Změnové požadavky JAAS – I. část požadavek ISVRHD - 26966

Ministerstvo spravedlnosti
České republiky

asseco

Projekt:	ISVR – změnové požadavky JAAS		
Datum:		Stav:	final
Autor:			
Dodavatel:	AssecoCentralEurope, a.s.		
Zákazník:	Ministerstvo spravedlnosti ČR		
Číslo dokumentu:	Webové služby	Verze:	V0.1

Schválení

Jméno	Podpis	Pozice	Datum	Verze

Distribuční seznam

Jméno	Podpis	Organizační jednotka	Datum	Verze

1 ISVRHD- 26966 - Úprava JASS – Řízení syntetických účtů JAAS v IDM

1.1 Popis požadavku řízení syntetických účtů JAAS v IDM

1.1.1 Popis současného stavu

Pro potřeby interního testování mohou být na testovacím interním federátoru JAAS zřízeny takzvané syntetické účty. Tyto účty reprezentují virtuální osoby reprezentující typové uživatele systému (persony) s potřebnou sadou oprávnění. Tyto účty mají přidělené username a password, kterým je možné se za danou personu přihlásit a snadno měnit různé typy uživatelů během procesu testování, narozdíl od nutnosti využívat reálné osoby identitních providerů (IdP) NIA/ISDS nebo testovací osoby zde existující.

Aby bylo možné syntetické účty používat, musí být pro danou aplikaci (SeP) v testovacím prostředí aktivní přihlašování pomocí username/password.

Aktuálně jsou syntetické účty vytvářeny ručním zásahem na straně JAAS/RDM, navíc se pak musí určité údaje synchronizovat na cílovém systému, obvykle opět ručním zásahem mnohdy až na úrovni databáze. Úpravy těchto účtů a jejich oprávnění jsou pak zcela manuálním procesem na straně JAAS. S ohledem na stále širší využívání JAAS pro justiční systémy a stále větší množství potřebných účtů, je tato situace nevyhovující.

1.1.2 Popis cílového stavu

Cílový stav: S nově vybudovaným Identitiy Management systémem (IDM) Justice se nabízí otázka přenést řízení těchto účtů právě do IDM. Tento přístup má hned několik benefitů:

1. Zpřehlednění evidence syntetických účtů.
2. Využití stávajících služeb pro zakládání a ověřování uživatelů mezi JAAS a koncovými systémy.
3. Při napojování nového systému (SePu) na JAAS je možné už v testovacím prostředí snadno vyzkoušet všechny metody na těchto účtech místo spoléhání se na testovací účty IdP (NIA/ISDS)
4. Pro hromadné založení testovacích účtů je možné využití nativních funkcí IDM.

1.1.3 Seznam požadavků

Disclaimer: Požadavky jsou děleny mezi JAAS/RDM a IDM podle současné znalosti věci. BRQ se mohou následně upravit po revizi oběma stranami (např. když jeden systém nebude schopen snadno implementovat požadavek na svojí straně).

BRQ-JAAS-001 vytvoření nové služby na RDM API, která umožní vytvoření nového syntetické uživatele včetně možnosti zvolení username/password na straně IDM.

BRQ-JAAS-002–v případě kolize username je informace vrácena přes RDM API a uživatel není založen (aby bylo možné po opravě username uživatele založit), stejně tak v případě dalších chyb je informace vrácena přes rozhraní. V případě úspěchu jsou vráceny kompletní informace uživatele včetně identifikátorů NameIdentifier, SubjectIdentifier a MandateId.

BRQ-JAAS-003 – pro úpravy dat uživatelů, přidávání a odebírání rolí očekáváme použití stávajících služeb, pokud není z technických důvodů nutné provádět jinak.

BRQ-JAAS-004 - jelikož IDM bude zakládat uživatele pro různé SeP, je žádoucí, aby toto reflektovaly služby pro provisioning uživatelů do RDM – tj. aby IDM nevystupovalo jako konkrétní SeP s použitím RDM API credentials daného SePu, ale mělo vlastní ověření a následně pouze indikovalo, kterému SePu uživatele zakládá. Tento požadavek není specifická pro syntetické účty, ale měl by do budoucna reflektovat reálná stav spolupráce IDM a JAAS/RDM i na produkčním prostředí.

BRQ-IDM-001 - při zakládání uživatele do IDM mít možnost zadat pro konkrétní typy uživatelů username/password.

BRQ-IDM-002 - pravidla validace username a hesla definuje JAAS/RDM.

BRQ-IDM-003 – IDM bude volat pro specifické typy uživatelů novou/upravenou službu RDM API včetně username/password.

BRQ-IDM-004–v případě chyby na straně RDM API zobrazí IDM uživateli chybu, v případě úspěchu zobrazí všechny detaily založeného účtu z RDM API.

BRQ-IDM-005 – IDM umožní přidávat a odebírat role těmto uživatelům stejně jako normálním uživatelům včetně použití pravidel, hromadného importu apod.

BRQ-IDM-006 – IDM umožní přidělit oprávnění pro zakládání uživatelů pro konkrétní systémy a konkrétních rolí pouze určitým osobám.

Poznámky za stranu JAAS:

Vytvoření bude také rozdělené do dvou kroků jako u vytvoření uživatele z AD.

1. V JAASu se založí uživatel
2. V RDM se vytvoří mandáty pro fyzickou osobu.
3. V RDM se učet propojí s fyzickou osobou. Ale bude implementovaná jiná metoda, popř. upravená ConnectWithActiveDirectory.