Varen elektronski podpis kot temelj elektronskega poslovanja

Igor Lesjak
igor.lesjak@crea.si
CREA d.o.o., www.crea.si.

Elektronsko poslovanje in elektronski podpis

V zadnjih dveh desetletjih so se podjetja ukvarjala predvsem z informatizacijo svojega poslovanja. Povezava med poslovnimi procesi različnih partnerskih podjetij je večinoma ostala »tradicionalna«. Povezava še vedno temelji na papirnih dokumentih, ki jih pošiljatelj v svojem informacijskem sistemu natisne, prejemnik pa podatke iz dokumenta ročno prenese v svoj informacijski sistem. Elektronsko poslovanje pomeni predvsem informatizacijo povezave poslovnih procesov podjetja s svojimi poslovnimi partnerji in končnimi uporabniki. V praksi to pomeni predvsem odpiranje elektronskih tržnih poti do končnih uporabnikov ali manjših podjetij (npr. spletno elektronsko bančništvo) ali neposredno povezavo z informacijskim sistemom poslovnega partnerja (npr. elektronska preskrbovalna veriga trgovskega podjetja).

Elektronsko poslovanje doseže največji poslovni učinek, ko uspemo elektronsko povezati večino svojih partnerjev, saj lahko le na ta način ukinemo ali vsaj minimiziramo količino tradicionalnih papirnih dokumentov. Povezovanje z uporabo odprtega, javnega, globalnega omrežja, kot je Internet, je zaradi tega nujna. Prav zaradi odprtosti komunikacijskega medija pa je potrebno posebno pozornost nameniti zagotavljanju ustreznega nivoja varnosti. Kdo je odgovoren za podatke na poslovnem dokumentu? S čigavo aplikacijo delamo, čigave programske komponente se nameščajo na naš računalnik in s katero aplikacijo komuniciramo? Ali se je vsebina dokumenta od trenutka njegovega nastanka spremenila? Kdaj je nastal poslovni dokument? Ali lahko partner zanika oddajo podatkov? Ali lahko partner zanika prejem podatkov? To je samo nekaj vprašanj, ki se porajajo tipičnemu uporabniku elektronskega poslovanja. Eden temeljnih mehanizmov računalniške varnosti, ki prinaša odgovor na vsa omenjena vprašanja, je elektronski podpis.

Elektronski podpis kot pravni termin

Elektronski podpis lahko uporabljamo zgolj kot dodaten varnostni mehanizem, ki poviša nivo varnosti v računalniški aplikaciji. Vendar pa ne gre samo za tehnični ampak tudi pravni termin. Elektronski podpis je namreč tisti varnostni element, ki zagotavlja dokumentu v elektronski obliki pravno veljavo, npr. računu v elektronski obliki status verodostojne knjigovodske listine.

Podobno kot za druga področja velja tudi za področje elektronskega poslovanja in elektronskega podpisa, da morajo članice Evropske unije lokalno zakonodajo uskladiti s skupnimi priporočili. Smernice narekujejo ustrezne direktive Evropske unije in Združenih narodov. Najpomembnejša sta direktiva o elektronskem podpisu, Direktiva 1999/93/EC, s pripadajočimi aneksi in podrejenimi tehničnimi standardi ETSI in CEN ter Modelni zakon Komisije OZN za mednarodno gospodarsko pravo (UNCITRAL) o elektronskem poslovanju.

Zahteva po usklajenosti lokalne zakonodaje velja tudi za Slovenijo, kjer je Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) s pripadajočo uredbo že usklajen z direktivo in modelnim zakonom. Ker pa se evropske smernice (predvsem tehnična priporočila) še vedno dopolnjujejo, je v pripravi že novi zakon. ZEPEP med drugim opredeljuje pogoje, pod katerimi je elektronski podpis enakovreden lastnoročnemu podpisu.

Za vstop v svet elektronskega poslovanja podjetjem ne bo potrebno natančno analizirati zajetnega snopa omenjene zakonodaje. V Delovni skupini za elektronski podpis na GZS pripravljamo strnjena, razumljiva in praktično usmerjena priporočila, ki bodo podjetjem olajšala predvsem pripravo zahtev in ovrednotenje ponudb za varne aplikacije elektronskega poslovanja. Z upoštevanjem teh priporočil bo zagotovljena tudi skladnost z vso ustrezno zakonodajo na tem področju.

Elektronski podpis kot tehnični termin

Razumevanje elektronskega poslovanja in elektronskega podpisa najlažje dosežemo z vzpostavitvijo vzporednic s tradicionalnim poslovanjem. Poglejmo primer podpisa poslovne pogodbe. Na tradicionalni način bi s poslovnim partnerjem pogodbo najprej lastnoročno podpisala

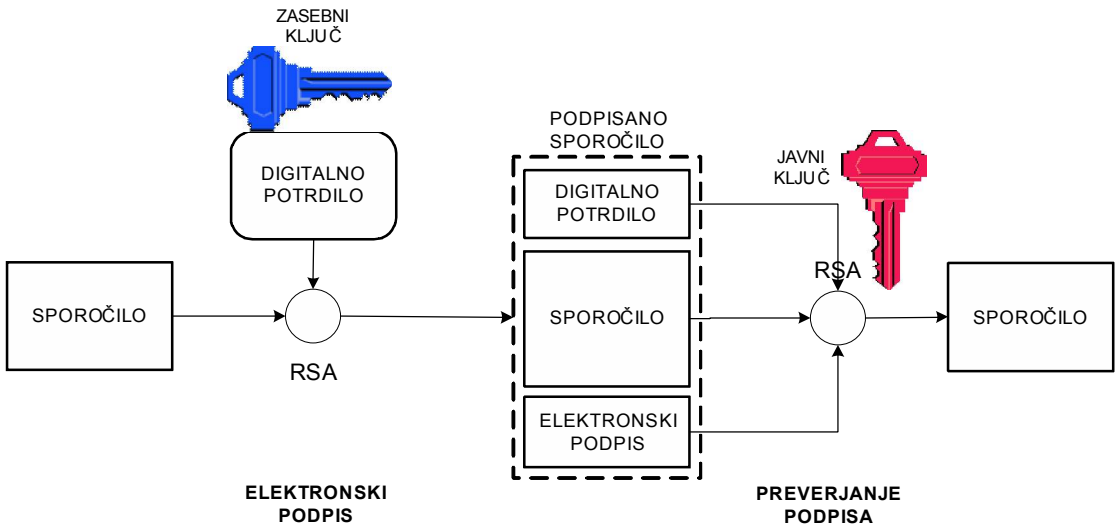
in jo overila pri notarju. Notar preveri istovetnost podpisnika s pomočjo podpisnikovega osebnega dokumenta. Primerja podpis na dokumentu s tistim na pogodbi ter sliko na dokumentu z lastnikom dokumenta. Notar na koncu s svojim žigom in podpisom potrdi obstoj pogodbe na datum overjanja. V opisanem primeru je osebna izkaznica tradicionalni mehanizem identifikacije podpisnika, ki ga izdaja pristojni občinski organ. Osebni dokument je zaščiten s številnimi grafičnimi in tiskarskimi mehanizmi, varnost »tradicionalnega« podpisa pa temelji na mehkih, grafoloških značilnosti človeške pisave.

Čeprav ZEPEP ne predpisuje tehnologije za izvedbo elementov varnega elektronskega poslovanja, temeljijo danes praktično vsi pristopi za izvedbo varnega elektronskega podpisa na asimetrični kriptografiji. Kriptografija je znanstvena veda, ki uporablja zapletene matematične algoritme za izvedbo različnih varnostnih mehanizmov. Skupna lastnost algoritmov je ta, da je iz javnih in zasebnih neznanih vhodnih podatkov preprosto izračunati rezultat, obratno pa je iz rezultata in javnih podatkov praktično nemogoče izračunati zasebne podatke, ki bi napadalcu omogočali npr. poneverbo elektronskega podpisa. Asimetrična kriptografija uporablja v vseh mehanizmih par ključev, ki ga ustvarimo s posebno programsko opremo. Zasebni ključ je skrivni podatek, ki ga poseduje samo njegov imetnik, javni ključ pa je dostopen vsem udeležencem.

Javni ključ je potrebno povezati z njegovim imetnikom in ga javno objaviti. Asimetrična kriptografija v ta namen uporablja infrastrukturo javnih ključev (PKI). PKI s pomočjo digitalnih potrdil, ki jih izdajajo overiteljske agencije poskrbi za povezavo javnih ključev z realnimi objekti, razpečavo javnih ključev in vzpostavitev zaupanja v javne ključe. PKI lahko primerjamo s tiskarsko tehnologijo, ki zagotavlja varnost »tradicionalnih«, tiskanih dokumentov.

Podobno kot osebni dokument v vsakdanjem življenju je njegov elektronski ekvivalent digitalno potrdilo, saj zagotavlja avtentikacijo objektov, tj. fizičnih in pravnih osebo ali strežnikov, v elektronskem svetu. Digitalno potrdilo vsebuje med drugim tudi podatke o njegovem imetniku in overiteljski agenciji, njegov javni ključ in namen za katerega je bilo digitalno potrdilo izdano (npr. za izvedbo digitalnega podpisa). Če občina skrbi za izdajo dokumentov v tradicionalnem svetu, poskrbi za izdajo digitalnih potrdil in avtentičnost podatkov v potrdilu kvalificirana overiteljska agencija, pri nas npr. Sigen-CA na Centeru vlade za informatiko ali PoštarCA na Pošti Slovenije. Storitev kvalificiranega časovnega žigosanja, ki jo ponuja overitelj, je elektronska izvedba notarja. V Sloveniji bo storitev verjetno prva ponudila Pošta Slovenije. Merila za vzpostavitev omenjenih storitev so opredeljena v ZEPEP in pripadajoči uredbi.

Elektronski podpis je elektronski ekvivalent lastnoročnega podpisa. Podobno kot »tradicionalni« podpis zagotavlja v povezavi z osebno izkaznico avtentikacijo podpisnika, vzpostavi elektronski podpis z imetnikovim digitalnim potrdilom elektronsko avtentikacijo podpisnika. Dodatno zagotavlja elektronski podpis tudi celovitost (nespremenljivost) sporočila, podpisnik pa ne more zanikati, da je prav on dokument podpisal (nezatajljivost).



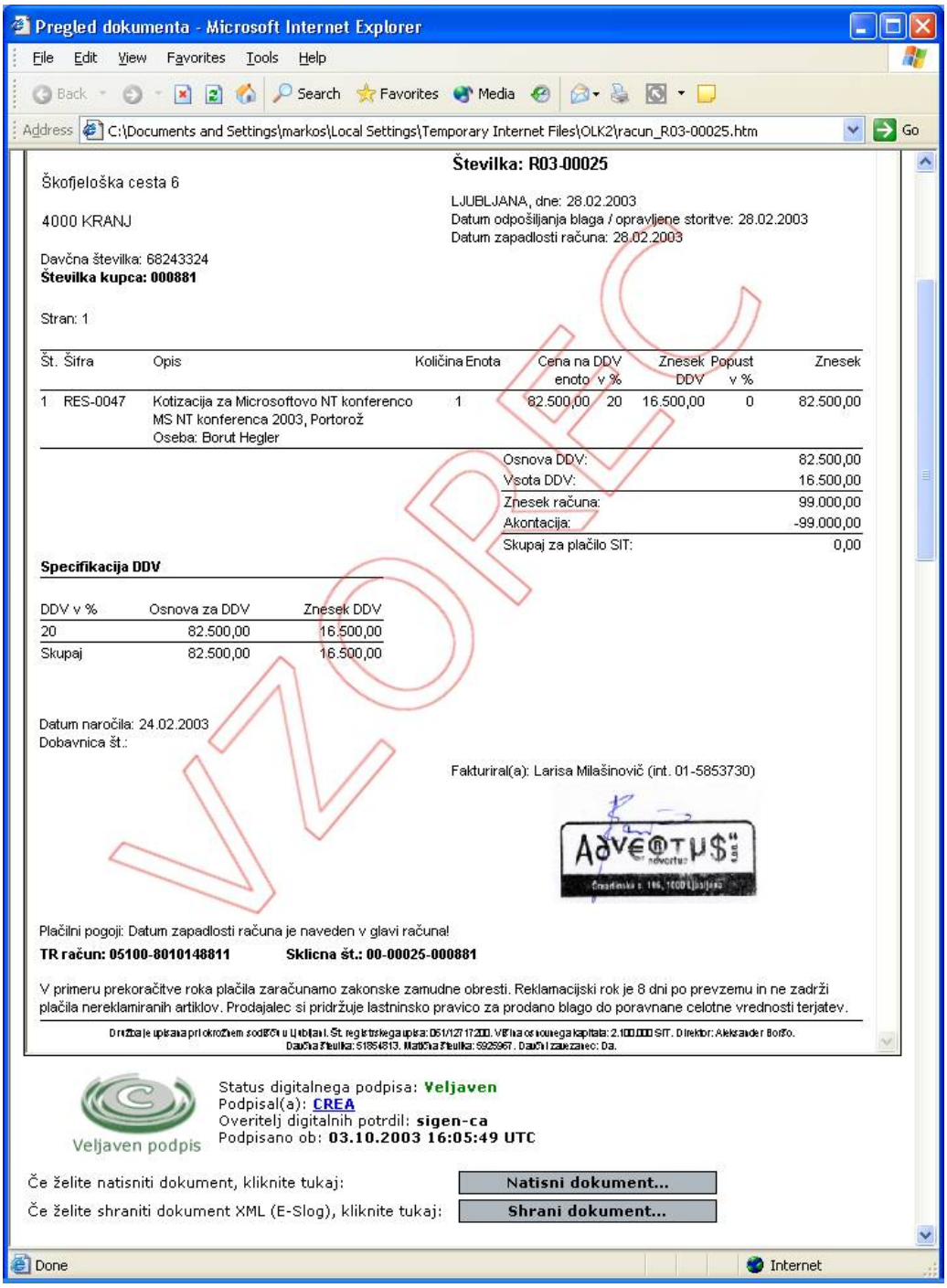
Slika 1: Poenostavljen prikaz izvedbe elektronska podpisa.

Poenostavljen prikaz izvedbe elektronskega podpisa je prikazana na sliki 1. Izvorno sporočilo, ki se

nahaja v levem delu slike, podpiše njegov pošiljatelj. Pri tem uporabi svoj zasebni ključ, elektronski podpis pa skupaj s svojim digitalnim potrdilom in izvornim sporočilom združi v podpisano sporočilo. Na desni polovici slike prejemnik s pomočjo javnega ključa, ki ga dobi iz pošiljateljevega digitalnega potrdila, preveri veljavnost podpisa, s čimer potrdi njegovo celovitost. Iz podatkov v digitalnem potrdilu lahko identificira (avtenticira) podpisnika.

ZEPEP opredeljuje več vrst elektronskih potrdil in elektronskih podpisov. Le varni elektronski podpis, izveden s kvalificiranim elektronskim potrdilom, tj. potrdilom izdanim od kvalificirane overiteljske agencije, je enakovreden običajnemu podpisu.

Poudariti je potrebno, da je varnost celotnega opisanega postopka zagotovljena le, če poskrbimo za varno hranjenje zasebnega ključa. Najbolj razširjena strojna oprema, s katero lahko pri uporabniku vzpostavimo najvišji nivo varnosti hranjenja zasebnih ključev je pametna kartica, saj je zasebni ključ z nje praktično nemogoče razkriti. Pri nas so najbolj razširjene kartice podjetja ActivCard.



Slika 2: Vzorec v spletni brskalnik integriranega elektronsko podpisanega računa spletne aplikacije.

Elektronski podpis ni vse!

Elektronski podpis sam zase ne zagotavlja popolne varnosti. Za doseganje najvišjega nivoja računalniške varnosti, ga je potrebno uporabiti v povezavi z ostalimi aplikacijskimi varnostnimi mehanizmi, npr. avtorizacijo dostopa do podatkov, kriptiranjem komunikacijske povezave, po potrebi pa tudi z dodatnim kriptiranjem samih podatkov ipd.

Čeprav je elektronski podpis v praksi lahko izveden tudi v okviru samostojne aplikacije, ki je usklajena z zakonodajo in tehničnimi priporočili, je takšnih primerov v praksi malo. Elektronski podpis je ponavadi le ena izmed infrastrukturnih funkcij tipične poslovne aplikacije, ki jo uporablja podpisnik. Poslovna aplikacija, s katero je uporabnik že navajen delati, je predvsem preprostejša za uporabo. Zato je za uporabnika najbolj priročno, da je funkcionalnost elektronskega podpisa integrirana v končno aplikacijo. V tem primeru moramo varen način integracije funkcionalnosti za elektronsko podpisovanje v osnovno aplikacijo izvesti na način, ki bo zagotavljal, da bo osnovna aplikacija podrejena zahtevam ZEPEP in usklajena s pripadajočimi tehničnimi priporočili. Tovrstna integracija zahteva dobro poznavanje tako elektronskega podpisa kot celotnega področja računalniške varnosti, saj je bistveni element varnosti celotne aplikacije. Na sliki 2 vidimo v spletno aplikacijo integriran elektronski podpis računa za plačilo kotizacije udeležbe na Microsoftovi NT konferenci.

Pravilna zasnova in arhitektura rešitve, ki vsebuje elektronski podpis, pravilna integracija z ostalimi varnostnimi mehanizmi ter varna in uporabniku prijazna integracija v končno aplikacijo zagotavljajo trenutno najvišji nivo računalniške varnosti. Rešitve, ki omočajo varno in uporabniku prijazno integracijo elektronskega podpisa v končno aplikacijo, na trgu že obstajajo. Mirno lahko rečemo, da je opravljanje storitev na elektronski način, ki se izvaja s pomočjo tovrstne programske opreme, neprimerno varneje, kot opravljanje storitev na »tradicionalni« način. Nespremenljivost podatkov, nezatajljivost, avtentičnost dokumentov ali njihovo kriptiranje je namreč z uporabo »tradicionalnih« tehnologij v praksi nemogoče uveljaviti.