PA-1919 /ČJ-2017-821012
EDNÁVKA PA - SL/12/2017

Zhotovitel:
Computer Help spol. s.r.o
Blanická 533
120 00 Praha 2
IČ: 49617320
DIČ: CZ49617320
tel: [redacted]
e-mail: [redacted]

olicejní akademie ČR

Vyřizuje : Bc. Jan Nejedlý
: [redacted]

e-mail: [redacted]
nákladové středisko: oit2058510153

Objednatel:
Česká republika-Policejní akademie ČR
Lhotecká 559/7,
143 01 PRAHA 4
bankovní spojení: ČNB, č.ú.: [redacted]
IČ:48135445, DIČ:CZ48135445

Fakturace na adresu:
Policejní akademie ČR
Lhotecká 559/7
143 01 PRAHA 4
způsob úhrady: bankovním převodem

Na základě Vaší cenové na

Nákup služby - integrace AD a
Konzultační a analytické sl — M. j-104 hod
Cena M.j. 950,- Kč bez DPH
Realizace bude provedena do 1. 12. 2017

nabídková cena bez DPH
DPH 21%
cena celkem s DPH
částka k úhradě - zaokrouhleno

Platba po dodání, splatnost fak ry je 14 dnů ode dne jejího doručení objednateli.
fakturu uveďte v!!!

olicejní akademie České republiky v Praze
Lhotecká 559/7, 143 01 Praha 4
P. O. Box 54
IČO 481 35 445

Praha 1.12. 2017

[redacted]

COMPUTER HELP
advantage for professionals

Specifikace pr je mu

M O

Policejní ka

v

V Pra e, 15 11. 2017

Vypracovali:

Ing. Jan Pavel, vedoucí oddělení s užeb a vývoje softwa e

1. Úvod do problematiky

Na základě předběžných konzultací jsme připravili technickou specifikaci implementace systému MSOLIT pro potřeby organizace. Do procesu vstupují další subjekty a a technologie. Základem specifikace produktu MSOLIT je dokument ze dne 14. 9. 2016, avšak funkce budou zásadně upraveny. Tento dokument má za cíl specifikovat celý proces a zajistit komunikaci mezi systémy i dodavateli. Aktuální verze dokumentu spojuje informace z nabídky ze dne 13.8. 2017 s daty zaslanými pro systém SIS.

2. Výchozí podmínky, aktuální stav

Pro potřeby této specifikace předpokládáme existenci a funkčnost následujících technologických prvků či služeb:

- Windows Active Directory – ideálně ve verzi schématu Windows 2008 a vyšší
- Office 365 Azure Active Directory v rámci tenantu, zprovozněná služba Azure AD Sync
- studijní systém Erudio a s nim spolupracující součásti

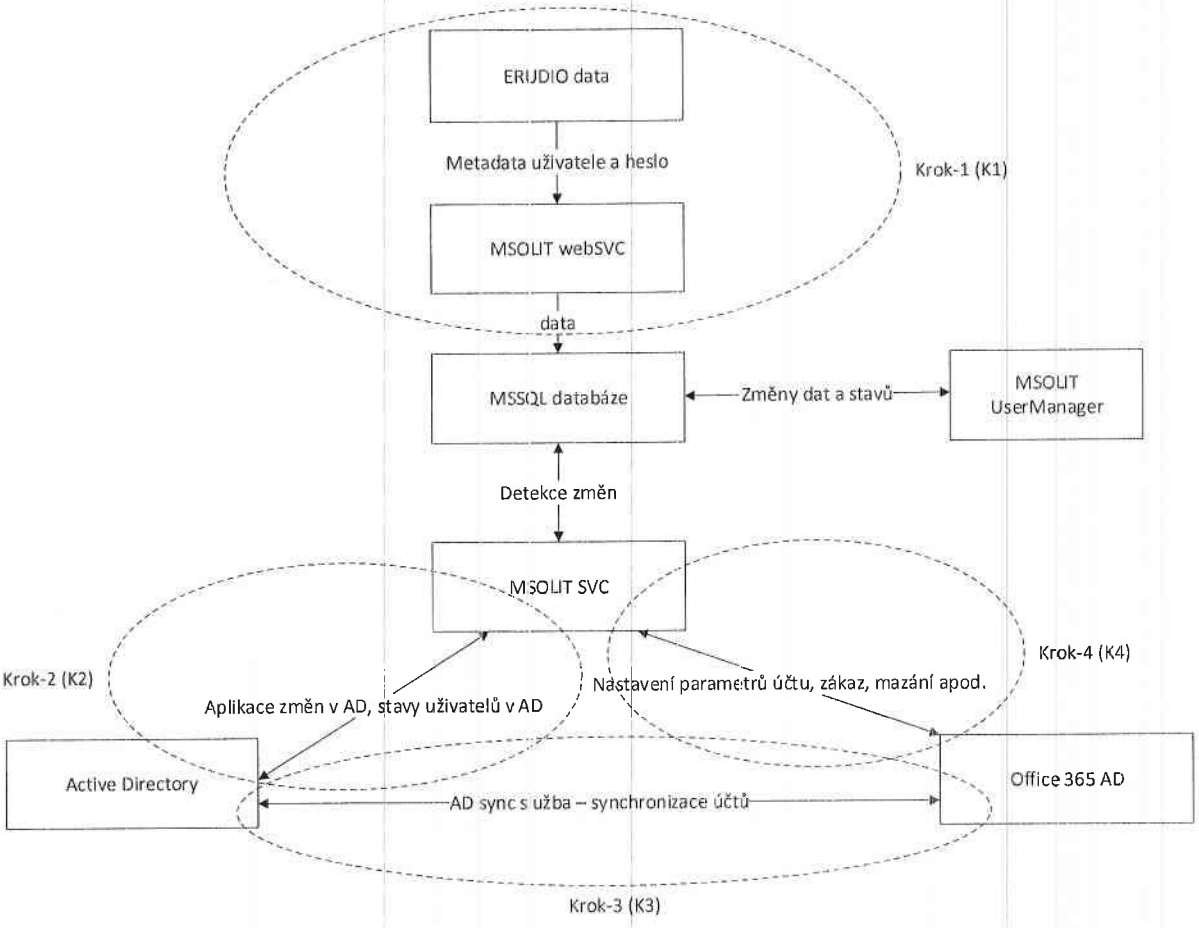
Aktuálně je plně integrován systém Active Directory se synchronizací účtů do Office 365. Cílem systému je zejména automatizovat procesy vytváření účtů, jejich nastavení a zajištění správy životního cyklu účtu.

3. Návrh řešení

Řešení správy uživatelů navrhujeme realizovat formou vícekrokového asynchronního workflow, které provede požadované operace nad uživatelskými objekty v jednotlivých systémech. Asynchronnost nám pravděpodobně nebude nijak vadit, protože cílem rozhodně není rychlost povedené změny ale spolehlivost. Některé procesy jsou na sobě navíc značně nezávislé a jinak něž asynchronně je řešit nelze (např. MSOLT vs AdSync).

V návrhu jsme rozdělili celý systém do procesní mapy a označili jednotlivé kroky, platné zejména pro vytváření účtu – v případě dalších operací bude workflow mírně odlišné. Předpokládáme vznik dat na straně ERUDIO, kde jsou zaslána data uživatele a iniciální heslo (to se pak již mění jinde) – to je KROK 1. V KROKu 2 bude provedeno vytvoření účtů v AD. Následně je třeba počkat na provedení

synchronizace AdSyncu (KROK 3) a po detekci UPN v AzureAD se provede konečný krok 4 s nastavením parametrů Office 365 AD účtu. Základní situaci ukazuje následujícící schéma:



V K1 se poskytnou následující data:

Integrace SIS a Active Directory na PA

Cílem integrace z hlediska SIS je:

1. předávat a aktualizovat relevantní data v AD při práci se studii a osobními daty v SIS
2. ověřování studentů při přihlašování do webové části SISu provádět oproti AD (stejně tak bude v režii AD správa hesel)

Shrnutí:

V SISu jsou osobní údaje evidovány v tabulce OSOBA a informace o studiu v tabulce STUDIUM. Tyto dvě tabulky jsou propojeny pohledem STUD, takže nedochází k duplikaci osobních údajů. S tím je potřeba počítat při práci s účty v AD, protože např. založení nového studia nemusí znamenat založení nového účtu v AD, ale také „probuzení" nebo jen aktualizaci stávajícího účtu.

Pro identifikaci osoby v AD bude použit hlavní email ve tvaru neco@pacr.cz (položka OSOBA.omail, UPN), jako login se nyní v SIS používá šesti ciferné číslo uložené ve sloupci OSOBA.ologin.

Pro zařazení aktivní osoby v AD do nějaké „studijní skupiny" můžeme zasílat různé kombinace informací, viz níže.

Kvůli ověření správnosti dat v AD bude SIS 1x denně posílat dávkově všechny relevantní informace o všech aktivních studiích. Pravděpodobně s nějakým příznakem, že jde o kontrolní dávku.

Poznámky:

- Pouze data o studentech (pohled STUD = tabulky STUDIUM a OSOBA), uchazeči (přijímací řízení) se zde neřeší
- Akce:
  - založení studia – založení osoby, „probuzení" osoby, doplnění odpovídající studijní skupiny pro osobu v AD
  - úprava relevantních dat – již existující studium
  - ukončení/smazání studia – při nastavení stavu studia A nebo Z. Pokud už osoba nemá v AD žádné aktivní studium – expirace účtu. Pokud ještě nějaké jiné aktivní studium má, zruší se mu členství ve skupině odpovídající ukončenému studiu.
- číselník stavů studia (STAV)
  - A – absolvoval
  - D – podmíněný zápis
  - O – opakuje
  - P - přerušeno
  - R – rozlož. ročník – ISP
  - S - studuje
  - U - uzavřel studium
  - V - výjezd na stáž
  - X - přijat k studiu
  - Z – zanechal
- ukončená studia jsou ve stavu A nebo Z
- relevantní data

Proměnná	DB sloupec	Hodnota
OID	OSOBA.oident ??	number(10)
Heslo		
Jméno	OSOBA.ojmeno	varchar(50)
Příjmení	OSOBA.oprijmeni	varchar(50)
Titul před	OSOBA.otitul	varchar(100)
Titul za	OSOBA.otitulza	varchar(100)
Rodné číslo (bez lomítka)	OSOBA.orodc	varchar(10)
Adresa trvalá	Viz dále	
Telefon	Viz dále	

Datum narození	Není	Počítá se z RČ
Stav studia	STUDIUM.sstav	varchar(1), číselník STAV
Email vygenerovaný	OSOBA.omail	varchar(100)
Email soukromý	OSOBA.oumail	varchar(100)
Číslo karty	OSOBA.ocipcislo	varchar(20)
Studijní skupina, popis v AD	Viz dále	

- Adresa – evidujeme více položek odděleně
  - ulice
  - číslo popisné a orientační
  - upřesnění bytu
  - obec
  - PSČ
  - kód obce
  - kód části obce
  - okres
  - stát
- Telefon – evidujeme tři telefony i s předvolbou (telefon 1, telefon 2, mobil)
- Studijní skupina, popis v AD – zde je možno kombinovat více položek: fakulta, studijní program, druh a obor studia, rok přijetí atd.
  - rok přijetí
  - studijní obor
  - forma studia
  - referent
  - studijní stav

Na straně MSOLIT bude připravena webová služba, která bude mít jednu metodu se vstupními parametry dle tabulky a výstupem bude result objekt s hodnotami:

Proměnná	Hodnota/comment
Result	true/false - jestli se podařilo nebo ne
Message	string – OK nebo nějaká hláška

Služba bude WCF SOAP na HTTPS s podporou MEX pointu – tedy inteligentní konzumer webových SOAP služeb si bude umět vygenerovat rozhraní automaticky. Ověřování bude na úrovni AUTH http/s požadavku jménem a heslem. Technicky se bude jednat o zhruba toto:

https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/wcf/basichttpbinding

Detaily a příklad demo služby jen pro ukázku vystavím později, aby se vše dalo připravit na straně ERUDIO.

Dalším krokem K2 je vytvoření účtu v AD. Protože již máme vygenerované UPN a dodané v rámci pole E-mail vygenerovaný, snadno ověříme existenci účtu v AD (e-mail = UPN) a tak tedy nastávají následující situace:

- vytvoření uživatele – UPN v AD neexistuje, použijí se data z K1 a vytvoří se účet
- v rámci vytvoření by se měl uživatel přiřadit do AD skupin
- aktualizace uživatele – provede se změna všech atributů až na UPN a heslo –
- blokování uživatele – shodné se smazáním, uživatel bude zakázán a přesunut do nějaké OU a samozřejmě mu má být odebráno členství ve skupinách – Proces vstupu z normálního režimu bude pomocí příznaku Status studenta – jakmile bude jiný než aktivní, spustí se expirační workflow.

Data pro AD a jejich napojení na ERUDIO data jsou v následující tabulce:

Proměnná	ERUDIO data	Hodnota/comment
Jméno	Jméno	
Příjmení	Příjmení	
Zobrazovací název	Titul, titul za	jméno včetně titulů
Popis: studijní obor – kód fakulty, druh- Bc nebo Mgr-forma-denní nebo kombi-	Studijni skupina?	v jakém bude formátu?
Telefon	Výběr ze 3 telefonů	Jak zvolíme ten správný?
e-mail	email vygenerovaný	
alternativní E-mail	email soukromý	
Číslo karty (záložka pager)	Karta studenta - číslo	
Trvalý pobyt	Adresa	
ÚČET	email vygenerovaný	login example@pacr.eu
Platnost účtu	není třeba	otázka životnost v AD
Je členem	není třeba	Studenti

Otázky k dořešená v průběhu implementace:

- jakým způsobem budou chodit změny uživatelských metadat z ERUDIO (jaká data?) – v případě, že již uživatel existuje a jakým způsobem budeme toto promítat do účtů? Předpokládám, že UPN je neměnné. – tady předpokládáme, že budeme updatovat jen smysluplné údaje a ignorovat kolize
- když bude již uživatel existovat, bude se při update dat v K1 ignorovat pole Heslo?
- jak se určí OU nového uživatele v AD, jak se určí OU do které se uživatel po zakázání přesune? nutné naspecifikovat
- nemáme nadefinované AD skupiny, do kterých by se měl uživatel dávat a nebo zase vyndávat.. nutné naspecifikovat

- co se stane, když bude změna UPN? v zásadě by mělo workflow projít vytvořením nového uživatele se všemi následky

Fáze K3 je prováděna automaticky, což je dobré. V našem případě to však způsobí problém s vykonatelností fáze 4 – účet musí být nejdříve v Office 365, abychom mohli provést jeho nastavení. Proto tedy bude K4 zcela asynchronní a bude v pravidelných intervalech opakovat dotazy na existenci UPN v Azure AD (podle stavu uživatelů v MSOLIT – příznak „create"). V okamžiku úspěšné detekce se provede workflow K4 a to zejména:

Operace	Hodnota/comment
Nastavení jazyka, UsageLocation, Language	CZ, bude také nějaký jiný jazyk?
Nastavení licence	bude natvrdo v konfiguráku
Operace blokování a mazání podle expiračního WF	viz. specifikace MSOLIT, to zůstane stejné
Něco dalšího?	Snad ne...

Kontrolní cyklus

Vzhledem k tomu, že operace mezi ERUDIO a MSOLIT budou v zásadě synchronní a ERUDIO nebude opakovat zaslání dat v případě chyby, navrhujeme kontrolní cyklus, který 1x za den provede:

- zaslání všech aktuálních dat (účtů platných) do MSOLIT – formou webové služby, bylo by dobré tato data nějak označit příznakem, aby to bylo MSOLITu zřejmé že jde o kontrolu (pro jistotu)
- po dokončení procesu MSOLIT provede kontrolu integrity účtů v AD a v Office 365 (existence, klíčové parametry – nutné upřesnit co udělat)
- provede případné korekce nebo vyreportuje zjevné nebo neopravitelné chyby

Self service password reset portal

Zde bych s tím nedělal žádné složitosti a použil nějaké hotové OSS řešení – například toto: https://unopasscore.codeplex.com/

případně se inspiroval v rozhraní a aplikaci zjednodušil. Licence je poměrně volná a aplikace se zdá být pěkná. Bude třeba upřesnit funkce jako použití recaptcha a případně nějaké další ochranné prvky (e-mailové potvrzení apod.).

4. Požadavky na systém a služby

Pro provoz systému MSOLIT v této specifikaci je třeba zajistit:

- běhové prostředí Windows Server 2008 R2 a vyšší, nejlépe Windows 2016 Standard
- 2 core CPU, 4 GB paměti, 20 GB na disku (parametry jsou celkem jedno, je to nenáročné)
- instalovaný .NET Framework 4.5 a vyšší, IIS 7+
- server musí být připojený do domény Active Directory
- SQL server 2008 R2 a vyšší, možno i ExpressEdition nebo instance na jiném serveru, SQL autentifikace (mixed mode)
- účet s oprávněním pro správu uživatelských účtů v AD (nemusí být domain admin ani to není vhodné!!!)
- účet s oprávněním globální správce pro Office 365
- přístup k SMTP serveru pokud nebudeme posílat e-maily přes Office 365

5. Předpokládané práce k realizaci systému

Pro realizaci tohoto systému prozatím předpokládáme následující práce:

Položka	Počet hodin
Reimplementace jádra systému MSOLIT	25
WebService pro příjem dat z ERUDIO	10
Konektor pro ActiveDirectory	20
Self service portal	30
Instalace a konfigurace, ladění a testování	19
Celkem	**104h**

V aktuální specifikaci odhadujeme objem práce na 120 hodin práce, hodinová sazba je 950 CZK/h bez DPH, celkem tedy 98.800,- CZK bez DPH.

6. Závěr

Tato verze je konečnou specifikací projektu. Některé otázky však nejsou vyřešeny a předpokládáme, že budou objasněny během vývoje nebo testování systému.