***Příloha č. 1 Zadávací dokumentace – Technická specifikace zadavatele***

***Příloha č. 1 Smlouvy o dílo – Technická specifikace zadavatele***

Technická dokumentace

**Implementace opatření v oblasti kybernetické bezpečnosti MěÚ Cheb**

Část 1 – Řízení identit a přístupových oprávnění

# Obsah

[Obsah 2](#_Toc8987294)

[1 Úvod 3](#_Toc8987295)

[1.1 Popis plnění podle této technické dokumentace 3](#_Toc8987296)

[2 Systém správy identit (Identity Management) 4](#_Toc8987297)

[2.1 Obecné požadavky na řešení 4](#_Toc8987298)

[2.2 Funkční požadavky na řešení 5](#_Toc8987299)

[2.3 Požadavky na grafické rozhraní 7](#_Toc8987300)

[2.4 Funkční požadavky na reporty 7](#_Toc8987301)

[2.5 Požadavky na notifikace 7](#_Toc8987302)

[2.6 Požadavky na synchronizaci 8](#_Toc8987303)

[2.7 Požadavku na administraci 8](#_Toc8987304)

[2.8 Požadavky na webové služby 8](#_Toc8987305)

[2.9 Požadavky na logování a logy 9](#_Toc8987306)

[2.10 Integrační vazby 10](#_Toc8987307)

[2.11 Migrace dat 11](#_Toc8987308)

[3 Ověřování identit uživatelů a řízení přístupů k tisku 12](#_Toc8987309)

[3.1 Obecné požadavky na řešení 12](#_Toc8987310)

[3.2 Funkční požadavky na řešení 12](#_Toc8987311)

[4 Dokumentace k dodanému řešení 14](#_Toc8987312)

[4.1 Prováděcí dokumentace 14](#_Toc8987313)

[4.2 Uživatelská dokumentace 14](#_Toc8987314)

[4.3 Administrátorská a systémová dokumentace 14](#_Toc8987315)

[5 Implementace předmětu plnění 16](#_Toc8987316)

[5.1 Instalace SW řešení 16](#_Toc8987317)

[5.2 Implementační služby 16](#_Toc8987318)

[5.3 Zaškolení administrátorů 16](#_Toc8987319)

[5.4 Testovací provoz 17](#_Toc8987320)

[5.5 Akceptační řízení 17](#_Toc8987321)

[6 Harmonogram projektu 18](#_Toc8987322)

[7 Projektové řízení 19](#_Toc8987323)

[Příloha 1 – Popis API rozhraní IS GINIS pro IDM systémy 20](#_Toc8987324)

[Příloha 2 – Struktura nastavení Active Directory 21](#_Toc8987325)

[Příloha 3 – Struktura výměnného souboru XLS pro FLUXPAM5 22](#_Toc8987326)

# Úvod

Tento dokument je technickou specifikací, tedy konkrétním popisem parametrů a vlastností plnění, které jsou předmětem smlouvy o dílo uzavřené na základě veřejné zakázky s názvem „Implementace opatření v oblasti kybernetické bezpečnosti MěÚ Cheb“, část 1 – „Řízení identit a přístupových oprávnění".

## Popis plnění podle této technické dokumentace

Předmět díla, dle smlouvy o dílo a této technické dokumentace, se skládá ze dvou základních částí, u nichž je na straně objednatele požadováno, aby mu byly dodány a nasazeny do jeho prostředí současně, v souladu a společné harmonii. Taký postup je požadován z toho důvodu, že obě oblasti řešení spolu souvisejí a tvoří ucelené bezpečnostní opatření v oblasti řízení identit a přístupových oprávnění.

V případě, že by tyto samostatné oblasti plnění byly dodávány samostatně, a nikoliv jako dílo, které má v prostředí objednatele vzniknout, jednalo by se o roztříštěné plnění, bez benefitů pro objednatele plynoucích z této společné a současné realizace, jíž se objednatel snaží dosáhnout komplexní dodávky, u níž spatřuje zásadní přínos zejména v oblasti řízení identit a přístupových oprávnění.

**Předmětem plnění** této technické dokumentace je dodávka a implementace řešení pro řízení identit a přístupových oprávnění (Identity Management) do informačních systémů a ověřování identit uživatelů v rámci MěÚ Cheb, a to včetně nedílně souvisejících požadavků typu dodání licencí, příslušenství, zaškolení, zpracování dokumentace a poskytování služeb technické podpory.

Předmětem plnění jsou následující činnosti zhotovitele:

* dodávka licencí, implementace, testovací provoz a předání do řádného užívání.

Pro výše uvedený rozsah plnění:

* provedení integrací na další systémy objednatele,
* úprava dodaného řešení dle potřeb a požadavků objednatele,
* zaškolení IT administrátorů,
* provedení testovacího provozu a předání do řádného užívání.

Dále je předmětem plnění dodávka:

* dokumentace k dodanému plnění v požadovaném rozsahu,
* dalších licencí potřebných pro provoz SW komponent,
* listinného potvrzení dodaných licencí co do jejich počtu a rozsahu.

# Systém správy identit (Identity Management)

Dodavatel předmětu plnění provede nasazení sjednocujícího řešení správy identit (Identity Management, dále jen IDM) pro správu identit, uživatelských rolí a oprávnění uživatelů, včetně jejich evidence, v prostředí zadavatele.

IDM bude čerpat základní údaje o identitě z referenčního systému – personálního systému FLUXPAM5. Podle získaných údajů (jméno a příjmení, pracovní pozice, typ pracovního poměru atd.) dojde v IDM na základě přednastavených pravidel k přidělení odpovídajících rolí a následně automaticky nebo po schválení příslušnými osobami (např. vedoucí, personalista atd.) k vytvoření, úpravě, uzamknutí či zrušení uživatelských účtů a nastavení oprávnění v napojených / integrovaných systémech.

## Obecné požadavky na řešení

IDM zajistí centrální správu identit, uživatelských rolí a oprávnění uživatelů v aplikacích a informačních systémech, u kterých bude provedena integrace na takové IDM.

Cílem je zefektivnit a automatizovat proces řízení identit v organizaci zadavatele a zavést centrální platformu pro řízení identit). IDM umožní automatizovaně spravovat identity (osoby, uživatelské role a oprávnění) ve vybraných systémech zadavatele, a to zejména v návaznosti na personální systém a adresářové služby.

Součástí nasazení takového řešení bude i vytvoření systematizovaných pracovních míst, jím odpovídajícím uživatelským rolím a dále skupin takových míst/uživatelských rolí. IDM musí dále umožnit tvorbu a správu hierarchické struktury systematizovaných míst v organizační struktuře zadavatele.

IDM bude mít provedenou vazbu na Jednotný identitní prostor (JIP) a Katalog autentizačních a autorizačních služeb (KAAS) se kterými bude spolupracovat, a to do plného rozsahu těchto IS ve vztahu k povaze objednatele jako orgánu vykonávajícímu přenesenou i samostatnou působnost pro územní samosprávný celek.

Systém IDM bude reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí objednatele a ve vazbě na všechny na IDM napojené informační systémy, ve kterých bude mít daná identita uživatelské role a oprávnění. Takové změny budou reflektovány ve všech napojených informačních systémech vždy v konkrétní rozhodné době.

Ve vztahu k napojeným systémům musí IDM zajistit samostatnou a úplnou správu v oblasti identity a uživatelských rolí ve vztahu k těmto systémům, včetně skupin uživatelů a systematizovaných míst. Ze strany objednatele není rozhodné o kolik politik a konfiguračních operací se na straně informačních systémů jedná, ale je pro něj důležitý výsledek, tedy například správné nastavení uživatelských rolí, zařazení do skupiny a konfigurace oprávnění pro všechny funkcionality Microsoft Active Directory užívané v prostředí objednatele. IDM bude autoritativním zdrojem informací o identitách a jejich účtech a přidělených rolí. IDM bude provádět správu automaticky, tak aby byly spravované systémy vždy aktuální.

IDM a jeho funkcionality musí respektovat standardní architekturu IS v prostředí objednatele a pro svou integraci využít standardizovaná rozhraní a existující prostředky IS.

IDM bude dále realizováno při naplňování nových legislativních požadavků. V případě tohoto plnění zejména s dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tj. IDM zajistí auditní záznamy oprávnění uživatelů a umožní reporting stavu těchto oprávnění.

Integrovaná podpora eIDAS umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit či napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace zadavatele (počet záznamů, velikost databází atd.).

IDM musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent IDM na více serverů – minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.

IDM musí být možné nasadit na více serverů v režimu vysoké dostupnosti.

## Funkční požadavky na řešení

IDM musí udržovat a spravovat kompletní životní cyklus identity. V typovém případě se jedná o příchod zaměstnance, jeho založení, přidělení rolí v informačních systémem dle jeho organizačního zařazení (systematizovaného místa), změna rolí v případě jeho změny jeho zařazení, odchod zaměstnance spočívající v deaktivaci jeho identity. Minimálně se jedná o procesy:

* vznik nové identity,
* nový pracovněprávní vztah,
* úprava identity a pracovněprávního vztahu,
* úpravy popisných atributů, např. jméno,
* úpravy organizačního zařazení,
* změny platnosti,
* automatická změna rolí na základě změny stavu / typu identity, případně jiného příznaku identity,
* změna evidenčního stavu identity,
* ukončení pracovněprávního vztahu,
* aktivace/deaktivace (ruční, automatická).

IDM umožní přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami.

IDM musí detekovat situaci, kdy se v napojeném zdrojovém (personálním) systému vyskytne uživatel, který již byl dříve v IDM založen a přiřadit jej k existující identitě.

IDM umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy.

IDM umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.

IDM umožní přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.

IDM umožní přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.

IDM umožní zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.

IDM umožní přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce.

IDM umožní správu uživatelských rolí, včetně zařazení uživatele do odpovídající role.

IDM umožní dočasné nastavování aplikačních rolí, po uplynutí nastaveného intervalu se role automaticky odebere.

IDM umožní kopírovat role mezi jednotlivými systematizovanými místy.

IDM musí obsahovat funkcionalitu kopírování veškerého nastavení oprávnění jednoho uživatele na druhého.

IDM umožní definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou organizace mohli delegovat v případě potřeby (nemoc, dovolená atd.) svoje role, nebo jejich část na jiné pověřené osoby, a to i tak, že jeden uživatel může mít pro každou svou činnost nastaveného jako zástupce jiného různého uživatele. Delegace oprávnění bude moc být dočasná, kdy se po nastaveném intervalu nastavená delegace automaticky v IDM zruší.

Správa organizační struktury bude možná pro interní i externí identity, a to jako samostatné „větve“ struktury.

IDM zajistí přidávání a správu dalších typů referenčních objektů (min. min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát) a to i v průběhu zakládání či úpravy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity.

IDM zajistí dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci i těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.

Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. IDM provede automatické zneplatnění uložených certifikátů po vypršení data platnosti.

IDM umožní k jednotlivým účtům (identitám) přikládat obrazové soubory (fotografie)

IDM musí obsahovat registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.

IDM musí obsahovat integrovanou správu uživatelských rolí, včetně zařazení uživatele do odpovídající role v napojených IS.

IDM musí obsahovat integrovanou správu samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát.

Integrovaná podpora automatizace – na úrovni intuitivní tvorby pravidel v grafickém prostředí (např. pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů – aplikační role, systematizované místo atd.).

Integrovaná automatizace pro řízení životního cyklu změn identit a schvalování změn musí umožnit minimálně:

* zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným,
* možnost sledování stavu svých požadavků uživateli,
* emailové upozornění schvalovatele na požadavek ke schválen,
* vytvoření a zobrazení přehledu úloh ke schválení pro každého schvalovatele,
* schvalování či zamítnutí požadavků včetně uvedení zdůvodnění,
* vícekrokové schvalování,
* schvalování jedním nebo více schvalovateli (skupinou),
* větvení pro ošetření výjimek vzniklých při schvalování,
* řešení zastupitelnosti,
* eskalace – upozornění při překročení termínu splnění,
* vkládání systémových kroků s voláním webových služeb a spuštěním skriptů,
* pro správce IDM pracovat se všemi úlohami.

Průběh automatizovaných procesů lze sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý jejich stav.

IDM umožní správu evidence osobních údajů, která bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.

IDM bude obsahovat automatizaci (workflow) pro správu životního cyklu osobních údajů subjektu údajů.

IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.

IDM umožní autonomní správu hesel (samoobsluha)., tj. bude obsahovat uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).

IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.

IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.

Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.

IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní, min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.

## Požadavky na grafické rozhraní

IDM musí obsahovat grafické uživatelské rozhraní portálového typu funkční v obvyklých webových prohlížečích (Internet Explorer, Edge, Chrome, Firefox, Safari) bez potřeby instalace doplňku do prohlížeče, které bude sloužit uživatelům pro využívání systému i administrátorů pro jeho správu.

Rozhraní bude implementováno s responzivním designem – přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno (stolní počítač, notebook, tablet).

Zobrazení organizační struktury musí být v přehledné stromové struktuře, s možností vyhledávání identit / uživatelských účtů a seskupování / rozklikávání struktury až do úrovně jednotlivých uživatelských účtů (identit). Musí být možné oddělit jednotlivé stromy identity, např. interní / externí.

Uvedené vyhledávání musí pracovat i bez diakritiky (např. při filtrování slova *zlutoucky* vyhledá i *žluťoučký*)

IDM musí obsahovat integrovaný filtrovací nástroj pro vyhledávání identit a referenčních identit a umožnit (1) filtrování libovolných atributů identity včetně přidružených referenčních objektů a (2) uložení filtrů pro opakované použití.

IDM bude komunikovat v českém jazyce.

## Funkční požadavky na reporty

IDM musí umožňovat generování min. těchto kontrolních reportů:

* zobrazení rolí přidělených k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role,
* souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda a odkud má nějakou roli od někoho delegovánu,
* auditní report – report z údajů o identitách uložených v IDM a to i historických – auditní reporty musí obsahovat souhrnné zobrazení uživatelů (identit) a jejich rolí v systémech napojených na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti, identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.
* souhrnný online přehled o aktuálním stavu hlavních částí systému a případných chybách – chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu automatizovaných úloh,
* zobrazení výpisu napojených informačních systémů (vzájemných vazeb, typů synchronizací apod.). přímo u jednotlivých synchronizovaných IS,

IDM musí umožnit generování výše uvedených reportů ve strojově čitelném formátu (např. v XML).

IDM umožní automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení a stažení.

Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.

## Požadavky na notifikace

IDM zajistí zasílání konfigurovatelných e-mailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.

Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. počet dnů) musí být možno konfigurovat pro každý typ upozornění samostatně.

Systém upozornění bude obsahovat správu šablon. Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.

Pro zasílání jednotlivých typů upozornění bude možno konfigurovat podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Např. notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.

## Požadavky na synchronizaci

IDM umožní obousměrnou synchronizace s napojenými informačními systémy. Podporované typy synchronizací ze strany IDM:

* plná – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému,
* jedna identita – synchronizace vybrané identity bez nutnosti pouštět plnou nebo změnovou synchronizaci,
* změnová – synchronizuje vždy jen změny od poslední spuštěné synchronizace,
* simulační – vytvoří report očekávaných změn v napojeném systému pro provedení skutečné synchronizace.
* porovnávací – vytvoří porovnávací report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM versus nastavení identit a oprávnění přímo v připojeném systému.

Jednotlivé průběhy synchronizací budou logovány.

* Log plné synchronizace musí obsahovat odkazy na objekty, které byly synchronizovány a informace, co bylo u těchto objektů změněno v synchronizovaném systému.
* Log změnové synchronizace musí obsahovat informace o události, která změnovou synchronizaci vyvolala + informace požadované v logu plné synchronizace.

## Požadavku na administraci

Po přihlášení do IDM bude administrátor IDM notifikován v případě, že v systému došlo k chybovému stavu. Tato notifikace musí být zřetelná po přihlášení do systému a může být formou (barevného podbarvení části aplikace např. menu, pop-up okna oznamující, že je v IDM nějaký chybový stav, centrální dashboard aplikace apod.). Z notifikace musí být zřetelné, která funkcionalita nebo část IDM je chybovém stavu.

Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity atd.)

Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů.

Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikace, synchronizace, konfigurace systému, reporty, automatizace, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.

Pro identity a referenční objekty bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.

Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky.

Integrovaný ochranný mechanismus zabránění hromadným změnám např. z důvodu chybných dat na vstupu, aby nedošlo k hromadným nežádoucím změnám (např. smazání objektů v Active Directory). Tato funkcionalita umožní při větším počtu změn zastavit frontu změn a upozornit administrátora IDM emailem a zapsat tuto informaci do logu IDM. Tato vlastnost je požadována pro všechny vstupně/výstupní integrační rozhraní.

Integrovaná správa synchronizací včetně nastavení připojení na synchronizované systémy, nastavení typu synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění.

## Požadavky na webové služby

IDM musí poskytovat rozhraní webových služeb pro programové napojení dalších systémů. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům IT technologií do prostředí objednatele za účelem napojení se na takové rozhraní.

Webové služby budou definované v rozšířeném standardu WSDL a podporovat SOAP protokol. Součástí dokumentace bude proto i popis řešení webových služeb v podobě XSD. Rozhraní webových služeb a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné jen se zapojením administrátora objednatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS (tedy bez nutného zapojení nebo součinnosti dodavatele IDM).

Základní konfigurace přístupu k webovým službám musí být dostupná z grafického rozhraní IDM.

Rozhraní IDM musí poskytovat minimálně následující služby:

* získání organizační struktury
* získání hierarchie systematizovaných míst,
* získání seznamu identit,
* získání nadřízené osoby pro daného zaměstnance,
* získání seznamu rolí pro daného zaměstnance, včetně případné informaci o delegaci role,
* získání seznamu uživatelů dané aplikace,
* získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci
* zápis seznamu rolí uživatele do IDM,
* zápis certifikátů do IDM
* zápis a změna identit

Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.

## Požadavky na logování a logy

Řešení musí umožňovat publikovat kopie logů do externího systému určeného pro sběr logů typu Security Information and Event Management, log manažer atd.

Systém bude obsahovat logování min. následujících typů událostí:

* události systému (aplikační log),
* změny entit evidovaných systémem a změny konfigurace systému (auditní log),
* synchronizace s napojenými systémy (synchronizační log) včetně volání webových služeb,
* odeslané notifikace a upozornění (notifikační log).

Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.

Pro zajištění důvěryhodnosti logů bude možné veškeré požadavky na změny v IDM zadávat výhradně prostřednictvím uživatelského nebo administrátorského rozhraní. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.

Veškeré komponenty/ moduly dodaného řešení IDM musí vést a umožňovat jednoduchý export anonymizovaných logů o počtu užití těchto jednotlivých komponent / modulů.

Tyto logy musejí být přehledné a oproštěné od osobních dat, aby umožnily jednoduchou kontrolu užívání těchto nových modulů ze strany i například kontrolních orgánů včetně oblasti kofinancování IROP.

## Integrační vazby

Součástí předmětné části plnění je provedení napojení na následující informační systémy a aplikace způsobem, kdy IDM převezme správu identit a řízení uživatelských rolí v těchto informačních systémech a aplikacích objednatele za využití odpovídajících standardizovaných rozhraní těchto systémů:

| Informační systém / aplikace | Popis způsobu napojení a komunikace |
| --- | --- |
| Active Directory  (MICROSOFT s.r.o.) | IDM bude napojen na Active Directory, tj. na stávající implementované adresářové služby LDAP. Popis komunikace systému je dostupný neomezeným dálkovým způsobem viz URL: <https://docs.microsoft.com/cs-cz/>  Struktura stávajícího nastavení Active Directory je uvedena v příloze číslo 2 tohoto dokumentu. |
| Emailový server Exchange  (MICROSOFT s.r.o.) | IDM bude napojen na stávající emailový server Microsoft Exchange 2010, v rámci kterého bude automaticky spravovat mailové schránky uživatelů a zařazení těchto uživatelů do komunikačních skupin. Popis komunikace systému je dostupný neomezeným dálkovým způsobem viz URL <https://docs.microsoft.com/en-us/exchange/> |
| Personální a mzdový systém FLUXPAM5  (FLUX, spol. s r.o.) | IDM bude napojen na stávající personální systém FLUXPAM5. Personální systém bude sloužit jako primární zdrojový systém identit MěÚ Cheb. FLUXPAM5 umožňuje komunikaci prostřednictvím webových služeb s předáváním souborů ve formátu XML a dále také exportem XML souboru a jeho uložením do filesystému (export na vyžádání nebo při změně v personálním systému).  Předpokládaná struktura výměnného souboru XML z FLUXPAM5 je uvedena v příloze číslo 3 tohoto dokumentu (v této struktuře je aktuálně realizováno propojení FLUXPAM do EOS4). |
| EOS4 – evidence organizační struktury  (MARBES Consulting s.r.o.) | IDM bude napojen na stávající systém EOS4. Ten umožňuje komunikaci prostřednictvím webových služeb, datové rozhraní aplikace EOS4 je vystavěno na protokolu SOAP, veškeré vstupní a výstupní soubory rozhraní SOAP podléhají WSDL. Dostupné jsou následující webové služby:   * pro čtení/zápis informací o aplikacích, * pro čtení informací o atributech, * pro práci s kontakty, * pro čtení informací o struktuře organizačních rolí, * pro čtení/zápis organizační struktury, * pro čtení činností.   Základní popis EOS4 je dostupný neomezeným dálkovým způsobem viz URL:  https://www.marbes.cz/ostatni-agendy/identitni-system  Konkrétní popis webových služeb bude pro implementaci řešení IDM dodavateli zpřístupněn. |
| IS GINIS – ekonomické a majetkové agendy  (GORDIC spol. s r.o.) | IDM bude napojen na stávající systém ekonomických a majetkových agendy GINIS. Systém obsahuje vlastní komplexní integrační platformu určenou pro realizaci propojení různých SW systémů do spolupracujícího celku – platforma umožňuje komunikaci prostřednictvím webových služeb  Popis rozhraní GINIS je uveden v příloze číslo 1 tohoto dokumentu. |
| Evidence správních řízení ESPI9  (INISOFT s.r.o.) | Systém Evidence správních řízení je vybavena vlastním modulem „Modul Active Directory ESPI 9“, který umožňuje napojení na Active Directory a na externí systém IDM a umožní následnou správu uživatelů a jejich účtů. Napojení je umožněno prostřednictvím webových služeb nad protokolem SOAP. IDM bude napojen přímo na systém ESPI9. Popis komunikace systému je dostupný neomezeným dálkovým způsobem viz URL:  <https://confluence.inisoft.cz/display/KBxSPRAVA/Modul+Active+Directory+ESPI+9>  Konkrétní popis webových služeb bude pro implementaci řešení IDM dodavateli zpřístupněn. |

Veškeré případné náklady spočívající v konfiguraci, testování nebo nezbytných úpravách informačních systémů uvedených výše a dodaných třetí stranou, které je potřeba provést za účelem integrace těchto systémů na nově dodané IDM ze strany dodavatelů těchto systémů ponese objednatel samostatně mimo tento předmět plnění.

Dodané řešení ID musí obsahovat následující vestavěné obecné komunikační moduly (konektory) pro správu identit v napojovaných systémech:

* konektor pro spouštění CMD příkazů,
* konektor pro práci s CSV soubory,
* konektor pro práci s databázi Microsoft SQL,
* konektor pro napojení na SOAP webové služby,
* konektor pro napojení na REST webové služby,
* konektor pro napojení na LDAP server s podporou LDAP v3.

Dodavatel do nabídky uvede, na jaký počet informačních systémů veřejné správy a na jaké (např. JIP, KAAS, ISZR atd.) má pro dodávané řešení IDM provedeny integrace a nabízí je.

## Migrace dat

Pro úvodní naplnění dojde k úvodnímu převzetí organizační struktury z personalistiky FLUXPAM5, která do budoucna zůstane výhradním zdrojem organizační struktury a dále i zdrojem informací o uživatelských účtech zejména v podobě založení, změna pracovního zařazení uživatele a vyřazení uživatele z organizace.

Nad výše uvedenou strukturou a základní skladbou uživatelů v organizaci objednatele provede zhotovitel analýzu struktury uživatelských účtů v jednotlivých dalších informačních systémech, u kterých je požadována integrace výše a to za plné součinnosti objednatele, ve vztahu k těmto IS třetích stran, u kterých potřebné informaci zajistí objednatel.

Na základě odsouhlasení výsledku analýzy a způsobu provedení správy uživatelských účtů v těchto systémech, uživatelských rolích a jednotlivých oprávněních bude moci dojít k implementaci řešení i ve vazbě na tyto informační systémy.

# Ověřování identit uživatelů a řízení přístupů k tisku

Pro zajištění tiskových služeb (tisku výstupů z agendových a provozních systémů) zadavatel využívá skupinové multifunkční stroje – tiskárny s integrovaným skenerem v celkovém počtu 11 ks ve složení:

* 6× Canon iR-ADV C3325
* 2× Canon iR-ADV 4225
* 1× Konica Minolta Bizhub C360
* 1× Canon C2225i
* 1× Xerox WorkCenter 5325

Uvedená zařízení jsou umístěna ve společných prostorech (tzv. technologické místnosti MěÚ Cheb). Po odeslání tiskové úlohy uživatelé musí k tiskárně dojít a vyzvednout si vytištěné dokumenty. Mezi vytištěním a vyzvednutím dokumentů nejsou vytištěné dokumenty nijak zabezpečeny (mohou obsahovat citlivé či osobní informace) a může tak dojít k jejich kompromitaci – neoprávněnému přečtení, odcizení nebo záměně.

## Obecné požadavky na řešení

V rámci předmětu plnění dodavatel zavede a nasadí **systém pro ověřování identity uživatelů a řízení tisku**, tj. systém, který umožní správu a monitorování tiskových a multifunkčních zařízení s ověřováním uživatelů a řízením jejich přístupu k tiskovým úlohám.

Pro identifikaci uživatelů budou multifunkční zařízení doplněna autentizačními terminály s vestavěným čtečkami bezkontaktních karet standardu EM-Marine (těmito kartami jsou již zaměstnanci MěÚ Cheb vybaveni).

Čtečky budou prostřednictvím vnitřní sítě MěÚ komunikovat se systémem pro ověřování identity uživatelů a řízení tisku, který zajistí ověření identity uživatele vůči adresářové službě Active Directory a následně jeho autorizaci (přidělení příslušných oprávnění) a v případě úspěchu uvolní tiskovou úlohu k vytištění na tiskárně, u které se uživatel kartou přihlásí. Na všechny HW komponenty, které jsou součástí řešení je požadován nárok na nejnovější firmware a bezpečnostní aktualizace výrobce po dobu 2 let (bude uhrazeno současně a v rámci ceny díla).

## Funkční požadavky na řešení

Systém pro ověřování identity uživatelů a řízení tisku

Řešení jako celek musí splňovat následující minimální funkční parametry:

|  |  |
| --- | --- |
| Provedení | Systém pro správu a monitorování tiskových a multifunkčních zařízení s ověřováním uživatelů a řízením přístupů |
| Centrální správa zařízení | Integrovaná centrální správa síťových tiskových a multifukčních zařízení |
| Nová zařízení | Automatické vyhledání nových zařízení |
| Ovladače | Automatická instalace tiskových ovladačů |
| Monitorování | Monitorování lokálních tiskáren i síťových zařízení |
| Instalace | Vzdálená instalace a konfigurace tiskáren a zařízení |
| Správa | Podpora SNMP v1, v2 a v3 |
| Personifikace | Podpora individuálních skenovacích formulářů a profilů, individuální tisková fronta, skenování do osobní složky a osobního e-mailu, účtování soukromého tisku |
| Podpora úložišť | Skenování do cloudových úložišť, min. Onedrive a Onedrive for Business, Google Drive a Dropbox |
| Rozpoznávání textu | Podpora OCR (rozpoznání textu) při skenování |
| Tiskové úlohy | Integrovaná správa tiskových úloh |
| Reporty | Integrovaný reportovací systém |
| Adresářové služby | Podpora adresářových služeb - min. LDAP, Active Directory |
| Pokročilý tisk | Zabezpečený tisk (po ověření uživatele), tandemový tisk, delegovaný tisk, odložený tisk, modifikace parametrů tiskových úloh |
| Náhledy | Náhledy tiskových úloh |
| Kompatibilita | S nabízenými terminály pro ověřování uživatelů |
| Vysoká dostupnost | Podpora běhu v clusterovém režimu pro vysokou dostupnost služeb |
| Mobilní zařízení | Podpora tisku z tabletů a chytrých telefonů, aplikace pro Android a IOS |
| Účtování | Podrobné účtování uživatelů a jejich úloh |
| Podpora QR | Podpora přihlášení QR kódem |
| Monitorování zařízení | Monitorování síťových zařízení, výstrah a hlášení |
| Rozhraní | Webové rozhraní pro správu a obsluhu |
| Automatizace | Integrovaná podpora skriptování a workflow |

11× Terminál k multifunkčním zařízením

Zařízení musí splňovat následující minimální funkční parametry:

|  |  |
| --- | --- |
| Základní funkce | Autorizační a ovládací terminál k tiskovému a multifukčnímu zařízení |
| Provedení | Externí dotykový barevný displej min. 7" |
| Ověřování uživatelů | Podpora ověřování uživatelů bezkontaktními kartami |
| Funkce | Řízení a správa tiskových a skenovacích úloh ověřenými uživateli |
| Příslušenství | Včetně montážního materiálu, držáků a propojovacích kabelů |
| Skenování | Podpora řízení skenerů, pokud multifunkční zařízení umožňuje |
| Podporovaná - řízená zařízení | 1× Konica Minolta Bizhub C360 6× Canon iR-ADV C3325 2× Canon iR-ADV 4225 1×  Canon C2225i 1× Xerox WorkCenter 5325 |

11× Čtečka k terminálům

Zařízení musí splňovat následující minimální funkční parametry:

| Základní funkce | Čtečka k nabízeným terminálům pro bezkontaktní karty EM-Marine 125 kHz |
| --- | --- |

# Dokumentace k dodanému řešení

## Prováděcí dokumentace

Objednatel požaduje v rámci plnění zpracování tzv. prováděcí dokumentace (někdy také analogicky nazýváno jako cílový koncept nebo implementační analýza).

Zhotovitel zpracuje komplexní a detailní řešení nasazení díla, a to ve vazbě na požadavky uvedené v této technické dokumentaci a smlouvě o dílo jako jednotlivé části díla a na jejich hlavní funkcionality. Cílem je zpracování dokumentu v takové míře detailu jednotlivých postupů a prací zasazení do prostředí a jeho nastavení, která umožní dosažení zavedení řešení do rutinního provozu řízenou formou. Dokument proto bude jednoznačně a jasně konkretizovat jednotlivé kroky prací a to min. v rozsahu, které kroky a jakým způsobem budou řešeny, kým budou řešeny, za jaké součinnosti objednatele a v jakém čase. Taková konkretizace bude dále dodržovat časovou, věcnou a logickou souslednost a bude z ní tedy možné v každém okamžiku realizace jednotlivých částí díla určit co je právě realizováno a v jakém stavu a co bude následovat. Objednatel bude moci na základě takových podkladů alokovat své potřebné kapacity na součinnost a průběžnou kontrolu plnění díla. Bez odsouhlasené prováděcí dokumentace ze strany objednatele, tedy shody objednatele a zhotovitele na způsobu a formě nasazení jednotlivých částí díla nebude moci být započata implementace. Dokument bude dále konkretizovat minimálně tyto oblasti:

* návrh designu – architektura technického řešení,
* detailní harmonogram realizace včetně uvedení kritických milníků,
* požadované součinnosti zadavatele a jejich rozsah,
* vazby na stávající systémy a jejich konfigurace,
* popis způsobu provedení napojení okolních informačních systémů a aplikací – návrh technického řešení vazeb (vazby mezi subsystémy, vazby s vybranými aplikacemi objednatele),
* pro řešení správy identit (Identity Management)
  + revize způsobu a stavu současného nastavení uživatelských oprávnění v napojovaných systémech,
  + návrh na možné změny v nastavení uživatelských oprávnění,
* návrh akceptačních kritérií a akceptačních testů.

Prováděcí dokumentace bude připomínkována objednatelem a připomínky budou ze strany zhotovitele vypořádány (tj. zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany objednatele nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na zhotoviteli jejich řádné zhojení. Na základě provedené implementace bude prováděcí dokumentace aktualizována na skutečně provedenou konfigurace a to jak funkční, tak provedené nastavení včetně podložení provedenými analytickými podklady a dokumenty.

Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

## Uživatelská dokumentace

Zhotovitel dodá uživatelskou dokumentaci, která bude obsahovat minimálně základní popis práce s dodaným řešením, dále bude popisovat funkcionality řešení, a to pro potřebu řádné orientace a práce uživatele.

Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

## Administrátorská a systémová dokumentace

Zhotovitel dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat detailní popis správy a údržby dodaného řešení.

Zhotovitel dodá systémovou dokumentaci pro objednatele, která bude obsahovat následující:

* součástí plnění bude dále i navržení či úprava metodiky pro správu identit
* jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů),
* mechanismu práce s hesly (přidělení, změna, samoobslužný reset),
* postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění),
* návrh členění objektů v rámci IDM (osoby, účty, funkce, organizační jednotky, skupiny),
* definice bezpečnostních zásad a pravidel pro práci s IDM,
* popis rozhraní IDM, kdy tato dokumentace bude určena k přímému poskytnutí dalším dodavatelům IT technologií do prostředí zadavatele za účelem napojení se na takové rozhraní.

Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

# Implementace předmětu plnění

## Instalace SW řešení

Pro potřebu nasazení a provozu dodávaného řešení budou zhotoviteli poskytnuty systémové prostředky ze strany objednatele.

Veškerá nabízená softwarová řešení musí být provozovány v současném prostředí serverové virtualizace MěÚ Cheb na stávající platformě Hyper-V. Objednatel poskytne potřebný počet licencí Windows Server 2016 a sdílený Microsoft SQL 2016 Standard (tento musí dodavatel využít, vyžaduje-li jeho řešení databázovou platformu Microsoft SQL Standard) a odpovídající systémové prostředky (v rozsahu max. 8 vCPU, 64 GB RAM a 1 TB HDD).

Výše uvedené systémové prostředky budou alokovány po dobu min. 5 let, kdy musí zhotovitel garantovat, že budou po celou uvedenou dobu naprosto dostatečné, tedy, že za účelem optimálního běhu řešení nebude minimálně po tuto dobu zhotovitel po objednateli požadovat navýšení takových systémových prostředků.

V případě, že se zhotovitel rozhodne neužít nabízenou licenci operačního a databázového systému, musí v rámci své dodávky dodat i odpovídají licence operačního a databázového systému k provozu nad virtualizovanou platformou objednatele. Veškeré další potřebné licence software potřebného pro běh předmětu plnění musí v rámci své dodávky zajistit zhotovitel.

## Implementační služby

Dodavatel v rámci předmětu plnění provede následující implementační služby:

|  |
| --- |
| instalace a konfigurace systému IDM,  převzetí konfigurací identity a uživatelských rolí ze současných informačních systémů,  sjednocení identit napříč napojenými informačními systémy v IDM,  vytvoření systematizovaných míst a organizační struktury identit a uživatelských rolí v organizaci objednatele, |
| přípravu kabelových rozvodů pro dodávané technologie (ověřování identity uživatelů a řízení tisku) dle specifikace:   * max. 10 m Cat včetně lištování pro každý terminál,   instalaci autentizačních terminálů k multifunkčním zařízením a čteček (pro 11 multifunkčních zařízení),  napojení autentizačních terminálů k multifunkčním zařízením a čteček na datové rozvody,  konfiguraci všech autentizačních terminálů a čteček,  instalaci a konfigurace SW pro ověřování identity uživatelů a řízení tisku (systém pro správu a monitorování tiskových a multifunkčních zařízení s ověřováním uživatelů a řízením přístupů), a to včetně napojení na Active Directory, terminály, tisková a multifunkční zařízení a nastavení tiskových front, |
| ověření funkčnosti díla formou testovacího provozu,  provedení akceptačních testů včetně výkonových testů. |

## Zaškolení administrátorů

Zhotovitel zrealizuje v sídle objednatele prezenční zaškolení pro IT administrátory objednatele minimálně v rozsahu provozní dokumentace. Školení bude pokrývat všechny komponenty dodávané v rámci předmětu plnění, a to minimálně v rozsahu:

* běžných administrátorských činností pro implementované systémy,
* standardní údržby systémů pro administrátory zadavatele
* základní identifikace nestandardních stavů systému a jejich příčin.

Minimální požadovaný rozsah zaškolení pro administrátory je 12 hodin, z toho min. 8 hodin pro oblast systému správy identit (Identity Management).

Předpokládaný počet administrátorů (účastníků školení) je max. 7 osob.

Objednatel pro účely zaškolení zajistí a zpřístupní učebnu vybavenou notebooky, prezentační technikou (ve smyslu projektor, tabule pro psaní / kreslení) a dále zajistí konektivitu do vnitřní sítě objednatele.

## Testovací provoz

Testovací provoz proběhne po dobu uvedenou v harmonogramu realizace, a to se zvýšeným dohledem a podporou ze strany zhotovitele.

Cílem testovacího provozu je poskytnout metodické vedení a prostor uživatelům pro ověření funkcionalit a vlastní funkčnosti dodaného řešení, pro cvičnou práci se systémem a prostor pro zhotovitele pro identifikaci a opravu případných chyb a neshod. Dalším cílem testovacího provozu je možnost případné definice změnových požadavků ze strany objednatele. Během testovacího provozu provede zhotovitel aktualizaci prováděcí dokumentace. Úspěšný průběh testovacího provozu, jehož výstupem bude faktické uživatelské ověření schopnosti nasazení nového řešení v prostředí objednatele na základě této technické dokumentace a jejich příloh, je jednou z nezbytných podmínek objednatele pro možnost akceptace plnění na základě této technické dokumentace a jejích příloh.

## Akceptační řízení

### Dílčí akceptační řízení

Dílčí akceptační řízení bude provedeno pro milník 1 a 2 vyznačený v harmonogramu projektu dle této technické dokumentace. Dílčí akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům této technické dokumentace a jejím přílohám (milník číslo 1 a 2) a požadavků daných prováděcí dokumentací (milník číslo 2).

Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno nebo Nesplněno, podepsaný oprávněnými osobami smluvních stran.

Součástí akceptačního protokolu ke každému milníku plnění částí díla bude i uvedení jednotlivých částí díla a stavu a konkrétních výhrad nebo souladu pro každou část díla samostatně.

Započetí dalších prací spadajících pod milník následující je možné pouze za předpokladu, že bude provedena akceptace s výsledkem Splněno všech milníků předcházejících.

### Souhrnné akceptační řízení – akceptace díla

Souhrnné akceptační řízení bude zahrnovat:

* ověření splnění akceptace všech milníků u všech částí díla, které akceptaci plnění předcházely,
* porovnání skutečného stavu vůči požadavkům smlouvy o dílo a této technické dokumentace, která je její přílohou, a jejích příloh, funkčního i nefunkčního charakteru – licence a příslušenství.

Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno / Splněno s výhradou / Nesplněno, podepsaný oprávněnými osobami smluvních stran a to s výsledným uvedením každé části díla na tomto akceptačním protokolu a výsledku akceptačního řízení. Klasifikace Splněno s výhradou umožní pokračování v realizaci díla v případě vad drobných, pro které může být opakování akceptačního řízení zbytečně nákladné.

### Opakované akceptační řízení

Jestliže plnění nesplňuje podmínky stanovené pro akceptaci, bude obsahem akceptačního protokolu vyjádření Nesplněno spolu s popisem závad a uvedením termínů pro jejich nápravu. Zhotovitel napraví tyto nedostatky a akceptační řízení v odpovídajícím rozsahu bude provedeno znovu. Proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně. Proces testování a následných oprav lze opakovat, dokud zhotovitel nesplní požadavky pro akceptaci řádnou s výsledkem Splněno, nejvýše však 2× (dvakrát). V situaci, kdy by bylo nutné opakovat akceptační řízení více jak 2× (dvakrát) pro konkrétní milník projektu nebo celé plnění, bude takové opakování považováno za podstatné porušení smlouvy ze strany zhotovitele a objednatel bude oprávněn odstoupit od smlouvy o dílo. Prodlení vzniklé v souvislosti s potřebou opakování akceptačních řízení bude považováno vždy za prodlení vzniklé na straně zhotovitele se zachováním důsledků takového prodlení, tedy zejména smluvních pokut na základě uvařené smlouvy o dílo. Opakované akceptační řízení bude probíhat jednotlivě samostatně pro jednotlivé části díla tak, aby na již akceptované části díla dané opakované akceptační řízení nemělo vliv.

# Harmonogram projektu

Objednatel požaduje realizaci předmětu plnění dle následujícího harmonogramu. Harmonogram je sestaven tak, aby jednotlivé práce na sebe logicky navazovaly a zároveň byl v souladu s požadavky výzvy číslo 10 IROP, ze které má být předmět plnění spolufinancován (s ohledem na termín dokončení předmětu plnění).

S ohledem na možnost kontroly realizace díla z pohledu času (tj. dílčí vyhodnocování dodržování harmonogramu realizace) je harmonogram doplněn milníky. Započetí každého milníku je možné pouze za předpokladu, že bude provedena akceptace všech milníků předcházejících.

|  |  |
| --- | --- |
| Aktivita projektu | Termín nejpozději do: |
| Zpracování prováděcí dokumentace, připomínkování ze strany objednatele, vypořádání připomínek, finalizace dokumentu. | 4 týdny |
| Akceptační řízení pro Milník 1. | 1 |
| **Milník číslo 1** – Předání prováděcí dokumentace. | T + 5 týdnů |
| Instalace dodávaného řešení. Konfigurace dodaného řešení pro potřeby objednatele – nastavení / konfigurace / parametrizace jednotlivých oblastí, provedení integrací na spolupracující systémy, nastavení přístupových oprávnění. | 4 týdny |
| Akceptační řízení pro Milník 2. | 1 týden |
| **Milník číslo 2** – Připravené prostředí pro testovací provoz, předání do testovacího provozu. | T + 10 týdnů |
| Zaškolení IT administrátorů.  Zpracování a dodávka dokumentace (uživatelská, administrátorská a systémová).  Testovací provoz s dohledem a podporou zhotovitele.  Oprava chyb a neshod, případná definice změnových požadavků.  Dodávka licencí (listinné potvrzení dodaných licencí co do jejich počtu a rozsahu).  Akceptační řízení – porovnání skutečných vlastností se požadavky smlouvy. | 3 týdny |
| **Milník číslo 3** – Akceptace projektu, předání systému do rutinního provozu. | T + 13 týdnů |

# Projektové řízení

Jako součástí plnění jsou požadovány pravidelné projektové schůzky v sídle objednatele min. 1× každých 14 kalendářních dní a dále ad-hoc pracovní schůzky k problematice řešení jednotlivých částí díla, včetně projednání a odsouhlasení výstupů pro konfiguraci a nastavení jednotlivých částí díla pro potřebu objednatele.

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti objednatele je v rámci předmětu plnění objednatelem požadováno aplikování základních principů projektového řízení ze strany zhotovitele. Jedná se zejména o řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na:

* věcné plnění – rozsah, posloupnost a hloubku projektových prací,
* závazný harmonogram projektu – dodržování termínů v harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem k objednateli, aktivní řešení výše uvedených nestandardních situací).

Dále se jedná o zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů ze všech konzultačních a projektových schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých způsobů řešení dílčích částí projektu atd.). Uvedené zápisy budou zpracovány během schůzek a jednání, případně budou zpracovány a předány objednateli nejpozději do dvou pracovních dnů po těchto jednáních.

# Příloha 1 – Popis API rozhraní IS GINIS pro IDM systémy

Příloha je tvořena souborem „Popis API rozhraní IS GINIS pro IDM systémy.PDF“

# Příloha 2 – Struktura nastavení Active Directory

|  |  |
| --- | --- |
| Doména | mestocheb.cz |
| Cesta ke skupinám | OU=Globalni,OU=Skupiny,DC=mestocheb,DC=cz |
| Cesta pro vyhledávání uživatelů NsP | OU=Město Cheb,OU=Uzivatele,DC=mestocheb,DC=cz |
| Security group název | Popis |
| Mestska\_policie\_G | Městská policie |
| MP\_stala\_sluzba\_G | Stálá služba městské policie |
| Odbor\_financni\_G | odbor finanční |
| Odbor\_informatiky\_G | odbor informatiky |
| Odbor\_investicni\_G | odbor investiční |
| Odbor\_kancelare\_starosty\_G | odbor kanceláře starosty |
| Odbor\_majetkopravni\_G | odbor majetkoprávní |
| Odbor\_organizacni\_G | odbor organizační |
| Odbor\_projektoveho\_managementu\_a\_rozvoje\_G | odbor projektového managementu a rozvoje |
| Odbor\_skolstvi\_telovychovy\_a\_kultury\_G | odbor školství a kultury |
| Odbor\_socialnich\_veci\_a\_zdravotnictvi\_G | odbor sociálních věcí a zdravotnictví |
| Odbor\_spravnich\_cinnosti\_a\_obecni\_zivnostensky\_urad\_G | odbor správních činností a obecní živnostenský úřad |
| Odbor\_spravy\_majetku\_G | odbor správy majetku |
| Odbor\_stavebni\_a\_zivotniho\_prostredi\_G | odbor stavební a životního prostředí |
| Oddeleni\_kultury\_a\_cestovního\_ruchu\_G | oddělení kultury a cestovního ruchu |
| Oddeleni\_obecni\_zivnostensky\_urad\_G | oddělení obecní živnostenský úřad |
| Oddeleni\_pravni\_G | oddělení právní |
| Oddeleni\_registru\_vozidel\_a\_ridicu\_G | oddělení registru vozidel a řidičů |
| Oddeleni\_socialne-pravni\_ochrany\_deti\_G | oddělení sociálně-právní ochrany dětí |
| Oddeleni\_spravnich\_agend\_G | oddělení správních agend |
| Oddeleni\_spravnich\_deliktu\_G | oddělení správních deliktů |
| Oddeleni\_spravy\_budov\_G | oddělení správy budov |
| Oddeleni\_zivotniho\_prostredi\_G | oddělení životního prostředí |
| Uzivatele\_G | všichni uživatelé |
| Vedeni\_G | vedení |
| Vedouci\_odboru\_G | vedoucí odborů |

# Příloha 3 – Struktura výměnného souboru XLS pro FLUXPAM5

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<xs:schema version="1.0" targetNamespace="http://ws.v1\_0\_0.eos4.marbes.cz" xmlns:tns="http://ws.v1\_0\_0.eos4.marbes.cz" xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="interface" type="tns:interface"/>

<xs:complexType name="interface">

<xs:sequence>

<xs:element name="configuration" type="tns:configuration"/>

<xs:element name="org-structure" type="tns:org-structure"/>

<xs:element name="persons" type="tns:person-list" minOccurs="0"/>

<xs:element name="role-connections" type="tns:role-connection-list" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="configuration">

<xs:sequence>

<xs:element name="global-configuration" type="tns:global-configuration"/>

<xs:element name="org-role-configuration" type="tns:org-role-process-configuration" minOccurs="0"/>

<xs:element name="org-unit-configuration" type="tns:entity-process-configuration" minOccurs="0"/>

<xs:element name="person-assignment-configuration" type="tns:entity-process-configuration" minOccurs="0"/>

<xs:element name="person-configuration" type="tns:entity-process-configuration" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="global-configuration">

<xs:sequence>

<xs:element name="debug" type="xs:boolean" default="false" minOccurs="0"/>

<xs:element name="create-time" type="xs:dateTime"/>

<xs:element name="external-system" type="xs:string"/>

<xs:element name="sync-mode" type="tns:synchronization-mode"/>

<xs:element name="root-id" type="xs:string" minOccurs="0"/>

<xs:element name="rootUnitsImport" type="xs:boolean" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="org-role-process-configuration">

<xs:complexContent>

<xs:extension base="tns:entity-process-configuration">

<xs:sequence>

<xs:element name="org-role-tree-type" type="tns:org-role-tree-type"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="entity-process-configuration">

<xs:sequence>

<xs:element name="pairing-mode" type="tns:pairing-mode" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="org-structure">

<xs:sequence>

<xs:element name="person-assignments" type="tns:person-unit-assignment-list" minOccurs="0"/>

<xs:element name="org-roles" type="tns:org-role-list" minOccurs="0"/>

<xs:element name="org-units" type="tns:org-unit-list" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="person-unit-assignment-list">

<xs:sequence>

<xs:element name="person-assignment" type="tns:person-unit-assignment" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="person-unit-assignment">

<xs:sequence>

<xs:element name="person-id" type="xs:string"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="org-role-list">

<xs:sequence>

<xs:element name="role" type="tns:org-role" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="org-role">

<xs:complexContent>

<xs:extension base="tns:extern-entity">

<xs:sequence>

<xs:element name="alt-name" type="xs:string" minOccurs="0"/>

<xs:element name="person-assignments" type="tns:person-assignment-list" minOccurs="0"/>

<xs:element name="code" type="xs:string" minOccurs="0"/>

<xs:element name="master" type="xs:boolean" minOccurs="0"/>

<xs:element name="name" type="xs:string"/>

<xs:element name="sentence" type="xs:int" minOccurs="0"/>

<xs:element name="type-code" type="xs:string" minOccurs="0"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="extern-entity" abstract="true">

<xs:complexContent>

<xs:extension base="tns:simple-extern-entity">

<xs:sequence>

<xs:element name="building-info" type="tns:building-info" minOccurs="0"/>

<xs:element name="phones" type="tns:phones" minOccurs="0"/>

<xs:element name="user-fields" type="tns:user-fields" minOccurs="0"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="simple-extern-entity" abstract="true">

<xs:sequence>

<xs:element name="eos-identifier" type="xs:string" minOccurs="0"/>

<xs:element name="external-id" type="xs:string"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="person-assignment-list">

<xs:sequence>

<xs:element name="person-assignment" type="tns:person-assignment" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="person-assignment">

<xs:complexContent>

<xs:extension base="tns:simple-extern-entity">

<xs:sequence>

<xs:element name="date-end" type="xs:dateTime" minOccurs="0"/>

<xs:element name="connection-factor" type="xs:int"/>

<xs:element name="date-start" type="xs:dateTime" minOccurs="0"/>

<xs:element name="person-id" type="xs:string"/>

<xs:element name="personal-factor" type="xs:int"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="building-info">

<xs:sequence>

<xs:element name="name" type="xs:string" minOccurs="0"/>

<xs:element name="floor" type="xs:string" minOccurs="0"/>

<xs:element name="room" type="xs:string" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="phones">

<xs:sequence>

<xs:element name="phone" type="tns:phone" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="phone">

<xs:sequence>

<xs:element name="description" type="xs:string" minOccurs="0"/>

<xs:element name="extension" type="xs:string" minOccurs="0"/>

<xs:element name="number" type="xs:string"/>

<xs:element name="prefix" type="xs:string" minOccurs="0"/>

<xs:element name="type" type="tns:phone-type"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="user-fields">

<xs:sequence>

<xs:element name="field" type="tns:user-field" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="user-field">

<xs:sequence>

<xs:element name="code" type="xs:string"/>

<xs:element name="value" type="xs:string"/>

<xs:element name="name" type="xs:string"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="org-unit-list">

<xs:sequence>

<xs:element name="unit" type="tns:org-unit" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="org-unit">

<xs:complexContent>

<xs:extension base="tns:extern-entity">

<xs:sequence>

<xs:element name="abbrev" type="xs:string" minOccurs="0"/>

<xs:element name="alt-name" type="xs:string" minOccurs="0"/>

<xs:element name="person-assignments" type="tns:person-unit-assignment-list" minOccurs="0"/>

<xs:element name="code" type="xs:string" minOccurs="0"/>

<xs:element name="description" type="xs:string" minOccurs="0"/>

<xs:element name="name" type="xs:string"/>

<xs:element name="org-roles" type="tns:org-role-list" minOccurs="0"/>

<xs:element name="org-units" type="tns:org-unit-list" minOccurs="0"/>

<xs:element name="sentence" type="xs:int"/>

<xs:element name="type-code" type="xs:string" minOccurs="0"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="person-list">

<xs:sequence>

<xs:element name="person" type="tns:person" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="person">

<xs:complexContent>

<xs:extension base="tns:extern-entity">

<xs:sequence>

<xs:element name="degree-after" type="xs:string" minOccurs="0"/>

<xs:element name="degree-before" type="xs:string" minOccurs="0"/>

<xs:element name="account-disabled" type="xs:boolean"/>

<xs:element name="display-name" type="xs:string" minOccurs="0"/>

<xs:element name="email" type="xs:string" minOccurs="0"/>

<xs:element name="date-end" type="xs:dateTime" minOccurs="0"/>

<xs:element name="firstname1" type="xs:string"/>

<xs:element name="firstname2" type="xs:string" minOccurs="0"/>

<xs:element name="locked" type="xs:boolean"/>

<xs:element name="personal-id-number" type="xs:string" minOccurs="0"/>

<xs:element name="personal-number" type="xs:string" minOccurs="0"/>

<xs:element name="signature" type="xs:string" minOccurs="0"/>

<xs:element name="date-start" type="xs:dateTime" minOccurs="0"/>

<xs:element name="surname1" type="xs:string"/>

<xs:element name="surname2" type="xs:string" minOccurs="0"/>

<xs:element name="username" type="xs:string" minOccurs="0"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="role-connection-list">

<xs:sequence>

<xs:element name="role-connection" type="tns:role-connection" maxOccurs="unbounded" minOccurs="0"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="role-connection">

<xs:sequence>

<xs:element name="child-role-id" type="xs:string"/>

<xs:element name="master-role-id" type="xs:string"/>

</xs:sequence>

</xs:complexType>

<xs:simpleType name="synchronization-mode">

<xs:restriction base="xs:string">

<xs:enumeration value="FULL"/>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="org-role-tree-type">

<xs:restriction base="xs:string">

<xs:enumeration value="ROLE\_CONNECTIONS"/>

<xs:enumeration value="MASTER\_FIELD"/>

<xs:enumeration value="NONE"/>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="pairing-mode">

<xs:restriction base="xs:string">

<xs:enumeration value="MANUAL"/>

<xs:enumeration value="CODE"/>

<xs:enumeration value="NAME"/>

</xs:restriction>

</xs:simpleType>

<xs:simpleType name="phone-type">

<xs:restriction base="xs:string">

<xs:enumeration value="FAX"/>

<xs:enumeration value="MOBILE"/>

<xs:enumeration value="WORK"/>

</xs:restriction>

</xs:simpleType>

</xs:schema>