Autentizační metody

Martin Komenda

Obsah

Terminologie

- **Autentizace** = ověření identity daného subjektu (jsem opravdu ten, za koho se vydávám), zajišťuje poskytovatel identit (IdP = Identity Provider).
- **Autorizace** = umožnění přístupu či souhlas s provedením konkrétní operace daným subjektem na základě autentizace (mám povolení k provádění daných operací, využívání daných služeb, přístupu k daným souborům, …), autorizační rozhodnutí provádí poskytovatel služeb (SP = Service Provider) na základě výsledku autentizace a dále na základě uživatelských atributů v případě úspěšné autentizace.

Autentizační metody

- ověřující uživatele (user-centric)
  - **OpenID**, Live ID, OpenAuth
- ověřující oprávnění a roli v instituci (institution-centric)
  - **Shibboleth**

User-centric autentizace

Založena na faktu, že uživatel má u někoho důvěryhodného založen účet, pomocí něhož se může přihlašovat i na jiných službách. Je vhodné, aby si sám uživatel mohl vybrat, kdo bude daným důvěryhodným subjektem (OpenID). Oproti tomu v jiných případech je důvěryhodným subjektem někdo pevně daný (Live ID, OpenAuth).

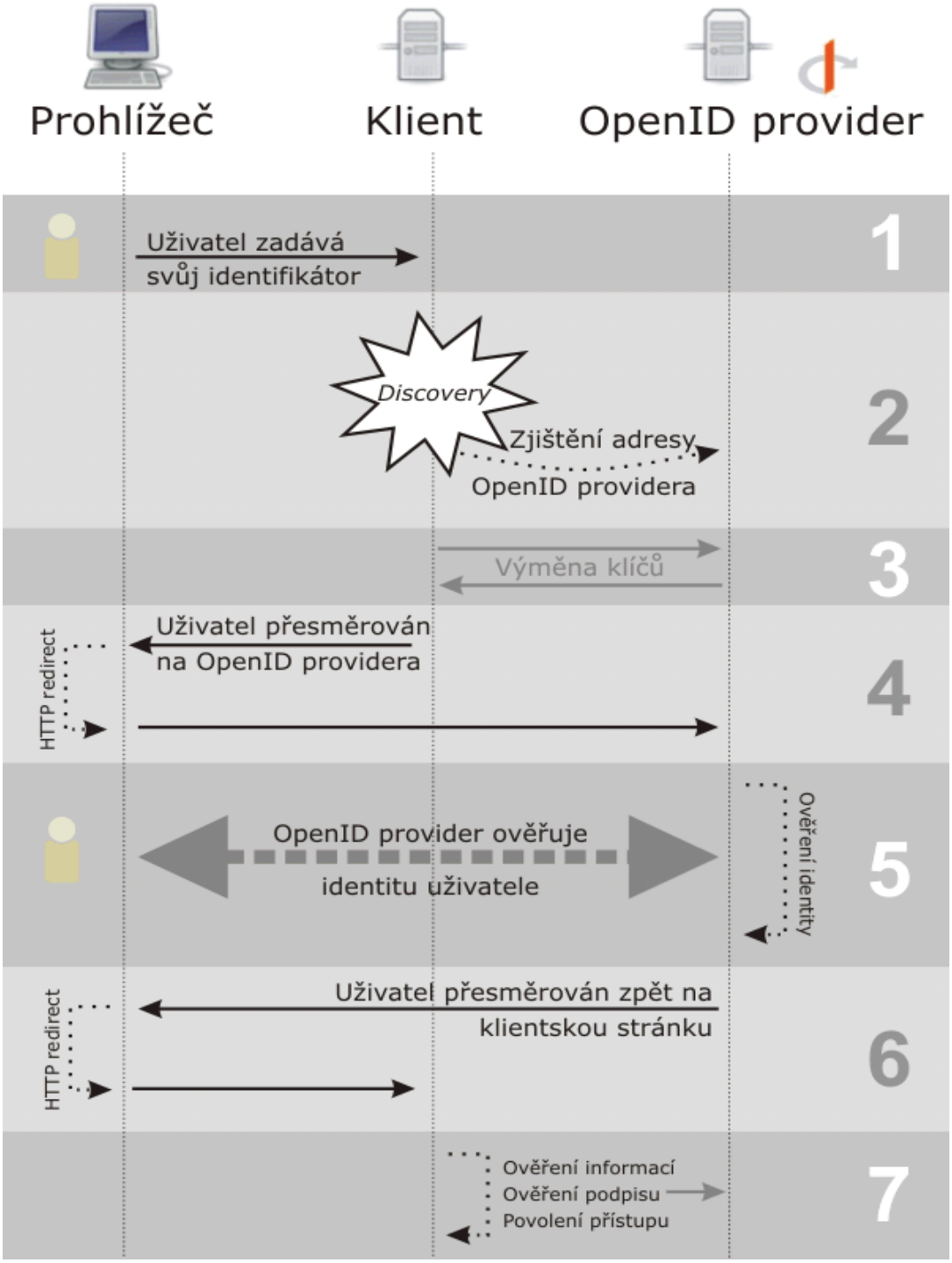
OpenID

OpenID je otevřený standard popisující decentralizovaný způsob autentizace uživatelů, který odstraňuje potřebu na straně provozovatele služby poskytovat a vyvíjet vlastní systémy pro autentizaci. Má tvar unikátního URL, ke kterému je přiřazeno heslo. Služba, která uživatelům autentizaci pomocí OpenID nabízí, při přihlašování uživatele přesměruje požadavek na ověření identity na správce daného OpenID účtu (tzv. Poskytovatel OpenID). Ten vrátí informaci o povolení či zamítnutí žádosti o autentizaci.

OpenID identity nejsou spravovány, na rozdíl od ostatních metod, jedním centrálním správcem, což dává uživateli značnou míru svobody při rozhodování, komu svěřit své údaje. Tento typ autentizace je v současné době poskytován a používán řadou portálů jako AOL, BBC, Google, IBM, MySpace, Orange, PayPal, VeriSign, LiveJournal, Yandex, Ustream and Yahoo! V České republice mezi přední zástupce patří portál Seznam.cz.

Standard OpenID nepředepisuje způsob, jakým je samotné ověření realizováno – pokud to bude ověření na základě spárování uživatelského jména a hesla, autentizace SMS kódem, elektronickým klíčem či biometrickými údaji, to záleží na poskytovateli OpenID. Jednotlivé identity nejsou spravovány jedním jediným centrálním správcem, ale hned několika, což uživatelům nabízí velkou svobodu.

Proces ověření pomocí OpenID



OpenID ověření probíhá v několika krocích, kdy spolu komunikují prohlížeč, poskytovatel a klient. Na začátku je požadavek od uživatele, který zadá svůj identifikátor (USID), na konci je informace o tom, zda se dotyčný uživatel tímto identifikátorem prokazuje oprávněně.

1. V prvním kroku uživatel - slovy specifikace - sdělí (pomocí prohlížeče) svůj identifikátor RP. Laicky (a míň šroubovaně) řečeno: Napíše svůj identifikátor do příslušného políčka ve formuláři na klientových stránkách a odešle.
2. Klient normalizuje (viz specifikace) dodaný identifikátor. Po jeho normalizaci se snaží získat adresu OP Endpointu zjišťovacím procesem (ve specifikaci nazývaný Discovery).
3. (Volitelný) Klient a poskytovatel si vytvoří tzv. přiřazení (Association, viz specifikace) – pomocí Diffie-Hellman algoritmu (RFC2631) si vymění klíč, kterým poskytovatel bude podepisovat odpovědi a klient ověřovat jejich pravost. Tento krok odstraňuje nutnost dalších dotazů na ověření podpisu při každém autentizačním požadavku či odpovědi.
4. Klient přesměruje uživatelův prohlížeč na stránky poskytovatele buď pomocí HTTP redirektu nebo JavaScriptem a v URL předá autentizační požadavek (viz specifikace).
5. Poskytovatel ověří, zda je uživatel oprávněn prokazovat se daným identifikátorem a zda si to opravdu přeje. Standardně OpenID nijak nepředepisuje způsob, jakým to má poskytovatel dělat – jestli ověří uživatele jménem a heslem, SMS kódem, elektronickým klíčem či biometrickými údaji, to záleží jen na něm. V budoucnu bude možné pomocí rozšíření PAPE požadovat vyšší nároky na ověření – např. požadovat vícenásobné potvrzení identity či požadovat, aby alespoň jeden způsob ověření byl fyzický (biometrické údaje, hardwarový klíč apod.) Specifikace PAPE je nyní ve stádiu návrhu a členové OpenID nadace o ní právě v těchto dnech hlasují.
6. Poskytovatel přesměruje uživatelův prohlížeč zpět na klientovy stránky a zároveň předá (v URL) informaci o tom, zda je autentizace potvrzena, nebo zda selhala.
7. Klient ověří informace předané Poskytovatelem: Zkontroluje návratové URL, informace o endpointu, zkontroluje nonce kód (unikátní kód požadavku) a ověří podpis, buď pomocí společného klíče, dohodnutého v kroku 3 (přiřazení klient-poskytovatel), nebo dodatečným dotazem na poskytovatele.

Google účet a OpenID

Postačí vložit do formulářového pole místo OpenID url https://www.google.com/accounts/o8/id a uživatel bude přesměrován na přihlášení přes google id.

OpenID software

- http://openiddirectory.com/openid-software-c-28.html

Institution-centric autentizace

Výhody federativní správy identit

- uživatel používá pouze jednotné přihlašovací jméno a heslo pro přístup k více aplikacím,
- správci jednotlivých aplikací neshromažďují přístupové údaje uživatelů,
- autentizace uživatele probíhá u domovské instituce,
- citlivé autentizační údaje uživatele neopouští domovskou síť,
- federační infrastruktura poskytuje snadný, standardizovaný a bezpečný způsob výměny informací o uživatelích,
- celé řešení je rozšiřitelné a škálovatelné,
- jednotné rozhraní pro připojení k federaci bez nutnosti implementovat rozhraní zvlášť pro každého poskytovatele služeb a obsahu,
- úrovně přístupu může řídit u svých uživatelů jak domovská instituce, tak i poskytovatel služby,
- autorizaci provádí vždy poskytovatel služby.

Federace jsou zakládány většinou na národních úrovních. V ČR jsou poskytovatelé zdrojů a identit organizováni například ve federaci **eduID.cz**, jejímž cílem je poskytnout svým členům rámec pro vzájemné využívání identit uživatelů při řízení přístupu k síťovým službám při respektování ochrany osobních údajů. Operátorem federace je CESNET, který koordinuje dění ve federaci a je vykonavatelem federační politiky. Zároveň se stará o běh federace jako celku – provádí registraci členů, poskytuje podporu, řeší bezpečnostní incidenty.

eduID.cz a technologie Shibboleth

Shibboleth řeší autentizaci i autorizaci, tedy nejen identitu, ale i oprávnění. Shibboleth je vázán na instituce a role jednotlivých uživatelů. Ve světě mimo instituce ztrácí svou zásadní výhodu a stává se z něj pouze těžkopádná autentizační metoda s mnoha nevýhodami – což poznáte v okamžiku, kdy z VŠ odejdete a váš Shibboleth účet skončí. Na rozdíl od OpenID ale v prostředí Shibboleth platí, že domovská organizace dodává poskytovatelům webových služeb garantované informace o uživatelích. Na základě toho poskytovatelé mohou provádět informovaná autorizační rozhodnutí, mohou nabídnout právě ty služby, ke kterým na základě licenčních smluv mezi organizací a poskytovatelem mají mít uživatelé přístup. Tento princip funguje velmi dobře napříč akademickým světem, nicméně v rovině uživatelů, kteří stojí mimo vybrané instituce, se jeví jako problematický.

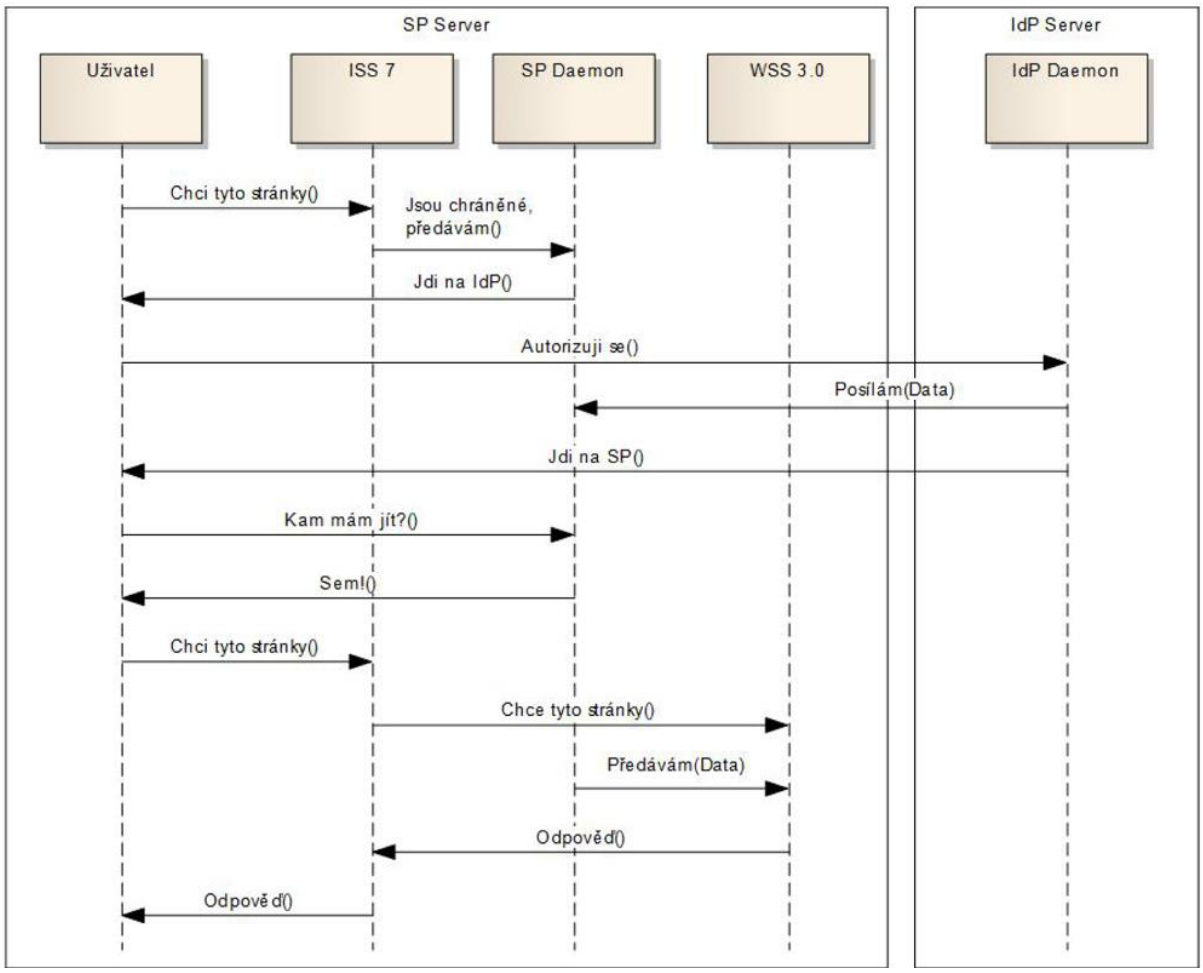
Shibboleth implementuje federativní infrastrukturu založenou na SAML (Security Assertion Markup Language) – XML standard určený k výměně autentizačních a autorizačních dat. V současné době jsou podporovány zejména webové aplikace (prostřednictvím internetového prohlížeče), protože Shibboleth využívá některé specifické rysy HTTP (Hypertext Transfer Protocol) protokolu.

Proces ověření pomocí Shibbolethu

1. Nepřihlášený uživatel chce využít služeb aplikace.
2. Uživatel je přesměrován ke správci identit jeho vlastní organizace k přihlášení.
3. Příslušný SP potřebuje uživatele ověřit a musí ho přesměrovat na přihlašovací stránku jeho domovské organizace.
4. Pokud SP nedisponuje mechanismy, jak zjistit domovskou organizaci uživatele, přesměruje ho na tzv. WAYF (Where Are You From) stránku, kde si může uživatel svou domovskou

organizaci zvolit. Služba WAYF poskytne uživateli seznam organizací a následně přesměruje webový prohlížeč uživatele na vybraného IdP v případě WAYF přístup (Shibboleth 1.x) nebo zpět na SP v případě Discovery Service přístupu (Shibboleth 2.x). Více o WAYF/DS, více o WAYF v eduID.cz.

5. Uživatel je pak přesměrován k přihlašovací stránce domovské organizace a může podstoupit autentizační proces.
6. Po úspěšné autentizaci je uživateli umožněno využít služeb příslušné aplikace.



Na Shibboleth infrastrukturu lze nahlížet jako na aplikační vrstvu mezi uživatelem a aplikací. Aplikace se nemusí zabývat autentizací, dostává pouze potřebné informace z infrastruktury. Tím se mimo jiné výrazně zjednodušuje vývoj aplikací podporujících Shibboleth.

Shibboleth IdP a SP

Shibboleth Identity Provider je aplikace napsaná v programovacím jazyce Java a je spouštěna jako servlet v nějakém aplikačním kontejneru, nejčastěji to bývá Apache Tomcat. Jako frontend je používán web server Apache, který přijímá spojení obsahující dotazy a předává je aplikačnímu kontejneru. Poskytuje dvě služby:

- autentizaci (vydává rozhodnutí o autentizaci v SAML)
- výdej atributů (pro potřeby autorizačních rozhodnutí, jinými slovy řečeno, jaká oprávnění může autentizovaný uživatel dostat/získat)

Shibboleth Service Provider je implementován jednak jako modul do web serveru a potom jako daemon (proces na pozadí), který běží samostatně. Modul zachytává HTTP dotazy a slouží jako rozhraní mezi web serverem a daemonem. Na základě konfigurace modul chrání určité adresáře nebo lokace. Pro přístup k těmto adresářům je potřeba splnit zadané podmínky (autentizace, autorizace na základě atributů). Poté modul předává chráněné aplikaci informace o identitě přistupujícího uživatele, příslušné atributy a také další informace, například z jakého správce identit uživatel pochází, jakou metodou se autentizoval apod.

SAML

Security Assertion Markup Language (SAML) je standard založený na XML poskytující mechanismus pro výměnu autentizačních a autorizačních dat mezi zúčastněnými stranami, tj. SP a IdP. V praxi řeší SAML problém jednotného přihlašování na více webů - Single Sign-On (SSO). Pokud chce uživatel přistupovat ke zdrojům SP, pak jeho identitu zkontroluje jeho IdP a ten posílá informace SP, u kterého uživatel žádá o poskytnutí služby. Tímto se odpovědnost za ověření identity přesunuje vždy na IdP. Tato koncepce vede k ustanovení tzv. federací, které si mohou navzájem vyměňovat informace o autentizaci subjektu. SAML poskytuje pouze distribuci samotné informace mezi zúčastněnými stranami, a proto nezáleží na jejím počtu. Standard nespecifikuje konkrétní implementaci samotného ověřování identity u poskytovatele identit.

Klíčovým principem SAML jsou, jak už název napovídá, tzv. tvrzení (assertions). Tvrzení jsou prohlášením důvěryhodné strany o někom jiném. Tato tvrzení jsou vydávána poskytovateli identit a zpracovávána poskytovateli služeb (v jazyce SAML jsou obě tyto federační role označovány jako entity). Tvrzení jsou deklaracemi pravd o uživatelích. Ve federačním prostředí jsou to tvrzení o identitě uživatele a jeho právech, přičemž mohou být velmi obecná, např. „Toto je náš zaměstnanec.“, uživatele pak nelze identifikovat nebo získat osobní údaje. Jednotliví poskytovatelé služeb nepotřebují mít přímý přístup k informacím o uživateli nebo uživateli přímo důvěřovat, musí důvěřovat jen zdroji tvrzení o uživateli.

Základem zprávy je tedy SAML tvrzení na jehož základě je prosazena důvěra na jiném serveru. V podstatě se jedná o XML dokument, který obsahuje bezpečnostní informace, které učinila tzv. identifikační autorita. Tvrzení neprovádějí autentizaci, ale slouží pouze k obalení, zapouzdření tohoto procesu autentizace.

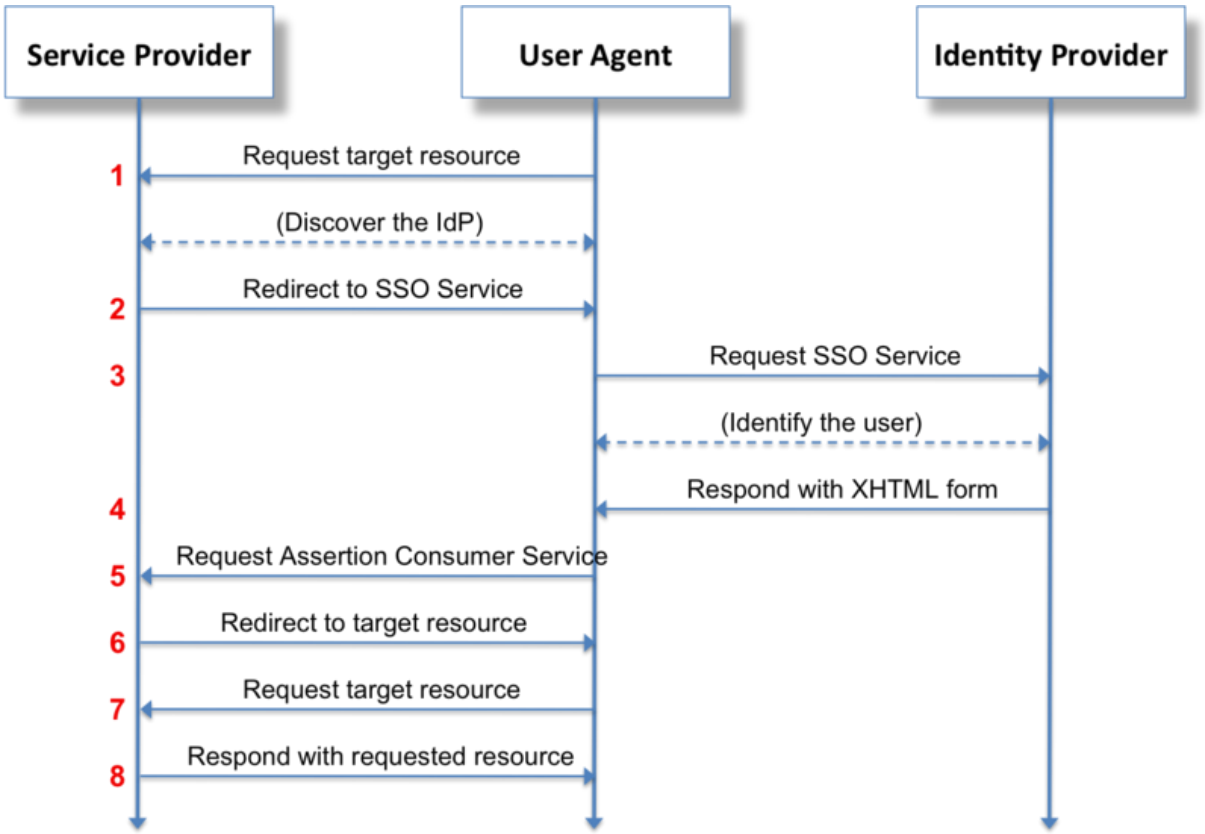
Každé tvrzení obsahuje:

- ID tvrzení, Subjekt jméno + bezpečnostní doména, Podmínky pro ověření tvrzení, Přídavné informace, Vydavatel tvrzení, podpis

Autorita může o subjektu prohlásit 4 druhy výroků:

- Autentizace - říká, že uvedený subjekt byl autentizován konkrétními prostředky M (jméno, heslo, lístek Kerberos, klíčem od XKMS aj.) v konkrétním čase T. Toto tvrzení je reprezentováno elementem <AuthenticationStatement> a typicky ho vydává tzv. identity provider (SAML autorita). Autentizace se používá z důvodů zavedení SSO.
- Atribut - Tvrzení, že uvedený subjekt je svázán s atributy A, B a tedy s odpovídajícími hodnotami a, b atd. Výrok atribut je použitelný pro distribuovanou transakci a autorizační službu.
- Autorizace - Žádost o povolení přístupu typu A (číst, psát, mazat) uvedeného subjektu k uvedeným zdrojům R (webové zdroje) byla povolena nebo zamítnuta. O tomto rozhoduje vydávající autorita. Rozhoduje o tom na základě přítomnosti evidence E žádající strany. Zdroj R může být webová služba nebo webová stránka. Toto tvrzení je reprezentováno elementem <AuthorizationDecisionStatement>.

SAML tvrzení (assertion)



Single Sign-On

Single Sign-On (SSO) [21] je metoda řízení přístupu, která umožňuje uživatelům přistupovat k více zdrojům za pomocí jediných přihlašovacích údajů. Principem je se v rámci sezení autentizovat jen u prvního zdroje a poté k ostatním zdrojům volně přistupovat. Toho lze dosáhnout jednoduše např. za pomoci cookie u intranetových aplikací nebo u více aplikací spadajících pod jednu organizaci,

problém nastává v momentě rozšíření SSO pro extranet nebo na více serverů mezi více aplikací (organizací).

Řešením pak může být dohoda o používání jednotné implementace SSO všemi aplikacemi. Tato dohoda ovšem může vést ke složitým a pracným změnám ve správě uživatelů u jednotlivých organizací. Dalšími možnými řešeními jsou centralizace správy uživatelů všech organizací do jedné databáze, což může být nepraktické z hlediska soukromí uživatelů, nebo organizace zapojit do federace identit. Cílem SSO je zredukovat počet přihlašovacích údajů k různým systémům, které si uživatel musí pamatovat.

Uživatel se přihlásí na serveru A, je zde autentizován. Později se chce přihlásit na server B. Bez užití SSO by musel své údaje zadávat znovu. Pokud je užit SAML, pak B pošle požadavek na A s dotazem, zda se již uživatel na A autentizoval. A odpoví prohlášením, že uživatel je autentizován. Poté B zpřístupňuje své zdroje, aniž by vyžadoval znovu přihlašovací údaje. Nejčastější řešení SSO je pomocí tzv. poskytovatele identity a poskytovatele služeb.

Použití v praxi

Federativní autentizaci využívají velké biomedicínské databáze na platformách např.:

- OvidSP,
- EBSCOhost,
- Elsevier Science Direct a Scopus,
- MEFANET,
- Atlases.

Moje ID

Služba dostupná http://www.mojeid.cz/

	OpenID	mojeID
založení a užívání identity zdarma	✓	✓
výběr uživatelských údajů, které se přenáší	✓	✓
přístup postytovatelů k databázi identit zdarma	✓	✓
moduly pro implementaci do open source platforem	✓	✓
ověření existence uživatele		✓
možnost plné ověření totožnosti uživatele		✓
omezení zakládání duplicitních identit		✓
české uživatelské prostředí		✓
česká technická podpora (telefon, mail)		✓
více metod autentizace uživatele		✓
doplňkové služby k identitě (přístup k registru domén)		✓
jednotná struktura dat v profilu uživatele		✓
doplňkové údaje v uživatelském profilu (18+, student,...)		✓

Zdroje

[1] Slabý, Kryštof. Výhody federativní autentizace z pohledu uživatele biomedicínských informačních zdrojů. http://creativeconnections.cz/medsoft/2011/Medsoft_2011_Slab%C3%BD_Kry%C5%A1tof.pdf

[2] Duda, Martin. Federativní autentizační a autorizační infrastruktura Shibboleth v KNAV. http://www.lib.cas.cz/casopis-informace/federativni-autentizacni-a-autorizacni-infrastruktura-shibboleth-v-knav/

[3] SWITCH - WAYF Service. http://www.switch.ch/aai/support/tools/wayf.html

[4] Oficiální web federace eduID.cz. http://www.eduid.cz/

[5] Security Assertion Markup Language. http://cs.wikipedia.org/wiki/Security_Assertion_Markup_Language

[6] OpenID: Historie, terminologie a mechanismus autentizace. http://www.zdrojak.cz/clanky/openid-historie-terminologie-autentizace/

[7] Moderní internetové autentizační metody. http://www.zdrojak.cz/clanky/moderni-internetove-autentizacni-metody/

[8] Porovnání moderních autentizačních metod. http://www.zdrojak.cz/clanky/porovnani-modernich-autentizacnich-metod/

[9] Oficiální web OpenID. http://openid.net/

[10] Řekni Shibboleth :-) webové jednotné přihlašování nejen pro vzdálený přístup v knihovnách. http://knihovna.nkp.cz/knihovna91/pavlik.htm

[11] Aplikace pro sběr metadat ve federaci identit. http://is.muni.cz/th/172704/fi_b/bc-print.pdf

[12] Shibboleth - identifikujte se jen jednou: http://www.lupa.cz/clanky/shibboleth/