MUNI
ICS

Správa identit a řízení přístupu na Masarykově univerzitě

Verze 1.0

Adrián Rošinec, Slávek Licehammer
24.8.2020

Ústav výpočetní techniky
Masarykova univerzita
Šumavská 416/15, 602 00 Brno, Česká republika
T: +420 549 49 2100, E: it@muni.cz, W: www.muni.cz, www.ics.muni.cz

Záznam změn

Dátum	Verze	Změna	Autor
2020/08/24		Prví pracovní verze	Adrián Rošinec
2020/10/12	1.0.0	Revidovaná první verze	Adrián Rošinec, Slávek Licehammer
2020/10/13	1.0.1	Změny formátování + řešení zjištěných problémů	Adrián Rošinec
2020/10/13	1.0.2	Změna emailu pro kontakt na it@muni.cz	Adrián Rošinec

Obsah

1. Základy správy identit a řízení přístupu na MU

Kapitola popisuje aplikaci základních pojmů důležitých pro správu identit a řízení přístupu v prostředí Masarykovy Univerzity.

1.1. Uživatelé

Každá osoba se vztahem k univerzitě má záznam v systému pro správu identit a řízení přístupu (IAM systém), který slouží pro autentizaci a autorizaci uživatelů k IT zdrojům. Na univerzitě rozeznáváme dva typy uživatelů. Dělí se na základě zdroje identity a podle funkce účtů (sponzorovaný, servisní účet). Uživatel může být reprezentován několika identitami (viz. External identity). v současnosti se primárně využívá UČO ve spojení s primárním a sekundárním heslem.

1.1.1. Interní uživatelé

Vznik interní identity je podmíněn aktivním závazkem vůči univerzitě. Standardně jde o zaměstnance a studenty, ale patří sem například i emeritní profesoři. Tito uživatelé se do systému pro správu identit a řízení přístupu synchronizují primárně ze studijní agendy IS MU a ekonomického systému INET MU.

1.1.2. Sponzorované účty

V případě, že uživatel nemá aktivní závazek vůči univerzitě, ale přesto má mít možnost využívat IT zdroje univerzity, IAM systém rozpoznává tzv. sponzorované uživatele (účty). Díky sponzorovaným účtům získává osoba interní identitu, aniž by taková osoba vznikla v primárním zdroji identit (IS / INET). Tuto osobu sponzor zná (dokáže ji kontaktovat) a ví, za jakým účelem sponzorství vydal (například ví, že jde o účastníka konference). Z tohoto titulu je možné definovat i dobu platnosti, po kterou daný účet zůstává aktivní. V kontextu řízení přístupu se sponzorovaný účet neliší od interních uživatelských účtů.

Sponzorovat je možné i účet s aktivním vztahem k univerzitě. Takový účet po skončení vztahu k univerzitě zůstane použitelný pro autentizaci nebo autorizaci k vybraným službám. Sponzorem může být jakýkoliv zaměstnanec Masarykovy Univerzity a účet může mít i několika sponzorů současně.

Koncept sponzorovaných účtů nám na umožňuje lépe řešit situace vůči osobám, které na univerzitu přicházejí nebo z ní odcházejí (například prodloužením přístupu k nějakému zdroji). Sponzorované účty nahrazují pojmy **Guest a Guest Manager**, které **byly zrušeny 1.11.2020**.

Sponzorování účtů je možné provádět zaměstnanci MU v uživatelském rozhraní systému pro správu identit a řízení přístupu Perun na adrese: https://perun.aai.muni.cz.

> ***Příklad 1: Návštěvník konference***
>
> *Typický příklad sponzorování účtů jsou účty pro návštěvníky konferencí, které pořádají zaměstnanci MU.*
>
> *Vytvoří sponzorované účty a přidají je do skupin, které řídí přístup* například *k wifi síti. Obdobně je možné přidat sponzorovanému účtu jakékoli přístupy ke službám, které daný sponzor může v té době přidělovat konceptem členství ve skupinách.*
>
> *Přístupy se automaticky odeberou* na základě expirace nastavené na *konec dané konference.*

> ***Příklad 2: Přicházející zaměstnanec***
>
> *Sponzorovaný účet je možné využít i v případě příchodu nového zaměstnance do oddělení. Kolegovi lze efektivně zajistit přístupy* například *k dokumentaci ještě před tím, než ho zaregistruje ekonomický systém INET jako aktivního uživatele.*

1.1.3. Externí identity

V budoucnu plánujeme ověření identity celou řadou běžně využívaných a důvěryhodných poskytovatelů identit. Mezi ně patří například eID, eduID.cz, eduGAIN, Google, Microsoft, Apple, ... Takto ověřený uživatel dostane automaticky účet bez jakýchkoliv přístupů - podobně jako sponzorovaný účet. Práva tomuto účtu musí nastavit pravomocný sponzor (zaměstnanec MU). Externí identitu lze propojit s interní identitou a zde využívat k přihlášení do služeb.

V současnosti neexistuje možnost ověřovat svoji identitu externím poskytovatelem identit.

1.1.4. Servisní identita

Servisní identita nereprezentuje fyzickou osobu ale vzniká pro účel převážně strojového přístupu (machine-to-machine) a využívá koncept sponzorovaného účtu.

> ***Příklad:***
>
> *Databázový účet pro webovou aplikaci.*

1.2. Skupiny

Skupiny seskupují uživatele, resp. osoby a jsou klíčovým mechanismem řízení přístupu uživatelů k různým IT zdrojům. Skupiny má právo zakládat jakýkoliv aktivní uživatel. Skupina samotná nemá v systému pro řízení přístupů žádný význam - svoji funkci získává až v momentě přiřazení na zdroj (resource), kde skupina reprezentuje přístup uživatelů k němu. Členy skupiny jsou libovolní uživatelé (zaměstnanci, studenti, sponzorované, či servisní účty).

1.2.1. Synchronizované skupiny

Skupiny mohou být plněné také pomocí synchronizace ze skupin z externích systémů, například z IS MU nebo INET. Synchronizaci skupin nastavuje uživatelská podpora systému Perun - požádat o aktivaci je možné na adrese it@muni.cz. Standardně nebude synchronizovaná skupina spravována samotným žadatelem - skupina bude vložena do jiné skupiny (viz. Skládání skupin), kterou žadatel vlastní a tudíž ji může spravovat. Bez uživatelské podpory lze využívat skupiny jednotlivých pracovišť, studentů a doktorandů na fakultách (tyto skupiny mohou využít jen zaměstnanci MU). Další typy synchronizovaných skupin (například studenti konkrétního předmětu) jsou řešeny synchronizací z IS MU.

1.2.2. Skládání skupin

Skupinu lze vložit do jiné skupiny, čímž se členové vkládané skupiny stanou zároveň členy cílové skupiny. Tímto způsobem je možné vytvořit skupinu, jejíž členové skládají z jiných skupin bez zbytečného duplicitního definování skupin.

1.2.3. Správce skupiny

Každá skupina má správce, který tyto členy spravuje (přidává a odebírá členy skupiny). Správce je definován výčtem uživatelů nebo celou vybranou skupinou v systému Perun (například celé pracoviště).

1.2.4. Podskupiny

Samotné skupiny mohou obsahovat podskupiny. Toto členění je výhodně v případě reprezentace hierarchických organizačních struktur. Člen každé podskupiny je automaticky členem její nadskupiny.

> ***Příklad: Archeologičtí nadšenci*** *(Ilustrativní příklad)*
>
> *Existuje tým, který reprezentuje skupinu nadšenců archeologie. Tento tým osob, nebo jeho reprezentace ve světě řízení přístupů – skupina, se skládá z:*
>
> *automatické skupiny pracoviště geologie na přírodovědecké fakultě,*
>
> *skupiny ručně přidávaných studentů a kolegů z jiných pracovišť MU.*
>
> *Takto definovaná skupina je v zápětí použitelná v mnoha IT zdrojích:*
>
> *týmová dokumentace*
>
> *fyzický přístup do skladu s nálezy (čtečka karet),*
>
> *přístup pro přihlášení do online databáze archeologických nálezů*
>
> *skupina v O365 / Team*
>
> *...*

1.3. Zdroje

Zdroje (resources) jsou v kontextu řízení přístupu vnímány jako flexibilní jednotka reprezentující přístup k využití služby nebo její části. Technický správce služby vytváří zdroj reprezentující službu, definuje jeho význam a deleguje jeho správu na administrativního vlastníka. Sémantiku, tj. co konkrétní zdroj v kontextu dané služby reprezentuje, definuje a popisuje technický správce. Tento popis lze nalézt v technické dokumentaci dané služby.

Pod zdrojem je možné si například představit:

- přístup ke konkrétní webové stránce na službě "správa webů",
- roli uživatele - například "editor", "admin", ... na konkrétní službě,
- oprávnění - "read", "write" na konkrétní službě.

Může jít i o různou kombinaci těchto významů.

Administrativní správce opravňuje skupiny uživatelů dané zdroje využívat tím, že je na tyto zdroje přiřazuje. Může jít o skupiny, které sám vlastní (čím přímo spravuje přístup pro jednotlivé uživatele) nebo o již existující skupiny, které vlastní jiní uživatelé (např. existující skupina pro výzkumný tým). Kromě toho technický nebo administrativní správce deleguje nad daným zdrojem roli "self-service", která opravňuje jiné uživatele přidávat skupiny a odebírat jen jimi přidané skupiny na daném zdroji. Díky roli "self-service" lze nechat řídit přístup více uživatelů bez vzájemného ovlivňování.

Cílem delegování správy zdrojů je, aby uživatel, který rozhoduje o přístupech (administrativní správce), mohl přístupy nastavit, přičemž by se technický správce mohl prioritně věnovat technickým aspektům služby a nemusel řešit jednotlivé přístupy. Roli technického a administrativního správce může zastávat tatáž osoba.

2. Další klíčové funkce řízení přístupů

2.1. Autentizace

ÚVT zajišťuje služby autentizace uživatelů Jednotným přihlášením MU. Podporované protokoly jsou OpenID Connect a SAML2.0. Registraci služby do Jednotného přihlášení MU je možné provést v registračním portálu (https://spreg.aai.muni.cz). Po odeslání registrace začne manuální schvalovací proces administrátorem autentizační brány.

Více informací o službě Jednotného přihlášení MU a technická specifikace je dostupná na https://it.muni.cz/sluzby/jednotne-prihlaseni-na-muni.

Pro aplikace, které technicky nepodporují autentizaci uživatelů s využitím Jednotného přihlášení MU, poskytneme alternativní způsob autentizace. V takovém případě prosím kontaktujte uživatelskou podporu na adrese idm@ics.muni.cz. Součástí žádosti by mělo být odůvodnění proč není možné využít Jednotné přihlášení MU.

2.2. Provisioning

V některých případech aplikace požadují informace o uživatelích ještě před tím, než s ní začnou pracovat - standardně před jeho prvním přihlášením. Systém Perun podporuje distribuci uživatelských dat a informace o skupinách do různých aplikací a zajišťuje tak přístup pouze autorizovaným osobám.

Aby bylo možné distribuovat data o uživatelích, je nutné specifikovat potřebné informace, které služba vyžaduje. Na straně příjemce těchto dat je nutné tato data zpracovat způsobem typickým pro danou aplikaci (např. přenášení těchto dat do databáze aplikace). Systém Perun posílá data ve strojově zpracovatelných formátech, typicky: LDIF, JSON nebo CSV.

Aktuální seznam podporovaných konektorů k aplikacím je možné nalézt zde (dle platformy):

- Linux: https://github.com/CESNET/perun-services/tree/master/gen,
- Windows: https://github.com/CESNET/perun-services-windows/tree/master/services.

V případě zájmu o využití této možnosti nás prosím kontaktujte na adrese idm@ics.muni.cz.

> ***Příklad:***
>
> *Uživatelský účet na unix-based systémech - musí existovat dříve než se uživatel přihlásí.*

2.3. De-provisioning

De-provisioning je důležitou součástí řízení životního cyklu uživatele, při kterém jsou uživateli při ztrátě členství ve skupině odebírány jednotlivé zdroje na které měl nárok díky členství ve zmíněné skupině (např. přístup do místnosti čipovou kartou). Je to přímý opak provisioningu a v praxi se nejčastěji odehrává při změně pracovní pozice, odchodu zaměstnance či odchodu studenta z prostředí univerzity.

Technicky není nad rámec správně fungujícího procesu provisioningu nutná žádná další konfigurace. V případě, že systém Perun nepošle do zdroje daného uživatele, znamená to, že uživatel nemá mít ke zdroji přístup (t.j. služba by mu měla deaktivovat případně smazat z interní databáze).

> ***Příklad:***
>
> *Při odchodu zaměstnance automatizovaně řešíme odebírání přiřazených licencí, přístupů ...*

2.4. Grace period

Koncept který dovoluje řešit opožděné zrušení členství ve skupině. Zpoždění je možné definovat v řádech několika dní. Jeho využití můžeme hledat primárně u služeb, kde po skončení platnosti členství chceme nějaký čas počkat, než se uživateli přístup ke službě odstraní.

> ***Příklad:***
>
> *Opožděné odebrání přístupu k* osobnímu úložišti dat, kdy uživatel dostává více času aby si stáhl vše potřebné. Je možné po dobu grace periody nastavit o omezení práv. V tomto konkrétním případě by šlo omezit přístup pouze na čtení.

3. Základní pojmy

V kontextu správy identit a řízení přístupů na Masarykově Univerzitě rozeznáváme následující pojmy.

3.1. Osoba

Fyzická osoba, která může přistupovat ke službám.

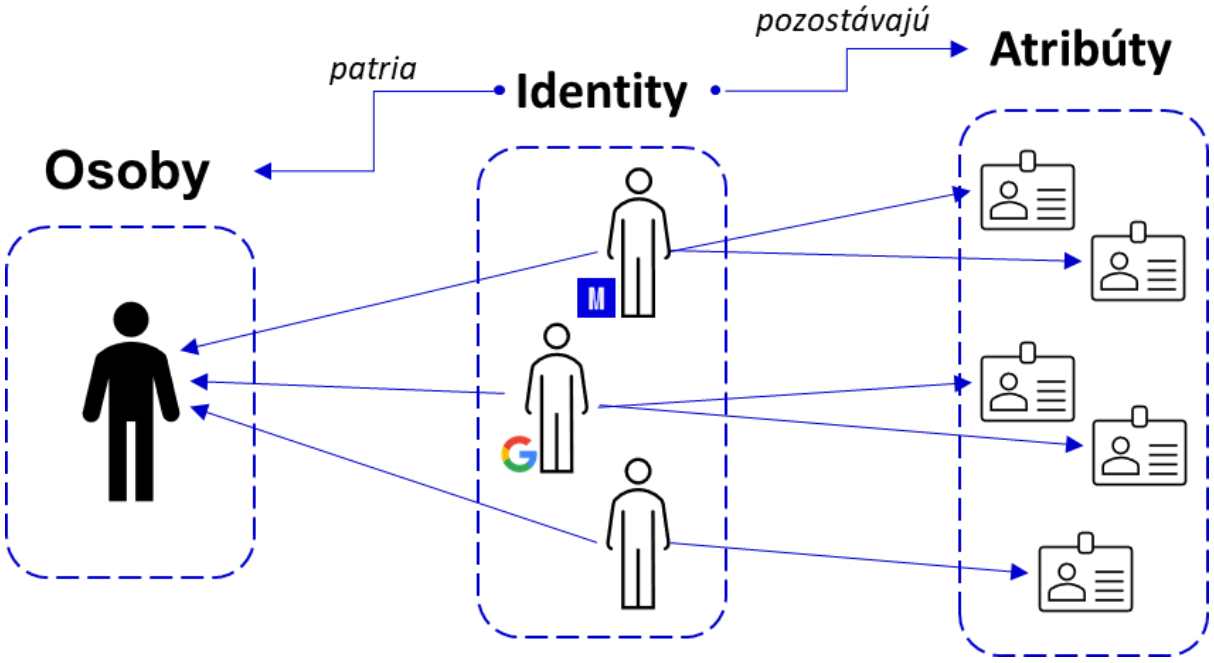
3.2. Identita

Množina atributů, které souvisí s osobou, na základě které je možné určit o jakou osobu jde. Jde o digitální reprezentaci osoby.

3.3. Uživatel

Osoba mající záznam v IAM systému.

3.4. Správa identit



3.5. Služba

Službou v kontextu řízení přístupu rozumíme jakoukoli aplikaci, která vyžaduje přístup uživatelů.

3.6. Technický správce služby

Osoba zodpovědná za technický provoz služby.

3.7. Administrativní správce služby

Osoba zodpovědná za řízení přístupu ke službě.

3.8. Uživatel s rolí self-service pro službu

Osoba s právem řídit oprávnění přístupu ní spravovaných skupin ke službě, pro kterou má roli self-service.

3.9. Identita

Datový identifikátor jednoznačně určující osobu/službu/zařízení.

- Interní identita
  - Identita ověřené osoby v IdM systémech MU.
- Externí identita
  - Identita osoby spravovaná v jiném systému než v IdM systémech MU.
- Servisní identita
  - Identita reprezentující službu nebo zařízení, jsou k ní odpovědné osoby.

3.10. Autentizační údaje (credentials)

Údaje použitelné pro prokázání identity, např. jméno a heslo nebo osobní certifikát.

- Autentizace “Primární heslo”
  - Autentizace pomocí hesla, které se používá v rámci MU k vybraným systémům s vysokou důležitostí. V budoucnu může být použit jiný autentizačních mechanismus.
- Autentizace “Sekundární heslo”
  - Autentizace heslem, používá se k ostatním systémům, které nejsou pokryty primárním heslem. V budoucnu může být použit jiný autentizační mechanismus.
- Autentizace alternativními hesly
  - Umožňují přístup k vybraným službám, které jsou přístupné přes sekundární heslo. Princip alternativních hesel spočívá ve vytvoření hesla pro každé zařízení přistupující ke službě. Všechna alternativní hesla jsou si z pohledu přístupu ke službám rovna. Alternativní heslo má omezené pravomoci pro správu účtu osoby z důvodu bezpečnosti (např. nelze jim měnit sekundární heslo).
- Externí autentizace
  - Identita je autentizována důvěryhodným systém mimo MU.

3.11. Skupina

Seskupení osob.

3.12. Správa přístupu

— Definice, která identita má mít na danou službu přístup.

— Správa přístupu je několika úrovňová.

— Základní řízení přístupu: IAM systém poskytuje seznam uživatelů oprávněných využívat danou službu společně s dalšími atributy uživatelů, včetně informace o členství ve skupinách.

— Rozšířené řízení přístupu: další rozdělení práv uvnitř služby (fine-grained authorization) je prováděno na základě výše zmíněných informací z IAM systému.

3.13. Ban

Omezení přístupu konkrétního uživatele na danou službu nebo její část. Ban je vždy časově omezen a důvod banu musí být popsán.