Identity a Access Management

Organizace a komunikace projektu od plánu k používání

František Křesák
Česká správa sociálního zabezpečení

Marta Vohnoutová
Siemens IT Solutions and Services

SIEMENS

Konference ISSS
6. - 7. dubna 2009



Lidé na prvním místě ...

Identity a Access Management/Obsah

1/ Identity management - jak to vidí dodavatel

- Těžké začátky
- Jak najít společnou řeč
- Proof of concept
- Workflow a jeho změny
- Ach ta personální data
- Vše o disciplíně

2/ Identity management - jak to vidí odběratel

- Heterogenní prostředí v ČSSZ
- Problémy s bezpečností v heterogenním prostředí
- Vytvoření AAA prostředí
- Závěr a shrnutí

Jak to vidí dodavatel

SIEMENS

Problémy s údržbou v heterogenním prostředí

Ve většině větších firem a organizací existuje heterogenní prostředí.

- Různé aplikace na různých OS, různých DTB, centralizované, decentralizované i lokální, s přístupy přes terminál, klient server, webové rozhraní.
- Každá platforma, příp. i skupina OS, DTB, skupina aplikací má svou:
  - vlastní správu,
  - vlastní seznam uživatelů a jejich uživatelské oprávnění,
  - vlastní bezpečnostní politiku atd.

Jak to vidí dodavatel

SIEMENS

Problémy s údržbou v heterogenním prostředí

- Správa je náročná, ovládání aplikací a přístup k datům klade nároky jak na správce systémů, tak na vlastníky dat i běžné uživatele.
- Ani pro celkovou bezpečnostní politiku organizace není tento stav vhodný.

Jak to vidí dodavatel

SIEMENS

Cíle nasazení

- Vytvoření jednotné autentizace uživatele v rámci IS úřadu či společnosti.
- Centrální správa uživatelských identit.
- Vytvoření jednotného systému autorizace uživatelů a přidělování autorizačních oprávnění.
- Vytvoření centrálního přístupového bodu k aplikacím.
- Vytvoření centrálního auditovacího systému – auditovací systém bude zaznamenávat přístup ke všem aplikacím integrovaným do IAM.
- Zmapování aplikací z hlediska jejich integrace do IAM a definování požadavků na nové aplikace pro jejich integraci do IAM.

Jak to vidí dodavatel

SIEMENS

Těžké začátky I.

- Odběratel a dodavatel si věci představují jinak.
- Zavedeni IAM klade velké nároky i na odběratele, který musí měnit zavedené způsoby a učit se nové.
- IAM není krabicový produkt, ale integrační projekt, který výrazně zasáhne do chování celé organizace. Protože jsme však v konkurenčním prostředí, ani dodavatel neslibuje „pot a slzy".
- Změny, změny, změny. Ne všechny činnosti u odběratele jsou zmapovány.
- I odsouhlasené se může měnit – třeba proto, že odběratel nepochopil plně dopad.
- Zmapování aplikací z hlediska jejich integrace do IAM a definování požadavků na nové aplikace pro jejich integraci od IAM.

Jak to vidí dodavatel

SIEMENS

Těžké začátky II.

- IAM ovlivňuje vlastnosti integrovaných aplikací.
- Správnost personálních a jiných vstupních dat je základem.
- IAM je ve středu dění. Nesprávná data či špatně nastavené filtry na síti ... – IAM je vždy první na vině.
- Důvěřuj a prověřuj! Nasazení IAM musí vždy počítat s dlouhým obdobím testování.
- I po dlouhé době testování se může ještě objevit „kostlivec ve skříni".
- IAM je destruktivní systém – zpočátku se nastavuje systém MARK, až potom CORRECT.

Jak to vidí dodavatel

SIEMENS

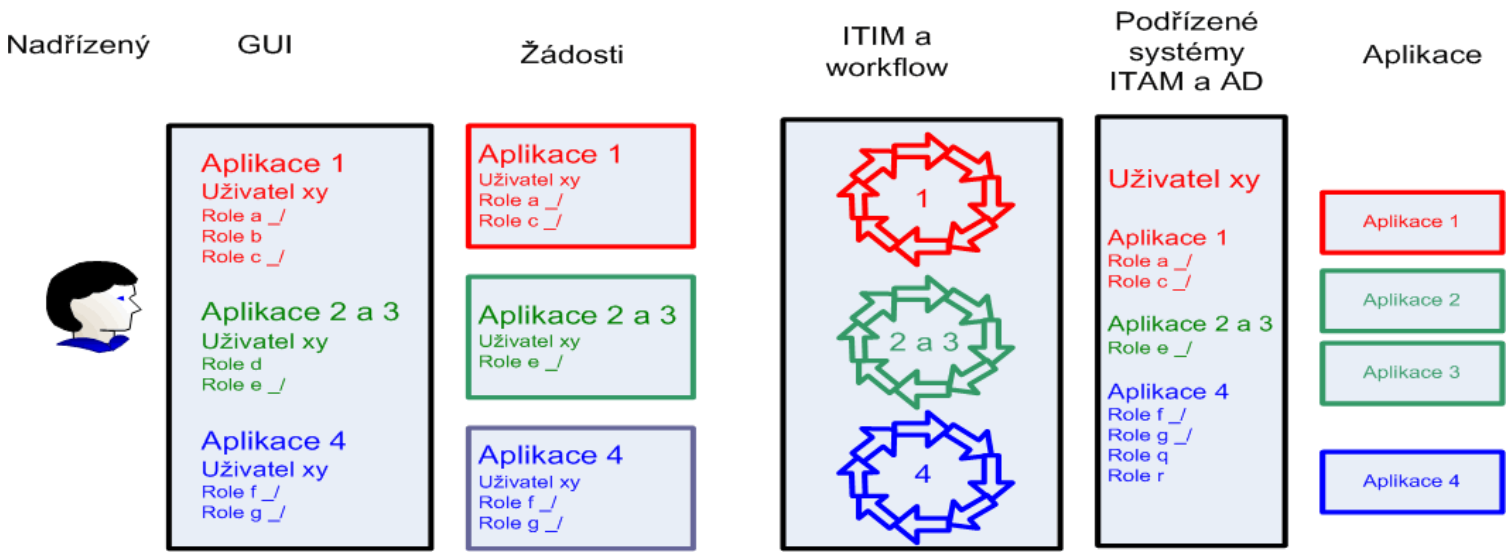
Proof of Concept = POC

- POC musí být jednoduché.
- Zvolíme nejjednodušší operace v IAM a nastavíme je na testovacím prostředí.
- Na POC pochopí odběratel základní filozofii IAM.
- Teprve schválením POC fakticky projekt startuje.

Jak to vidí dodavatel

SIEMENS

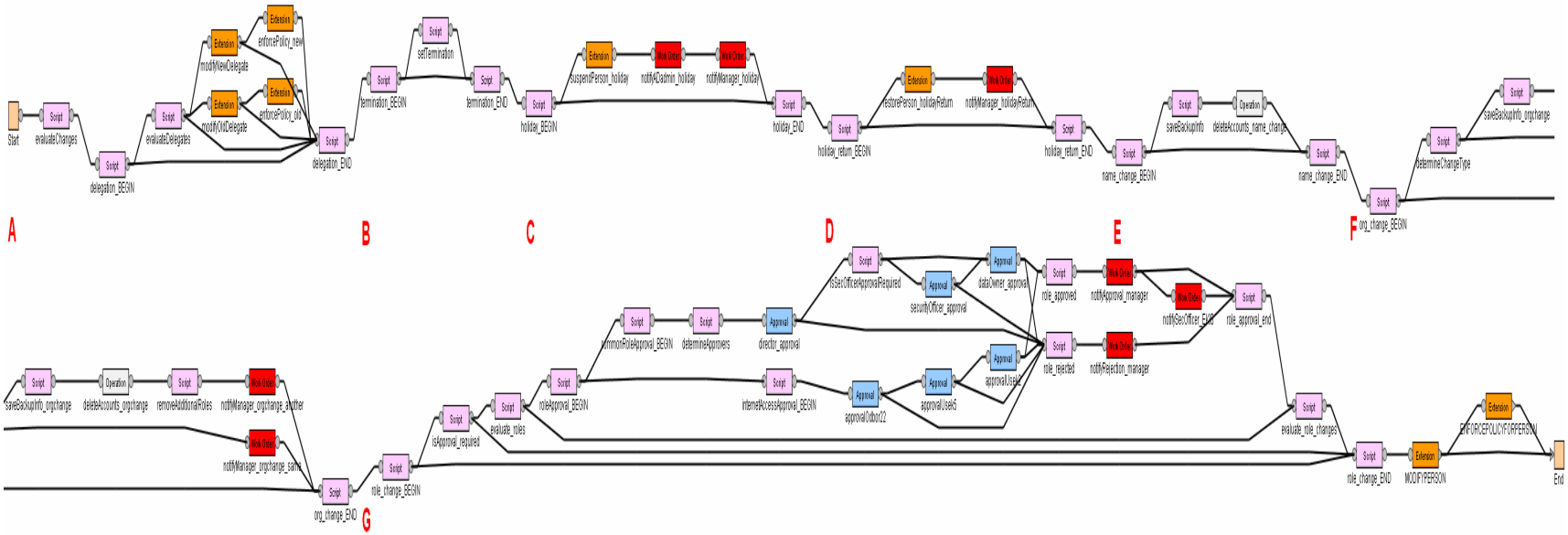
Schvalovací worklow je základ



Jak to vidí dodavatel

SIEMENS

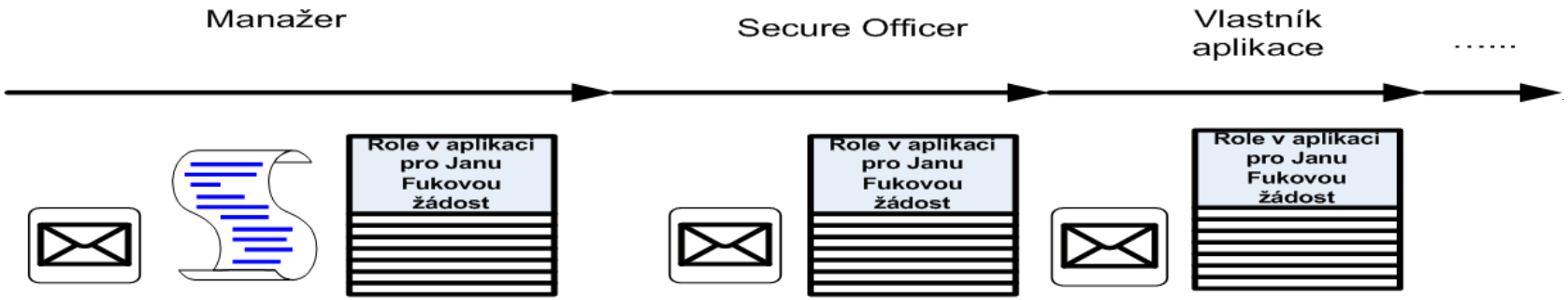
Schvalovací worklow je složité

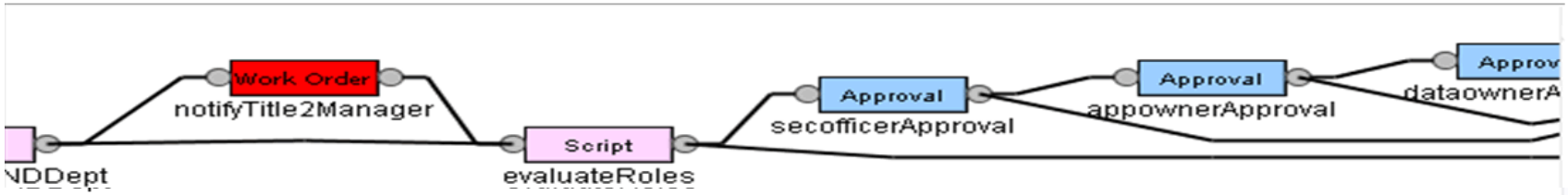


Jak to vidí dodavatel

SIEMENS

Schvalovací worklow z pohledu zaměstnanců





Jak to vidí dodavatel

SIEMENS

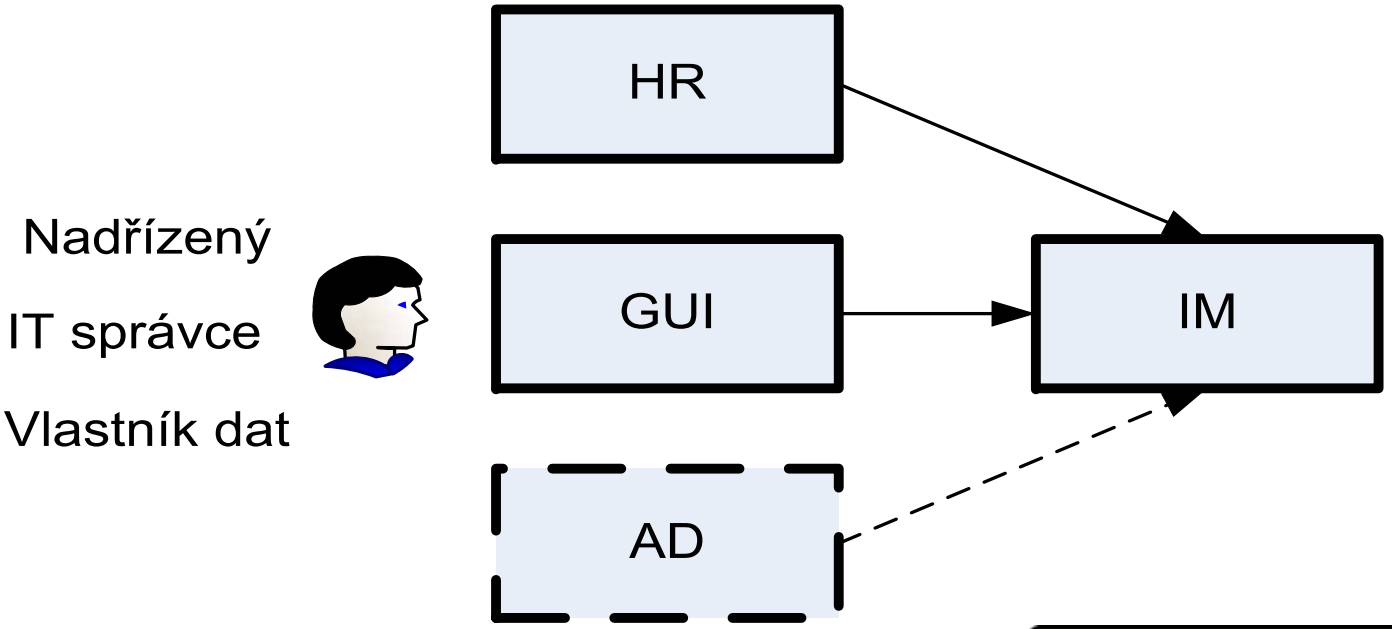
Změna rolí zaměstnanců

- Starost o zakládání, modifikaci a rušení uživatelských účtů přechází z administrátorů na IAM.
- Důležitost personalistů a personálních dat je vyšší.
- Velkou práci dá vyčištění a nastavení personálních dat.
- Administrátorům se odebírá starost o uživatelská oprávnění.
- O uživatelská oprávnění a role uživatele v aplikacích žádá nadřízený.
- Pro aplikace je IAM základním zdrojem informací o uživatelích, uživatelských účtech a rolích.

Jak to vidí dodavatel

SIEMENS

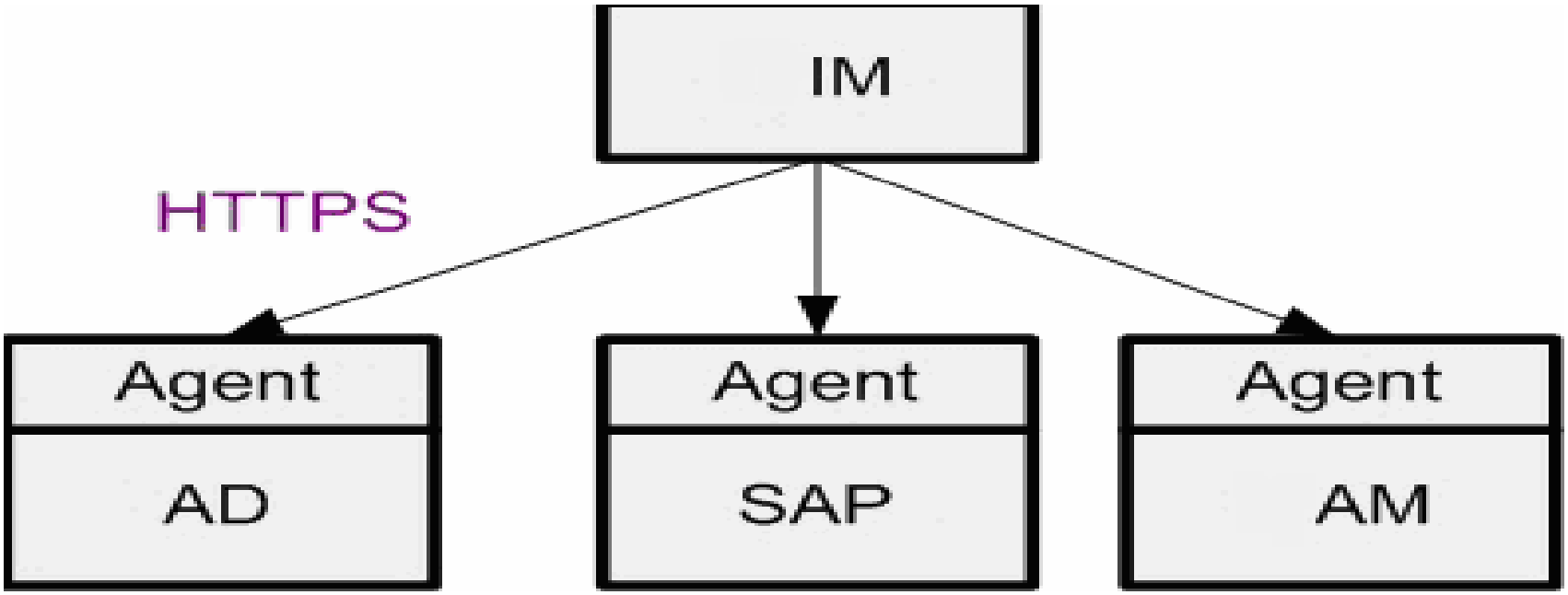
Vstupy do IM



Jak to vidí dodavatel

SIEMENS

Aplikace podřízené IM



Jak to vidí dodavatel

SIEMENS

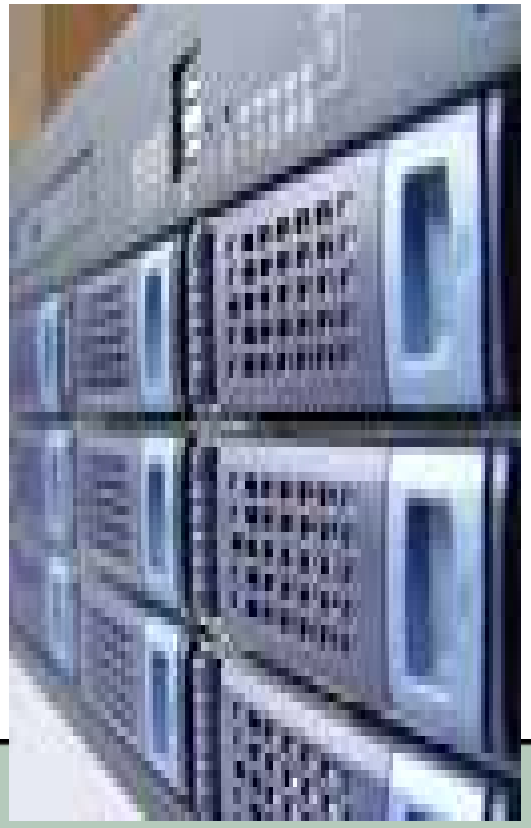
Vše o disciplíně

- IAM vyžaduje disciplínu od zaměstnanců odběratele.
- Implementace IAM je úspěšná pouze pokud zaměstnanci odběratele respektují požadavky plynoucí z IAM.
- Pokud schvalovatelé neschvalují žádosti na přidělení uživatelských oprávnění včas, budou zaměstnanci s funkcí IAM nespokojeni.
- Administrátorům se ne vždy líbí, že se jejich význam a pravomoci snižují.
- Personalistům se ne vždy líbí, že se jejich význam a pravomoci zvyšují.
- Aplikacím se ne vždy líbí, že jsou podřízeny IAM.

Jak to vidí odběratel

Heterogenní prostředí ČSSZ

- Operační systémy: Main Frame BS2000, Unix orientované servery, Windows servery, Windows stanice
- Různé aplikace: BS2000 cca 1 mil. řádků kódu, databáze SESAM, ISAM, +
- centralizované – Main Frame-Cobol, Unix, C++
- decentralizované i lokální – Unix, Windows, cca 2 mil. řádků kódu
- přístupy – emulace Unix terminálu, emulace MF terminálu, klient-server, webové rozhraní.



Jak to vidí odběratel

Heterogenní prostředí ČSSZ

Každá platforma, případně i skupina operačních systémů apod., databáze, skupina aplikací má svou:

- vlastní správu – BS2000, Unix servery (cca 100 lokalit), Windows severy (dtto),
- vlastní seznam uživatelů a jejich uživatelských oprávnění,
- vlastní bezpečnostní politiku atd.

Jak to vidí odběratel

Problémy s bezpečností v heterogenním prostředí

Nutné kroky

1. krok: se změnou operačních systémů Windows, připraven záměr nasadit jednotnou správu uživatelů.

2. krok: udělat něco, co bude integrovat správu uživatelů nejen ve Windows prostředí, ale přes všechny platformy.

Výsledek

Zpracovat koncepci bezpečnosti přístupu k datům a aplikacím.

Snáze se píše, hůře uskutečňuje.

Jak to vidí odběratel

Problémy s bezpečností v heterogenním prostředí

V rámci koncepce formulováno 10 projektů, mezi nimi:

- dokončení Active Directory v oblasti Windows – nasazení platformy Windows 2003 a Windows XP, vytvoření Active Directory,
- nasazení PKI a čipových karet,
- vytvoření AAA prostředí, pracovně známé také jako AAA portál,
- integrace všech platforem a aplikací do tohoto prostředí.

Jak to vidí odběratel

Vytvoření AAA prostředí

Definice AAA prostředí
- jednotná autentizace
- jednotná autorizace
- audit – monitorování všech přístupů k datům a aplikacím

Výchozí stav
- centrální správa MF v oblasti
- rozpracovaná koncepce Active Directory v rámci redesignu celé Windows doménové oblasti - vytváření jediné domény s centrální správou všech uživatelských účtů
- rozpracována realizace nového IS pro řízení a správu (ISŘS)
- rozsáhlá oblast aplikací na decentralizovaných serverech s emulací terminálu
- aplikace client/server (centralizované i lokální)

Jak to vidí odběratel

Vytvoření AAA prostředí – komentář

Definice AAA prostředí

- představa jak dosáhnout tohoto prostředí u uživatele – minimálně
- konzultace s odbornými kruhy – co osoba a firma, to jiný názor, atd.
- klíčový význam Proof of Conceptu jako sjednocujícího konceptu před zahájením realizace

Jak to vidí odběratel

Vytvoření AAA prostředí – komentář

Model AAA prostředí postaven na následujících postulátech:

- základem musí být systém rolí v organizaci,
- systém rolí musí být provázán s organizačním schématem a udržován nezávisle na IT oblasti jako součást personalistiky – rozhodování o oprávnění, čipové karty (vazba na SSO) a PKI,
- systém rolí musí být promítnut do systému žadatele – schvalovatel jako základ správy účtů a oprávnění,
- prakticky to u nás znamenalo provázání 3 evidencí:
  - HR-SAP jako zdroj podnětů,
  - Centrální evidence ITIM/ITAM,
  - Active Directory pro oblast Windows.

Jak to vidí odběratel

AAA prostředí – komentář k vazbě na HR

HR SAP jako zdroj dat

Myšlenka jednoduchá, ale IAM přece jen vyžaduje některá data navíc a v tomto smyslu je nutno uvažovat s určitými problémy:

- koordinace mezi 2 nezávislými projekty je náročná a vyžaduje pečlivou přípravu,
- nástrahy jako např.: neobsazené nejvyšší funkce, neobsazené funkce schvalovatelů, 2 zaměstnanci na 1 systemizovaném místě, 1 zaměstnanec na 2 místech; atd.

Shrnutí: všechno je v podstatě jinak (nutno počítat s výjimkami) a jestliže bývá personální evidence přesná, IAM nároky umocňuje.

Jak to vidí odběratel

AAA prostředí – komentář ke správě AD

AD jako podřízený systém. Myšlenka jednoduchá. Podněty se promítnou do IAM a ty se promítnou do AD.

- Koordinace velmi náročná a dosažení stavu automatického promítání podnětů IAM do AD vyžaduje mnoho úsilí.
- Realizace za ostrého provozu AD vyžaduje důsledné otestování před nasazením.
- Mění se procesy, mění se navyklé toky dat.
- Některá oprávnění mají velmi komplikované workflow.
- K přepojení na přímou aktualizaci AD prostřednictvím IAM vyžaduje hodně odvahy.

Závěr: oblast správy účtů v AD je velmi náročná a vyžaduje pečlivé otestování před nasazením správy pod IAM.

Jak to vidí odběratel

AAA prostředí – vazba na vlastníky dat

Myšlenka jednoduchá, ale vlastník dat jako schvalovatel vyžaduje splnit určité předpoklady:

- musí být bezpečnostní politika, která tyto role vymezuje;
- vlastník dat nemůže obvykle udělovat oprávnění každému jednotlivému zaměstnanci (v ČSSZ jich je > 9 000) – nutnost delegací;
- vlastník dat bude chtít vědět, komu bylo oprávnění uděleno – nutnost reportingu;
- vlastník dat chce vědět, kdo žádá, kdo schválil před ním – nutnost správných notifikací.

Jak to vidí odběratel

AAA prostředí – vazba na vlastníky dat

Závěr

Přestože na počátku bylo věnováno maximum pozornosti nastavení výše uvedených procesů, ukázalo se, že značný okruh problému nebyl vůbec při analýze zachycen. Vlastníci dat si faktickou odpovědnost uvědomovali až při zahájení schvalovacích procesů naostro!

Jak to vidí odběratel

AAA prostředí – vazba na vlastníky procesů

Myšlenka jednoduchá, ale ...

- vlastník procesu jako schvalovatel a vlastník dat jako schvalovatel nemusí být totožná osoba
- musí být bezpečnostní politika, která tyto role a jejich vztahy vymezuje
- musí být další dokumenty, které vymezují další role v rámci realizace procesů

Závěr: problém vztahu vlastníka dat a vlastníka procesu se objevil prakticky až při realizaci schvalovacího workflow a jeho vyřešení kladlo značné nároky na koordinaci rolí.

Jak to vidí odběratel

AAA prostředí – k definici rolí

Při nasazení IAM se nabízí představa, že je užitečné předdefinovat co největší množství rolí a maximálně proces automatizovat.

Zvolili jsme jinou cestu:

- při nástupu zaměstnance se stanovuje pouze zřízení uživatelského účtu a nejsou přidělovány žádné další role,
- role jsou záležitostí workflow, která proběhne až po registraci zaměstnance a vystavení čipové karty.

Praktické zkušenosti ukazují, že to byla správná cesta, protože počty rolí mohou dosáhnout velkého počtu, a z toho by mohly vyplynout neúměrné nároky na vývoj.

Jak to vidí odběratel

AAA prostředí – k definici rolí

Výhoda

Realizovatelnost workflow (i takovýto přístup je velmi náročný na realizaci). Tento postup doporučujeme a považujeme jej za dostatečně pružný a zvládnutelný.

Nevýhoda

Vedoucí zaměstnanci schvalují role každému zaměstnanci individuálně.

Jak to vidí odběratel

AAA prostředí – vazba na čipové karty

Při nasazení IAM bylo požadováno:

- zavést Single-Sign-On, tj. uživatel se autentikuje pouze jednou, při zahájení práce,
- vazba na projekt zaměstnaneckých čipových karet a PKI.

Zajištění vazby znamená přesně definovat procesy zřizování uživatelských účtů a integrovat je s procesy HR SAP, přidělování karet a osobních klíčů.

Shrnutí

Vazba na SSO, PKI a zaměstnanecké čipové karty není triviální záležitostí. Vyžaduje opět pečlivé testování a přípravu zaměstnanců, kteří se tím zabývají.

Jak to vidí odběratel

K disciplinovanosti a kázni

IAM vyžaduje disciplínu od zaměstnanců odběratele. ČSSZ patří mezi instituce s vysokou organizační kulturou a vzhledem k peněžním procesům, které zde probíhají, i s vysokou kázní.

O to více je nutné zaměstnance na novou oblast aktivit připravit. Klíčový význam má zaškolení zaměstnanců a jejich praktická příprava.

Nejhorším faktorem při náběhu systému je bezradnost a nepochopení. Přestože nebylo podceněno, jsou s tím problémy, které vyžadují od dodavatele i členů realizačního týmu uživatele velkou trpělivost.

Je to o to důležitější, že aktivními subjekty jsou vedoucí zaměstnanci.

Jak to vidí odběratel

K disciplinovanosti a kázni

Pokud schvalovatelé neschvalují žádosti na přidělení uživatelských oprávnění včas, budou zaměstnanci s funkcí IAM nespokojeni.

Nespokojenost projevují zejména vedoucí zaměstnanci. Po pochopení faktu, že už není jiná cesta než přes IAM, se většina vedoucích snaží tuto oblast hlídat, což má za následek okamžitou reakci na tým a požadavky na vyřešení. Nicméně jsme museli upravit některé lhůty na eskalaci.

Jak to vidí odběratel

K disciplinovanosti a kázni

Administrátorům se ne vždy líbí, že se jejich význam a pravomoci snižují.

Jde o očekávaný jev, ale je nebezpečný vzhledem k vlivu, který tito lidé mají na atmosféru. Neprojevuje se zatím v plném dopadu, protože ne všechny oblasti byly vyřešeny, tudíž se očekává, že bude působit ještě v budoucnu.

Jak to vidí odběratel

K disciplinovanosti a kázni

Personalistům se ne vždy líbí, že se jejich význam a pravomoci zvyšují.

Projevuje se určitá únava z inovací. Náběh HR SAPu a registračních autorit a jejich neustálenost hrají své důvody. Nutnost dialogu a školení.

Jak to vidí odběratel

K disciplinovanosti a kázni

Aplikacím se ne vždy líbí, že jsou podřízeny IAM.

Musím konstatovat, že jsem čekal odpor daleko větší a oceňuji práci dodavatelského týmu. Náš vlastní vývoj požadavky též akceptoval. Myslím si, že je vše otázka správných návyků a existence standardů. Tyto standardy by měly existovat předem a požadavky na aplikace z titulu integrace pod AAA portál by měly být jejich součástí. Dodatečné zavádění je vždy velmi komplikované.

Jak to vidí odběratel

Závěrem shrnutí

Předpoklady úspěchu u odběratele:

- Kázeň, disciplina a pochopení účelu a hlavně významu a vůle vedení IAM zavést.
- Vyřešená organizační struktura a organizace procesů, definované kompetence a role.
- Zpracovaná bezpečnostní politika, zejména vymezení rolí vlastníků dat a procesů.
- Zpracovaná koncepce bezpečnosti přístupu k datům a informacím.
- Vyřešená architektura sítě a zamezení obcházení integrační role IAM.

Jak to vidí odběratel

Závěrem shrnutí

- Pořádek v aplikacích a architektuře informačního systému.
- Pořádek ve standardech a vnitřních předpisech IKT.
- Příprava a zaškolení zaměstnanců – jak žadatelů, tak zejména schvalovatelů.
- Koordinace a důkladné otestování jak vazby na HR, tak i vazby na AD, LDAPy apod.
- Součinnost dodavatele a odběratele, trpělivost při překonávání obtíží, zejména ve fázi přípravy a náběhu systému.

Děkujeme za pozornost

František Křesák
Česká správa sociálního zabezpečení

Marta Vohnoutová
Siemens IT Solutions and Services

SIEMENS