1 INTEGRACE IDM A PIS FLUXPAM VČETNĚ AGENTURNÍCH OSOB

Zadání vychází z dokumentů analýzy provedené firmou AMI.

Komunikace mezi PIS FLUXPAM a IDM, resp. Agenturními osobami (dále jen FLUX AO) a IDM bude probíhat na úrovni webových služeb (dále jen WS), které budou vytvořeny dle níže uvedeného zadání.

Návrh řešení vychází z předpokladu, že bude využit nadstavbový modul PIS FLUXPAM pro ověřování uživatelů v AD, jehož licenci bude potřeba ze strany MHMP pořídit.

Dalším předpokladem je potřebná součinnost ze strany MHMP při zabezpečení https:// protokolu a instalace potřebného certifikátu pro provoz WS.

1.1 NÁVRH INTEGRACE PIS FLUXPAM DO IDM

Tato kapitola popisuje, jakým způsobem bude systém FLUXPAM zapojen do centrální správy identit přes systém IdM.

Tvorba přístupu pro vedoucí zaměstnance a zaměstnance pověřené dočasným řízením některého organizačního uzlu ORS bude probíhat v nezměněné podobě přímo v systému FLUX. Do IdM budeme tyto uživatele načítat včetně rolí, které jim byly přiděleny.

Rozsah rolí, jejichž přidělování bude řízeno systémem IdM, bude omezen na role „základní". Tyto základní role budou role pouze umožňující přístup do jednotlivých modulů a jejich výčet bude upřesněn ze strany MHMP, další konkrétní přístupy budou nastavovány přímo v systému FLUXPAM. Základní roli bude možné přidělit i ve FLUXPAMu, IdM to zjistí na základě rekonciliace, uloží přidělení role do své DB a pošle o tom notifikaci.

Informace o potřebných právech, které se dnes vkládají do požadavku v Service Desku, budou obsaženy v požadavku o přidělení „základní" role v IdM.

Jsou popsány operace, jaké budou mezi IdM a FLUXPAM probíhat a jaké atributy budou přenášeny.

1.1.1 Synchronizace pracovně právních vztahů

Při operacích s pracovněprávními vztahy budou ze systému FLUXPAM přenášeny níže uvedené atributy.

Atribut	Poznámka
Jméno	
Příjmení	
Osobní číslo	
Uživatelské jméno	Login
Mail	firemní
Telefon	Pevná i mobil (odděleně)
Funkční zařazení	Název SM
Název oddělení	
Název odboru	
Název sekce	

Organizační jednotka (MHMP, P1, P2, ...)	MHMP
Lokalita – pracoviště	ID Adresy budovy
Fotografie	V systému se sice využívá ale je pouze předmětem akce tvorby karty. V systému není uchovávána. Zatím se nebude přenášet. Bude zasíláno prázdno.
ID pracovněprávního vztahu	ID zaměstnance
Zaměstnání vykonávané v organizaci	Kód - text
Kmenový pracovní poměr	Ano/Ne (1/0)
Číslo karty	Identifikátor karty (v současné době přenášený jako identifikátor do ABI), null pokud karta neexistuje
GUID osoby	Identifikátor osoby napříč pracovně právními vztahy
Mobilní telefon	Dle vyplnitelných položek.
Pevná linka	Dle vyplnitelných položek
Další telefon ..	Dle vyplnitelných položek
Titul před	
Titul za	
Datum Nástupu	Datum zavedení do evidence.
Datum Ukončení	Datum vyřazení z evidence.
ID Budovy	Reference na budovu
Patro	Viz. Export - floor
Název Budovy	Viz. Export - name

Místnost	Viz. Export - room

1.1.2 Synchronizace uživatelů

- Jednoznačný identifikátor (GUID),
- login,
- vazba na pracovně právní vztah, ID zaměstnance pokud je připojen (jinak bude null),
- seznam přiřazených základních rolí (synchronizovaných do IDM)

1.1.3 Synchronizace rolí

Ze systému FLUXPAM budou do IdM synchronizovány základní role. Přenášeny budou atributy:

- identifikátor role (GUID),
- jméno role,
- popis role (v případě že je k dispozici - vysvětlení, co role znamená).

1.1.4 Synchronizace organizačních uzlů

Ze systému FLUXPAM budou do IdM synchronizovány veškeré organizační uzly. Přenášeny budou atributy:

Atribut	Poznámka
identifikátor uzlu	TreeNum
jméno uzlu	
popis uzlu	v případě že je k dispozici
Identifikátor nadřazeného uzlu	Parent TreeNum
zkratka uzlu	Viz. Export: abbrev
pořadí uzlu	Viz. Export: sentence
kód organizační jednotky	Viz. Export: code

1.1.5 Synchronizace funkčních zařazení

Atribut	Poznámka
identifikátor SM	TreeNum

jméno SM	ve variantě rodu podle zařazeného zaměstnance
popis jednotky	v případě že je k dispozici
Identifikátor nadřazeného uzlu	Parent TreeNum
je vedoucí	Příznak, zda jde o vedoucí SM org. člení z ORS
pořadí uzlu	Viz. Export: sentence
kód organizační jednotky	Viz. Export: code
Seznam pracovněprávních vztahů zařazených do systematizovaného místa	ID veškerých pracovněprávních vztahů majících vazbu na systematizované místo

1.1.6 Synchronizace budov

Ze systému FLUXPAM budou do IdM synchronizovány veškeré budovy. Přenášeny budou atributy (atributy jež nejsou dostupné nebudou ve zprávě vyplněny):

Atribut	Poznámka
ID Budovy	Identifikátor budovy
Název	Název budovy - uživatelské pojmenování budovy.
Městská část	Viz. Export – city-part
Stát	Viz. Export – country
Okres	Viz. Export – district
Ústředna	Viz. Export: exchange
Domovní číslo	Viz. Export: house number
Typ domovního čísla	Viz. Export – house number type
Odkaz do map	Viz. Export – map url
Obec	Viz. Export – municipality

Část obce	Viz. Export – municipality part
Číslo orientační	Viz. Export – orientation-number
Kraj	Viz. Export – region
Ulice	Viz. Export – street
PSČ	Viz. Export – zip-code

1.1.7 Neadresované uživatelské účty

V rámci přenosu budou identifikovány účty, jež nejsou vázány na osobu, ale jsou využívané pro vykonávání určité činnosti v rámci systému (např. uzávěrka měsíce, přechod na nové období atd.). Na tyto účty má v současné době přístup více lidí.

V IdM budou tyto účty evidovány ve formě rolí, o které bude možno normálně žádat a přidělovat je. Toto bude sloužit jen k evidenci, na základě přiřazení těchto rolí nebude IdM provádět žádnou akci.

1.1.8 Technické – systémové účty

Systémové účty FLUXPAM nebudou synchronizovány s IdM. V IdM budou mít takové účty nastaven status „protected" zabraňující jakýmkoliv akcím nad těmito účty ze strany IdM.

1.2 PŘIPOJOVACÍ ROZHRANÍ

Integrace systému FLUX s IdM bude realizována prostřednictvím webových služeb, kde první částí bude rozhraní poskytované systémem FLUXPAM pro získání identitních dat. Druhou částí pak mechanismus notifikace systému IdM o změně provedené nad pracovně-právním vztahem.

1.2.1 Webové služby (web services) – rozhraní FLUXPAM

Pro rozhraní je třeba zajistit následující:

- Webové služby rozhraní musejí být dostupné přes zabezpečený přístup (SSL) v rámci domény MHMP.
- Zajištění testovací i produkční verze rozhraní.
- V případě chyby během zpracování požadavku musí rozhraní vracet informaci s vhodným popisem dané chyby.
- Rozhraní podporuje nejlépe standard SOAP verze 1.0 - 1.2 nebo jiný obecně uznávaný standard.
- Pro každou část (seznam uživatelů, rolí, ORS uzlů, SM) bude WS volána samostatně

- Při volání WS pro celé seznamy entit (seznam uživatelů, rolí, ORS uzlů, SM, zaměstnanců) budou v seznamu uvedeny pouze atribut identifikátor a u zaměstnance ještě login.
- Budou vytvořeny metody pro poskytnutí detailu jednotlivých entit na základě zaslaného identifikátoru a typ entity.

Ze strany FLUXPAM je přes rozhraní třeba zpřístupnit následující akce:

Název	Popis
čtiOsobu(ID)	Vrátí detail osoby včetně vazeb na organizační strukturu (pokud se nevrací reference na osobu v rámci detailu org. jednotky) podle interního ID nebo osobního čísla.
čtiOsoby()	Vrátí kompletní seznam osob (možno stránkovat)
čtiUživatele(ID)	Vrátí detail uživatele podle interního ID včetně vazeb na role (pokud se nevrací reference na uživatele v rámci detailu role)
čtiUživatele()	Vrátí kompletní seznam uživatele (možno stránkovat)
vytvořUživatele(Object Uživatel)	Vstupem je objekt uživatele obsahující veškeré atributy vyplněné. Návratová hodnota bude vytvořený Identifikátor.
smažUživatele(ID)	Vymaže uživatele ze systému.
čtiRoli(ID)	Vrátí detail role.
čtiRole()	Vrátí kompletní seznam rolí systému (možno stránkovat)
čtiPřiřazenéRoleUživateli(ID uživatele)	Vrátí seznam rolí přiřazených uživateli.
přiřaďUživateliRoli (ID uživatele, ID role)	Přiřadí uživateli roli
odeberUživateliRoli (ID uživatele, ID role)	Odebere uživateli roli
čtiOrgJednotku(ID org.jednotky)	Vrátí detail org. jednotky vč. ID nadřazené jednotky.
čtiOrgJednotky()	Vrátí kompletní seznam organizačních jednotek (možno stránkovat)
čtiFunkčníZařazení(ID fn. zařazení)	Vrátí detail funkčního zařazení vč. ID

	nadřazené jednotky.
čtiFunkčníZařazení ()	Vrátí kompletní seznam funkčních zařazení (možno stránkovat) součástí by měla být reference na nadřazenou jednotku a příznak zda-li jde o vedoucího či nikoliv.
delegujOprávnění(ID delegující osoby, ID delegované osoby, platnost delegace od - do)	Deleguje oprávnění delegující osoby na osobu delegovanou, vrátí ID delegace.
zrušDelegaci(ID delegující osoby, ID delegované osoby)	Zruší delegaci oprávnění.
ČtiDelegace()	Vráti seznam delegací.
čtiBudovy()	Vrátí kompletní seznam budov.
čtiBudovu(ID budovy)	Vrátí detail budovy.

Delegování znamená nastavení zastupování pro WF.

1.2.1 Notifikace IdM

Při změně atributů (jméno, přijmení, e-mail a číslo karty) pracovně-právního vztahu bude třeba volat SOAP rozhraní IdM, které bude umožňovat volat přepočítání uživatele.

Pro tyto účely bude vytvořen systémový účet „flux-notifikace“ s heslem, které bude nastavené dle dohody.

URL rozhraní bude specifikováno po realizaci testovacího a produkčního prostředí ze strany MHMP.

Klient na straně bude využívat basic autentifikace a bude volat následující, kde osobní číslo bude variabilní parametr:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mod="http://midpoint.evolveum.com/xml/ns/public/model/model-3">
  <soapenv:Header/> <soapenv:Body>
    <mod:executeChanges>
      <mod:deltaList>
        <apit:delta xmlns:apit="http://midpoint.evolveum.com/xml/ns/public/common/api-types-3"
xmlns:ns_xmlns="http://prism.evolveum.com/xml/ns/public/types-3">
          <ns_xmlns:changeType>add</ns_xmlns:changeType>
          <ns_xmlns:objectType xmlns:c="http://midpoint.evolveum.com/xml/ns/public/common/common-
3">c:TaskType</ns_xmlns:objectType>
          <ns_xmlns:objectToAdd xsi:type="c:TaskType" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:c="http://midpoint.evolveum.com/xml/ns/public/common/common-3">
            <c:name>Recompute user x</c:name>
          <extension xsi:type="c:ExtensionType" xmlns:se="http://midpoint.evolveum.com/xml/ns/public/model/scripting/extension-3">
            <se:executeScript xmlns:s="http://midpoint.evolveum.com/xml/ns/public/model/scripting-3">
              <s:search>
                <s:type>c:UserType</s:type>
                <s:searchFilter xmlns:q="http://prism.evolveum.com/xml/ns/public/query-3">
                  <q:and>
                    <q:substring>
                      <q:matching>polyStringNorm</q:matching>
                      <q:path>c:employeeNumber</q:path>
                      <q:value>$OSOBNI_CISLO$</q:value>
                    </q:substring>
                  </q:and>
                </s:searchFilter>
                <s:action>
                  <s:type>recompute</s:type>
                </s:action>
              </s:search>
            </se:executeScript>
          </extension>
                                <c:ownerRef oid="00000000-0000-0000-0000-000000000002" type="tns:UserType"
xmlns:tns="http://midpoint.evolveum.com/xml/ns/public/common/common-3"/>
                               <category>BulkActions</category>
 <handlerUri>http://midpoint.evolveum.com/xml/ns/public/model/scripting/handler-3</handlerUri>
                               <recurrence>single</recurrence>
                                <executionStatus>runnable</executionStatus>
          </ns_xmlns:objectToAdd>
        </apit:delta>
      </mod:deltaList>
    </mod:executeChanges>
  </soapenv:Body>
</soapenv:Envelope>
```

1.3 NÁVRH INTEGRACE FLUX AO DO IDM

Tato kapitola popisuje, jakým způsobem bude systém FLUX AO zapojen do centrální správy identit přes IdM.

Jsou popsány operace, které budou mezi IdM a FLUX AO probíhat a jaké atributy budou přenášeny.

1.3.1 Synchronizace smluvních vztahů

Při operacích nad smluvnímy vztahy budou do systému FLUX AO přenášeny níže uvedené atributy. Ze systému FLUX AO pak pomocí notifikace budeme občerstvovat atribut číslo karty.

Atribut	Synchronizace	Poznámka
Jméno	Ano	
Příjmení	Ano	
Osobní číslo	Ano	
Uživatelské jméno	Ne	login
Mail	Ne	
Telefon	Ne	
Funkce (pracovní zařazení)	Ne	
Název oddělení	Ano	
Název odboru	Ano	
Název sekce	Ne	
Organizační jednotka (MHMP, P1, P2, ...)	Ano	MHMP
Lokalita – pracoviště	Ne	
Fotografie	Ne	V systému se sice využívá, ale je pouze předmětem akce tvorby karty. V systému není uchovávána.
ID zaměstnance		Bude přiděleno v FLUX AO

Číslo karty	Ano	bude null dokud nebude existovat karta

1.3.2 Vytvoření Agenturní osoby

Na základě zaslaných dat z IDM bude WS zakládat záznam do FLUX AO. Jako odpověď bude vráceno ID agenturní osoby.

Kmenové středisko (název firmy) bude zasíláno null a bude se vyplňovat na straně aplikace FLUX AO. Informace o firmě (kmenové středisko) bude zasílána v rámci notifikace z IDM pověřené osobě, správci agenturních osob.

Agenturní osobě bude možno přidělit zaměstnaneckou kartu, při přidělení karty bude odeslána notifikace do IDM.

1.3.3 Synchronizace uživatelů

Ze systému FLUX AO budou do IdM synchronizováni uživatelé. Přenášeny budou atributy:

- identifikátor uživatele, GUID
- login

1.3.4 Synchronizace rolí

Ze systému FLUX AO budou do IdM synchronizovány „základní" role. Přenášeny budou atributy:

- identifikátor role, GUID
- jméno role,
- popis role (v případě že je k dispozici).

1.3.5 Systémové účty

Systémové účty FLUX AO nebudou synchronizovány do IdM. V IdM budou mít takové účty nastaven status „protected" zabraňující jakýmkoliv akcím nad těmito účty ze strany IdM.

1.4 PŘIPOJOVACÍ ROZHRANÍ

Integrace systému FLUX AO s IdM bude realizována prostřednictvím webových služeb, kde první částí bude rozhraní poskytované systémem FLUX AO pro získání identitních dat. Druhou částí pak mechanismus notifikace systému IdM o změně provedené nad smluvním vztahem.

1.4.1 Webové služby (web services)

Pro rozhraní je třeba zajistit následující:

- Webové služby rozhraní musejí být dostupné přes zabezpečený přístup (SSL) v rámci domény MHMP.
- Zajištění testovací i produkční verze rozhraní.
- V případě chyby během zpracování požadavku musí rozhraní vracet informaci s vhodným popisem dané chyby.
- Rozhraní podporuje nejlépe standard SOAP verze 1.0 - 1.2 nebo jiný obecně uznávaný standard.

Ze strany FLUX AO je přes rozhraní třeba zpřístupnit následující akce:

Název	Popis
vytvořOsobu(Object Osoba)	Vstupem bude kompletně vyplněný objekt osoby dostupnými daty z Idm. (bude třeba zadefinovat povinné atributy). Výstupem volání bude ID osoby.
čtiOsobu(ID)	Vrátí detail osoby včetně vazeb na organizační strukturu (pokud se nevrací reference na osobu v rámci detailu org. jednotky) podle interního ID nebo osobního čísla.
čtiOsoby()	Vrátí kompletní seznam osob (možno stránkovat)
čtiUživatele(ID)	Vrátí detail uživatele podle interního ID včetně vazeb na role (pokud se nevrací reference na uživatele v rámci detailu role)
čtiUživatele()	Vrátí kompletní seznam uživatele (možno stránkovat)
vytvořUživatele(Object Uživatel)	Vstupem je objekt uživatele obsahující veškeré atributy vyplněné. Návratová hodnota bude vytvořený Identifikátor.
smažUživatele(ID)	Vymaže uživatele ze systému.
čtiRoli(ID)	Vrátí detail role.
čtiRole()	Vrátí kompletní seznam rolí systému (možno stránkovat)
čtiPřiřazenéRoleUživateli(ID uživatele)	Vrátí seznam rolí přiřazených uživateli.
přiřaďUživateliRoli (ID uživatele, ID role)	Přiřadí uživateli roli

odeberUživateliRoli **(ID uživatele, ID role)**	Odebere uživateli roli

1.4.2 Notifikace IdM

Při změně atributů (jméno, příjmení a číslo karty) smluvního vztahu bude třeba volat REST/SOAP rozhraní IdM, které bude umožňovat volat přepočítání uživatele.

Pro tyto účely bude vytvořen systémový účet „flux-notifikace" s heslem, které bude nastavené dle dohody.

URL rozhraní bude specifikováno po realizaci testovacího a produkčního prostředí ze strany MHMP.

Klient na straně bude využívat basic autentifikace a bude volat následující, kde osobní číslo bude variabilní parametr:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mod="http://midpoint.evolveum.com/xml/ns/public/model/model-3">
  <soapenv:Header/> <soapenv:Body>
    <mod:executeChanges>
      <mod:deltaList>
        <apit:delta xmlns:apit="http://midpoint.evolveum.com/xml/ns/public/common/api-types-3"
xmlns:ns_xmlns="http://prism.evolveum.com/xml/ns/public/types-3">
          <ns_xmlns:changeType>add</ns_xmlns:changeType>
          <ns_xmlns:objectType xmlns:c="http://midpoint.evolveum.com/xml/ns/public/common/common-
3">c:TaskType</ns_xmlns:objectType>
          <ns_xmlns:objectToAdd xsi:type="c:TaskType" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:c="http://midpoint.evolveum.com/xml/ns/public/common/common-3">
            <c:name>Recompute user x</c:name>
           <extension xsi:type="c:ExtensionType" xmlns:se="http://midpoint.evolveum.com/xml/ns/public/model/scripting/extension-3">
            <se:executeScript xmlns:s="http://midpoint.evolveum.com/xml/ns/public/model/scripting-3">
              <s:search>
                <s:type>c:UserType</s:type>
                <s:searchFilter xmlns:q="http://prism.evolveum.com/xml/ns/public/query-3">
                  <q:and>
                    <q:substring>
                      <q:matching>polyStringNorm</q:matching>
                      <q:path>c:employeeNumber</q:path>
                      <q:value>$OSOBNI_CISLO$</q:value>
                    </q:substring>
                  </q:and>
                </s:searchFilter>
                <s:action>
                  <s:type>recompute</s:type>
                </s:action>
              </s:search>
            </se:executeScript>
           </extension>
                                    <c:ownerRef oid="00000000-0000-0000-0000-000000000002"  type="tns:UserType"
xmlns:tns="http://midpoint.evolveum.com/xml/ns/public/common/common-3"/>
                                   <category>BulkActions</category>
 <handlerUri>http://midpoint.evolveum.com/xml/ns/public/model/scripting/handler-3</handlerUri>
                                   <recurrence>single</recurrence>
                                    <executionStatus>runnable</executionStatus>
          </ns_xmlns:objectToAdd>
        </apit:delta>
      </mod:deltaList>
    </mod:executeChanges>
  </soapenv:Body>
</soapenv:Envelope>
```