »provider«. Drugi podpis je naredil naročnik (identifikacija »user«), tretjega pa spet SiOL, tokrat v vlogi neodvisnega ponudnika varnostnih storitev, saj je preveril veljavnost digitalnih potrdil obeh podpisnikov v času podpisovanja dokumenta (identifikacija »confirmation«). Ker Varnost XML omogoča podpisovanje le dela dokumenta, je nujno, da se znotraj dokumenta jasno nakaže, kaj je podpisnik podpisoval. Oba podpisnika sta podpisovala polje pod identifikacijo »digital contract«, medtem ko je zadnji podpisoval celotno polje obeh podpisnikov. V sistemu SiOL WebSign se uporablja normalizacijska metoda c14n, za podpisovanje pa kombinacija protokolov RSA-SHA1 in za zgoščevanje SHA1. Za lažje delo z dokumenti so dodani tudi vsi javni deli digitalnih potrdil vseh podpisnikov.

[53] Preizkusna različica programa je na volja na spletnih straneh http://www.altova.vom.

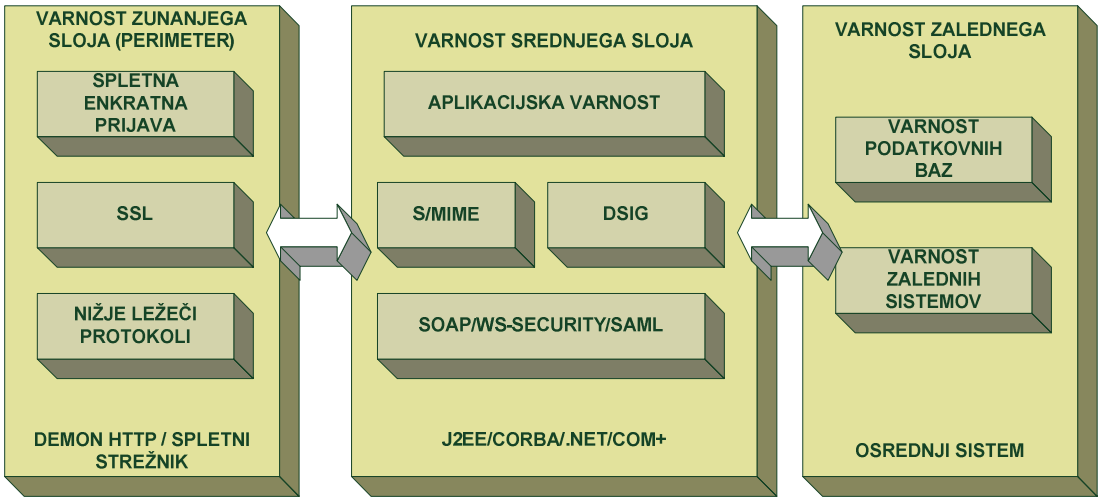
Slika 34 - Strukturno prikazan podpisan dokument



4.2.4 Vzpostavitev varnega okolja

Zadnji korak, ki je zagotovil uspeh projektu, je zelo premišljena vzpostavitev arhitekture za varno elektronsko komuniciranje v okolje SiOL. V tem poglavju so navedene tehnologije, ki podpirajo vzpostavitev varnega okolja za varno elektronsko komuniciranje. Razvrstijo se lahko na pozicijo njihovega delovanja, ali je to na zunanjem okolju v »prvi frontni črti« ali v sredinskem ali na zadnjem nivoju, kjer delujejo zaledne aplikacije podjetja.

Slika 35 - - Primer implementacije varnosti v spletne storitve



Vir: Hartman, 2003, str. 11

Zunanji sloj

Tako varnostni strežnik kot tudi zaledne aplikacije se morajo naslanjati na varnostne mehanizme na prvi ravni, ki tvorijo prvo linijo obrambe, preden različni zahtevki dosežejo spletni strežnik. Te v grobem delimo na požarne zidove in na sisteme za detekcijo vsiljivcev. Le njihova pravilno nastavljena kombinacija delovanja lahko zelo doprinese k skupni varnosti sistema.

Požarni zid varuje eno omrežje od drugega, tako da preverja ves promet, ki prehaja v varovano omrežje. Če obstaja kakršna koli druga možnost vstopa v omrežje, je celotna varnost ogrožena. Požarni zid ima nastavljeno politiko prepuščanja prometa v odvisnosti od prometnih značilnosti. Njegova osnovna dejavnost je tako preprečevanje vstopa v notranje omrežje oziroma prepuščanje prometa le do nekaterih točno določenih strežnikov (http, FTP, poštni strežnik ipd.). Le-ti se po navadi nahajajo na vmesnem področju med dvema požarnima zidovoma v sloju DMZ. V zadnjem času se pojavlja nova vrsta požarnih zidov, ki so namenjeni preverjanju http-prometa, saj ravno spletne storitve in uporaba SOAP povzroča velike preglavice tradicionalnim požarnim zidovom. To so požarni zidovi XML, ki se nahajajo v coni DMZ, delujejo kot posredovalni strežniki (angl. proxy), preverjajo zahtevke SOAP prek http(s) in jih ustrezno overijo ter pooblaščajo. Naloge požarnih zidov so tako zagotavljanje overjanja, nadzora dostopa, varnosti pred napadi od zunaj (napadi tajitve storitve, sleparjenje, pregledovanje vrat, preplavljanje ipd.), beleženja vseh aktivnosti in varnostnih posredovalnih strežnikov, kot je npr. že omenjeni požarni zid XML.

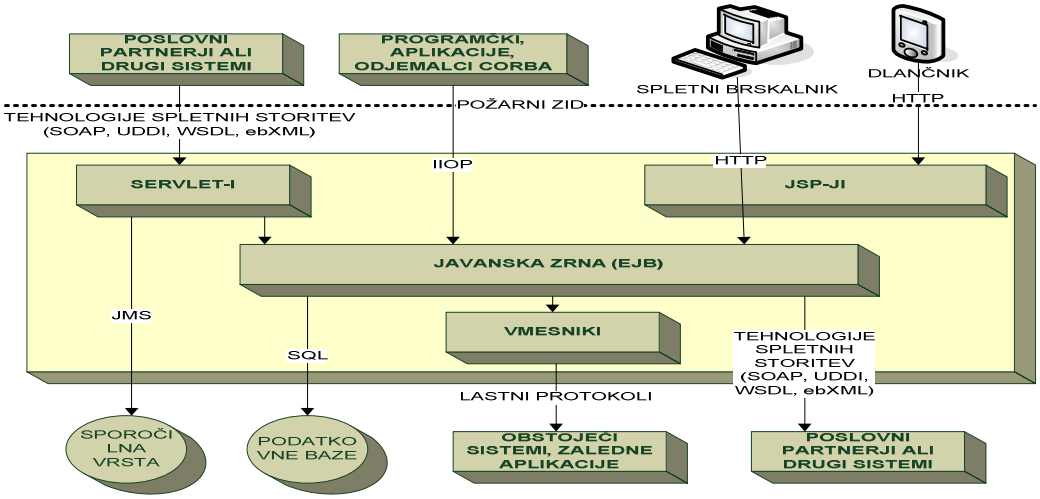
Sistemi za odkrivanje vsiljivcev so drugi nujni del zagotavljanja varnosti na prvi ravni. Uporabljajo dva osnovna modela, prvi je odkrivanje anomalij (iskanje aktivnosti, ki so drugačne od aktivnosti ob normalnem delovanju omrežja), drugi pa odkrivanje napačne uporabe (iskanje aktivnosti, ki ustrezajo poznanim tehnikam vsiljivcev ali odkritim pomanjkljivostim).

Srednji sloj

Komunikacija med sistemi je zelo odvisna od varnosti na srednji ravni. Odvisna je od izbrane tehnologije, ki je lahko CORBA, COM+, .NET ali J2EE (Hartman et. al., 2003, str. 157–217). Lahko se uporabljajo še dodatni varnostni moduli, kot je strežnik za dodeljevanje pravic. Ta je zelo navezan na poslovna pravila podjetja, izvira pa iz bančnega okolja, od koder se je prenesel tudi na ostala okolja, vendar v precej poenostavljeni obliki. V projektu je bilo na strežniški strani uporabljeno okolje J2EE, saj zagotavlja odprtost uporabe spletnih storitev različnih ponudnikov programske opreme, po drugi strani pa je z varnostnega vidika precej bolj nadzorljiv.

Java 2 Platform, Enterprise Edition (J2EE) pridobiva popularnost kot platforma za izvedbe javanskih okolij, ki tečejo na strani strežnika. Podobno kot CORBA je tudi J2EE specifikacija, ki definira pogodbo med razvijalci aplikacij in ponudniki opreme za delovno infrastrukturo in storitve. Na sliki je prikazana arhitektura J2EE, njenih modulov in relacij med njimi. Z varnostnega vidika sta najpomembnejša modula EJB (javanska zrna) in JAAS (javanska storitev za overjanje in nadzor dostopa).

Slika 36 - Namestitev v arhitekturo J2EE



Vir: Hartman, 2003, str. 203

Zaledni sloj

Varnostne tehnologije v zalednih sistemih se nanašajo na dva osrednja sistema – na zaledno strežniško aplikacijo in na podatkovno bazo. Nujno je, da se upoštevajo pravila uporabe teh sistemov in predvsem zagotavljanja njihove varnosti. Ker z njimi komunicirajo aplikacije na srednji ravni, na tem mestu ni treba navajati posebnosti njihove uporabe, treba jih le upoštevati pri načrtovanju pošiljanja in sprejemanja zahtevkov od njih.

4.2.5 Priprava dokumentov za elektronsko poslovanje

Poleg same izvedbe projekta s tehničnega in funkcionalnega stališča smo vzporedno izvajali tudi pripravo vsebine. Poleg celotnih navodil in ostalega vsebinskega materiala, ki je namenjen predvsem uporabnikom, da lahko preverijo, kaj jim elektronska izmenjava dokumentov s SiOL-om prinese, in se naučijo, kako se sploh to naredi na takšen nestandarden način[54], se je skupina za vsebino veliko ukvarjala predvsem s pogodbami in ostalimi dokumenti, ki nosijo pravno-formalne posledice. V prvi sklop dokumentov sodijo naročniške pogodbe, aneksi k pogodbam, standardizirane zahteve in drugi obrazci, ki jih SiOL dnevno izmenjuje s svojimi naročniki. Poleg same pretvorbe v elektronski format, primeren za izmenjavo prek sistema SiOL WebSign, je bilo treba uskladiti vsebino z elektronskim poslovanjem, poleg tega pa še vnesti potrebne programske kontrole (npr. preverjanje vnosa številk ISDN, matične številke ipd.) in v primeru obstoječih naročnikov izdelati aplikacije, ki so polnile obstoječe podatke v ustrezna polja v dokument (npr. ime in priimek naročnika).

V drug sklop sodijo specifični dokumenti za elektronsko poslovanje, ki niso nujni, vendar priporočljivi, saj se z njimi poslovni partnerji (v tem primeru SiOL in naročniki internetnih storitev) dogovorijo za posebne pogoje, ki nastanejo pri izmenjavi elektronskih dokumentov prek sistema SiOL WebSign in njihovega digitalnega podpisovanja s kvalificiranimi digitalnimi potrdili. Ti dokumenti so »Sporazum o elektronskem poslovanju« in »Politike elektronskega podpisa«, ki jih SiOL ima in po želji naročnika oziroma ob posebnih zahtevah tudi posreduje in elektronsko sklepa. Več o teh dokumentih se nahaja v poglavju 2.3.6.

4.2.6 Preizkušanje delovanja

Testiranje sistema SiOL WebSign je bilo razdeljeno na sedem delov (Friedlein, 2001, str. 202–212):

- testiranje uporabnosti/uporabniški sprejem,
- funkcionalno testiranje,

[54] Spletne strani z opisom elektronskega poslovanja na splošno in predvsem, kako je to implementirano v omrežje SiOL, so oblikovane kot del portala na naslovu http://www.siol.net/e-poslovanje.

- operativno testiranje,
- testiranje obremenitve,
- testiranje varnosti sistema,
- preverjanje pravilnosti podatkov (angl. copy proofing) in
- testiranje uporabnosti (angl. User Acceptance Testing – UAT).

Uporabniško testiranje se je izvajalo povsem enako, kot so se pozneje razdelile vloge v sistemu SiOL WebSign. Najpomembnejše (in najbolj občutljivo) je bilo testiranje končnega podpisovanja izdelanih dokumentov XML na strani uporabnika in SiOL-a. Testiranje uporabnosti je tako omejeno na uporabniški odjemalec SiOL WebSign, digitalno potrdilo in na elektronski arhiv, vzporedno s pregledom spletnih strani pa je treba še preveriti pravilnost samodejno izdelane elektronske pošte. Izvajalci testa so bili vsi zaposleni in študenti na SiOL-u, na testiranje pa so bili povabljeni prek interne elektronske pošte.

Testiranje uporabnosti je bilo usmerjeno na dva načina uporabe:

- podpis aneksa k obstoječi pogodbi prek servisnih strani SiOL-a (brez operaterjevega posega) in
- podpis nove naročniške pogodbe (potreben je operaterjev poseg – preverjanje razpoložljivosti in kreiranje naročnika).

Ciljni skupini sta bila omogočena izmenjava in podpisovanje dokumentov v testnem okolju s tesnimi digitalnimi potrdili, ki so se izdajali brez preverjanja identitete in z enotedensko veljavnostjo. Uporabniki so lahko naredili elektronske zahtevke, nato pa jim je skrbnik testiranja naročilo odobril ali preklical. Sledilo je pošiljanje samodejno kreiranih navodil o nadaljevanju postopka uporabniku po elektronski pošti, ki so lahko podpisali elektronske dokumente, sistem pa je poskrbel za njihovo izpolnitev skupaj ali brez operaterja.

Namen testiranja uporabnosti ni bil v generalnem spreminjanju modela delovanja storitve, temveč v odpravi manjših težav oziroma nepreglednosti v uporabniškem vmesniku, vse z namenom izboljšanja uporabniške izkušnje.

Funkcionalno testiranje je namenjeno preverjanju delovanja celotnega sistema v smislu zagotavljanja pravilnosti delovanja, to je delovanja brez javljanja napak, sesutja brskalnika oziroma nepričakovanega obnašanja sistema. Preveriti je bilo treba povezave, čase nalaganja, navigacijo, oblikovne elemente, delovanje poosebljenja, samodejnih aktivnosti (obveščanje po elektronski pošti), tiskanje in tudi videz v vseh brskalnikih (MSIE, Mozzila, Netscape, Opera) pri vseh resolucijah.

Operativno testiranje se je izvajalo z namenom testiranja uporabniške (potencialni naročnik, obstoječi naročnik, operater SiOL) interakcije s spletno aplikacijo in z uporabniškimi odjemalci (SiOL WebSign, zaledni sistem SiOL). Standardna opravila pri poslovanju (dostavni časi, točnost vpisanih podatkov ipd.) se niso preverjala, saj so za to zadolženi naročniki sami. Vsekakor pa je bilo treba preveriti skladnost podatkov (točnost zapisa vsake akcije v sistemu SiOL WebSign) in uporabniško službo na splošni ravni (Kontaktni center SiOL).

Simulacija velike obremenitve spletnega strežnika (**testiranje obremenitve**) je zelo pomembno opravilo pred postavitvijo storitve v produkcijo. Za takšne namene se namesto resničnih uporabnikov uporabljajo raje različna orodja za simulacijo, kot so npr. avtomatizirane ukazne datoteke. Rezultat je prikaz delovanja spletnega strežnika v konicah, kot je npr. prednovoletna akcija, in na podlagi tega se izbire pravilni model bodočega razširjanja strojne opreme, potrebne za zagotavljanje storitve. Simulacija se izvede s klici GET in POST, rezultat pa je podan v obliki časa prenosa, povprečnega časa odziva ipd.

Ključno opravilo pred produkcijo je **testiranje varnosti celotnega sistema** za zagotavljanje storitve SiOL. V svetu obstaja mnogo načinov za vdor v sisteme, tako da je zagotavljanje popolne varnosti skoraj nemogoče, mogoče pa se je kar najbolj približati idealu. Zagotoviti je bilo treba ustrezne nastavitve požarnega zidu in ostalih mehanizmov zagotavljanja varnega sistema, ki so natančno opisani v poglavju 4.2.4. S pomočjo zunanjih svetovalcev se je izvedla simulacija kontroliranih vdorov v sistem.

Zadnje testiranje je bilo **preverjanje pravilnosti podatkov**. To je metoda za zagotavljanje kakovosti, ki mora biti ustrezno formalizirana. Na straneh sistema SiOL WebSign (http://www.siol.net/e-poslovanje) se prikazujejo podatki, ki jih vidi marsikdo, zato na njih ne sme biti tipkarskih ali slovničnih napak, prav tako ne zavajajočih ali neresničnih podatkov ipd.

5 ANALIZA REŠITVE

Pregled in analiza je zadnja faza vsakega projekta, če je delan v skladu s priporočili projektnega vodenja (Friedlein, 2001, str. 234). Po predaji sistema v uporabo, kjer so naročniki lahko začeli uporabljati izmenjavo elektronskih sporočil na osnovi elektronskega podpisa XML s podjetjem SiOL, ne glede na to, ali so podjetja ali fizične osebe, je bilo treba po določenem času izpeljati kritično analizo projekta in samega delovanja sistema kot načrtovane rešitve. Ker se internet vseskozi spreminja, se mora tudi delovanje sistema vseskozi prilagajati novim zahtevam, odkritjem, zakonom in tehnologijam. Tudi če v določenem trenutku predstavlja veliko prednost za vse sodelujoče, jo lahko sčasoma zgubi in postane sam sebi namen.

Analiza projekta je prinesla marsikatero znanje celotnemu projektnemu timu, ki je bil sestavljen iz zaposlenih v SiOL-u kot tudi v podjetjih, ki so nastopala kot zunanji izvajalci. Na samem začetku je vladalo splošno prepričanje, da projekt vsebuje celo vrsto negotovosti in kritičnih dejavnikov, ki bi lahko vodili k njegovem neuspehu. Po uspešnem zaključku tako predprodukcijske faze kot tudi same vpeljave projekta v produkcijo in z uvrstitvijo nove storitve v omrežje SiOL se je izkazalo, da je bila večina kritičnih dejavnikov, ki so sproti pokazali zobe, uspešno »nevtraliziranih«, tudi v skladu s predvidenimi scenariji. Na osnovi kritičnega pregleda izvajanja projekta, tako s strani projektnega vodje, vodstva kot tudi drugih, vpletenih v projekt, so se pridobila znanja, ki bodo lahko uspešno implementirana v razvoj in vodenje prihodnjih projektov v SiOL-u. V analizi projekta so bile obdelane naslednje teme:

- učinkovitost izvedbe projekta,
- komunikacija med člani projektne skupine,
- odzivni časi med naročnikom in izvajalci,
- primernost pripravljene vsebine, ki je opisana v poglavju 4.2.5,
- kakovost izvedene rešitve,
- glavne napake, ki so se storile med projektom, in ali se jim
- podjetje lahko izogne pri naslednjih projektih ter
- ali je bilo delovno okolje in projektna skupina ustrezno izbrana in ali lahko v podobni zasedbi izvede še kakšen projekt.

Še bolj je pomembna analiza rešitve, ki se sedaj uporablja v resničnem poslovnem okolju. Izvedle so se analize na osnovi kriterijev uspeha, ki so bili definirani v fazi predprodukcije, torej pred dejansko izvedbo, opisani pa so v poglavju 4.1.5. Ker se morajo takšne analize nepretrgoma izvajati (Stutely, 2002, str. 223), se lahko na tem mestu opiše le ena izmed njih, ki po določenem času seveda ne bo več aktualna. Pri pregledu neposrednih koristi se je ugotovilo, da število izmenjanih e-dokumentov iz začetnega malega deleža v celotni masi izmenjanih dokumentov stabilno narašča. Naročniki (za zdaj) bolj zaupajo izmenjavi tistih dokumentov, ki niso neposredno povezani z naročniškimi podatki, temveč na same storitve (menjave prenosnih hitrosti, zahteva dodatnih storitev ipd.), čeprav imajo na voljo možnost sklenitve naročniške pogodbe v elektronski obliki (proces je prikazan v Prilogi 0). Tudi število posledičnih akcij, kot je plačilo računov, poslanih v nematerializirani obliki, s kreditnimi karticami prek interneta, se iz meseca v mesec povečuje, kar pomeni tudi zmanjšanje stroškov za SiOL na osnovi manjšega potrebnega obsega pošiljanja računov v papirni obliki. Poleg tega se je zelo povečal odzivni čas od izdanega naročila do izvedene storitve in s tem začetka obračunavanja storitve, saj ni več zamudnih komunikacijskih poti za pošiljanje dokumentov, kjer vsak poslani dokument pomeni en delovni dan, hkrati pa še

stroške tiskanja, razpošiljanja in ostalih stroškov. Ker temelji celotna rešitev na javanski tehnologiji in odprtih standardih, pri čemer je bila posebna pozornost namenjena zagotavljanju varnosti in stabilnosti sistema, se strežniki niso nikoli ugasnili oziroma nehali odzivati. Posredne koristi, kjer so na prvem mestu blagovna znamka, servisiranje uporabnikov in intelektualni kapital, se merijo z različnimi metodami, kjer je najboljša kombinacija uporaba spletnih in navadnih marketinških raziskav, izvedenih s strani specializiranih podjetij. Takšna raziskava, ki bi se posebej ukvarjala z omenjenim projektom, še ni bila izpeljana.

Analiza je prinesla trenutne rezultate uvedbe sistema za izmenjavo sporočil, vsekakor pa je to predvsem naložba v prihodnost, saj papir kot nosilec informacij vse bolj zamenjuje elektronska oblika. Ta prinaša veliko prednosti, ki lahko ob hitrem odzivu postanejo tudi konkurenčne, po drugi strani pa tudi celo vrsto slabosti, ki so sčasoma lahko bolj ali manj odpravljene, zahtevajo pa tisto, česar se ljudje najbolj upirajo – spremembe, v tem primeru predvsem poslovnih procesov.

6 SKLEP

Izmenjava sporočil v podjetniškem poslovanju je prisotna že od samega začetka podjetništva, nosilec, na katerem so zapisana, pa je bil predvsem papir. Z dobo računalništva se je začel uporabljati tudi elektronski način zapisovanja sporočil, na začetku le v zaprtih okoljih, kjer so bile relacije med poslovnimi partnerji natančno pogodbeno dogovorjene. Po definiciji standardnega formata (npr. EDIFACT) in načina pošiljanja je bila varnost zaradi zaprtosti sistema in znanih udeležencev manj upoštevana. Po prihodu interneta, predvsem ob njegovi masovni uporabi, so se začela implementirati odprta okolja za izmenjavo sporočil, vendar se je kmalu pokazalo, da bo zagotavljanje varnosti eden izmed najtežjih delov pri implementaciji takšnih sistemov, ki bodo resnično zaživeli in zagotavljali na eni strani ustrezno stopnjo zaščite, zaupanja in stabilnosti delovanja oziroma na drugi strani pravno-formalne pogoje, ki so potrebni za podjetniško poslovanje. Uporaba infrastrukture javnih ključev in matematičnih metod za zagotavljanje elektronskega podpisovanja ter šifriranja je postala edini način zagotavljanja teh pogojev, tako da so standardizacijska telesa dala velik poudarek na razvoj standardov, ki bi podpirala tovrstno poslovanje. Zaostajala ni niti zakonodaja, saj je večina razvitih držav sprejela zakone o elektronskem podpisu in ustrezno popravila oziroma dopolnila druge zakone v smislu omogočanja elektronskega poslovanja, med drugim tudi z varno izmenjavo sporočil. Na tržišču je v zadnjih letih zagotovo prevladal XML, ki kot metajezik omogoča nastanek novih protokolov, s katerimi se lahko elektronsko posluje. Na začetku ni bilo ustreznih protokolov za zagotavljanje varnosti v teh sporočilih. S prihodom priporočil W3C za zagotavljanje varnosti v dokumentih zapisanih v XML so se odprle možnosti po izvedbi sistemov, ki bi omogočali izmenjavo sporočil v elektronski obliki v formatu XML, ki so digitalno podpisani in po želji tudi digitalno šifrirani. Za razliko od drugih načinov podpisovanja in šifriranja omogočajo večjo transparentnost pri delu, saj ni

potrebno, da se podpiše ali šifrira celoten objekt, temveč le določen del. Razvoj novih standardov na osnovi XML-jezika je šel tudi v smeri zagotavljanja standardnih tipov sporočil (SOAP), standardnih načinov komuniciranja med aplikacijami brez posredovanja (Spletne storitve) in drugih podpornih standardov.

Vse našteto je predstavljalo osnovne gradnike, ki so lahko privedli do tega, da se danes lahko dejansko posluje na popolnoma elektronski način s popolno avtomatizacijo procesov, s katerimi se lahko obdelujejo izmenjana sporočila z namenom izpolnitve določenega poslovnega procesa. Model, ki temelji na teh tehnologijah in preslika poslovne procese na ustrezen pravno-formalen način, je bil razvit najprej kot koncept, ki se je zaradi vseh prednosti tudi v obliki projekta prenesel v realno poslovno okolje storitvenega podjetja SiOL. Potrdil je osnovno hipotezo magistrskega dela in hkrati postavil okvirni program, kako lahko tudi druga podjetja prenesejo elektronsko poslovanje v obliki izmenjave elektronskih sporočil v svoje vsakodnevno poslovanje.

7 LITERATURA

1. Adams Carlisle, Lloyd Steve: Understanding PKI: Concepts, Standards and Deployment Considerations. Boston: Addison Wesley Professional, 2002. 352. str.
2. Ahuja Vijay: Secure Commerce on the Internet. Orlando: AP Professional, 1997. 298. str.
3. Brouchet Dominique et. al.: Bela knjiga - Elektronsko poslovanje malih in srednje velikih podjetij, skupna pobuda skupine EITIRT, Evropske komisije in Lyona. Ljubljana: Slovensko društvo Informatka, 1997. 47. str.
4. Chissick Michael: The Perils of On-line Contracting, Coputer and Communications Law Review, Issue 5, 2000.
5. Clark Mike et.al.: Web Services Business strategies and Architectures. B.k.: Expert Press, 2002. 368. str.
6. Copeland Henry: Digital Signatures - Throw away your pens?, Entertainment Law Review, Vol. 11, Issue 5, 2000.
7. Dournaee Blake: XML Security. Berkeley: McGraw-Hill Osborne Media, 2002. 379. str.
8. E. Eastlake III Donald, Niles Kitty: Secure XML – The New Syntax for Signatures and Encryption. Boston: Addison-Wesley, 2003. 532. str.
9. Ford Warwick, Baum Michael: Secure Electronic Commerce. Upper Saddle River: Prentice Hall PTR, 1997. 470. str.
10. Friedlein Ashley: Web Project Management. San Diego: Academic Press, 2001. 324. str.
11. Hammond Ben: Digital Signatures. B.k.: McGraw-Hill Osborne Media, 2002, 368. str.
12. Hartman Bret et. al.: Mastering Web Services Security. Indianapolis: Wiley Publishing, 2003. 464. str.

13. Housley Russ, Polk Tim: Planning for PKI – Best Practices for Deploying Public Key Infrastructure. B.k.: Wiley Computer Publishing, 2001. 327. str.
14. Ilešič Tomaž, Perenič Gorazd: Temeljne pravne ureditve e-poslovanja v Evropski uniji in Republiki Sloveniji. Podjetje in delo, Ljubljana: Gospodarski vestnik, številka 6/7, 2001, str. 1299–1307.
15. Jerman Blažič Borka et.al.: Elektronsko poslovanje na internetu. Ljubljana: GV Založba, 2001. 206. str.
16. Jerman Blažič Borka, Klobučar Tomaž: Advanced Communications and Multimedia Security. Boston: Kluwer Academic Publishers, 2002. 307. str.
17. Kalakota Ravi, Robinson Marcia: e-Business – Roadmap for Success. Reading: Addison Wesley Longman, 1999. 378. str.
18. Loeb Larry et al: Hack Proofing XML. B.k.: Syngress Media Inc, 2002. 608. str.
19. Lynch Daniel, Rose Marshall: Internet System Handbook. Reading: Addison Wesley Longman, 1999. 790. str.
20. Makarovič Boštjan, Klemenčič Goran, Klobučar Tomaž, Bogataj Maja, Pahor David: Internet in pravo. Ljubljana: Založba Pasadena, 2001. 220. str.
21. Menezes Alfred, Ooorschot van Paul, Vanstone Scott: Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997. 780. str.
22. Moon Michael, Warwick Joel: Business Case for Automating Business-Forms Lifecycle. White Paper. Oakland ZDA: Gistics Incorporated, 2004. 23. str.
23. Nash Andrew, Duane William, Celia Joseph, Brink Derek: PKI Implementing and Managing E-Security. Berkeley: McGraw-Hill Osborne Media, 2001. 513. str.
24. Norris Mark, West Steve, Gaughan Kevin: eBusiness Essentials – Technology and Network for the Electronic Marketplace. Chichester: John Wiley & Sons Ltd, 2000. 296. str.
25. O'Neill Mark: Web Services Security. Berkeley: McGraw-Hill Osborne Media, 2003. 312. str.
26. Pavliha Marko, Jerman - Blažič Borka et. al.: Zakon o elektronskem poslovanju in podpisu s komentarjem. Ljubljana: GV Založba, d. o. o., 2002. 222. str.
27. Rayport Jeffrey, Jaworski Bernard: E-Commerce. New York: McGraw-Hill, 2000. 456. str.
28. Rescorla Eric: SSL and TLS: Designing and Building Secure Systems. Boston: Addison Wesley Professional, 2000. 499. str.
29. Schneier Bruce: Secrets and Lies - Digital Security in a Networked World. Chichester: John Wiley & Sons Ltd, 2000. 432. str.
30. Stutely Richard: The Definitive Bisiness Plan. Second Edition. London: Pearson Education Limited, 2002. 312. str.
31. Škufca Uroš: Zakon o elektronskem poslovanju in elektronskem podpisu. Pravna praksa - Priloga: Informatika in pravo. Ljubljana: Gospodarski vestnik, d. d., 2000, št. 11–12 (2000), str. 1—3.
32. Thomas Stephen: SSL and TLS Essentials. B.k.: John Wiley & Sons, 2000. 212. str.
33. Timmers Paul: Electronic Commerce. New York: John Wiley & Sons, 1999. 268. str.

34. Toplišek Janez: Elektronsko poslovanje. Ljubljana: Založba Atlantis, 1998. 336. str.
35. Turban Efraim, Lee Jae, Lee Kyu Jae, King David, Chung Michael: Electronic Commerce – A Managerial Perspective. New Jersy: Prentice Hall, 2001. 512. str.
36. Weill Peter, Vitale Michael: Place to Space - Migrating to e-business Models. Boston: Harward Business School Press, 2001. 372. str.
37. Westland Christoper, Clark H. K. Theodore: Global Electronic Commerce – Theory and Case Studies. Massachutes: MIT Press, 1999. 592. str.

8 VIRI

1. IETF/W3C XML-Dsig Working Group. [URL: http://www.w3.org/Signature/], 1.6.2004.
2. Simon Ed, Madsen Paul, Adams Carlisle: An Introduction to XML Digital Signatures. [URL: http://www.xml.com/pub/a/2001/08/08/xmldsig.html], 8.8.2001.
3. DataPower Technology, Inc.: Essential XML Web Services Security Best Practises. [URL: http://www.datapower.com/docs/XMLWSS_BP0503.pdf], maj 2003.
4. Mehlhorn Herb, Leblanc Kevin: e-Signatures – The e-Business Enabler. [URL: http://www.rsa.com], 13.3.2002.
5. Mactaggart Murdoch: Enabling XML Security – An Introduction to XML encryption and XML signature. [URL:http://www-106.ibm.com/developerworks/xml/library/s-xmlsec.html/index.html], 1.9.2001.
6. Eastlake 3rd Donald: RFC 3275 - XML-Signature Syntax and Processing. [URL: http://www.ietf.org/rfc/rfc3275.txt], 12.8.2002.
7. Kermaier Ari, Morgan Joe: Digital Signatures and Encryption. [URL: http://www.sys-con.com/xml/articleprint.cfm?id=544], 1.12. 2002.
8. Igor Lesjak: Pasti pri digitalnem podpisovanju dokumentov XML. Ljubljana. [URL: http://www.ltfe.org/pdf/XMLSigning.pdf], 22.5.2003
9. e-SLOG: Dokumentacija delovne skupine za elektronski podpis. Ljubljana. [URL: http://www.gzs.si/Nivo1.asp?ID=15875&IDpm=1975], 15.6.2004.
10. Bray Tim, Paoli Jean, Sperberg-McQueen C.M, Maler Eve: Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation 6. [URL: http://www.w3.org/TR/REC-xml], 6.10. 2000.
11. Bartel Mark, Boyer John, Fox Barb, LaMacchia Brian, Simon Ed: XML-Signature Syntax and Processing - W3C Recommendation, [URL: http://www.w3.org/TR/xmldsig-core], 12.2.2002.
12. McCullagh Adrian, Caelli William: Non – Repudiation in the Digital Environment, [URL: http://www.firstmonday.org/issues/issue5_8/mccullagh/index.html], 19.7.2000.
13. UNCITRAL: UNCITRAL Model Law on Electronic Signatures. [URL: http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf], 2001.
14. UNCITRAL: UNCITRAL Model Law on Electronic Commerce with Guide to Enactment. [URL: http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm], 1996.

15. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal št. 013 (2000), str. 0012–0020. [URL: http://europa.eu.int/information_society/topics/ebusiness/ecommerce/8epolicy_elaw/law_ecommerce/legal/documents/1999_93/1999_93_en.pdf] , 2000.
16. W3C: Canonical XML, Version 1.0, W3C Recommendation. [URL: http://www.w3.org/TR/xml-c14n] , 2001.
17. Security in a Web Services World - A Proposed Architecture and Roadmap. [URL: http://www-106.ibm.com/developerworks/security/library/ws-secmap/], 2002.
18. ETSI SEC: Electronic Signature Formats, v.1.2.2., Technical Specification ETSI TS 101733, 2000.
19. ETSI SEC: XML Advanced Electronic Signatures (XAdES), Technical Specification ETSI TS 101903, 2002.
20. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [URL: http://www.ietf.org/rfc/rfc3280.txt] , 2002.
21. XML Encryption Syntax and Processing W3C Candidate Recommendation. [URL: http://www.w3.org/TR/xmlenc-core/], 2002.
22. Dumortier Jos et.al.: The Legal and Market Aspects of Electronic Signatures, Study for the European Commission. [URL: http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf], 10.2.2004.
23. Council of Europe: Convention on Cybercrime. [URL:http://conventions.coe.int], 2004.
24. Zakon o elektronskem poslovanju in elektronskem podpisu ZEPEP (Uradni list RS, št. 57/00).
25. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00 in 193/01).
26. Zakon o gospodarskih družbah ZGD (Uradni list RS, št. 30/93).
27. Zakon o obligacijskih razmerjih ZOR (Uradni list SFRJ, št. 29/78).
28. Zakon o pravdnem postopku ZPP (Uradni list RS, št. 26/99).
29. Zakon o splošnem upravnem postopku ZUP (Uradni list RS, št. 80/99).
30. Zakon o varstvu konkurence ZVK (Uradni list RS, št. 18/93).
31. Zakon o varstvu osebnih podatkov ZVOP-1 (Uradni list RS, št. 86/04).
32. Zakon o varstvu potrošnikov ZVPot (Uradni list RS, št. 20/98).
33. SiOL, d.o.o., interna gradiva, 2004.

9 SLOVARČEK SLOVENSKIH PREVODOV TUJIH IZRAZOV

Tuj izraz	**Slovenski prevod**
Application Service Provider (ASP)	Ponudnik aplikacij
Time Stamp	Časovni žig
Digital Signature	Digitalno potrdilo
Electronic Bill Presentment and Payment (EBPP)	Elektronska predstavitev in plačilo računa
Electronic Data Interchange (EDI)	Računalniško izmenjavanje podatkov
Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)	EDI za administracijo, trgovino in transport
The European Electronic Signature Standardization Iniciative (EESSI)	Evropska iniciativa za standardizacijo elektronskih podpisov
Electronic Signature	Elektronski podpis
Electronic Commerce	Elektronsko poslovanje
Lightweight Directory Access Protocol (LDAP)	Enostavni protokol za dostop do imenika
European Union	Evropska unija
Internet Engineering Task Force (IETF)	Delovna skupina za internetno inženirstvo
Java 2 (Platform) Enterprise Edition (J2EE)	Java 2 podjetniška različica
Qualified Certificate	Kvalificirano potrdilo
Organization for the Advancement of Structured Information Standards (OASIS)	Organizacija za napredek na strukturnih informacijskih standardih
Certificate Authority (CA)	Overitelj, agencija za overjanje (AC)
Public-key cryptography Standards (PKCS)	Kriptografski standardi
Public Key Infrastructure (PKI)	Infrastruktura javnih ključev
Business to Business e-commerce (B2B)	Poslovanje med podjetji
Business to Consumer e-commerce (B2C)	Poslovanje podjetje - posameznik
Time Stamp Protocol	Protokol za časovno žigosanje
File Transfer Protocol (FTP)	Protokol za prenos datotek
Online Certificate Status Protocol (OCSP)	Protokol za sprotno preverjanje statusa potrdila
HyperText Transport Protocol - Secure (HTTPS)	Protokol za varni prenos hiperteksta
Security Assertion Markup Language (SAML)	Jezik za označevanje z izjavo o varnosti
Certificate Revocation List (CRL)	Seznam preklicanih potrdil
Directive	Smernica
Service-Oriented Architecture (SOA)	Storitveno orientirana arhitektura
Simple Object Access Protocol	Protokol za enostaven dostop do objektov

(SOAP)	
Hardware Security Module (HSM)	Strojni varnostni modul
Universal Description Discovery and Integration (UDDI)	Imeniki za spletne storitve
United Nations Commission on International Trade Law (UNCITRAL)	Komisija Združenih narodov za mednarodno gospodarsko pravo
Universal Resource Identificator (URI)	Enolični identifikator virov
World Wide Web Consortium (W3C)	Konzorcij svetovnega spleta
Web Services Description Language (WSDL)	Standard za opis spletnih storitev
What You See Is What You Sign (WYSIWYS)	Koncept »kar si videl, si podpisal«
XML Advanced Electronic Signatures (XAdES)	Standard za napredne elektronske podpise
XML Key Management Specification (XKMS)	Standard W3C za upravljanje s ključi
eXtensible Markup Language (XML)	Razširljivi označevalni jezik
XML-Signature Syntax and Processing (XMLDSIG)	Standard W3C za podpisovanje dokumentov, zapisanih v XML
XML Encryption Syntax and Processing (XMLENC)	Standard W3C za šifriranje dokumentov, zapisanih v XML

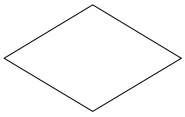
PRILOGE

Diagrami postopka varne izmenjave elektronskih dokumentov

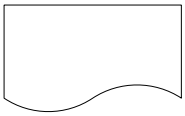
Legenda:

Začetek oziroma konec postopka

Aktivnost, dogodek, dejavnost, ravnanje

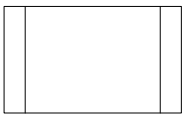


Odločitev

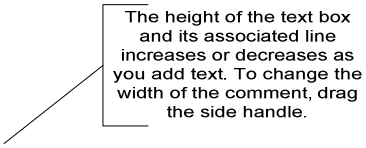


Obvezen dokument v postopku

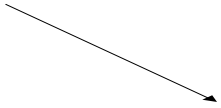
Opcijska aktivnost, dogodek, dejavnost, ravnanje



Vnaprej določena aktivnost, dogodek, dejavnost, ravnanje

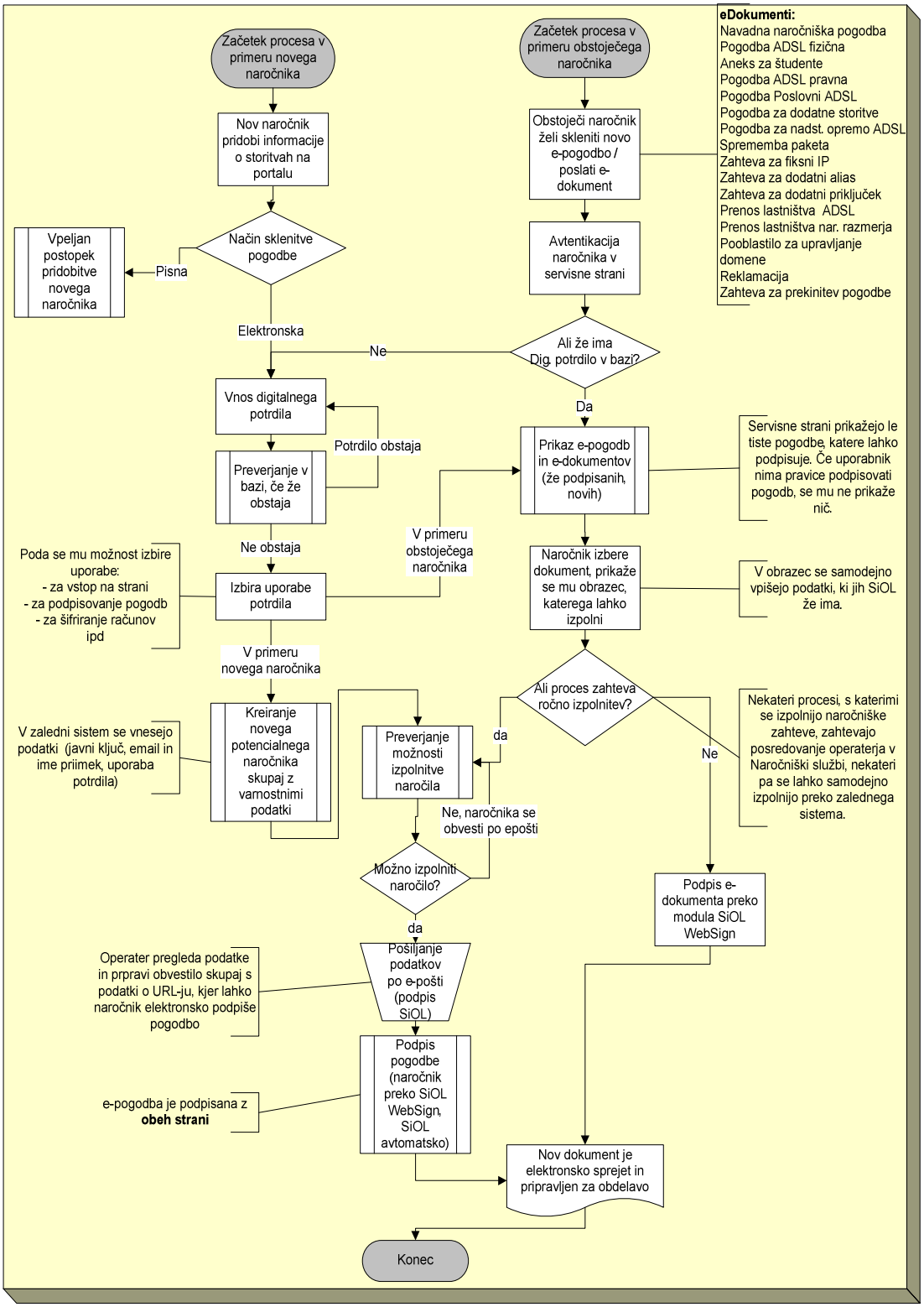


Pojasnilo



Smer izvajanja postopka

Priloga 1: Splošen postopek varne izmenjave elektronskih dokumentov v omrežju SiOL



Priloga 2: Postopek sprejemanja naročniške pogodbe za širokopasovni priključek ADSL