



Opis predmetu zákazky

Nahradenie integračných funkcií CDO prostredníctvom rozšírenia-presunu na systém midPoint na Univerzite Komenského v Bratislave

1. Súčasný stav

Univerzita Komenského v Bratislave (ďalej len „objednávateľ“) požaduje vhodné IDM riešenie na správu identít používateľov, zvýšenie bezpečnosti a prehľadnosti identít a nahradenie funkcionalít zastaralého systému CDO. Objednávateľ rozhodol z množstva dostupných produktov použiť open source provisioning systém midPoint, ktorý je vyvíjaný na Slovensku a je mu poskytovaná podpora výrobcom. V rámci univerzitných interných kapacít bol spustený pilotný projekt proof of concept (PoC) na overenie vhodnosti tohto nástroja. Výsledkom projektu je úspešná implementácia nasledovných procesov:

- import študentov z akademického informačného systému AISz
- import zamestnancov, preukazov
- poskytnutie týchto údajov pre nový systém turniketov na rektoráte vo formáte XML.

Tento projekt bude riešený pre:

- počet aktívnych študentov: 23 400
- počet aktívnych zamestnaneckých pomerov: 5 700
- počet aktívnych externistov: 620
- počet alumných študentov a zamestnancov evidovaných od roku 2006: 244 000

2. Nový/Očakávaný stav

Predmetom zákazky je:

- Výber vhodného dodávateľa, ktorý je partnerom spoločnosti Evolveum na rozšírenie funkcionality existujúcej inštalácie systému midPoint.
- Revízia a úprava aktuálnej PoC konfigurácie (ktorá je v prípade potreby k dispozícii na nahliadnutie).
- Implementácia, testovanie a nasadenie nových funkcionalít, ktoré sú popísané ďalej v tomto texte.
- Funkcionalita a práce budú rozdelené do troch fáz.
- Zabezpečenie podpory zo strany vendora (product support) predplatený na jeden kalendárny rok dopredu od dodania prvej fázy.
- 8x5 podpora existujúceho PoC riešenia vrátane jeho rozšírení popísané nižšie predplatený na jeden kalendárny rok od uvedenia danej fázy systému do ostrej prevádzky.
- Zaškolenie IDM administrátora na bežné prevádzkové úlohy.
- Dodávka konfigurácie systému vrátane midscribe dokumentácie.

Požadované nové funkcionality:

1. konfigurácia servisného účtu a vytvorenie **REST API** príkladov volaní s možnosťou zabezpečenia:
 - a) zistenie Univerzitného Osobného Čísła (UOČ),



- b) overenie existujúceho hesla a zmena hesla,
- c) zistenie prístupového kódu pre WIFI,
- d) zmena prístupového kódu,
- e) midPoint zabezpečí provizioning/distribúciu hesla a prístupového kódu do napojených cieľových systémov,
- f) univerzita internými zdrojmi použitým tejto REST API vytvorí aplikáciu vo farbách univerzity (používateľské rozhranie),
- g) predpokladá sa, že midPoint sa zabezpečí, čím nebude verejne dostupný, ale výlučne cez VPN pre vybraných zamestnancov,
2. vytvorenie autorizačnej midPoint role pre **hotline a správcov hesiel** na súčastiach univerzity na
 - a) vynútené zablokovanie prístupu (hodinová výpoveď),
 - b) overenie konca rodného čísla a zobrazenie aktuálneho prístupového kódu,
 - c) overenie konca rodného čísla, reset hesla a poslanie cez SMS na zadané mobilné číslo,
3. konfigurácia, testovanie a nasadenie **OpenLDAP** cieľového systému s podporou
 - a) vytvorenie, úprava a zmena hesla používateľov v OpenLDAP
 - b) vytvorenie automatických a manuálnych grúp/skupín
 - c) automatické zaradenie používateľov do týchto grúp/skupín
4. konfigurácia, testovanie a nasadenie univerzitných **Active Directory** ako cieľových systémov s podporou. Univerzita má takéto systémy aktuálne dva, kde počas inštalácie sa rozhodne, či bude pokračovať v takomto nasadení alebo nasadí len jeden centrálny. Nadceniť ale požadujeme oba body 4a) a 4b).
 - a) vytvorenie, úprava, zakázanie a zmena hesla používateľov v AD
 - b) vytvorenie automatických a manuálnych grúp/skupín
 - c) automatické zaradenie používateľov do týchto grúp/skupín
5. vytvorenie používateľa a zmena hesla v **KERBEROS**
6. evidovanie **email aliasov**
7. vytvorenie nového web service **SAP** connId konektora napojeného na SOFIA2 pre vysoké školy na
 - a) import organizačnej štruktúry (OS)
 - b) import nákladových stredísk (NS)
 - c) import zamestnaneckých pomerov a zaradenie do OS a NS
 - d) starý SAP konektor je deprecated a JCO API na strane SOFIA2 bude pravdepodobne čoskoro vypnutý
 - e) konfigurácia, testovanie a nasadenie nového zdrojového systému cez nový WS SAP konektor
8. koordinácia pripojenia **OpenVPN** voči OpenLDAP

Predpokladá sa, že synchronizácia do Exchange a O365 zostane nezmenená.

3. Fázy riešenia

Predpokladané míľniky a dodávky / jednotlivé fázy:

- prvá fáza – dodanie bodov 1) a 2) vrátane evolveum product support na 1 rok dopredu
 - uvedomujeme si, že evolveum product support sa aktivuje po 3 mesiacoch od jeho zaplattenia
- druhá fáza – dodanie 3), 4a), 4b), 5), 6) konfigurácie predvedené v testovacom prostredí, čo zahŕňa L2 5x8 podporu na 1 rok dopredu
- tretia fáza – dodanie 7) a 8) a nasadenie riešenia do produkcie