



Přírodovědecká
fakulta
Faculty
of Science

Identity a Access Management



Marta Vohnoutová a Pavel Horal



Osnova

Teorie I

- Potřeby organizace, kdy je vhodné v organizaci zavádět Identity Management (IdM)
- Co je IdM a na co řeší
- Co je Access Management (AM) a co řeší
- Propojení IdM a AM
- Jakým způsobem je IdM provázáno s okolím
- Pravidla zavádění IdM a úroveň jeho integrace s okolím
- Nadřízené systémy
- Vnitřní struktura IdM
- Filosofie přidělování přístupových práv
- Workflow a co vše musí řešit
- Hierarchie, role sady, oprávnění
- Oprávnění vztažená k uživateli
- Oprávnění vztažená k pozici, jakou uživatel aktuálně zastává





Osnova

Teorie II

- RBAC model
- Rozšířený RBAC model
- Optimalizace RBAC modelu
- Mandatorní atributy, skills ...
- Vnitřní role v IdM - schvalovatelé, správci rolí, správci dat...
- Uživatelský self-service (žádosti o vlastní práva, přehled práv a účtů)
- Podřízené systémy
- IdM jako informační základna pro aplikace - propagace dat do AD, do Exchange, do intranetového portálu, API pro aplikace
- problém rozevírání nůžek mezi daty v IdM a v podřízených systémech
- Souboj s administrátory - snižování jejich pravomocí
- Disciplína - nastavování uživatelských účtů a jejich práv shora
- Popisy pracovních činností - definice sad
- Systemizace - definice, teorie a dopady
- Katalog typových pozic a optimalizace organizační struktury
- Cvičení - Návrh provázání Katalogu typových pozic s návrhem sad v IdM



Osnova

Praxe

- Seznámení s logikou jednoho z IdM produktů
- Instalace Apache Directory Studio a OpenIDM
- Nastavení systému
- Seznámení se systémem
- Cvičení
 - Nadřízený systém - personální data - připravený csv soubor
 - Nastavení vnitřní struktury IdM
 - uživatel
 - uživatelova práva
 - uživatelův účet v AD
 - Podřízený systém AD
 - založení uživatelova účtu prostřednictvím IdM - počáteční impuls - přidání řádky do csv souboru
 - přidělení přístupových práv uživateli v AD (přidání do skupin) podle nastavení v IdM





Na konci každého bloku budou kontrolní otázky, ze kterých bude možné dosáhnout pomocné body k dosažení zápočtu



Slovník pojmů I

Pojem	Definice
Osoba / fyzická osoba	Fyzická osoba – v systémech lidských zdrojů TO2 je identifikována pouze jako vazba mezi jednotlivými záznamy / kontrakty pracovníka. Tato vazba neexistuje u externistů.
Pracovník / osobní číslo pracovníka	Osobní číslo pracovníka reprezentuje zaměstnanecký nebo jiný vztah osoby k TO2 (tzv. kontrakt). Jedna osoba může mít založeno více vztahů (kontraktů) a tedy přiděleno i více (historicky i současně) platných osobních čísel. V každém okamžiku je jedno z aktuálně platných osobních čísel považováno za tzv. hlavní osobní číslo a ostatní záznamy pracovníka se k tomuto hlavnímu osobnímu číslu odkazují (neplatí pro externisty).
Uživatel	Uživatelem rozumíme pracovníka identifikovaného v IS systémech na základě přihlašovacího jména a identity, která je zpravidla odvozena od osobního čísla pracovníka. Jedna osoba může mít přiděleno více (historicky i současně) platných osobních čísel a více přihlašovacích jmen a účtů do IS systémů.
Zdrojový systém	Systém IS, který slouží (samostatně, nebo ve spojení s jinými) pro IAM jako autoritativní zdroj informací o osobách, uživateli a těch rozhodných událostech, na které má řešení IAM automaticky reagovat
Cílový systém	Systém IS pro který IAM řídí správu přístupových účtů a přístupových oprávnění.
Účet	Přístupový účet je objekt cílového systému, jehož funkce slouží k autentizaci uživatele a ke zprostředkování přístupu k funkcím cílového systému. Pojmově odlišujeme ‚uživatelské‘ a ‚technické‘ účty. Uživatelský účet je spojen s identitou uživatele, technický účet s ní nutně spojen být nemusí (např. unix root).
Oprávnění	Objekt vztažený k účtu, jehož hodnota (přímo nebo spolu s jinými) určuje rozsah dostupných informací a funkcí na cílovém systému v případě přihlášení na daný účet nebo je i z jiného důvodu potřebná pro plnohodnotné využívání účtu.
Přístup	Přístupem rozumíme přístupový účet a hodnoty jednotlivých oprávnění, která jsou poskytována pro daný cílový systém pro jeho konkrétního uživatele. Přístupy jsou evidovány jako položky konfigurace IS v konfigurační databázi CMDB.



Slovník pojmů II

Pojem	Definice
Role	Skupina přístupových oprávnění do jednoho nebo více cílových systémů. Role vytváří „přístupový vzor“ pro typové činnosti uživatelů. Spolu s profilem je evidován i seznam uživatelů zařazených do dané role.
Sada	Sada rolí a (samostatných) oprávnění, která má být v řešení IAM přiřazená k pracovní pozici podle organizačních struktur TO2/SK CZ a TO2/SK. O sadu se nežádá, práva z ní plynoucí jsou uživatelům přidělena automaticky při příchodu na danou pozici. Sada je svázána s pozicemi, reprezentuje souhrn práv nutných k výkonu povolání
Základní role	Seznam oprávnění svázaných s osobním číslem. Reprezentuje souhrn práv, které jsou spojené s osobou (typicky email)
Právo	souhrn sad, rolí a oprávnění
Požadavek	Požadavek na nějakou akci v IAM, typicky žádost o přidělení nebo odebrání oprávnění
HP OV SD - Service Desk	Rozhraní na předávání servisních požadavků - založeno na HP OpenView
LN SD - Service Desk (Lotus Notes)	Rozhraní na předávání servisních požadavků - založeno na Lotus Notes
Konfigurační databáze (CMDB)	Databáze obsahující konfigurační položky. Podle zadání bude IAM s touto databází synchronizovat vybrané položky
Konfigurační položka (KP)	Položka konfigurační databáze
Servisní požadavek (SP) (Service Order)	Požadavek na provedení zadané operace na některém z cílových systémů. Servisní požadavek se dále rozpadá na jeden nebo více pracovních požadavků.
Pracovní příkaz (PP) Work Order)	Požadavek na systémové administrátory jednotlivých aplikací na provedení zadané operace, typicky založení uživatelského účtu nebo přidělení oprávnění uživateli.
Hlavní osobní číslo	Osobní číslo přidělené pracovníkovi na hlavní pracovní poměr
Vedlejší osobní číslo	Osobní číslo přidělené pracovníkovi na vedlejší pracovní poměr
Workflow	rozhodovací proces v IAM pro provedení nějaké akce



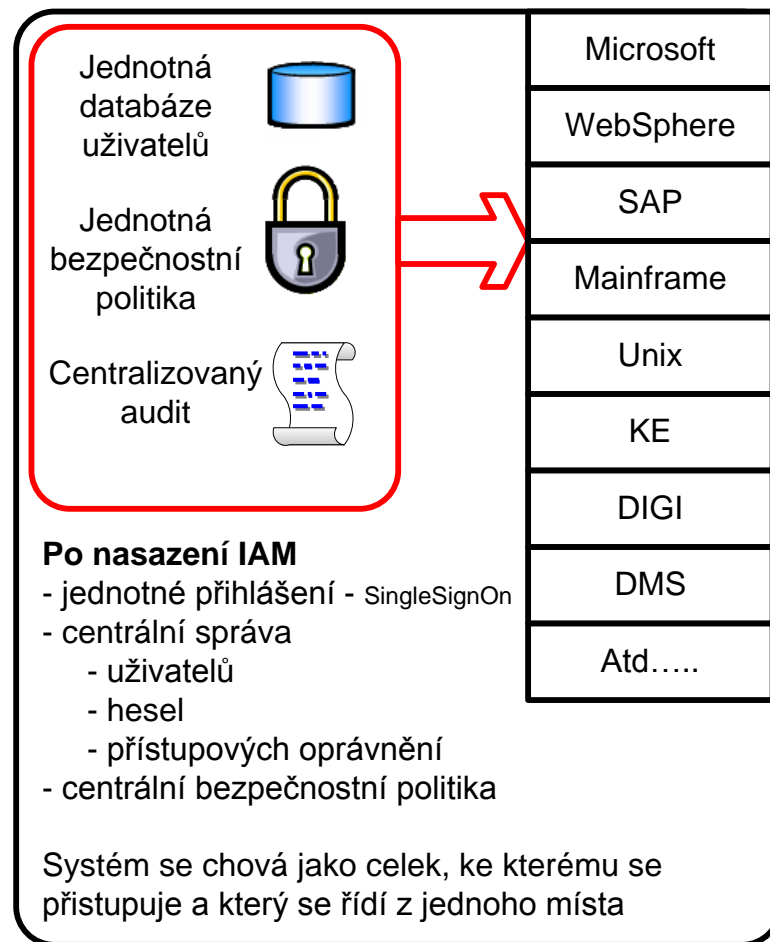
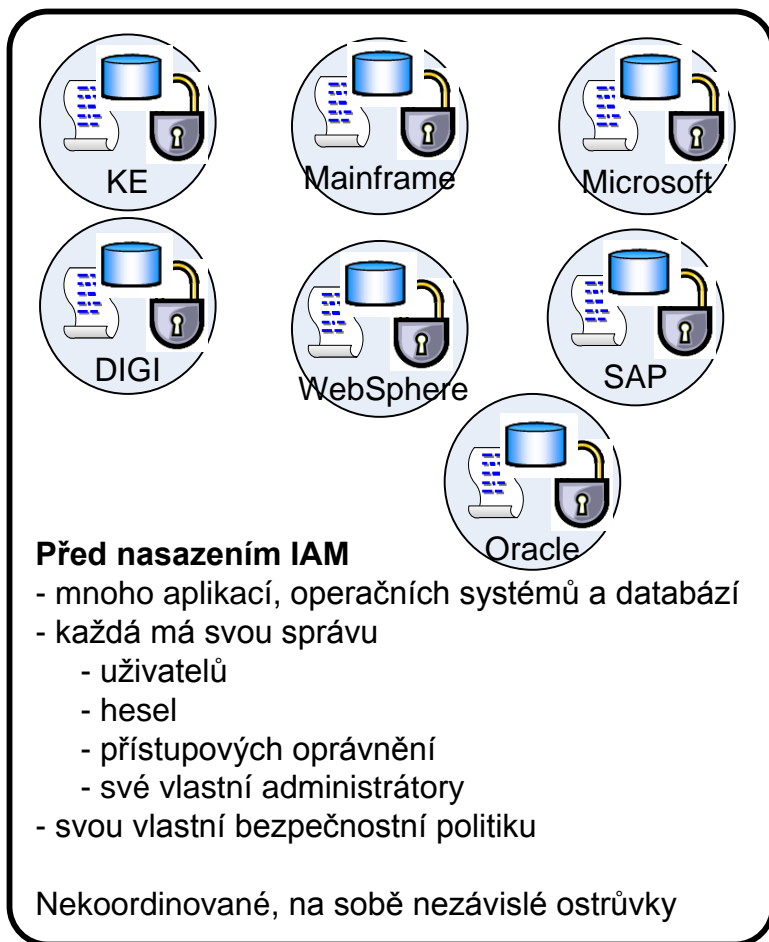
Slovník pojmů III

Pojem	Definice
Schvalovací workflow	schvalovací proces žádosti v IAM
Realizační workflow	realizační proces pro provedení schválené žádosti
Rekonciliace	načítání skutečného stavu z cílových systémů
Správa přístupů	aktualizace přístupových oprávnění v cílových systémech
Vedoucí organizační jednotky	
Nadřízený pracovníka	
Garant aplikace	osoba odpovědná za aplikaci
Garant oprávnění	osoba odpovědná za oprávnění
Garant sady	osoba odpovědná za sadu
Garant role	osoba odpovědná za roli
Garant technického účtu	uživatel odpovědný za technický účet
Odpovědná osoba externisty	nadřízený externisty (může to být jak odpovědná osoba externisty tak jiný externista)
Garant externisty	osoba, od níž odvíjí externisté svou viditelnost a místo, kde se připojují k organizační struktuře
Technický účet	účet, který není uživatelský a který může být přiřazen více uživatelům. Může být jak zakládán prostřednictvím IAM tak v cílových systémech a do IAM načítán
Technologický přístup	všechny požadavky na SD, které nejsou spojeny s aplikacemi registrovanými v SD. Požadavky jsou zpravidla volné texty a jsou vyřizovány manuálně - maily, telefony apod.
Pozice	konkrétní pracovní místo v organizaci, zpravidla obsazené jedním osobním číslem nebo neobsazeno
Profese	katalogové číslo dle číselníku - určuje pracovní zařazení
Viditelnost	filtr omezující možnost přiřazení objektů IAM uživateli na určitou podmnožinu, v IAM je viditelnost proti SUK rozšířena



Potřeby organizace, kdy je vhodné v organizaci zavádět Identity Management (IdM)

Stav před a po IAM



Obecné cíle při nasazení IAM

- **Vytvoření technické infrastruktury IAM pro zajištění následujících činností:**
 - **Vytvoření jednotné autentizace uživatele - AM**
 - **Centrální správa uživatelských identit - IM**
 - **Vytvoření jednotného systému pro autorizaci uživatelů a přidělování autorizačních oprávnění - AM**
 - **Vytvoření centrálního přístupového bodu k aplikacím - AM**
- (každý uživatel bude k aplikacím přistupovat výhradně prostřednictvím centrálního webového rozhraní, které mu poskytne takové prostředí a seznam aplikací, který odpovídá jeho aktuálním rolím a oprávněním)
- **Vytvoření centrálního auditovacího systému - IAM**
- (auditovací systém bude zaznamenávat přístup ke všem aplikacím integrovaným do IAM)

Test

1.otázka Jednotná autentizace uživatelů je zajištěna:

A	<input type="checkbox"/>	Identity Managementem
B	<input type="checkbox"/>	Ani Identity ani Access Managementem
C	<input type="checkbox"/>	Jak Identity tak Access Managementem
D	<input checked="" type="checkbox"/>	Access Managementem



Co je IdM a na co řeší

Co je tedy Identity Management

- **Identity Management** je strategie zahrnující různé postupy, procesy a informace sloužící k identifikaci identity během jejího životního cyklu. Touto identitou je jedinec, jeho identita je specifikována množinou příslušných atributů (oprávnění).
- K vyřešení Identity Managementu slouží nástroj tzv. **Identity Manager**. Identity Management produktů (dále IM) je na trhu celá řada a jejich kvalita je různá.
- Identity Management centralizuje všechny potřebné údaje o uživateli (neboli identitách) do jednoho místa. Pomocí Identity Managera lze uživatelské účty snadno vytvořit a/nebo zrušit, čímž přestanou v systémech existovat tzv. „mrtvé duše“, které tam zůstaly po dřívějších zaměstnancích nebo po různém testování apod.

Komponenty Identity Managementu

- Adresářové služby
- Správa elektronických identit
 - Registrace
 - Aktivace (provisioning)
 - Schvalovací workflow
 - Delegování pravomocí
 - Self-service vybraných činností – uživatel si např. smí sám změnit heslo apod.
- Synchronizace údajů

Aplikace integrované do Identity Managementu

– **Aplikace celosvětově rozšířené nebo založené na standardech**

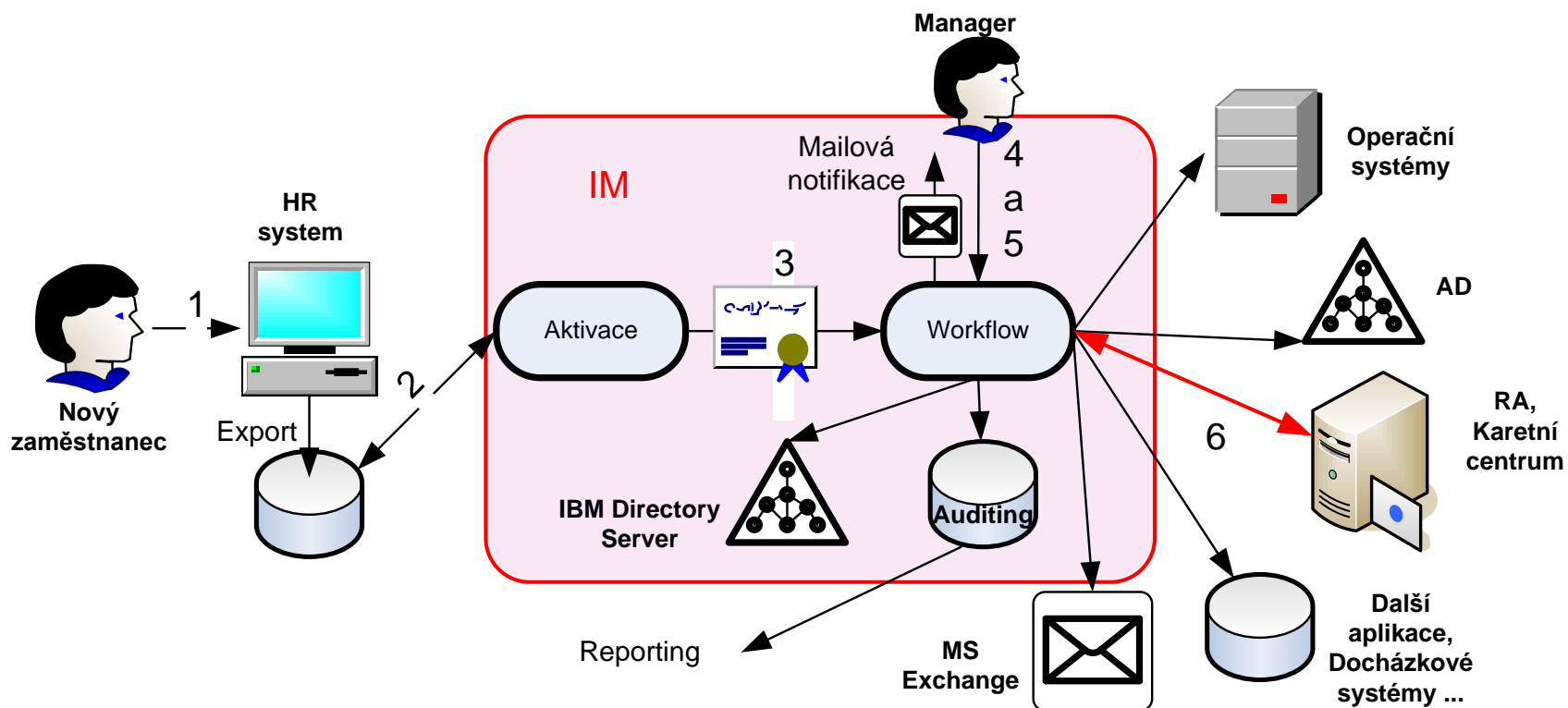
Tyto aplikace jsou integrovány pomocí předefinovaných konektorů (adaptérů), které jsou součástí dodávky Identity Manageru. Příkladem aplikací a systémů, ke kterým jsou dodávány již hotové konektory, jsou:

- Operační systémy – např. RedHat Linux, Solaris apod.
- Databáze – např. Oracle, MS SQL apod.
- Webové servery – např. WebSphere, MS IIS, apod.
- Rozšířené aplikace – např. SAP

– **Aplikace proprietární**

- Proprietární aplikace jsou integrovány pomocí konektorů, které je potřeba nejprve naprogramovat – detailně popsané API je také součástí dodávky Identity Manageru.

IM - centrální správa uživatelů



1. Úvod - test

1.otázka IdM je:

A	<input type="checkbox"/>	Vytváření nových pracovních příležitostí
B	<input type="checkbox"/>	Vytvoření jednotné autentizace uživatele
C	<input checked="" type="checkbox"/>	slouží k identifikaci identity během jejího životního cyklu
D	<input type="checkbox"/>	Komplex procesů a opatření založených na důsledném využívání jednotně koncipovaného souboru systemizovaných míst



Co je Access Management (AM) a co řeší

Access Management

- IM a AM se výrazně liší
- IM není mission critical
- AM je mission critical – musí se zohlednit v návrhu
- Pro IM je AM jen jeden z podřízených systémů

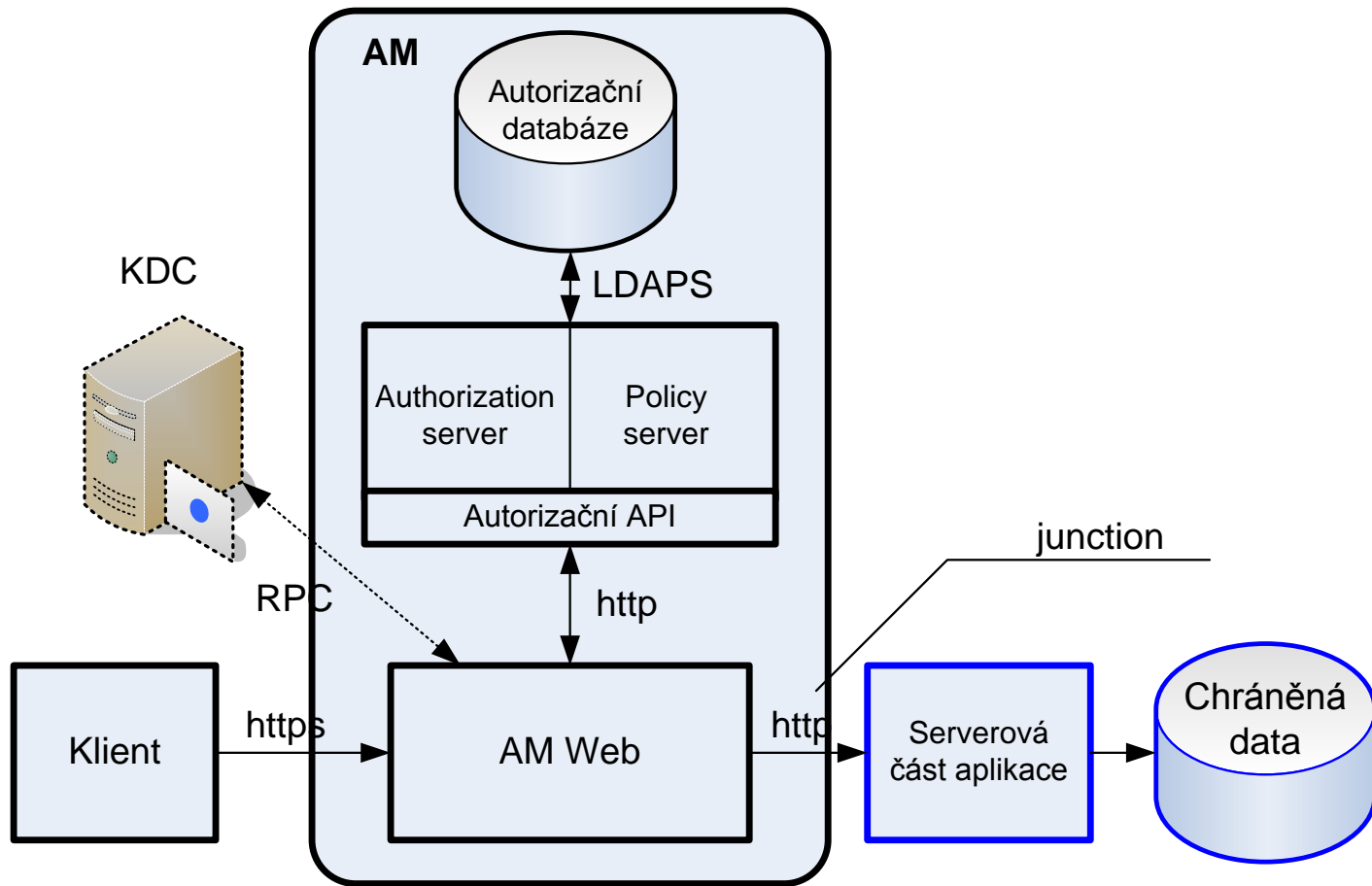
Access Management

User/password
Form based logon
SSL v.3 s X.509 certifikátem
RSA Secure ID token
Custom CDAS autentizace
IP adresa
Bez autentizace
MPA gateway – http header
...

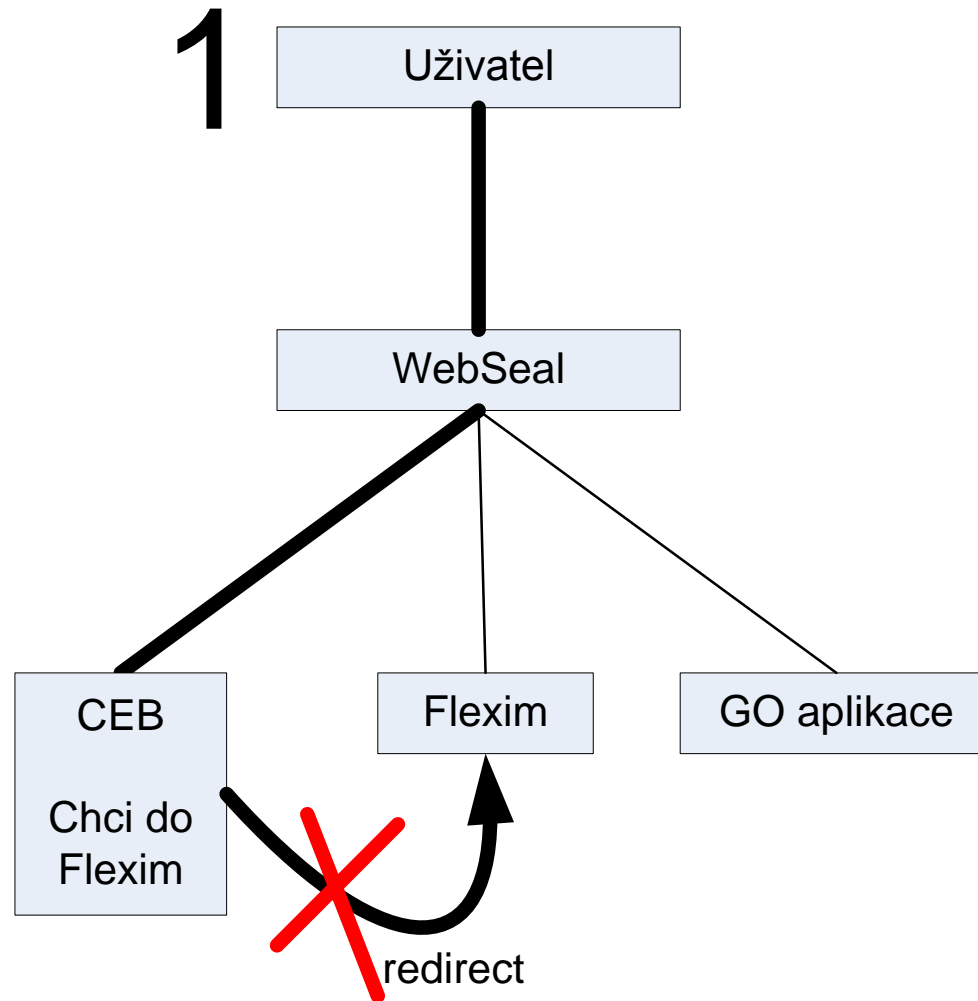


Http proměnné s informací o uživateli
Jméno/heslo
GSO user / GSO password
TAI
IV-credentials
LTPA token přes cookie
E-community cookie
Nic
...

Princip AM

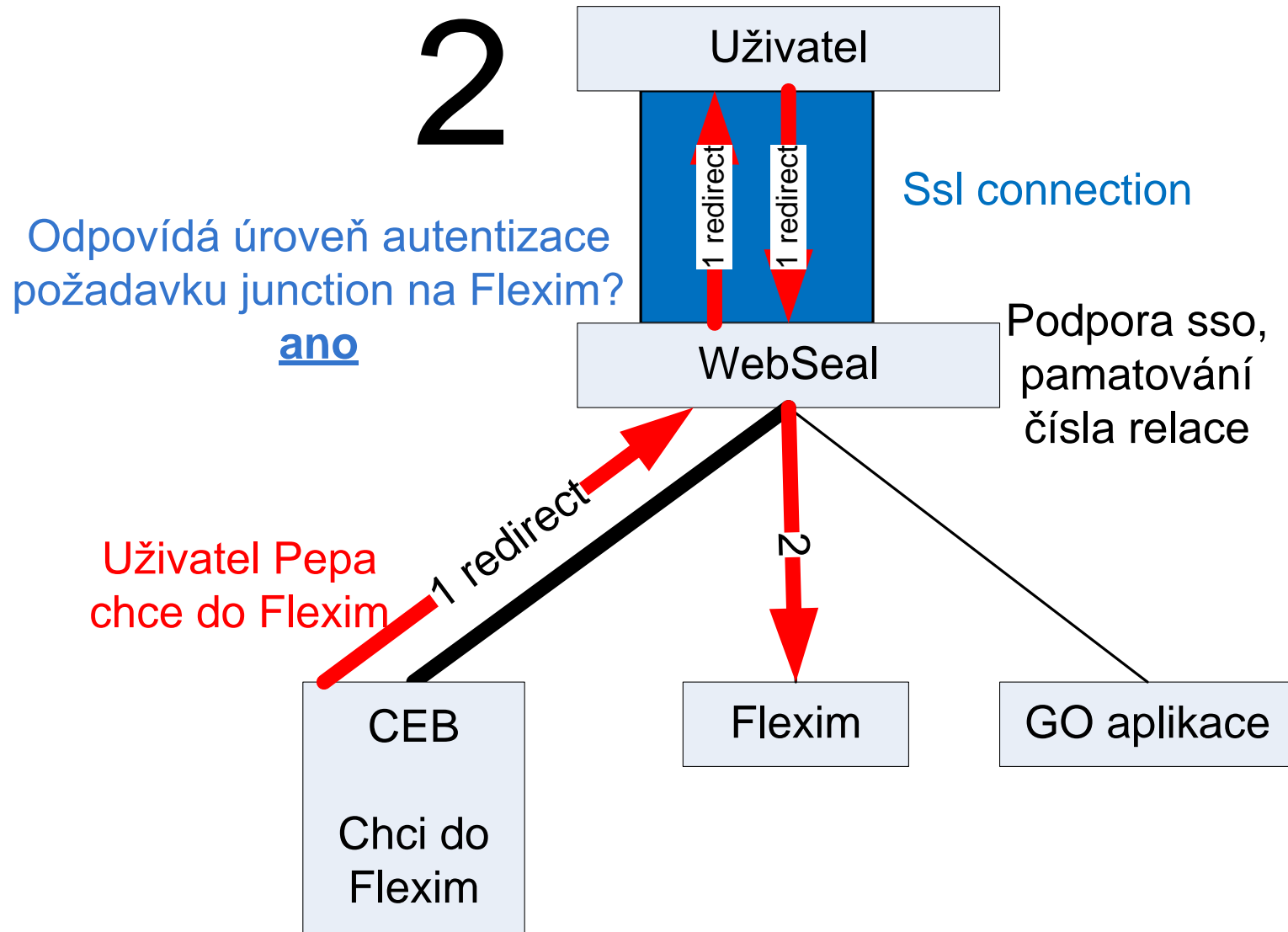


Součástí AM je reverzní webová proxy

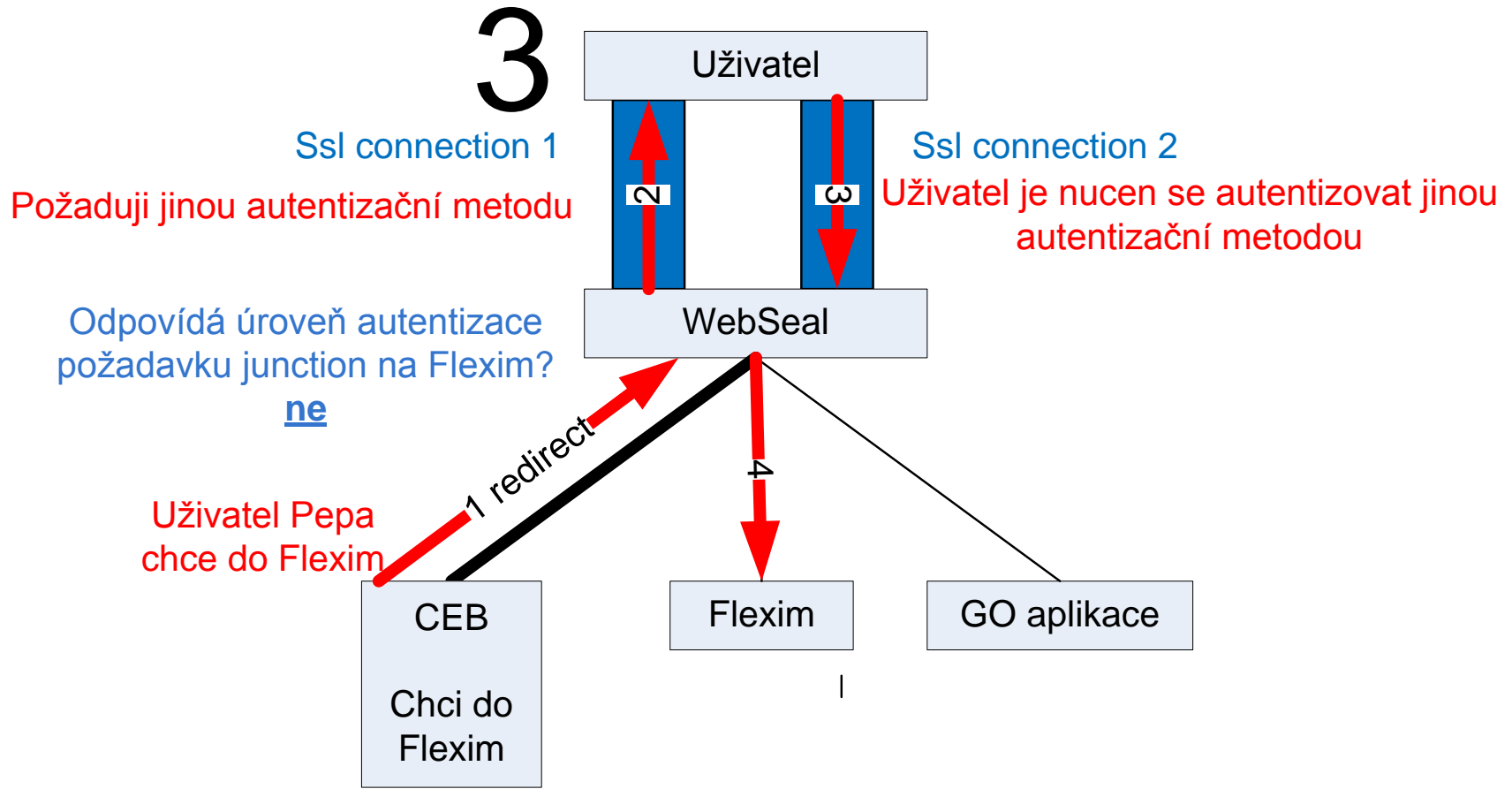


Přesměrování z CEB na Flexim nepřípadá v úvahu

Součástí AM je reverzní webová proxy



Součástí AM je reverzní webová proxy



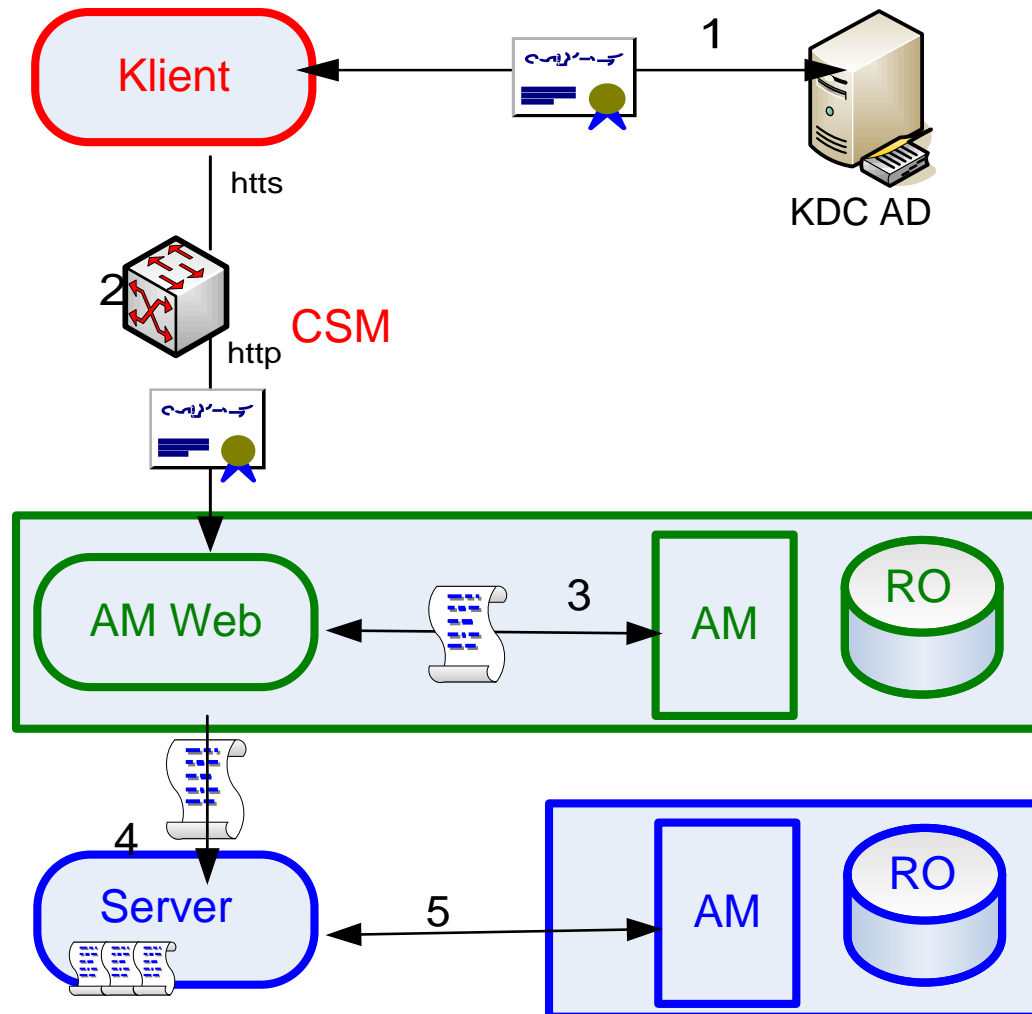
Součástí AM je reverzní webová proxy

Hlavní důvody pro využití

Bezpečnost: proxy je další úroveň zabezpečení a chrání webové servery, které jsou přes ní připojeny

- [Šifrování](#) / urychlení [SSL](#): při vytváření zabezpečených internetových stránek často nezajišťuje SSL samotný server, ale reverzní proxy server, vybavený hardwarem pro urychlení SSL.
- [Vyvažování zátěže](#): reverzní proxy může rozkládat provoz mezi několik připojených serverů, aby se zabránilo přetížení
- [Kešování](#): reverzní proxy může kešovat statický obsah a tím odlehčit připojeným aplikačním serverům a zkrátit odezvu
- [Komprese](#): proxy může komprimovat obsah a optimalizovat jeho odesílání a tím zkrátit odezvu
- [Zasílání po částech](#): dynamicky generovaná stránka může být vytvořena jako celek a klientovi zasílána po částech, takže program generující stránku na centrálním serveru nemusí zůstat otevřený a zbytečně využívat systémové prostředky

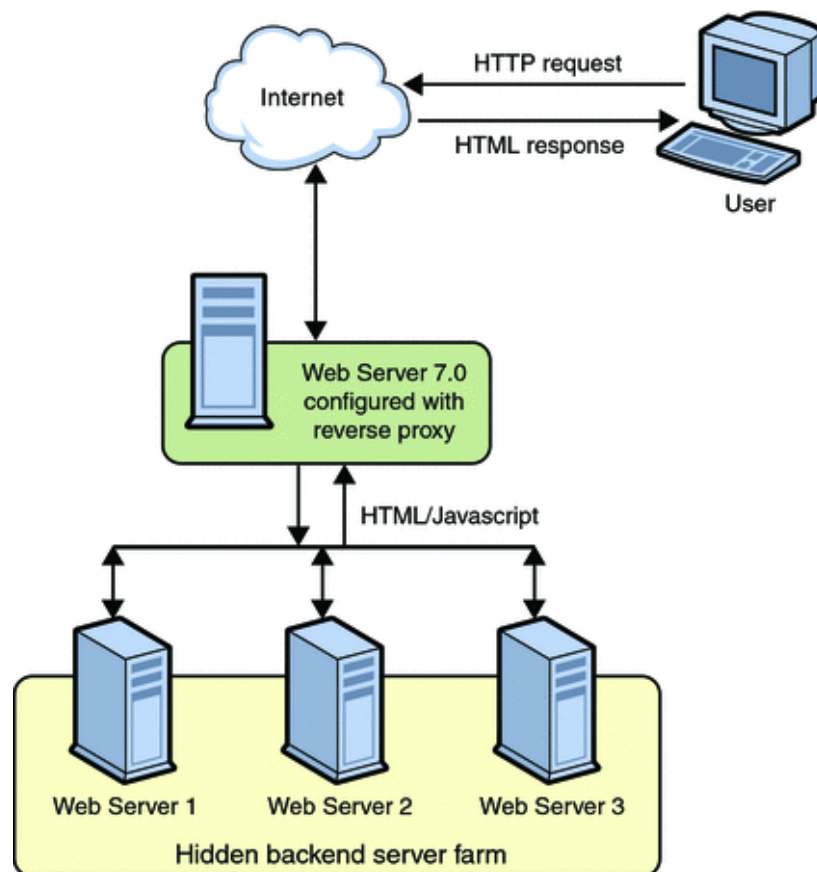
Příklad nasazení AM



Test

1.otázka Reverzní webová proxy je:

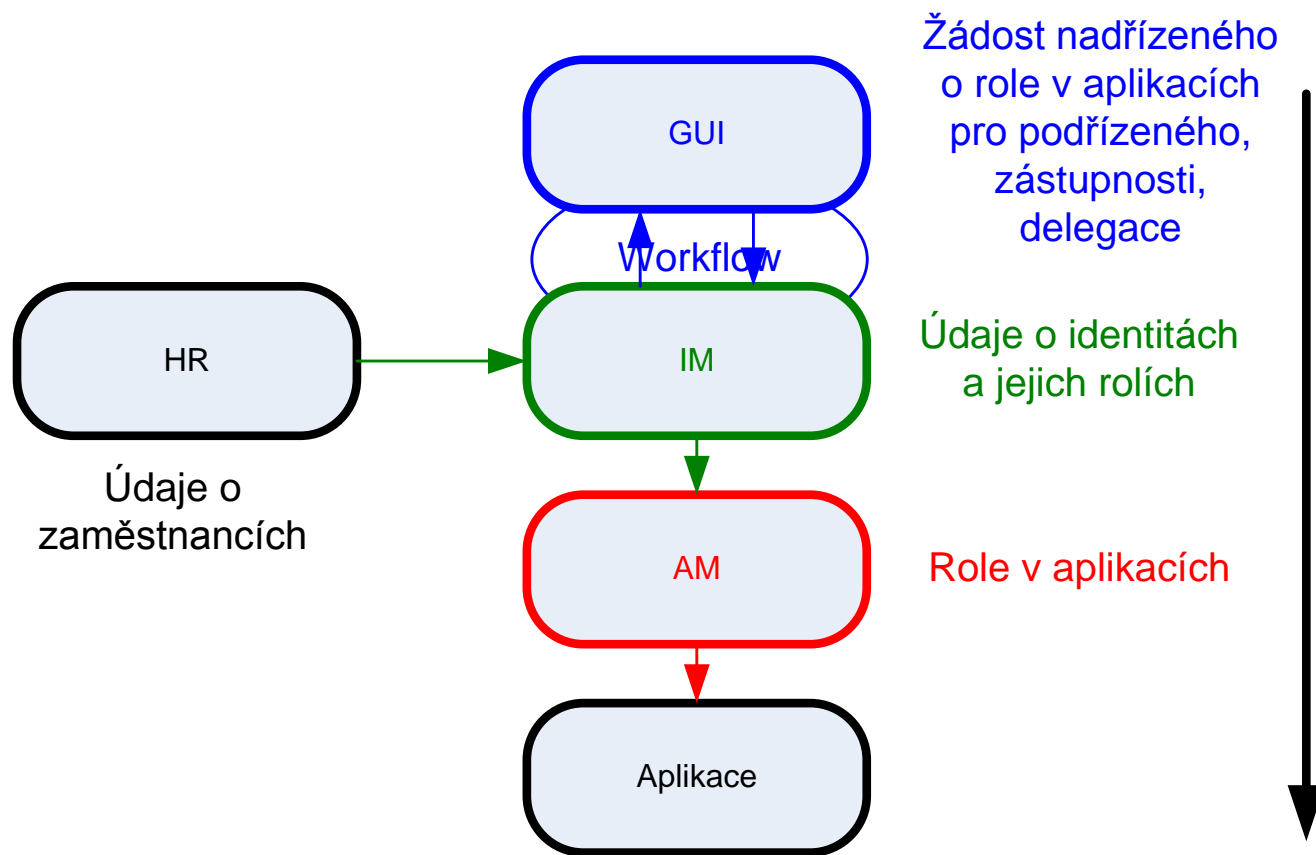
A		Reverzní proxy přenáší vystupující provoz (tj. z vnitřní do vnější sítě) na jediný server zachovávající jediný vnitřní interface pro uživatele intranetu.
B	<input type="checkbox"/>	Reverzní proxy rozděljuje vystupující provoz (tj. z vnitřní do vnější sítě) na několik serverů zachovávající jediný vnitřní interface pro uživatele intranetu.
C	<input checked="" type="checkbox"/>	Reverzní proxy rozděljuje vstupující provoz (tj. z vnější do vnitřní sítě) na několik serverů zachovávající jediný vnější interface pro klienta.
D	<input type="checkbox"/>	Reverzní proxy je obdobou běžné proxy



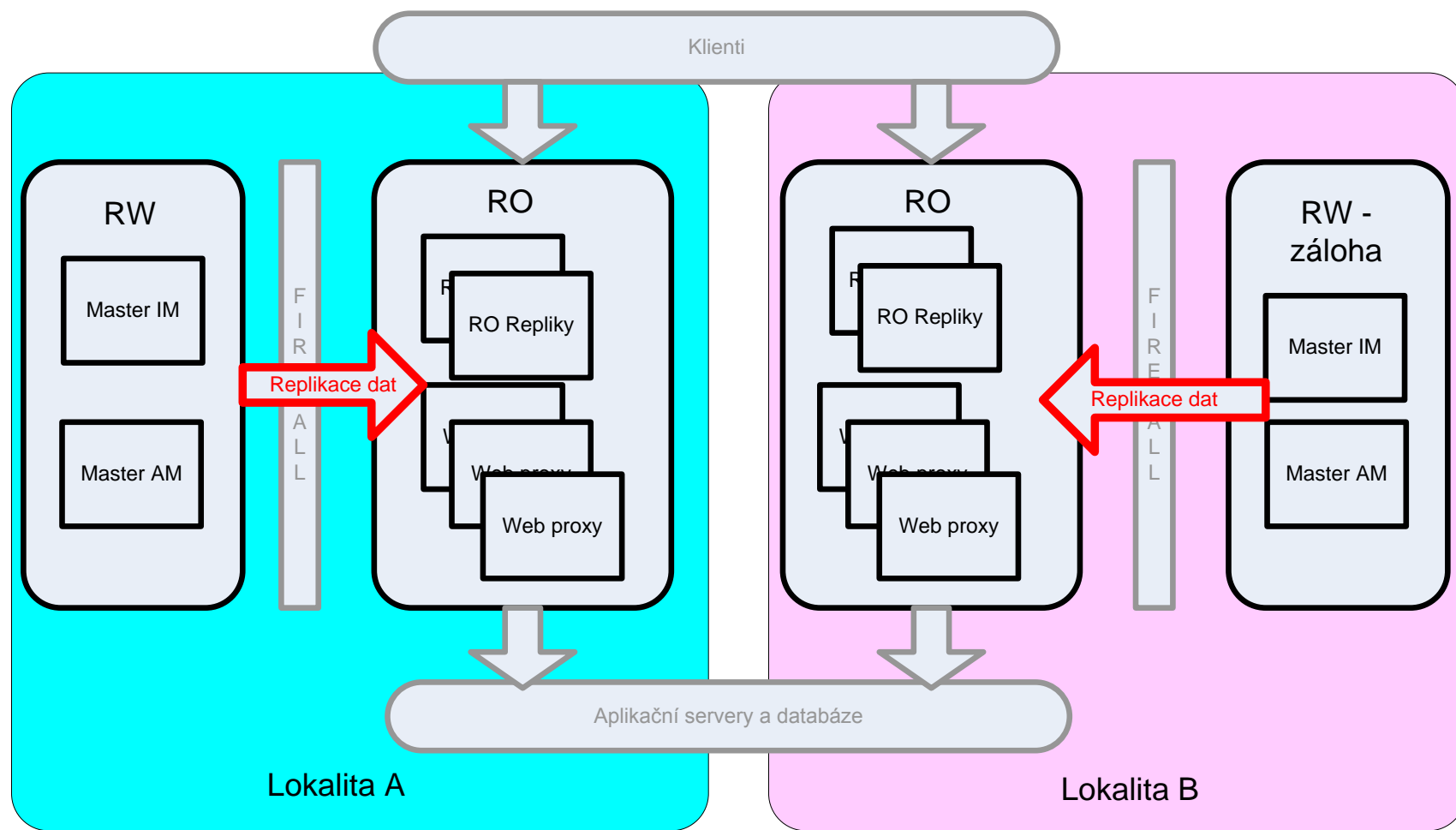


Propojení IdM a AM

IM a AM a jejich vztah



IM a AM a jejich vztah



1. Úvod - test

1.otázka Proč je vhodné oddělit provoz Access Managementu (kdy AM poskytuje data uživatelům) od nastavování AM, kde jsou data zapisována :

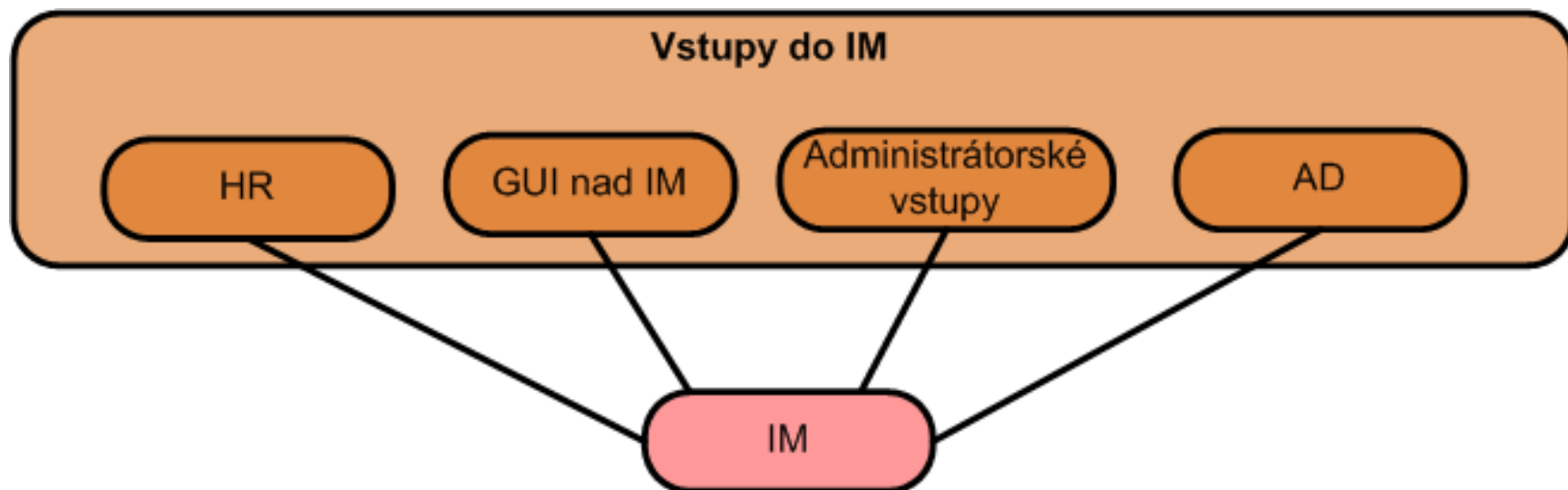
<input checked="" type="checkbox"/>	A	Bezpečnostní důvody
<input checked="" type="checkbox"/>	B	Výkonové důvody
<input checked="" type="checkbox"/>	C	Architektonicky správnější řešení
<input checked="" type="checkbox"/>	D	Snazší škálovatelnost při zvyšování výkonu



Jakým způsobem je IdM provázáno s okolím

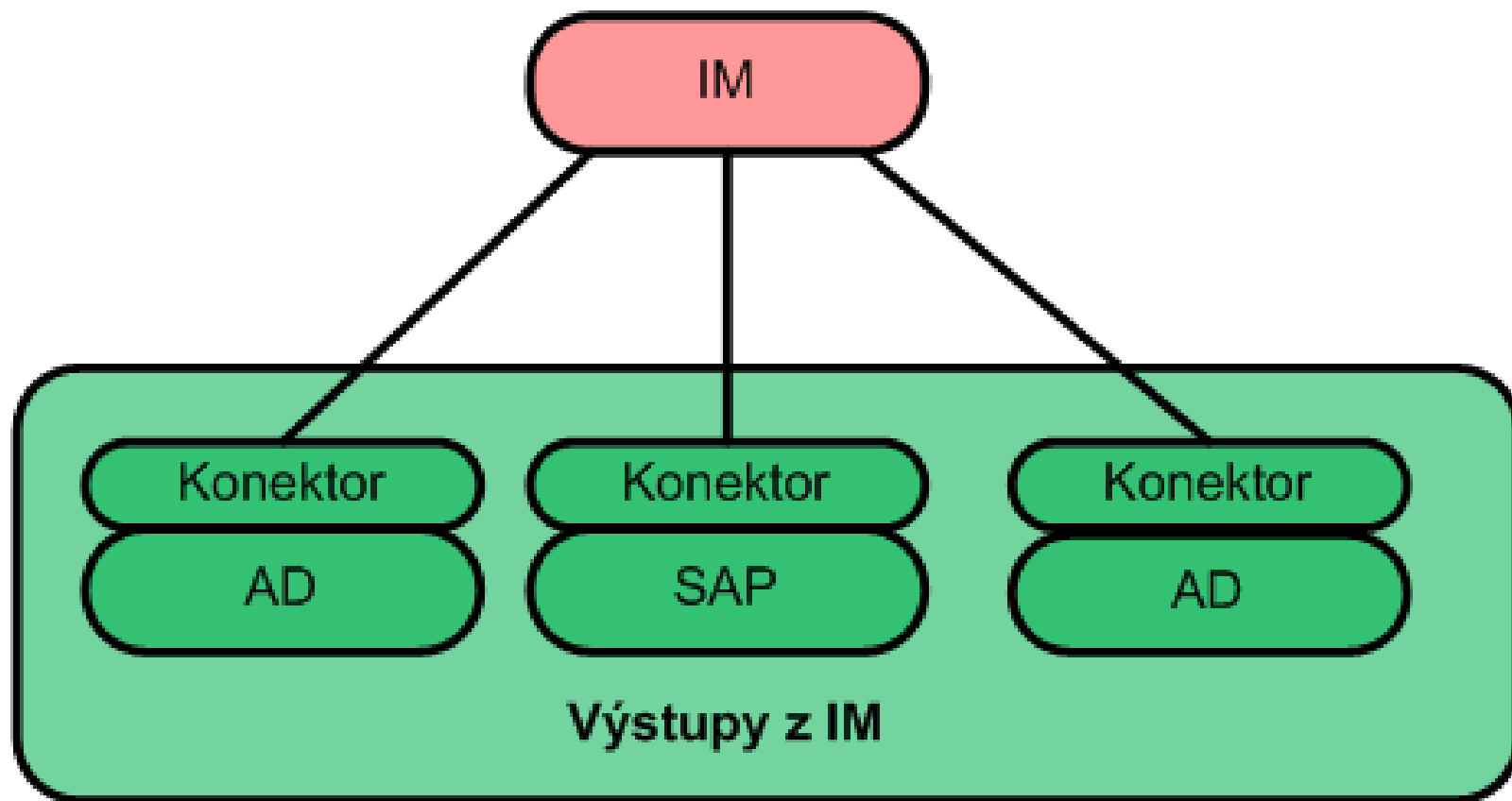
Dodržení nadřízenosti a podřízenosti

Nadřízené systémy

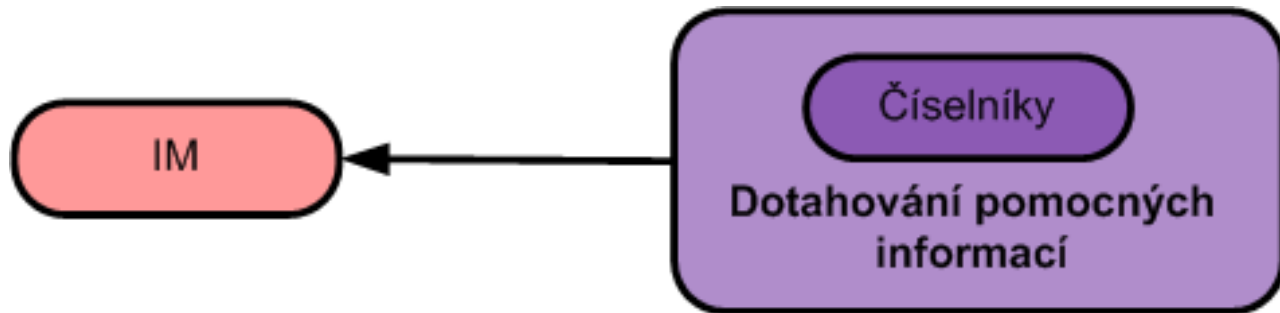


Dodržení nadřízenosti a podřízenosti

Podřízené systémy



Dodržení nadřízenosti a podřízenosti Systémy na stejné úrovni



Test

1.otázka IM vztah nadřízenosti a podřízenosti vůči ostatním systémům:

A	<input checked="" type="checkbox"/>	Musí striktně dodržovat
B	<input type="checkbox"/>	Není důležité definovat vztah nadřízenosti a podřízenosti IM s ostatními systémy
C	<input type="checkbox"/>	Je důležité definovat vztah nadřízenosti a podřízenosti IM s ostatními systémy, ale v běžném procesu se nemusí tak striktně dodržovat
D	<input type="checkbox"/>	Vztah nadřízenosti musí být striktní, vztah podřízenosti nikoliv



Pravidla zavádění IdM a úroveň jeho integrace s okolím

Synchronizace s okolím

- Výměna informací s okolními systémy – typicky s konfigurační databází
- Načítání různých číselníků a jejich aktualizace
- Vstup pomocných informací, které je potřeba pro zakládání uživatelů, uživatelských účtů a jejich oprávnění
- Zpětná synchronizace dat – systémy na stejné úrovni – cesta do pekel

Best practices a realita 😊

- Tvorba IAM je vždy (bohužel) o kompromisu.
- Odběratel má snahu nutit dodavatele, aby přizpůsobil logiku řešení již existujícímu prostředí a zvykům ve firmě – čili „ohýbal produkt a řešení proti best practices“.
- Dodavatel naopak – díky zkušenosti a znalosti produktu nutí odběratele změnit prostředí podle IAM.
- Rozumně se sejdou někde mezi
- **Naučte se mluvit stejnou řečí – vytvořte si slovník pojmů – už jen slovník produktů se liší – natož slovník dodavatele a odběratele**

Best practices a realita ☺

- Pozor při implementaci!!! IAM je vždy složitý produkt mající své vlastnosti. Nelze „splnit cokoliv“ jako při programování.
- Složité věci jdou jednoduše
- Jednoduché však mnohdy složitě
- Slíbit odběrateli např. vazbu n:m místo 1:1 může vést k extrémnímu nárůstu pracnosti a nutnosti programovat (a někdy ne ☺)
- Nutnost konzultovat s týmem, co lze (co dovolí produkt a co ne)

Best practices a realita 😊

- Implementace IAM jsou obtížné a mnohdy i nevděčné
- Velké nároky na projektové řízení
- Nebezpečí nárůstu víceprací
- Nutnost podpory vedení odběratele
- Mění se zvyky lidí – **lidský faktor**
- **Na druhé straně**
- **Jde o dlouhodobou spolupráci a dlouhodobý rozvoj, údržbu, integrace nových aplikací, externího portálu apod.**

Těžké začátky I

– Odběratel a dodavatel si věci představují jinak.

Zavedení 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 organizace. Protože jsme však v konkurenčním prostředí – ani dodavatel neslibuje odběrateli „pot a slzy“.

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
Definování požadavků na nové aplikace pro jejich integraci do IAM.

Těžké začátky II

- IAM ovlivňuje vlastnosti integrovaných aplikací. Aplikace se diktátu IAM brání.

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 ale prověřuj. Nasazení IAM musí vždy počítat s dlouhým obdobím testování.

I po dlouhé době testování se může ještě objevit „kostlivec ve skříni“.

IM je destruktivní systém – zpočátku se nastavuje systém „MARK“ až později „CORRECT“.

Změna rolí zaměstnanců

- Starost o zakládání, modifikaci a rušení uživatelských účtů přechází z administrátorů na IAM.

Důležitost personalistů a personálních dat se zvyšuje.

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 pracovník.

Pro aplikace je IAM základním zdrojem informací o uživateli, uživatelských účtech a rolích

Proof of Concept, analýza

- POC musí být jednoduché.

Zvolíme nejjednodušší operace v IAM a nastavíme je na testovacím prostředí.

Na POC pochopí odběratel základní filosofii IAM. Marketingové slidy bohužel tuto informaci postrádají

Teprve schválením POC fakticky startujeme projekt.

Test

1.otázka Proč je implementace IAM velmi často neúspěšná:

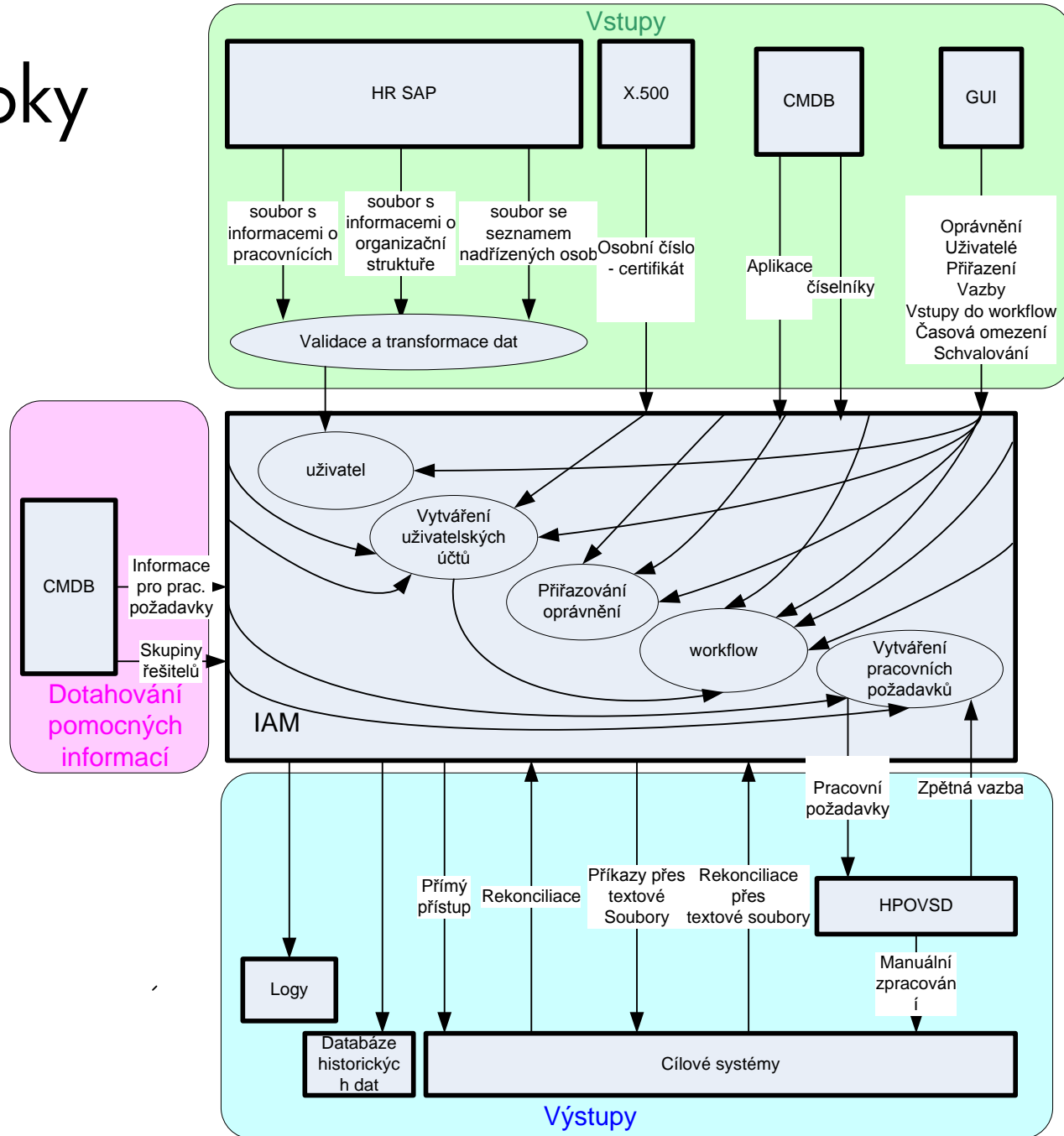
A	<input checked="" type="checkbox"/>	Je obtížné odhadnout celkovou pracnost, velké nebezpečí víceprací
B	<input checked="" type="checkbox"/>	Velké nároky na projektového manažera
C	<input checked="" type="checkbox"/>	Testování a souběžný provoz bývá dlouhý
D	<input checked="" type="checkbox"/>	Implementace je o kompromisech – jak IAM tak zákazník se musí přizpůsobit, změna chování lidí, změny v pracovních postupech



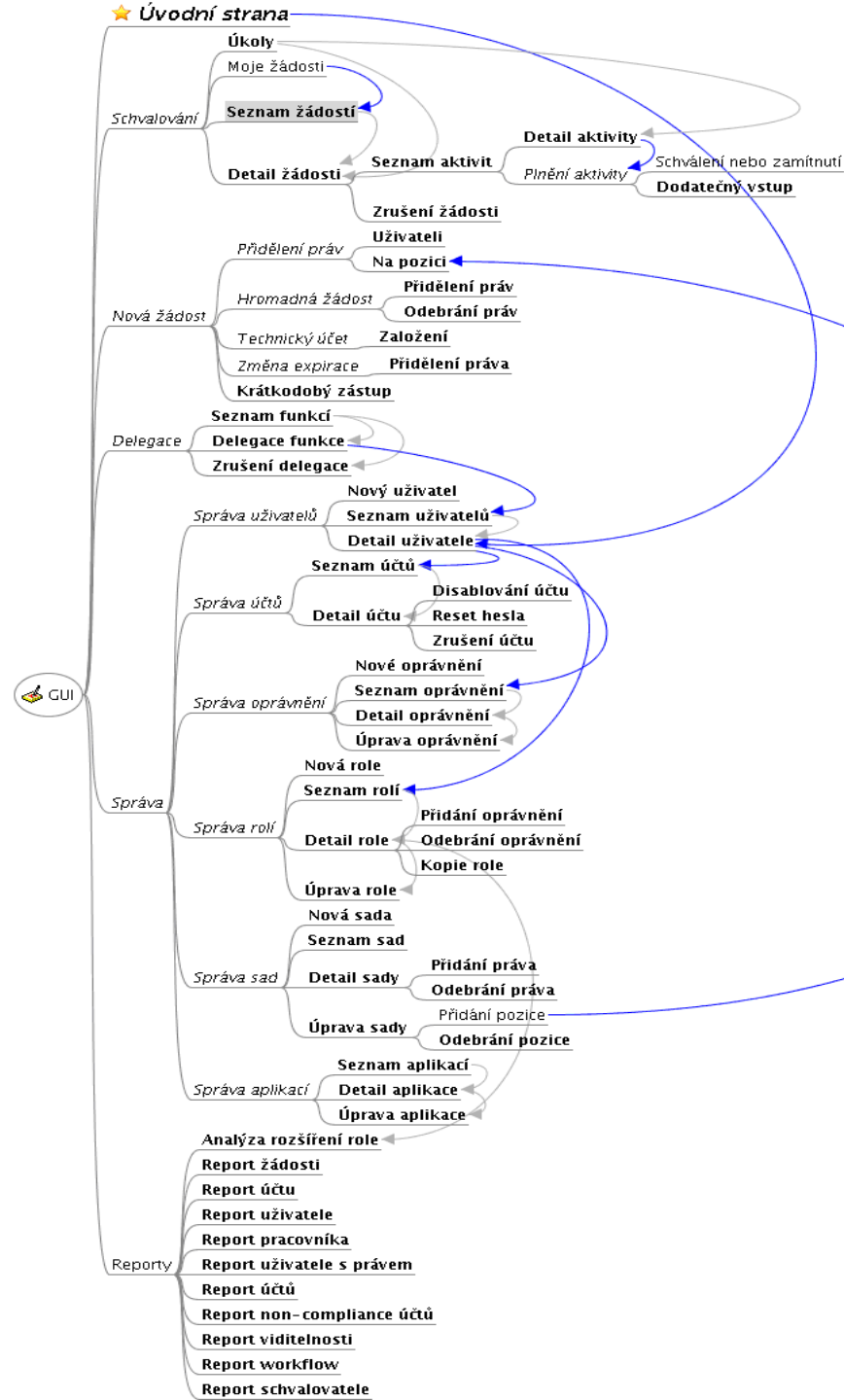
Nadřízené systémy

- Propojení IdM s personálními systémy a jaké situace mohou nastat
- Úvodní načítání dat
- Organizační struktury a jejich změny
- Proces čištění personálních dat
- Propojení s číselníky - heslové politiky, seznamy aplikací
- Propojení s intranetovými portály

Datové toky



Datové toky vstupy - GUI



Datové toky vstupy - HR

- Soubor s informacemi o pracovnících
 - Soubor s informacemi o organizační struktuře
 - Soubor se seznamem nadřízených osob
 - Číselníky
-
- Validační program
 - Co s chybami na vstupu?
 - Dílčí chyby
 - Chyby ohrožující integritu IAM

Datové toky vstupy - HR

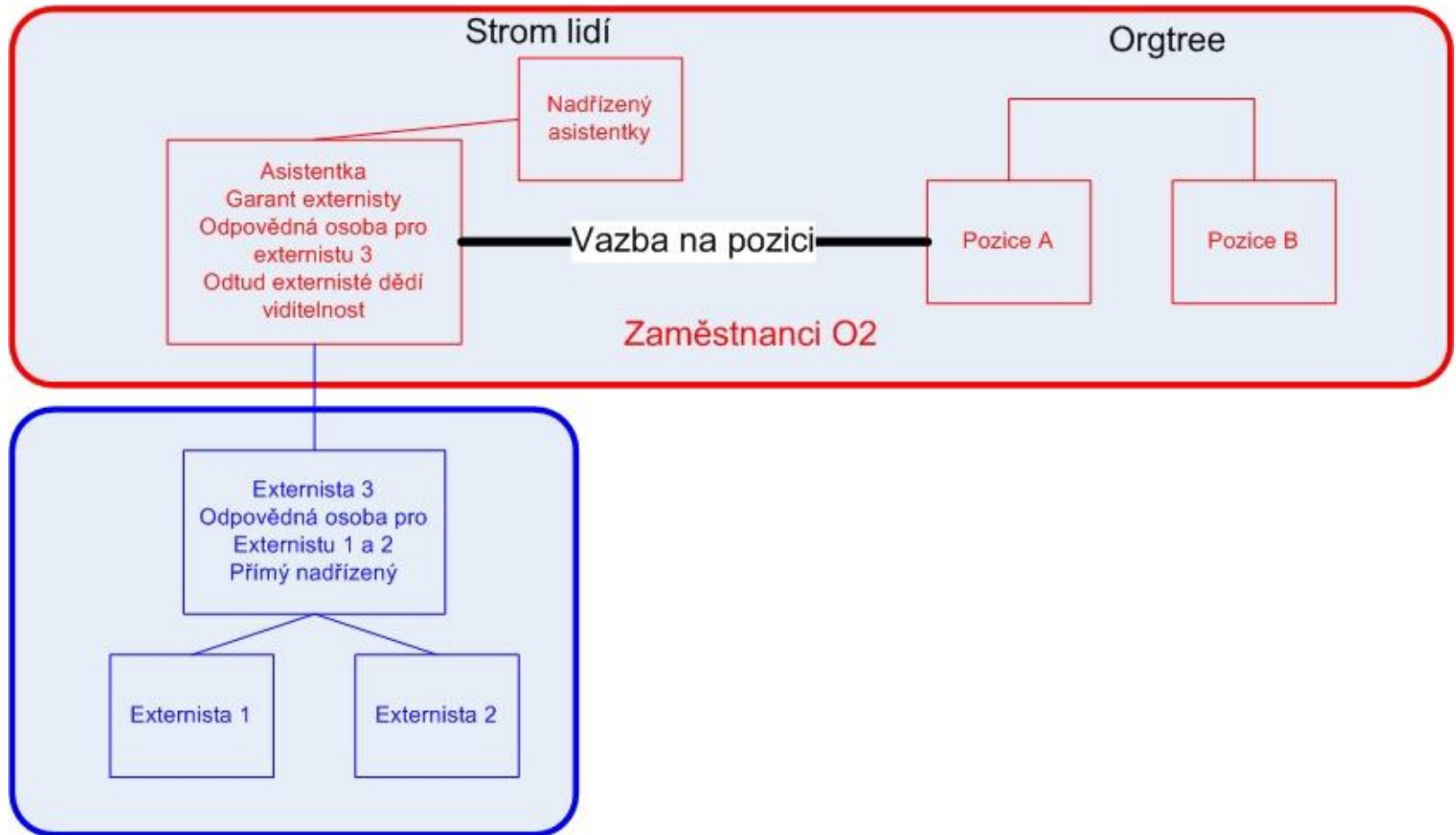
- Načítání dat z HR – periodicky nebo na vyžádání
 - Přes interface HR systému
 - Překladiště – filesystem
 - Potvrzení o úspěšném načtení
 - Chybové zprávy
 - Vracení souboru
- Validace na vstupu, řešení chybových stavů
 - validace po řádcích – kontrola jednotlivých atributů
 - integrita datových souborů.
- Rekonstrukce organizační struktury

Vazba na HR

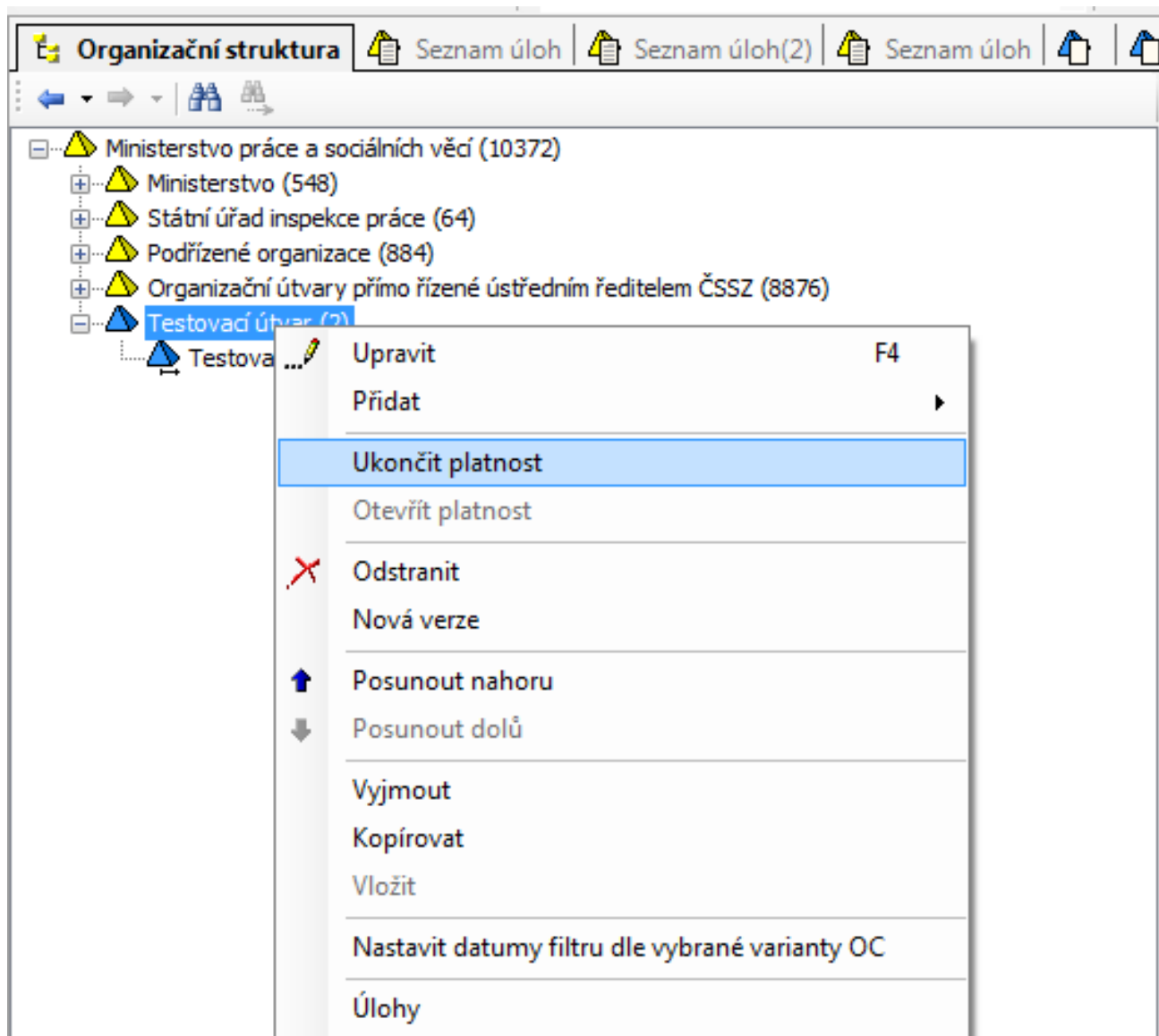
HR SAP jako zdroj dat – **nadřazený systém**:

- Myšlenka na první pohled jednoduchá a bezproblémová
- Řešené problémy:
 - Schvalovací workflow je svázáno s org. strukturou firmy
 - Neobsazené nejvyšší funkce – chybí špička org. stromu
 - Neobsazené funkce schvalovatelů – odvolaní, noví ředitelé
 - Dva zaměstnanci na jednom systemizovaném místě
 - Jeden zaměstnanec na dvou místech (kumulované funkce)
 - Náhlá úmrtí schvalovatelů
 - Externisté, zaměstnanci cizích firem

HR – stromy, systém napojení externistů



HR – jak vypadá takový organizační strom



Vazba na HR

- Myšlenka jednoduchá, ale IAM přece jen vyžaduje některá data navíc a v tomto s určitými problémy:
- Koordinace mezi dvěma nezávislými projekty je náročná a vyžaduje pečlivou přípravu.
- Neočekávané problémy:
 - Neobsazené nejvyšší funkce – chybí špička pyramidy.
 - Neobsazené funkce schvalovatelů – odvolaní, noví ředitelé.
 - Dva zaměstnanci na jednom systemizovaném místě.
 - Jeden zaměstnanec na dvou místech (kumulované funkce).
 - Náhlá úmrtí schvalovatele.
 - Externisté, zaměstnanci cizích firem.

Shrnutí: - Je třeba počítat s výjimkami

- Jestliže bývá personální evidence tradičně přesná, IAM nároky umocňuje

Personálně-systémová workflow

- Načtení nového zaměstnance
- Ukončení pracovního poměru
- Vynětí zaměstnance ze stavu
- Návrat z vynětí zaměstnance ze stavu
- Přejmenování zaměstnance
- Přesun mezi lokalitami

Heslové politiky

- Proces vytváření iniciálních hesel podle heslové politiky dané aplikace
- Proces resetu hesla zaměstnancem jako self-service přes intranetový portál
- Vynucená změna hesla při prvním přihlášení

Propojení s intranetovým portálem organizace

- Systém self-service
- Nahlašování dovolených
- Nepřítomnosti, nemoci ap.

Test

1.otázka HR systém je vůči IAM:

A	<input checked="" type="checkbox"/>	Nadřízený
B	<input type="checkbox"/>	Podřízený
C	<input type="checkbox"/>	Vztah nadřízenosti a podřízenosti nelze určit
D	<input type="checkbox"/>	Záleží na situaci, může být jednou nadřízený a jednou podřízený

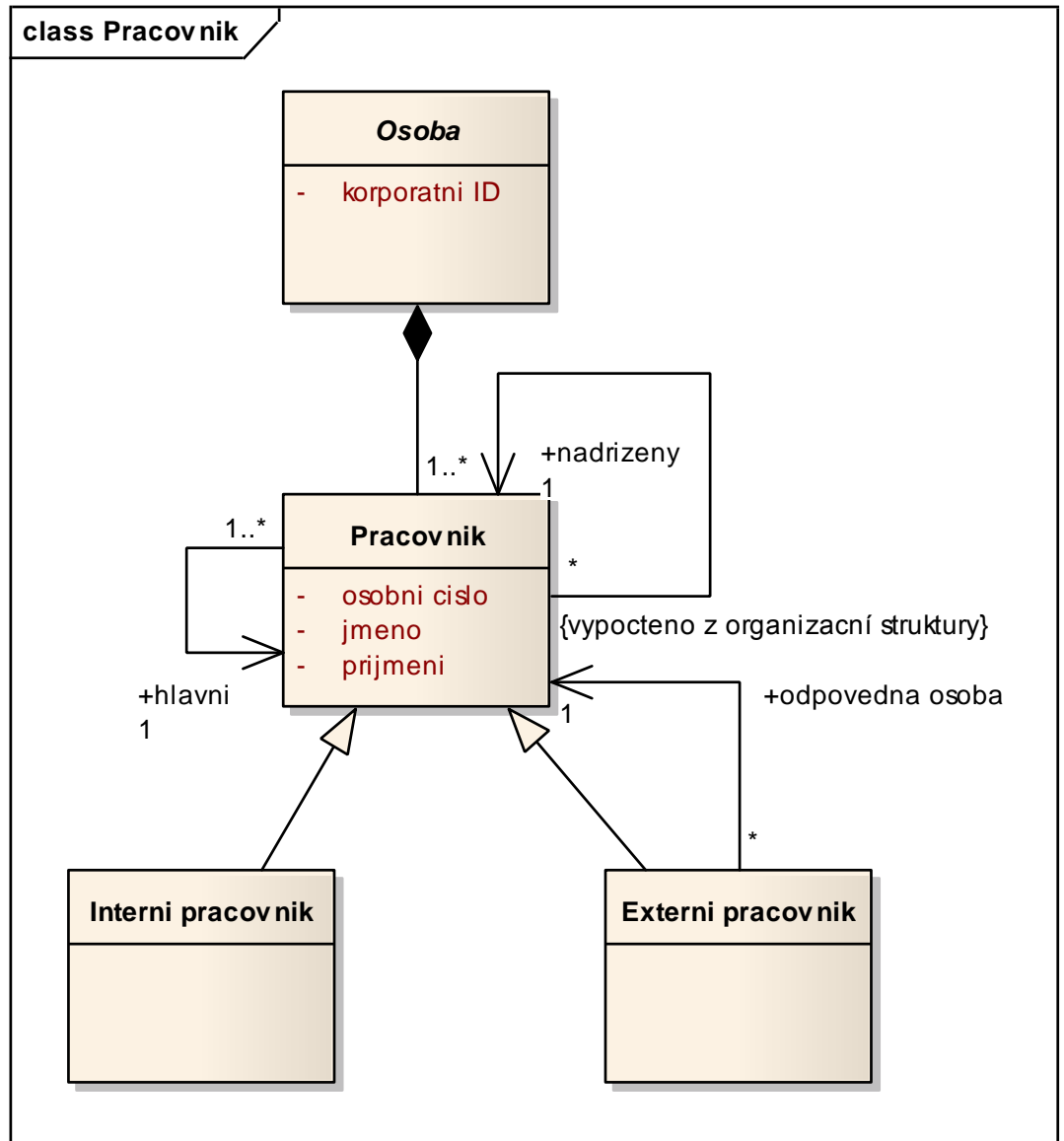


Vnitřní struktura IdM

- Uživatelé
- Aplikace
- Technické účty
- Externisté
- Více pracovních poměrů jednoho uživatele
- Mateřská dovolená, vězení, dlouhodobé nemoci

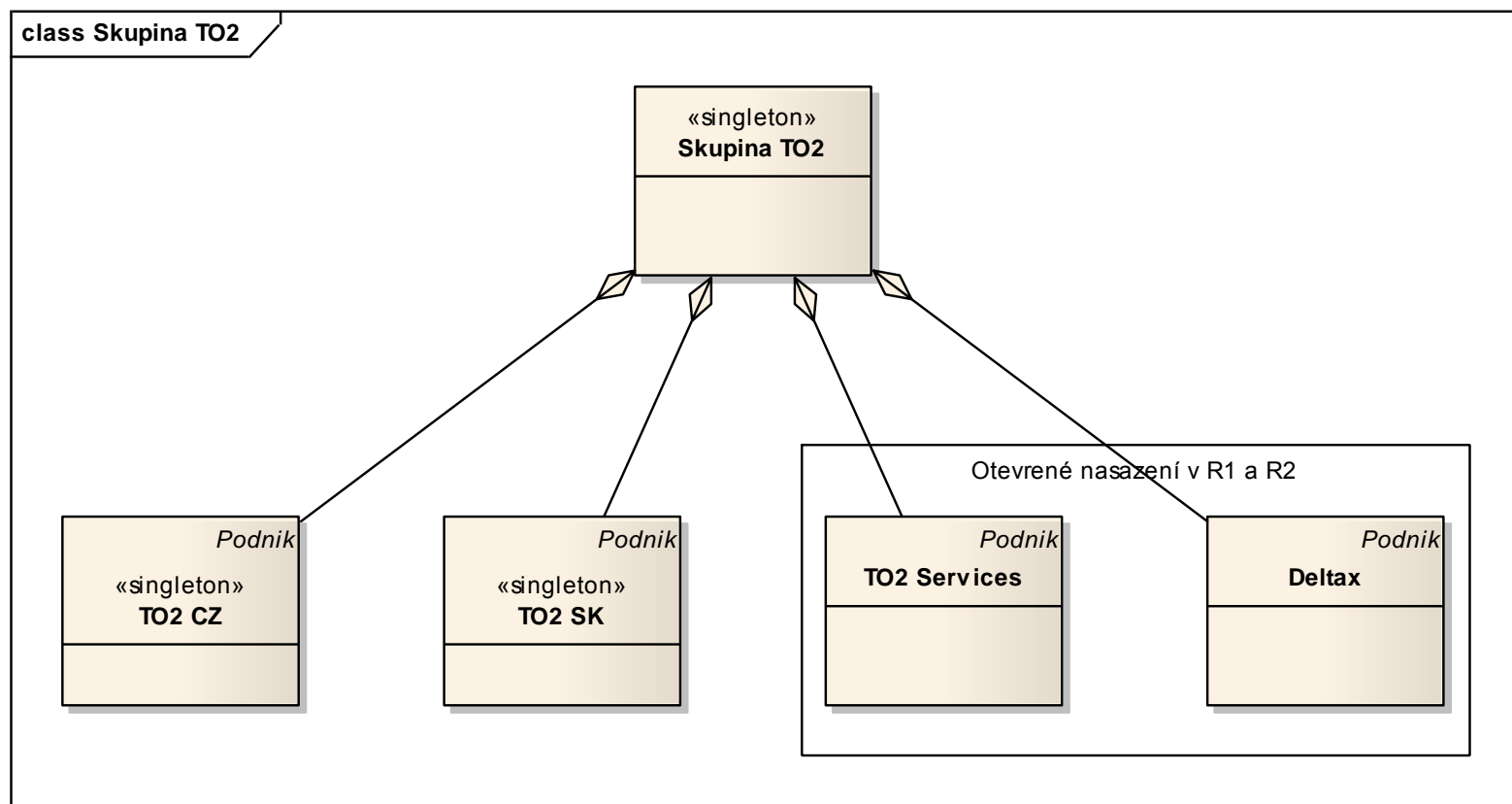
HR – doménový model

- Fyzická osoba může být přímo či nepřímo ve více právních vztazích s organizací:
 - pracovní poměr,
 - dohodu o pracovní činnosti,
 - dohodu o provedení práce,
 - obchodní smlouvu mezi organizací a právnickou osobou.



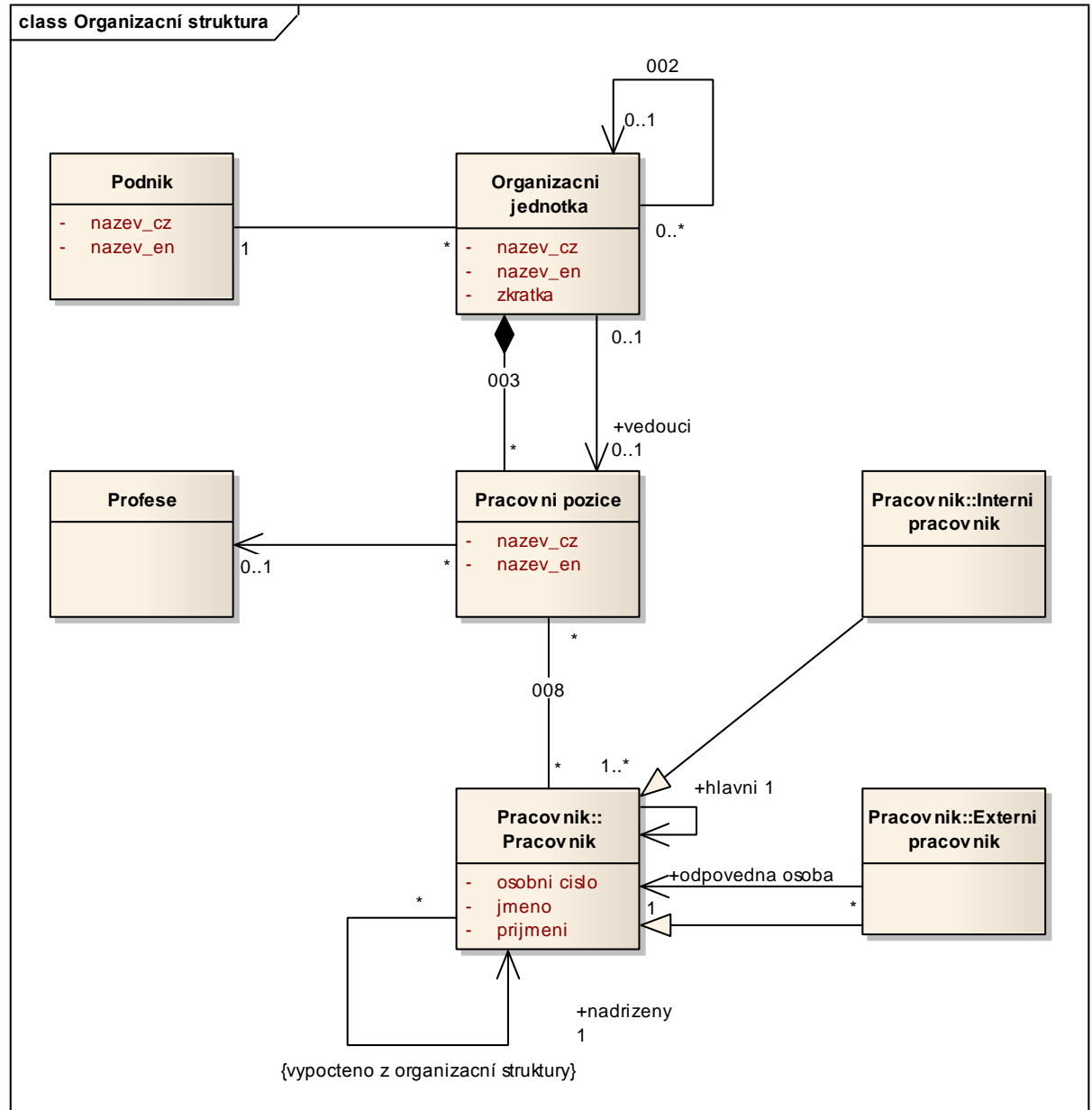
HR – doménový model

Skupina organizací



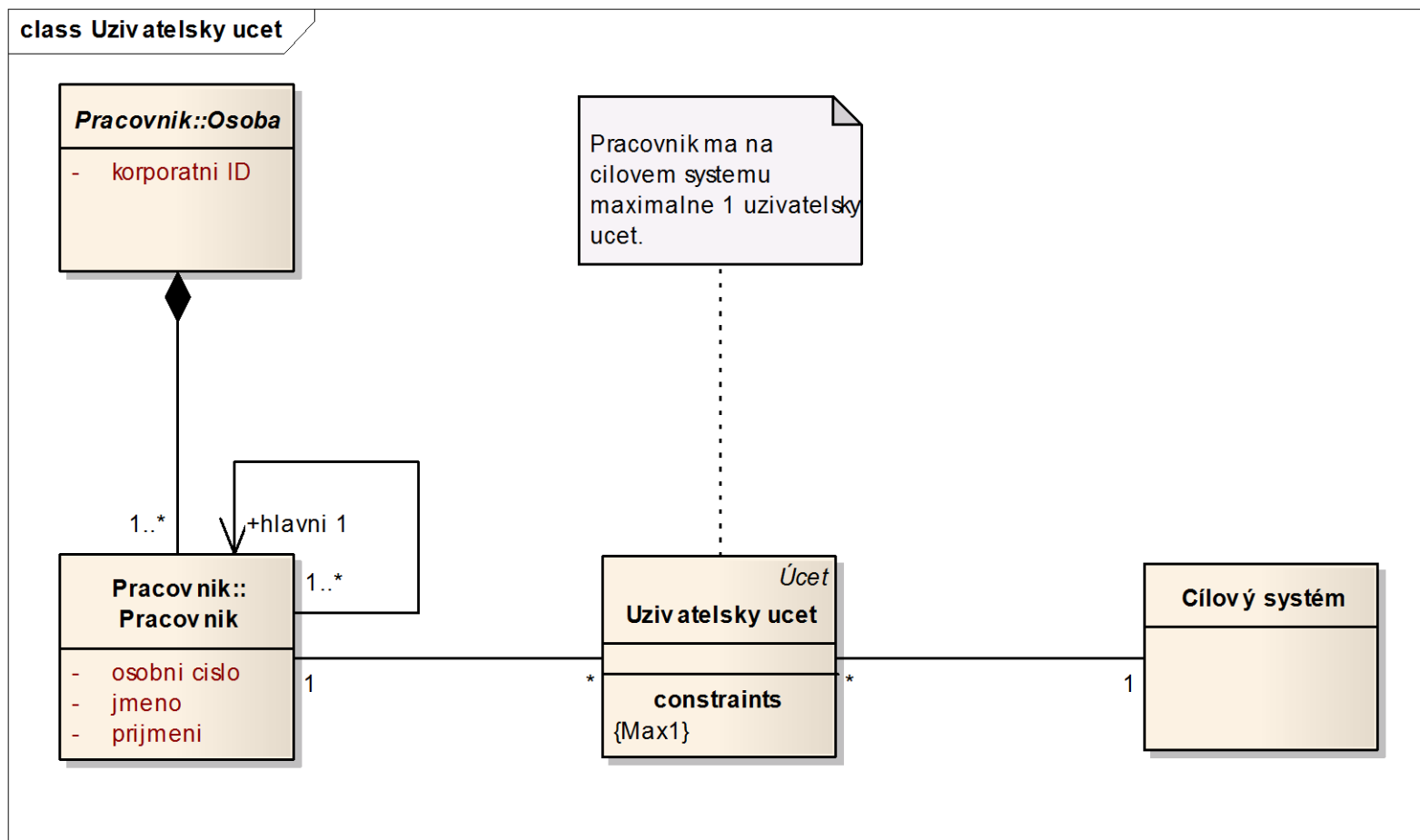
HR – doménový model

Organizační struktura



HR – doménový model

Účty fyzické osoby v cílových systémech



Číselníky

Systém	Číselník	Popis			Poznámka
		Položky	Vazby mezi položky	Způsob načítání: z DB, Souboru, ...	
AD	Číselník typu				
AD	Číselník typu systému				
AD	Identifikátor oprávnění				
AD	Identifikátor uživatele/skupiny				
CMDB	Číselník aplikací	Bude načítán správcem IAM			
Databáze LN Profily					
Neos	Číselník responsibilit Databáze zaměstnanců - funguje jako číselník zaměstnanců				Bude řešeno v rámci R2
Neos	POS Setup				
POS				Databáze	
SAP	Parametry účtů SAP	Bude spravován manuálně. IAM jej automaticky nenačítá			
SAP HR	Číselník profese				
SAP HR	Infotyp 9852 - Evidence externistů				
SAP HR	Infotyp 0000 - Opatření				
SAP HR	Infotyp 0001 - Organizační přiřazení				
SAP HR	Infotyp 0001 - Organizační přiřazení				
SAP HR	Účel zpracování				
Telefonie					Bude řešeno v rámci R2

Test

1.otázka technologický účet je:

A	<input type="checkbox"/>	Účet v operačním systému
B	<input type="checkbox"/>	Účet, který je sdílený více uživateli
C	<input checked="" type="checkbox"/>	Účet, který je využíván službou (procesem)
D	<input type="checkbox"/>	Účet svázaný s konkrétní technologií



Filosofie přidělování přístupových práv

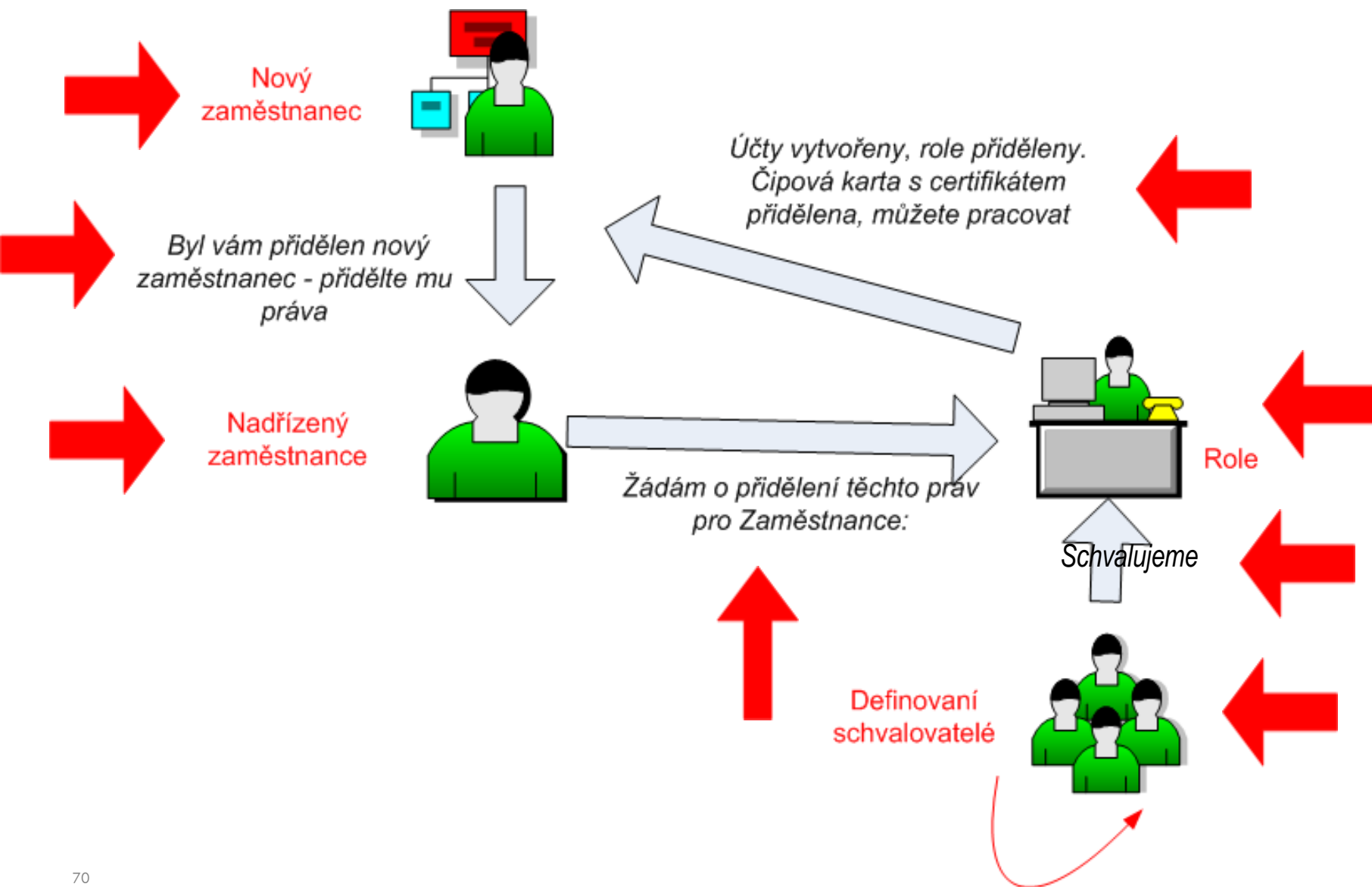
- automatické přidělování
- ruční přidělování - žádosti a schvalování
- odebrání přístupových práv

Filisofie přidělování přístupových práv

- automatické přidělování – na základě znalosti požadavků na pracovní činnosti
 - Přidělování uživateli
 - Přidělování na pozici
 - Přidělování uživateli, pokud se ocitne na konkrétní pozici – podmíněné právo
- ruční přidělování - žádosti a schvalování
- odebírání přístupových práv
 - Při odchodu z pozice
 - Blokování přístupu při dlouhodobé nepřítomnosti
 - Ztráta důvěry
 - Mateřské, vězení

Jak má IAM reagovat při rozporu mezi stavem IAM a stavem v podřízených systémech

Filosofie – o vše se žádá, vše se schvaluje



Filosofie – o vše se žádá, vše se schvaluje

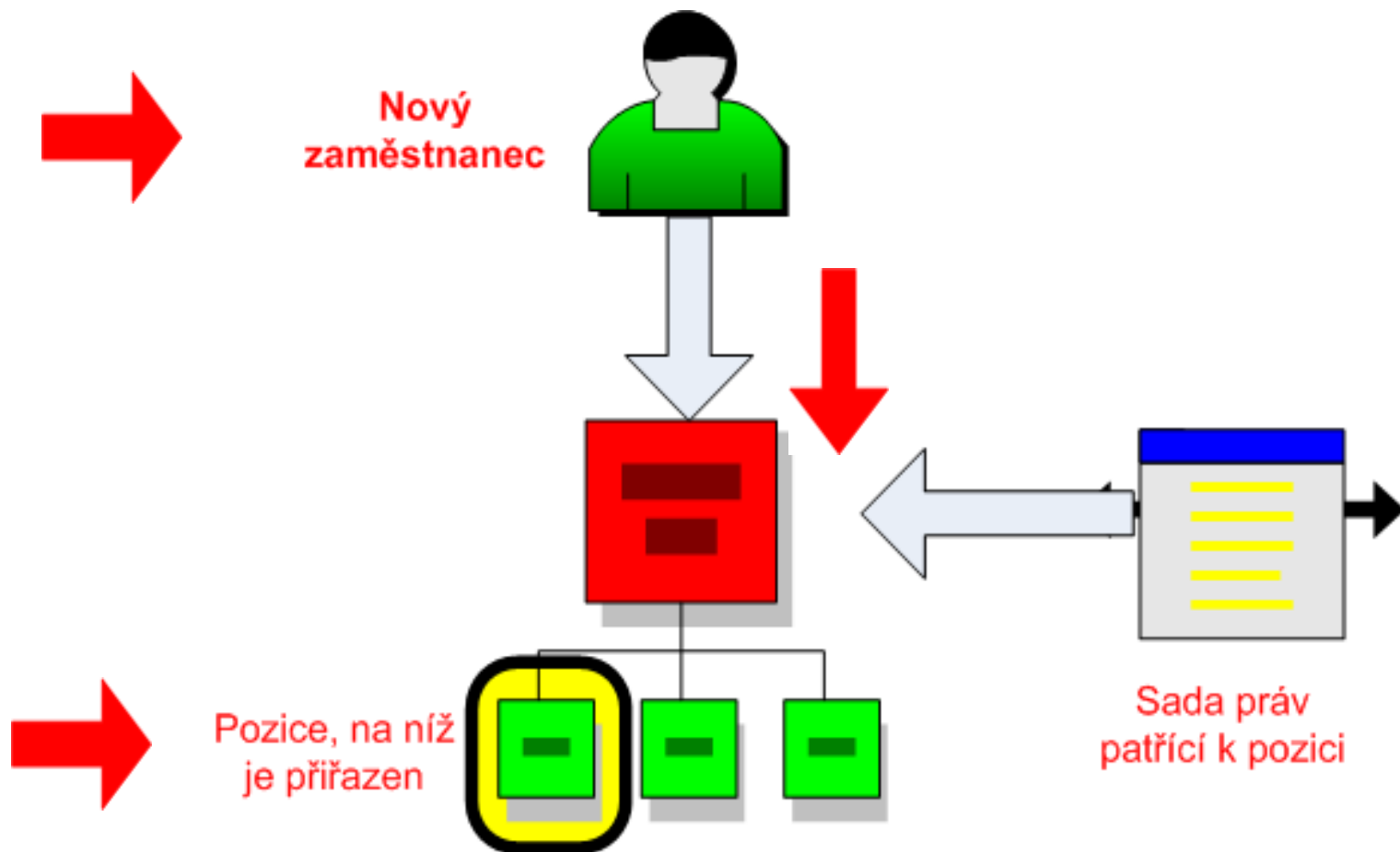
Výhoda:

- nemusí se přesně popsat pracovní pozice
- přidělení každé role je pod individuální kontrolou schvalovatelů

Nevýhoda:

- zátěž na schvalovatele
- není vyřešeno odebírání rolí

Filosofie – automatizace procesů – RBAC model



Filosofie – automatizace procesů – RBAC model

Výhody:

- nižší zátěž na schvalovatele
- je vyřešeno odebírání rolí
- Přidělování práv se řeší přes příchod nebo odchod z pozice

Nevýhoda:

- Musí se přesně popsat pozice

Test

1.otázka Automatické a manuální přidělování přístupových práv:

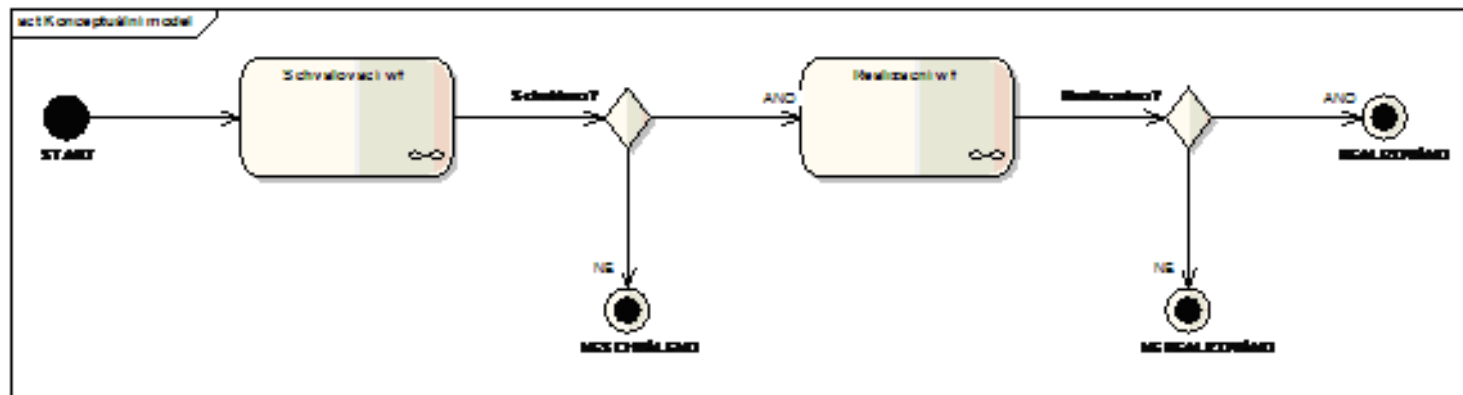
A	<input checked="" type="checkbox"/>	Lze kombinovat
B	<input type="checkbox"/>	Nelze kombinovat
C	<input type="checkbox"/>	Automatické přidělování přístupových práv je v IAM nemožné
D	<input type="checkbox"/>	Manuální přidělování přístupových práv je v IAM nemožné



Workflow a co vše musí řešit

- Paralelní a sériová workflow
- Způsoby vyhodnocování workflow
- Slepé uličky ve workflow
- Jak dlouho musí workflow čekat
- Eskalace
- Delegace
- Zástupy a záskoky

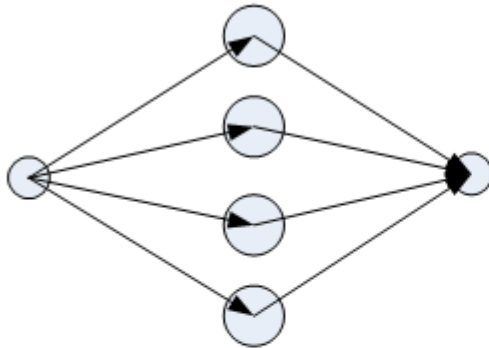
Workflow – schvalovací, realizační



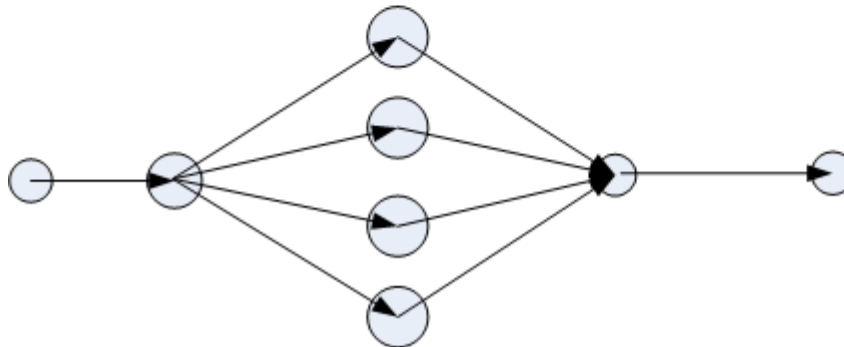
Workflow – paralelní, sériové, kombinace



Sérové wf



Paralelní wf



Kombinované wf

Schvalovací workflow – podle typu role

Delegace

Eskalace

Expirace workflow

Změny schvalovatelů

Vyhodnocování - paralelní

Vyhodnocování - sériové

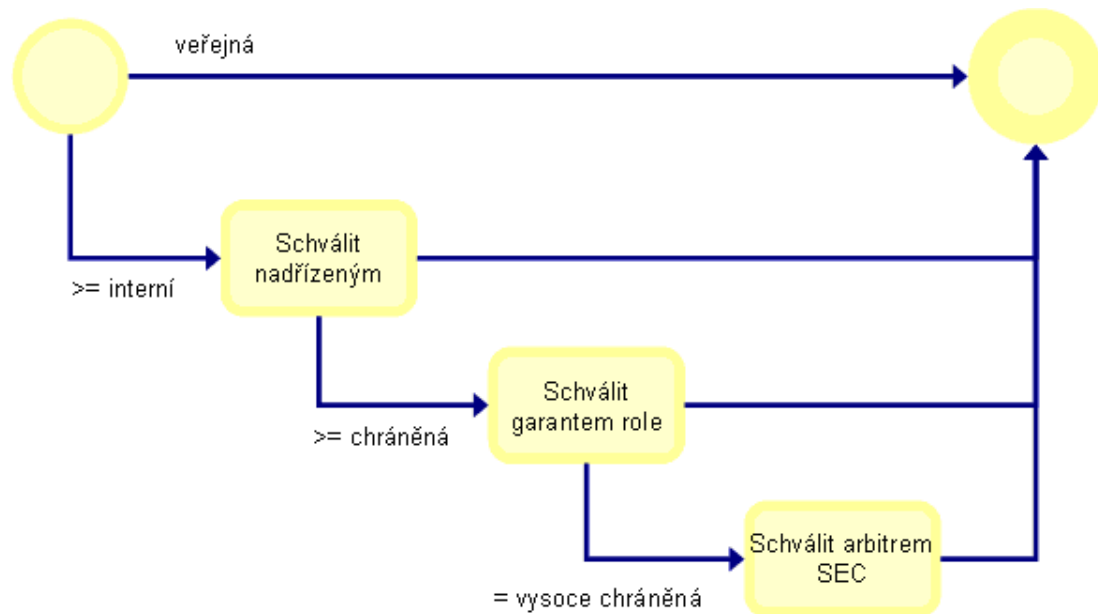
Vyhodnocování - kombinace

Nepřipustit ve workflow slepé uličky

Jak dlouho nechat schvalovateli

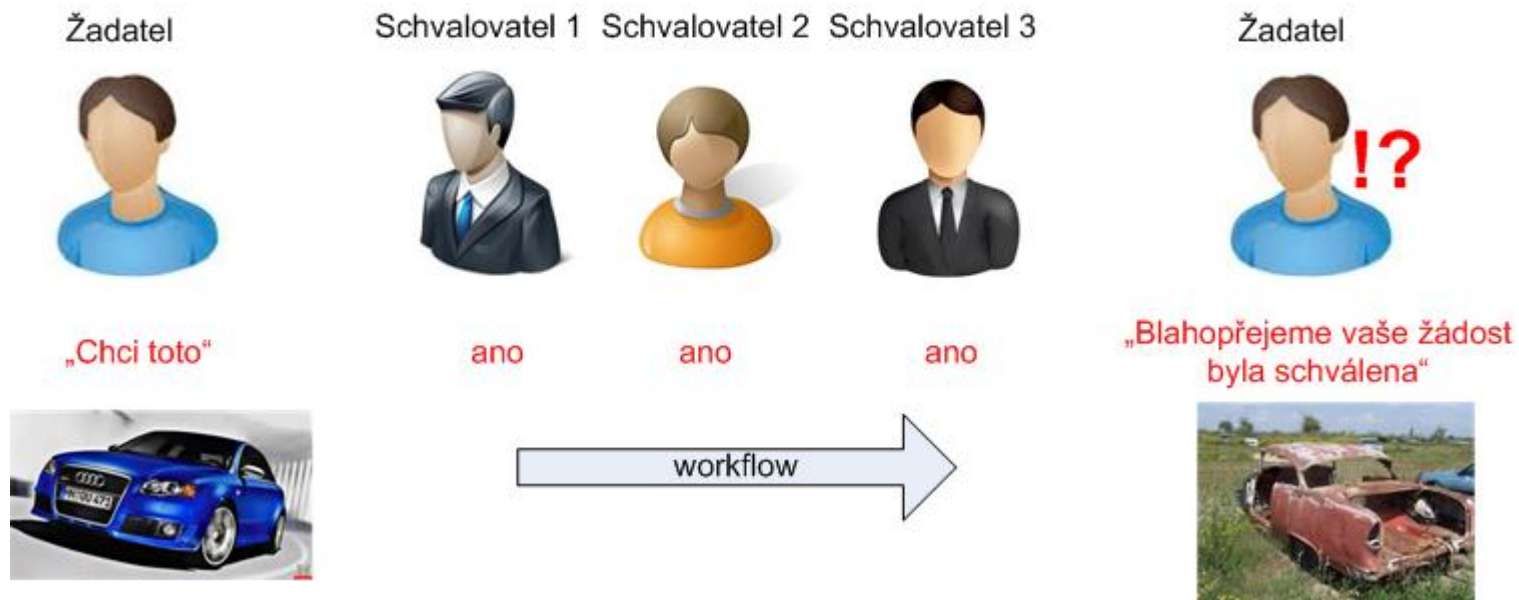
Co s víkendy a svátky

Běžící workflow musí být viditelné v GUI



Schvalovací workflow – může schvalovatel modifikovat žádost?

Workflow s právem modifikace



Schvalovací workflow

- Workflow je klíčové
- Spouští je vždy GUI

Nadřízený

GUI

Žádosti

ITIM a
workflow

Podřízené
systémy
ITAM a AD

Aplikace



Aplikace 1
Uživatel xy
Role a _/
Role b
Role c _/

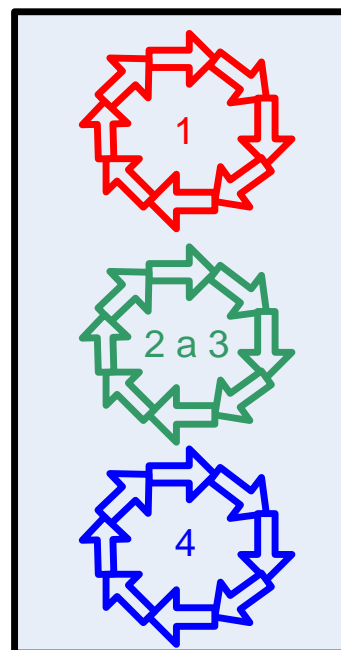
Aplikace 2 a 3
Uživatel xy
Role d
Role e _/

Aplikace 4
Uživatel xy
Role f _/
Role g _/

Aplikace 1
Uživatel xy
Role a _/
Role c _/

Aplikace 2 a 3
Uživatel xy
Role e _/

Aplikace 4
Uživatel xy
Role f _/
Role g _/



Uživatel xy

Aplikace 1
Role a _/
Role c _/

Aplikace 2 a 3
Role e _/

Aplikace 4
Role f _/
Role g _/
Role q
Role r

Aplikace 1

Aplikace 2

Aplikace 3

Aplikace 4

Schvalovací workflow – high level pohled

Pozice	Žádost podává	1. kolo workflow 1. schvalovatel	2. kolo workflow 2. schvalovatel	3. kolo workflow 3. schvalovatel
Ústřední ředitel	Ústřední ředitel	Ústřední ředitel	Ředitelé odpovědných organizačních útvarů (viz kap. 5.1) s možností delegace	
Náměstek ÚŘ	Přímý nadřízený zaměstnance (podle organizační struktury ČSSZ) s možností delegace	Ústřední ředitel s možností delegace náměstka		
Vrchní ředitelé úseků ústředí				
Ředitelé odborů úseku 1				
Ředitelé pracovišť, PSSZ a MSSZ Brno				
Ředitelé OSSZ		Ředitel pracoviště s možností delegace		
Zaměstnanci OSSZ		Ředitel OSSZ s možností delegace		
Zaměstnanci pracoviště		Ředitel pracoviště s možností delegace		
Zaměstnanci PSSZ		Ředitel PSSZ s možností delegace		
Zaměstnanci MSSZ Brno		Ředitel MSSZ s možností delegace		
Zaměstnanci ústředí (mimo náměstka ÚŘ, vrchních ředitelů úseků ústředí a ředitelů odborů úseku 1)		Ředitel odboru na ústředí s možností delegace Ředitel úseku na ústředí s možností delegace (v případě žádostí pro ředitele odboru)		
Přístup k internetu		Ředitel odboru 22 s možností delegace	Ředitel úseku 5 s možností delegace	Ředitel úseku 2 s možností delegace

Schvalovací workflow – konkrétní pohled

Č.	Oblast	Aplikace /moduly	Vede no v AAA	1. schvalovatel	2. schvalovatel	3. schvalovatel
	DMS	DKA	DKA	OSSZ - Ředitel OSSZ s možností delegace Pracoviště - Ředitel pracoviště s možností delegace PSSZ - Ředitel PSSZ s možností delegace MSSZ - Ředitel MSSZ s možností delegace Ústředí - Ředitel odboru na ústředí s možností delegace	odbor 51 <i>Jen pro informaci</i>	úsek 4 <i>Jen pro informaci</i>
		DKE	DKE			
		DKP	DKP			
		DKS	DKS			
	ZDD	ZDD	ZDD	OSSZ - Ředitel OSSZ s možností delegace Pracoviště - Ředitel pracoviště s možností delegace PSSZ - Ředitel PSSZ s možností delegace MSSZ - Ředitel MSSZ s možností delegace Ústředí - Ředitel odboru na ústředí s možností delegace	odbor 42	odbor 51 <i>Jen pro informaci</i>

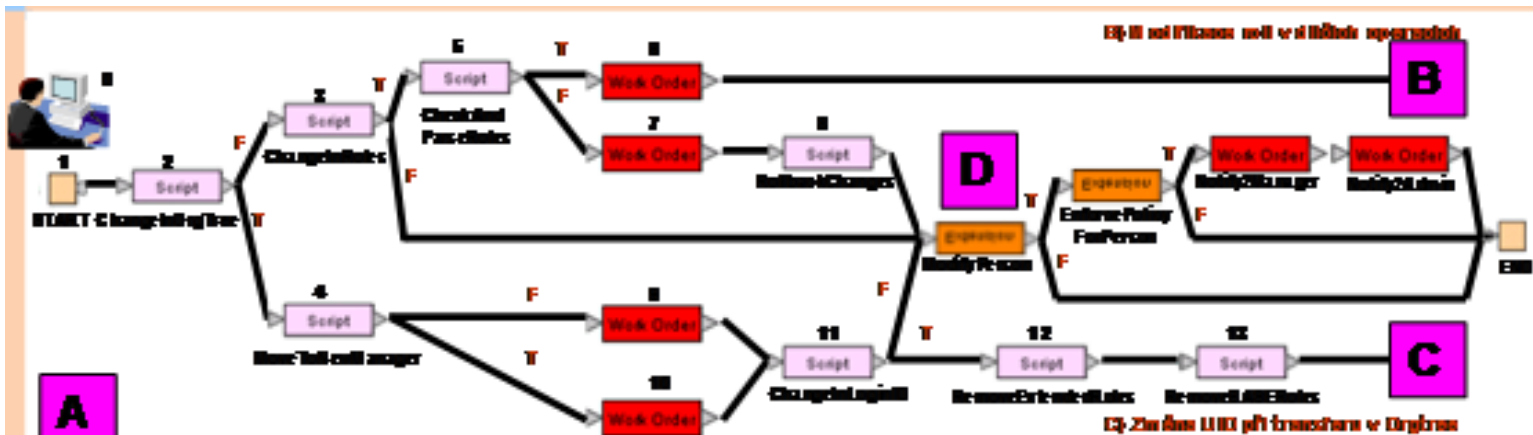
Personálně-systémová workflow

- Načtení nového zaměstnance
 - Ukončení pracovního poměru
 - Vynětí zaměstnance ze stavu
 - Návrat z vynětí zaměstnance ze stavu
 - Přejmenování zaměstnance
 - Přesun mezi lokalitami
-
- Jak má IM určit schvalovatele ? Problematika určení schvalovatele podle jména
 - Kdo schvaluje generálního ředitele ?
 - Časy do kdy schválit
 - Soboty, neděle, svátky

Workflow obecně

- Každé workflow (personální, systémové i schvalovací) má definovány účastníky a je závislé na jejich spolupráci a součinnosti
- Schvalovací workflow je sériové, tj. schvalovatelé schvalují požadavky po sobě. každý má lhůtu 6 kalendářních dní, po 3 dnech je zasílána 2. notifikace
- V případě, že je konkrétní zaměstnanec v pozici navrhovatele rolí i jejich schvalovatele, dojde k jejich automatickému schválení (včetně případných delegací); toto není provedeno, pokud je konkrétní zaměstnanec v pozicích obou schvalovatelů
- Po nastavení **delegace** přebírá delegovaný podřízený všechna práva svého nadřízeného
- Po určité době workflow **eskaluje** na nadřízeného
- **Žádné workflow se nikdy nesmí dostat do slepé uličky**

Workflow obecně



0. **Manager** upraví seznam rolí nebo z HR importu se přidá, změní, popř. zmažne osobu
1. **Start** – Start workflow
2. **Script** – Vyhodnocení zda se změnil atribut osoby „department“, tedy její pozice v OrgTree
3. **Script** – Vyhodnocení zda se změnil atribut osoby „role“
4. **Script** – Vyhodnocení zda se mění se změnou „departmentu“ i „manager“
5. **Script** – Vyhodnocení logičnosti změny rolí (odebrání base role aniž by se neodebrali extende d role, odebrání rolí do závislého systému, role neplatná v dané oblasti OrgTree, apod ...) a rozklad změn rolí (přidání, odebrání, seskupení podle aplikací).
6. **Notify** – Žadatel s tím, že jeho požadavky jsou rozděleny do dílčích operací, vždy s request ID.
7. **Notify** – Neodvolaná změna rolí směřovaná na žadatele (typicky Manager)
8. **Script** – Vrázení sady rolí do původní podoby
9. **Notify** – „malá“ změna pozice v OrgTree a mail na stávajícího managera, že došlo k přesunu jeho podřízeného. Stávající manager je upozomen, aby zrevizoval přiřazení ROLÍ
10. **Notify** – „velká“ změna pozice v OrgTree a mail na stávajícího a nového managera, že jednomu ubyl a druhému přibyl podřízený. Nový manager je zároveň upozomen, aby zrevizoval přiřazení ROLÍ
11. **Script** – Vyhodnocení, zda se bude měnit i login do aplikací
12. **Script** – Odebrání rozšiřujících rolí
13. **Script** – Odebrání základních rolí s notifikací admina

Workflow – Příklady

Založení nebo zrušení uživatele v DXI Managerovi
Zařazení uživatele na pozici
Obnovení hesla k účtu
Žádost o přidání Oprávnění nebo Role uživateli
Žádost o opětovné schválení Oprávnění nebo Role uživateli
Žádost o odebrání Oprávnění nebo Role uživateli
Žádost o přidání Sady k pozici
Žádost o opětovné schválení Sady k pozici
Žádost o odebrání Sady z pozice
Žádost o změnu plánovaných termínů přidání/odebrání práva
Žádost o přiřazení sady externistovi na osobní číslo
Odvolání dosud nezpracované žádosti
Nastavení a zrušení delegace svých povinností ve schvalování
Žádost o dočasné zastupování uživatele na pozici
Žádost o dočasný překryv oprávnění při změně pozice
Suspendování přístupů uživatele
Obnovení suspendovaných přístupů uživatele
Žádost o přidání Práva do Role nebo Sady
Žádost o odebrání Práva z Role nebo ze Sady
Žádost o vytvoření nového Oprávnění
Žádost o zrušení Oprávnění
Žádost o vytvoření nové Role nebo Sady
Žádost o zrušení Role nebo Sady
Žádost o změnu [Garanta] Práva
Žádost o změnu atributů práva mimo [Garanta] a [Bezpečnostní klasifikace]
Žádost o změnu [Bezpečnostní klasifikace] Práva
Žádost o technický přístup (vznik nového tech. účtu)
Žádost o přidání uživatele technického přístupu
Žádost o odebrání uživatele technického přístupu
Žádost o přidání práva technického přístupu
Žádost o odebrání práva technického přístupu
Žádost o změnu Vlastníka technického přístupu
Žádost o zrušení technického přístupu (zrušení tech. účtu)
Sdílený disk v AD - přidání
Sdílený disk v AD - odebrání
Zrušení libovolné běžící žádosti
Přesměrování běžící žádosti na jiného schvalovatele
Vytváření a rušení všech editovatelných DXI entit
Změny všech atributů všech editovatelných DXI entit
Vytváření a rušení všech druhů vazeb mezi editovatelnými DXI entitami
Změna předpisů pro průběh workflow

Uživatelé

- Uživatelé aplikací
- Uživatelé v pozicích žadatelů, resp. jejich delegátů, o uživatelská oprávnění
- Uživatelé v pozicích schvalovatelů, resp. jejich delegátů, uživatelských oprávnění
- Operátorky registračních autorit
- Administrátoři/místní správci
- Administrátoři IM a AM

Schvalovací workflow - příklady

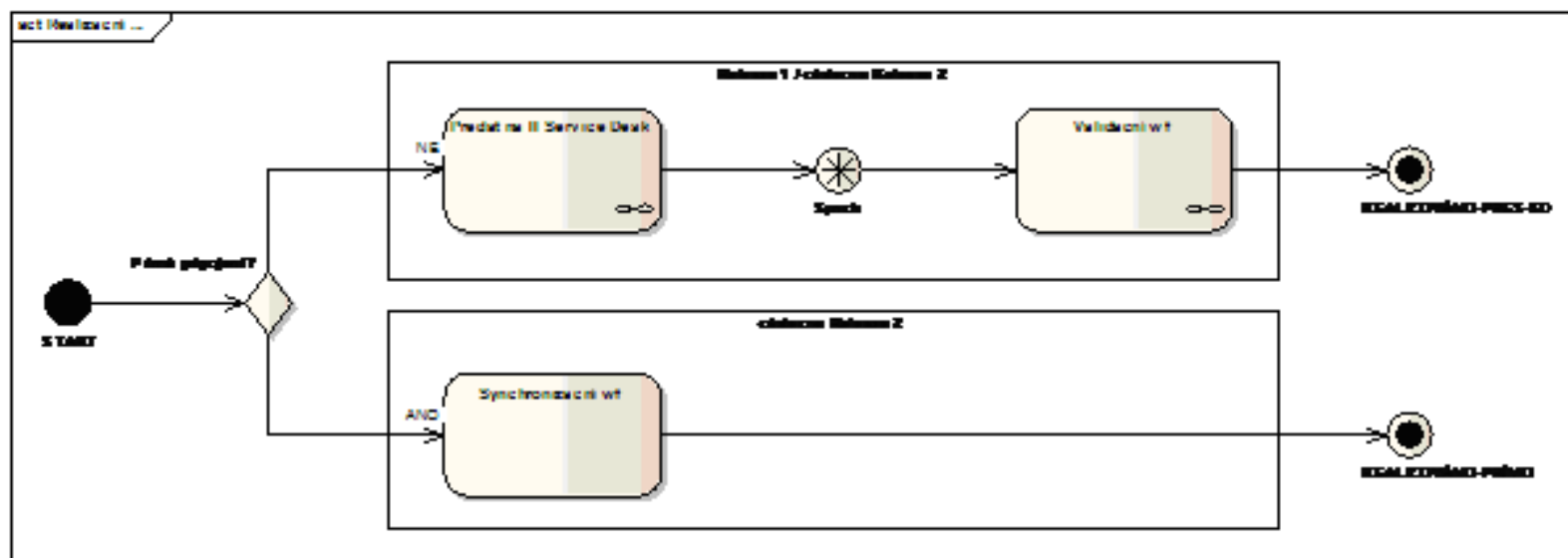
- Přidání oprávnění do role
 - Přidání aplikace
 - Přidání oprávnění do aplikace
 - Přidání oprávnění uživateli
 - Přidání role uživateli
- Stejně modifikace a odebrání – workflow nemusí být nutně stejná

Hromadná workflow

- Hromadné zadávání požadavků
 - Vstup přes formulářové okno v GUI nebo ze souborů
- Hromadné workflow je netriviální a provází ho řada problémů. IAM produkty jej vidí jinak než je požadováno nebo jej nepodporují

Hromadná schvalování – i právní problém – schvalovatel musí vidět, co podepisuje

Realizační workflow



Test

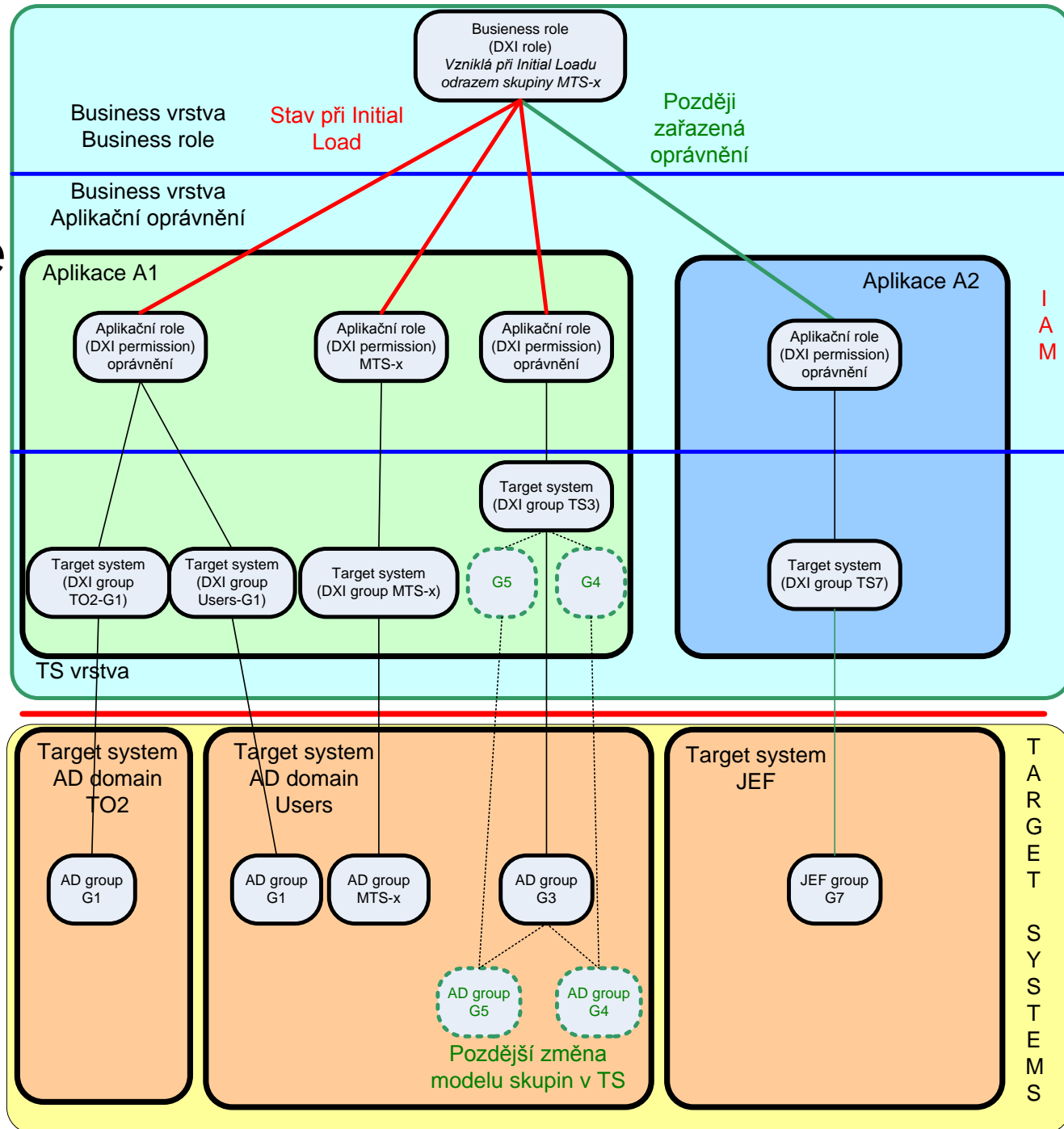
1.otázka Co nepetří do schvalovacího workflow:

A	<input type="checkbox"/>	Notifikace
B	<input type="checkbox"/>	Eskalace
C	<input type="checkbox"/>	Delegace
D	<input checked="" type="checkbox"/>	Zapsání práva přiděleného uživateli do cílového systému

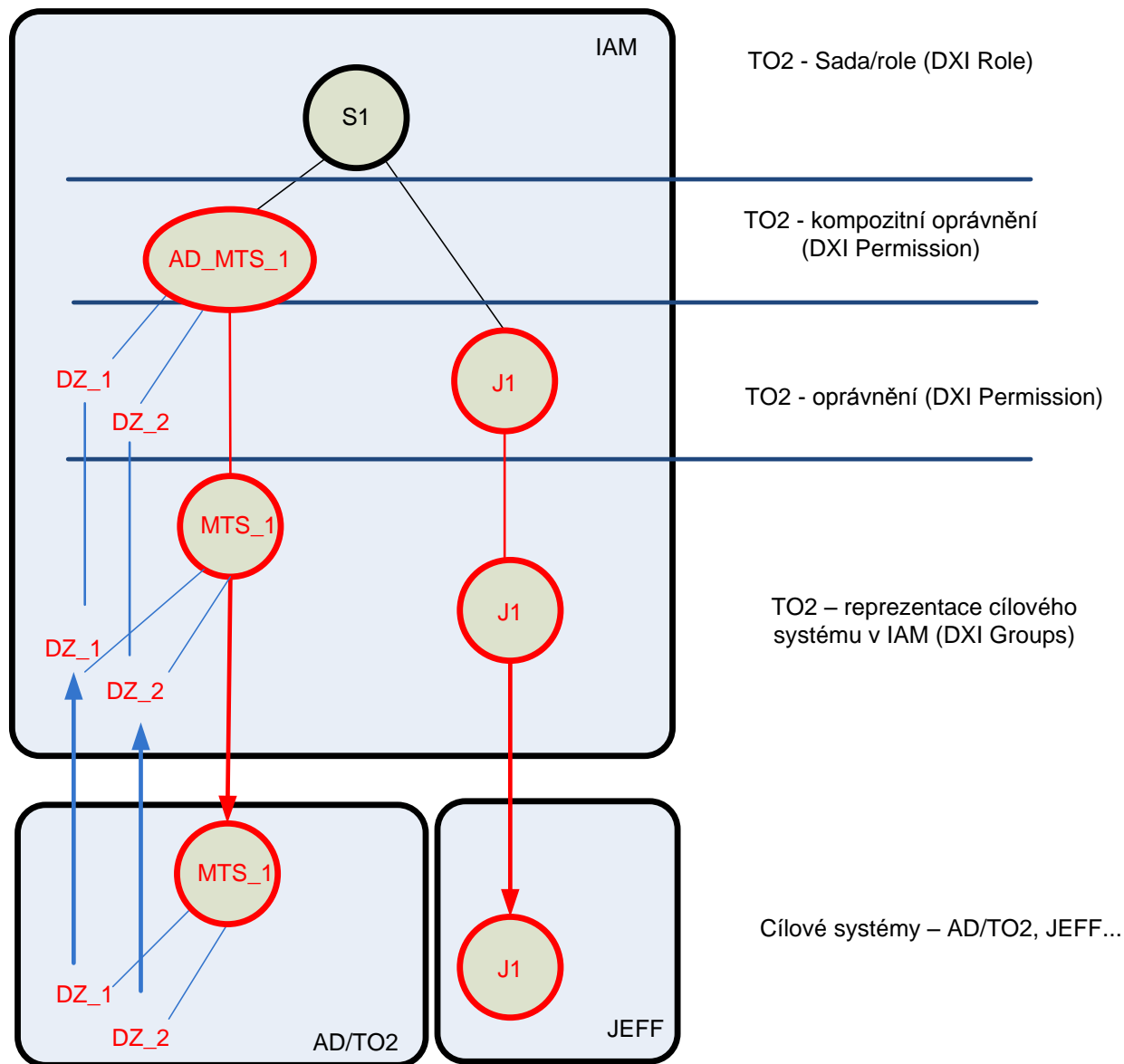


Hierarchie, role sady, oprávnění

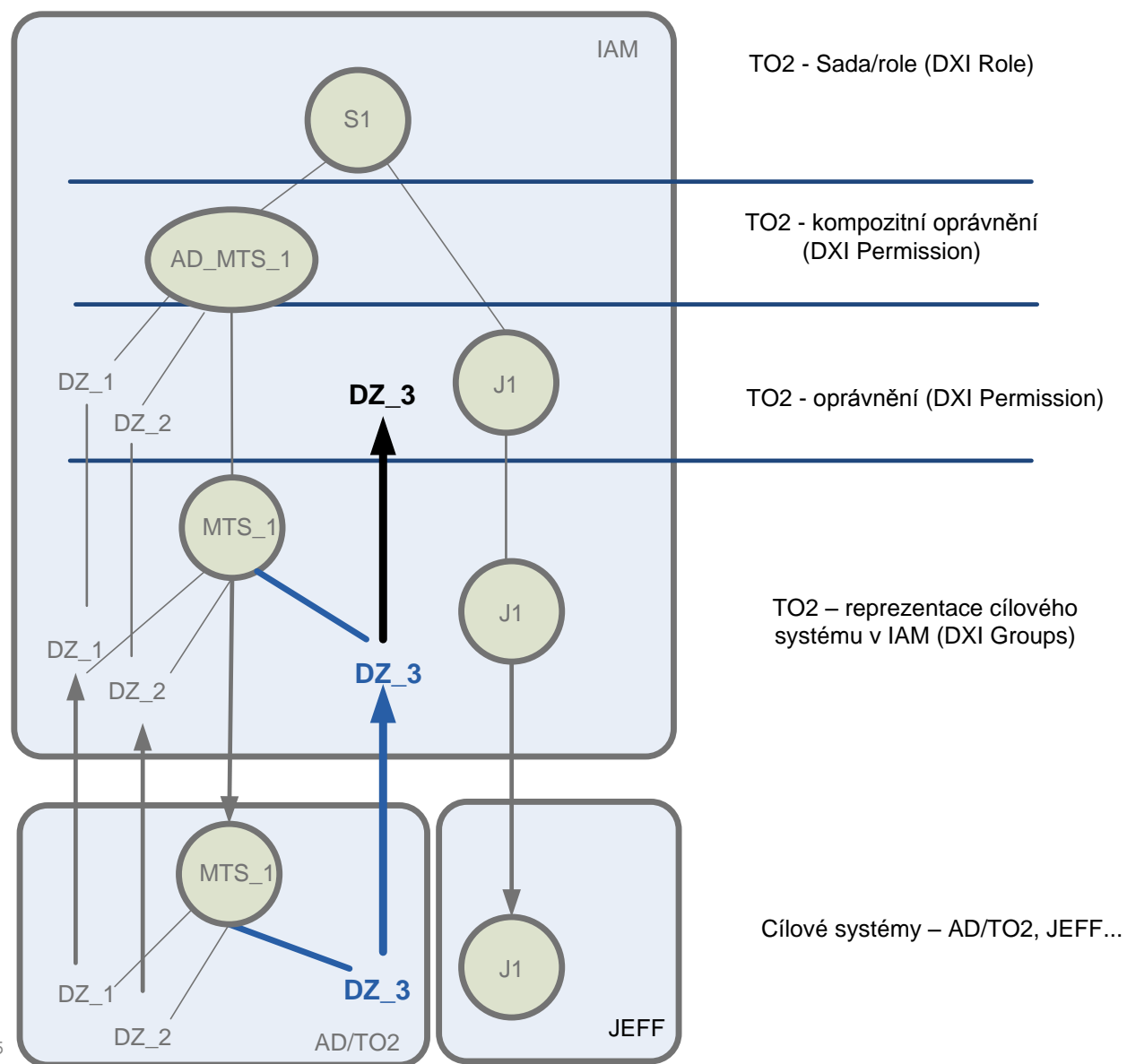
Hierarchie business vrstva, cílové systémy



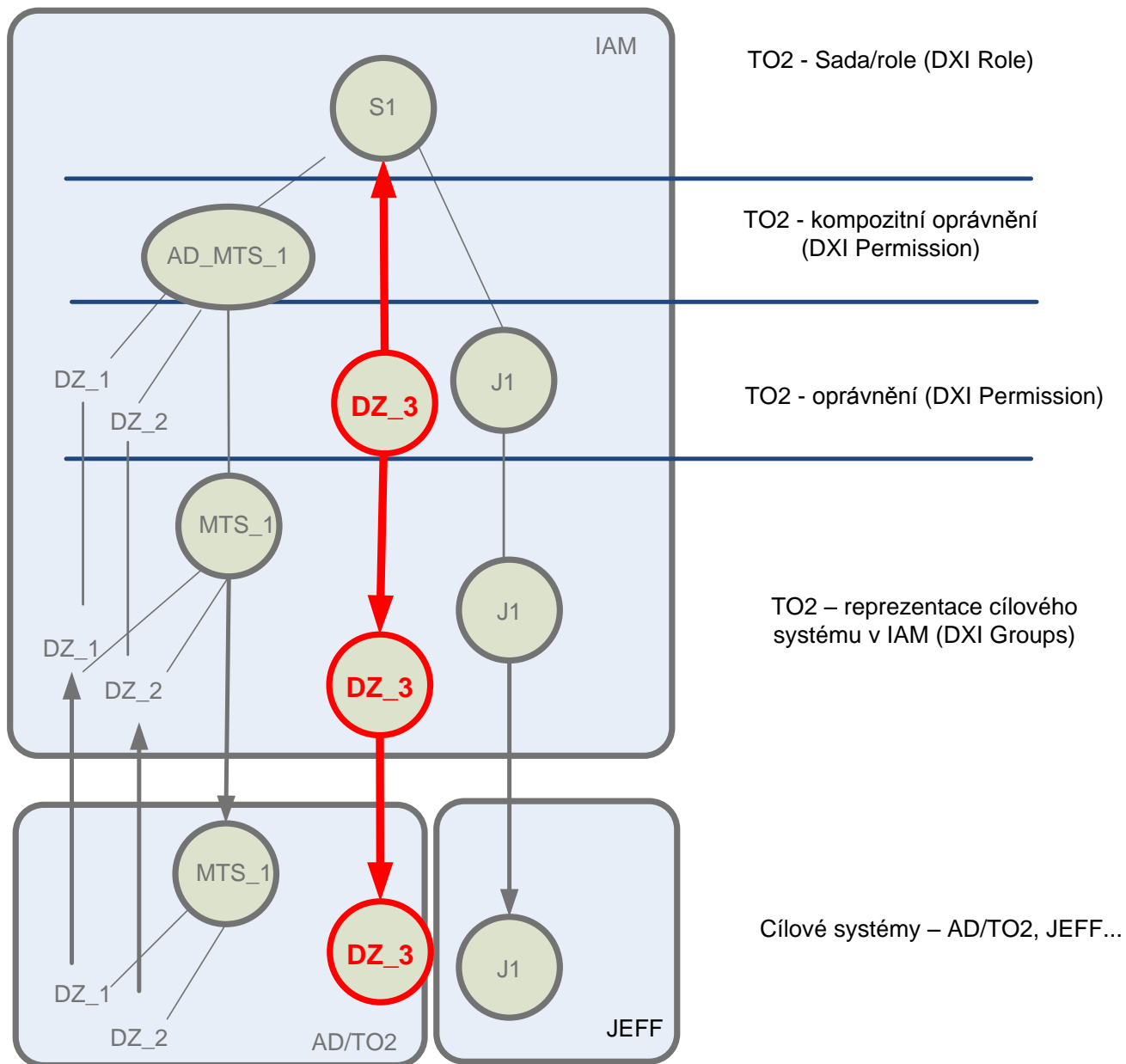
Hierarchie stav po úvodním načtení



Hierarchie stav řízení zdola



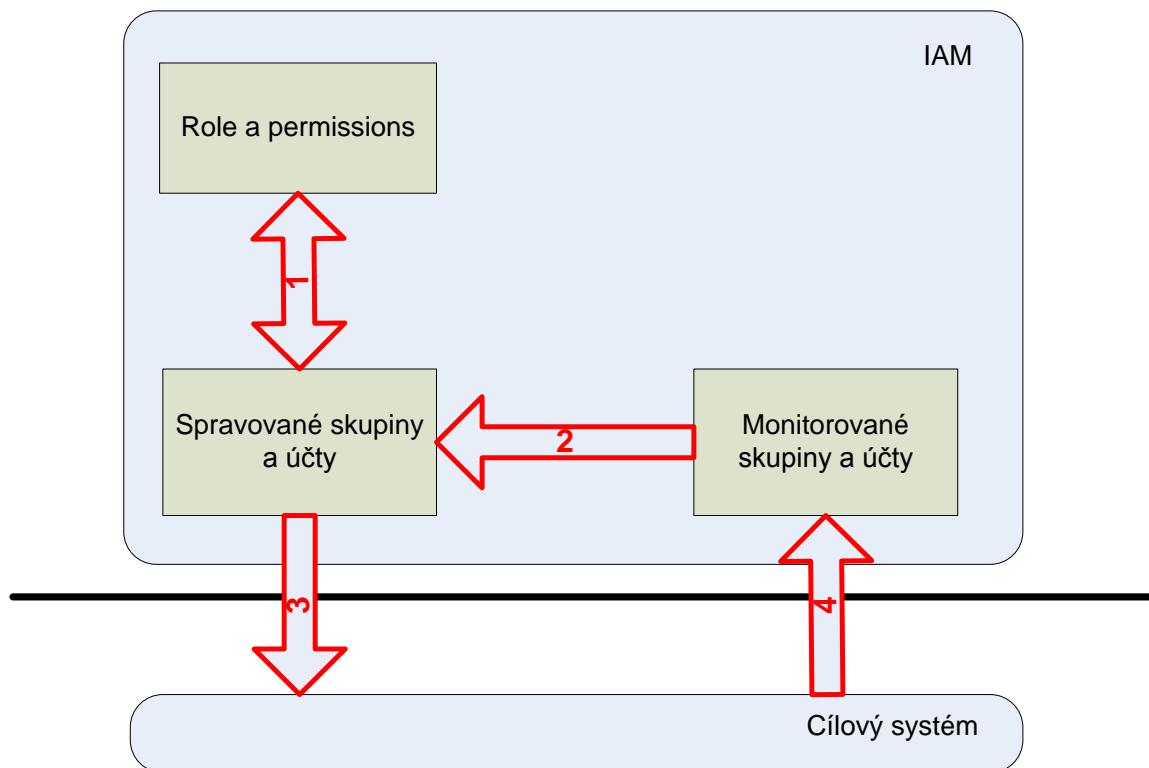
Hierarchie stav řízení zhora



Hierarchie stav řízení zhora – co se stane když

Neshoda mezi stavem v IAM a stavem načteným z podřízeného systému

- Přepíše se v cíl.systému podle IAM
- IAM se přepíše podle cílového systému
- Řeší se případ od případu – nevyřešené stavy
- IAM notifikuje neshodu a volá po vyřešení



Test

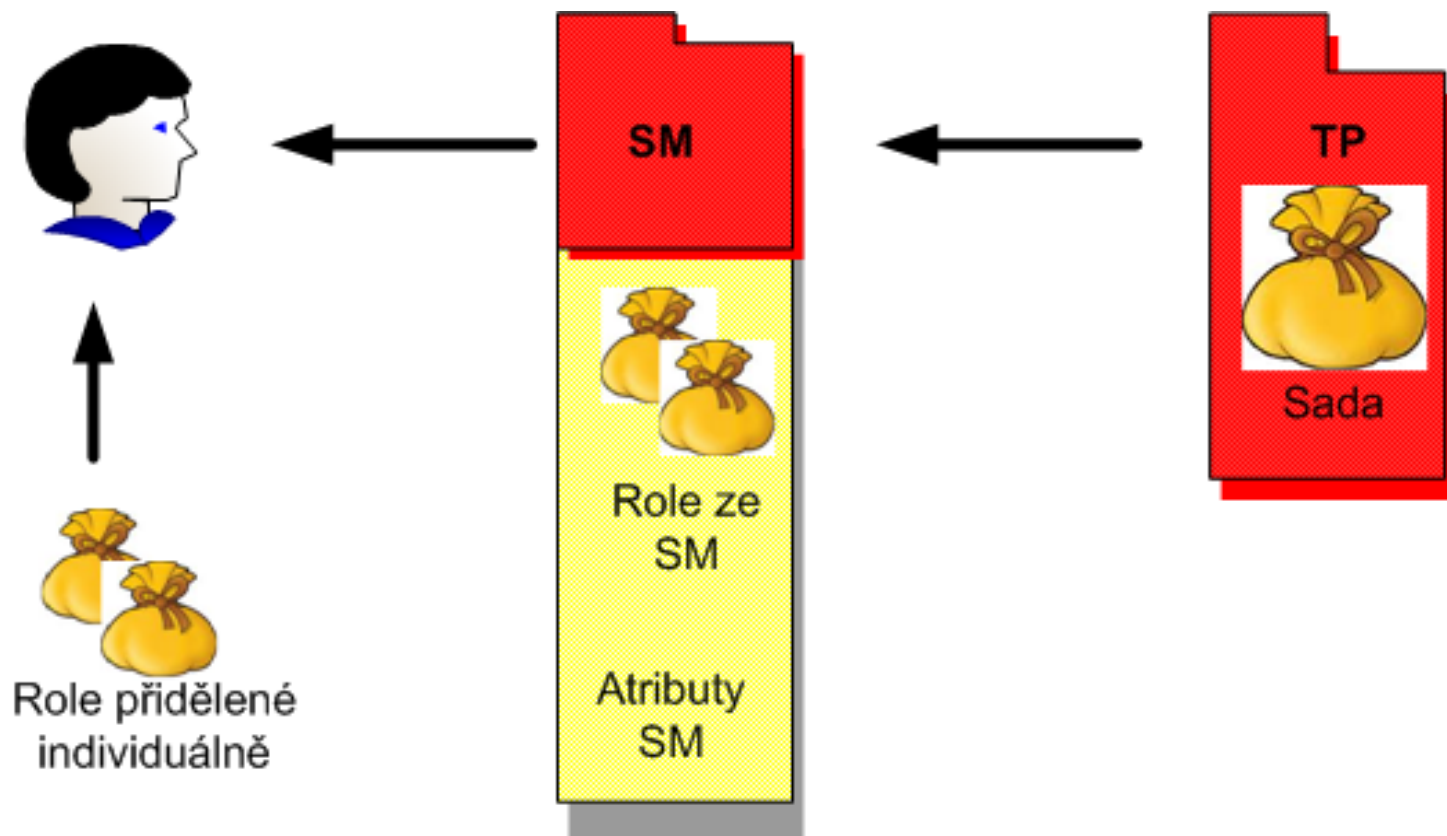
1.otázka Hledejte nesprávnou odpověď na to, jak může IAM reagovat na neshodu při načítání stavu z cílových systémů:

A	<input type="checkbox"/>	IAM si přepíše stav podle cílového systému
B	<input type="checkbox"/>	IAM si přepíše svůj stav do cílového systému
C	<input checked="" type="checkbox"/>	IAM ponechá oba stavy (v IAM i cílovém systému) nezměněny
D	<input type="checkbox"/>	IAM notifikuje neshodu a rozhodnout musí člověk

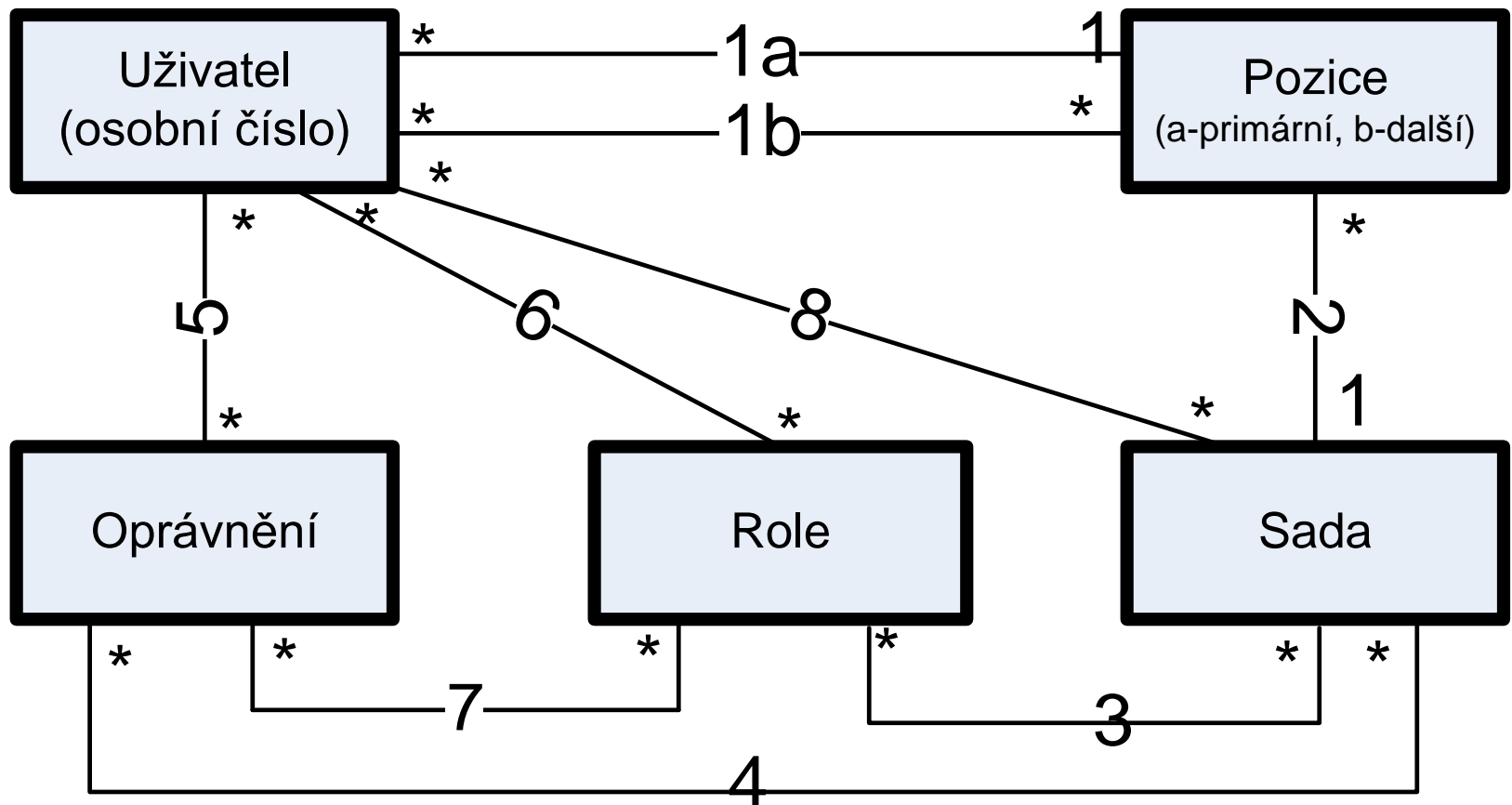


Oprávnění vztažená k uživateli
a
oprávnění vztažená k pozici,
jakou uživatel aktuálně zastává

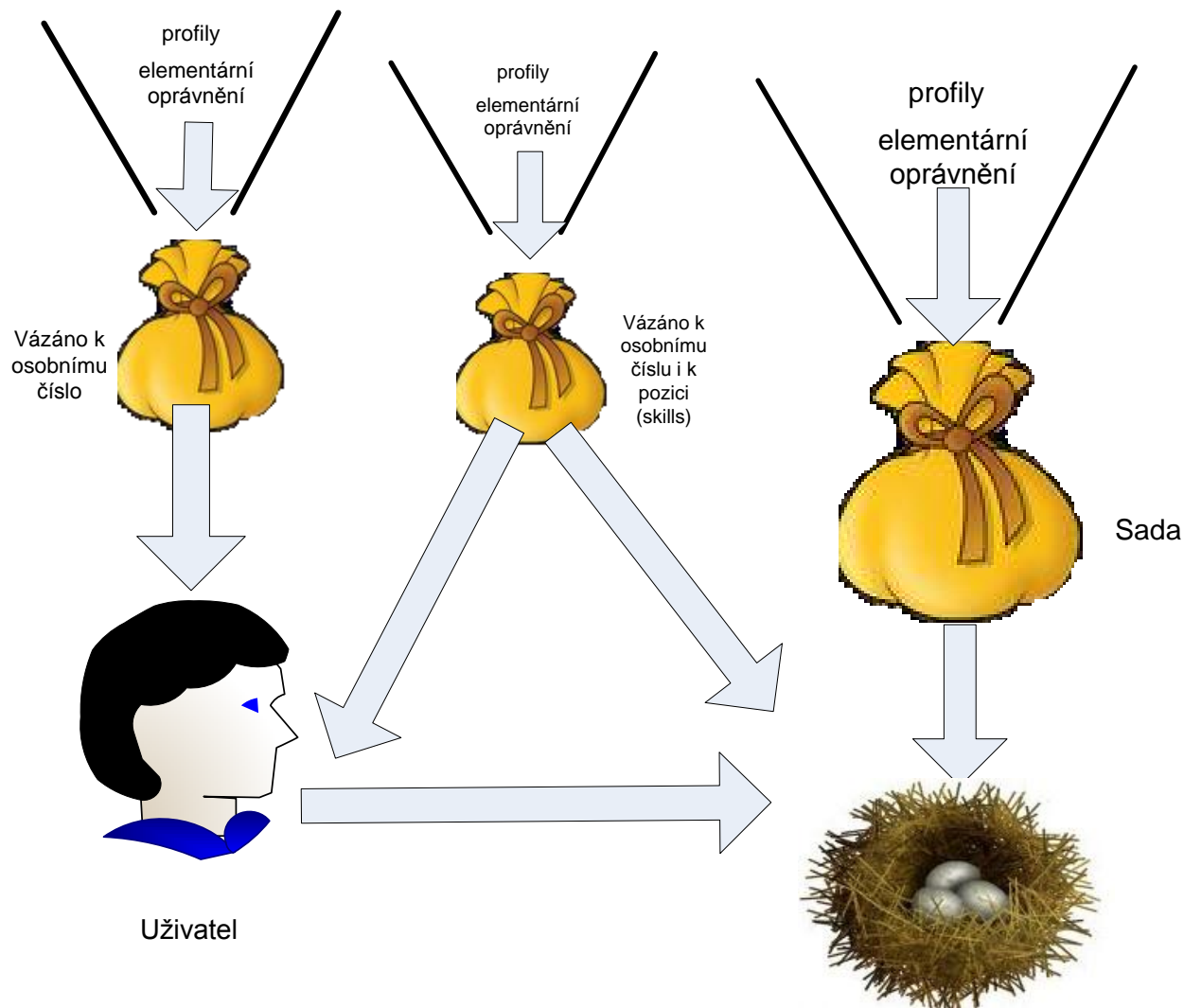
Oprávnění a rozdíly v jejich přidělování



Oprávnění a jejich přidělování



Oprávnění a jejich přidělování



Test

1.otázka Co je sada:

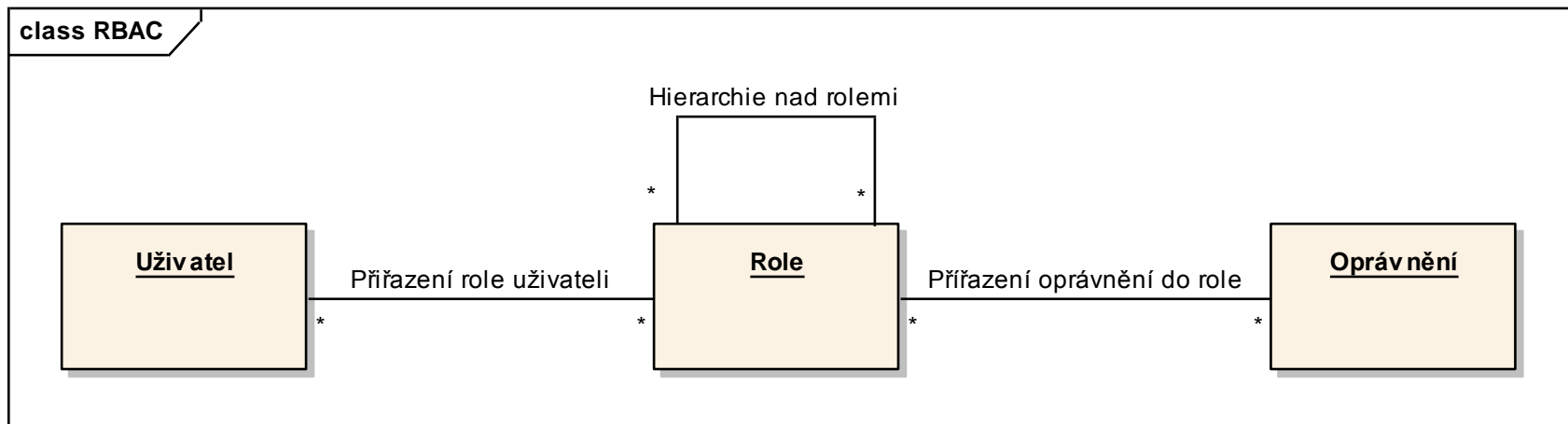
A	<input type="checkbox"/>	Množina oprávnění přidělená uživateli při nástupu
B	<input checked="" type="checkbox"/>	Množina oprávnění přidělená uživateli při přidělení na pozici
C	<input type="checkbox"/>	Množina oprávnění přidělená uživateli pro přístup ke konkrétní aplikaci
D	<input type="checkbox"/>	Množina oprávnění přidělená uživateli pokud má alespoň jednoho podřízeného



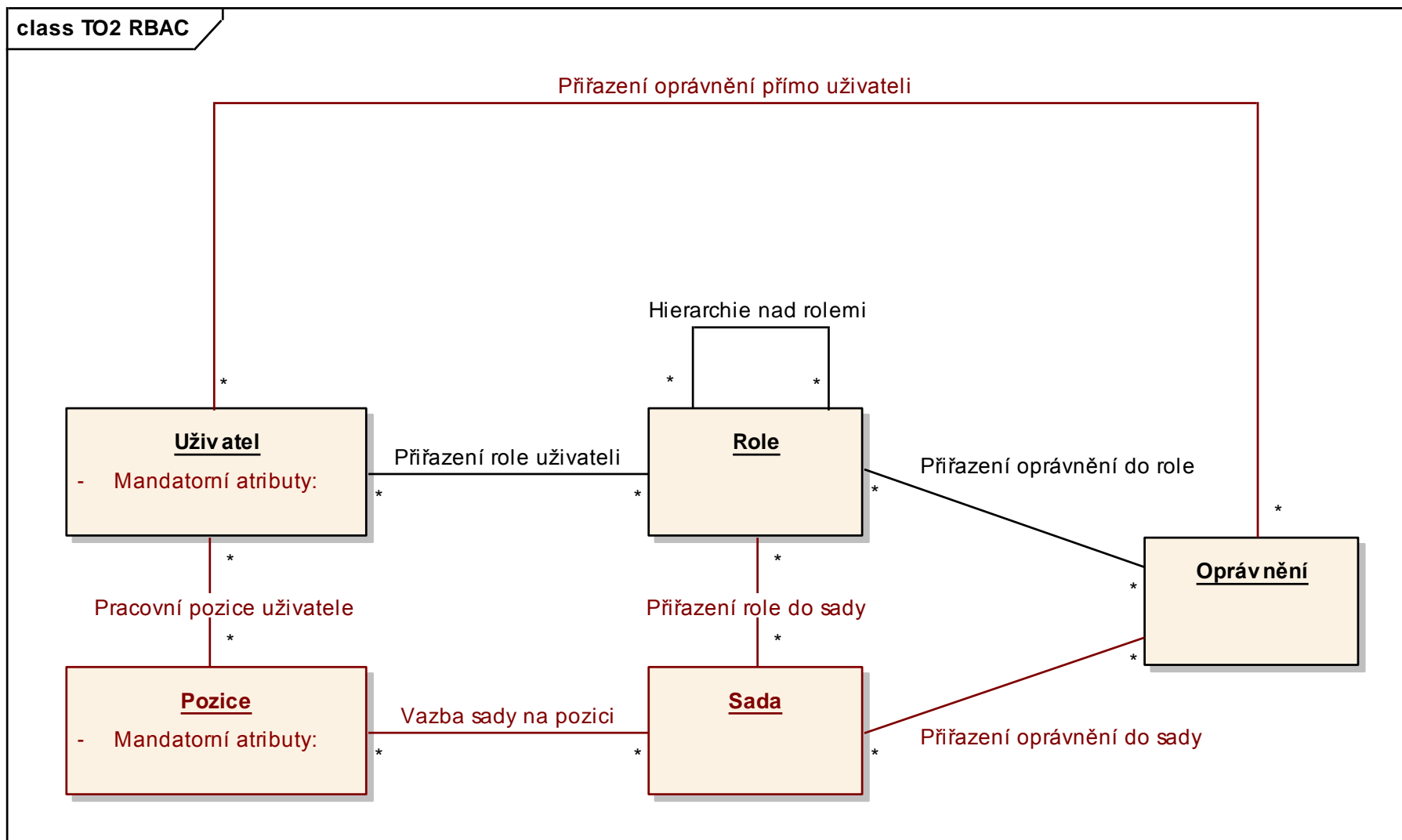
RBAC model a rozšířený RBAC model

Mandatorní atributy, skills ...

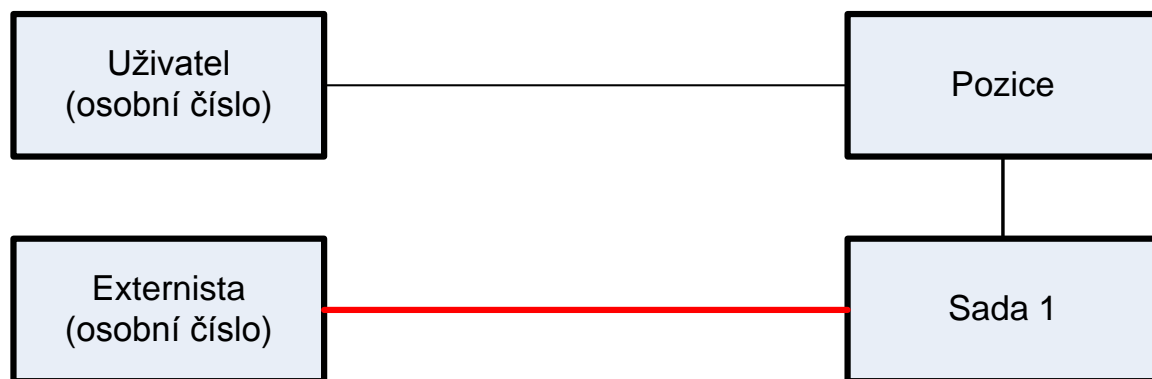
RBAC model



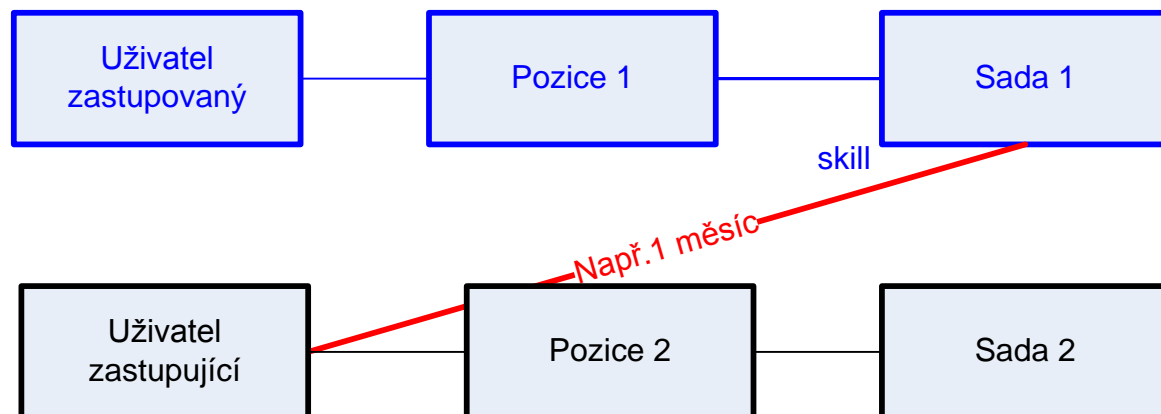
Rozšířený RBAC model



Příklady životních situací

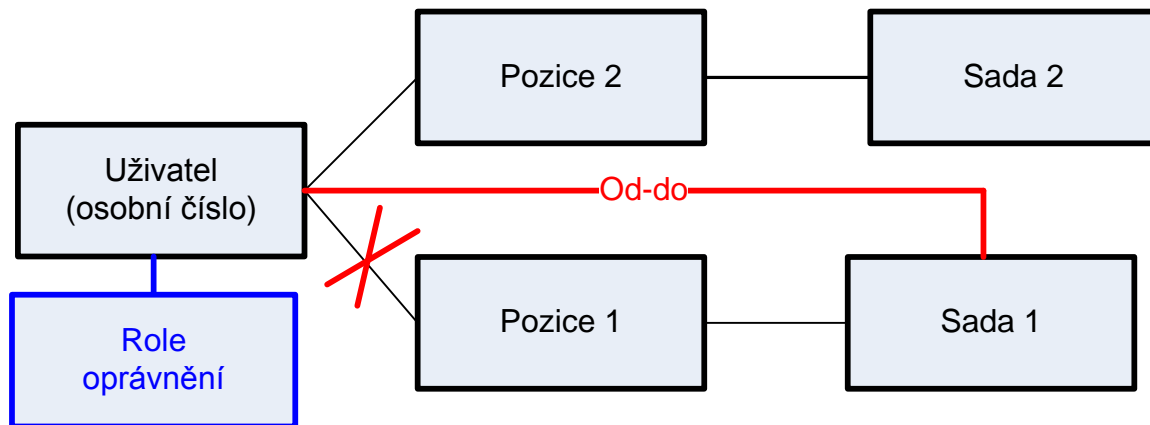


Sada pro externistu



Záskok

Příklady životních situací



Překryv

Test

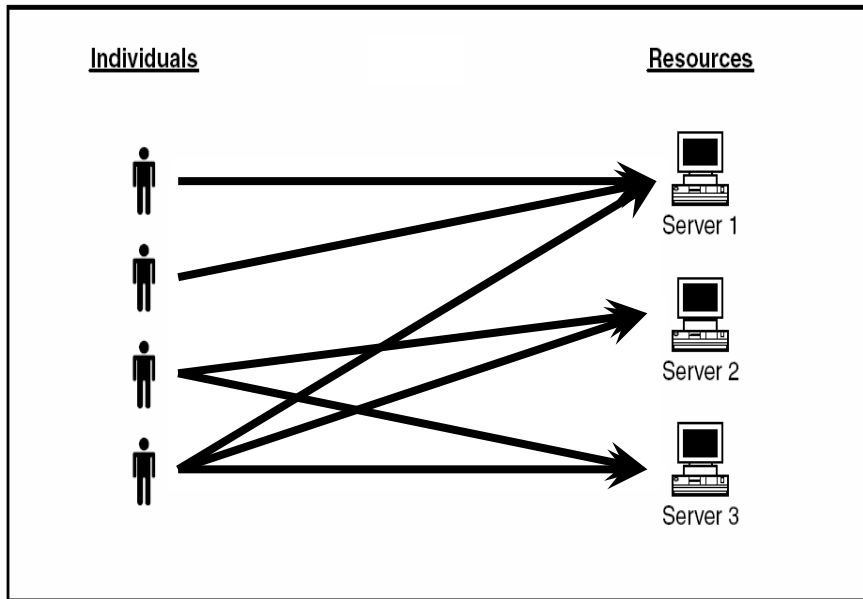
1.otázka Mezi příklady životních situací nepatří :

A	<input checked="" type="checkbox"/>	Přeskok
B	<input type="checkbox"/>	Záskok
C	<input type="checkbox"/>	Externista dostává sadu
D	<input type="checkbox"/>	Překryv



Optimalizace RBAC modelu

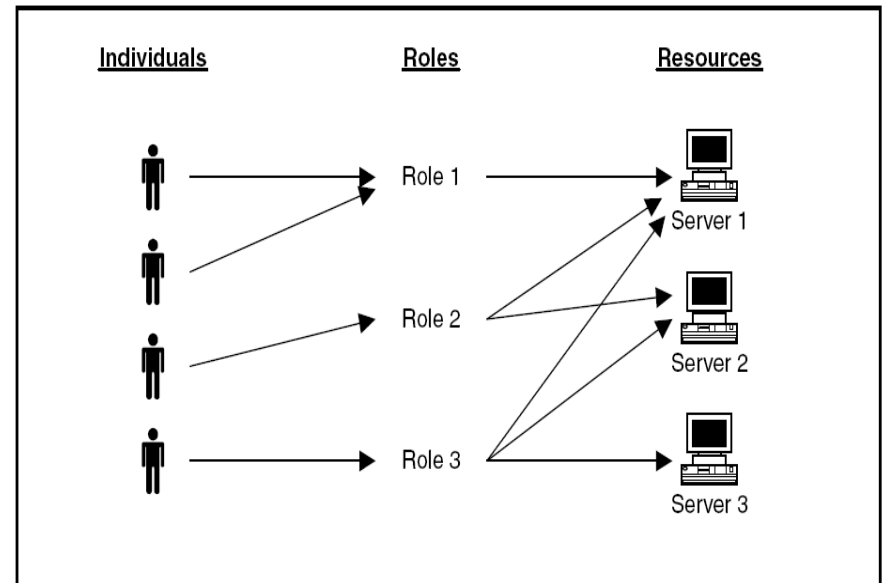
Bottom-up role mining



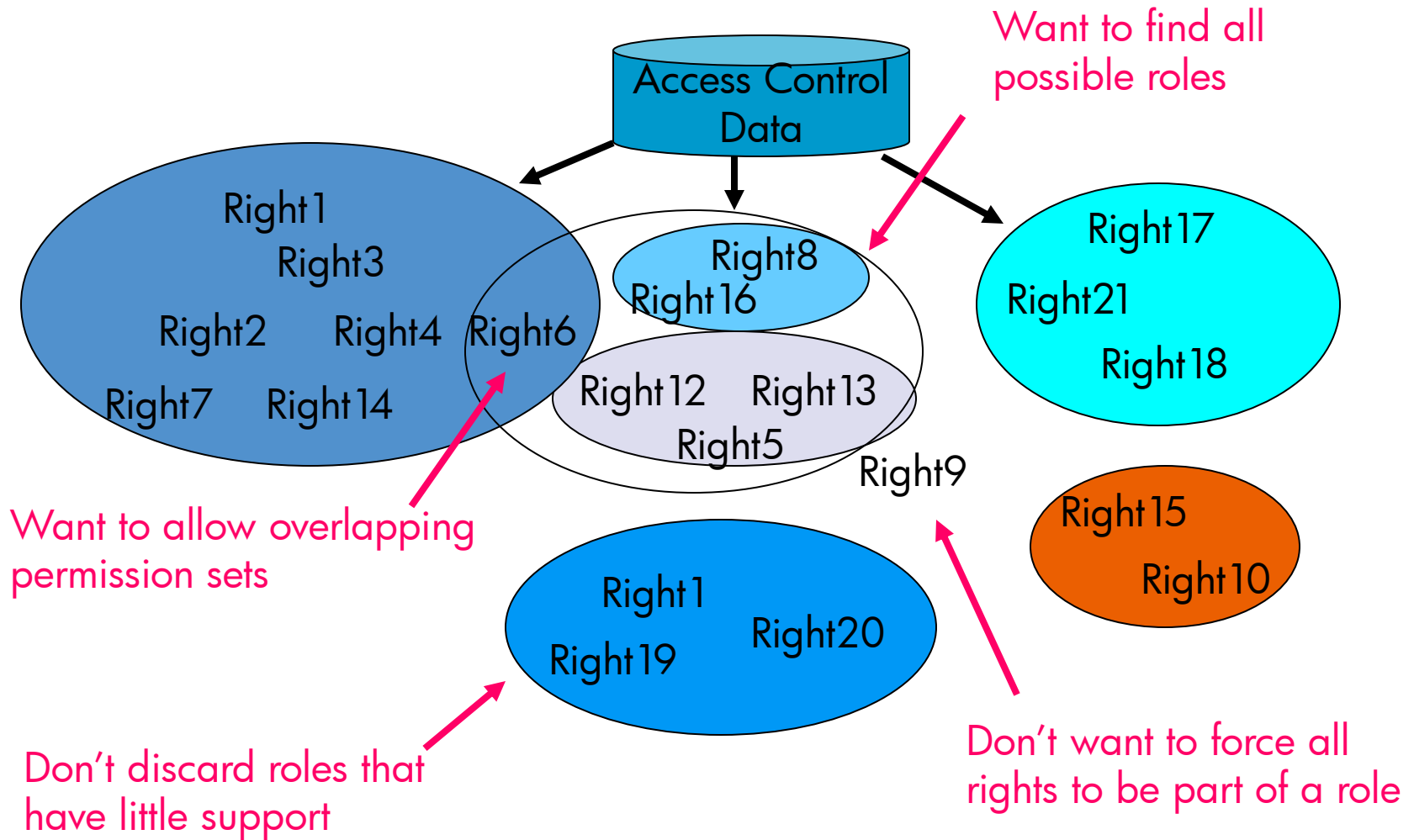
Traditional Scheme



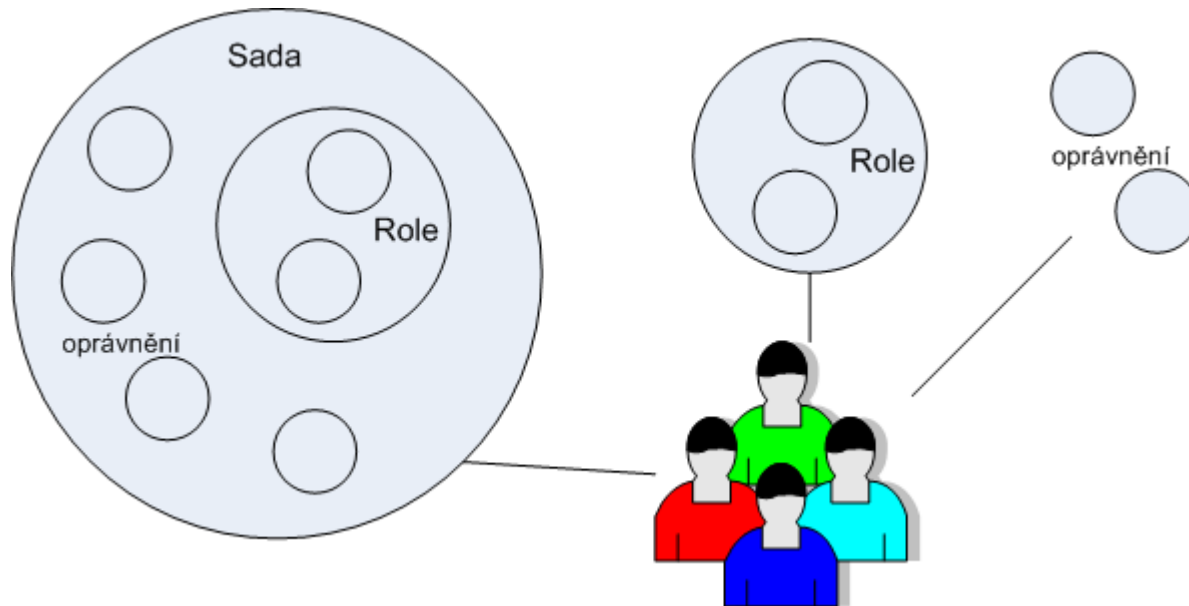
Role Based Access Control



Discovering Inherent Roles



Optimalizace RBAC modelu



Když:

- Přidám více oprávnění do sady
- Odeberu některá oprávnění ze sady
- Jak najdu optimum ?
- Jak definuji co nejpřesněji sadu odpovídající pozici?

Kdybyste chtěli fakt zajímavou diplomku – tak
tady je



Vnitřní role v IdM -
schvalovatelé, správci rolí,
správci dat...

Interní IAM role

Příklad – interní role.docx



Uživatelský self-service (žádosti o vlastní práva, přehled práv a účtů)

Uživatelský self-service (žádosti o vlastní práva, přehled práv a účtů)

- Realizuje se přes IAM Portál
- Uživatel má možnost např. zadávat dovolené, nemoc, nepřítomnosti ap., což váže na chování IAM
- Uživatel může prohlížet svá práva
- Uživatel může žádat o práva
- Uživatel může měnit některá svá data – nalř. Tel.linky, adresy ap.

Test

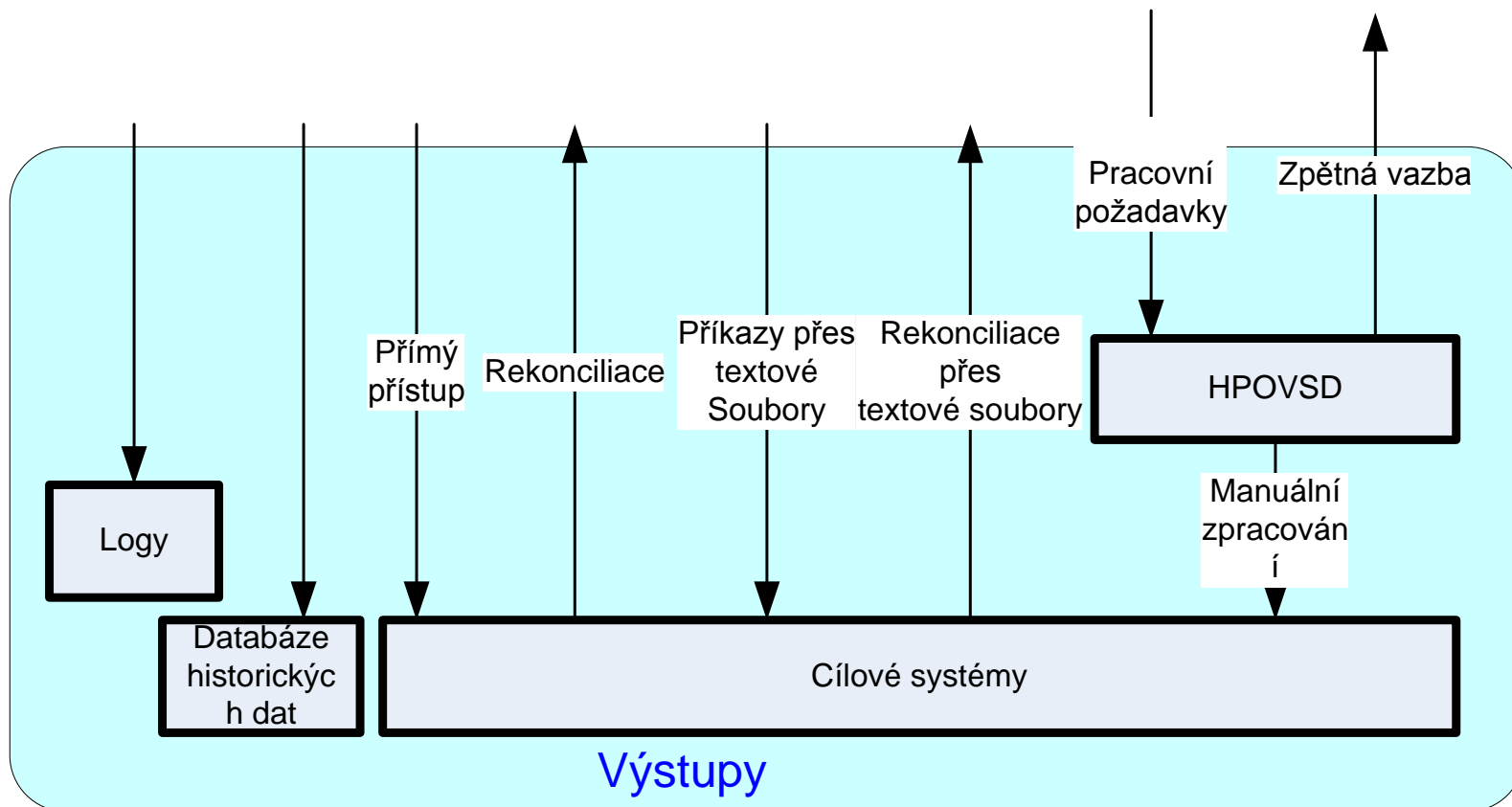
1.otázka jaké mohou být příklady self-service služeb v IAM:



Podřízené systémy

- Typy aplikací a možné způsoby jejich připojení
- Webservices
- Proprietární konektory
- Komunikace přes soubory
- Propojení přes Service Desk
- Zpětná vazba z podřízených systémů - reconciliace, synchronizace...
- Hesla, správa hesel, heslová politika, resety hesel, samospráva

Podřízené systémy



Podřízené systémy

- Typy aplikací a možné způsoby jejich připojení
- Webservices
- Proprietární konektory
- Komunikace přes soubory
- Propojení přes Service Desk
- Zpětná vazba z podřízených systémů - reconciliace, synchronizace...
- Hesla, správa hesel, heslová politika, resety hesel, samospráva

Test

1.otázka Jmenujte nějaké příklady, jak lze napojit podřízené systémy:



IdM jako informační základna
pro aplikace - propagace dat
do AD, do Exchange, do
intranetového portálu, API pro
aplikace

Vazba na AD

Active Directory jako **podřízený systém**:

- Myšlenka na první pohled opět jednoduchá a bezproblémová: podněty z HR se promítnou do IAM a ty se promítnou do AD
- Koordinace velmi náročná a dosažení stavu automatického provisioningu z AAA do AD si vyžádala mnoho úsilí
- Změnily se procesy, navyklé toky dat apod.
- Některé procesy ve vztahu k AD/Exchange/PKI mají velmi komplikované workflow
- Specifika ČSSZ:
 - Tvorba doménového účtu závisí na lokalitě a jméně, tj. při přestěhování nebo změně jména je třeba založit nový účet (vazba na uživatelův certifikát, jiný mailstore)
 - Jiná konfigurace mailstore pro vedoucí zaměstnance (změna mailstore při změně pozice)
 - WF pro administrátory čekající na manuální zásah



Problém rozevíraných nůžek mezi daty v IdM a v podřízených systémech

- Odebírání práv - o to nikdo nežádá
- Odchody - zombie v systémech
- Nucené rušení účtů při nedostatku licencí
- Nedodržování systému nadřízenosti a podřízenosti

Problém rozevíraných nůžek – jeden z největších problémů, co máte

- Odebírání práv - o to nikdo nežádá
- Odchody - zombie v systémech
- Nucené rušení účtů při nedostatku licencí
- Nedodržování systému nadřízenosti a podřízenosti



Souboj s administrátory - snižování jejich pravomocí

Administrátor by měl být rád



Ale není !!!

Test

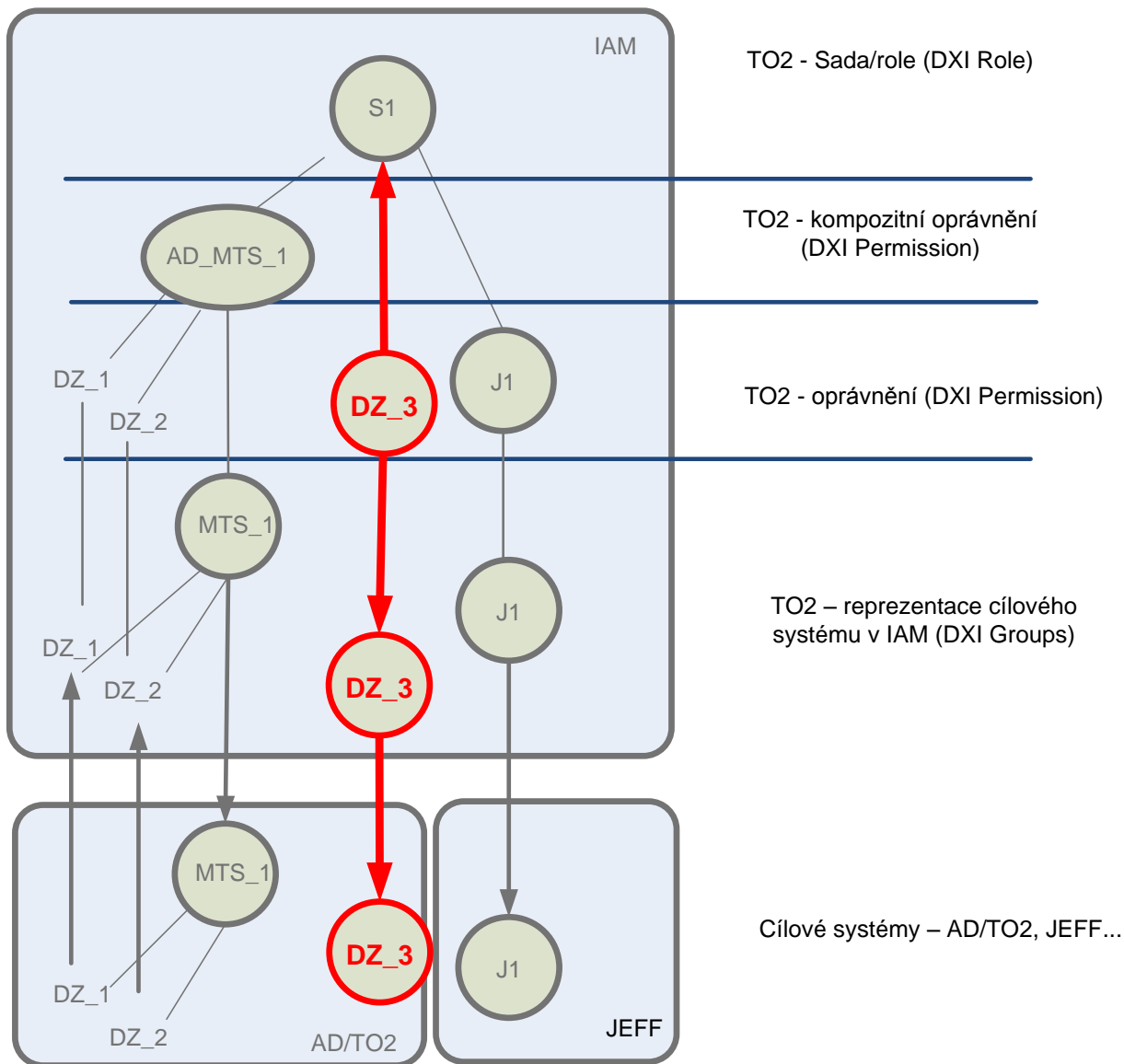
1.otázka Jak si nerozházet administrátory při implementaci IAM?





Disciplína - nastavování uživatelských účtů a jejich práv shora

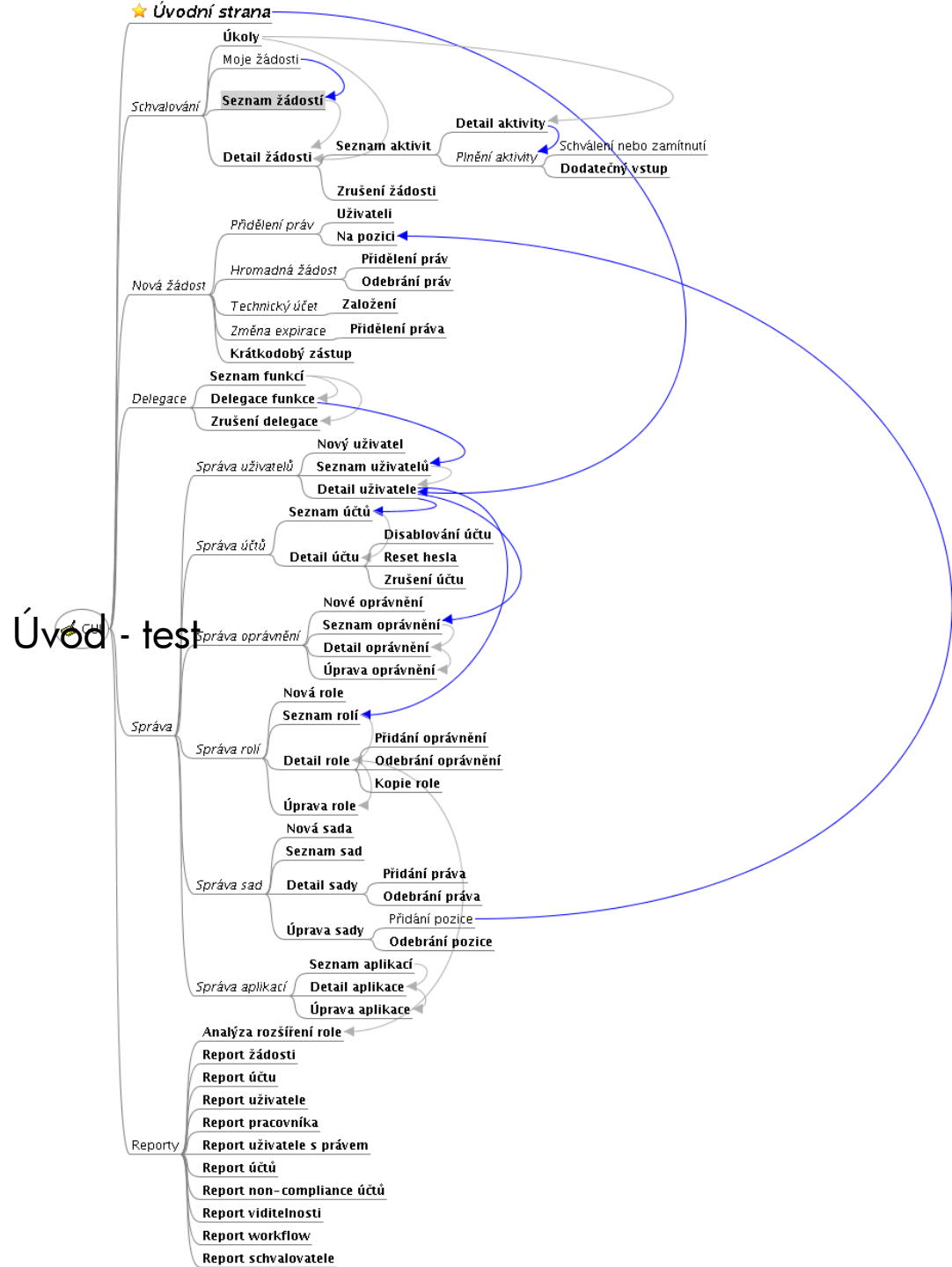
Diskuse – tohle už jsme brali



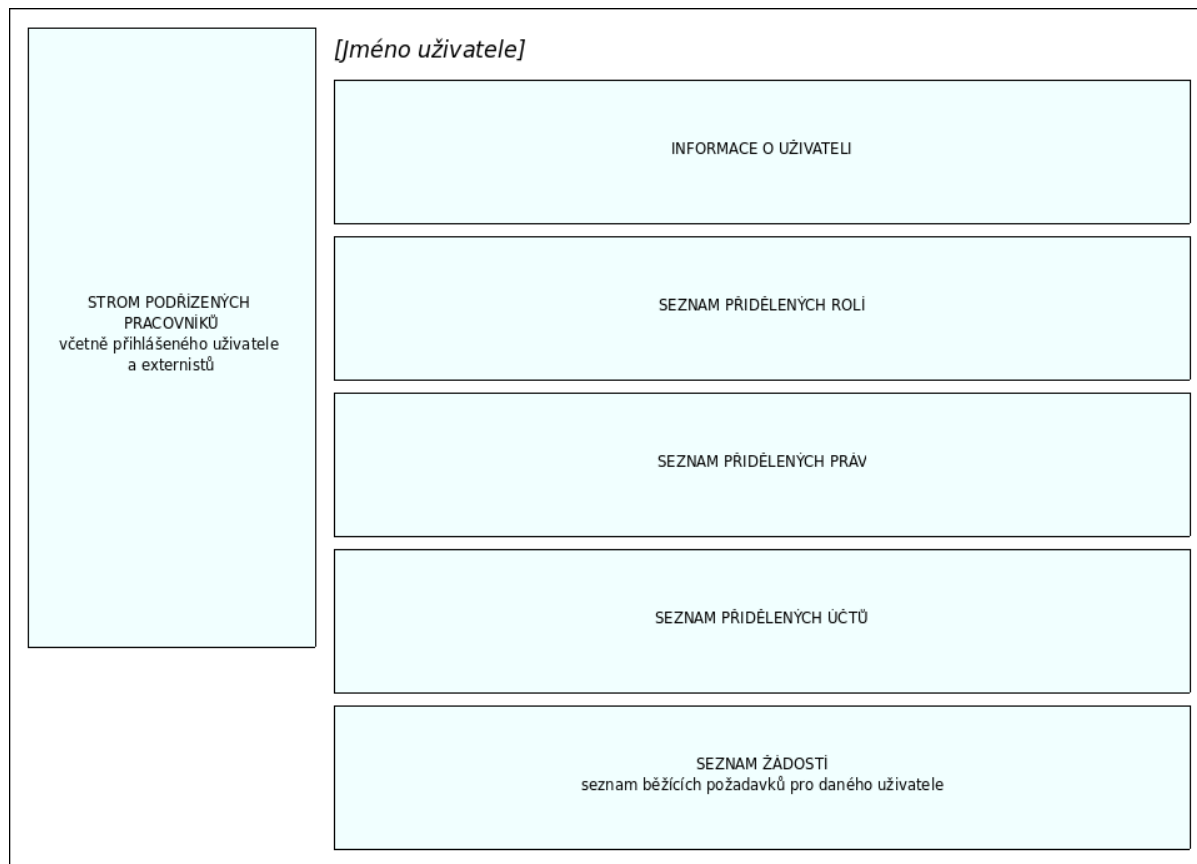


IAM Portál

Struktura GUI



Struktura GUI



Přehled práv Schvalování Nová žádost Delegace

Klazar Karel 5329

[Zažádat o změnu mandátových atributů](#)

Informace o uživateli

ID	cn=Klazar Karel 5329,o=1000,o=T02,cn=Users,cn=T02
Jméno	Karel
Příjmení	Klazar
Stav	ENABLED
Primární pozice	specialista vývoje systému 113737
Útvar	Systemy pro správu dokumentu 26834
Nadřízený	Ořlovský Petr 1145

Seznam sad

Název	Viditelnost	Stav	Platnost od	Platnost do
-------	-------------	------	-------------	-------------

Nebyly nalezeny žádné záznamy.

Seznam rolí

Některá Vaše práva jsou v realizaci, pro bližší informace zkontrolujte [seznam svých účtů](#)

Název	Viditelnost	Stav	Platnost od	Platnost do
-------	-------------	------	-------------	-------------

AD

schváleno

Seznam oprávnění

Některá Vaše práva jsou v realizaci, pro bližší informace zkontrolujte [seznam svých účtů](#)

Název	Viditelnost	Stav	Platnost od	Platnost do
RAS-RAS	✓	schváleno		
PB-CCO2ADMINISTRATOR	✓	schváleno		
PB-ECMS-ADMINISTRATORS	✓	schváleno		
SAP-R3(ET)-S-GLOBAL	✓	schváleno		
PA-EXPORT	✓	schváleno		
SERVICEDESK-SPECIALIST	✓	schváleno		
PKI-SILNA-AUTENTIZACE	✓	schváleno		

Seznam účtů

Název účtu	Stav účtu	Realizace	Cílový systém	Popis účtu
ka005329@user.ct.cz	zakázán	✓	Exchange	specialista vývoje systémů
Klazar_k@ad.eurotel.cz	povoleno	✓	MultiDomain	221003 IT CRM
ka005329	povoleno	⚠	SERVICEDESK	5329, Karel Klazar, Document Management Systems 26834, AD
ka005329	povoleno	⚠	RAS	5329, Karel Klazar, Document Management Systems 26834, AD
ka005329	povoleno	⚠	PKI-SILNA-AUTENTIZACE	5329, Karel Klazar, Document Management Systems 26834, AD
ka005329	povoleno	⚠	LN	5329, Karel Klazar, Document Management Systems 26834, AD
ka005329	povoleno	⚠	SAP-R3(ET)	5329, Karel Klazar, Document Management Systems 26834, AD
	zakázán	✓	PB	
Klazar_k@to2.to2cz.cz	povoleno	✓	PB	221003 IT CRM

Seznam běžících žádostí

Název žádosti	Stav	Iniciátor žádosti	Čas vytvoření
---------------	------	-------------------	---------------


Nebyly nalezeny žádné záznamy.

IM GUI

- Grafická nadstavba systému IM
- Umožňuje nadřízeným, případně vlastníkům dat, komfortní přidělování a schvalování rolí pro podřízené
- Implementováno jako webová aplikace
- Podporuje Single Sign On
- Základní funkčnosti:
 - přidělení funkčních, lokalizačních a VIP rolí pro podřízené
 - hromadné přidělení funkčních rolí pro více podřízených
 - schvalování požadavku na přidělení rolí vlastníkem dat
 - potvrzení naplánované akce z workflow
 - delegování zástupce vedoucího pracovníka

IM GUI – změna role podřízeného

Česká správa sociálního zabezpečení

 **ITIM GUI**
Výběr podřízeného

[Hlavní stránka](#) [Změnit role pro podřízeného](#) [Hromadná změna rolí](#) [Zobrazit požadavky z workflow](#) [Změnit zástupce](#) [Zobrazit role](#) [Report pro schvalovatele](#) [Dokumenty](#)

Vyberte podřízeného a upravte mu role:

☒ Brzobohatá Kateřina ➤

☐ Malý Petr ➤

☐ Večeřová Lenka ➤

IM GUI – změna role podřízeného

Česká správa sociálního zabezpečení

ITIM GUI
Nastavení rolí - 1. krok

Petr Němec
Pracoviště: reditel

Hlavní stránka Změnit role pro podřízeného Hromadná změna rolí Zobrazit požadavky z workflow Změnit zástupce Zobrazit role Dokumenty

Upravujete role osobě: **Petr Němec**

Vyberte role, které chcete podřízenému upravit

- ČSSZ
 - ACP - Aplikace čistého průběhu
 - ATR - Automatizovaná tvorba rozhodnutí
 - AVD - Automatický výpočet důchodů
 - BAM - Správa aplikačních požadavků mezi UI44, UI08, KL, VZT
 - BZD - Prohlížení XML datových vět v dbZDV
 - DAK - Datový katalog
 - DKA - Aktivní klient
 - Aktivní
 - Manažer
 - Pasivní
 - Univerzální aktivní
 - Univerzální pasivní
 - DKE - Podatelna
 - Uživatel podatelny
 - DKU - Univerzální klient
 - Univerzální
 - Uživatel univerzálního klienta
 - DMA - Document Management Archiv
 - EDS - Elektronický dávkový spis
 - EXK - Exekuce a konkurzy
 - HRP - Hromadné podněty
 - INN - APV pro oblast nemocenského pojištění
 - INTERNET
 - KL - Kontrolní linka
 - NEM - APV pro oblast nemocenského pojištění
 - NP2 - NPRJIMY2
 - POJ - Centrální výběr pojistného
 - ROD - Rozhodování o nároku
 - SI2 - Rozhraní SI2 do KE
 - SLH - Sledování lhůt
 - TCL - Tenký klient Kmenových evidencí (KE2)
 - UI44 - Správa Kmenových evidencí
 - UI8 - Zpracování odmítnutých dokladů na OSSZ
 - UIP - UIP3 v rámci NPD
 - VYP - Výplaty

UC0102	xxnempet-e	1.0.0	SBS
--------	------------	-------	-----

IM GUI – zobrazení požadavků z workflow

Česká správa sociálního zabezpečení



ITIM GUI

Výběr požadavku

[Hlavní stránka](#) [Změnit role pro podřízeného](#) [Hromadná změna rolí](#) [Zobrazit požadavky z workflow](#) [Změnit zástupce](#) [Zobraz role](#) [Nápověda](#)

Vyberte požadavek na schválení role, který chcete potvrdit

Schválit	Typ	Žádané pro	Žádající	Datum žádosti	Požadované role	
<input type="checkbox"/>	Schválení role	Vratislav Lokvenc →	Milan Baroš	16.1.2007	Aplikace UI44-Administrátor Aplikace UI44-Aprobant	Zobraz
<input type="checkbox"/>	Schválení role	Vratislav Lokvenc →	Milan Baroš	16.1.2007	NEM-Aprobant NEM-Kontrolor KLR NEM-Nadřízený orgán NEM- _Brno - město (1500)	Zobraz
<input type="checkbox"/>	Schválení role	Vratislav Lokvenc →	Milan Baroš	16.1.2007	VZT-Referent administrace stavu registru plátců VZT-Referent registru plátců VZT-Referent zahraničních zaměstnanců	Zobraz
<input type="checkbox"/>	Schválení role	Vratislav Lokvenc →	Milan Baroš	16.1.2007	INN-Aprobant INNP INN-Došetřující referent INNP INN- _Beroun (221) INN- _Blansko (771)	Zobraz


Schválit vybrané

Nemáte žádné požadavky na potvrzení pracovního příkazu.

[Zpět](#)

IM GUI – seznam rolí

Česká správa sociálního zabezpečení

 **ITIM GUI**
Zobrazení přidělených rolí

[Hlavní stránka](#) [Změnit role pro podřízeného](#) [Hromadná změna rolí](#) [Zobrazit požadavky z workflow](#) [Změnit zástupce](#) [Zobraz role](#) [Nápověda](#)

Osoba: Vratislav Lokvenc

Aplikace: VZT

- Referent administrace stavu registru plátců
- Referent registru plátců
- Referent zahraničních zaměstnanců
- Referent DOPOJ
- Referent OSVČ

Aplikace: Elektronický dávkový spis

- Aprobant SDD

Aplikace: NEM

- Aprobant
- Kontrolor KLR
- Nadřízený orgán
- Referent DNP
- Referent EPN
- Referent KLR
- Referent KLR - výsledky
- Referent LPS
- LOKALIZAČNÍ ROLE: Benešov (220)
- LOKALIZAČNÍ ROLE: Beroun (221)

Aplikace: BZD

Portál– report pro schvalovatele

Report pro schvalovatele

Zavřít

Celkem 11 položek.


<u>OS. ČÍSLO</u>	<u>UŽIVATEL</u>	<u>LOKALITA</u>	LOKALIZAČNÍ ROLE	EXK ADMINISTRÁTOR (EXK_ADMIN)	EXK DOHLED (EXK_DOHLED)	EXK DRUHÝ PRACOVNÍK (EXK_DRUHÝ)	EXK MANAŽER (EXK_MNG)	EXK MANIPULANT (EXK_MNP)	EXK PRVNÍ PRACOVNÍK (EXK_PRVNI)	EXK VEDOUCÍ (EXK_VED)
267238	Eva VÁCHOVÁ	CZ0105		x	x	x	x	x	x	x
258690	Ing. Michaela HENDRYCHOVÁ	CZ0105			x					x
294706	Ing. Michal RAJDL	CZ0105				x	x	x	x	
272375	JUDr. Eliška VOLFOVÁ	CZ0105			x					x
265078	JUDr. Jitka STEHLÍKOVÁ	CZ0105		x						x
254665	JUDr. Marie BAĐUROVÁ	CZ0105		x	x	x	x	x	x	x
258001	Marie HORKÁ	CZ0105				x				
275738	Mgr. Dagmar BASTLOVÁ	CZ0105		x	x	x	x	x	x	
257086	Milada DOHNALOVÁ	CZ0105							x	x
267173	Monika BOCKOVÁ	CZ0105				x	x	x	x	
257510	Monika CIHLÁŘOVÁ	CZ0105			x					x

Celkem 11 položek.

Možnosti exportu: [CSV](#)

Portál – požadavková fronta

Česká správa sociálního zabezpečení


ITIM GUI
Report fronty požadavků

[Hlavní stránka](#)
[Změnit role pro podřízeného](#)
[Hromadná změna rolí](#)
[Zobrazit požadavky z workflow](#)
[Změnit zástupce](#)
[Zobrazit role](#)
[Report pro schvalovatele](#)
[Fronta požadavků](#)
[Dokumenty](#)

Report fronty požadavků

Datum od: 10.03.2007
Datum do: 17.03.2008
Zobrazit požadavky v stavu: Všechno

Seznam požadavků:

Datum žádosti	Datum vyřízení	Žádáno pro	Role	Stav	Akce
23.01.2008	23.01.2008	NEM - _Benešov (220)	NEM - _Benešov (220)	Schváleno	Detail
01.02.2008	01.02.2008	NEM - _Blansko (771) NEM - _Břeclav (774)	NEM - _Blansko (771) NEM - _Břeclav (774)	Schváleno	Detail
07.02.2008	17.02.2008	NEM - Vedoucí pracovník	NEM - Vedoucí pracovník	Schváleno	Detail
09.02.2008	21.02.2008	NEM - _Brno-venkov (773) NEM - _Bruntál (885) NEM - _Česká Lípa (550)	NEM - _Brno-venkov (773) NEM - _Bruntál (885) NEM - _Česká Lípa (550)	Schváleno	Detail
17.02.2008	29.02.2008	DKA - Referent s právem prohlížení dat	DKA - Referent s právem prohlížení dat	Schváleno	Detail
17.02.2008	29.02.2008	NEM - _Benešov (220)	NEM - _Benešov (220)	Schváleno	Detail
19.02.2008	02.03.2008	ACP - Aprobant ACP ACP - Referent ACP	ACP - Aprobant ACP ACP - Referent ACP	Schváleno	Detail
19.02.2008	19.02.2008	NEM - _Benešov (220)	NEM - _Benešov (220)	Zamítnuto	Detail
21.02.2008	04.03.2008	NEM - _Benešov (220)	NEM - _Benešov (220)	Schváleno	Detail
21.02.2008	26.02.2008	NEM - _Benešov (220)	NEM - _Benešov (220)	Zamítnuto	Detail
04.03.2008	16.03.2008	NEM - _Břeclav (774) NEM - _Brno - město (1500) NEM - _Brno-město (772) NEM - _Brno-venkov (773) NEM - _Bruntál (885)	NEM - _Břeclav (774) NEM - _Brno - město (1500) NEM - _Brno-město (772) NEM - _Brno-venkov (773) NEM - _Bruntál (885)	Schváleno	Detail
12.03.2008	Nevyřízeno	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	Běžící	Detail
12.03.2008	Nevyřízeno	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	Běžící	Detail
12.03.2008	Nevyřízeno	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	Běžící	Detail
12.03.2008	Nevyřízeno	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	KL - Administrátor KL - Aprobant KL - Dispečer KL - Referent	Běžící	Detail

Zpět

Portál – průchod organizační strukturou

Česká správa sociálního zabezpečení

AAA portál – Přehled uživatelských oprávnění

JUDr. Božena Micháková

Cesta:

- JUDr. Božena Micháková
- JUDr. Božena Micháková
- Ing. Vladimír Fanta
- Ing. Radka Poláková
- Mgr. Petra Langová

Filtr:

Apkace: - vše -

Lokalita: - vše -

Informace o uživateli:

Titul: Mgr.
Jméno: Petra
Příjmení: Langová
Titul za jménem:
Uživatelské jméno: xxlangpet
Telefon: 257062395
Kód pracoviště: 10510200
Adresa: Křížová 25|Praha 5|225 08
E-mail: petra.langova@cssz.cz
Role:

Podřízení:

- Ing. Zuzana Hájková
- Ing. Karel Havlíček C.Sc.
- Václav Kohl
- Pavel Pačes
- Ing. František Průckner
- Pavel Vosáhlo
- Radim Vlček



Federace identit

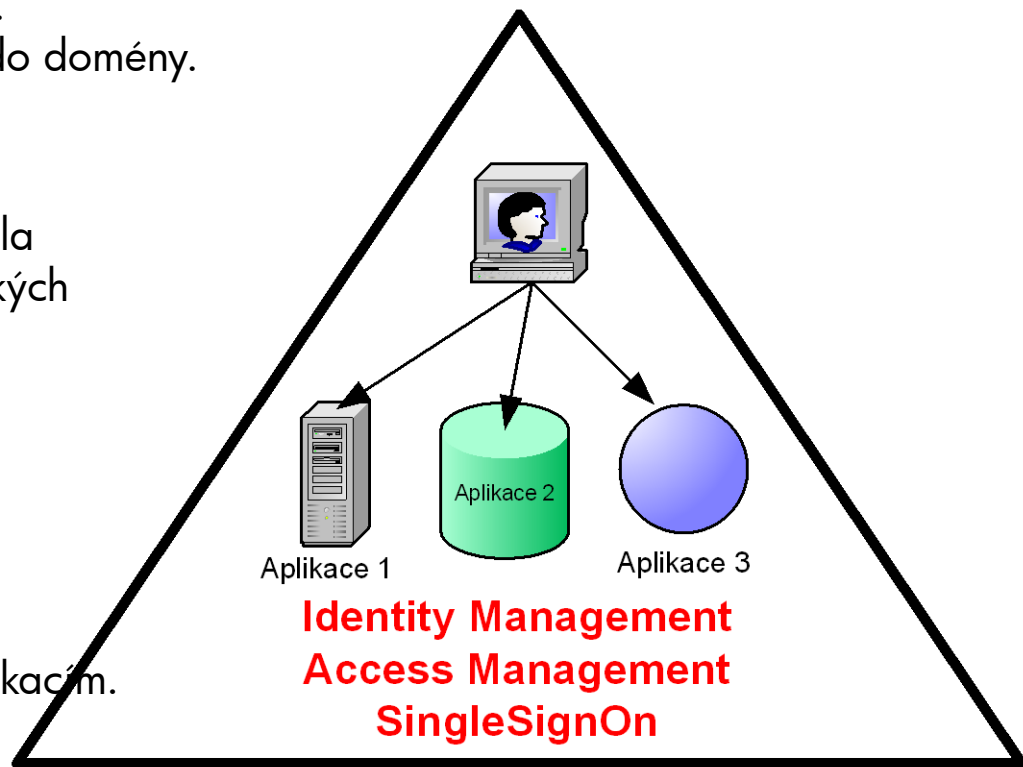
Federated Identity

Co je Identity Management

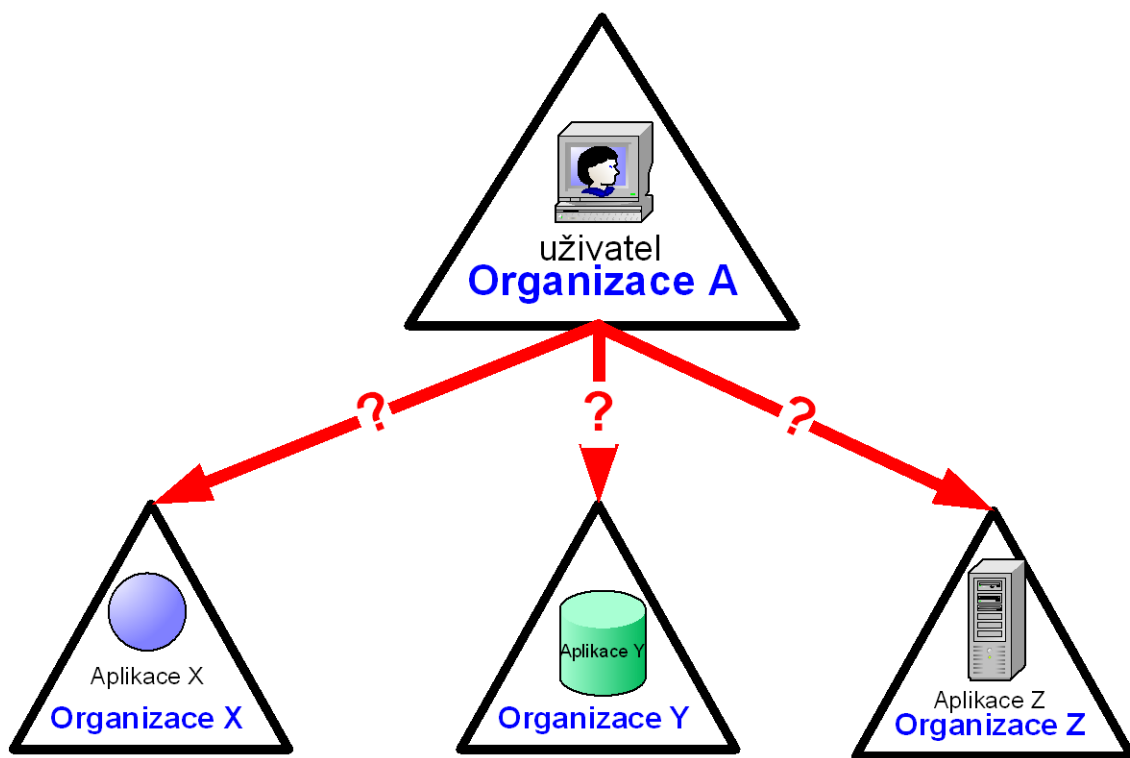
Když přistupuje uživatel k aplikacím vlastní domény, nechce se hlásit ke každé aplikaci zvlášť. Již se jednou autentizoval při přihlášení do domény. Toto řeší tzv. SingleSignOn

Každá organizace se také snaží, aby měla informace o uživateli a jejich uživatelských oprávněních pod kontrolou a na jednom místě, pokud je to možné. Toto řeší tzv. Identity Management

Je také žádoucí mít plně pod kontrolou přístup k datům a systém přidělování přístupových oprávnění k jednotlivým aplikacím. Toto řeší tzv. Access Management



Přístup k aplikacím a datům jiných organizací



- Co když však má uživatel komunikovat s aplikací, která není v jeho doméně, ale patří jiné organizaci?

–

- Co teď'?

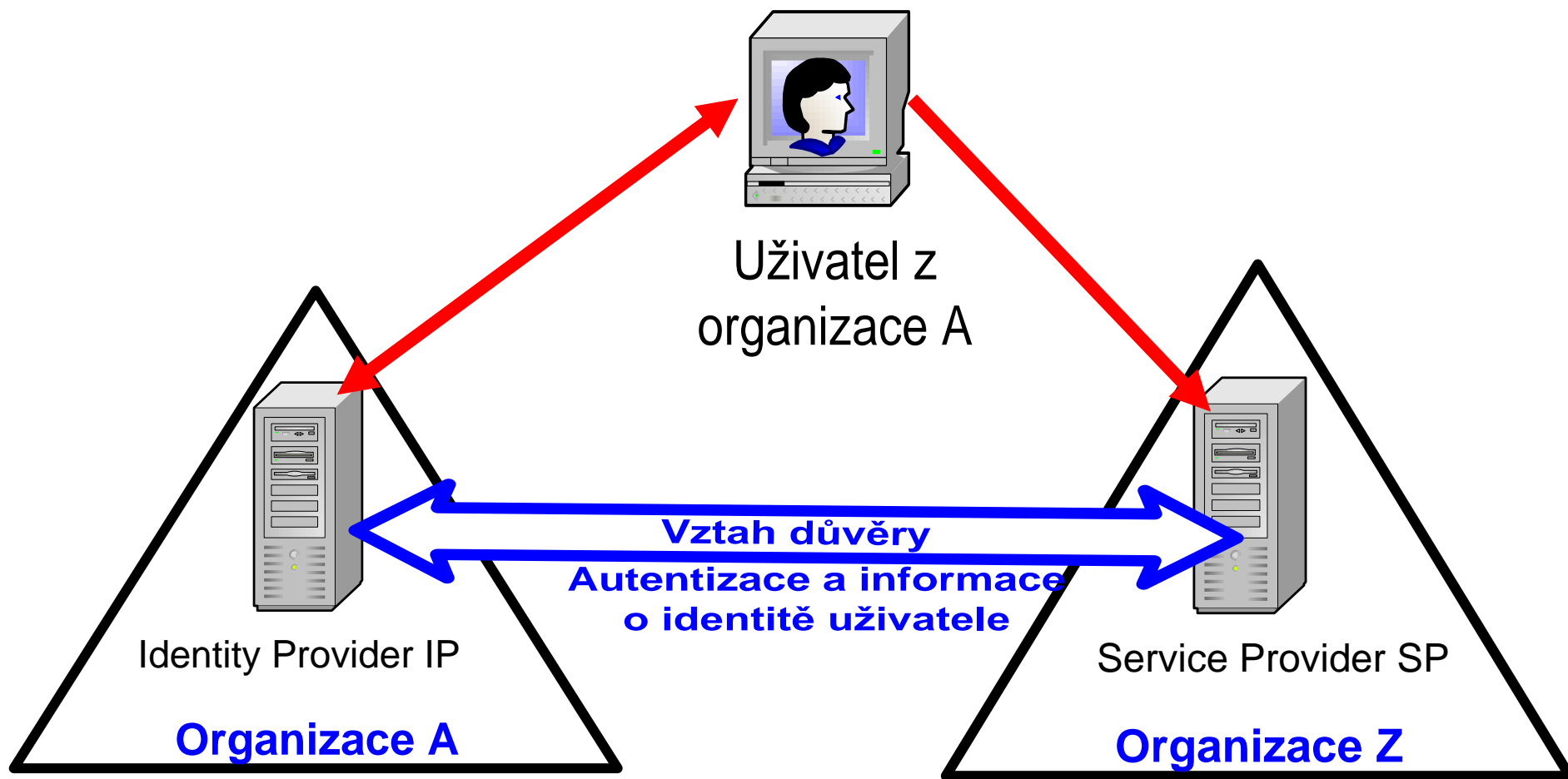
Odpovědí je

Federated Identity

Princip Federated Identity

- Velmi trefným přirovnáním je **podoba s pasy**.
- Naše vlastní země (zde naše doména) nám vydá pas opravňující nás navštívit cizí země (domény jiných organizací).
- Je to tak proto, že se země dohodly, že budou důvěřovat dokladu vydaného jinou zemí. V pasu má jeho nositel některé údaje, např. datum platnosti pasu, které jsou důležité pro to, jestli mu bude povolen vstup nebo nikoliv.
- Stejně tak funguje i FID.
- Aby mohla FID fungovat, musí si organizace navzájem důvěřovat.
- To ovšem neznamená, že nutně musí důvěřovat i jednotlivým uživatelům, princip je opět stejný s pasem, který může nositel padělat.
- **Na důvěře se musí dohodnout organizace vstupující do FID.**
- **Tato důvěra však není slepá, je zabezpečena velmi důsledně prostředky FID.**

Princip Federated Identity

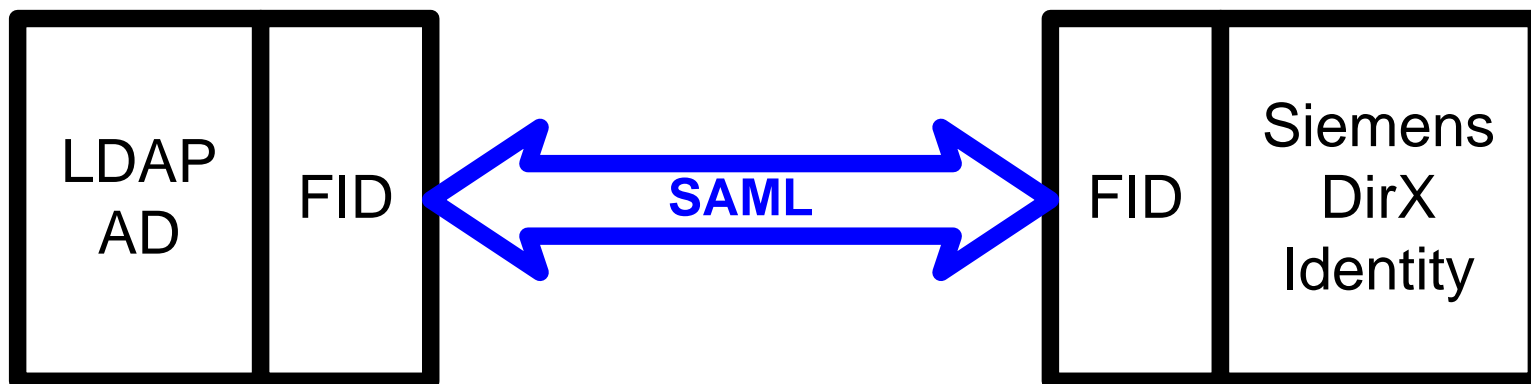


Jaké informace se může Service Provider o uživateli dozvědět?

- **Takových informací je celá řada**
- **Informace o identitě uživatele**
- **Atributy** – doplňující informace o uživateli, jméno, příjmení, pozice v organizaci apod.
- **Autorizační oprávnění**
- **Servisní informace** – sem patří např. jednoznačné označování zpráv (tzv. assertions), identifikace vydavatele zprávy (v našem případě IP organizace A), časová razítka, elektronické podpisy apod. Jde tedy o zabezpečení a důvěryhodnost FID komunikace

Mapování identit

- Je zde ještě jeden nezodpovězený problém.
- FID musí totiž pracovat ve velmi heterogenním prostředí. Každá organizace má svůj systém práce s identitami - řekněme, že jedna používá např. Active Directory, druhá Siemens DirX Identity.
- Jde tedy o různé formáty dat, různé logiky tvorby účtů apod.
- Proto musí být před každým nasazením FID provedeno mapování identit.

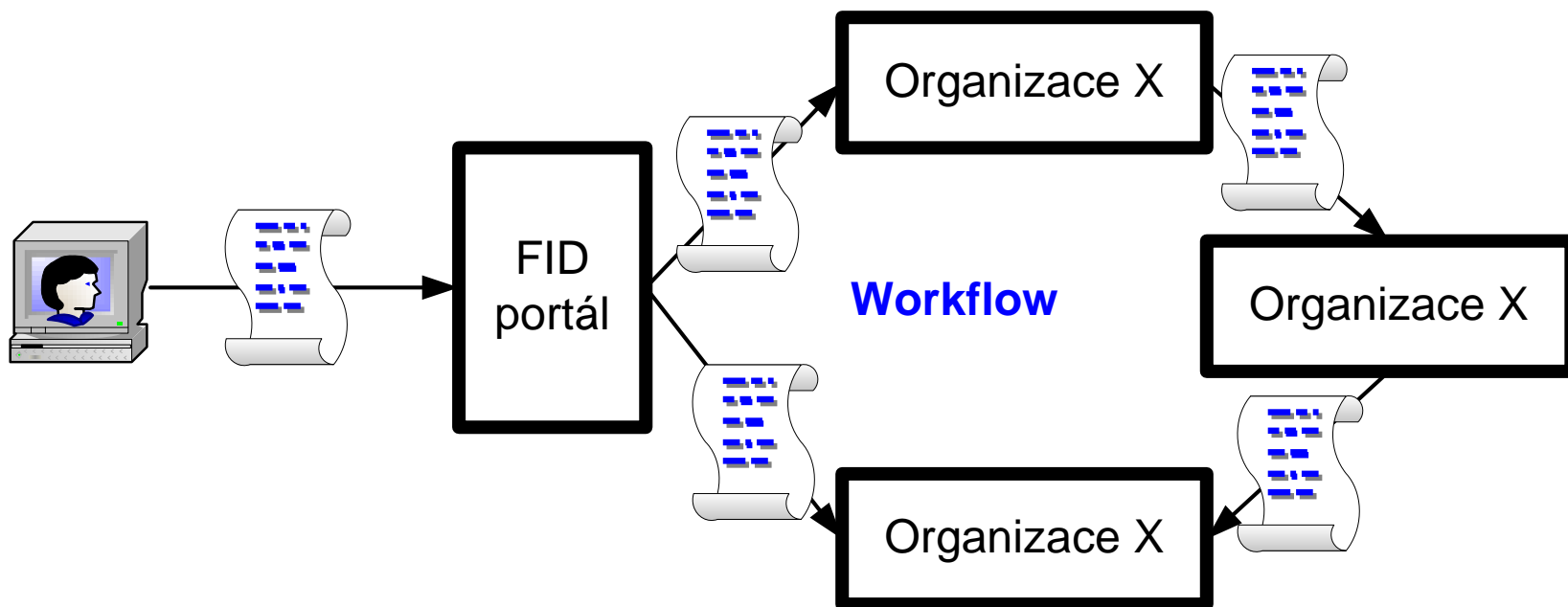


Ach ty standardy.....

- Kvůli tomu, že FID musí pracovat v heterogenním prostředí, je velmi důležité, aby se držel platných standardů. V oblasti FID existuje komise OASIS Security Services Technical Committee (SSTC), která stojí za tvorbou standardů používaných FID.
- **K nejdůležitějším patří:**
 - Security Assertion Markup Language (SAML), díky kterému mohou komunikovat v rámci FID různé subjekty heterogenního prostředí
 - WS-* specifikace (mezi které patří např. WS-Trust, WS-Security, WS-Federation) je zabezpečení v rámci SOAP.

Co by mohla implementace FID přinést státní správě?

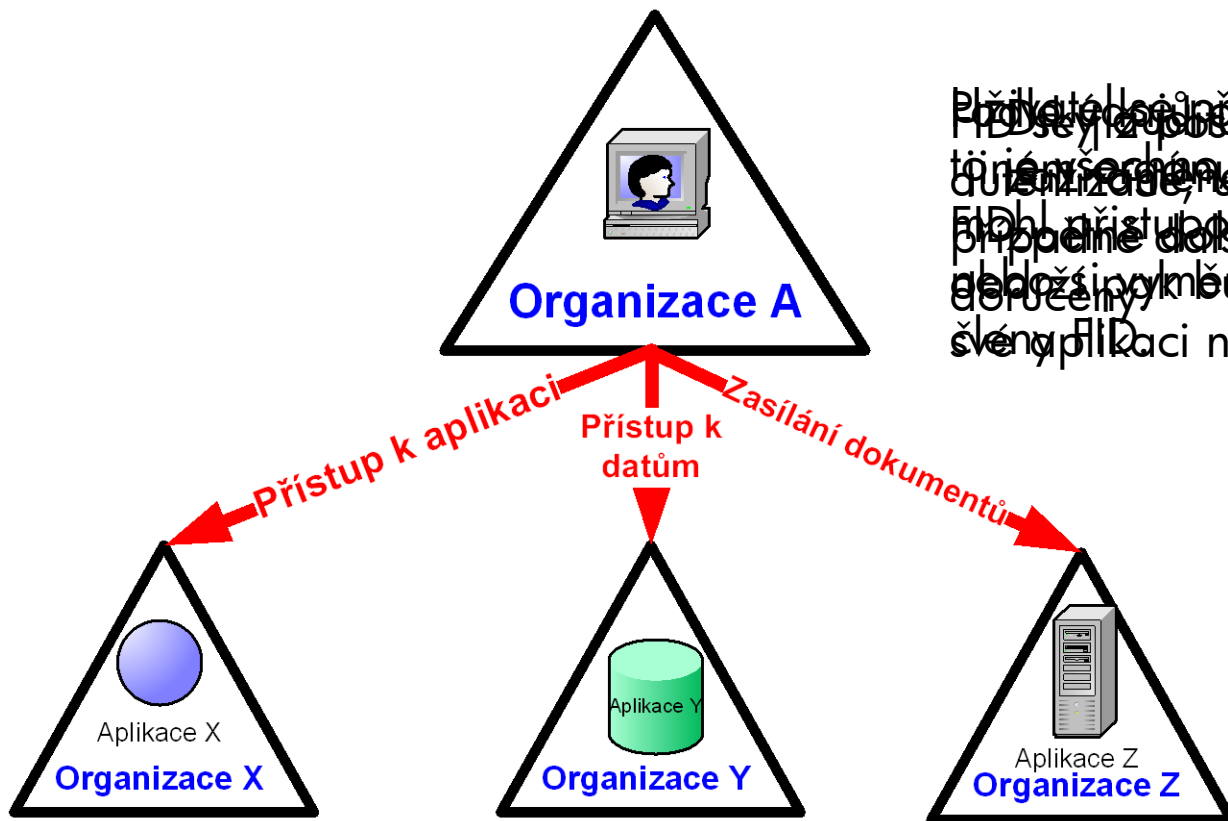
Komunikace veřejnosti se státní správou



Oběh dokumentů a dat mezi organizacemi (workflow) po implementaci FID

Co by mohla implementace FID přinést organizacím?

Komunikace organizací mezi sebou



Přijetím sdílení aplikací a dat mezi organizacemi v rámci FID se zjednoduší a zlepší komunikace v rámci organizace, musí být přednostním důrazem na zabezpečení oprávnění a FID by měl přistupovat k aplikacím, datům a případně dokumentům, které by byly bezpečně předloženy k účelům dokumentu, přístupu a zpracování, nebo ho odmítne.

Přístup k aplikacím jiných organizací po implementaci FID

FID

Test

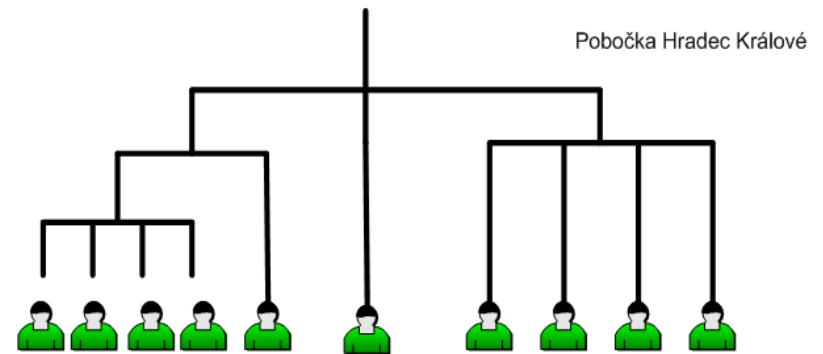
1.otázka SAML je:

A	<input type="checkbox"/>	Security Authorization Markup Language
B	<input checked="" type="checkbox"/>	Security Assertion Markup Language
C	<input type="checkbox"/>	Synthetized Assertion Markup Language
D	<input type="checkbox"/>	Synthetized Authorization Markup Language



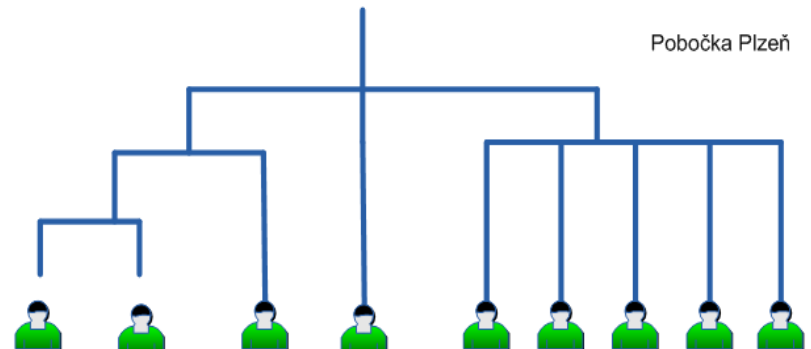
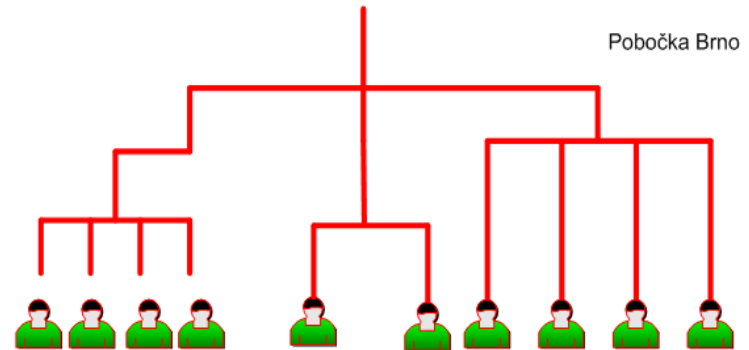
Systemizace - definice, teorie a dopady

Systemizace, využití systemizace v praxi



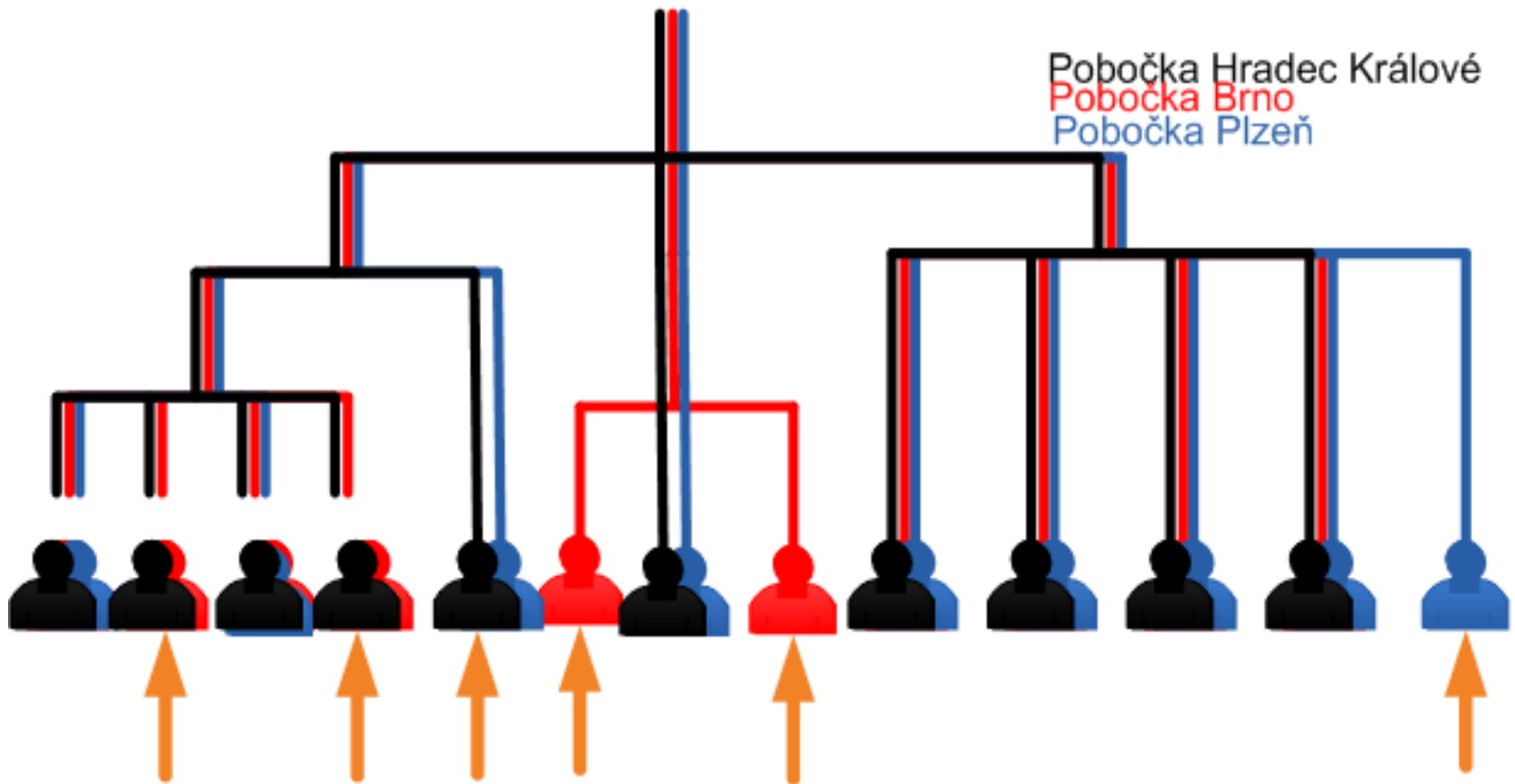
SYSTEMIZACE

- Porovnání organizačních
stromů poboček

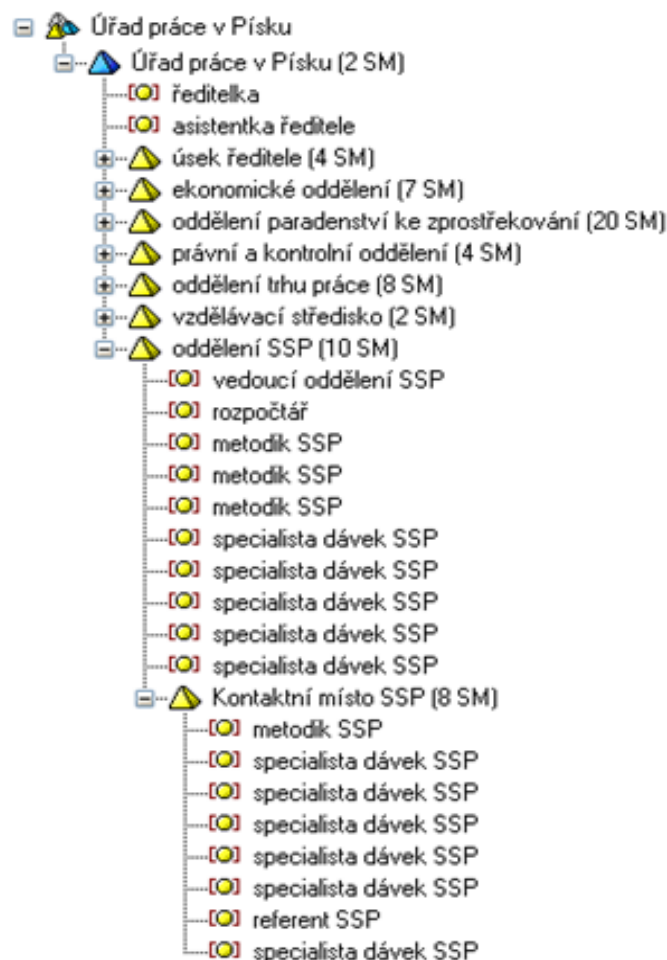


Sytemizace, využití systemizace v praxi

SYSTEMIZACE - porovnání organizačních stromů poboček



Systemizace, využití systemizace v praxi



1. Úvod - test

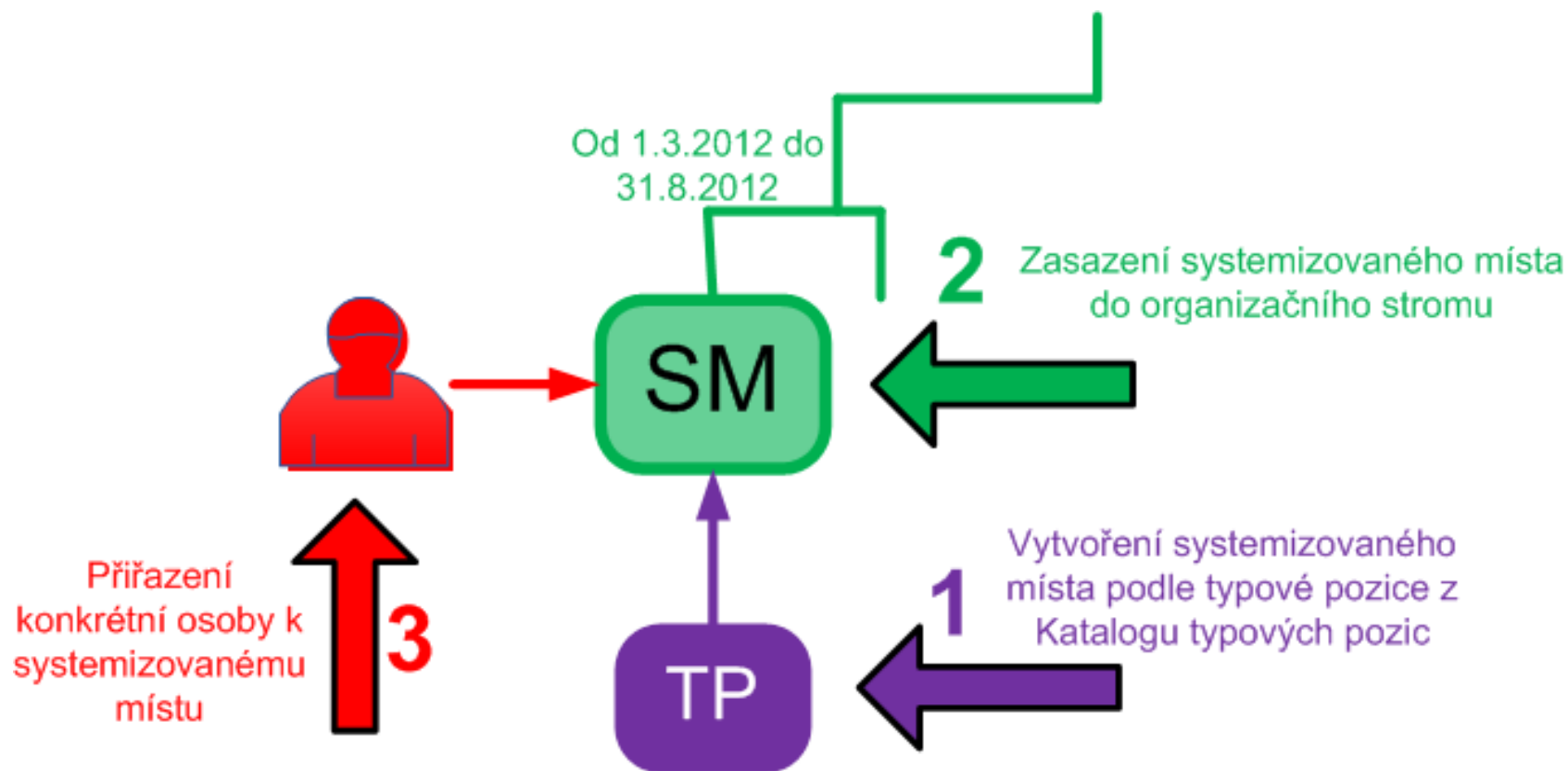
1.otázka Systemizace ve veřejné správě je:

A	<input type="checkbox"/>	Vytváření nových pracovních příležitostí ve státní správě
B	<input type="checkbox"/>	Vedení Informačního systému o službě a platech
C	<input type="checkbox"/>	Koordinace vzdělávání státních zaměstnanců a koordinace vzdělávání fyzických osob
D	<input checked="" type="checkbox"/>	Komplex procesů a opatření založených na důsledném využívání jednotně koncipovaného souboru systemizovaných míst

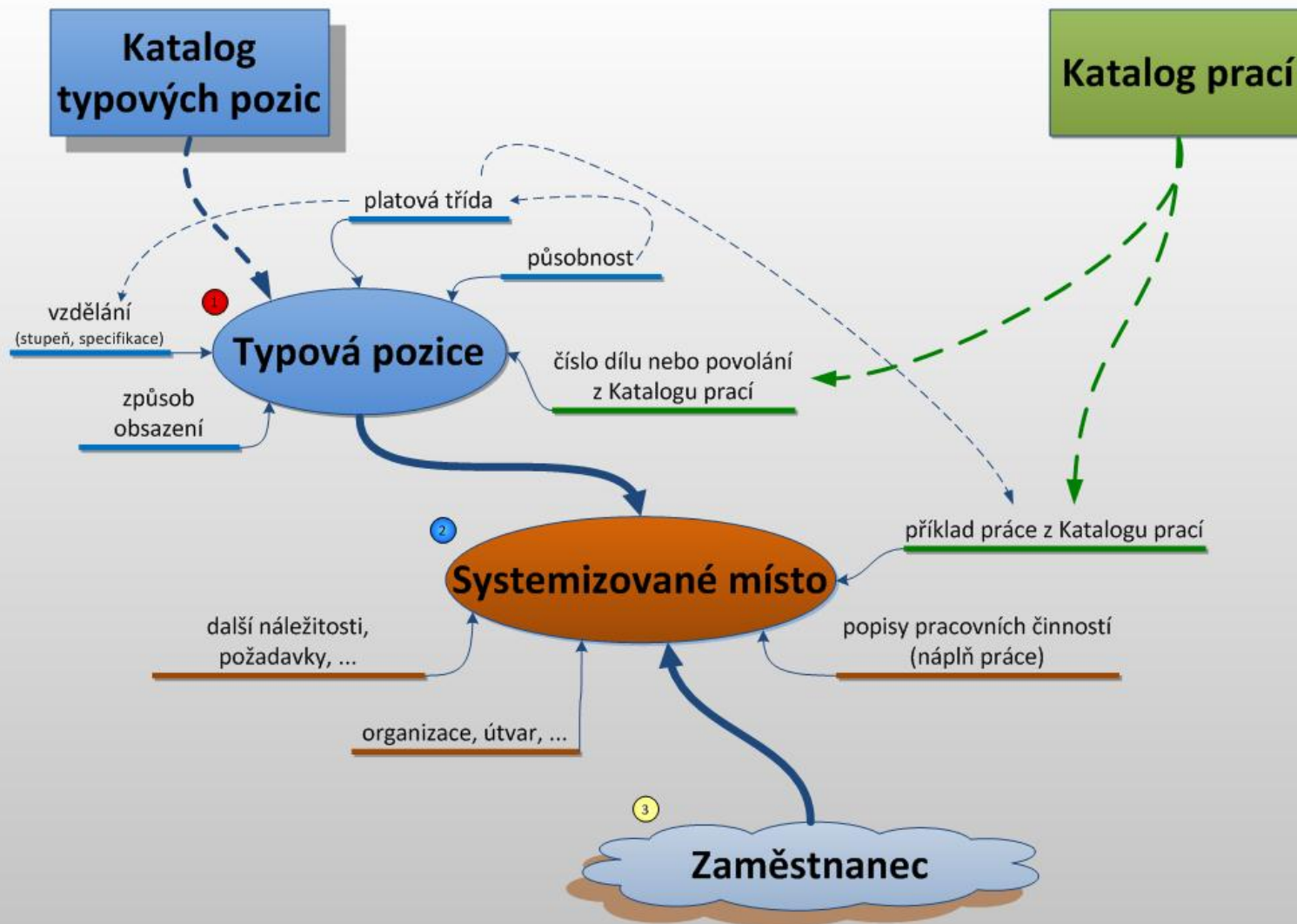


Systemizace - Katalog typových pozic a optimalizace organizační struktury

Systemizované místo



Systemizace



Diskuse

Jak by šlo propojit systemizaci a Identity management ?





Cvičení - Návrh provázání Katalogu typových pozic s návrhem sad v IdM



The
End ?