CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

OpenID

NCERT-PUBDOC-2011-07-329

Nacionalni CERT

Sadržaj

Ovaj dokument je vlasništvo Nacionalnog CERT-a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet–a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana kaznenim zakonom RH.

1 Uvod

Naš identitet u digitalnom svijetu razlikuje se od onog u stvarnom svijetu. I dok nam je u stvarnom svijetu dovoljna jedna osobna iskaznica ili putovnica kako bi jednoznačno dokazali svoj identitet, u digitalnom svijetu za svaku uslugu ili web mjesto imamo različite identitete. Uz različite identitete dolaze i različite lozinke i korisnička imena, a tada to postaje i sigurnosni problem budući da su korisnici pod pritiskom da zapamte mnogo korisničkih imena i lozinki. Odgovor na taj pritisak je uporaba jedne te iste, jednostavne, lozinke na više različitih mjesta.

Već dulje vrijeme se pokušava efikasno riješiti problem višestrukih digitalnih identiteta za jednu te istu fizičku osobu. Cilj je da dva ista korisnička imena na različitim stranicama označavaju istu fizičku osobu. OpenID jedno je rješenje koje postiže taj cilj. Razvijen 2005. godine danas je stekao zavidnu popularnost te obećaje da će u budućnosti pojednostaviti upravljanje digitalnim identitetom. Cilj ovog dokumenta je ukratko opisati OpenID, opisati koje prednosti on ima za obične korisnike i vlasnike web stranica, te koje opasnosti se u njemu skrivaju.

2 Osnovna definicija i povijest

OpenID je otvoreni standard koji opisuje način izvedbe decentralizirane autentikacije na Internetu. Decentraliziranom autentikacijom uklanja se potreba za ad-hoc sustavima autentikacije koje implementira svako web mjesto zasebno. Osim toga, korisnicima se olakšava upravljanje digitalnim identitetom. Korisnik može jednom otvoriti svoj OpenID račun, upisati sve svoje podatke te potom na svakom mjestu gdje se želi autenticirati koristiti svoj OpenID račun. Pri tome, korisnik ima samo jedno korisničko ime i lozinku.

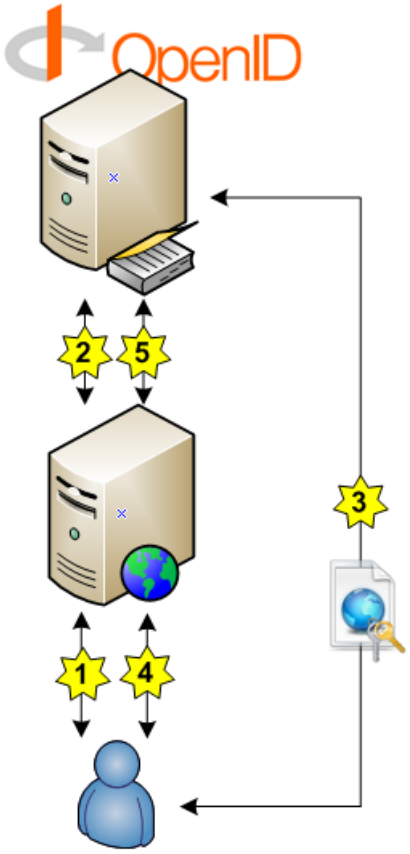
OpenID autentikacijski protokol svoje početke bilježi u svibnju 2005. godine kada ga je razvio Brad Fitzpatrick. Prvo web mjesto koje je pružilo podršku za OpenID je bio LiveJournal – popularno web mjesto za izradu blogova i vijesti čiji je autor također Brad. Od kraja 2006. godine počinje ubrzano prihvaćanje OpenID-a kao jednostavnog standarda za autentikaciju i upravljanje digitalnim identitetom, jedan od razloga za to je i članak na ZDNet portalu koji je promovirao OpenID.

U prvom mjesecu 2007. godine Symatec je objavio kako će podržati OpenID, a svega tjedan dana kasnije Microsoft, JanRain, Sxp i VeriSign objavili su kako će integrirati Windows CardSpace i OpenID. Kroz 2008. i 2009. godinu OpenID-u je iznimno narasla popularnost budući da su pružatelji OpenID usluga postali neki od najvećih web mjesta na internetu. Svakako treba istaknuti Yahoo, koji je implementirao OpenID 2008. godine. Potom su iste godine uslijedili Google, IBM, Microsoft. A 2009. godine Facebook i Paypal prihvatili su OpenID.

Slika 2.1 - Logotip OpenID-a

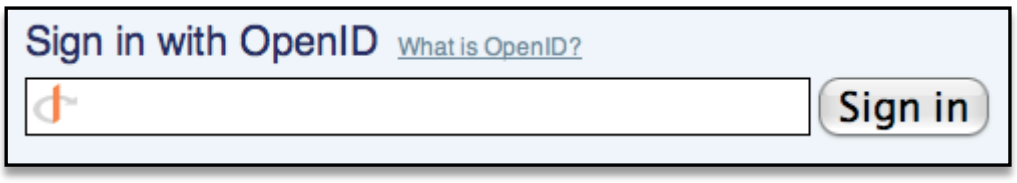
Važno je naglasiti da je OpenID decentralizirani sustav. Ne postoji centralna baza podataka koja sadrži podatke svakog korisnika koji ima OpenID račun. Zapravo, ne postoji niti jedna organizacija koja ima neograničeno pravo upravljanja OpenID računima. Kako se u tom slučaju korisnicima osigurava autnetikacija?

Odgovor leži u pružateljima OpenID usluga (eng. *OpenID provider*). Oni su osnovna komponenta sustava autentikacije i oni čuvaju podatke o OpenID računu: njegovu lozinku, korisničko ime, e-mail adresu itd. Decentraliziranost se postiže činjenicom da različite organizacije mogu biti pružatelji OpenID usluga. Sva web mjesta koja podržavaju prijavu korisnika kroz OpenID sustav autentikacije će od OpenID pružatelja usluga zatražiti provjeru identiteta. OpenID pružatelj usluga će potom web mjesto informirati o tome da li je provjera uspjela ili ne. Sljedeća slika prikazuje pojednostavljen način prijave na web mjesto putem OpenID sustava.



Slika 2.2 - Pojednostavljen prikaz autentikacije u OpenID sustavu

U **prvom koraku** korisnik dolazi na web mjesto na koje se želi prijaviti i traži prijavu putem OpenID sustava. Web mjesto koje svojim korisnicima želi omogućiti takav način prijave mora biti posebno prilagođeno. O potrebnim prilagodbama biti će više riječi kasnije, a za sada je dovoljno istaknuti da korisnik mora samo upisati svoje OpenID korisničko ime. Obično, na web mjestima koje podržavaju OpenID, polje za unos izgleda kako je prikazano na slici:



Slika 2.3 - Polje za unos OpenID korisničkog imena

Nakon što korisnik upiše svoje OpenID korisničko ime slijedi **drugi korak**. U tome koraku web mjesto prema korisničkom imenu određuje kojeg pružatelja OpenID usluga treba kontaktirati za nastavak autentikacije. Više riječ o izgledu korisničkog imena biti će u nastavku dokumenta. Kada je odredilo pružatelja usluga, web mjesto od njega traži da provjeri identitet navedenog korisničkog imena.

Proces autentikacije prelazi na **treći korak** u kojem se korisnik preusmjerava na svojeg pružatelja OpenID usluga koji će od njega tražiti lozinku kako bi utvrdio njegov identitet. Nakon autentikacije s OpenID pružateljem usluga, u **četvrtom koraku**, web preglednik korisnika obavještava izvorno web mjesto o tome da li je ona prošla uspješno ili ne.

Na kraju je nužan i **peti korak** u kojem izvorno web mjesto mora provjeriti s pružateljem OpenID usluge da li je stvarno autentikacija bila uspješna. Ova dodatna provjera postoji

budući da web mjesto ne može u potpunosti vjerovati pregledniku korisnika koji tvrdi da je autentikacija s pružateljem OpenID usluge bila uspješna. Ukoliko i ova provjera prođe, korisnik je uspješno autenticiran i prijavljen u željeno web mjesto.

Važno je istaknuti nekoliko ključnih točaka vezanih uz upravo opisani proces autentikacije:

- Izvorno web mjesto (ono na koje se korisnik želi prijaviti) niti u kojem trenutku ne može vidjeti lozinku korisnika.
- Korisnik se autenticira samo svojem OpenID pružatelju usluga gdje se nalaze podaci o njegovom korisničkom računu.
- Izvorno web mjesto vjeruje pružatelju OpenID usluga u uspješnost autentikacije.

3 Pružatelji OpenID usluga

Pružatelji OpenID usluga osnovna su komponenta cijelog sustava. Oni omogućuju provjeru identiteta i jednostavnu prijavu korisnika. Korisnik koji želi koristiti OpenID mora odabrati jednog od pružatelja OpenID usluga i kod njega registrirati svoj korisnički račun. Nakon toga, taj račun može koristiti za pristup bilo kojem web mjestu koji podržava OpenID identifikaciju. Trenutno postoji mnoštvo različitih pružatelja OpenID usluga. Neki od najpopularnijih su navedeni na sljedećim slikama.

Slika 3.1 - Popularni OpenID pružatelji usluga

Riječ je zapravo o poznatim servisima na internetu koji su samo uveli podršku za OpenID te se od tada njihova korisnička imena mogu koristit i unutar OpenID sustava autentikacije. Veliki broj korisnika interneta zapravo nije ni svjestan da ima OpenID korisničko ime. Npr. svatko tko koristi e-mail adresu na google-u isto korisničko ime može koristiti i kao OpenID. U tome slučaju Google je njegov pružatelj OpenID usluga.

Pružatelji OpenID usluga korisnicima daju njihov URL koji oni potom mogu koristiti za prijavu na web mjesta koja podržavaju OpenID. Različiti pružatelji usluga imaju različiti izgled URL-ova. Sljedeća tablica navodi primjer nekoliko pružatelja usluga i izgled URL-a za određeno korisničko ime:

Pružatelj usluge	Korisničko ime	OpenID URL
Google	pero	https://www.google.com/accounts/o8/id[1]
Yahoo	pero	me.yahoo.com[1]
MySpace	pero	myspace.com/pero
Blogger	pero	pero.blogger.com
WordPress	pero	pero.wordpress.com

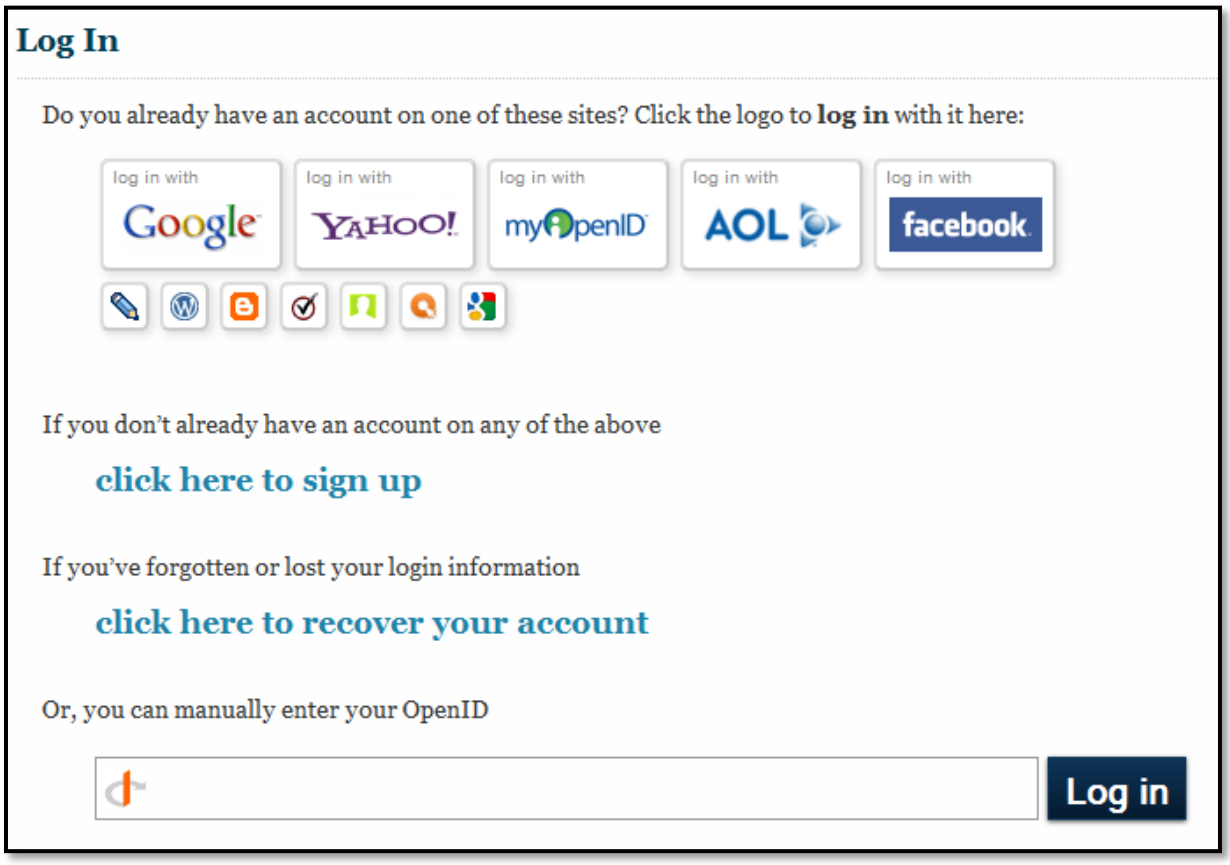
Navedene URL-ove svaki korisnik mora upisati kao svoje korisničko ime prilikom OpenID autentikacije, a sustav će automatski, prema URL-u, prepoznati kojeg pružatelja mora kontaktirati kako bi proveo autentikaciju.

Osim što URL sadrži informaciju o pružatelju usluga kojega je potrebno kontaktirati, on ima još jednu važnu ulogu. Naime, na tom URL-u pružatelj usluga postavlja OpenID servis koji implementira OpenID protokol i time zapravo omogućuje autentikaciju. Pružatelj usluge i izvorno web mjesto komuniciraju putem OpenID protokola kako bi uspješno proveli autentikaciju.

Mnoga izvorna web mjesta kada traže unos OpenID korisničkog imena olakšavaju posao korisnicima tako da već ponude gumbe s predefiniranim pružateljima usluga. U tome slučaju

[1] Google i Yahoo imaju isti URL za bilo koje korisničko ime

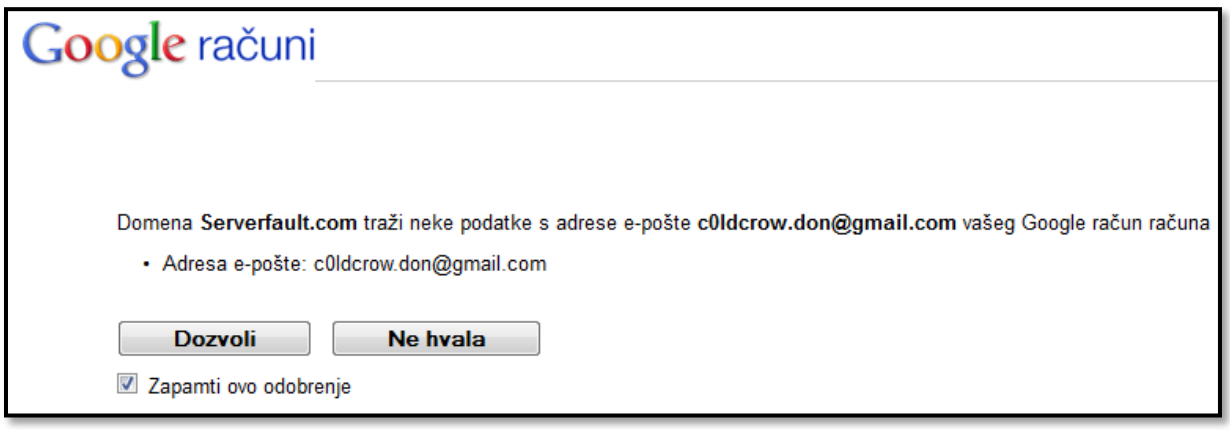
korisnik ne mora pamtiti svoj URL već autentikacija započinje klikom na gumb. Na sljedećoj slici prikazano je jedno izvorno mjesto koja korisnicima nudi tu opciju.



Slika 3.2 - Prikaz autentikacije OpenID sustavom

Kao što je već bilo navedeno pružatelj OpenID usluge sadrži sve podatke o korisničkom računu za kojega je zadužen. To uključuje njegovo pravo ime i prezime, e-mail adresu, kućnu adresu i sve ostalo što je korisnik upisao prilikom otvaranja svog korisničkog računa. Sve te podatke može zatražiti i izvorno web mjesto gdje se korisnik želi prijaviti.

Pružatelj OpenID usluge neće podatke predati izvornom web mjestu bez prethodnog odobrenja korisnika. Zapravo, tražiti će odobrenje korisnika da provede i autentikaciju. Sljedeća slika prikazuje Google koji kao OpenID pružatelj usluge traži odobrenje korisnika za provedbu autentikacije i pružanje osobnih podataka izvornom web mjestu.



Slika 3.3 - Prikaz upozorenja koje OpenID pružatelj usluga prikazuje korisniku

3.1 Kako postati OpenID pružatelj usluga?

S obzirom da je OpenID visoko decentralizirani protokol za autentikaciju, svako web mjesto može postati OpenID pružatelj usluge. Iako se na prvi pogled čini kako zbog težine implementacije OpenID-a pružatelji usluga mogu biti samo velika web mjesta istina je zapravo potpuno suprotna.

Svatko tko ima svoje web mjesto može relativno jednostavno postati OpenID pružatelj usluga. Time je omogućeno da korisnici imaju OpenID URL s vlastitim domenama, tj. da u potpunosti sami odrede izgled URL-a. Npr. ukoliko netko želi imati korisničko ime *ivan* a posjeduje web mjesto s nazivom *mojweb.com*, tada on lagano može izraditi OpenID URL oblika *ivan.mojweb.com*. Tri su osnovna načina kako jedno web mjesto može postati pružatelj OpenID usluga:

- Davanjem u najam OpenID funkcionalnosti. Ovaj način prikladan je za ona web mjesta koja nemaju resurse za implementaciju i konfiguraciju OpenID protokola. Riječ je o najjednostavnijem rješenju u kojem se implementacija, upravljanje i održavanje prebacuje na treću stranu.

- Korištenjem postojećih biblioteka. Ovo je prikladno za ona web mjesta koja se odluče na samostalno upravljanje i održavanje OpenID sustava, ali bez želje za razvojem programskog koda koji implementira sam protokol. Postoje brojna rješenja za različite programske platforme i okruženja. Neki od njih su:

    - mod_auth_openid kao modul za web poslužitelj Apache

    - DotNetOpenAuth je biblioteka za programski jezik C# i .NET razvojnu okolinu. Posebno je prilagođena ASP skriptnom jeziku.

    - JOpenID – biblioteka za programski jezik Java. Odlikuje je jednostavnost uporabe i mala veličina.

    - PHP OpenID Library – skup biblioteka ugrađenih u programski jezik PHP.

- Zadnja opcija za implementaciju podrške OpenID autentikaciji najsloženija je opcija i prikladna je onim web mjestima koja imaju dovoljno resursa. Naime, ovdje je riječ o potpunoj implementaciji OpenID protokola bez korištenja vanjskih biblioteka. Obično se ovaj pristup koristi kada je potrebno OpenID podršku dodati u neki već postojeći alat gdje nema mogućnosti korištenja gotovih biblioteka.

4 Impelentacija OpenID-a na strani izvornog web mjesta

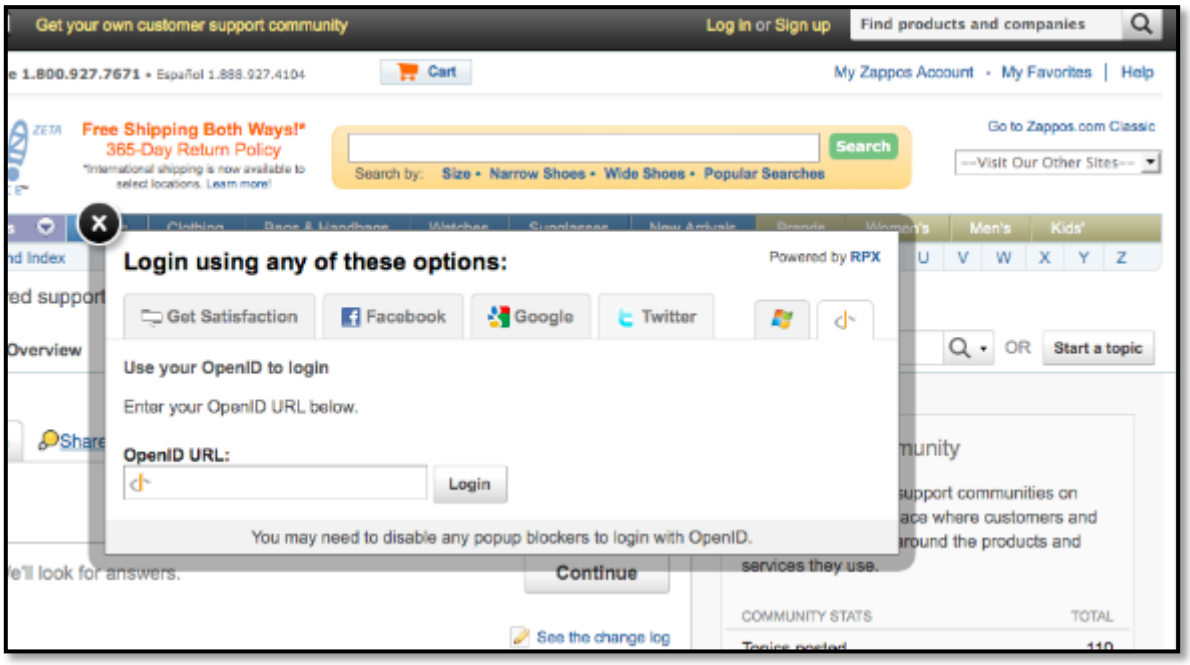
Do sada je bilo riječi o pružateljima OpenID usluga, no cijeli OpenID sustav ne bi mogao funkcionirati bez web mjesta koje omogućuju prijavu s OpenID korisničkim imenom. Takva web mjesta se unutar OpenID terminologije nazivaju i *OpenID consumers.* Termin ćemo prevesti kao *izvorno web mjesto* a ne *korisnik OpenID* usluge kako bi izbjegli nejasnoće budući da termin *korisnik* označava fizičku osobu koja se želi autenticirati.

Dakle, izvorno web mjesto je ono web mjesto koje korisnicima nudi određene usluga za koje je potrebna autentikacija. Ugradnja podrške za autentikaciju, slično kao i kod OpenID pružatelja usluga, svodi se na implementaciju OpenID protokola. Za izvorna web mjesta situacija je nešto jednostavnija budući da oni ne moraju provjeravati identitet korisnika već komuniciraju s pružateljima OpenID usluga.

Tehnička izvedba implementacije OpenID-a na izvornim web mjestima jednostavna je zahvaljujući velikom broju različitih programskih biblioteka, dodataka i okruženja koja već postoje i mogu se slobodno koristiti za izgradnju web stranica.

Tako postoje dodaci za popularne CMS sustave: Drupal, WebGUI, WordPress, MediaWiki, DokuWiki, phpBB… Za ona web mjesta koja ne koriste CMS sustave korisne mogu biti biblioteke predložene u prijašnjem poglavlju budući da one nude implementaciju OpenID mehanizma i na strani izvornog web mjesta i na strani pružatelja usluga. A najjednostavnija opcija u implementaciji je hosting paket koji već nudi ugrađenu podršku za OpenID.

Dobra praksa prilikom implementacije podrške za OpenID autentikaciju je korisnicima ponuditi jednostavan unos pružatelja usluga, tako da oni ne moraju pamtiti svoj OpenID URL. Primjer dobro izrađenog sučelja za autentikaciju dan je na sljedećoj slici:



Slika 4.1 – Primjer dobro dizajniranog sučelja za autentikaciju

Na poveznici *http://wiki.openid.net/w/page/25453698/Gallery* moguće je pronaći još mnoštvo primjera dizajna različitih stranica.

5 Prednosti i nedostaci OpenID-a

Kao i svaka druga tehnologija i OpenID ima svoje prednosti i nedostatke. OpenID nije zlatno rješenje svih problema s digitalnim identitetom, a nije ni još jedan nepotreban sustav autentikacije koji nikada neće zaživjeti. Osnovne prednosti OpenID sustava su:

- **Jednostavnije upravljanje digitalnim identitetom** – Korisnici često žele izgraditi jedinstveni identitet na internetu. Žele da ih jedno korisničko ime predstavlja na svim stranicama i da ne moraju održavati nekoliko različitih profila. Jedan od osnovnih ciljeva OpenID-a je olakšano upravljanja digitalnim identitetom.

- **Poboljšana razina sigurnosti** – Kada je u pitanju sigurnost uvijek je bolje imati manje različitih ulaznih vektora za napad. Jednostavnije rečeno – korisnik će lakše osigurati jedan identitet nego njih 10, 20 ili čak 50. Budući da OpenID nudi mogućnost korištenja samo jednog korisničkog imena i lozinke za sve usluge, dovoljno je zaštiti samo jednu lozinku i jednu kopiju privatnih podataka. Nema više jednakih i lako pamtljivih lozinki.

- **Decentraliziranost** – Kod OpenID-a korisnik sam može odabrati svojeg pružatelja usluga. Ne ovisi o jednom pružatelju i njegovoj politici privatnosti. OpenID je napravljen tako da omogućuje izbor kod kojeg pružatelja usluga želimo pohraniti podatke. Ukoliko se korisniku ne sviđa niti jedan pružatelj usluga, on može i sam izgraditi svoju podršku za OpenID i time biti neovisan od bilo koga.

- **Veliki broj korisnika već ima OpenID identitet** – Zahvaljujući velikim web mjestima koje su integrirale podršku za OpenID veliki broj korisnika Interneta već ima identitet unutar OpenID sustava. Njihov broj procjenjuje se na jednu milijardu.

Mane unutar OpenID sustava su:

- **Sigurnosni problem –** Činjenica da se sigurnost nalazi kao prednost i mana OpenID sustava govori o složenosti ovog pitanja. Iako je korisniku sada dovoljno zapamtiti jednu lozinku, on je izložen povećanoj mogućnosti provođenja phishing napada. Naime, potencijalni napadači mogu jednostavno postaviti zlonamjerno izvorno web mjesto, dopustiti prijavu s OpenID identitetom te potom korisnika preusmjeriti na lažiranu stranicu za njegovog pružatelja OpenID usluga.

- **Privatnost –** Budući da se OpenID temelji na korištenju jedinstvenog korisničkog imena za sva web mjesta na internetu, privatnost korisnika može biti dodatno ugrožena. Lakše je pratiti jednu fizičku osobu koja koristi isti digitalni identitet na različitim mjestima, nego fizičku osobu koja ima nekoliko različitih identiteta.

- **Nije prikladan za početnike –** OpenID sustav je još uvijek nerazumljiv običnim korisnicima Interneta. Razlog tomu je odmak od uobičajene prakse registracije na web mjestima koje posjećujemo. Potrebno je dodatno promovirati OpenID kako bi on zaživio među prosječnim korisnicima.

6 Zaključak

OpenID predstavlja jedno moguće rješenje za problem upravljanja digitalnim identitetom. No, kao i brojna druga sigurnosna rješenja OpenID nije savršen. Iako je korisnicima jednostavno upravljati samo jednim digitalnim identitetom, tj. jednom lozinkom i korisničkim imenom, mogu biti ranjiviji na phishing napade ili praćenje identiteta. Ne treba zaboraviti da usprkos činjenici kako na internetu postoji veliki broj OpenID identiteta relativno mali broj korisnika je upoznat s njime, a neki ga doživljavaju kao nespretnu i nejasnu tehnologiju. OpenID će i dalje rasti i razvijati se, a vrijeme će pokazati koliko je uspješan uistinu bio.