Příloha č. 1 smlouvy

# Specifikace díla

## A. Obecné požadavky

| Požadavek | | | |
|---|---|---|---|
| **Systémové požadavky** | Podpora jednoho z operačních systémů: UNIX/Linux, Windows | | |
| | Jediné úložiště dat (repozitory) a to relační databázi, pro svůj provoz nevyžaduje LDAP server | | |
| | Repozitory podporuje minimálně jednu z těchto relačních databází - MySQL 5, MS SQL Server 2014, Oracle DB 12, PostgreSQL 9.4, nebo novější verze | | |
| | Řešení podporuje technologii Java 8 či .NET 4.5, nebo novější verze | | |
| | Řešení je možné provozovat na jednom z aplikačních serverů: Apache Tomcat 8, Oracle Glassfish 3.1, Oracle WebLogic 12c, nebo novější verze | | |
| | Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC | | |
| **Licence** | Počet licencí bez omezení na počet uživatelů, koncových systémů, procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů | | |
| | Dodávka zdrojových kódů | | |
| | Možnost připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do systému IDM bez dodatečných licenčních nákladů | | |
| **Servis a podpora** | *Implementátora* | Garance reakční doby | |
| | | Hlášení požadavků na telefonickou hotline a do helpdeskové aplikace v režimu 5x8, pracovní doba od 9:00 hod do 17:00 hod | |
| | | Reporting o průběhu řešení požadavků v helpdeskové aplikaci provozované Dodavatelem | |
| | | 192 hodin na konzultace, případně drobný rozvoj řešení. Tyto hodiny bude možné využít libovolně v průběhu doby platnosti smlouvy | |
| | | Měsíční report o provedených službách | |
| | *Výrobce* | Garance oprav jádra produktu | |
| | | Přístup k novým verzím a patchům produktu | |
| | *Řešení vad* | P1 – kritické vady se zásadními dopady do běhu procesů Zadavatele | Reakce do 4 hod |
| | | | Odstranění do 8 hod |
| | | P2 – vady způsobující významné zhoršení funkčnosti systému | Reakce do 8 hod |
| | | | Odstranění do 32 hod |
| | | P3 – vady s nízkými dopady, ostatní požadavky | Reakce do 16 hod |
| | | | Odstranění dle dohody |

Obecné požadavky - pokračování

| Požadavek | | | |
|---|---|---|---|
| **Demo** | *Obecné* | V době podání nabídky on-line přístupné demo produktu bez nutnosti instalace jakéhokoliv SW či provedení konfigurace na straně zadavatele (např. VPN přístup) | |
| | | dostupnost po dobu minimálně 20 pracovních dní od zpřístupnění | |
| | *Požadovaná funkcionalita* | Admin. přístup | Přehled uživatelů |
| | | | Detail uživatele |
| | | | Koncové systémy s možností přidat nový koncový systém |
| | | | Serverové úlohy |
| | | | Minimálně dva reporty z části Reporting tabulky Požadavků na funkcionalitu (viz níže) |
| | | Uživ. přístup | Změna hesla z jediného místa pro všechny systémy |
| | | | Přehled o přidělených oprávněních v systémech |
| | | | Žádosti o role |
| | Ukázková data | | |

## A. Požadavky na funkcionalitu

| Požadavek | | |
|---|---|---|
| **Technické požadavky** | *Všeobecné* | Administrátorská a vývojářská dokumentace |
| | | Dávkové akce (příklad: hromadné přejmenování) |
| | | Export/import konfigurace IDM ve formátu XML |
| | | Logování a reporty chyb |
| | | Možnost definovat a pravidelně spouštět serverové úlohy (nejrůznější transformační, kontrolní a notifikační úlohy) |
| | | Možnost vytvářet vlastní konektory ke koncovým systémům jako komponenty nezávislé na verzi IDM |
| | | Podpora některého z rozšířených skriptovacích jazyků v konfigurovatelných částech Identity Manageru |
| | | Podpora vícejazyčného uživatelského rozhraní |
| | | Řešení musí být schopno pracovat v tzv. odlehčeném režimu, kdy funguje pouze jako integrační datový nástroj mezi koncovými systémy. Jedná se o volitelné vypínání náročných administrativních funkcí, jako je workflow apod. |
| | | Schopnost pracovat v režimu vysoké dostupnosti |
| | | Správa různých typů objektů (identit uživatelů, funkčních míst, místností, organizační struktury, rolí apod.) |
| | *Autorizační model* | Autorizační model je založen na RBAC (Role-Based Access Control) přístupu |
| | | Oprávnění jsou součástí rolí, role jsou přiděleny uživatelům |
| | | Musí být možné nastavit, k jaké části uživatelského rozhraní mají uživatelé přístup |

Požadavky na funkcionalitu - pokračování

| | | Požadavek |
|---|---|---|
| **Technické požadavky** | *Rozhraní pro integraci* | Možnost volání za pomoci Web service API (SOAP/WSDL) nebo REST API. |
| | | Možnost volat ekvivalent jakékoli funkcionality, která je dosažitelná z webového rozhraní (možnost volání jen některých funkcí jádra IDM je pro tyto potřeby nedostatečná) |
| | *Integrace s access managementem* | Zajištění Web SSO (Single Sing On) do IDM |
| | | IDM musí podporovat SLO - Single Log - Out (uživatel se odhlásí v Access managementu a následně je při příštím dotazu odhlášen i v nástroji Identity managementu) |
| | *Synchronizace a rekonciliace* | Synchronizace změn v reálném čase s odolností proti výpadkům informačních systémů - vestavěná podpora opakování propagace změn v případě neúspěchu |
| | | Obousměrná synchronizace dat jak z IDM do spravovaného systému (např. uživatele a jejich atributy), tak ze spravovaného systému do IDM (např. role v konkrétním systému). |
| | | Mapování atributů mezi informačními systémy na základě pravidel/vzorců |
| | | Práce s komplexními (tabulky) či binárními atributy uživatele - certifikáty, fotografie, autentizační tokeny |
| | | Rekonciliace účtů - pravidelná automatická kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu |
| | | Rekonciliace účtů - zaznamenání stavu účtu vzhledem k ne/existenci vlastníka v IDM |
| | | Rekonciliace oprávnění - pravidelná automatická kontrola stavu oprávnění na koncových systémech oproti stavu chtěnému a náprava (notifikace, zápis do logů, výmaz nadbytečných oprávnění apod.) |
| | | Nastavení párovacích pravidel mezi identitou a účtem (například email identity na login účtu) |
| | | Synchronizace hesel z IDM do koncového systému |
| | *Emailové notifikace* | Možnost definice šablon emailů s podporou vícejazyčnosti |
| | | Možnost konfigurace parametrů odesílání zpráv (SMTP server apod.) |
| | *Delegování správy* | Delegovaní správci musí mít administrátorská práva nad zvolenými komunitami nebo skupinami uživatelů - účelem je umožnit lokálnímu administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty) |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | |
|---|---|---|---|
| **Podporované procesy spustitelné z GUI IDM** | *Vznik identity* | Zdrojem dat je externí systém nebo samotná IDM aplikace | |
| | | Propagace identity do úložiště Identity managementu | |
| | | Automatické přidělení oprávnění dle nadefinovaných pravidel | |
| | | Propagace účtů do koncových systémů včetně časového omezení | |
| | | Odeslání emailové notifikace | |
| | *Změna identity* | Zdrojem dat je externí systém nebo samotná IDM aplikace | |
| | | Propagace změn do Identity managementu | |
| | | Propagace změn do koncových systémů | |
| | *Změna pozice (reorganizace)* | Zdrojem dat je externí systém nebo samotná IDM aplikace | |
| | | Propagace změn do Identity managementu | |
| | | Odebrání původních oprávnění k definovanému datu | |
| | | Přidělení nových oprávnění dle nadefinovaných pravidel | |
| | | Propagace změn do koncových systémů | |
| | | Odeslání emailové notifikace | |
| | *Žádost o změnu oprávnění* | Zdrojem je Helpdesk systém nebo samotná IDM aplikace | |
| | | Propagace změn do Identity managementu | |
| | | Identity Management zajistí schvalovací workflow a zpětnou informaci Helpdesku o stavu požadavku | |
| | | Propagace změn do koncových systémů | |
| | | Odeslání emailové notifikace | |
| | *Zánik identity* | Zdrojem dat je externí systém nebo samotná IDM aplikace | |
| | | Propagace změn do Identity managementu | |
| | | Zrušení (fyzický výmaz, zneplatnění) identity v koncových systémech dle nadefinovaných pravidel | |
| | | Možnost zpožděného výmazu účtů počítaného od data zneplatnění identity | |
| **Správa uživatelů** | Administrační webové rozhraní pro správu uživatelů | | |
| | Editace profilu uživatele | | |
| | Uložení a zobrazení fotografie uživatele | | |
| | Evidence atributů uživatele (jednohodnotové, vícehodnotové, binární či definované komplexní struktury – tabulky) | | |
| | Zneplatnění uživatele k určitému datu | | |
| | Přiřazení koncových systémů, rolí či organizace k uživateli | | |
| | Vyhledávání a filtrování podle atributů | uživatelů | podle loginu |
| | | | podle jména |
| | | | podle příjmení |
| | | | podle celého jména |
| | | rolí | podle jména |
| | | organizací | podle jména |

Požadavky na funkcionalitu - pokračování

| | Požadavek | |
|---|---|---|
| Správa rolí | Webové rozhraní pro správu rolí (soubor oprávnění) | |
| | Roli je možné přiřazovat uživatelům i organizacím | |
| | Možnost nastavení platnosti přiřazení role uživateli i organizaci od-do. | |
| | Možnost nastavit další atributy přiřazení (např. dle lokality uživatele) | |
| | Možnost dynamického výpočtu u schvalovací role | |
| | Role je možné hierarchicky skládat | |
| | Řízení autorizačních objektů v koncovém systému | Možnost svázat definici role s existencí objektu oprávnění v koncovém systému |
| | | Schopnost role vytvořit objekt v koncovém systému (např. vytvoření objektu v AD) |
| | Mechanismus konfliktních rolí (SoD – Segregation Of Duties) | Možnost systému nastavit pravidla pro vzájemně se vylučující role |
| | | Ochrana systému v případě pokusu o přiřazení konfliktní role (pokud dojde k pokusu o přiřazení role uživateli, který již má jinou konfliktní roli, musí systém konflikt oznámit a vlastní přiřazení neprovede) |
| | Časově omezené role | Řešení musí umožňovat nastavit časové období od-do pro přiřazení role uživateli |
| | | Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení role uplatnit |
| | Nastavení práv | Řešení musí umožňovat nastavit práva až na úroveň atributu libovolného typu objektu. Práva musí být přidělena uživateli, roli nebo organizaci |
| | Certifikace rolí | V nástroji IDM je možné spustit úlohu z grafického rozhraní, která zajistí schvalování pro všechny role přidělené identitám |
| | | Možnost recertifikace rolí (opakované spouštění schvalování) |
| Organizační struktura | Administrační webové rozhraní pro správu stromové struktury | |
| | Možnost vytváření libovolného počtu stromů | |
| | Možnost vytváření nezávislých entit (pracovní pozice, funkční místa) ve stromě | |
| | Možnost definovat atributy entit ve stromě | |
| | Možnost přiřazovat entitám ve stromě jiné objekty, zejména | role |
| | | jiné entity stromu |
| | | účty v koncových systémech |
| | Možnost vizualizace entit pomocí stromové struktury | |
| | Entity ve stromě přiřazovat k libovolnému objektu, zejména | roli |
| | | uživateli |
| | Uživatel nebo role může být přiřazen ve více entitách stromu zároveň | |
| | Uživatel nebo role může být přiřazen ve více stromech zároveň | |
| | Uživatel může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.) | |
| | Časové omezení při zařazení do stromové struktury | Řešení umožňuje nastavit časové období od-do pro přiřazení uživatele do stromové struktury |
| | | Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení uživatele do stromu uplatnit |

Požadavky na funkcionalitu - pokračování

| Požadavek | | |
|---|---|---|
| **Schvalovací proces** | Grafické rozhraní pro schvalovací procesy | |
| | Notifikace schvalovatele minimálně emailem | |
| | Schvalovatelé si mohou zobrazit přehled svých úloh | |
| | Možnost úlohu schválit či zamítnout včetně uvedení zdůvodnění | |
| | Schvalovací workflow musí podporovat vícekrokové schvalování | |
| | Schvalovat může jednotlivec nebo skupina schvalovatelů | |
| | Je možné určit typ schválení "všichni ze skupiny" nebo "jeden ze skupiny" | |
| | Správce IDM musí být schopen pracovat se všemi úlohami (pro řešení nestandardních situací) | |
| **Firemní politiky** | Možnost zavádění, vynucování a kontroly firemních politik | |
| | Politiky hesla | Řešení umožňuje nastavení pravidel pro minimální a maximální délku hesla, povolené skupiny znaků, počet opakování znaků, minimální a maximální výskyt znaků ze skupiny |
| | Politiky účtu | Řešení umožňuje nastavení pravidel pro název účtu - minimální a maximální délka, povolené znaky, zakázaná slova v názvu (například *admin*, *info*), kontrola na platný formát emailové adresy |
| **Reporting** | Auditní report | Kompletní přehled změn provedených nad uživatelem – například synchronizace atributů, přidělení role včetně časového omezení, změna hesla atd. |
| | | Kompletní přehled změn provedených nad klíčovými entitami řešení - role, organizace, definice politik a konfigurací |
| | | Záznam o přihlášení uživatele do webové rozhraní IDM |
| | Report uživatelů | Informuje o tom, jaké mají uživatelé přiřazené role a účty v koncových systémech |
| | | Možnost reportovat uživatele v určité organizaci |
| | Report rekonciliace | Přehled účtů v koncových systémech, které jsou známy IDM, v momentu spuštění reportu |
| | | Možnost identifikace účtů, ke kterým nebyl v IDM nalezen vlastník |
| | Možnost exportovat minimálně do všech následujících formátů: PDF, CSV, HTML, XML a formát MS Word a MS Excel | |

Požadavky na funkcionalitu - pokračování

| Požadavek | | | |
|---|---|---|---|
| **Uživatelské rozhraní** | *Obecné požadavky* | Jedno webové rozhraní pro administrátory i pro koncové uživatele, responzivní design (použití tlustého klienta není přípustné pro uživatelské, konfigurační ani správcovské činnosti) | |
| | | Kompletní lokalizace prostředí IDM do českého jazyka | |
| | | Možnost grafického přizpůsobení korporátní identitě úřadu (rozhraní je možné upravovat dle potřeb klienta) | |
| | | Dvě úrovně administrace | Administrátor – správce IDM, zasahuje do poloautomatických procesů, řeší výjimečné stavy, kontroluje reporting a flow identit |
| | | | Lokální informatik – přistupuje do IDM s omezeným oprávněním – provádí reset zapomenutých hesel |
| | *Koncoví uživatelé* | Zobrazení základních informací o profilu přihlášeného uživatele | přehled schválených rolí |
| | | | přehled rolí, které jsou svázány se zastávanou pracovní pozicí |
| | | | přehled oprávnění na jednotlivých koncových systémech |
| | | Možnost změny hesla na všech nebo vybraných koncových systémech | |
| | | Možnost změny definovaných atributů přihlášeného uživatele - podle typu uživatele možnost na nastavit práva na změnu atributů v profilu uživatele (např. externistům umožnit změnu kontaktní adresy, zaměstnancům naopak pouze změnu osobního emailu) | |
| | | Možnost zadat požadavek na zařazení do role, do stromu nebo na přístup do aplikace - možnost změny v přiřazení rolí podléhá schvalovacímu workflow | |
| | | Vedoucím pracovníkům umožňuje vložit požadavky na změny v přiřazení rolí pro podřízené pracovníky a sledovat stav vyřizování jejich žádostí | |
| | | Schvalovatelům umožňuje rozhodování o schválení či zamítnutí vznesených požadavků | |

# Popis konkrétního nabízeného řešení
## Manažerské shrnutí

Zadavatel: **ČR – Česká obchodní inspekce**
Štěpánská 567/15, 120 00 Praha 2

Dodavatel: **AMI Praha a. s. (AMI)**
Pláničkova 11, 162 00 Praha 6

Předmětem nabídky je implementace a technická podpora systému pro správu, řízení a monitoring identit, který zajistí jednotnou elektronickou správu, řízení a monitoring uživatelských identit včetně integrací do níže vyjmenovaných IS.

Pro řešení oblasti Identity Manageru je v tomto řešení navrhnut produkt midPoint od společnosti Evolveum.

- Řešení poběží na operačním systému CentOS, nebo dodaném Zadavatelem (Unix/Linux/Windows schopné provozovat Tomcat 7 s Java JDK 1.7).
- Řešení bude využívat relační databázi MySQL nebo poskytnutou Zadavatelem (MySQL 5.6, MS SQL Server 2014, Oracle DB 12, PostgreSQL 9.4, nebo novější verze).
- Produkt midPoint, operační systém CentOS ani relační databáze MySQL nepotřebují licence ke svému běhu.
- V případě dodání operačního systému či databáze zadavatelem, je na zadavateli zajistit i potřebné licencování.

Součástí nabídky jsou zejména následující části:

- vypracování detailní analýzy a návrhu řešení,
- vypracovaná požadovaná dokumentace,
- implementace a konfigurace IdM,
- v rámci nasazení systému IdM budou připojovány následující systémy:
    - personální systém Elanor Odysea 2001,
    - MS Active Directory,
    - MS Exchange 2013,
    - Mercurius (kontrolní informační systém) společnosti INISOFT,
    - GINIS® (spisová služba) společnosti GORDIC,
    - JASU® CS (ekonomický informační systém) společnosti Múzo Praha,
- školení administrátorů zadavatele,
- poskytování služeb technické podpory provozu a maintenance IdM po dobu 24 měsíců.

## Představení Evolveum midPoint


Produkt Evolveum midPoint je open-source řešení Identity managementu s otevřeným kódem, bez nutnosti nakupovat licence. Má otevřenou a rozšiřitelnou architekturu založenou na standardech Java, XML a REST. Filosofií produktu je docílit maximální efektivnost při minimálním úsilí.

Historicky je kód midPointu odvozen z kódu OpenIDM 1.6, přičemž se jeho tvůrci snažili o odstranění známých vad, zjednodušení zdrojového kódu a stabilizaci produktu.

Veliký důraz je kladen na neustálý vývoj a implementaci nových funkcionalit, nové verze jsou typicky vydávané 2x-3x ročně.

Při vývoji IdM Evolveum midPoint jsou v maximální míře využívány standardy a frameworky založené na jazyku Java - Spring, Spring Security, Prism Objects, Wicket. Dále je možné využít skriptovací jazyky, jako je například Groovy, JavaScript, Python, XPath v2 a další. K připojení zdrojových a koncových systémů je použito frameworku Identity Connector Framework, dále je možné připojit webové služby SOAP/WSDL. Konektory pro připojení je možné čerpat hned ze tří nezávislých projektů ConnId, OpenICF a Polygon.

Součástí produktu je webové rozhraní, které umožňuje administrátorům konfigurovat IdM midPoint a uživatelům provádět nastavení hesla a zpracování požadavků jako například žádosti o role.

Vývoj produktu midPoint je zastřešen společností Evolveum. Na rozvoji kódu se podílejí i jiné týmy, přičemž společnost Evolveum koordinuje tuto činnost a poskytuje komunitní podporu i placený support. Výhodou společnosti Evolveum je její know-how a cca 11 let zkušeností jejích inženýrů v oblasti IdM implementací, zejména Sun Microsystems.

Díky otevřenosti produktu midPoint je možné jej bezproblémově rozšiřovat a integrovat do něj další požadovanou funkcionalitu. Příkladem takové přidané funkčnosti může být:

- úpravy uživatelského rozhraní,
- SSO,

- distribuce PKI klíčů,
- governance funkce,
- registr business a aplikačních rolí,
- vícefaktorová autentizace,
- správa privilegovaných účtů.

Společnost Evolveum k produktu nabízí možnost zakoupení plné podpory produktu.

Více informací na http://www.evolveum.com/midpoint/

### Vybrané vlastnosti midPoint

Webové rozhraní aplikace midPoint nabízí:

- Kompletní správu Identity managementu – identit uživatelů, rolí, organizačních jednotek, koncových systémů, pravidelných a kontrolních úloh, bezpečnostních politik a dalších konfigurací.
- Samoobslužné rozhraní pro koncové uživatele s přehlednou nástěnkou (dashboard), změnou hesla či registrovaných údajů a žádostmi o role.

IdM umožňuje spravovat identity a jejich zařazení do rolí, do stromů organizačních struktur a funkčních míst. Umožňuje spravovat všechny tyto typy objektů, vytvářet je, měnit jejich atributy či vlastnosti a mazat je, umožňuje nastavit práva pro čtení nebo změnu na jednotlivé atributy objektů. Uživatelům umožňuje vytvářet žádosti o role a schvalovat žádosti ostatních.

Celé uživatelské rozhraní dodaného řešení je v českém jazyce a to včetně nápovědy. Kromě toho řešení obsahuje GUI také v jazycích angličtina, španělština, turečtina a slovenština. Všechny údaje jsou ukládány v kódování UTF-8, IdM umí správně pracovat se všemi znaky (nejen českými).

Podporovány jsou nejnovější verze prohlížeče IE, FireFox, Opera, Google Chrome. GUI zobrazuje uživatelům mimo jiné jejich přiřazení do rolí, zařazení do organizační struktury, navázané aplikace a účty v nich, zobrazuje zadané požadavky, požadavky čekající na schválení. Dále umožňuje uživatelům provést změnu hesla v IdM i v navázaných aplikacích. Vedoucím pracovníkům umožňuje měnit vlastnosti účtů svých podřízených pracovníků, zakládat požadavky na přiřazení rolí pro své podřízené a sledovat jejich stav.

Dále midPoint nabízí diferencovaný přístup jednotlivých uživatelů nebo komunit buď nastavením práv, nebo členstvím v roli, nebo zařazením do organizační struktury, která má nadefinována požadovaná práva. Umožňuje řídit přidělování rolí, zařazování do org. struktury a vytváření přístupů do aplikací např. na základě hodnoty určeného atributu.

IdM umožňuje pracovat s libovolným počtem stromů organizačních struktur. Každá identita může být současně zařazena v libovolném počtu těchto stromů a dokonce může být zařazena současně v několika organizacích v rámci jednoho stromu (např. při souběhu pracovních vztahů nebo souběhu funkcí).

MidPoint má implementován mechanismus nastavování pravidel pro vzájemně se vylučující role. Pokud pak dojde k pokusu o přiřazení role uživateli, který již má jinou konfliktní roli, systém konflikt oznámí a přiřazení role neprovede. Také lze nastavit platnost identity jako takové (od-do, pak je identita zablokována jak v IdM, tak v koncových systémech), umožňuje nastavit časově omezené přiřazení uživatele do role, nebo časově omezené přiřazení do stromu v organizační struktuře.

IdM umožňuje nastavit připojení do aplikací tak, aby byl tok dat jednosměrný z aplikace do IdM, jednosměrný z IdM do aplikace, nebo obousměrný. Směry toku dat lze libovolně kombinovat až na úroveň jednotlivých atributů. Aplikace rovněž nativně obsahuje mechanismus pro vyrovnání se s aktuální nedostupností koncového systému, nevyřízené operace jsou dočasně uloženy do objektu v IdM a provedeny až po obnovení komunikace s koncovým systémem.

MidPoint obsahuje reportovací modul a auditní modul, jejichž úkolem je zaznamenávat veškeré činnosti jak v rámci IdM, tak směrem ke koncovým systémům. Standardní součástí je podrobný auditní report o všech činnostech v IdM, dále report o uživatelích, přidělených rolích a zařazení do org. struktury a report o rekonciliacích z připojených aplikací.

Vývoj produktu je díky open-source povaze velmi otevřený a transparentní, důkazem je veřejně dostupná road-mapa s komentáři a prioritami výrobců software:

https://jira.evolveum.com/browse/MID

## Online demo

Společnost Evolveum ve svém internetovém prostředí nabízí funkční online demo aplikace midPoint verze 3.1.1. Nabízená verze v tomto řízení je 3.2.

URL: http://demo.evolveum.com

Login: Administrator

Heslo: 5ecr3t

Návod: https://wiki.evolveum.com/display/midPoint/Live+Demo

## Servisní podpora a SLA

Pro spolehlivý provoz řešení doporučujeme podporu, která zajistí garanci základních servisních parametrů. Nabízíme podporu v režimu 5x8, tj. v pracovní době 9:00 – 17:00 v pracovních dnech. Součástí jsou následující položky:

- garance reakční doby,
- garance odstranění vady,
- hlášení požadavků v helpdesku /telefonicky,
- měsíční report zákazníkovi.

SLA bude splňovat následující parametry:

| Kategorie vady | Reakční doba | Odstranění vady |
|---|---|---|
| Vysoká | 4 hodiny | 8 hodin |
| Střední | 8 hodin | 32 hodin |
| Nízká | 16 hodin | dle dohody |

Všechny hodiny uvedené v tabulce jsou počítány v rámci pracovní doby. Reakční dobou se rozumí doba od zahájení požadavku do doby potvrzení zahájení jeho řešení.

### Specifikace kategorií vad:

- Kategorie vady „vysoká“, tj. vady zabraňující provozu – systém není použitelný ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující činnost systému. Tento stav může ohrozit běžný provoz zadavatele a nelze jej dočasně řešit organizačním opatřením.
- Kategorie vady „střední“, tj. vady omezující provoz – funkčnost systému je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz zadavatele. Jedná se také o vady způsobující problémy při užívání a provozování systému nebo jeho části, ale umožňující provoz, jimiž způsobené problémy lze dočasně řešit organizačními opatřeními.
- Kategorie vady „nízká“, tj. vady neomezující provoz – znamená drobné vady, které nespadají do kategorií „vysoká“ nebo „střední“.

Zařazení vady do jednotlivých kategorií určuje zadavatel.

Součástí této nabídky je 192 hodin prací, které je možné využít na jakékoli činnosti související s předmětem smlouvy po dobu platnosti smlouvy. Jakékoli práce na požadavcích s výjimkou oprav záručních vad budou odečítány z tohoto objemu hodin, případně po jeho vyčerpání mohou být objednány na základě hodinové sazby.