Smlouva o dílo na Identity management

I. Smluvní strany

BCV solutions s. r. o. (dále jen Dodavatel)

se sídlem: 7. května 1168/70, 149 00 Praha 4 - Chodov

zapsaná v obchodním rejstříku u Městského soudu Praha, oddíl C, vložka 136075

IČO: 28360851

DIČ: CZ28360851

bankovní spojení: 2800049696/2010

zastoupená: Lukášem Cirkvou, jednatelem

Česká republika – Ústav pro studium totalitních režimů (dále jen Objednatel)

se sídlem: Siwiecova 2, Praha 3 – Žižkov, 130 00

zřízena na základě zákona č. 181/2007 Sb. jako organizační složka státu,

jejímž jménem jedná ředitel Ústavu, Mgr. Zdeněk Hazdra, Ph. D.

IČO: 75112779

bankovní spojení: ČNB Praha 1

č. účtu: 2720001/0710

uzavřeli níže uvedeného dne, měsíce a roku dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, v platném znění a na základě vyhodnocení výsledků veřejné zakázky: „Systém pro správu uživatelských identit" tuto smlouvu o dílo (dále jen „smlouva").

II. Předmět smlouvy

1. Předmětem plnění této smlouvy (Dílo), je dodávka software a implementačních služeb pro řešení identity managementu pro objednatele (dále jen IdM), která zahrnuje:

   a) dodání základní instalace a zprovoznění systému

   b) integrace s připojenými systémy a kompletní implementace předmětu smlouvy, poskytnutí veškeré nezbytné součinnosti a podpory k zajištění plné funkčnosti předmětu smlouvy objednateli

2. Podrobný popis předmětu plnění, rozsah a úroveň služeb a jejich cena, je uvedena v Příloze č. 1, která je nedílnou součástí smlouvy.

III. Cena a platební podmínky

1. Celková cena za plnění dle čl. II odst. 1 této smlouvy je stanovena dohodou smluvních stran a činí**: 370 000 Kč bez DPH (slovy: tři sta sedmdesát tisíc korun českých), tj. 447 700 Kč včetně 21% DPH (slovy: čtyři sta čtyřicet sedm tisíc sedm set korun českých).** Podrobná cenová specifikace je uvedena v Příloze č. 1, která je nedílnou součástí smlouvy.
2. Smluvní cena díla zahrnuje veškeré práce, výkony a služby související s provedením díla. V celkové ceně jsou zahrnuty činnosti uvedené v čl. II odst. 1 písm. a) a b) této smlouvy realizované dodavatelem v termínech dle čl. IV odst. 1 této smlouvy. Cenovou nabídku vypracoval zhotovitel. Cenová nabídka je nedílnou součástí této smlouvy. Cena stanovená v nabídce je nepřekročitelná a maximální s výjimkou toho, že může být měněna při zákonné změně sazby DPH.
3. Uskutečněný předmět smlouvy bude hrazen bankovním převodem na účet objednatele, který je uveden v záhlaví této smlouvy, a to na základě vystavené faktury zhotovitelem. Fakturu lze vystavit po provedení dodání a zprovoznění systému podle čl. IV odst. 1 písm. a) této smlouvy a po oboustranném odsouhlasení. Faktura bude vystavena a uhrazena v Kč.
4. Faktura musí mít zákonem předepsané náležitosti daňového dokladu – v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
5. Faktura je splatná do 14 kalendářních dnů ode dne jejího doručení objednateli, den doručení v to nepočítaje. Fakturu je možno zaslat poštou na adresu: Ústav pro studium totalitních režimů, Siwiecova 2, Praha 3, 130 00 nebo elektronicky na e- mail podatelna@ustrcr.cz. Faktury vystavené v období od 10. prosince do 10. ledna jsou splatné do 45 kalendářních dnů ode dne jejich doručení, den doručení v to nepočítaje. Faktura je považována za proplacenou okamžikem odepsání příslušné finanční částky z účtu objednatele.
6. Nebude-li vystavená faktura obsahovat zákonem stanovené náležitosti, jak je uvedeno v bodu 3 tohoto článku nebo v ní budou uvedeny nesprávné údaje, je objednatel oprávněn ji vrátit zpět zhotoviteli s uvedením, resp. vytčením chybějících náležitostí nebo nesprávných údajů. Oprávněným vrácením faktury

přestává běžet lhůta splatnosti. Nová lhůta v původní délce splatnosti běží znovu ode dne prokazatelného doručení opravené nebo nově vystavené faktury objednateli. Faktura se považuje za vrácenou ve lhůtě splatnosti, je-li v této lhůtě odeslána, není nutné, aby byla v téže lhůtě doručena zhotoviteli, který ji vystavil.

7. Zálohové platby objednatel neposkytuje.

IV. Místo a termín plnění

1. Zhotovitel se zavazuje provést dílo v rozsahu předmětu plnění dle požadavku objednatele takto:
   - a) do 9. 12. 2016 včetně dodat základní instalaci a zprovoznění systému (fáze 1 podle čl. II odst. 1 písm. a);
   - b) do 28. 2. 2017 včetně provést integraci s připojenými systémy a kompletní implementaci předmětu smlouvy, poskytnout objednali veškerou nezbytnou součinnost a podporu k zajištění plné funkčnosti předmětu smlouvy (fáze 2 podle čl. II odst. 1 písm. b)
2. Konečné předání předmětu smlouvy si smluvní strany navzájem písemně potvrdí na základě protokolu o dodání a zprovoznění, který vyhotoví zhotovitel.
3. Místem plnění je sídlo objednatele na adrese Siwiecova 2, Praha 3 – Žižkov, 130 00.

V. Komunikace

1. Osobami pověřenými jednat jménem smluvních stran při plnění této smlouvy ve věcech projektových jsou:

   - **za objednatele:** Jiří Lundák
   - **tel:** +420 221 008 215
   - **e-mail:** jiri.lundak@ustrcr.cz
   -

   - **za dodavatele:** Lucie Cirkvová
   - **tel:** 777 785 847
   - **email:** lucie.cirkvova@bcvsolutions.eu
2. Osobami pověřenými jednat jménem smluvních stran při plnění této smlouvy ve věcech technických jsou:

   - **za objednatele:** Jiří Lundák
   - **tel:** +420 221 008 215
   - **e-mail:** jiri.lundak@ustrcr.cz

   - **za dodavatele:** Marcel Poul
   - **tel:** 723 272 319
   - **email:** marcel.poul@bcvsolutions.eu
3. Osoby pověřené jednat ve věcech projektových, zodpovídají za akceptaci jednotlivých fází plnění, uvedených v Příloze č. 1 - část 2 „Podrobná cenová kalkulace, harmonogram plnění".
4. Osoby pověřené jednat ve věcech technických, zodpovídají za průběžnou akceptaci dílčích plnění a technických dokumentů.
5. Jakákoli komunikace mezi smluvními stranami ve věcech projektových může

být učiněna osobně nebo doporučeným dopisem (včetně kurýra) nebo prostřednictvím elektronické pošty (e-mail).

6. Smluvní strany se dohodly, že běžné technické a organizační konzultace týkající se plnění této smlouvy mohou být prováděny telefonicky.
7. V případě, že dojde z objektivních důvodů k odklonu od předpokládaných termínů realizace projektu uvedených v čl. IV odst. 1 této smlouvy, mohou se osoby pověřené jednat ve věcech projektových dohodnout na termínech nových, odpovídajících aktuálnímu stavu projektu a požadavkům Objednatele. O tomto rozhodnutí vytvoří oboustranně podepsaný zápis.

VI. Povinnosti smluvních stran

1. Povinnosti Dodavatele:

1. Poskytovat služby v rozsahu a specifikaci stanovených v Příloze č. 1 této smlouvy a termínech dle čl. IV odst. 1 této smlouvy.
2. Zachovávat mlčenlivost o všech skutečnostech, se kterými přijdou pracovníci Dodavatele při provádění jakékoliv činnosti u Objednatele či zákazníka do styku.
3. Pracovníci Dodavatele nebudou bez písemného povolení osoby pověřené ve věcech technických pořizovat kopie programových produktů nebo dat Zákazníka.
4. Přidělit dostatečný počet kvalifikovaných zaměstnanců do týmu, který bude pracovat na provádění Díla v souladu s touto smlouvou.
5. Informovat objednatele bez zbytečného prodlení o všech skutečnostech, které mají vliv na termín, rozpočet, kvalitu nebo rozsah prováděných prací např. v podobě odůvodněných víceprací nebo identifikovaných rizik.

2. Povinnosti Objednatele:

1. Provést platby v termínech a výši určené v článku III této smlouvy.
2. Informovat Dodavatele o jakékoliv změně týkající se konečného umístění, použití produktů krytých smlouvou.
3. Dodržovat podmínky provozování a užívání produktů krytých smlouvou, které jsou uvedeny v průvodní dokumentaci k těmto produktům.
4. Urychleně nejpozději do tří (3) pracovních dní poskytnout dodavateli na základě žádosti veškeré požadované informace a dokumenty nezbytné pro plnění závazků Dodavatele v souvislosti se spoluprací poskytovanou v souladu s touto Smlouvou. Přesná specifikace součinností je uvedena v příloze č. 1 kapitola součinnost objednatele.
5. Přidělit dostatečný počet kvalifikovaných zaměstnanců do týmu, který bude pracovat na provádění Díla.
6. Vyčlenit pro zaměstnance Dodavatele dostatečné prostory a nástroje pro umožnění dodávky Díla, zejména adekvátní pracovní místo, elektrické přípojky a možnost vzdáleného připojení do sítě Dodavatele.

VII. Přechod vlastnictví

1. Vlastnické právo k Dílu nebo jeho části přechází na Objednatele úplným zaplacením ceny stanovené Smlouvou.

2. Bez předchozího písemného souhlasu Dodavatele není Objednatel oprávněn vytvářet a poskytovat kopie Díla třetím osobám.

VIII. Odstoupení od smlouvy, smluvní pokuty, náhrady škod

1. Smluvní strany podpisem této smlouvy stvrzují, že pokud zhotovitel neprovede řádně předmět plnění podle čl. V odst. 1 písm. b), považují to smluvní strany za podstatné porušení této smlouvy a objednatel si vyhrazuje právo od této smlouvy odstoupit. Odstoupení musí být učiněno písemně a doručeno na adresu zhotovitele uvedené v záhlaví této smlouvy.
2. Dodavatel má právo odstoupit od smlouvy v případě prodlení Objednatele s úhradou faktur Dodavatele překračujícím o 60 dnů termín splatnosti. Dodavatel v rámci této doby písemně vyzve k úhradě splatného závazku.
3. Při nedodržení podmínek uvedených v článku VII. odst. 2. Smlouvy ze strany Objednatele, neručí Dodavatel za dodržení sjednaných termínů plnění a má nárok na úhradu prokazatelně účelně vynaložených nákladů poskytovaných služeb, které mu nedodržením této povinnosti ze strany Objednatele vznikly.
4. Náhrady škody se řídí příslušnými ustanoveními občanského zákoníku, není-li v této smlouvě stanoveno jinak.
5. Zaplacením smluvní pokuty není dotčeno právo smluvní strany na náhradu škody vzniklé porušením smluvní povinnosti, které se smluvní pokuta týká.

6. V případě nedodržení termínu splatnosti faktury se smluvní strany dohodly na úroku z prodlení ve výši 0,05 % z fakturované ceny plnění včetně DPH, a to za každý i započatý den prodlení.

7. V případě nedodržení termínů dokončení díla dle článku IV. odst. 1 písm. b) této smlouvy, uhradí zhotovitel objednateli smluvní pokutu ve výši 0,5% z ceny díla včetně DPH za každý i započatý den prodlení.

8. Maximální celková výše pokut a škod je stanovena celkovou hranicí na 370 000 Kč.
9. Smluvní pokuta je splatná do 14 dnů poté, co bude písemná výzva jedné strany v tomto směru druhé straně doručena.

IX. Převzetí díla

1. Strany se dohodly, že jednotlivé fáze plnění definované v Příloze č. 1 této smlouvy (část 2 „Podrobná cenová kalkulace, harmonogram plnění") budou vždy předány k převzetí Objednateli následujícím způsobem, nebude-li výslovně písemně dodatkem k této smlouvě dohodnuto jinak: Do tří (3)

pracovních dní následujících po předání Díla Objednatel toto Dílo posoudí v přímém souladu s požadavky a specifikacemi sjednanými v Příloze č. 1 a písemně sdělí Dodavateli, zda odpovídá popisu a specifikaci uvedenému v Příloze č. 1. Pokud Dílo tomuto odpovídá, Objednatel bezodkladně podepíše protokol potvrzující jeho převzetí. V případě, že Objednatel rozhodne, že Dílo požadavkům a specifikacím neodpovídá, předá ve výše uvedené lhůtě Dodavateli písemný seznam vad, pro které Dílo neodpovídá (dále je každý „vadou"). Dodavatel opraví každou vytknutou vadu ve lhůtě dohodnuté s Objednatelem a po opravě znovu Dílo předloží Objednateli. Do tří (3) pracovních dní Objednatel znovu Dílo posoudí s jediným účelem potvrdit, že dříve označené vady byly opraveny. Tento postup bude pokračovat až do opravení všech objednatelem označených vad. Jakmile budou všechny vady Díla opraveny, Objednatel bezodkladně podepíše protokol o převzetí Díla. Pokud Objednatel způsobem uvedeným v této Smlouvě neoznámí Dodavateli některou vadu (ať už na počátku nebo při existenci dříve označené vady) a zároveň odmítne podepsat protokol o převzetí způsobem uvedeným výše, bude Dílo považováno za převzaté ke dni bezdůvodného odmítnutí podepsání protokolu o převzetí.

2. Výše zmíněné lhůty se prodlužují v oboustranně písemně odsouhlasených případech.

X. Záruka

1. Dodavatelem poskytnuté práce, dodávky nebo služby mají vady, jestliže jejich provedení neodpovídá požadavkům uvedeným v dokumentaci, vztahující se k jejich provedení.

2. Nedohodnou-li se smluvní strany jinak, zavazuje se objednatel veškeré zjištěné vady v záruční době (dále jen „vady") nahlásit dodavateli neprodleně po jejich zjištění.

3. Dodavatel neodpovídá za vady a škody, které byly způsobeny nesprávným užitím výsledků poskytnutých dodavatelem podle této smlouvy, ani za vady vzniklé na straně objednatele nebo jinými příčinami, které nevyplývají z výsledků poskytnutých dodavatelem podle této smlouvy.

4. Dodavatel neodpovídá zejména za vady, které:
   - byly způsobeny nesprávnými podklady nebo informacemi poskytnutými objednatelem;
   - vznikly neodborným zacházením objednatele nebo nedodržením návodu k obsluze poskytnutým dodavatelem;
   - vznikly použitím nevhodných technických prostředků v rozporu s dokumentací poskytnutou dodavatelem;
   - vznikly provozováním či užíváním programových produktů, implementovaných dodavatelem, v rozporu s jím dodanou dokumentací k těmto produktům;
   - vznikly změnou parametrů programových produktů objednatelem bez souhlasu dodavatele nebo v rozporu s dodavatelem dodanou dokumentací k těmto produktům;

- vznikly v důsledku nesprávnosti a nekompletnosti dat vkládaných do programových produktů přímo objednatelem;
- způsobila třetí osoba, za třetí osobu dle této smlouvy nejsou považováni řádně proškolení zaměstnanci objednatele;
- vznikly neodvratitelnou okolností;
- byly zjištěny nebo vznikly v období, kdy nebyla zajištěna podpora řešení dodavatelem.

5. V návaznosti na tato ustanovení se obě strany dohodly na záruční době na veškeré práce a služby dodavatele, v trvání 36 měsíců od předání a převzetí příslušné fáze díla. V této době dodavatel garantuje, že implementované produkty budou vykazovat vlastnosti popsané v předané dokumentaci k jejich užití a možnost užití k účelu popsanému v této smlouvě, a že v těchto vlastnostech a způsobech užití nebudou vykazovat žádné vady.

6. Provedenou opravu vady dodavatel objednateli předá písemným zápisem.

XI. Závěrečná ustanovení

1. Smluvní strany se zavazují poskytnout veškerou nezbytnou součinnost k naplnění účelu smlouvy.
2. Smluvní strany se dále dohodly, že obsah této smlouvy nepodléhá obchodnímu tajemství, tzn., že ji lze v plném rozsahu zveřejnit.

3. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.

4. Smlouva se řídí právním řádem České republiky. Práva a povinnosti neupravené touto smlouvou se řídí ustanoveními zákona č. 89/2012 Sb., občanský zákoník.

5. Smluvní strany se zavazují vyvinout maximální úsilí k řešení případných sporů vyplývajících z této smlouvy nejdříve smírčí cestou. Nedosáhnou-li strany smíru, má každá ze stran právo předložit spor místně a věcně příslušnému soudu.

6. Poruší-li některá ze smluvních stran některou ze svých povinností uvedených v této smlouvě, je druhá smluvní strana oprávněna od smlouvy odstoupit. Odstoupení od smlouvy musí být provedeno písemnou formou. Účinky odstoupení nastávají dnem doručení druhé smluvní straně.

7. Jakékoliv změny či doplnění smlouvy je možné činit výhradně formou písemných a číselně označených dodatků ke smlouvě schválených oběma smluvními stranami.

8. Za adresu pro doručování písemností se považuje adresa uvedená v záhlaví této smlouvy, nebo adresa, kterou smluvní strany, po uzavření smlouvy, písemně oznámí druhé smluvní straně. S odkazem na ustanovení § 573 zákona č 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, mají smluvní strany za to, že zásilka je druhé smluvní straně doručena třetí

pracovní den po jejím odeslání a že tímto dnem nastávají právní účinky. To neplatí, pokud se smluvní strany dohodnou jinak.

9. Smlouva se vyhotovuje ve 2 stejnopisech, přičemž každá ze smluvních stran obdrží po jednom vyhotovení.

10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, s jejím obsahem souhlasí a že byla sepsána na základě jejich pravé a svobodné vůle, a na důkaz toho připojují své podpisy.

11. Smluvní strany souhlasí s tím, že všechny přílohy této smlouvy tvoří její nedílnou součást. Ke dni podpisu tato smlouva obsahuje následující Přílohy: Příloha č. 1 - Nabídka dodavatele - návrh řešení

V Praze dne:	V Praze dne:
…….	…….
Za Objednatele:	Za Dodavatele:
Mgr. Zdeněk Hazdra, Ph.D ředitel Ústavu	Ing. Lukáš Cirkva Jednatel

Příloha 1 smlouvy – nabídka dodavatele

1 Návrh řešení

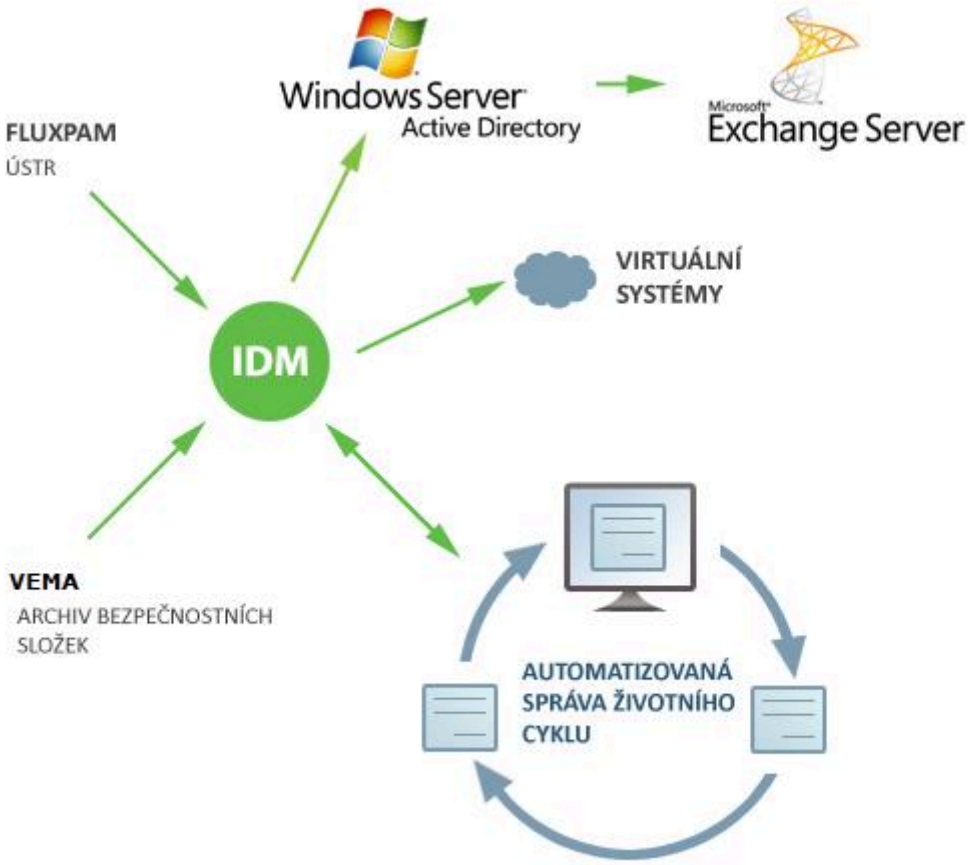
Správa identit vyžaduje instalaci základní komponenty Identity Manageru. Pro správu identit bude využito produktu **CzechIdM** (dále jen IdM nebo Identity Manager). Identity manager bude centrálně řídit životní cyklus uživatelů.

1.1 Základní přínosy řešení

- **Cena:** Veškerý SW využitý na projektu je poskytován **zdarma**, placena jsou pouze **implementační práce**. Většina prostředků se investuje do nastavení specifických pro prostředí zákazníka.
- **Udržitelnost:** Velikost a cena podpory je opět dána **pouze cenou práce**, lze ji zajistit i pomocí vlastních zdrojů. Nedochází k **závislosti na dodavateli** a jeho cenové politice.
- **Flexibilita:** Díky architektuře řešení a vlastnostem použitých SW lze velice rychle **měnit parametry prostředí** s pouze minimálními výdaji a to v obou směrech.
- **Zvýšení bezpečnosti:** Nasazením identity managementu jsou odstraněny tzv. mrtvé duše, je zamezena akumulace oprávnění uživatelem, také lze vynutit centrální politiku hesel. To spolu s auditními informacemi (kdo má kam přístupy, kdo a kdy mu ho schválil) **výrazně zvyšuje úroveň zabezpečení** v celé společnosti a naplňuje některé body zákona o **kybernetické bezpečnosti.**
- **Možnosti rozvoje:** Navržené řešení je pouze **základním stavebním kamenem** řešícím aktuální potřebu správy účtů a rolí. Pokud již existuje vybudované prostředí, je jeho další rozvoj výrazně levnější a lze u něj i využít vlastních zdrojů.
- **Zapojení virtuálních systémů do IDM:** V rámci řešení budou vybrány další systémy, které nebudou napřímo napojeny do IDM. Tak lze zvýšit **množství systémů** zapojených do centrální správy uživatelským účtů, při **minimálních nákladech**. Postupně lze systémy zapojovat fyzicky podle reálné zkušenosti s prostředím, čímž dochází k významné úspoře nákladů.

1.2 Popis a schéma architektury řešení

Informace o identitách interních uživatelů budou přebírány z databáze personálních systémů (dle organizace) do identity manageru a po zpracování budou, dle definovaných pravidel a procesů, propagovány do spravovaných aplikací.



Uživatelé budou mít do Identity Manageru přístup přes webové rozhraní. Uživatelské rozhraní zajišťuje samoobsluhu, kde si uživatelé mohou zkontrolovat správnost údajů o nich v Identity Manageru vedených a existenci uživatelských účtů a oprávnění v koncových aplikacích a v přístupu k datům. Samoobslužné rozhraní také umožňuje uživateli z jednoho místa provést změnu hesla, případně požádat o přístup do nové aplikace nebo o změnu oprávnění ke stávajícímu účtu.

Identity Manager provádí správu uživatelských účtů standardní cestou přes tzv. konektory, kterými se připojuje ke spravovaným systémům. Dále umožňuje zpracovávat automatizované procesy a zpřístupnit data o uživatelích přes webové služby (REST API). Není tedy většinou nutné zasahovat do koncových aplikací.

1.3 Systémy zapojené do IDM

1.3.1 Zdroje identit – FLUX PAM, VEMA

Identity manager bude napojen na personální systém FLUX. Protože USTR i ABS má vlastní instanci personálního systému, bude napojení provedeno dvakrát a z obou personalistik si bude identity manager načítat informace o uživatelích.

FLUX PAM

Napojení bude realizováno čtením dat modulu Personalistika z MS SQL databáze, ve které má personální systém FLUX uložená data. Personální systém bude autoritativním zdrojem informací o identitách uživatelů s pracovně právním vztahem v USTR.

VEMA

Připojení personalistiky VEMA bude realizováno specializovaným konektorem, který je součástí CzechIdM. Personální systém bude autoritativním zdrojem informací o identitách uživatelů s pracovně právním vztahem v ABS.

Personální systémy budou hlavním zdrojem informací o uživatelích. Podle zjištěných změn bude identity manager spouštět odpovídající procesy správy životního cyklu identit.

1.3.2 Spravované systémy

MS Active Directory

Správa uživatelů bude realizována standardním konektorem, který je součástí CzechIdM, bude umožněno minimálně založení uživatele, změnu atributů u uživatele, zrušení uživatele, změny zařazení uživatele do skupin. IDM musí dále umožnit načítání skupin z AD do IDM.

Exchange

Správa uživatelů bude realizována standardním konektorem, který je součástí CzechIdM. Bude umožněno minimálně spravovat mailový systém objednatele (objednatele), tj. adresy, aliasy, distribuční skupiny.

1.3.3 Virtuální systémy

Systémy, které nebudou přímo napojené na identity manager, budou spravovány jako tzv. „virtuální systémy". V identity manageru bude systém zaveden pro evidenci všech požadavků na něj. Správu bude provádět administrátor ručně na základě emailové výzvy zasílané z identity manageru. Provedení úkonu správy potvrdí administrátor v identity manageru.

V rámci projektu bude takto řízen GINIS USTR, GINIS ABS.

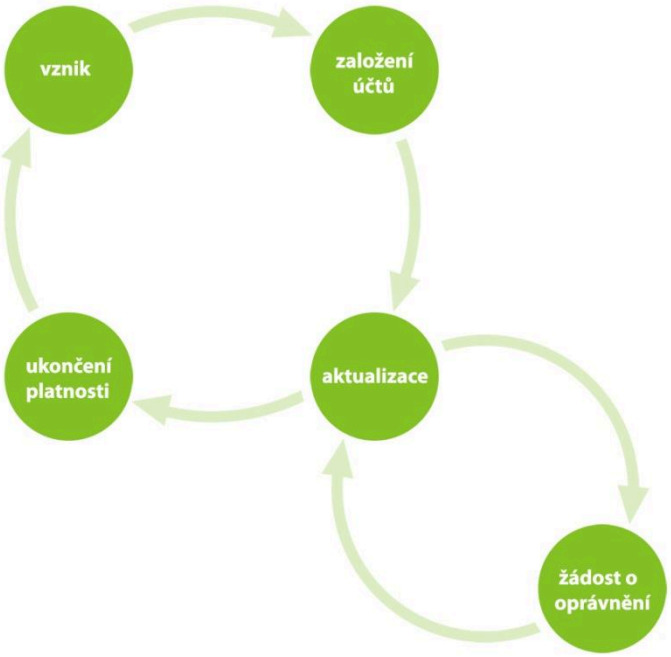
1.4 Procesy správy identit

CzechIdM řídí správu identit skrz parametrizovatelné a dle potřeby upravitelné procesy. Identity manager bude zpracovávat následující procesy iniciované událostmi z personálního systému:

- založení uživatelského účtu
- aktualizace popisných atributů
- přejmenování uživatele
- změna rolí uživatele
- zrušení uživatelského účtu

Seznam konkrétních procesů a jejich vazeb bude definován v rámci analýzy řešení.

Procesy lze spouštět automaticky na základě přijaté události od autoritativního systému, automaticky dle naplánované úlohy nebo manuálně pokud k tomu má uživatel oprávnění. Vybrané procesy jako je žádost o přidělení role nebo účtu v aplikaci lze zpřístupnit uživatelům v uživatelském rozhraní a tím zajistit možnost sebeobsluhy.



1.5 Role management

Vzhledem k přechodu na CzechIdM bude možné začít využívat systém rolí pro přidělování oprávnění uživatelům.

Správu rolí je nutné řešit jak v organizaci formou různých opatření, případných změn v evidenci dat o lidech v personalistice apod., tak i technicky na straně identity manageru a aplikací na něj napojených.

Projekt nasazení CzechIdM nemá ambice vyřešit kompletně správu rolí, ale zajistí infrastrukturu pro práci s nimi – jejich evidenci a vytváření v katalogu rolí a přidělování a odebírání uživatelům. Uživatelé si o role mohou žádat sami přes samoobsluhu, role mohou být také přidělovány uživatelům automaticky na základě např. organizačního zařazení nebo typu uživatelského účtu**. Pro tyto aktivity bude využito standardní funkčnosti CzechIdM**.

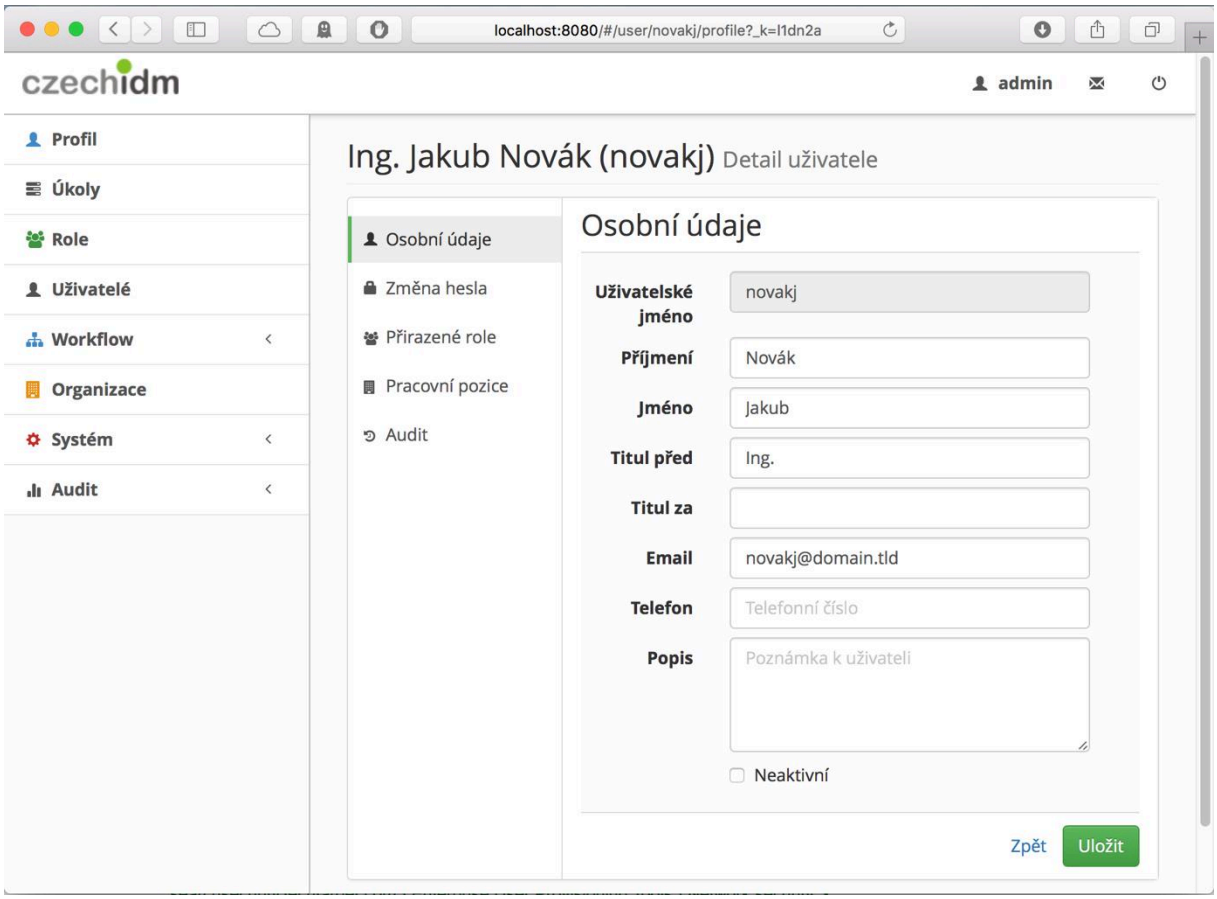
1.6 Zabezpečení dat

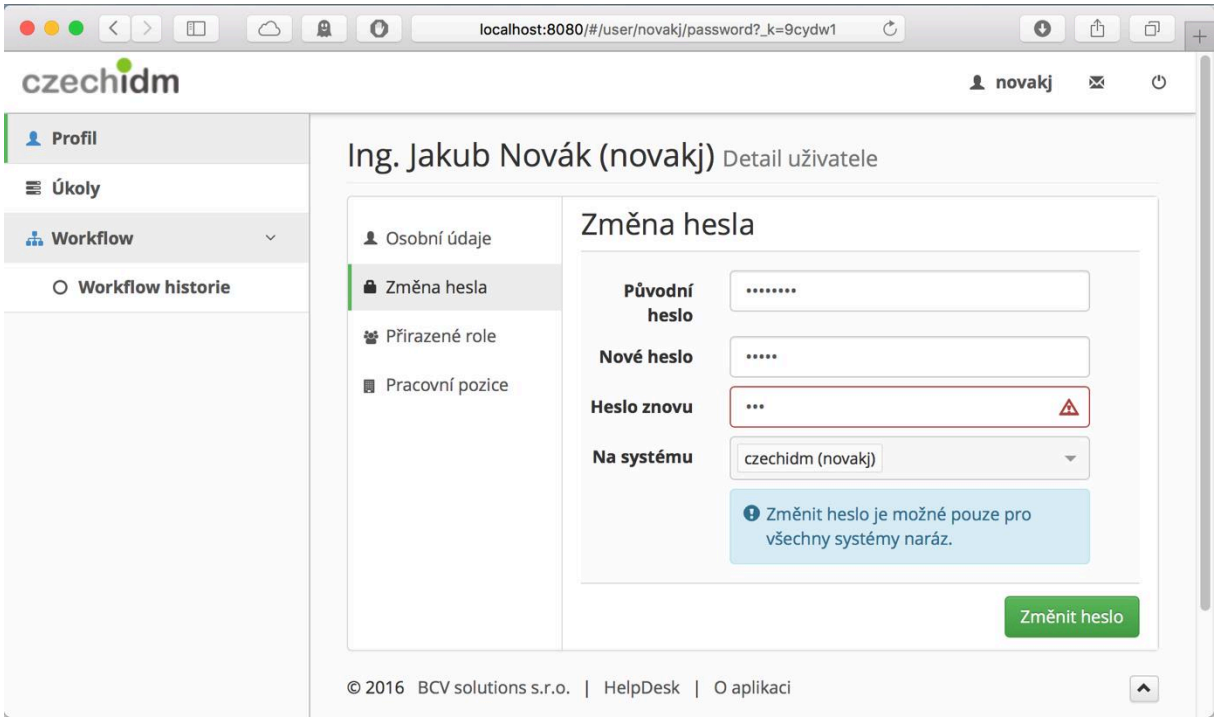
Všechna komunikace mezi identity managerem CzechIdM a napojenými systémy bude primárně provozována přes zabezpečené připojení (HTTPs, LDAPs, SSL šifrování při spojení do databáze).

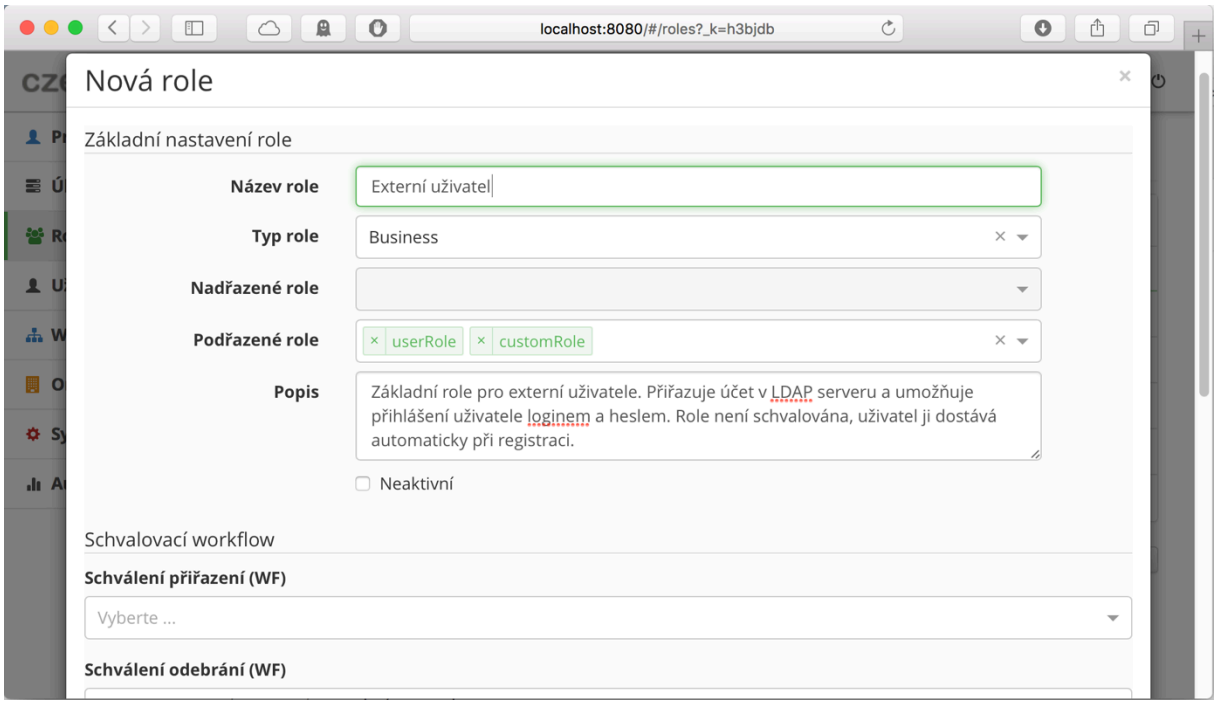
Uživatelské webové rozhraní i REST API CzechIdM bude zpřístupněno přes zabezpečený protokol HTTPs.

1.7 Uživatelské rozhraní

Identity manager CzechIdM má webové rozhraní, které v závislosti na oprávnění uživatele zpřístupňuje jednotlivé funkce. Oprávnění uživatelů jsou řízena dle modelu RBAC. Identity Manager obsahuje webové uživatelské rozhraní jako standardní součást a je **plně lokalizované do českého jazyka.**




localhost:8080/#/user/novakj/password?_k=9cydw1
czechidm
novakj
Profil
Úkoly
Workflow
Workflow historie
Ing. Jakub Novák (novakj) Detail uživatele
Osobní údaje
Změna hesla
Přiřazené role
Pracovní pozice
Změna hesla
Původní heslo
Nové heslo
Heslo znovu
Na systému
czechidm (novakj)
Změnit heslo je možné pouze pro všechny systémy naráz.
Změnit heslo
© 2016 BCV solutions s.r.o. | HelpDesk | O aplikaci


localhost:8080/#/roles?_k=h3bjdb
Nová role
Základní nastavení role
Název role
Externí uživatel
Typ role
Business
Nadřazené role
Podřazené role
userRole
customRole
Popis
Základní role pro externí uživatele. Přiřazuje účet v LDAP serveru a umožňuje přihlášení uživatele loginem a heslem. Role není schvalována, uživatel ji dostává automaticky při registraci.
Neaktivní
Schvalovací workflow
Schválení přiřazení (WF)
Vyberte ...
Schválení odebrání (WF)

1.8 Dokumentace

Dokumentace řešení bude vytvářena v českém jazyce a bude zahrnovat následující dokumenty:

- „Analýza a Návrh řešení" bude na základě analýzy popisovat aktuální stav a navrhovaný stav. Tento dokument bude sloužit jako výchozí pro realizaci celého řešení.
- „Dokumentace skutečného řešení" bude obsahovat všechny změny platné pro prostředí objednatele proti standardní konfiguraci jednotlivých komponent případně změny provedené proti návrhu řešení.
- Dokumenty „Administrátorská dokumentace" a „Uživatelská dokumentace" budou popisovat základní pracovní postupy.

1.9 Technologické zázemí

1.9.1 Prostředí pro běh aplikace

Vzhledem k povaze projektu – nasazuje se integrační nástroj pro automatizovanou správu identit – bude provozován ve třech prostředích:

- Vývojové – v provozu u dodavatele
- Testovací – v provozu u zákazníka, prostředí odpovídá vlastnostmi produkci. Slouží pro otestování změn před nasazením do produkce.
- Produkční

1.9.2 Software a potřebné licence

Navrhovaný software pro implementaci projektu je dostupný pod opensource licencí a je distribuován zdarma. Všechen software je aktivně využíván širokým spektrem uživatelů (jedná se o „živé" projekty) a je rozvíjen renomovanými firmami.
Dodavatel preferuje využít volně dostupný opensource software. Dodávka komerčního software není součástí projektu.

Software preferovaný dodavatelem:

Identity manager:	CzechIdM
Operační systém:	CentOS
Databáze pro IdM:	PostgreSQL
Aplikační server:	Apache Tomcat

Součástí nabídky není zajištění HW pro provoz nabízeného řešení.

Doporučená konfigurace HW:

Účel serverů	Doporučená konfigurace HW	Počet serverů
Testovací prostředí Identity Manager, Databáze pro IdM	2 jádra CPU, 4 GiB RAM	1
Produkční prostředí Identity Manager,Databáze pro IdM Databáze pro IdM	2-4 jádra CPU, 4GiB RAM	1

CzechIdM je možné provozovat ve virtualizovaném prostředí.

1.10 Seznam použitého SW

Název SW	Výrobce	Licence	www	Počet uživatelů	Počet Instancí	Počet spravovaných systémů
CzechIdM	BCV solutions	MIT	www.czechidm.com	není omezen	není omezen	není omezen

1.11 Školení

Délka školení	6 hodin
Účastníci	Pověření uživatelé a administrátoři (pro max. 10 osob)
Obsah školení	Základní seznámení s identity managementem, seznámení s implementovanými procesy správy životního cyklu identity a jejich dopady, schvalovací proces.

1.12 Součinnost objednatele

Zákazník se zavazuje dodavateli poskytovat veškeré informace a prostředky níže popsané nejpozději do tří (3) pracovních dnů od výzvy Dodavatele.

Konkrétně se jedná o tyto požadavky související s projektem:

- Zajistit veškerou dokumentaci dotčených informačních systémů vzhledem ke správě identit.
- Zpřístupnit vzdálené připojení – VPN do vývojového/testovacího prostředí.
- Poskytnout vývojové a testovací prostředí připojovaných systémů včetně reprezentativního vzorku dat.
- Vytvořit organizační, časové a materiální podmínky pro zaměstnance do projektu začleněných, včetně nastavení potřebných kompetencí. Zejména se jedná o nekuřácký pracovní prostor, připojení k internetu, dostupnost zodpovědných osob na straně Objednatele atd.
- Zajistit pověřené zodpovědné pracovníky na straně Objednatele – zejména projektového manažera odpovědného za akceptaci plnění a správce systémů.
- Zajistit spolupráci třetích stran, nebude-li možné toto zajistit pracovníky Objednatele. Lze i formou pověření, tak aby měl dodavatel pravomoc s třetí stranou jednat.
- Určit administrátora odpovědného za běh IdM. Případně dále vybrat osobu, která bude mít na starosti změnu (reset) zapomenutých hesel uživatelů a další podpůrné úkoly.
- Obeznámit administrátory s dopadem ručních zásahů provedených v systémech napojených na IdM.
- Seznámit uživatele s webovým rozhraním IdM a systému centrální autentizace a autorizace a s postupem řešení běžných úkolů. Může jít například o schválení požadavku, podání žádosti a podobně.
- Zařídit pravidelné zálohy repository IdM.
- Poskytnout HW zázemí pro běh IdM
- Administrátoři starající se o systém IdM budou proškoleni v rámci projektu.

2 Podrobná cenová kalkulace, harmonogram plnění

Popis	Nabídková cena bez DPH
Instalace a zprovoznění systému (fáze 1) • Příprava testovacího prostředí • Instalace produkce • Analytické činnosti	144 000,-
Integrace s připojenými systémy a kompletní implementace (fáze 2) • Analýza a návrh řešení • Procesy • Připojované systémy • Dokument: „Analýza a návrh řešení • Připojení personalistiky FLUX • Připojení personalistiky VEMA • Implementace procesů • Připojení MS AD pro správu • Připojení Exchange pro správu • Virtuální systémy • Testování • Zaškolení obsluhy • Přechod do produkce • Dokumentace	226 000,-
Celkem za implementaci řešení bez DPH	**370 000 Kč**
Celkem za implementaci řešení včetně 21% DPH	**447 700 Kč**

3 Splnění požadavků objednatele

- IDM umožní automatizovat správu uživatelských identit, uživatelských účtů a oprávnění uživatelů v jednotlivých systémech.	ANO splňujeme
- Objednatel požaduje licencování nabízeného softwarového řešení bez omezení na všechny klíčové prvky systému, zejména: počet spravovaných identit, rolí, počet přistupujících uživatelů, správců a připojených systémů.	ANO splňujeme
- Objednatel preferuje Open-Source řešení, a i v opačném případě trvá na zpřístupnění zdrojových kódů.	ANO splňujeme
- Objednatel požaduje vytvoření produkčního a testovacího prostředí.	ANO splňujeme
- IDM musí udržovat identity, skupiny identit a organizační struktury ve své vnitřní databázi. Identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní informační systémy.	ANO splňujeme
- IDM musí udržovat a spravovat kompletní životní cyklus identity.	ANO splňujeme
- Přihlašovací jméno uživatele musí být generováno podle algoritmu, který určí objednatel.	ANO splňujeme
- IDM musí umožnit hierarchizaci identit ve stromové (organizační) struktuře a umožní pracovat s více organizačními strukturami podle různých atributů. (např. dle AD, dle firemní struktury, dle projektů…)	ANO splňujeme
- IDM musí umožnit správu uživatelských rolí, včetně zařazení uživatele do odpovídající role. IDM musí k roli umožnit přiřazení sady upřesňujících atributů.	ANO splňujeme
- IDM musí umožnit nastavení schvalovacího workflow (při přidělení práva, role atd.), včetně emailových notifikací a potvrzování.	ANO splňujeme
- Systém pro správu identit musí umožnit obousměrnou synchronizaci dat jak z IDM do spravovaného systému, tak ze spravovaného systému do IDM.	ANO splňujeme
- Veškeré požadavky, které provedou uživatelé na IDM, musí být historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM. Záznam v historii musí obsahovat původní i novou hodnotu.	ANO splňujeme
- IDM musí umožnit přehledný náhled na historický stav identit, rolí a procesů ve vybraném čase (kompletní historie, audit). Audit musí umožnit správci systému zobrazit si historii změn na konkrétním uživateli. Auditní nástroj musí mít schopnost rekonstruovat objekt (uživatele) do původní podoby, tedy tak, jak vypadal například před rokem a to včetně navázaných dalších entit (například role).	ANO splňujeme
- IDM musí mít kompletní podporu českého jazyka i z hlediska dat, se kterými pracuje.	ANO splňujeme
- IDM musí mít možnost případného ořezání diakritiky (např. v algoritmech tvorby uživatelského jména), a to i u jiných znaků než jsou v české abecedě.	ANO splňujeme

- IDM musí být modulární - moduly může instalovat správce systému bez účasti dodavatele. Instalace musí spočívat pouze v nakopírování modulu do IDM a následném restartu systému.	ANO splňujeme
- IDM musí mít oddělený frontend a backend. IDM musí umožnovat vystavit pouze vybrané části aplikace do DMZ (demilitarizované zóny).	ANO splňujeme
- IDM musí umožnit notifikovat emailovou zprávou o vybraných operacích nad identitami či rolemi.	ANO splňujeme
- IDM musí umět reporty, přehledy stavu, přehledy změn, diagramy struktury, procesů, vlastníky informačních aktiv/procesů/aplikací, telefonní seznamy dle různých organizačních struktur.	ANO splňujeme
- IDM musí umět různé procesy pro různé druhy identit (uživatel, správce, technický účet).	ANO splňujeme
- IDM musí umět aplikovat různé politiky hesel (např. jen ASCII pro Radius, dlouhá víceslovná, speciální znaky a podobně, a musí obsahovat nástroj na „generování" bezpečných hesel dle daných politik, a to jak startovních pro administrátory, tak jako pomůcku pro uživatele.	ANO splňujeme
Zdrojem dat o zaměstnancích je personalistika FLUX PAM (USTR) a VEMA (ABS). IDM musí umožňovat načtení dat uživatelů:	ANO splňujeme
- z FLUX PAM včetně relevantních atributů a organizační struktury pomocí databázového pohledu (view).	ANO splňujeme
- VEMA musí být připojitelná bez dalších licenčních nákladů výrobce nebo musí být tyto náklady zahrnuty v ceně řešení.	ANO splňujeme
- Pod pojmem správa rozumíme automatizované nebo ruční založení, smazání, zneplatnění nebo změnu dat ve spravovaném systému na základě změny v některém ze zdrojových systémů dle definovaných procesů.	ANO splňujeme
- Kromě níže uvedených systémů musí IDM umožnovat napojení i dalších systémů pomocí obecného konektoru nebo integrační platformy. Napojení dalších systémů musí být možné provést vlastními silami objednatele bez nutnosti spolupráce s dodavatelem a bez dalších licenčních nákladů.	ANO splňujeme
- IDM musí umožnit připojení libovolného množství dalších spravovaných systémů a to bez dalších licenčních nákladů.	ANO splňujeme
- Součástí nabídkové ceny poptávaného řešení nejsou úpravy ve spravovaných systémech objednatele.	ANO splňujeme
Předmětem zakázky je napojení těchto systémů:	
- **MS Active Directory (dále jen „AD")** – IDM musí umožnovat komplexní správu účtů a členství ve skupinách v systému MS Active Directory, zejména musí umožnit založení uživatele, změnu atributů u uživatele, zrušení uživatele, změny zařazení uživatele do skupin. IDM musí dále umožnit načítání skupin z AD do IDM.	ANO splňujeme
Exchange 2007 a výhledově novější 2010 a cílově 2016 - IDM musí umět spravovat mailový systém objednatele.	ANO splňujeme v rozsahu nabídky a parametrů konektoru

- **Virtuální systémy**: GINIS USTR, GINIS ABS – jedná se o Systémy, které nebudou přímo napojené na IDM. V IDM bude systém zaveden pro evidenci všech požadavků na něj. Správu bude provádět administrátor ručně na základě emailové výzvy zasílané z IDM. Provedení úkonu správy potvrdí administrátor v IDM	ANO splňujeme
- IDM musí obsahovat webové rozhraní pro přístup jak běžných uživatelů, tak administrátorů systému pro správu a výkon jednotlivých integračních a provozních úloh. Webové rozhraní musí podporovat minimálně internetové prohlížeče Chrome, Firefox a Internet Explorer.	ANO splňujeme
- Webové rozhraní musí běžnému uživateli zobrazovat údaje o jeho identitě.	ANO splňujeme
- Webové rozhraní musí běžnému uživateli umožnit změnit si prostřednictvím webového rozhraní heslo.	ANO splňujeme
- Webové rozhraní musí běžnému uživateli umožnit zobrazení průchodu schvalovacím procesem v grafické podobě ve formě vývojového diagramu (například u žádosti o změnu oprávnění) a to tak, aby uživatel (nebo nadřízený) byl schopen v kterékoliv fázi procesu zjistit, kde požadavek „visí" a v jakém je stavu.	ANO splňujeme
- Všechny části řešení, které budou samoobslužně využívat běžní uživatelé, musí být plně lokalizovány do českého a anglického jazyka s možností přepínání mezi jazyky. U ostatních částí řešení objednatel připouští i možnost jen českého jazyka nebo jen anglického jazyka.	ANO splňujeme
- Přístup uživatelů k datům IDM musí být zajištěn prostřednictvím tohoto webového rozhraní. Řešení musí umožňovat zobrazení přidělených rolí k jednotlivým identitám.	ANO splňujeme
- Webové rozhraní musí umožňovat správu identit uživatelů a jejich případnou úpravu, založení, zneplatnění nebo smazání.	ANO splňujeme
- Webové rozhraní musí umožnit grafické zobrazení identit (uživatelských účtů) v organizační struktuře (ve více organizačních strukturách). V rámci jednoho pohledu musí být možné zobrazit organizační strukturu včetně pracovních pozic organizace až do úrovně jednotlivých uživatelských účtů (identit).	ANO splňujeme
- Webové rozhraní musí umožnit správci systému úpravu definice procesů. Pokud dojde k úpravě procesu, IDM musí umožnit ukončit již existující instance procesů podle původních pravidel. Na nově vzniklé instance již ale aplikovat pravidla nová.	ANO splňujeme
- IDM musí být možné nativně provozovat na níže uvedeném technickém vybavení objednatele:	ANO splňujeme
- prostředí virtuálních serverů Hyper-V cluster verze 2012r2 a novější	ANO splňujeme
- IPV4 síť	ANO splňujeme
- objednatel preferuje operační systém pro IDM server Linux – CentOS, případně RHEL – licence musí být v ceně nabídky, nebo MS Windows Server 2012R2 a vyšší (licence není vyžadována)	ANO splňujeme
- objednatel preferuje databázi bez licenčního zatížení (Postgres, MySQL) nebo databázi MS SQL (licence není vyžadována). Pokud bude užita jiná licencovaná databáze, musí být potřebné licence v ceně nabídky	ANO splňujeme
Součástí zakázky není dodávka HW vybavení.	ANO splňujeme

A) Analýza a návrh řešení	
Musí obsahovat minimálně:	
Model struktury organizace	ANO splňujeme
Analýzu procesů a systémů organizace se zaměřením na oblast správy uživatelských účtů	
Přidělování oprávnění a rolí	
Popis životního cyklu identity uživatelů	
Popis pravidel uživatelských hesel a nastavení centrální politiky hesel, včetně výjimek	
Analýzu zdrojových (FLUX PAM, VEMA) a spravovaných systémů (Active directory) s ohledem na	
nasazení IDM	
Analýzu a návrh postupů pro správu AD prostřednictvím IDM, včetně nastavení práv a pravidel	
pro správce	
Analýzu virtuálních systémů: GINIS USTR a GINIS ABS	
Analýzu a návrh životního cyklu rolí v organizaci	
Detailní popis navrženého řešení	
Detailní návrh technologické infrastruktury	
Návrh akceptačních scénářů a testů.	
Vypracovaný dokument je dodavatel povinen dodat v písemné podobě. Před předáním analýzy je dodavatel povinen podrobit ji připomínkovému řízení ze strany objednatele, připomínky vzešlé z tohoto řízení do výstupu zapracovat a zohlednit v rámci druhé fáze provádění díla. O předání a převzetí analýzy vyhotoví dodavatel písemný protokol.	
B) Instalace a implementace v testovacím prostředí	
Instalaci a implementaci je dodavatel povinen provádět v souladu se schválenou analýzou a návrhem řešení. V této etapě dodavatel provede instalaci systému a jeho kompletní implementaci včetně potřebných doplnění, specifických úprav a nastavení, naplní systém testovacími daty a umožní objednateli provedení příslušných testů. O ukončení instalace a implementace v testovacím prostředí vyhotoví dodavatel písemný protokol.	ANO splňujeme
Nebude-li předávané dílo prosto vad či nedodělků, objednatel uvede zjištěné vady či nedodělky do předávacího protokolu a zároveň stanoví dodavateli lhůtu k jejich odstranění. Předání části díla s vadami či nedodělky není splněním dodavatelova závazku, pokud objednatel v protokolu neuvede, že plnění s vytknutými vadami a nedodělky přebírá.	
C) Instalace a implementace v produkčním prostředí	
Instalaci a implementaci je dodavatel povinen provádět v souladu se schválenou analýzou a návrhem řešení, včetně případných změn vyplývajících z testování aplikace V této etapě dodavatel provede instalaci systému a jeho kompletní implementaci, naplnění systému produkčními daty. Součástí této fáze je předání dokumentace prostředí a zaškolení pracovníků objednatele. O ukončení instalace a implementace v produkčním prostředí bude vyhotoven písemný protokol.	ANO splňujeme

Objednatel požaduje vytvoření a předání kompletní technické a uživatelské dokumentace v elektronické podobě v českém jazyce.	ANO splňujeme
V editovatelné formě:	
- Dokumentace skutečné realizace	
- Uživatelská příručka	
- Administrátorská příručka	
Alespoň přístup ke čtení:	ANO splňujeme
- Programátorská dokumentace produktu	
- Zdrojové kódy produktu, souvisejících knihoven a zakoupených modulů	
7) Zaškolení obsluhy	
V rámci předmětu plnění a v rámci celkové nabídkové ceny bude provedeno školení administrátorů systému a vybraných uživatelů objednatele (max. 6 osob) v rozsahu minimálně 6 vyučovacích hodin školení.	ANO splňujeme