Způsoby autentizace uživatelů v informačních bezpečnostních systémech

Methods of user authentication in information security systems

Jana Fuková

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jana FUKOVÁ**
Osobní číslo:	**A09773**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Způsoby autentizace uživatelů v informačních bezpečnostních systémech**

Zásady pro vypracování:

1. **Seznamte se s problematikou nedostatečné úrovně autentizačních metod uživatelů výpočetní techniky v informačních bezpečnostních systémech.**
2. **Charakterizujte nejznámější metody procesu autentizace.**
3. **Objasněte pojem pro strategii postupů, procesů a informací k identifikaci identity systému Identity Management.**
4. **Implementujte systém Identity Management v praxi a popište jeho přínosy .**
5. **Verifikujte stav aplikací po implementaci Identity manageru v jednotné správě identit.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MATYÁŠ, Vašek a Jan KRHOVJÁK. Autentizace uživatelů a autorizace elektronických transakcí: příručka managera. Praha: Tate International, 2007, 318 s. Příručka manažera, 8. ISBN 978-808-6813-141.**
2. **BÜCKER, Axel. Identity management design guide with IBM Tivoli identity manager. 1st ed. Austin, Tex.: IBM International Technical Support Organization, 2003, 414 s. IBM redbooks. ISBN 07-384-5332-3.**
3. **BÜCKER, Axel. Enterprise security architecture using IBM Tivoli security solutions. 2nd ed. San Jose, Calif.: IBM, International Technical Support Organization, 2004, 660 s. ISBN 07-384-9897-1.**
4. **DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-802-5126-196.**
5. **MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. Kriminalistika. 2., přeprac. a dopl.vyd. Praha: C. H. Beck, 2004, 606 s. ISBN 80-717-9878-9.**

Vedoucí bakalářské práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Předložená bakalářská práce se zabývá způsoby autentizace v informačních systémech, jako jsou jméno a heslo, certifikát vydaný veřejným poskytovatelem certifikačních služeb, jednorázové heslo a biometrie. V rámci celkové bezpečnostní politiky organizace je správa uživatelů náročná, proto se implementuje Identity Management, strategie zahrnující různé postupy, procesy a informace sloužící k identifikaci identity během jejího životního cyklu. Praktická část práce je zaměřena na implementaci systému Identity Managementu ve státní správě.

Klíčová slova: autentizace, heslo, certifikát, Identity Management

ABSTRACT

The Bachelor thesis deals with methods of authentication in information systems, such as the name and the password, a certificate that was issued by a public certification service provider, one-time passwords and biometrics. Within the overall security policy, an user Management organization is difficult, therefore, implements the Identity Management, a strategy involving a variety of procedures, processes and information used to identify the identities during its life cycle. The practical part is focused on the implementation of Identity Management in Public Administration.

Keywords: authentication, password, certificate, Identity Management

V úvodu své bakalářské práce bych chtěla poděkovat Ing. Jánu Ivankovi za odborné znalosti a rady poskytnuté v rámci odborných konzultací a za připomínky k úpravě a formě zpracování bakalářské práce. Dále bych ráda poděkovala své rodině za podporu během mého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

……
podpis diplomanta

OBSAH

ÚVOD **9**
TEORETICKÁ ČÁST **11**
1. AUTENTIZACE **12**
2. METODY AUTENTIZACE UŽIVATELŮ **14**
2.1. KOMBINACE JMÉNA A HESLA 14
2.2. POUŽITÍ CERTIFIKÁTŮ 15
2.2.1. Certifikátem a klíčem uloženým na lokálním počítači 15
2.2.2. Certifikátem vydaným veřejným poskytovatelem certifikačních služeb 15
2.3. BIOMETRICKÉ ÚDAJE 16
2.3.1. Daktyloskopická identifikace 17
2.3.2. Snímání oční duhovky a sítnice 18
2.4. SMS JEDNORÁZOVÁ HESLA 19
2.5. ČIPOVÉ KARTY 21
3. SPRÁVA IDENTIT V PODNIKOVÉM PROSTŘEDÍ - IDENTITY MANAGEMENT **23**
3.1. ARCHITEKTURA IDENTITY MANAGEMENTU 24
3.2. ROLE BASED ACCESS CONTROL 25
3.3. IDENTITY MANAGER 28
3.4. WORKFLOW 29
3.5. ŽIVOTNÍ CYKLUS IDENTITY 29
3.6. ZPŮSOB AUTENTIZACE 30
3.7. AUDIT 31
3.8. PŘÍNOSY IMPLEMENTACE IDENTITY MANAGEMENTU 31
3.9. TRENDY DALŠÍHO ROZVOJE 33
PRAKTICKÁ ČÁST **35**
4. IMPLEMENTACE IDENTITY MANAGERU VE STÁTNÍ SPRÁVĚ **36**
4.1. INICIALIZACE ITIM 36
4.2. ARCHITEKTURA ITIM 37
4.3. KONEKTORY – HR, AD, ITIM A JEJICH KOMUNIKACE 38
4.4. IBM TIVOLI DIRECTORY INTEGRATOR 39
4.5. KERBEROS A PROCES KOMUNIKACE 40
4.6. GRAFICKÉ ROZHRANÍ ITIM GUI 42
4.7. SITUACE PŘED IMPLEMENTACÍ 43
4.7.1. Nástup nového zaměstnance 43
4.7.2. Aplikace před implementací 44
4.8. SITUACE PO IMPLEMENTACI 45
4.8.1. Nástup nového zaměstnance 45
4.8.2. Založení uživatele v ITIM 46
4.8.3. Aplikace po implementaci 47
4.9. AUDIT 48

4.10. PŘÍNOSY IMPLEMENTACE ITIM PRO STÁTNÍ SPRÁVU 49
ZÁVĚR 50
ZÁVĚR V ANGLIČTINĚ 52
SEZNAM POUŽITÉ LITERATURY 53
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 54
SEZNAM OBRÁZKŮ 57

ÚVOD

V dnešní době lze jen stěží nalézt počítačový systém, u kterého by nebyly otázky autentizace a autorizace součástí základních požadavků. Problematika zabezpečení dat v počítačích se dnes netýká pouze dat ve státních či soukromých organizacích, ve společnostech nebo v agenturách průmyslu komerční bezpečnosti, ale i dat, které máme uložená doma v osobních počítačích a noteboocích a které se již staly nedílnou součástí našeho života. Ochrana dat a informací je důležitá, ať už se jedná o oblast bezpečnostního průmyslu nebo další oblasti využívající informační technologie.

Cílem mé bakalářské práce je rozšířit podvědomí uživatelů výpočetní techniky o nedostatečné úrovni bezpečnostních záruk některých používaných autentizačních metod a seznámení s bezpečnějšími způsoby autentizace. Málokdo si uvědomuje, že bezpečná autentizace je základem pro ochranu dat a osobních údajů, a to především v dnešní době neustálého rozvoje a zdokonalování informačních technologií. Data podléhající chráněnému zájmu nevlastní pouze velké společnosti, ale i řada soukromých společnostní, mezi něž se řadí i bezpečnostní a detektivní agentury.

V současné době je nejpoužívanější nejjednodušší způsob autentizace pomocí jména a hesla. Většina uživatelů je informována o nedostatečné úrovni bezpečnostních záruk, které poskytuje kombinace jména a hesla při identifikaci a autentizaci do informačních systémů. Přesto si většina uživatelů myslí, že jsou jejich údaje v bezpečí a téměř polovina uživatelů se dokonce domnívá, že jejich heslo je extrémně bezpečné. V posledních letech se objevují zcela nové útoky reálně aplikované i na poměrně dlouhá hesla, která byla dříve považována za bezpečná. Na většinu útoků existují různá protiopatření, neodstraní však základní slabinu používání hesla, a to je jednání uživatele. Uživatel si pro možnost případného zapomenutí heslo ukládá např. pod funkční klávesy, nebo píše lístečky, které pak visí na monitorech a klávesnicích. Z výše uvedených i jiných důvodů se odborníci informačních technologií snaží vyvíjet nové metody autentizace s cílem omezit úspěšnost útoků na překonání těchto metod na minimum. V teoretické části se seznámíme s nejznámějšími metodami autentizace běžného uživatele a také s Identity Managementem, produktem pro správu identit v organizacích.

V praktické části si představíme implementaci IBM Tivoli Identity Managementu ve státní správě. V rámci celkové bezpečnostní politiky organizace je správa uživatelů náročná, ovládání aplikací a přístup k datům klade velké nároky jak na správce systémů, tak na vlastníky dat i běžné uživatele. Identity Management velmi úzce souvisí s problematikou

autentizace uživatelů, i když provádí pouze správu identit. Představuje bezpečné, automatizované řešení správy identit na bázi pravidel, zahrnující různé postupy, procesy a informace sloužící k identifikaci identity během jejího životního cyklu. Touto identitou je jedinec a jeho identita je specifikována množinou příslušných oprávnění.

TEORETICKÁ ČÁST

1. AUTENTIZACE

Základním kamenem téměř každého řešení systému je autentizace uživatele. Autentizace má přinést potřebnou míru jistoty o identitě[1], se kterou komunikujeme při vstupu do systému. Autentizace uživatelů je proces ověřování identity uživatele, to znamená, zda je uživatel na druhé straně spojení skutečně tím, za koho se vydává. K uživatelské autentizaci dochází například při přihlašování pomocí uživatelského jména a hesla. Po zadání server zašle klientovi session token, což je náhodně vygenerovaný jedinečný identifikátor aktuální session[2]. Token si prohlížeč obvykle uchovává v podobě cookie[3] ve své paměti a odesílá serveru s každým dalším dotazem. Server si tak podle něj může navzájem pospojovat všechny klientovy dotazy.

Autentizace se často zaměňuje s autorizací. Jsou to ale zcela rozdílné pojmy. Při autentizaci se ověřuje identita uživatele, ale při autorizaci se kontroluje, zda již autentizovaný uživatel má dostatečná oprávnění pro přístup k určitému souboru, aplikaci nebo jestli je daný uživatel oprávněn provádět určitou činnost.

Autentizace se skládá ze dvou částí, identifikace uživatele a autentizace uživatele. Identifikace uživatele je proces určení identity uživatele. Uživatel zadá svoji identitu (např. přihlašovací jméno) a následně probíhá autentizace uživatele neboli proces ověřování identity uživatele. Prověření, že je skutečně tím, za koho se prohlašuje. Uživatel prokazuje svou identitu tím, že poskytne určitá data, která má k dispozici pouze on.

Základní metody autentizace uživatelů jsou založeny:

- na něčem co daný uživatel zná (PIN[4], heslo),
- na něčem co daný uživatel má (token, nebo platební karta),
- na něčem, čím daný uživatel je (biometrická informace).

[1] Identita - Totožnost. Digitální označení entity takovým způsobem, který umožnuje jeho rozlišení od jiných entit.

[2] Session - (nebo-li relace) je permanentní síťové spojení mezi klientem a serverem, zahrnující výměnu paketů.

[3] Cookie - Malý textový soubor vytvářený webovým serverem a ukládaný v počítači prostřednictvím prohlížeče.

[4] PIN – (Personal Identification Number) - Osobní Identifikační Číslo.

Autentizační metody dělíme na slabé a silné. Mezi slabé metody patří zejména využívání hesel a PIN. Na pomezí mezi silnými a slabými metodami leží metody autentizace využívající jednorázových hesel. Za silné autentizační metody jsou dnes označovány metody na principu výzva-odpověď, které využívají elektronické tokeny a čipové karty.

V současné době je autentizace klíčovou součástí každé pokročilé aplikace. Špatně realizovaná autentizace může mnohé uživatele odradit od přihlášení, v horším případě může přímo představovat vážnou bezpečnostní díru do systému a následné zneužití citlivých údajů a dat obecně.

2. METODY AUTENTIZACE UŽIVATELŮ

2.1. Kombinace jména a hesla

Jedná se o nejdéle používaný způsob autentizace do informačních systémů. Důvodem, proč je uvedené řešení tak rozšířené, je jeho jednoduchost (způsob nevyžaduje žádný dodatečný hardware) a nízká cena jeho implementace (systém pouze porovná řetězec poskytnutý uživatelem s řetězcem uloženým ve své databázi). Uživatelé jsou zvyklí způsob autentizace přes jméno a heslo používat nejčastěji, přestože se již delší dobu hovoří o nedostatečné úrovni bezpečnostních záruk. Úroveň těchto záruk je nedostačující zejména pro kritické a Single-Sign-On systémy (dále jen SSO[5]). SSO systém je dnes již také považován za kritický systém, protože jedno přihlášení postačuje pro získání přístupu k více informačním zdrojům.

Typické heslo bývá řetězec dlouhý 6 až 10 znaků obsahující malá a velká písmena a číslice, ale uživatelem snadno zapamatovatelný. Uživatel předkládá heslo systému společně se svou identifikací, kterou je uživatelské jméno (login). Systém autentizační údaje kontroluje s daty uloženými k danému uživateli. Provázání správnosti je vyhodnoceno systémem jako korektní prokázání identity.

Za bezpečné heslo lze považovat takové, jehož prolomení obvyklými technikami je časově náročné. Jedná se o řetězce dlouhé 8 až 12 znaků skládající se z malých i velkých písmen, číslic a dalších tisknutelných znaků.

Negativa tohoto řešení jsou snadná možnost uhodnutí, odpozorování, nebo prolomení hesla pomocí nástrojů pro generování hesel. To nutí k nastavení přísných kritérií pro kvalitu řetězce tvořícího heslo a periodu změny hesla. Přísnější kritéria ale kladou nepříjemně vysoké nároky na uživatele. Pokud neexistuje centrální databáze uživatelů a uživatel musí pečovat o celou řadu hesel pro různé aplikace, pak to situaci ještě zhoršuje. Uživatelé si pak hesla někam poznamenají, aby je nezapomněli. Kromě bezpečnostních problémů systém přináší i vysoké zatížení pracovníků administrátorské podpory (problémy týkající se uživatelských hesel tvoří cca 30 až 50% z celkového počtu řešených problémů).

[5] SSO - (Single Sign On) Systém jednorázového přihlašování – uživatel se autentizuje do systému pouze jedenkrát, jeho identita je pak předávána a uznávána jednotlivými aplikacemi, databázemi a operačními systémy.

2.2. Použití certifikátů

2.2.1. Certifikátem a klíčem uloženým na lokálním počítači

Uvedený způsob patří do obdobné kategorie jako kombinace jména a hesla. Nabízí ale vyšší úroveň záruk a větší funkcionalitu. Největší slabinou systému je uložení soukromého klíče v lokálním počítači. Přestože na jeho utajení celý systém stojí, je soukromý klíč chráněn pouze prostředky operačního systému. Jen malá část uživatelů používá ještě dodatečné přístupové heslo. Uvedená metoda není také příliš vhodná pro kritické a SSO systémy.

2.2.2. Certifikátem vydaným veřejným poskytovatelem certifikačních služeb

Jedním z dalších přístupů pomáhajících řešit identifikaci uživatele je použití certifikátů vydaných veřejným poskytovatelem certifikačních služeb. Zmíněná metoda patří do skupiny k těm nejbezpečnějším způsobům autentizace. Předpokladem je možnost využití kryptografie v autentizačním mechanismu (nejčastěji SSL[6]), což je již dnes ve většině systémů standard, a to jak na straně serveru nebo aplikace tak na straně klienta.

Celý autentizační proces probíhá zhruba v těchto krocích:

1. navázaní spojení (výměna kryptografických informací),
2. ověření platnosti certifikátu uživatele serverem, popř. ověření platnosti certifikátu serveru uživatelem (identifikace),
3. ověření identifikačních informací z certifikátu v adresářové službě - ověření existence uživatelských pověření (autorizace uživatele).

Do systému, který má ověřovat identitu uživatele, je třeba nainstalovat serverový certifikát a certifikát certifikační autority. Tím určíme, ke kterému certifikačnímu úřadu (certifikační autoritě) nastavujeme důvěru. Platnost certifikátu se ověřuje kontrolou pomocí aktuálního revokačního listu (CRL[7]), který vydává certifikační autorita nebo mechanismus vydávající certifikáty. Uživatel tedy musí mít certifikát vydaný certifikační autoritou nebo mechanismem, kterému aplikace nebo server důvěřuje.

[6] SSL – (Secure Sockets Layer) Služba sloužící k šifrování spojení pro protokol http.

[7] CRL - (Certificate revocation list) Seznam zneplatněných certifikátů.

Po úspěšné implementaci autentizace pomocí certifikátů lze již snadno implementovat elektronický podpis, popř. sledování oběhu dokumentů ve společnosti. Certifikáty jako takové řeší jednotnou identifikaci uživatelů, nad kterou lze pak stavět SSO řešení, nebo lze poskytovat služby správy identity jiným subjektům. Autentizaci pomocí certifikátů lze využívat pro přihlášení k desktopu počítače, do domény Windows, pro terminálové připojení, webové aplikace, k přihlášení ke konzolím systémů UNIX nebo LINUX.

2.3. Biometrické údaje

Zmíněná kategorie autentizačních metod je relativně zajímavá a má svoji budoucnost. V současné době se používají v komerčně bezpečnostní biometrické identifikaci metody založené na poznatcích o daktyloskopii, o oční duhovce a sítnici, o anatomických rozměrech a závislostech dlaně a prstů a o tvarech obličeje.

Výhody biometrických identifikačních metod jsou:

- univerzálnost - každý uživatel je jejich nositelem,
- jedinečnost - neexistují dvě osoby se stejnými biometrickými charakteristikami,
- přijatelnost - snímání biometrických charakteristik je pro uživatele nenáročné,
- permanence - biometrická charakteristika je časově neměnná.

Biometrické systémy snímají biometrické charakteristiky, které následně porovnávají s údaji v předem vytvořené databázi. V rámci registrační etapy uživatelé poskytují reprezentativní biometrický vzorek, pomocí kterého se registrují do biometrického systému. Vzorek je uložen do šablony v odpovídajícím matematickém kódu, který vznikne extrakcí jeho unikátního znaku. V další etapě je šabloně přidělen identifikátor (číslo karty, PIN,…), který se používá k vyhledání reprezentativního vzorku. Pro úspěšné využívání biometrického systému jsou kvalita a zápis výsledného reprezentativního biometrického vzorku klíčové. Šablona se ukládá do biometrického čtecího zařízení nebo do vzdálené centrální databáze. Vytvoření databáze následně umožňuje vlastní identifikaci uživatele. Pomocí čtecího zařízení získáme biometrický vzorek, dle kterého se opět vytvoří odpovídající šablona a ta se porovná s uloženou šablonou. K vyhledání správné šablony slouží identifikátor.

Biometrické technologie mají vysoký stupeň přesnosti a jejich síla není v utajení informací používaných pro autentizaci, ale v jedinečnosti těchto informací. Výhody biometrické

autentizace jsou silná metoda pro autentizaci a to i z hlediska obrany proti zneužití, odolnost vůči krádežím a uživatel se nemusí obávat ztráty karty nebo zapomenutí hesla či PIN. Nevýhody jsou nutnost zabezpečení identifikační databáze a náročnost na snímání a porovnání snímaného údaje s reprezentativním vzorkem.

S ohledem na bezpečnostní politiku, která je specifická dle činností jednotlivých organizací, systém biometrie umožňuje uživateli nastavit různé bezpečnostní priority. Záznamy o „úspěšný"/„neúspěšný" přístup jsou zachovány v systému pro možnost sledování celého systému. Důležité je omezit počet pokusů o přihlášení, aby po určitém počtu neúspěšných pokusů o přihlášení, systém uživateli další pokus zakázal.

Biometrická data lze využít při kombinaci všech metod autentizace, protože tak se využijí všechny tři pilíře bezpečnosti: uživatel něco má (kartu), něco zná (PIN) a něco je (např. otisk prstu).

2.3.1. Daktyloskopická identifikace

Mezi nejznámější a nejrozšířenější technologie patří daktyloskopická identifikace. Do databáze se nejdříve uloží vytvořený referenční biometrický vzorek. Uživatel přiloží prst na snímač otisku prstů a dojde k porovnání s referenčním vzorkem uloženým v databázi. Po potvrzení, že se jedná o oprávněnou osobu, je následně umožněn přístup do systému. Daktyloskopická identifikace je založena na obrazech papilárních linií, které se nachází na vnitřní straně článků prstů, dlaních a chodidlech. Daktyloskopie vychází ze tří obecně uznávaných zákonů:

1. zákon o individuálnosti obrazců papilárních linií - neexistují dvě osoby, které mají naprosto stejné obrazce papilárních linií. Variabilnost obrazců papilárních linií je tak vysoká, že není možné, aby na zemi existovali dva lidé s naprosto stejnými obrazci papilárních linií, a to ani za celou dobu existence člověka na zemi,
2. zákon o neměnnosti obrazců papilárních linií - obrazce papilárních linií člověka (tvar, sled, skladba, …) zůstávají celý život relativně neměnné,
3. zákon o neodstranitelnosti papilárních linií - linie nelze odstranit, pokud se neodstraní nebo zničí i zárodečná vrstva kůže. I po zhojení zranění se vytvořily tytéž obrazce papilárních linií.

V systémech určených pro autentizaci jsou ukládány pouze údaje o identifikačních bodech, které postačují k rozhodnutí, zda je či není nasnímaný otisk shodný s uloženou šablonou, zatímco v identifikačních systémech jsou ukládány celé otisky.

Základním předpokladem pro opakované daktyloskopické vyhodnocování je čistý povrch snímacího zařízení a správné položení prstu na snímací zařízení. Nesprávná pozice (natočení prstu, umístění prstu příliš k okraji snímače,…) má za následek snížení počtu získaných bodů v otisku. Tím se snižuje výkonnost celého systému a zvýšení chybovosti. Dalšími faktory ovlivňujícími kvalitu snímaného otisku jsou čistota prstů, vlhkost pokožky a tlak při přiložení prstu na snímač.

Snímací zařízení využíváme interní - integrované do klávesnic stolních počítačů, do notebooků a myší, externí - připojená přes port USB[8], nebo fixní – připevněné na stěně.

2.3.2. Snímání oční duhovky a sítnice

Další nejčastěji využívanou biometrickou identifikační metodou je snímání oční duhovky (barevná část kolem tmavé zornice) a sítnice. Oční duhovka je jedinečná pro každého člověka. Odlišné jsou duhovky v pravém a levém oku téhož člověka, a na rozdíl od DNA mají jiné duhovky i jednovaječná dvojčata. Uživatel se pohledem zaměří na snímací zařízení, černobílou CCD kameru, které automaticky pořídí několik snímků pro jeho registraci. Při snímání zaznamená rozmístění pigmentu i tvary svalů v oční duhovce a získané informace přenese do počítače. K vytvoření šablony postačí snímek s více stupni šedi ve vysokém rozlišení. Pro softwarové nalezení duhovky a určení detailů o každém významném bodě pořízený snímek poskytne dostatek informací.

Skenování oční sítnice je ve srovnání se snímáním duhovky o něco složitější. Při skenování oční sítnice je sledována oblast v okolí slepé skvrny. Uživatel se zaměří na specifikovaný bod optického snímače (vzdálenost musí být okolo 2 cm) a oko je skrz zornici nasvíceno infračerveným paprskem, který dále zpracovává vzor cév ze zadní strany oka (v několika stupních šedi).

Výhody jsou nízká chybovost, vysoká rychlost porovnání kódů (miliony srovnání za sekundu) a hlavně, že použití sítnice oka nebo oční duhovky jako unikátního biometrického otisku je považováno za jednu z nejpřesnějších technologií vůbec. Nevýhody jsou výška umístění fixní čtečky na zdi (uživatelé vybočující z „výškového průměru“ nemohou poskytnout snímači sítnici ve správném úhlu), nepříjemné pocity některých uživatelů při snímání (přiblížit se blízko ke snímači a nechat si svítit do oka), nutnost snímání brýlí a v neposlední řadě také vyšší pořizovací cena.

[8] USB - (Universal Serial Bus) Univerzální sériová sběrnice pro připojení periferií k počítači.

2.4. SMS jednorázová hesla

Systémy silné autentizace využívající mechanismů jednorázových hesel a kombinaci více autentizačních faktorů nalézají stále větší uplatnění v řešení bezpečnosti informačních technologií. Zjednoduší přihlašování do firemních systémů a přitom zachová pevně definovaná bezpečnostní pravidla. Autentizace uživatelů k firemním zdrojům by na jedné straně měla splňovat ty nejpřísnější nároky na bezpečnost a na straně druhé komfort uživatelů, kteří autentizaci dennodenně využívají.

Bezpečnou autentizaci lze dnes zajistit pomocí jednorázových hesel zasílaných formou SMS[9] do mobilního telefonu. Uživateli pak stačí, když má u sebe svůj mobilní telefon, a dostane se ke všem potřebných zdrojům.

Jednorázová hesla jsou taková hesla, která lze použít jen jednou, a nikoli opakovaně. Pro další úkon si musíme opět nechat vygenerovat další nové jednorázové heslo. Jednorázové heslo si můžeme představit jako několikamístné číslo nebo řetězec písmen a dalších znaků, které nám vygeneruje generátor hesel, který funguje sekvenčně (vždy na vyžádání nám vygeneruje další nové heslo).

K vygenerování One Time Password (dále jen OTP[10]) pomocí mobilního telefonu a SIM karty slouží služba OneID. Služba řeší pro poskytovatele služeb a aplikací bezpečné a prokazatelné ověření uživatelů a komunikaci s nimi. Služba OneID[11] využívá mobilní telefon jako terminál s klávesnicí a displejem, SIM kartu[12] jako nositele bezpečnostní aplikace a SIM toolkit[13] jako jediné univerzální rozhraní mezi SIM kartou a libovolným mobilním zařízením.

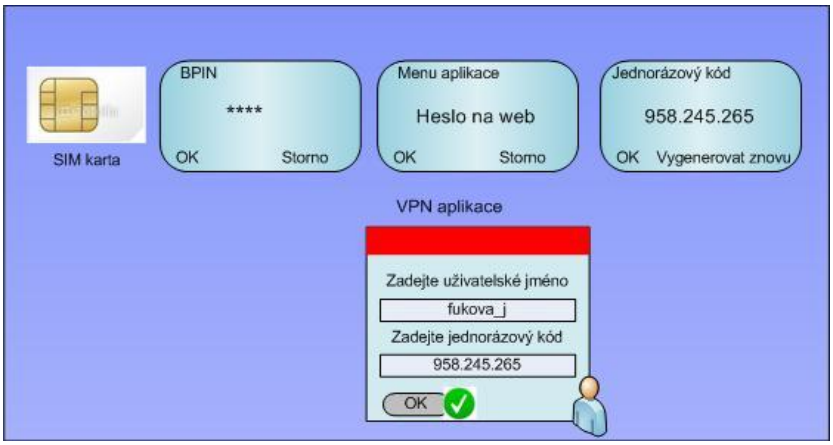
[9] SMS - (Short Message Service) krátká textová zpráva. Jako služba je dostupná ve většině mobilních telefonů.

[10] OTP - (One Time Password) Jednorázové heslo vygenerované pouze pro jedno použití.

[11] OneID - Služba zabezpečené identifikace.

[12] SIM karta - (Subscriber Identity Module) Je to účastnická identifikační karta která slouží pro identifikaci účastníka v mobilní síti.

[13] SIM toolkit - Technologie umožňující nahrávání a provozování aplikací v mobilním telefonu.



Obr. 1. *Funkce One Time Password*

Řešení je primárně velmi užitečné pro GSM[14] operátory, virtuální operátory a organizace poskytující elektronické služby svým zákazníkům. Dále pro organizace s požadavky na vysokou míru zabezpečení vnitropodnikových informačních systémů (banky, stavební spořitelny, obchodníci s akciemi, …). Řešení je mimo jiné vhodné i pro společnost, která hledá na stejné úrovni bezpečnou a přesto levnější variantu za RSA tokeny[15] bez nutnosti nákupu a správy dalšího hardware. Lze ho použít i pro autorizaci přístupu do aplikací, které se často používají v nechráněném prostředí (např. on-line placené počítačové hry).

Služba OneID je realizována formou měsíčního poplatku za každou SIM kartu, pro kterou byla služba povolena. Jedná se o konečnou cenu, zákazník nepotřebuje žádné další HW ani SW vybavení ani nehradí žádné další skryté náklady. A to s důrazem na vysokou úroveň zabezpečení a jednoduché, pro uživatele přívětivé ovládání. Výhodami této služby jsou nezávislost funkčnosti na službách GSM operátora (může být využívána i v místě bez mobilního pokrytí - práce off-line) a opakované generování OTP (vygenerování nic nestojí).

Službu OneID je možné použít pro přihlášení do firemní VPN sítě, přístup ke svému bankovnímu účtu, autorizaci/potvrzení platebního příkazu v bankovním systému, zaslání zabezpečené SMS zprávy zákazníkovi, identifikované volání operátorovi, aj.

[14] GSM - (Globální Systém pro Mobilní komunikaci) Standard pro mobilní telefony.

[15] RSA token - USB zařízení zobrazující šestimístný kód pro potvrzení autentizace, který se mění každou minutu.

2.5. Čipové karty

Ukládání soukromých klíčů na čipové karty (resp. USB tokeny) nám nabízí možnost využít zařízení k autentizaci a opustit tak od klasického způsobu přihlašování přes jméno a heslo. Uživatel je nejprve autentizován vůči čipové kartě na základě:

- že něco má (čipovou kartu),
- že něco zná (přístupový PIN ke kartě),

a čipová karta se pak autentizuje vůči systému na základě, že něco umí.

Systém může být také doplněn o využití biometrických údajů také uložených na čipové kartě. Autentizace uživatele vůči kartě tak může být doplněna o to, že uživatel něčím je.

Přihlašování probíhá za využití soukromého klíče uloženého na čipové kartě. Na kartě může být více klíčů, ale jen jeden z nich může být označen jako klíč určený k přihlašování pomocí čipové karty. Veřejný klíč příslušející k tomuto soukromému klíči je certifikován certifikátem veřejného klíče.

Zmiňovaný mechanismus je standardně podporován většinou běžně využívaných systémů (Microsoft Windows, Linux, …). Při využití pro více aplikací je vhodné řešení přihlašování doplnit o SSO.

Mechanismus přihlášení do Windows pomocí čipové karty je založen na využití Active Directory[16] (dále jen AD). Z tohoto důvodu je mechanismus prakticky využitelný pouze v sítích s instalovanými AD. Pokud dodavatel čipových karet dodá middleware[17] pro Windows, pak zpravidla není třeba vyžadovat již nic dalšího pro podporu přihlášení čipových karet.

Přihlášení pomocí čipové karty se často používá také v systému LINUX jako přihlášení ke konzoli systému, ať se jedná o pracovní stanici nebo server. V případě systému UNIX je možné přihlášení pomocí čipové karty i pro servery samostatně stojící mimo síťovou infrastrukturu. Po dodavateli čipových karet je však třeba vyžadovat podporu přihlášení pro čipové karty pro jednotlivé platformy UNIX.

Pro nasazení čipových karet je nezbytné doplnit k pracovním stanicím čtečky karet s příslušnými ovladači a provést příslušné zásahy do konfigurace pracovních stanic. Z tohoto důvodu se karty převážně používají v prostředí, kde je možné plně kontrolovat pracovní stanice koncových uživatelů.

[16] Active directory - Adresářový server, kam se ukládají informace o entitách v prostředí Microsoft.

[17] Middleware - Počítačový software, který spojí komponenty softwaru nebo aplikace.

Výhodou čipových karet je jejich funkcionalita, kterou lze kromě identifikace a autorizace použít:

- pro tvorbu zaručeného elektronického podpisu,
- pro ukládání soukromých klíčů používaných pro dešifrování dat,
- pro zajištění přístupu do objektů a prostor (kombinace s bezkontaktním čipem),
- jako průkazu zaměstnance.

V případě používání čipové karty jako hlavního autentizačního prostředku se nesmí zapomenout i na řešení nestandardních stavů jako je zapomenutý PIN a zapomenuté, zničené nebo ztracené karty. Nevýhoda je nebezpečí ztráty (krádeže) nebo poškození čipové karty.

3. SPRÁVA IDENTIT V PODNIKOVÉM PROSTŘEDÍ - IDENTITY MANAGEMENT

Mezi nejčastěji řešené problémy v informačních technologiích dnes mimo snižování nákladů patří hlavně zlepšování služeb, které technologie poskytují. Je vyžadováno rychlé nasazování nových aplikací s důrazem na levné a efektivní provozování. Nárůst počtu aplikací však s sebou přináší větší bezpečnostní rizika. Uživatel má přístup do více aplikací a tím i více přístupových účtů. Pro podniky a organizace pak bývá problém spravovat velké množství účtů a správu přístupu k informacím. Aby měla organizace přehled o tom k jakým aplikacím či datům má daný uživatel možnost přístupu, je třeba spravovat uživatelské účty z jednoho místa.

Pro jednotnou správu účtů je vhodný software pro centralizovanou správu uživatelů, zvaný Identity Management. Systém identity dává Managementu a správcům informačních technologií nástroje potřebné ke kontrole přístupu uživatelů k podnikovým datům. Může se stát základem bezpečné sítě, neboť správa identit uživatelů je nepostradatelnou součástí kontroly přístupu.

Identity Management splňuje požadavky na informační systémy v oblasti bezpečnosti přístupu k informacím, jako jsou:

- přidělení přístupových práv uživatelům v informačních systémech,
- jednoznačnou identifikaci a autentizaci uživatele,
- zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačních systémů, ochranu bezpečnostních auditních záznamů modifikací nebo zničením, a jejich archivaci,
- statistické údaje o přístupech k aplikacím a datům.

Nyní uveďme charakteristiku Identity Managementu:

Identity Management je informační systém, který dokáže z jednoho místa ovládat životní cyklus všech uživatelských účtů, aby bylo možné zajistit bezpečný přístup k neustále rostoucímu počtu systémů a aplikací.

Nasazení Identity Managementu automatizuje únavný a manuální proces vytváření nových účtů a hesel, rušení nebo změny stávajících účtů pro zaměstnance a zákazníky podniku, jímž by se jinak museli zabývat administrativní pracovníci informačních technologií. Systém poskytuje administrátorům nástroje pro změny uživatelských rolí, zajišťování

dodržování nastavených pravidel a sledování činnosti uživatelů. Řešení je přínosné i pro uživatele, kteří mohou využívat funkce pro obnovení a synchronizaci vlastních hesel bez jednání s administrátorem. Šetří čas uživatelům i administrátorské podpoře. Software také dokáže identifikovat neoprávněné nebo nebezpečné změny, jež by poskytly uživatelům přístup k většímu množství aplikací, než pro svou práci potřebují. Odstraňuje nelegitimní přístup a v případě takové události upozorňuje příslušné odpovědné pracovníky. Monitorování neoprávněných přístupů k aplikacím a informacím je v dnešní době velmi důležité pro organizace pracující s osobními údaji, úřady a správy, agentury bezpečnostního průmyslu a ostatní instituce pracující s citlivými údaji.
Centrální správa uživatelů a jejich přístupů v Identity Managementu (dále jen IM) je založena na jednotném rozhraní, definovaných rolích, politikách (přístupy, jména a hesla) a reportingu. Z tohoto důvodu je nutné předem nadefinovat přístupové politiky a jejich přístupy k informacím. Pro správu identit a účtů využívá IM organizační strom, definované role a vlastní IM role. Celá správa identit je doplněna o workflow a reporty v needitovatelném PDF formátu.

Typický systém pro správu identit se skládá ze čtyř částí:

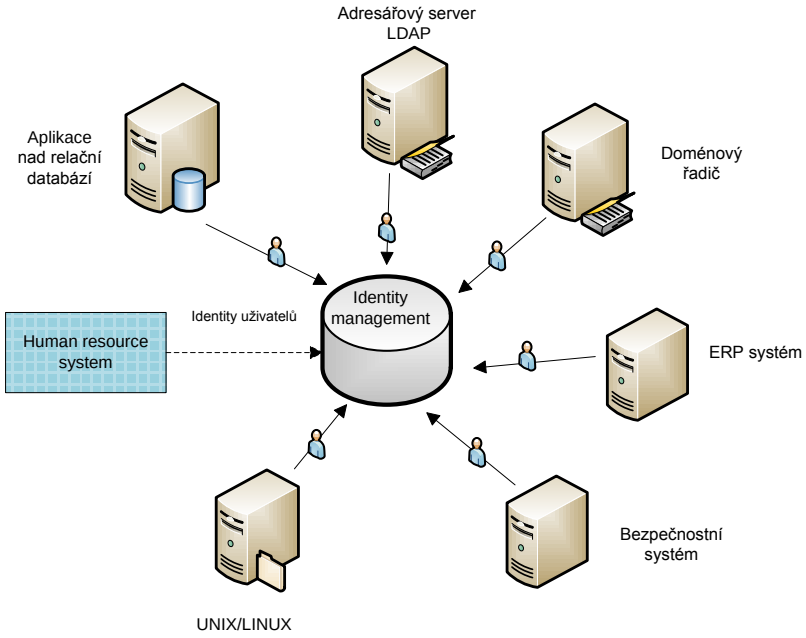
- úložiště digitálních identit (adresář osobních dat využívaný při definici uživatelů),
- správa přístupového životního cyklu (sada nástrojů pro modifikaci, přidávání a mazání těchto dat),
- systém pro regulaci přístupu uživatelů (přístupová práva aplikace a bezpečnostní pravidla),
- auditovací a reportovací systém.

V současné době působí na trhu řada výrobců softwaru pro centrální správy uživatelských přístupů a identit (identity & access Management). Mezi nejvýznamnější patří IBM, Oracle, společnost Novell, Ca nebo Sun Microsystems.

3.1. Architektura Identity Managementu

Typická architektura IM je centrálně orientovaná. Koncové systémy jsou na centrální uzel IM napojeny pomocí konektorů a adaptérů. Koncovými systémy jsou v tomto případě myšleny všechny systémy a aplikace, které mají vlastní úložiště uživatelských účtů. Konektor abstrahuje spojení ke koncovému systému a jeho úložišti uživatelů. Typy

konektorů jsou různé podle výrobce IM. Dnes však převažuje neinvazivní způsob komunikace, který využívá standardní protokoly a vrstvy jako je např. LDAP[18]. Výhodou tohoto způsobu je, že koncový systém není třeba upravovat. IM dodává potřebná data do koncových systémů na základě autoritativní informace, a ty si autentizaci a autorizaci řídí vlastními prostředky proti svému úložišti. Většina produktů IM má již předpřipravenou celou škálu konektorů pro řízení uživatelských účtů, čímž se nezvyšují náklady na úpravu vlastních řešení.



Obr. 2. *Architektura Identity Management*

3.2. Role Based Access Control

Základním předpokladem pro implementaci Identity Managementu je provedení analýzy na úrovni pracovního procesu, jejímž výsledkem bude identifikace a definice organizačních rolí. Je to jeden z klíčových faktorů pro nasazení IM.

Nejčastěji využívaný princip je postaven na přístupovém modelu Role Based Access Control[19] (dále jen RBAC), který využívá opakovaně přidělitelné role. Uživatelé jsou řazeni do skupin, které mají základ v jejich pracovním zařazení v organizaci nebo úloze

[18] LDAP - Přístupový protokol mezi klientem a adresářovým serverem (X.500). V současné době pod pojmem LDAP nerozumíme pouze komunikační protokol, ale i vlastní adresářový server.

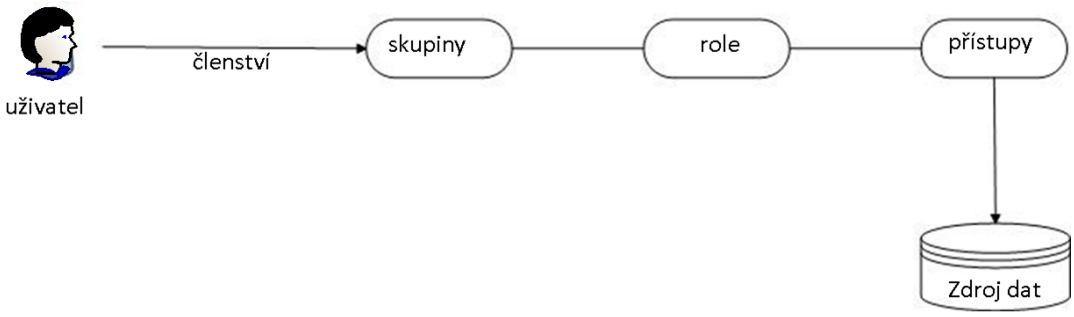
[19] RBAC - (Role Based Access Control) Bezpečnostní model, který uživatele rozděluje do skupin podle jejich rolí

v aplikaci. Skupina reprezentuje zaměstnance, kteří vykonávají podobné činnosti v rámci organizace, a zahrnuje většinu oprávnění, která zaměstnanec potřebuje pro vykonávání činnosti na příslušném organizačním místě. Ke skupině se váží definované role propojené na přístupovou politiku (nastavená přístupová oprávnění), která je svázána s cílovým systémem. Uživatel pak získá oprávnění přes tuto přidělenou roli, která může obsahovat i další atributy jako je popis, vlastník role nebo schvalovatel.

Za typické RBAC role můžeme považovat:

- „zákazník“ (přístup na webový server v DMZ[20]),
- „základní Zaměstnanec“,
- „senior Zaměstnanec“ a „Manager“.
-

Princip implementace RBAC ukazuje následující ilustrace:



Obr. 3. *Role Based Access Control*

Správa uživatelských účtů z jednoho místa řeší problematiku souladu s pravidly organizace, legislativou a koncovými systémy (operační systémy, databáze a aplikace). Pomocí IM je možné ohlídání souladu přes proces rekonciliace. V pravidelných intervalech dochází k ověřování, zda má uživatel přidělena stále jen ta práva, která potřebuje k vykonávání práce na své pozici. Případná nadbytečná oprávnění jsou pak automaticky odebrána. Vztah mezi uživatelem a rolemi, které mu přísluší, je tak neustále aktualizován. Jestliže je uživateli přiřazena určitá role a oprávnění příslušející této roli se změní, je všem uživatelům, kterým je konkrétní role přiřazena jejich oprávnění na základě synchronizace automaticky změněno.

[20] DMZ - (demilitarizovaná zóna) Část informačního systému, kde se se obvykle nachází zařízení, která zprostředkovávají určité služby jak pro prostředí vnitřní, tak pro prostředí vnější sítě.

Aktivace jednotlivých uživatelů probíhá právě prostřednictvím přidělování skupin a členství v aplikačních rolích na cílových systémech. V IM tohoto chování dosáhneme použitím aktivace politik, které obsahují nastavení skupin na cílovém systému.
Na úrovni rolí je dále možné řídit i Segregation of Duties, což jsou pravidla exklusivity. V praxi to znamená, že uživatel např. nemůže mít do jedné aplikace roli, která umožňuje vkládat data a zároveň roli kontrolní. Potřebné exklusivity jsou nastaveny v pravidlech a systém dané kombinace rolí automaticky nepovolí.

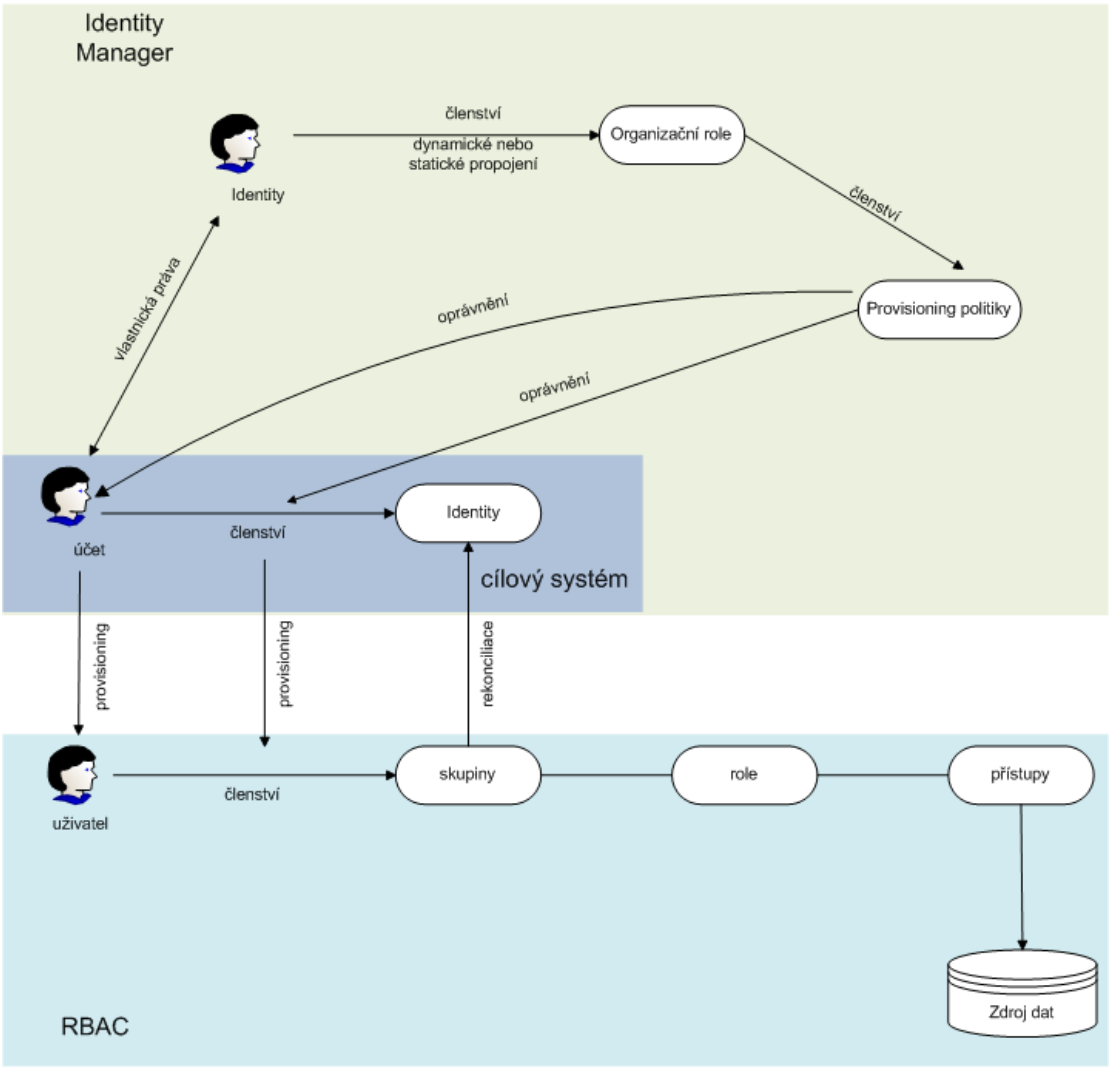
Interakce RBAC a IM zobrazuje obrázek (Obr. 4) s následujícím komentářem:
Rekonciliace je způsob přiřazení účtů pod identity, ale zároveň také zdroj informace o skupinách a rolích na spravovaném cílovém systému. Pro proces ověření Provisioning politiky lze stávající připojení ze zdroje kdykoliv načíst a následně s těmito definovanými pravidly porovnat. Proces spárování zdrojových účtů s centrálními účty lze nastavit automaticky nebo spouštět manuálně. Pokud bude zjištěna nesrovnalost u některého účtu, systém automaticky vyrozumí administrátora

Identity jsou naopak k rolím přiřazeny statickým nebo dynamickým propojením. Dynamická metoda určuje příslušnost na základě analýzy LDAP atributu identity. Přiřazují se automaticky na základě shody s hledanou znakovou nebo číselnou hodnotou. Statická přiřazení role jsou v rámci řešení IM přidělovány manuálně a jsou k dispozici v rámci celé organizace. Uživatel může např. zažádat o nový přístup k danému zdroji.

Oprávnění pak vyjadřuje propojení politik s koncovou aplikací pro dosažení požadované podoby účtu, který vystihuje danou roli. Je to sada atributů definujících přístupová práva a privilegia autentizovaného uživatele.

Provisioning je proces tvorby identit, definování jejich přístupových práv a zahrnutí do úložiště identit.

Provisioning politiky jsou pravidla a předpisy týkající se provázání centrálních a zdrojových účtů.



Obr. 4. *Systém Identity manager*

V čistém RBAC bychom každou roli museli definovat samostatně, i když by byla kombinací některých rolí stávajících. Uvedený přístup by v praxi vedl k produkci enormního množství rolí. Na rozdíl od čistého RBAC se v IM využívá spojování rolí a tím i politik (s využitím jejich priorit). Pro dosažení všech RBAC rolí v prostředí zákazníka, je pak možné provést pouze kombinace základních rolí. V praxi platí, že pokud má uživatel práva v koncovém systému řízena systémem více rolí, je jedna z nich rolí základní a ostatní jsou role doplňkové (rozšiřující).

3.3. Identity manager

Identity Management je strategie zahrnující různé postupy, procesy a informace sloužící k identifikaci entity během jejího životního cyklu. Touto entitou muže být jedinec i program, jeho identita je specifikována množinou příslušných atributů (oprávnění).

K vyřešení Identity Managementu slouží nástroj, tzv. Identity manager. Hlavními komponentami obvykle jsou:

- adresářové služby,
- správa elektronických identit - registrace, aktivace, schvalovací workflow, delegování pravomocí, self-service vybraných činností (uživatel si např. smí sám resetovat heslo apod.),
- synchronizace údajů.

Identity Management centralizuje všechny potřebné údaje o uživatelích (neboli identitách) do jednoho místa. Pomocí Identity managera lze uživatelské účty snadno vytvořit i zrušit. Uživatelské účty jsou napárovány na identity uložené v IM, čímž přestanou v systémech existovat účty bez vlastníka tzv. mrtvé duše, které tam zůstaly po dřívějších zaměstnancích nebo po různém testování. Účty bez vlastníka jsou reportovány, zneplatněny nebo přímo smazány z koncového systému.

3.4. Workflow

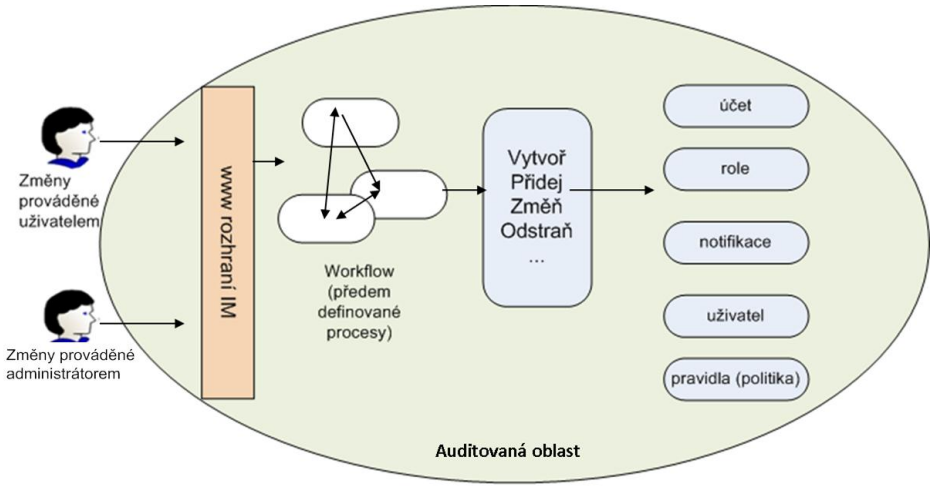
Kvalitní Identity manager obsahuje propracovaný systém tzv. workflow, které obsahuje řadu automatických akcí jako je synchronizace identit z personálního systému. Česky bychom jej nejspíše nazvali schvalovací proces. Jestliže organizace implementuje Identity manager, pak stačí, aby zaměstnanec navštívil pouze personální oddělení. Zakládání účtů a distribuce dat po jednotlivých systémech se děje automaticky přes Identity managera.
Nastavení workflow není jednoduché, ale jeho správná funkce má za následek, že povolování rolí a přístupových oprávnění provádějí opravdu ti, kdo mají (nadřízení, správci dat, apod.) a nikoliv ti, kdo rozumí informačním technologiím, jak tomu bylo doposud. Workflow oprávněným osobám totiž data ke schválení „předloží“ takovým způsobem a v takovém tvaru, že informačním technologiím opravdu rozumět nepotřebují. Workflow může také poskytovat data pro informaci, vyjadřovat se k požadavkům, apod.

3.5. Životní cyklus identity

Životní cyklus identity uživatele je základním procesem identity Managementu. Cyklus zpravidla začíná nástupem nového zaměstnance do organizace. Uživatel je zanesen do personálního systému a založen do provisioning účtů. Následně mu jsou přiděleny základní přístupy – e-mailová schránka, přístup na pracovní stanici a Intranet. Průběžně je uživateli

účet modifikován - přidělení či odebrání příslušných oprávnění, změna organizačního zařazení, nebo i změna jména. Pokud uživatel pracovní poměr ukončí, jsou mu účty zneplatněny, aby neměl možnost se k účtu přihlásit. Účet je vymazán, ale veškerá získaná oprávnění jsou zaznamenána takovým způsobem, aby byla zpětně dohledatelná např. z důvodu auditních kontrol.

Identita v IM vystupuje pod názvem Person. Je to záznam, pod který budou připojeny logicky související účty. Založením identity role Identity managera nekončí. Součástí je také webové rozhraní, přes které si může zaměstnanec povolené operace provádět sám – např. změnu bydliště. Údaj je pak z webového rozhraní IM automaticky distribuován na všechna místa, kam patří. Celý systém zároveň kontroluje integritu a správnost dat. Veškeré změny se provádí přes www rozhraní IM a životní cyklus identity pak vypadá následovně.:



Obr. 5. *Životní cyklus identity*

3.6. Způsob autentizace

Způsob autentizace při SSO by měl být bezpečnější než je autentizace k jednotlivým aplikacím. SSO může paradoxně bezpečnost snížit, protože jediná autentizace k systému otevírá přístup ke všem aplikacím. Je však zároveň nutné, aby řešení nebylo zbytečně finančně nákladné. Optimální je řešení, kde se křivky nákladu a rizika protínají.

Z pohledu autentizace jsou aplikace dvojího typu:

- aplikace umí přebírat autentizaci certifikátem automaticky nebo pouze s menší

úpravou – tzv. kerberizovaná aplikace[21],

- aplikace má jiný způsob autentizace a bylo by příliš pracné nebo neproveditelné jej přeprogramovat. V tomto případě se v SSO provede provázání vnitřní autentizace uživatele v aplikaci na autentizaci certifikátem uživatele.

3.7. Audit

Tivoli Identity Manager nabízí centrální úložiště pro ukládání dat o veškerých uživatelských přístupech a informace, kdo jednotlivá přístupová oprávnění přidělil. Auditoři, security administrátoři a jiné určené osoby si mohou zobrazit data pro jednotlivé uživatele, systémy, aplikace nebo kombinace těchto parametrů.

Tivoli Identity Manager poskytuje odpovědi na dotazy typu:

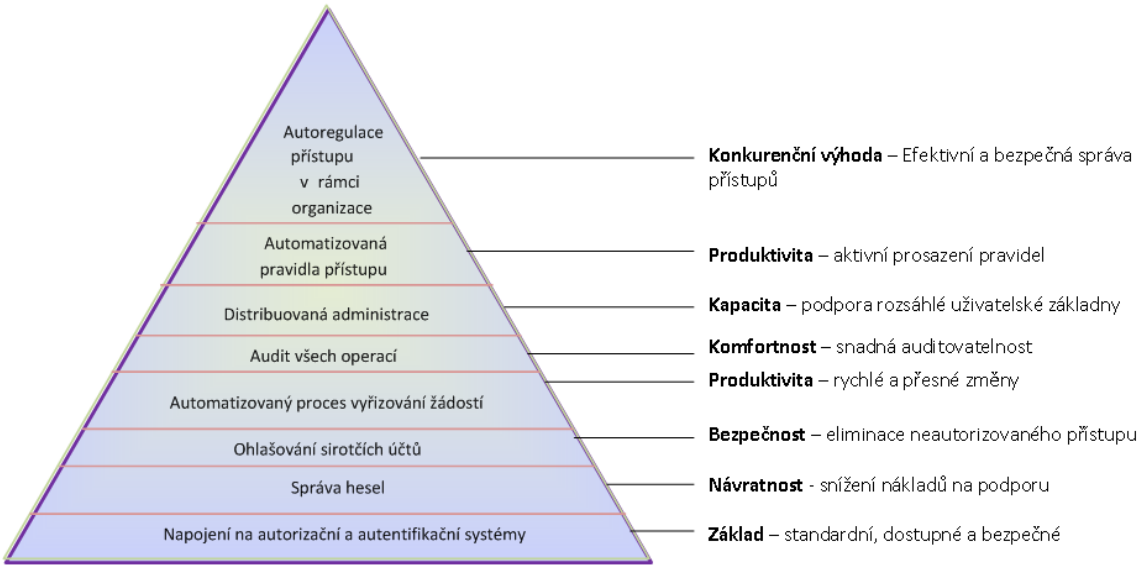
- kdo má přístup k danému zdroji,
- kam může daný uživatel přistupovat,
- kdo autorizoval daný přístup,
- kdy byl přístup povolen,
- jaký přístup byl povolen, změněn nebo zrušen mimo ITIM procesy,
- kdo vlastní neschválený přístup a kdo přístup povolil.

Identity Manager standardizuje a formalizuje procedury pro všechny požadavky na povolení, změnu či zrušení přístupu k danému zdroji. Nabízí pro administrátory možnost flexibilního dotazování a reportování informací z auditního logu. Umožňuje vytvářet dotazy založené na jedné či více podmínkách. Veškeré výstupy jsou ukládány v needitovatelném formátu, jako PDF dokumenty.

3.8. Přínosy implementace Identity Managementu

Identity Management pokrývá celou pyramidu od fyzické úrovně, přes konsolidaci informací, procesní řízení až po regulaci přístupu na základě delegované zodpovědnosti v rámci organizace. Přesto Identity Management zůstává kompaktním produktem, který je možné ihned po instalaci využívat.

[21] Kerberizovaná aplikace – aplikace využívající síťový autentizační protokol Kerberos, který umožňuje uživateli v nezabezpečené síti prokázat bezpečně jeho identitu někomu dalšímu.



Obr. 6. *Rozsah funkčností Identity Managementu*

Přínosy pro organizace obecně:

- zrychlené vyřizování požadavků na změny přístupových oprávnění a výmaz přístupových hesel - přináší úspory na straně administrace i v produktivitě pracovníků,
- snížení chybovosti - jedním předefinovaným administračním zásahem je provedena celá řada akcí automaticky nebo jsou iniciovány procesy,
- zajištění dodržování firemních pravidel - implementovaný systém neumožní jejich porušení,
- identifikace neoprávněného zásahu do cílových systémů,
- možnost monitorování přístupu k aplikacím,
- bezpečnostní administrace je transparentní - administrátoři informačních technologií nemají zodpovědnost za interpretaci požadavku,
- pravidla pro aplikace jsou umístěny na jednom místě - umožňuje auditu efektivnější činnost,
- možnost lépe analyzovat bezpečnostní rizika a reagovat na ně,
- jednodušší implementace organizačních změn.

Běžnému uživateli umožňuje ITIM prostředí provádět operace:

- změnit vlastní informace,
- nastavit kontrolní otázky a odpovědí pro reset hesla,
- zjistit stav svých požadavků.

Vedoucí pracovník má možnost přes web rozhraní provádět následující operace:

- spravovat svoje údaje a hesla jako koncový uživatel,
- spravovat oprávněním, která jsou mu delegována,
- schvalovat nebo zamítat žádosti v rámci workflow,
- delegovat své pravomoci jiné osobě,
- získávat informace prostřednictvím reportů.

Systémy Identity Management zavádějí přehlednost a pořádek do problematiky řízení přístupových oprávnění k informačním zdrojům bez nutnosti zásahu do provozovaných systémů. Díky větší efektivitě a automatizaci procesů v oblasti zabezpečení, správy účtů a auditu lze ve většině případů spočítat i poměrně rychlou návratnost investice, a to již po prvním roce provozování. Dokazují to analýzy renomovaných firem, jako jsou např. META Group nebo Gartner group. Dlouhodobé analýzy společnosti Gartner consulting a dalších společností se zaměřením na Return Of Investment[22] (ROI) v oblasti Identity and Access Management systémů ukazují, že nasazení řešení správy identit vede ke zřejmému a hlavně měřitelnému návratu investic.

3.9. Trendy dalšího rozvoje

V současné době je IT stále častěji chápáno jako služby s propojením na orientaci obchodních cílů podniku nebo organizace. Trendy dalšího vývoje budou směřovat k vývoji Identity Managementu na komplexnější systémy.

Nové trendy Identity Managementu pro organizace se otevírají především v následujících oblastech:

- Identity services,
- obchodně orientovaný Identity Management,
- rozvoj a využití nových platforem a zařízení podporujících Identity Management.

Identity services (služby identit), kde reflektují posun k SOA[23] a koncepcím Web 2.0[24]. Je to změna, která standardní model provozu informačních technologií mění na model

[22] ROI – (Return Of Investment) Návratnost investice.

[23] SOA - (Service Oriented Architecture) Architektura orientovaná na služby je kolekce služeb, které komunikují mezi sebou a ke komunikaci využívají standardizované protokoly a dohodnutá rozhraní.

orientovaný na základě služeb. Patří sem, autentizační služby v interakci s vnějším světem, autentizační služby v podniku, autorizační služby, služby SSO, služby řízení životního cyklu identit, kryptografické služby (digitální podpis, časová razítka a šifrování) a služby na archivaci záznamů a identity informací.

Obchodně orientovaný Identity Management – Management informačních technologií organizací, podniků a agentur je stále častěji prováděn z pohledu obchodních cílů se záměry snižovat náklady, optimalizovat využívání prostředků a řídit odchodní rizika. Jak lze sladit informační technologie s obchodními cíli organizace či podniku definuje soubor praktických postupů ITIL[25]. Postupy jsou založeny na propojení informačních technologií s obchodními cíli a na zabezpečení požadovaných úrovní služeb s primárním zaměřením na spokojenost s využíváním služeb informačních technologií. To směřuje k rozvoji funkcí Identity Managementu, které jsou orientovány na IT service Management, change Management, incident Management, Management auditu a správu bezpečnosti.

Rozvoj a využití nových platforem a zařízení podporujících Identity Management – velmi zajímavým rozvojovým trendem Identity Managementu je jeho propojení s Managementem zařízení. Jedná se především o mobilní telefony, laptopy, PDA[26], atd. a jejich využití jak v podnikových procesech, tak i v mezipodnikových vztazích. Jedná se především o flexibilnější využití těchto zařízení a jejich využití se službami informačních technologií jako jsou SSO a řízení přístupu.

[24] Web 2.0 - Označení pro etapu vývoje webu, kde pevný obsah webových stránek je nahrazen prostorem pro sdílení a společnou tvorbu obsahu.

[25] ITIL – (Information Technology Infrastructure Library) Soubor konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií.

[26] PDA – (Personal Digital Assistant) Kapesní počítač obvykle ovládaný dotykovou obrazovkou.

PRAKTICKÁ ČÁST

4. IMPLEMENTACE IDENTITY MANAGERU VE STÁTNÍ SPRÁVĚ

Implementace Identity manageru ve státní správě byla součástí projektu Autentizace, Autorizace a Auditing portál (dále jen AAA portál). Projekt AAA portál byl jedním z bezpečnostních projektů Implementace bezpečnosti přístupu k datům a službám. Úkolem projektu bylo vytvoření technické infrastruktury přístupového AAA portálu. Přístupový AAA portál měl tvořit jediný přístupový bod ke službám a informacím poskytovaným ve státní správě v rámci AAA prostředí. Klíčovou úlohou byla realizace mechanizmů identifikace, autentizace a autorizace takovým způsobem, aby byl zajištěn právě jen oprávněný přístup oprávněných uživatelů k aplikacím zapojeným do AAA prostředí. Za tímto účelem byla využita kombinace techniky bezpečných komunikačních kanálů, PKI[27] a dalších kryptografických operací. Úlohou AAA portálu bylo také řízení přístupu uživatele k více aplikacím a zdrojům na základě jednoho „přihlášení" – SSO.

Pro realizaci projektu byly vybrány produkty společnosti IBM. IBM Tivoli Identity Manager (dále jen ITIM) je produkt z rodiny IBM Tivoli Software. Byl získán na sklonku roku 2003 akvizicí společnosti Access360 a jmenoval se enRole. Ve státní správě byla nasazena verze ITIM 5.0. V současné době je aktuální verze ITIM 5.1, která podporuje na 50 typů aplikačních konektorů s možností přidat vlastní.

Jako optimální způsob autentizace byla zvolena možnost přes certifikát uživatele podle normy X.509 uložený na PKI čipové kartě. Certifikát uživatele je vydáván interní certifikační autoritou. Žádný jiný způsob autentizace pro uživatele není přípustný.

4.1. Inicializace ITIM

AAA portál je napojen na ostrý HR[28] systém. Iniciátorem spojení je vždy IBM Tivoli Directory Integrator (dále jen ITDI), služba, který synchronizuje data mezi více úložišti. V tomto případě zadává přes webové rozhraní v pravidelných 24- hodinových intervalech pokyn pro vytvoření XML souboru s daty zaměstnanců z personálního systému. Soubor se vždy vytváří změnový, nikoliv úplný. V případě potřeby, např. větších organizačních změn, změně organizačního stromu nebo celé organizační struktury, je ale možné využít i úplný HR import.

[27] PKI – (Public Key Infrastructure) Infrastruktura veřejných klíčů.

[28] HR – (Human Resources) V tomto pojetí myšleno jako systém pro zadávání personálních dat zaměstnanců.

ITIM tuto strukturu načítá přes ITDI a do ITIM jsou zapsána pouze data, kde:

- došlo ke změně,
- mají vyplněného nadřízeného,
- mají vyplněnou lokalitu,
- mají vyplněnou organizační jednotku.

Dále se přes webové rozhraní přenáší soubor s exportovaným organizačním stromem, pokud v něm došlo ke změně.

Fyzicky jsou data uspořádána ve dvou databázích na databázovém serveru a několika replikách na dalších serverech. Databáze obsahuje údaje o Identitách, účtech v ITIM a na připojených systémech, role, politiky, definice workflow a dalších definic objektů ITIM. Veškeré objekty ITIM jsou definovány v určitém místě organizačního stromu. Uvedený princip jednak přispívá k přehlednosti a jednak k bezpečnosti ITIM, neboť umístění objektu v organizačním stromu má vliv na jeho viditelnost nejen pro administrátory, ale i pro ostatní objekty ITIM mezi sebou.

Klíčovou vlastností ITIM je vytváření vazeb mezi definicí osob (objekt Person) a účty na koncových systémech (objekt typu Account). Fyzicky je základem propojení ITIM jako aplikace definice tzv. services, tj. konektorů na koncové ITIM agenty. Následně dochází k propojení Identit s účty na koncových systémech. V konečném stavu je ale vždy na straně ITIM definovaná Identita se svými atributy, umístěním v organizačním stromu, nadřízeným a rolemi a k ní připojenými účty.

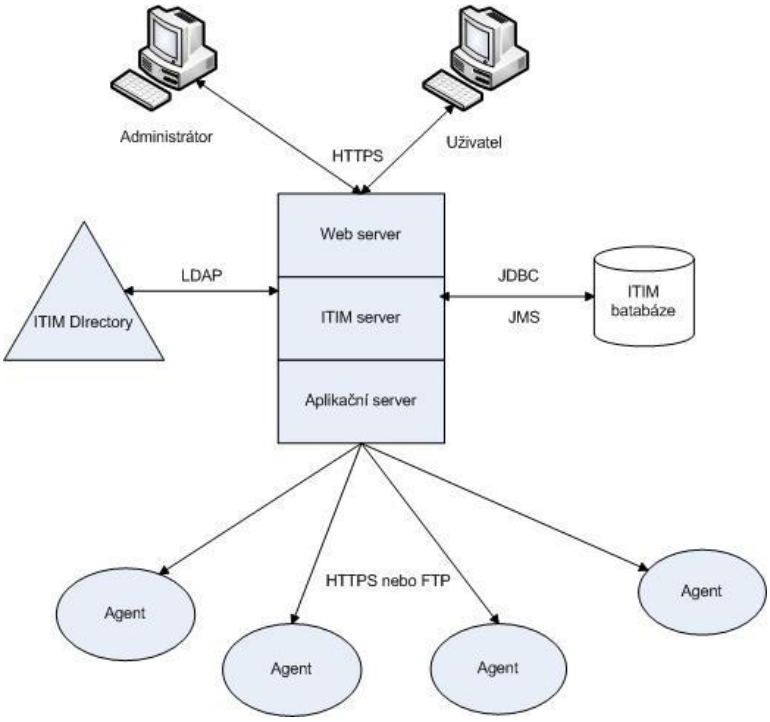
4.2. Architektura ITIM

IBM Tivoli Identity Manager je implementován v prostředí JAVA Aplikačního serveru a pro uložení dat využívá LDAP repository a relační databáze. Pro asynchronní notifikace využívá JMS rozhraní.

Standardně jsou s ITIM dodávány všechny komponenty a ty jsou v rámci funkce ITIM licencovány:

- IBM Directory Server,
- IBM Tivoli Directory Integrator,
- IBM WebSphere Application Server,
- IBM DB/2,
- IBM WebSphereMQ.

Fyzickou architekturu zachycuje obrázek (Obr. 7) s následujícím popisem:
Uživatelé přistupují k Identity manageru prostřednictvím Web prohlížeče a protokolu HTTPS přes Webserver. ITIM Server komunikuje s adresářovým serverem prostřednictvím protokolu LDAP a SSL. K databázi je přistupováno prostřednictvím rozhraní JDBC[29]. Asynchronní operace jsou zajištěny prostřednictvím JMS[30] (WebSphereMQ). Většina agentů je instalována na cílové systémy, ale některé mohou být instalovány na „proxy" systémy.



Obr. 7. *Fyzická architektura Identity manageru*

Dostupnost IM je sice důležitá, nejedná se však o „mission-critical" aplikaci. Z tohoto důvodu je IM umístěno na dvou serverech ve dvou lokalitách se vzájemnou synchronizací.

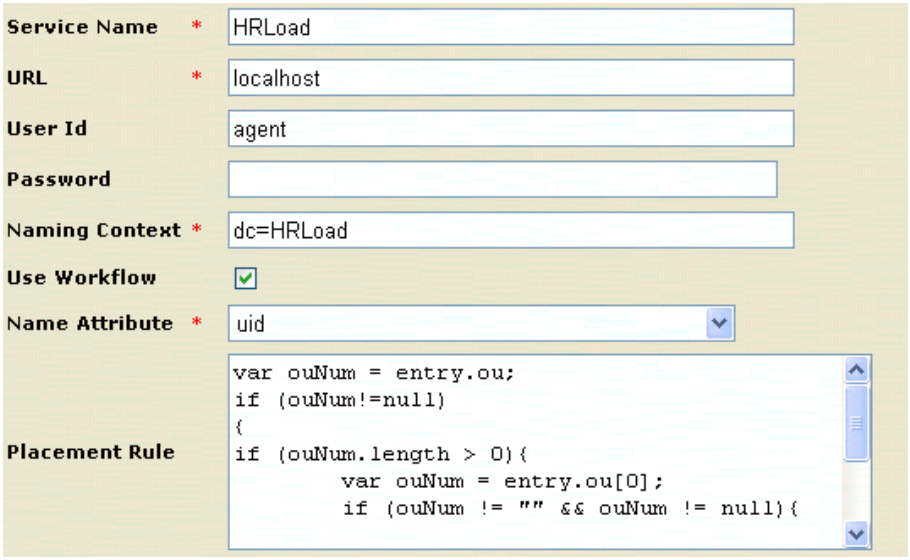
4.3. Konektory – HR, AD, ITIM a jejich komunikace

Pro úplnou funkci AAA portálu, kterého je ITIM částí, je nutná správná funkce tří konektorů:

[29] JDBC – (Java Database Connectivity) Univerzální aplikační rozhraní pro přístup k relačním databázím.

[30] JMS – (Java Message Service) Poskytuje možnost psát programy, které dokáží vytvářet, posílat, přijímat a číst zprávy posílané mezi aplikacemi.

- **HR konektor,** který načítá základní HR data obsahující informace o personách, jejich atributy umístění v organizačním stromě a relaci nadřízený x podřízený,
- **Active Directory konektor,** sloužící pro připojení ITIM a správu uživatele Active Directory domény,
- **ITIM konektor,** jediný povinný konektor, kterým ITIM spravuje své vlastní uživatele a uživatele zákaznického ITIM GUI.



Obr. 8. *Definice HR konektoru v ITIM*

ITIM agent komunikuje se serverem pomocí DSML (Directory Service Markup Language) protokolu a SSL zabezpečení. DSML je světový standard pro prezentaci LDAP v XML. DSML soubor je ASCII XML soubor, který prezentuje fragment LDAP datové struktury týkající se určité identity a operace, které jsou s ní požadovány. Umístění agentů je ve většině případů na cílovém systému, ale existují i konfigurace, kde je agent umístěn na jiném HW úplně mimo systém (databázoví agenti, proxy agent, apod.).

4.4. IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator (dále jen ITDI) je součástí produktu ITIM a používá se na tvorbu adaptérů ITIM do zákaznických aplikací a HR systémů. Je to produkt, jehož cílem je provádět synchronizaci dat uložených v adresářích, databázích, aplikacích, HR systémech a dalších podnikových aplikacích.

V této implementaci se produkt používá pro napojení na zdrojová HR data. ITDI je na ITIM serveru představován službou operačního systému „Tivoli Directory Integrator“.

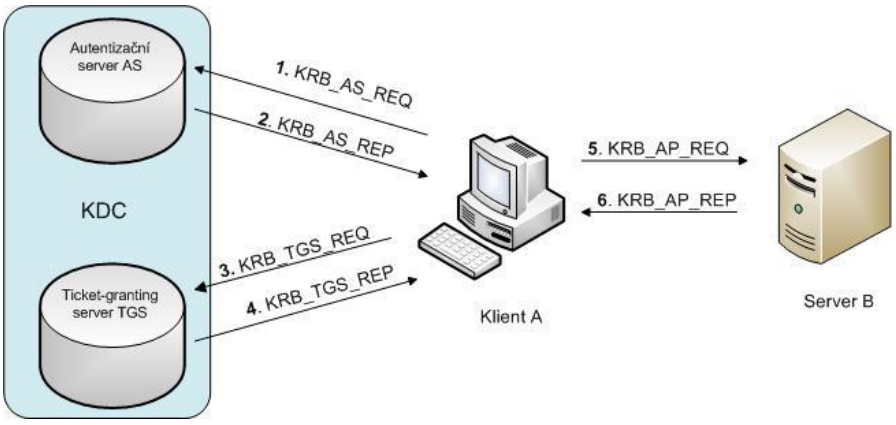
Základní komponenty ITDI jsou:

- **AssemblyLine** - provádí úpravy přijatých dat nebo vytváří zcela nové objekty a na přiřazených místech daný nový informační objekt přidává, aktualizuje nebo ruší,
- **Event Handler** - rozšiřuje flexibilitu komponenty ITDI tím, že umožňuje čekat na určité události, ke kterým došlo v určité infrastruktuře, jako jsou změny v adresáři, příchozí elektronická pošta, záznamy aktualizované v určitých databázích, příchozí stránky HTML z webového serveru nebo prohlížeče a reagovat na ně,
- **Parser** - syntaktické analyzátory pro interpretaci a převod informací do objektu strukturovaných informací, kde jsou jednotlivé části informace přístupné podle jména. Rozšiřitelných syntaktických analyzátorů existuje velké množství např. "hodnoty oddělené čárkou", "pevná šířka sloupce", formát XML nebo lze vytvořit zcela nový.

Konektory s podporou řady protokolů a přístupových mechanismů se dodávají jako součást produktu nebo je lze snadno vytvářet a upravovat.

4.5. Kerberos a proces komunikace

Kerberos je autentizační protokol, který umožňuje vzájemné prokázání identity mezi serverem a uživatelem. Protokol je založen na důvěryhodné třetí straně - KDC[31] serveru, který se skládá z Autentizačního serveru (AS) a Ticket-granting serveru (TGS). Služby jsou samostatné, ale většinou se provozují na stejném stroji. Protokol Kerberos má dílčí služby AS - autentizační služba, TGS - služba na vydávání lístků a CS - služba klient/server.



Obr. 9. *Komunikace protokolem Kerberos*

[31] KDC – (Key Distribution Center) Důvěryhodná třetí strana na které je založen princip Kerberos. Skládá se z dvou logicky oddělených částí, Autentikačního serveru a Ticket-granting serveru, a uchovává databázi tajných klíčů.

Komunikace protokolem Kerberos je znázorněna na Obr. 9 s následujícím popisem. Proces začíná uživatelovým přihlášením do sítě. Z hesla klienta si Kerberos klient jednocestnou funkcí vypočte svůj long-term klíč, který si uloží do bezpečné paměti. Pak Kerberos klient pošle KDC-AS žádost o přidělení lístku (ticketu) KRB_AS_REQ. Ten se skládá z označení uživatele a označení služby, kterou uživatel požaduje. Dále obsahuje předautentizační data, která identifikují uživatele (např. aktuální čas uživatelova počítače). Předautentizační data jsou zašifrována uživatelovým long-term klíčem.(1.) KDC vyhledá uživatele v databázi, přečte si odtud jeho long-term klíč, rozšifruje předautentizační data včetně vloženého času a ověří jejich správnost. Pokud vše souhlasí, vydá pro uživatele přihlašovací klíč relace, zašifruje jej uživatelovým long-term klíčem a vytvoří TGT[32], což je malý zašifrovaný soubor s omezenou platností, který obsahuje klíč sezení, datum a čas expirace a uživatelovu IP adresu. Uloží do něj také přihlašovací klíč relace, přidá autorizační data uživatele a celé to zašifruje svým long-term klíčem. Vznikne tím KBR_AS_REP, kterou pošle zpět Kerberos klientovi běžícím na uživatelově pracovní stanici. Klient pak pomocí svého long-term klíče získá ze zprávy přihlašovací klíč relace a ten si uloží do své bezpečné paměti. Zároveň sem také uloží TGT v takovém formátu, jak ho přijal.(2.) Když uživatel žádá o přístup ke službě na nějakém serveru, vyšle Kerberos klient na uživatelově počítači na KDC žádost o přidělení lístku relace KRB_TGS_REQ. Ten obsahuje uživatelovo označení a autentikátor zašifrovaný uživatelovým přihlašovacím klíčem relace, jméno služby, pro kterou uživatel požaduje přidělit lístek relace a TGT, kterou přidělil KDC-AS. (3.) KDC-TGS obdrží KRB_TGS_REQ a s pomocí svého tajného klíče se dostane k uživatelovu přihlašovacímu klíči relace. Tím rozšifruje uživatelův autentikátor a ověří jeho správnost. Pokud je vše v pořádku, vezme si z TGT uživatelova autorizační data a vytvoří klíč relace, který bude sdílet uživatel s požadovanou službou. Jednu kopii uživatelova klíče relace zašifruje uživatelovým přihlašovacím klíčem relace, druhou kopii pak vloží spolu s autorizačními daty uživatele do lístku relace a zašifruje ho long-term klíčem uživatele. To dohromady tvoří KRB_TGS_REP, který KDC odešle zpět Kerberos klientovi na uživatelovu pracovní stanici, kde Kerberos klient s pomocí uživatelova přihlašovacího klíče relace rozšifruje klíč relace pro požadovanou službu a spolu s lístkem relace si jej uloží do bezpečné paměti. (4.) Po uložení lístku relace se Kerberos klient obrátí na uživatelem požadovanou službu a pošle jí KRB_AP_REQ. Ten

[32] TGT - (Ticket Granting Ticket) Malý zašifrovaný soubor s omezenou platností, který obsahuje klíč sezení, datum a čas expirace a uživatelovu IP adresu.

obsahuje autentikátor zašifrovaný klíčem relace, který sdílí uživatel s požadovanou službou, lístek relace, který dodal KDC-TGS a příznak, který říká, jestli bude také požadována autentizace služby vůči klientovi (vzájemná autentizace). (5.) Uživatelem požadovaná služba rozšifruje lístek relace a dostane uživatelova autorizační data a lístek relace. Tím pak rozšifruje uživatelův autentikátor a ověří jeho správnost (včetně času). Je-li vše v pořádku, zkontroluje nastavení příznaku požadujícího vzájemnou autentizaci. Pokud je uživatelem požadována, vezme se z uživatelova autentikátoru čas, zašifruje se společným lístkem relace a pošle zpět. Kerberos klient na uživatelově straně rozšifruje KRB_AP_REP společným lístkem relace a získaný čas porovná s údajem, který posílal v autentikátoru. Pokud se shodují, klient nadále dané službě důvěřuje. (6.)

4.6. Grafické rozhraní ITIM GUI

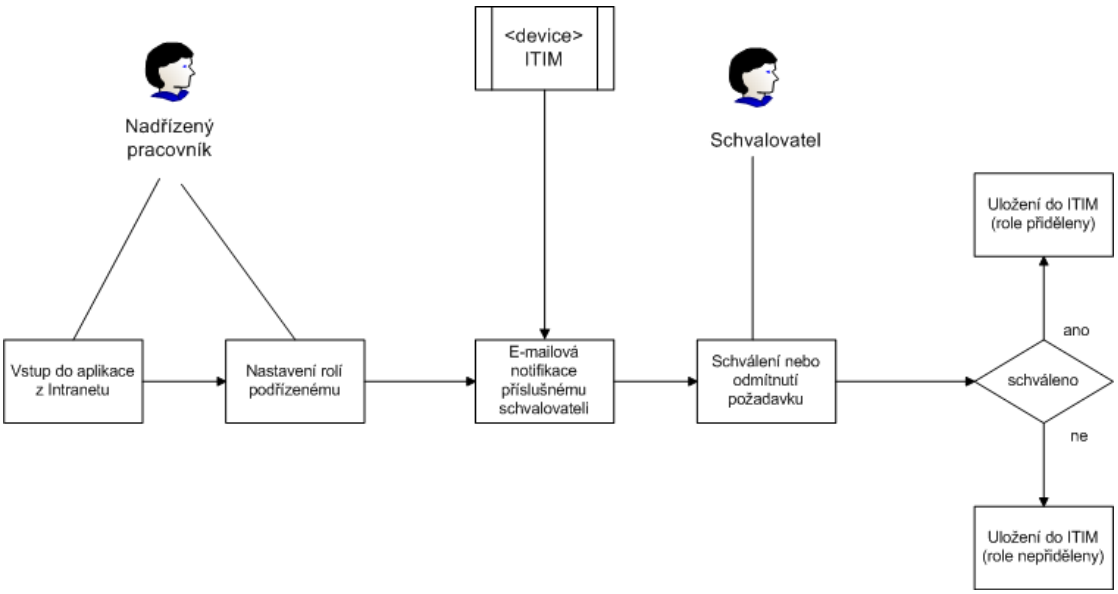
ITIM neumí nastavit požadovaný vzhled a strukturu pro netechnické uživatele, proto vznikla nad ITIM grafická nadstavba, tzv. ITIM GUI. Je to webová aplikace využívající jako zdroj i cíl dat ITIM. Přes ITIM API si vyzvedává z ITIM seznam rolí, zaměstnanců, apod. a vytváří z nich formuláře pro nadřízeného, žádajícího o nějakou roli v aplikaci pro své podřízené.

Vyplněním formuláře s žádostí o role v ITIM GUI se spouští v ITIM schvalovací workflow, které využívá opět ITIM GUI pro pověřené osoby schvalující žádost. Navíc je možné přes ITIM GUI vybrat zástupce vedoucího zaměstnance, tzv. delegovaného zaměstnance, který zastupuje vedoucího zaměstnance v jeho nepřítomnosti. Delegovaný zaměstnanec má v rámci delegace stejná přístupová oprávnění v ITIM GUI jako osoba, která mu delegaci nastavila. Může žádat o role, schvalovat přidělení rolí, odebírat role atd. Delegací je mimo jiné zajištěno i schválení požadavků ve stanovené době (např. šest kalendářních dnů). Nedojde tak k eskalaci nevyřízeného požadavku na kompetentní osobu nebo správce ITIM a opětovnému žádání o příslušnou roli.

ITIM GUI definuje 5 případů užití:
UC01 – Změna rolí pro podřízeného
UC02 – Schvalování žádostí
UC03 – Výběr zástupce
UC04 – Hromadná změna rolí
UC05 – Zobrazení rolí podřízených

Na obrázku (Obr. 10) je celkový pohled na operace, které se provádějí přes GUI. Nejprve nadřízený pracovník spustí GUI prostřednictvím odkazu z intranetu (klikne na odkaz, GUI se spustí v MSIE). Poté nastaví role jednomu nebo více podřízeným a odešle požadavek. GUI uloží změny do ITIM, čímž se spustí workflow, které pošle notifikaci schvalovateli. Ten spustí GUI a schválí či odmítne požadavek na schválení rolí. Odebrání role nepodléhá workflow a je vyřízeno okamžitě.

Dále může nadřízený pomocí GUI zvolit svého zástupce a zobrazit stav přidělených rolí podřízeným.



Obr. 10. *ITIM GUI – přehled funkcí*

4.7. Situace před implementací

4.7.1. Nástup nového zaměstnance

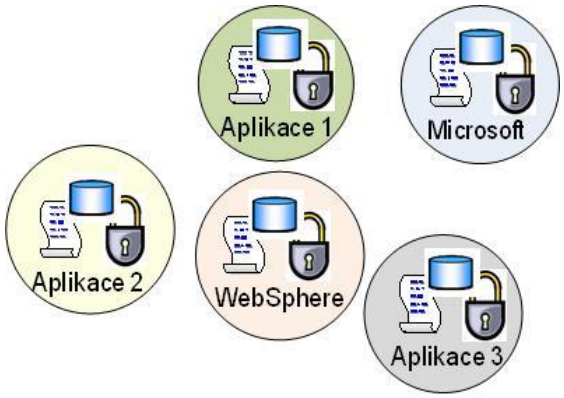
Nastoupí nový zaměstnanec a na personálním oddělení je zaregistrován do HR systému. Zaměstnanec dostane přidělené jednoznačné originální zaměstnanecké číslo a je zařazen do organizační struktury. Administrátor informačních technologií vytvoří zaměstnanci uživatelský účet v Active Directory, přihlašovací login, vygeneruje heslo a vytvoří e-mailovou schránku. Na personálním oddělení je uživateli vydána čipová karta pro docházkový systém.

4.7.2. Aplikace před implementací

Před nasazením ITIM bylo mnoho aplikací, operačních systémů a databází, kde každá/ý měl/a svou správu

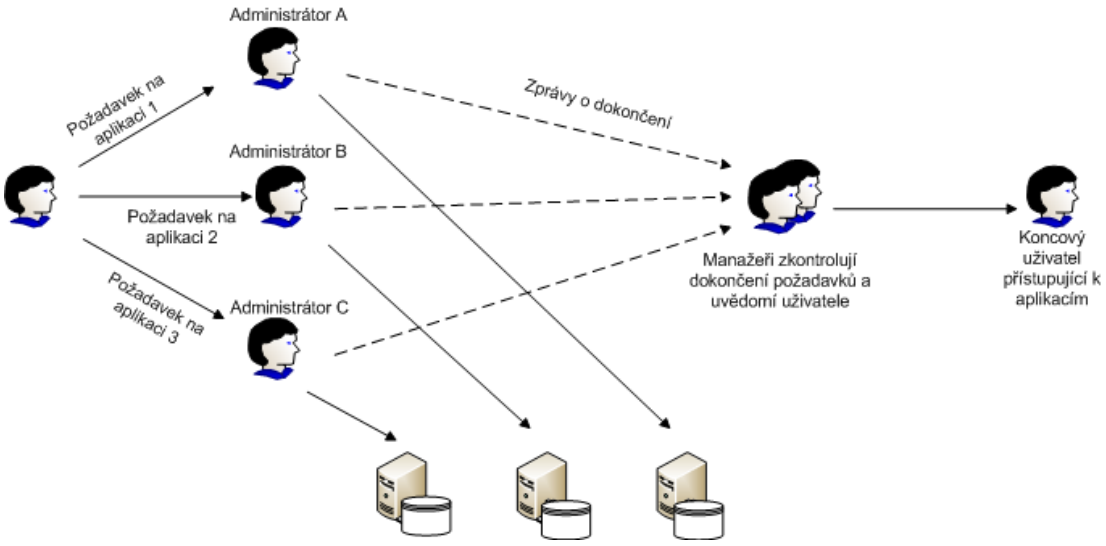
- uživatelů,
- hesel,
- přístupových oprávnění,
- své vlastní administrátory,
- svou vlastní bezpečnostní politiku.

Řešení bylo nekoordinované, aplikace byly na sobě nezávislé ostrůvky.



Obr. 11. *Stav aplikací před implementací Identity manageru*

Po absolvování uvedeného kolečka v kapitole Nástup nového zaměstnance, nadřízený nového zaměstnance zažádá příslušné osoby o schválení přístupů do jednotlivých aplikací. V každém systému a aplikaci se založí nový uživatel a přidělí se mu přístupová oprávnění. Následně zaměstnanec obdrží přístupová jména a hesla do jednotlivých aplikací.

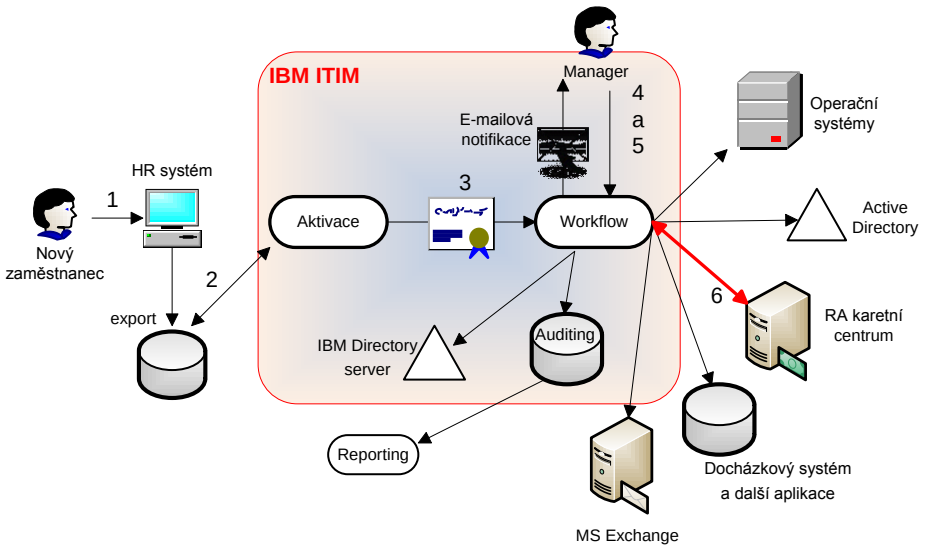


Obr. 12. *Přidělování rolí pře implementací ITIM*

4.8. Situace po implementaci

4.8.1. Nástup nového zaměstnance

Průběh nástupu nového zaměstnance po implementaci IM je graficky znázorněn na obrázku (Obr. 13).



Obr. 13. *Stav po implementaci Identity manageru*

Nastoupí nový zaměstnanec, jeho cesta vede na personální oddělení (1), kde ho zaregistrují do svého HR systému. Zaměstnanci je přiděleno originální zaměstnanecké číslo a je zařazen do organizační struktury. Následně mu vydá zaměstnanecký průkaz a čipovou kartu s instalovanými certifikáty, umožňující mu pohyb po budově i kontrolovaný přístup

k aplikacím a datům. Celý další proces je automatizován. Aktivace zjistí nový záznam (2) v HR systému a předá ho do Identity manageru k nastavení účtů zaměstnance a uživatelských atributů (3). Identity manager poté inicializuje tzv. workflow se žádostí o schválení pro odpovědné osoby (4) a po schválení (5) aktivuje účty uživatele v operačních systémech, aplikacích, elektronické poště apod. (6). Celý proces je auditován (7).

4.8.2. Založení uživatele v ITIM

Identity manager nabízí nástroje na automatizaci operací souvisejících se správou účtů. Typickým příkladem je zakládání účtu novému zaměstnanci:

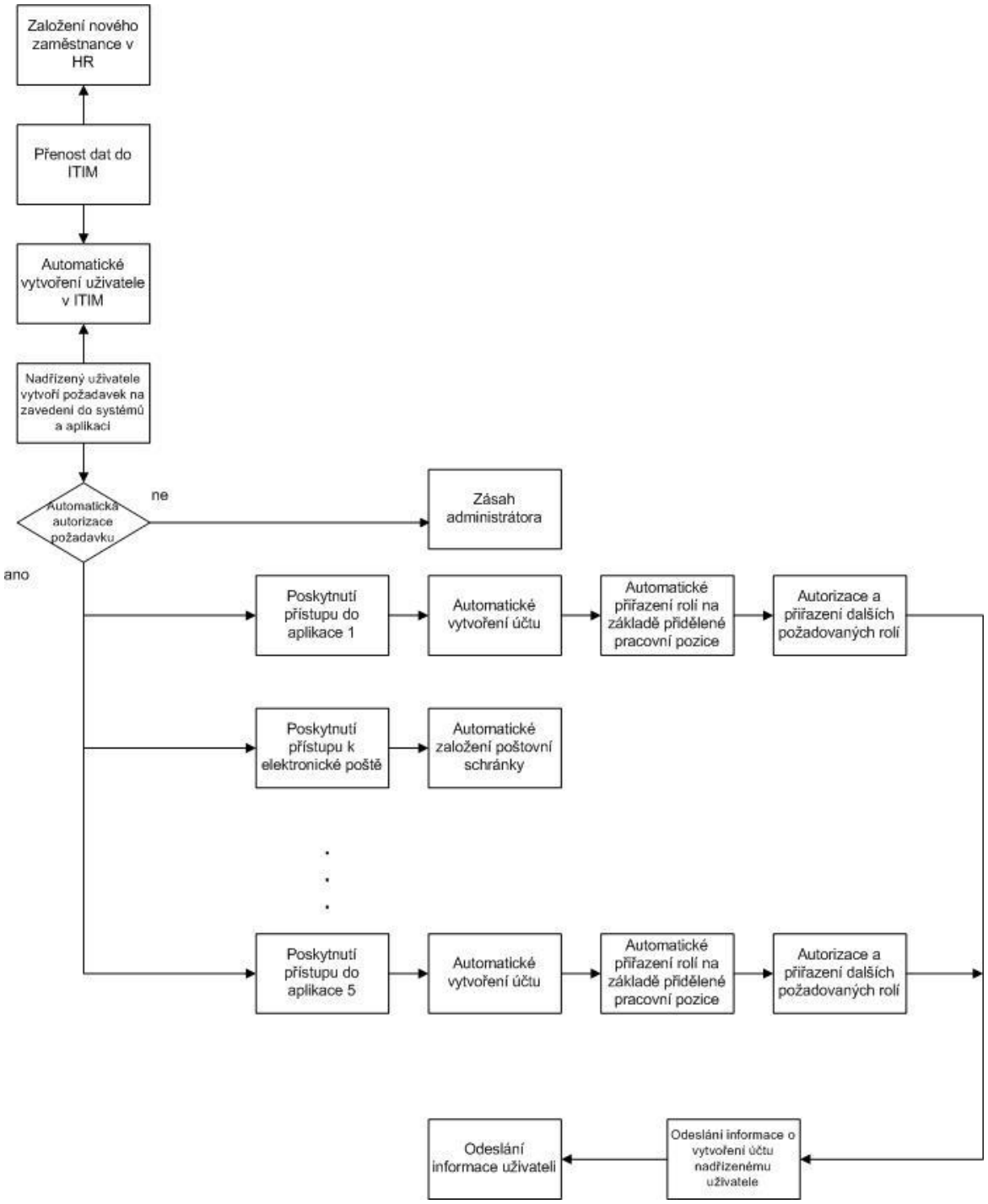
- na základě informací z personálního systému je založen uživatel v ITIM,
- nadřízený zaměstnance žádá prostřednictvím formuláře v ITIM o přidělení přístupů do systémů dle jeho pracovní pozice,
- následně ITIM provádí automatické vyhodnocení žádosti a ověření osoby, která žádost autorizovala (dle platné organizační struktury),
- na základě platné žádosti, pracovní pozice a zařazení v organizační struktuře jsou zaměstnanci automaticky přiřazeny role definované v ITIM. Těmto rolím jsou prostřednictvím Provisioning Policy[33] a Services[34] pro jednotlivé systémy a aplikace definována konkrétní přístupová oprávnění,
- vyžaduje-li uživatel ke své činnosti ještě další přístupová oprávnění, které přímo nevyplývají z jeho pracovního zařazení, musí nadřízený zaměstnance o příslušné role zažádat.

ITIM během zpracování požadavku realizuje kontrolu, zda požadavek splňuje podmínky dané Provisioning Policy. Pokud podmínky nejsou splněny, je požadavek odmítnut. O úspěšném i neúspěšném dokončení požadavku je informován pracovník i jeho nadřízený.

Celou operaci znázorňuje následující vývojový diagram:

[33] Provisioning Policy – politiky přístupových oprávnění

[34] Services - cílové systémy (operační systém, databáze a aplikace)

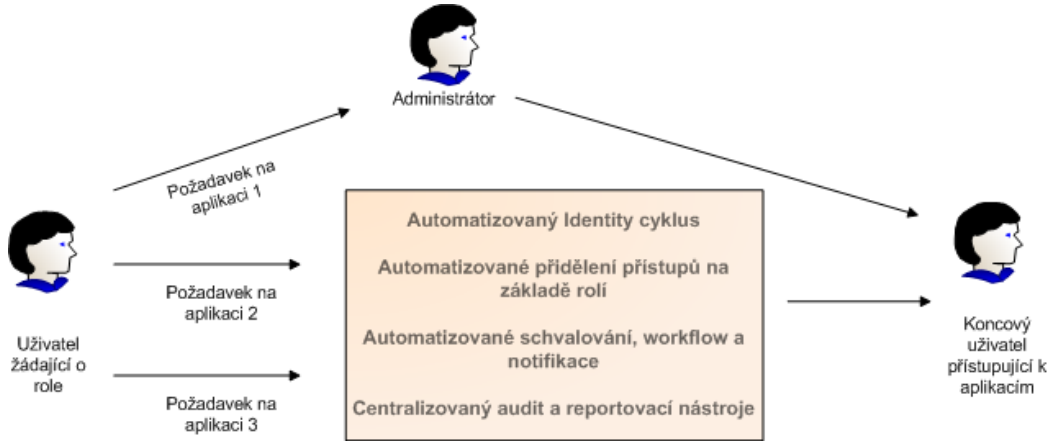


Obr. 14. *Vývojový diagram k založení uživatele v ITIM*

4.8.3. Aplikace po implementaci

Po nasazení ITIM se systém chová jako celek, ke kterému se přistupuje a který se řídí z jednoho místa. Pro přístup do aplikací již není třeba využívat dalších přihlašovacích údajů.

Uživatel se autentizuje čipovou kartou a aplikace mu přístup umožní, nebo případně přístup odepře. V obou případech je přístup zaznamenán do auditovacího logu. Uživatel si již nemusí pamatovat žádná hesla, je autentizován automaticky.



Obr. 15. *Stav aplikací po implementaci Identity manageru*

4.9. Audit

Audit v systému ITIM je standardně zapnutý a jeho úroveň je řízena vlastním konfiguračním souborem. Požadovaná úroveň auditu se nastavuje editací souboru. Audit v systému ITIM se týká všech akcí, které provádí ITIM uživatel (včetně ITIM administrátora) a které se týkají jak změn v nastavení systému, tak změn v nastavení spravovaných identit. Konkrétně jsou pokryty oblasti:

- **ACI Management** – audit oblasti pro přidělování oprávnění pro práci s ITIM a jeho GUI,
- **User Management** – audit oblasti pro vytváření, změny a rušení Identit, Role a organizačního stromu, který pokrývá také oblast delegování autority,
- **Policy Management** – audit oblasti pro vytváření, změny a rušení ITIM politik,
- **Service Management** – audit oblasti pro vytváření, změny a rušení klientských propojení na podřízené systémy a audit o provedených rekonciliacích,
- **Account Management** – audit oblasti pro vytváření, změny a rušení účtů pro existující identity a reset hesel,
- **Configuration Management** – audit oblasti pro vytváření, změny a rušení globálních nastavení ITIM,
- **Authentication Events** – audit oblasti pro pokrývající přístup (přihlášení) k systému ITIM.

Zkonfigurovaný auditní subsystém ukládá své informace do databáze aplikace ITIM. Auditní tabulkové schéma je složeno ze čtyř základních tabulek:

- **audit_event** – základní tabulka obsahující povinná pole všech auditních záznamů,
- **audit_mgmt_target** – tabulka obsahující doplňující data pro vybrané záznamy z tabulky audit_event jako je např. přestup osoby mezi odděleními,
- **audit_mgmt_delegate** – tabulka obsahující doplňující data pro vybrané záznamy z tabulky audit_event (např. informace spojené s delegováním autority),
- **audit_mgmt_provisioning** – tabulka obsahující doplňující data pro vybrané záznamy z tabulky audit_event (např. informace spojené se zpracováním uživatelských účtů).

Vlastní informace týkající se auditu jsou k dispozici v ITIM administrátorském rozhraní. Datové věty auditu obsahují identitu uživatele, typ události, čas události a případně i data o události. Souhrn všech těchto informací může být použit pro generování reportů z auditních záznamů. Kromě vlastních auditních a reportovacích záznamů, které si vytváří přímo ITIM a které primárně slouží pro prezentaci, existují i další logy, které poskytují cenné informace v případě implementace a ladění celého systému.

4.10. Přínosy implementace ITIM pro státní správu

- Jednotný administrativní proces napříč organizací /aplikacemi / platformami,
- jednotné prosazování bezpečnostních politik napříč organizací,
- jednodušší implementace organizačních změn,
- automatizace rutinních úloh,
- redukce celkových nákladů na administraci uživatelů,
- přehlednější systém přístupových oprávnění znamená méně bezpečnostních rizik - uživatelé mají pouze taková oprávnění ke službám a datovým zdrojům, které potřebují ke své práci,
- řešení problémů s účty, které kdysi byly pro uživatele zavedeny a v současné době je již žádný oprávněný uživatel nepoužívá,
- jednodušší a lépe dokladovatelný audit,
- centralizované vytváření auditních záznamů o přidělování přístupových oprávnění.

ZÁVĚR

V současné době rozvoje a zdokonalování informačních technologií se klade stále větší důraz na oblast bezpečnosti informačních a komunikačních technologií. Bezpečnou autentizaci uživatele lze již považovat za součást ochrany informačních systémů a s tím spojené ochrany dat a osobních údajů. Neboť špatně realizovaná autentizace může přímo představovat vážnou bezpečnostní díru do systému a následné zneužití citlivých údajů a dat obecně. Bezpečnou autentizaci a ochranu dat v dnešní době řeší téměř všechny společnosti, organizace a sdružení, průmysl komerční bezpečnosti nevyjímaje.

V teoretické části bakalářské práce jsou popsány nejběžnější autentizační metody a řešení jednotného autentizačního systému – Identity Managementu. Metody autentizace dělíme na slabé a silné. Mezi slabé metody patří zejména využívání hesel. Za silné autentizační metody jsou dnes označovány metody, které využívají elektronické tokeny a biometrické údaje. Při využívání biometrických dat, ale nesmíme zapomínat na to, že patří mezi citlivé osobní údaje a podléhají zákonu č.101/2000 Sb., o ochraně osobních údajů, a jeho pozdějším novelizacím. Biometrická data uložená v databázích je z tohoto důvodu třeba šifrovat. Z analýz, které je třeba provést před implementací Identity Managementu je patrné, že jeho zavádění je pro organizaci, společnost či agenturu velkou výzvou, protože většina používaných aplikací má pravděpodobně svá vlastní úložiště identit s autentizačními schématy. Nikde však již není řečeno, že musejí být organizovány standardním způsobem. Úspěšná implementace správy identit vyžaduje pořádný kus práce a určitou předvídavost. Na straně jedné si je třeba uvědomit, že snížením komplexity zabezpečení práci neusnadňujeme jen správcům informačních technologií v dané organizaci či agentuře, ale i hackerům a dalším zločincům. Hlavním rizikem představujícím lákavý cíl jsou centralizované operace. Pokud se případnému útočníkovi podaří zkompromitovat bezpečnost a proniknout do systému Identity Managementu, může si zde vytvořit vlastní identitu se všemi právy a získat tak neomezený přístup do celé vnitřní sítě organizace. Na straně druhé však dobře spravované identity obnášejí především lepší kontrolu přístupu uživatelů a to se projeví zejména ve sníženém riziku vnitřních a vnějších bezpečnostních narušení. Systém pro správu identit může rovněž zlepšit dodržování souladu s vládními nařízeními, neboť poskytuje nástroje k implementaci komplexního zabezpečení, kvalitního auditu a vytvoření vlastních přístupových pravidel.

Praktická část popisuje implementaci systému pro jednotnou správu identit, konkrétně produktu IBM Tivoli Identity Managementu ve státní správě, její přínosy pro IT oddělení, vedoucí management, ale i běžného uživatele.

ZÁVĚR V ANGLIČTINĚ

In the development and improvement of information technology today the main focus is set on the safety of information and communication technologies. Secure user authentication could be considered as part of the protection of information systems and associated data protection and personal data. For poorly implemented authentication may directly pose a serious security hole in the system and subsequent misuse of sensitive information and data in general. Nowadays almost all companies, organizations and associations, including the commercial security industry have to solve issues related to secure authentication and data protection.

The theoretical part of the thesis describes the most common authentication methods and solution of a single authentication system - Identity Management. Authentication methods are divided into weak and strong. One important point to mention here: whenever biometric data is used, we must not forget all sensitive personal data is subject to the Act No.101/2000 Coll. on personal data protection, and any amendments to amendments. This is the reason, why biometric data stored in databases should be encrypted. Fact is, that any implementation of Identity Management means a real challenge for the organization, company or agency because most used applications is likely to store their own identities, authentication schemes. However, there is no guarantee, they must be organized in a standard way. Successful implementation of identity management requires proper attitude and some foresight to say the least. On the one hand you should be aware that reducing the complexity of security just does not facilitate the work of information technology managers in the organization or agency, as well as hackers and other criminals. The main risks of presenting a tempting target are centralized operations. If a potential attacker can compromise the safety and penetrate into the Identity Management, he can also create his own identity with all the rights and get unlimited access to the entire organization's internal network. On the other hand, well-managed identities primarily provide a better control of user access and this is especially true in a reduced risk of internal and external security breaches. Identity management system can also improve compliance in accordance with governmental regulations, as it provides the tools to implement a comprehensive security audit quality and to create customized access rules.

The practical part describes the implementation of a uniform system for identity management, specifically the IBM Tivoli Identity Management in public administration, the benefits for the IT department, head of management, but the average user.

SEZNAM POUŽITÉ LITERATURY

[1] MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autentizace uživatelů a autorizace elektronických transakcí*: *příručka managera*. Praha: Tate International, 2007, 318 s. Příručka manažera, 8. ISBN 978-808-6813-141.

[2] BÜCKER, Axel. *Identity Management design guide with IBM Tivoli identity manager*. 1st ed. Austin, Tex.: IBM International Technical Support Organization, 2003, 414 s. IBM redbooks. ISBN 07-384-5332-3.

[3] BÜCKER, Axel. *Enterprise security architecture using IBM Tivoli security solutions*. 2nd ed. San Jose, Calif.: IBM, International Technical Support Organization, 2004, 660 s. ISBN 07-384-9897-1.

[4] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-802-5126-196.

[5] MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2., přeprac. a dopl. vyd. Praha: C. H. Beck, 2004, 606 s. ISBN 80-717-9878-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Active directory	Adresářový server, kam se ukládají informace o entitách v prostředí Microsoft.
Adresářové služby	Adresářovou službou se rozumí specializovaná aplikace pro ukládání dat, jejich organizaci a přístup k nim. Data jsou obvykle uložena ve formě položek, přičemž každá položka obsahuje několik atributu.
Cookie	Malý textový soubor vytvářený webovým serverem a ukládaný v počítači prostřednictvím prohlížeče.
CRL	(Certificate revocation list) Seznam zneplatněných certifikátů.
DMZ	(demilitarizovaná zóna) Část informačního systému, kde se obvykle nachází zařízení, která zprostředkovávají určité služby jak pro prostředí vnitřní, tak pro prostředí vnější sítě.
GSM	(Globální Systém pro Mobilní komunikaci) Standard pro mobilní telefony.
HR	(Human Resources) V tomto pojetí myšleno jako systém pro zadávání personálních dat zaměstnanců.
Identita	Totožnost. Digitální označení entity takovým způsobem, který umožnuje jeho rozlišení od jiných entit.
ITIL	(Information Technology Infrastructure Library) Soubor konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií.
ITDI	(IBM Tivoli Directory Integrator) Služba, která synchronizuje data mezi více úložišti.
JDBC	(Java Database Connectivity) Univerzální aplikační rozhraní pro přístup k relačním databázím.
JMS	(Java Message Service) Poskytuje možnost psát programy, které dokáží vytvářet, posílat, přijímat a číst zprávy posílané mezi aplikacemi.
KDC	(Key Distribution Center) Důvěryhodná třetí strana na které je založen princip Kerberos. Skládá se z dvou logicky oddělených částí, Autentikačního server a Ticket-granting Serveru, a uchovává databázi tajných klíčů.

Kerberizovaná aplikace	Aplikace využívající síťový autentizační protokol Kerberos, který umožňuje uživateli v nezabezpečené síti prokázat bezpečně jeho identitu někomu dalšímu.
KRB_AS_REQ	(Kerberos Authentication Service Request) Služba pro zaslání žádosti o přidělení ticketu TGT.
KBR_AS_REP	(Kerberos Authentication Service Reply) Služba zasílající zašifrovaný TGT.
KRB_TGS_REQ	(Kerberos Ticket-granting Service Request) Služba, která zasílá žádost na KDC o zaslání lístku relace pro danou službu.
KRB_TGS_REP	(Kerberos Ticket-granting Service Reply) Služba pro zaslání lístku relace Kerberos klientovi na uživatelovu pracovní stanici.
KRB_AP_REQ	(Kerberos Application Request) Služba zasílající autentikátor zašifrovaný klíčem relace, který sdílí uživatel s požadovanou službou a lístek relace, který dodal KDC-TGS.
KRB_AP_REP	(Kerberos Application Reply) Služba, která potvrdí nastavení příznaku požadujícího vzájemnou autentizaci.
LDAP	Přístupový protokol mezi klientem a adresářovým serverem (X.500). V současné době pod pojmem LDAP nerozumíme pouze komunikační protokol, ale i vlastní adresářový server.
Middleware	Počítačový software, který spojí komponenty softwaru nebo aplikace.
OneID	Služba zabezpečené identifikace.
OTP	(One Time Password) Jednorázové heslo vygenerované pouze pro jedno použití.
PDA	(Personal Digital Assistant) Kapesní počítač obvykle ovládaný dotykovou obrazovkou.
PIN	Personal Identification Number - Osobní Identifikační Číslo.
PKI	(Public Key Infrastructure) Infrastruktura veřejných klíčů.
Provisioning Policy	Politiky přístupových oprávnění
RBAC	(Role Based Access Control) Bezpečnostní model, který uživatele rozděluje do skupin podle jejich rolí.
ROI	(Return Of Investment) Návratnost investice.

RSA token	USB zařízení zobrazující šestimístný kód pro potvrzení autentizace, který se mění každou minutu.
Řízení identity	(Identity Management) Strategie zahrnující procesy a postupy. Slouží k identifikaci entity (např. uživatele) během jejího pracovního cyklu. Řízení identity definuje aplikování rolí a pravidel.
Services	Cílové systémy (operační systém, databáze a aplikace)
Session	(nebo-li relace) Je permanentní síťové spojení mezi klientem a serverem, zahrnující výměnu paketů.
SIM karta	(Subscriber Identity Module) Účastnická identifikační karta která slouží pro identifikaci účastníka v mobilní síti.
SIM toolkit	Technologie umožňující nahrávání a provozování aplikací v mobilním telefonu.
SMS	(Short Message Service) Krátká textová zpráva. Jako služba je dostupná ve většině mobilních telefonů.
SOA	(Service Oriented Architecture) Architektura orientovaná na služby je kolekce služeb, které komunikují mezi sebou a ke komunikaci využívají standardizované protokoly a dohodnutá rozhraní.
SSL	(Secure Sockets Layer) Služba sloužící k šifrování spojení pro protokol http.
SSO	(Single Sign On) Systém jednorázového přihlašování – uživatel se autentizuje do systému pouze jedenkrát, jeho identita je pak předávána a uznávána jednotlivými aplikacemi, databázemi a operačními systémy.
TGT	(Ticket Granting Ticket) Malý zašifrovaný soubor s omezenou platností, který obsahuje klíč sezení, datum a čas exspirace a uživatelovu IP adresu.
USB	(Universal Serial Bus) Univerzální sériová sběrnice pro připojení periferií k počítači.
Web 2.0	Označení pro etapu vývoje webu, kde pevný obsah webových stránek je nahrazen prostorem pro sdílení a společnou tvorbu obsahu.

SEZNAM OBRÁZKŮ

Obr. 1. *Funkce One Time Password* 20

Obr. 2. *Architektura Identity Management* 25

Obr. 3. *Role Based Access Control* 26

Obr. 4. *Systém Identity manager* 28

Obr. 5. *Životní cyklus identity* 30

Obr. 6. *Rozsah funkčností Identity Managementu* 32

Obr. 7. *Fyzická architektura Identity manageru* 38

Obr. 8. *Definice HR konektoru v ITIM* 39

Obr. 9. *Komunikace protokolem Kerberos* 40

Obr. 10. *ITIM GUI – přehled funkcí* 43

Obr. 11. *Stav aplikací před implementací* 44

Obr. 12. *Přidělování rolí pře implementací ITIM* 45

Obr. 13. *Stav po implementaci Identity manageru* 45

Obr. 14. *Vývojový diagram k založení uživatele v ITIM* 47

Obr. 15. *Stav aplikací po implementaci Identity manageru* 48