OpenID – jednotná digitálna identita v prostredí internetu

Už vás nebaví pamätať si heslá ku všetkým možným aplikáciám na internete či intranete, prípadne sa niekde registrovať len preto, že chcete zanechať komentár pod článkom, ktorý práve čítate? Nechcete, aby sa vaši zamestnanci počas dňa nespočetne veľakrát hlásili do rôznych vašich intranetových aplikácií, a chýba vám vhodný mechanizmus SSO (Single sign-on)? Práve pre vás je určené OpenID (*http://openid.net/*): jedno meno a heslo, jedna identita, pod ktorou môžete vystupovať v rôznych webových aplikáciách.

V súčasnosti sme svedkami rastúceho záujmu o nové technológie riešiace identity management. Tieto technológie vznikli na základe požiadaviek odlišných od tých, ktoré sa kladú na klasické „doménocentrické" podnikové systémy, určené na správu identít. Jednou z týchto nových technológií, ktoré v minulom roku zaznamenali najväčší rast popularity a adopcie, je OpenID (*http://openid.net/*).

OpenID vzišiel z prostredia open source komunity ako riešenie problémov, ktoré nebolo možné jednoducho odstrániť použitím iných technológií. Je to otvorený, decentralizovaný štandard pre identitu používateľa, umožňujúci prihlásenie sa do veľkého množstva webových aplikácií a služieb prostredníctvom tej istej digitálnej identity. Identita je vo forme URL (napr. *meno.myopenid.com*, *claimid.com/meno*) a je unikátna v tom, že používateľ sa autentifikuje pomocou jemu vlastného OpenID poskytovateľa. Autentifikáciu OpenID dnes používa a poskytuje celý rad webových portálov. Organizácie ako Google, AOL, Yahoo!, IBM, BBC alebo Orange plnia zároveň úlohu poskytovateľov.

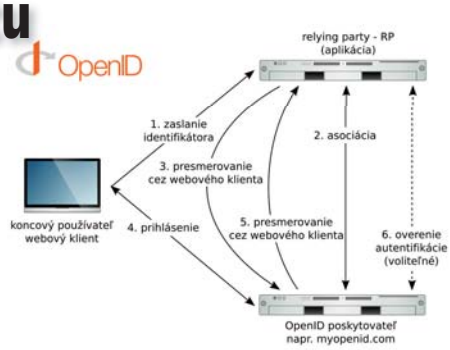
Prečo potrebuje svet práve OpenID, keď existujú iné technológie na identity management? Týmto dôvodom je skutočnosť, že táto technológia je fundamentálne odlišná od iných technológií minimálne v dvoch aspektoch:

1. OpenID je plne decentralizované na všetkých úrovniach protokolu, tak technickej, ako aj organizačnej.
   - Používatelia si môžu zvoliť ľubovoľného poskytovateľa OpenID na správu svojej identity alebo dokonca prevádzkovať svojho vlastného.
   - Poskytovatelia OpenID majú na výber z rôznych open source implementácií (*http://wiki.openid.net/Libraries*).
   - OpenID špecifikácie sa vyvíjajú v otvorenom procese, do ktorého môže hocikto prispieť.
   - Každý môže použiť svoje vlastné technické inovácie v rámci OpenID frameworku, aj keď kopírujú špecifikácie OpenID alebo im konkurujú.
2. OpenID má oveľa nižšiu ekonomickú a technickú náročnosť v porovnaní s inými alternatívami.

Princíp fungovania OpenID

Princíp mechanizmu autentifikácie OpenID je jednoduchý, prihlásenie prebieha podľa nasledujúcej schémy:

1. Používateľ navštívi stránku (v špecifikácii OpenID sa označuje ako relying party – RP), ktorá vyžaduje/podporuje autentifikáciu pomocou OpenID, a zadá adresu URL reprezentujúcu jeho OpenID (napr. *meno.myopenid.com*).



2. RP prevedie zadané OpenID URL do kanonickej formy (napr. *http://meno.myopenid.com/*) a pokúsi sa získať dokument z miesta, kam odkazuje. Tento dokument obsahuje adresu, kam presmerovať prehliadač na pokračovanie autentifikačného procesu. Nepovinným krokom pred presmerovaním je vytvorenie asociácie medzi RP a OpenID serverom.
3. RP presmeruje prehliadač na OpenID server.
4. Ak používateľ ešte nie je prihlásený u svojho poskytovateľa OpenID, autentifikuje sa voči nemu. Špecifikácia OpenID neurčuje, akou formou OpenID server autentifikuje používateľa. Najčastejší spôsob je použitie prihlasovacieho mena a hesla. Poskytovateľ OpenID môže použiť aj ľubovoľný iný spôsob, ako napríklad klientske certifikáty SSL, autentifikácia cez SMS, e-mail a pod.
5. OpenID server presmeruje prehliadač späť na RP.
6. RP overí prijaté informácie a prihlási používateľa.

Vďaka jednoduchému mechanizmu autentifikácie a dostatočnému počtu prevažne open source implementácií možno OpenID ľahko integrovať do ľubovoľnej webovej aplikácie.

OpenID v podnikových informačných systémoch

V súčasnosti absolútna väčšina veľkých spoločností má nejakým spôsobom riešený single sign-on (SSO), kde identita je centralizovaná a jediné prihlásenie do podnikovej siete získava prístup ku všetkým IT zdrojom a aplikáciám. No ako zamestnanci stále viac používajú aplikácie mimo firemnej siete, tradičné systémy na správu identít sa začínajú rúcať. V súčasnosti si musia používatelia vytvoriť nový účet na každej stránke veľmi podobne, ako si kedysi museli vytvárať nový účet pre každú podnikovú aplikáciu, kým sa neobjavilo riešenie SSO. Registrácia nových účtov je utrpením nielen pre zamestnancov, ale zrejme ešte viac pre IT administrátorov, ktorí musia spravovať tieto účty. Je zrejmé, že je potrebný bezpečný systém na SSO, ktorý funguje kdekoľvek.

Dôvodov, prečo prevádzkovať v rámci firemného informačného systému OpenID server ako alternatívu k tomu, aby si používatelia museli zakaždým vytvárať nové účty, je viacero:

1. **Vytváranie a odstraňovanie účtov:** Štandardne si používatelia musia vytvárať účet pre každú aplikáciu. Keď opustia organizáciu, môžu mať stále prístup k týmto účtom. OpenID môže byť integrovaná ako mechanizmus SSO s vaším existujúcim systémom na správu používateľov (LDAP, AD...) takým spôsobom, ktorý odstráni tieto problémy.
2. **Spôsob autentifikácie:** Keďže máte kontrolu nad OpenID serverom, máte kontrolu aj nad spôsobom autentifikácie, ktorú môžete realizovať rozlične, napríklad prihlasovacím menom/heslom, klientskymi certifikátmi SSL alebo hardvérovými a biometrickými tokenmi.
3. **Správa hesiel:** Aplikácie mimo vašej organizácie, ktoré majú kontrolu nad používateľovým účtom, nemusia mať dostatočne robustný systém na správu hesiel, čo kladie viac zodpovednosti na vašich zamestnancov. Ak kontrolujete autentifikáciu pomocou OpenID, môžete jednotne definovať pravidlá pre heslá. Súčasne je len jedno heslo, ktoré si používatelia musia pamätať.
4. **Firemná značka a menná konvencia:** OpenID používa URL ako používateľovu identitu, a preto môžete do nej zahrnúť meno vašej spoločnosti, ako napríklad meno.firma.sk. To umožňuje definovať množinu štandardných menných konvencií, ktorá je konzistentná v celej vašej organizácii, ako sú napríklad e-mailové adresy.

Vďaka OpenID bude môcť e-komercia, firemní alebo internetoví prevádzkovatelia webových aplikácií poskytovať svojim klientom lepšie služby. Zjednodušia registráciu používateľov, čo je v súčasnosti prekážkou hlavne pri získavaní nových zákazníkov. To umožní o nich nadobudnúť viac informácii a tým lepšie zamerať svoje ponuky pri súčasnej redukcii rizík spojených s krádežou identít a ochranou osobných údajov.

Vzhľadom na vlastnosti a možnosti, ktoré OpenID prináša, a podľa súčasných trendov penetrácie tejto technológie do oblasti IT je zrejmé, že OpenID ešte zohrá významnú úlohu na poli správy identít v prostredí webových aplikácií.

Klady:
- jednoduchý princíp
- decentralizovanosť
- protokol Single Sign On
- otvorený štandard
- postavené na existujúcich technológiách (DNS, HTTP, SSL/TLS, Diffie-Hellman)
- veľké množstvo implementácií pre rôzne platformy

Zápory:
- vyššia implementačná náročnosť
- vyššia zložitosť pre bežného používateľa
- náchylnosť na phishingové útoky

Zdroje:

http://openid.net/
http://en.wikipedia.org/wiki/OpenID
http://www.theserverside.com/tt/articles/article.tss?l=OpenID
http://www.computerworlduk.com/TOOLBOX/OPEN-SOURCE/blogs/index.cfm?entryid=252&blogid=14
http://blogs.zdnet.com/Hinchcliffe/?p=159
http://www.gnucitizen.org/blog/openid-provides-a-better-security-model/

PETER RYBÁR (Centaur, a. s.)
DANIEL BUCHTA (Centaur, a. s.)