**Smlouva o DODÁVCE**

**č. OVZ/VZZR/2025/003-1**

uzavřená dle ustanovení § 1746 odst. 2 s přihlédnutím k § 2586 a násl. zákona č. 89/2012 Sb.,

Občanský zákoník, v platném znění (dále jen občanský zákoník)

**Smluvní strany**

**Objednatel: Statutární město Pardubice**

Se sídlem: Pernštýnské náměstí 1

530 21 Pardubice

Zastoupený ve věcech smluvních:

Bc. Janem Nadrchalem, primátorem města

Zastoupený ve věcech technických:

Ing. Davidem Bakrlíkem, vedoucím odd. technické podpory Odboru informačních technologií MmP, tel. XXX XXX XXX, e-mail: [xxxxxxxxxxxx@mmp.cz](mailto:xxxxxxxxxxxx@mmp.cz)

IČO: 00274046 DIČ: CZ00274046

bankovní spojení: KB, a.s., Pardubice

číslo účtu: 326-561/0100

*(dále jen „objednatel“)*

a

**Dodavatel: Aricoma Systems a.s.**

Se sídlem: Hornopolní 3322/34, 702 00 Ostrava

Zastoupen: Jaroslavem Dvořákem, členem představenstva

Zastoupený ve věcech smluvních: Jaroslavem Dvořákem, členem představenstva

Kontaktní osoba: Petr Papoušek

Tel: XXX XXX XXX e-mail : [xxxxxxxxxxxx@aricoma.com](mailto:xxxxxxxxxxxx@aricoma.com)

IČO: 04308697 DIČ: CZ04308697

společnost je zapsána v obchodním rejstříku vedeném u Krajského soudu v Ostravě, oddíl B, vložka 11012

bankovní spojení: Česká spořitelna a.s.

číslo účtu: 6563752 / 0800

*(dále jen „dodavatel“)*

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu (dále jen „smlouva“):

**Kybernetická bezpečnost Pardubice –**

**posílení informačních systémů (IS) v rámci zabezpečení kyberbezpečnosti**

**ČÁST1: Identity management systém (IDM - IAM)**

**čl. I**

**Předmět smlouvy**

1. Předmětem plnění dle této smlouvy je dodávka a implementace Identity and Access management včetně řízení autentizace (IDM - IAM), který umožní správu identit, automatizovaný životní cyklus účtů a jejich oprávnění v řadě provozovaných systémů v prostředí Magistrátu města Pardubic. Implementace části Access managementu rozšíří stávající procesy správy, identifikace, autorizace a autentizace všech uživatelů a identit v rámci infrastruktury - dle specifikace uvedené v příloze č. 1 této smlouvy.

Součástí předmětu plnění dle této smlouvy je:

• Předimplementační analýza a vytvoření prováděcího dokumentu,

• Implementace IDM-IAM v testovacím a produkčním prostředí,

• Implementace požadovaných funkcionalit systémů,

• Integrace na systémy dle požadavků na konektory specifikované v rámci funkčních požadavků,

• Úspěšné provedení akceptačních testů,

• Předání Dokumentace skutečného provedení, databázového modelu a popis všech konektorů

včetně vazeb,

• Předání Administrátorské příručky,

• Předání Uživatelské příručky,

• Zaškolení 3 správců v rozsahu 3 dnů,

• Podpora a servis řešení na období 5 let,

• Délka implementace maximálně 120 dnů.

1. Dodavatel se zavazuje sjednaný předmět plnění a s tím související služby dodat a provést s odbornou péčí v rozsahu a za podmínek sjednaných v této smlouvě.
2. Předmět plnění musí být proveden v souladu s touto smlouvou a nesmí mít nedostatky, které brání použití k určenému účelu.
3. **Dodavatel bere na vědomí, že objednatel hodlá max. využít k realizaci akce podpory Evropské unie prostřednictvím Národního plánu obnovy / Ministerstva vnitra ČR z 41. výzvy – Kybernetická bezpečnost obce dle Obecných pravidel pro žadatele a příjemce vč. příloh** [**https://www.mvcr.cz/npo/narodni-plan-obnovy-web-dokumenty.aspx**](https://www.mvcr.cz/npo/narodni-plan-obnovy-web-dokumenty.aspx)

5. Předmět plnění bude proveden v rozsahu podle zadávací dokumentace zakázky:

- v rozsahu zadávacích podmínek veřejné zakázky,

- dle nabídky dodavatele podané dne 09.01.2025.

6. **Nejedná se o práce uvedené v číselníku CZ-CPA 41-43, který je součástí Klasifikace produkce zavedené Českým statistickým úřadem platné ke dni podpisu této smlouvy. Platné znění** [**Klasifikace produkce (CZ-CPA)**](http://www.czso.cz/csu/klasifik.nsf/i/klasifikace_produkce_%28cz_cpa%29) **je dostupné na stránkách Českého statistického úřadu.**

1. Dodavatel se zavazuje pro objednatele zajistit a provést dodávku předmětu plnění, na svůj náklad a na vlastní odpovědnost v termínu, rozsahu a za podmínek sjednaných v této smlouvě. Objednatel se zavazuje řádně provedený předmět plnění v souladu s touto smlouvou převzít a zaplatit cenu ve výši, způsobem a za podmínek uvedených v této smlouvě.
2. Součástí předmětu plnění je veškerá činnost dodavatele nezbytná k realizaci předmětu plnění a ke zdárné, kompletní a k danému účelu provozuschopné dodávce předmětu plnění.
3. Součástí ceny předmětu plnění uvedené v čl. III. této smlouvy jsou veškeré náklady spojené s bezvadnou a kompletní dodávkou předmětu plnění, které lze při realizaci předmětu plnění předpokládat např. dopravné apod.
4. Zadávání případných změn předmětu plnění bude realizováno v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.
5. Veškeré změny předmětu plnění musí být provedeny formou dodatku v elektronické verzi k této smlouvě opatřeného elektronickým podpisem obou smluvních stran.

**čl. II**

**doba a místo plnění**

1. Dodavatel se zavazuje dodat objednateli kompletní předmět plnění do místa plnění uvedeného v odst. 2 tohoto článku této smlouvy v termínu:

1.1.Termín zahájení plnění: **dnem nabytí účinnosti této smlouvy**

* 1. Termín dodání dodávky a implementace předmětu plnění včetně související dokumentace a zaškolení pracovníků objednatele dle přílohy č. 1 a č. 2 této smlouvy:

**do 120 dnů ode dne účinnosti této smlouvy.**

* 1. Poskytnutí služeb servisní a technické podpory řešení dle přílohy č. 2 této smlouvy:

**po dobu 5 let ode dne potvrzení podpisu akceptačního protokolu objednatelem**

1. Místo předmětu plnění dle této smlouvy:

Magistrát města Pardubic, Odbor informačních technologií, Štrossova 44, Pardubice

1. Strany smlouvy se dále dohodly, že pokud by v průběhu realizace dodávek předmětu plnění došlo k prodlení s plněním z důvodu neočekávaných okolností, které nastaly bez zavinění některého z účastníků ve smyslu § 2913 odst. 2 občanského zákoníku (vyšší moc – válka, mobilizace, zemětřesení, pád letadla a jiné), prodlužuje se termín plnění o stejný počet dní trvání těchto okolností. Smluvní strana, která se o takových okolnostech dozví, je povinna neprodleně písemně informovat druhou smluvní stranu, nesplní-li tuto povinnost, není oprávněna se těchto okolností dovolávat. Bude-li z těchto důvodů prodlení na straně dodavatele trvat déle než 15 dní, je objednatel oprávněn od této smlouvy odstoupit. Dodavatel je povinen pokračovat v dodání předmětu plnění bezodkladně poté, co důvod přerušení odpadne, v případě, že tak neučiní do dvou pracovních dnů poté, co důvod přerušení odpadl, je objednatel oprávněn od této smlouvy odstoupit.
2. Po dobu prodlení jedné smluvní strany s plněním jejích povinností stanovených touto smlouvou, není druhá strana v prodlení s plněním svých povinností, pokud jejich realizace je podmíněna splněním povinností, s jejichž plněním je druhá strana v prodlení.
3. Dodavatel je oprávněn provést dodávku předmětu plnění i před sjednaným termínem, pokud to postup prováděných dodávek a souvisejících služeb v místě plnění dovolí. V tomto případě se objednatel zavazuje poskytnout dodavateli potřebnou součinnost a předmět plnění dodaný ve zkráceném termínu převzít, pokud nevykazuje vady a žádné nedodělky.

**čl. III**

**cena za předmět plnění**

1. Cena za kompletní, řádné a včasné dodání předmětu plnění je nejvýše přípustná, platná po celou dobu realizace a obsahuje veškeré dodávky, práce, činnosti a náklady související s realizací předmětu plnění dle této smlouvy, a je uvedena v tomto členění:

**Celková cena bez DPH 4.932.000,-- Kč**

DPH 21% 1.035.720,-- Kč

Celková cena vč. DPH 5.967.720,--Kč

Podrobné členění ceny za předmět plnění je uvedeno v příloze č. 2 této smlouvy.

2. V ceně jsou zahrnuty veškeré náklady dodavatele související s realizací předmětu plnění dle této smlouvy.

3. Případné změny předmětu plnění dle této smlouvy musí být realizovány v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů a před jejich realizací písemně odsouhlaseny oprávněným pracovníkem objednatele a následně potvrzeny formou písemného dodatku v elektronické podobě opatřených elektronickým podpisem obou smluvních stran. Veškeré dodávky a práce s tím spojené, které by dodavatel provedl nad rámec předmětu této smlouvy, aniž by byl uzavřen tento dodatek, není objednatel povinen dodavateli uhradit.

**čl. IV**

**platební podmínky**

* + - 1. Objednatel nebude poskytovat dodavateli zálohy.

1. Objednatel se zavazuje zaplatit dílčí část smluvní ceny za dodávku a implementaci, konfiguraci, zaškolení a dokumentaci v rozsahu dle přílohy č. 1 a č. 2 na základě daňového dokladu – faktury vystavené Dodavatelem. Právo Dodavatele vystavit daňový doklad – fakturu vzniká řádným dodáním Předmětu plnění, o čemž bude mezi smluvními stranami vyhotoven předávací protokol, který bude nedílnou součástí daňového dokladu.

Splatnost daňového dokladu bude 30 dnů ode dne jeho prokazatelného doručení Objednateli. Přílohou daňového dokladu musí být předávací protokol podepsaný Objednatelem, jinak není Objednatel povinen celkovou smluvní cenu uhradit. Předávací protokol musí obsahovat sdělení, že předmět smlouvy byl odevzdán Objednateli řádně a včas. Dodavatel je povinen doručit objednateli daňový doklad nejpozději do 10-ti dnů od data uskutečnění zdanitelného plnění.

1. Objednatel se zavazuje zaplatit dílčí část smluvní ceny za dodavatelem poskytnuté služby servisní a technické podpory řešení v délce 5 let od od podpisu akceptačního protokolu s parametry dle přílohy č. 1 - na základě daňových dokladů – faktur vystavených Dodavatelem, a to za každý 1 rok poskytování služeb servisní a technické podpory řešení dle této smlouvy.

Splatnost daňového dokladu bude 30 dnů ode dne jeho prokazatelného doručení Objednateli. Dodavatel je povinen doručit objednateli daňový doklad nejpozději do 10-ti dnů od data uskutečnění zdanitelného plnění.

1. Fakturované částky budou hrazeny bezhotovostně, a to bankovním převodem na účet dodavatele uvedený v této smlouvě.
2. Fakturovaná částka se považuje za uhrazenou dnem, kdy bude odepsána z účtu objednatele ve prospěch účtu dodavatele.
3. Faktury musí obsahovat všechny náležitosti daňového dokladu stanovené platnými právními předpisy.

7. Faktury dodavatele musí obsahovat všechny obvyklé náležitosti platebních dokladů stanovené zákonem o DPH a občanským zákoníkem, zejména:

* označení faktury a číslo,
* obchodní název a sídlo objednatele a dodavatele, jejich IČO a DIČ,
* předmět plnění a den splnění,
* den vystavení faktury, den uskutečnění zdanitelného plnění a lhůtu splatnosti,
* označení banky a číslo účtu, na který má být placeno,
* fakturovanou částku a další náležitosti podle zákona č. 235/2004 Sb., o DPH, včetně razítka dodavatele a podpisu oprávněné osoby dodavatele,
* označení a číslo dotačního projektu,
* údaje pro daňové účely.
* jako přílohu oboustranně odsouhlasený protokol o předání a převzetí předmětu plnění a zápis o odstranění vad a nedodělků.

8. V případě, že faktura vystavená dle tohoto článku bude obsahovat nesprávné nebo neúplné údaje a nebude obsahovat všechny náležitosti uvedené v čl. IV odst. 7. této smlouvy, je objednatel oprávněn fakturu vrátit do termínu její splatnosti. Dodavatel podle charakteru nedostatků fakturu opraví, nebo vystaví novou. Vrácením faktury se ruší původní lhůta splatnosti. Nová lhůta splatnosti běží znovu ode dne prokazatelného doručení opravené faktury objednateli.

9. Objednatel provede úhradu ve splatnosti na bankovní účet dodavatele uvedený na faktuře za předpokladu, že dodavatel nebude ke dni uskutečnění zdanitelného plnění zveřejněný správcem daně jako nespolehlivý plátce v Registru plátců DPH. Pokud dodavatel bude zveřejněný správcem daně jako nespolehlivý plátce, objednatel uhradí dodavateli pouze částku bez DPH a DPH bude uhrazeno místně příslušnému správci daně dodavatele.

11. Objednatel provede úhradu ve splatnosti na bankovní účet dodavatele uvedený na faktuře za předpokladu, že tento účet bude ke dni platby zveřejněný správcem daně v Registru plátců DPH.

V případě, že tato podmínka nebude splněna, objednatel uhradí pouze částku bez DPH a doplatek bude uhrazen dodavateli až po zveřejnění čísla účtu. V případě, že účet nebude zveřejněn po uplynutí lhůty stanovené objednatelem, bude DPH uhrazeno místně příslušnému správci daně dodavatele.

12. Fakturu lze doručit elektronicky do datové schránky MmP na adresu: **ukzbx4z** nebo e-mailem na adresu: [**xxxxxx@mmp.cz**](mailto:xxxxxx@mmp.cz), případně zaslat poštou nebo prostřednictvím jiné osoby, která provádí přepravu zásilek (kurýrní služba), na adresu objednatele či předat osobně na podatelnu v sídle objednatele.

**čl. V**

**Odevzdání a převzetí místa plnění**

* 1. Místo plnění pro dílčí předmět plnění - dodávku a pro instalaci předmětu plnění bude dodavateli předáno po nabytí účinnosti této smlouvy, nebude-li mezi smluvními stranami dohodnuto jinak.
  2. Dodavatel je povinen udržovat místo provádění prací trvale v dobrém stavu, opatření k maximálnímu omezení prašnosti, hluku, ochraně životního prostředí a dodržování předpisů BOZP při realizaci předmětu plnění a je povinen zajistit bezpečnost svých pracovníků při provádění předmětu plnění. V případě porušení této povinnosti je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 5.000,- Kč za každé jednotlivé porušení této povinnosti a dále uhradit veškeré sankce, které by byly v důsledku porušení těchto povinností vyměřeny příslušnými orgány.
  3. Dodavatel je povinen udržovat na převzatém místě plnění pořádek a čistotu a je povinen odstraňovat odpady a nečistoty vzniklé jeho pracemi na své náklady. Dodavatel se zavazuje, že bude dodržovat zásady ochrany životního prostředí podle zákonů č. 17/1992 Sb., o životním prostředí, č. 114/1992 Sb., o ochraně přírody a krajiny, č. 541/2020 Sb., o odpadech, ve znění jejich pozdějších změn a předpisů. Všechen odpad činností dodavatele (např. obalový materiál apod.) bude dodavatel třídit, evidovat a následně zajistí likvidaci tohoto odpadu oprávněnou společností. Všechny tyto činnosti je povinen provádět na své náklady.
  4. Dodavatel je povinen seznámit se s riziky v místě plnění, upozornit na ně své pracovníky a určit způsob ochrany a prevence proti úrazům a jinému poškození zdraví.

5. Dodavatel odpovídá za veškeré škody, které by objednateli či třetím osobám v důsledku realizace předmětu plnění dle této smlouvy vznikly.

**čl. VI**

**KVALIFIKAČNÍ podmínky**

1. Dodavatel se zavazuje sjednaný předmět plnění provést s odbornou péčí v rozsahu stanoveném zadávací dokumentací, přitom je povinen dodržet příslušné technické normy, vztahující se k předmětu plnění. Předmět plnění musí být proveden v souladu s touto smlouvou a nesmí mít nedostatky, které brání použití předmětu plnění k určenému účelu.
2. Dodávka předmětu plnění a s tím související práce mohou být prováděny pouze kvalifikovanými pracovníky a firmami, které se mohou prokázat příslušnou kvalifikací. V případě porušení této povinnosti je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 5.000,--Kč za každé jednotlivé porušení povinnosti. Doklad o kvalifikaci pracovníků je dodavatel na požádání objednatele povinen doložit i v průběhu provádění předmětu plnění, neučiní-li tak na výzvu objednatele, má se za to, že povinnost dle předchozí věty nesplnil.
3. Předmět plnění bude dále proveden a dokladován v souladu se všemi právními normami, ČSN a vyhláškami. Všechny použité materiály a výrobky musí mít platný certifikát ve smyslu zákona a platných vyhlášek.

**čL. VII**

**povinnosti dodavatele**

1. Dodavatel je při plnění povinností vyplývajících ze smlouvy povinen postupovat s vynaložením odborné a veškeré potřebné péče. Dodavatel je povinen řídit se při plnění smlouvy příslušnými předpisy a je rovněž vázán odůvodněnými pokyny objednatele, které mu budou zadávány v průběhu plnění této smlouvy. Dodavatel je povinen upozornit objednatele na nevhodnou povahu těchto pokynů.
2. Dodavatel se zavazuje, že pokud při provádění předmětu plnění dle ustanovení této smlouvy zjistí z titulu své odbornosti, že pro bezchybné provedení a dodávku předmětu plnění co do rozsahu a funkčnosti je nezbytné provést další činnosti, které nejsou zahrnuty v předmětu plnění této smlouvy, bude o tom neprodleně informovat objednatele. V případě, že objednatel neuzná požadavek dodavatele na provedení dalších činností důvodným a mezi stranami nebude uzavřen dodatek o změně předmětu smlouvy, je dodavatel povinen provést předmět plnění tak, jak je vymezeno touto smlouvou.
3. Dodavatel se zavazuje v rámci předmětu plnění dle této smlouvy dodržovat obecně závazné právní předpisy, technické normy (ČSN), týkající se zejména bezpečnosti a ochrany zdraví při práci, požární ochrany a ochrany životního prostředí. V případě porušení těchto povinnosti je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 5.000,-- Kč za každé jednotlivé porušení této povinnosti a dále uhradit veškeré sankce, které by byly v důsledku porušení těchto povinností vyměřeny příslušnými orgány.
4. Dodavatel se zavazuje při provádění předmětu plnění šetřit práv třetích osob a postupovat vždy v souladu se zákonem, přičemž je plně odpovědný za veškeré zásahy do práv třetích osob, jichž by se při realizaci předmětu plnění dopustil.
5. Dodavatel je povinen zajistit, aby plněním povinností dle smlouvy nepřiměřeně nenarušoval provoz a činnosti uživatele objektu úřadu. V případě porušení těchto povinnosti je objednatel oprávněn uplatnit vůči dodavateli smluvní pokutu ve výši 5.000,-- Kč za každý jednotlivý zjištěný případ.
6. Dodavatel je povinen chránit majetek objednatele a je plně zodpovědný za škody, které vznikly z jeho činnosti v souvislosti s plněním předmětu smlouvy. Způsobí-li dodavatel při provádění prací škodu na majetku objednatele, bude odpovědný za nápravu takové škody na vlastní náklady. Možnost poskytnutí náhrady cestou pojistného plnění z příslušné pojistky dodavatele tím není dotčeno. Dodavatel je odpovědný za škodu na majetku i na zdraví, kterou při plnění povinností ze smlouvy případně způsobí i třetím osobám.

7. Dodavatel je povinen při plnění sjednaném smlouvou zabezpečit veškeré své činnosti tak, aby byly vždy dodržovány předpisy BOZP, hygieny práce, protipožární ochrany, životního prostředí a předpisy upravující nakládání s odpady. V případě porušení těchto povinnosti je objednatel oprávněn uplatnit vůči dodavateli smluvní pokutu ve výši 5.000,-- Kč za každý jednotlivý zjištěný případ.

8. Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných objednatelem na datovém nosiči. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena objednatelem. V případě porušení těchto povinností je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 5.000,-- Kč za každé jednotlivé porušení těchto povinností.

1. Dodavatel se zavazuje, že bude nakládat s odpady vzniklými v průběhu plnění smlouvy dle zákona č. 541/2020 Sb., o odpadech, a dle prováděcích vyhlášek k tomuto zákonu.

V případě porušení této povinnosti je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 5.000,-- Kč za každé jednotlivé porušení této povinnosti.

1. Objednatel je oprávněn sám, nebo prostřednictvím oprávněných osob kontrolovat plnění této smlouvy ze strany dodavatele. Zjistí-li objednatel, že dodavatel postupuje v rozporu se svými povinnostmi, je objednatel oprávněn dožadovat se toho, aby dodavatel ve stanovené lhůtě odstranil vady vzniklé vadným plněním předmětu smlouvy a dále postupoval řádným způsobem.
2. Dodavatel se zavazuje informovat objednatele o veškerých prováděných dodávkách a s tím souvisejících pracích, které mají zásadní význam pro kvalitu plnění dle této smlouvy a přizvat k nim zástupce objednatele ve věcech technických minimálně 3 dny předem.
3. Smluvní strany jsou si vědomy, že jednotlivé kontroly ze strany objednatele nezbavují dodavatele odpovědnosti za řádné a včasné předání předmětu plnění.
4. Technický dozor objednatele je oprávněn přerušit dodávky a s tím související práce v případě, je-li závažným způsobem ohrožena bezpečnost jeho pracovníků nebo dodavatel závažným způsobem porušuje své povinnosti plynoucí mu z této smlouvy. O dobu, po kterou bylo nutno dodávky a s tím související práce přerušit, se neprodlužuje lhůta stanovená pro dokončení předmětu plnění. Dodavatel nemá nárok na úhradu nákladů spojených s přerušením dodávek a s tím souvisejících prací.
5. Dodavatel prohlašuje, že má k datu podpisu této smlouvy uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou dodavatelem objednateli či třetí osobě v souvislosti s výkonem jeho činnosti ve výši nejméně **10.000.000,- Kč** a jejíž kopie nebo kopie pojistného certifikátu byla poskytnuta objednateli. Dodavatel se zavazuje, že po celou dobu provádění předmětu plnění a po dobu záruky bude pojištěn ve smyslu tohoto ustanovení a že nedojde ke snížení pojistného plnění pod částku uvedenou v předchozí větě. Stejné podmínky je dodavatel povinen zajistit u svých případných poddodavatelů.

Při porušení jakékoliv shora uvedené povinnosti, je dodavatel povinen objednateli uhradit jednorázovou smluvní pokutu ve výši 20.000,-- Kč. V tomto případně je dále objednatel oprávněn od této smlouvy odstoupit.

1. V případě pojistné události jsou smluvní strany povinny neodkladně si vzájemné poskytnout nezbytnou součinnost, zejména sdělit si potřebné údaje, resp. přijmout veškerá opatření, která jsou podle pojistné smlouvy potřebná k vyplacení plnění z pojistné smlouvy.
2. Dodavatel je povinen dodržovat veškeré právní předpisy, včetně předpisů týkajících se bezpečnosti práce a technických zařízení, zejména zákona č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších bezpečnostních podmínek bezpečnosti a ochrany zdraví při práci), nařízení vlády č. 362/2005 Sb., o bližších požadavcích na bezpečnost a ochranu zdraví při práci na pracovištích s nebezpečím pádu z výšky nebo do hloubky a nařízení vlády č. 591/2006 Sb., o bližších minimálních požadavcích na bezpečnost a ochranu zdraví při práci na staveništích. Dodavatel přejímá v plném rozsahu odpovědnost za řízení postupu prací, za bezpečnost a ochranu zdraví osob v místě plnění, požární ochrany a za zachování pořádku na místě plnění. V případě porušení takové povinnosti je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 20.000,- Kč za každý jednotlivý zjištěný případ porušení této povinnosti.
3. Dodavatel je povinen zajistit, že jím poskytované plnění dle této Smlouvy, odpovídá všem požadavkům vyplývajícím z platných a účinných právních předpisů či příslušných norem, které se na dané plnění vztahují. Dodavatel se zavazuje, že při plnění předmětu Smlouvy bude dbát o dodržování důstojných pracovních podmínek osob, které se na jejím plnění budou podílet, a ve vztahu k zaměstnancům bude zajištěno důsledné dodržování pracovněprávních předpisů, a to zejména, nikoliv však výlučně, předpisů upravujících mzdy zaměstnanců (včetně odpovídající odměny za případnou práci přesčas, práci ve svátek atp.), pracovní dobu, dobu odpočinku mezi směnami, bezpečnost práce apod. Dodavatel se zavazuje v souvislosti s touto povinností za účelem kontroly na výzvu Objednatele předložit (či zajistit předložení) příslušných dokladů (zejména, nikoli však výlučně pracovněprávních smluv), a to bez zbytečného odkladu od doručení výzvy, nejpozději však do 2 pracovních dnů. Totožné musí být zajištěno ze strany příp. poddodavatelů.
4. Dodavatel v plné míře zodpovídá za bezpečnost a ochranu zdraví všech osob v prostoru místa plnění, které se zde nacházejí oprávněně a zabezpečí jejich vybavení ochrannými pracovními pomůckami. Dodavatel je povinen zajistit bezpečnost práce a provozu podle platných právních předpisů a norem bezpečnostních, hygienických, požárních a ekologických. Za každý zjištěný případ porušení povinnosti v oblasti bezpečnosti práce a ochrany zdraví, ochrany životního prostředí stanovených závaznými předpisy zaplatí dodavatel objednateli smluvní pokutu ve výši 5.000,- Kč.
5. Dodavatel je oprávněn najmout si na své vlastní náklady poddodavatele, pro účely provedení některé části předmětu plnění dle této Smlouvy za předpokladu, že nedojde k porušení závazných předpisů, a že v takovém případě bude dodavatel odpovědný objednateli za jakoukoli takto dodávanou nebo prováděnou část svých povinností vyplývajících z této Smlouvy, jako kdyby je poskytoval dodavatel sám. Dodavatel je také odpovědný za koordinaci poddodavatelů.
6. Dodavatel je povinen vyklidit místo plnění do 2 kalendářních dnů po dokončení dodávky a s tím souvisejících prací, pokud nebude dohodnuto s objednatelem jinak, a protokolárně jej předá objednateli. Po uplynutí této lhůty může dodavatel na místě plnění ponechat pouze nástroje a zařízení, případně materiál potřebný k odstranění případných vad a nedodělků. V případě prodlení se splněním této povinnosti je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 5.000,- Kč za každý i započatý den prodlení.

**čl. VIII**

**Součinnost objednatele**

1. Objednatel nebo jím pověřený zástupce je oprávněn kontrolovat provádění předmětu plnění. Zjistí-li objednatel, že dodavatel provádí předmět plnění v rozporu se svými povinnostmi, je objednatel oprávněn dožadovat se toho, aby dodavatel odstranil vady vzniklé vadným prováděním a předmět plnění prováděl řádným způsobem. Jestliže dodavatel tak neučiní ani v přiměřené lhůtě mu k tomu poskytnuté a postup dodavatele by vedl nepochybně k porušení smlouvy, je objednatel oprávněn od smlouvy odstoupit.
2. Pokud dodavatel upozorní na nevhodnou povahu věcí přebíraných od objednatele, nebo na nevhodnou povahu pokynů nebo podkladů předaných objednatelem, je objednatel povinen vznesené připomínky bezodkladně zvážit a vydat písemné rozhodnutí v takové lhůtě, aby nebyl ohrožen plynulý průběh dodávek a s tím spojených prací. Totéž platí, zjistí-li se skryté překážky bránící provádění dodávek dohodnutým způsobem, které nebyly patrny ze zadávací dokumentace.
3. Objednatel vykonává v místě plnění občasný technický dozor a v jeho průběhu sleduje zejména, zda dodávky a práce s tím spojené jsou prováděny v souladu se smlouvou a podle zadávací dokumentace, technických norem a jiných právních předpisů. Na nedostatky zjištěné v průběhu prací neprodleně prokazatelně upozorní dodavatele písemnou zprávou, kterou zašle do datové schránky dodavatele, ale i elektronickou poštou na shora uvedené kontakty dodavatele.
4. Technický dozor objednatele není oprávněn zasahovat do činnosti dodavatele, je však oprávněn vydat pracovníkům dodavatele příkaz přerušit dodávky a práce s tím spojené na dobu nezbytně nutnou, pokud odpovědný zástupce dodavatele není dosažitelný, a je-li ohrožena bezpečnost v místě plnění, život nebo zdraví pracujících v místě plnění, nebo dodavatel provádí předmět plnění vadně či v rozporu s požadavky a potřebami objednatele. Další postup bude upřesněn na základě jednání smluvních stran a pokynů objednatele.
5. Objednatel je oprávněn na základě skutečností dodatečně zjištěných v průběhu prací upřesnit obsah a způsob provedení dodávek a s tím souvisejících prací.
6. Objednatel a dodavatel se dohodli, že aplikace ustanovení § 2591 a § 2595 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, se vylučuje.

**čl. IX**

**věci určené k realizaci předmětu smlouvy**

1. Veškeré základní energie a média potřebná pro realizaci předmětu plnění v místě plnění se zavazuje objednatel dodavateli poskytnout bezúplatně.
2. V průběhu realizace předmětu smlouvy bude dodavatel udržovat čistotu a pořádek v místě plnění a je povinen při realizaci plnění dle této smlouvy postupovat tak, aby nevznikly žádné škody na životním prostředí, majetku objednatele či majetku třetích osob.
3. Dodavatel bude chránit majetek objednatele (ať již mu byl svěřen do užívání nebo je umístěn v objektu objednatele) a bude plně zodpovědný za škody, které vznikly z jeho činnosti v souvislosti s plněním předmětu smlouvy, a to dle čl. VII odst. 6. této smlouvy.
4. Dodavatel se zavazuje na svůj náklad uvést dotčené plochy místa plnění a jejich okolí do původního stavu, zejména odvést a v souladu s právními předpisy zlikvidovat odpad, který vznikl, nevyužitý materiál apod. Původní stav před zahájením prací dodavatel prokazatelně zdokumentuje.

**čl. X**

**vlastnické právo a přechod nebezpečí škody**

1. Objednatel se stává vlastníkem dodaného, smontovaného a zkompletovaného vybavení okamžikem, kdy dojde k protokolárnímu převzetí předmětu plnění. Nebezpečí škody po celou dobu provádění předmětu plnění nese dodavatel až do předání předmětu plnění a vyklizeného místa plnění objednateli.
2. Dodavatel je povinen na vlastní náklady zabezpečit ochranu dodávaného předmětu plnění a veškerého materiálu dovezeného na místo plnění pro realizaci prací proti poškození a odcizení.

**čl. XI**

**PŘEDÁNÍ A PŘEVZETÍ PŘEDMĚTU SMLOUVY**

1. Závazek dodavatele dodat předmět smlouvy je splněn jeho dodáním bez vad a nedodělků, včetně řádné instalace předmětu plnění v rozsahu sjednaném touto smlouvou a protokolárním předáním objednateli v dohodnutém čase, místě a kvalitě.
2. Objednatel je povinen řádně dokončený předmět plnění případně i jeho dílčí část převzít, je-li prosta vad a nedodělků. Má-li předávaný předmět plnění nebo jeho dílčí část nedodělky, vady, a to i vady nebránící užívání vady nebo nedodělky, není řádně dokončený, a objednatel je oprávněn předmět plnění nepřevzít a dodavatel je v takovém případě v prodlení s plněním předmětu plnění. Předmět plnění se považuje za dokončený až poté, co budou dokončeny veškeré dodávky předmětu plnění bez vad a nedodělků a s tím spojené instalační práce a dojde k předání předmětu plnění.
3. K zahájení přejímacího řízení předmětu plnění dodavatel písemně vyzve oprávněného zástupce objednatele pro předání a převzetí dodávky nejméně 3 pracovní dny před zahájením přejímky. Oprávněnými zástupci pro předání a převzetí předmětu plnění jsou:

za objednatele :

Ing. David Bakrlík – vedoucí oddělení technické podpory, Odbor informačních technologií MmP

za dodavatele : Petr Papoušek – ředitel pobočky Aricoma Systems a.s Pardubice

1. O předání a převzetí předmětu plnění se sepíše předávací protokol. Předávací protokol musí obsahovat alespoň:

* popis předávaného předmětu plnění;
* soupis předaných dokladů;
* soupis vad, pokud je předávaný předmět plnění vykazuje;
* způsob odstranění případných vad;
* lhůta k odstranění případných vad;
* datum vyhotovení;
* jména a podpisy oprávněných osob smluvních stran, které předání a převzetí provedly;

1. Dodavatel je povinen předat objednateli veškeré objednatelem požadované doklady a dokumentaci dle přílohy č. 1 této smlouvy, které jsou nutné k užívání předmět plnění v okamžiku jeho převzetí objednatelem.
2. Objednatel má právo převzetí předmětu plnění nebo jeho části odmítnout, jestliže vykazuje vady, nedodělky nebo nebyly odstraněny vady vytýkané v průběhu realizace předmětu plnění; objednatel není povinen převzít předmět plnění i tehdy, vykazuje-li jen vady, které nebrání tomu, aby část předmětu plnění svému účelu. Jestliže objednatel převezme předmět plnění s vadami a nedodělky, ač k tomu nebyl povinen, je dodavatel povinen uvést jím realizovanou část předmětu plnění do bezvadného a úplného stavu a odstranit veškeré případné vady a/nebo nedodělky uvedené v předávacím protokolu do 14 dnů ode dne převzetí předmět plnění, nedohodnou-li se smluvní strany písemně jinak. Převzetím předmět plnění s vadami není dotčeno ustanovení smlouvy o smluvní pokutě.
3. Až do okamžiku odstranění poslední vady dodáním předmětu plnění dle této smlouvy se nepovažuje za řádně dodaný.
4. Pokud dodavatel neuzná některou z vad vytknutých objednatelem, bude vytčená vada dána k posouzení autorizovanému znalci jmenovanému objednatelem. Jeho názorem se strany zavazují řídit. V případě, že tato osoba vadu, byť částečně potvrdí, hradí veškeré náklady spojené s posouzením vady dodavatel. V opačném případě uhradí tyto náklady objednatel.
5. Nedokončí-li dodavatel předmět plnění dle této smlouvy řádně ve stanoveném termínu, je objednatel oprávněn tuto část předmětu plnění dokončit prostřednictvím odborně způsobilé osoby, a to na náklady dodavatele. To platí i pro případ předání předmětu plnění Objednateli, vykazuje-li předaný předmět plnění nebo jeho část vady, jež dodavatel v přiměřené lhůtě po jejich vytknutí neodstranil.

**čl. XII**

**záruka za jakost**

1. Dodavatel poskytuje objednateli záruku za jakost předmětu plnění, tj. všech dodaných položek předmětu plnění s tím, že po dobu záruční doby bude vše způsobilé pro použití ke smluvenému účelu, jinak k obvyklému účelu nebo že si zachová smluvené, jinak obvyklé vlastnosti, v délce a za podmínek uvedených v této smlouvě, a to ode dne převzetí Předmětu plnění a podpisem předávacího protokolu a záručního list Objednatelem. Dodavatelem poskytnutá záruka se vztahuje na funkčnost dodané Předmětu plnění, jakož i na jeho vlastnosti požadované Objednatelem.
2. Záruční doba pro předmět plnění začíná běžet od okamžiku převzetí předmětu plnění objednatelem a končí uplynutím minimálně 12 měsíců od řádného předání předmětu plnění. Je-li výrobcem na předmět plnění poskytnuta doba delší, platí tato delší záruční doba.
3. Po dobu záruky Dodavatel odpovídá za to, že dodaný Předmět plnění bude prostý jakýchkoli vad a bude mít vlastnosti dle obecně závazných právních předpisů, technických norem a této smlouvy. Po celou dobu záruky se Dodavatel zavazuje zajistit bezplatný záruční servis v sídle Objednatele s provedením opravy do následujícího dne od nahlášení závady, nebude-li mezi smluvními stranami dohodnuto jinak.
4. V případě, že budou Objednatelem po převzetí Předmětu plnění na tomto zjištěny vady, má Objednatel právo uplatnit vůči Dodavateli nároky v souladu s ustanoveními § 2099 až 2117 občanského zákoníku.
5. Veškeré náklady Objednatele související s opravou vad, na které se prokazatelně vztahuje záruka, budou hrazeny Dodavatelem. Záruční doba neběží po dobu, po kterou objednatel nemůže užívat předmět plnění nebo jeho část pro jeho vady, za které odpovídá dodavatel.
6. Jestliže objednatel zjistí během záruční doby, že předmět plnění nebo jeho část vykazuje vady, bez zbytečného odkladu uvědomí písemným oznámením vad (dále „reklamace“) dodavatele o zjištěných vadách zaslaným do datové schránky dodavatele, ale i elektronickou poštou na kontakty shora uvedené.
7. V reklamaci je objednatel povinen specifikovat konkrétní vadu, nebo její projev, a uvést, jaký nárok z vady vůči dodavateli uplatňuje.
8. Odpovědnost za vady předmětu plnění se řídí ujednáním smluvních stran v této smlouvě a následně ustanoveními občanského zákoníku.
9. Pro uplatnění práva z odpovědnosti za vady předmětu plnění je nezbytná reklamace objednatele u dodavatele nejpozději do konce doby, po kterou dodavatel odpovídá za vady předmětu plnění.
10. Dodavatel se zavazuje do 24 hodin po doručení příslušné reklamace, potvrdit její přijetí a sdělit objednateli, zda reklamaci uznává či nikoliv. Pokud tak dodavatel v této lhůtě neučiní, má se za to, že reklamaci uznává. V případě odmítnutí reklamace je dodavatel povinen se sdělením o neuznání reklamace objednateli písemně uvést jasné a jednoznačné důvody takového odmítnutí.
11. O odstranění vady bude sepsán protokol, který podepíší obě smluvní strany. V tomto protokolu, který vystaví dodavatel, musí být mimo jiné uvedeno: jména zástupců obou smluvních stran, číslo smlouvy, datum uplatnění a č.j. reklamace, popis a rozsah vady a způsob jejího odstranění, datum zahájení a ukončení odstranění vady, celková doba trvání vady (doba od zjištění do odstranění vady) a vyjádření, zda vada bránila užívání předmětu plnění k účelu, ke kterému bylo určeno.
12. Dodavatel se zavazuje v případě potřeby dodat objednateli veškeré nové, případně opravené doklady vztahující se k opravené, případně vyměněné části předmětu plnění (atesty, certifikáty apod.) potřebné k jeho užívání, a to v termínu stanoveném pro odstranění předmětné vady. V případě porušení této povinnosti není objednatel povinen předmět odstranění vady převzít, a dodavatel je tak v prodlení s plněním odstranění vad a je povinen uhradit smluvní pokutu ve výši 500,- Kč za každý den prodlení.
13. Neodstraní-li dodavatel vadu předmětu plnění, resp. předmětu plnění ve stanovené lhůtě, je objednatel oprávněn vadu odstranit prostřednictvím třetí odborně způsobilé osoby, a to na náklady dodavatele.
14. Reklamaci lze uplatnit nejpozději do posledního dne záruční doby, přičemž i reklamace odeslaná objednatelem v poslední den záruční doby se považuje za včas uplatněnou.
15. Záruční doba se nevztahuje na vady způsobené neodbornou manipulací nebo mechanickým poškozením při činnosti nesouvisející s činností dodavatele.
16. Reklamovaná vada se považuje za vadu, za kterou dodavatel odpovídá, dokud není dodavatelem prokázán opak.

**čl. XIII**

**sankce**

1. Smluvní strany jsou povinny uhradit smluvní pokutu v případech stanovených touto smlouvou.

2. Dodavatel je povinen zaplatit objednateli smluvní pokutu:

1. za prodlení dodavatele s dodání a předáním kompletního předmětu plnění v termínu dle čl. II odst. 1.2 této smlouvy, a to ve výši 5.000,--Kč za každý i započatý den prodlení,
2. za prodlení dodavatele s poskytnutím služeb servisní a technické podpory řešení v termínu dle čl. II odst. 1.3 této smlouvy, a to ve výši 5.000,--Kč za každý jednotlivý případ porušení,
3. za nesplnění povinnosti dodavatele odstranit vady části předmětu plnění v záruční době ve stanovené lhůtě, a to ve výši 500,--Kč uvedené v čl. XII odst. 3. této smlouvy za každou vadu a za každý i započatý den prodlení.

3. Objednatel je oprávněn započíst smluvní pokuty proti platbám za plnění objednatele a dodavatel s tímto bez výhrad souhlasí.

4. Objednatel se zavazuje pro případ prodlení s placením daňového dokladu zaplatit dodavateli smluvní pokutu ve výši 0,1% z dlužné částky bez DPH za každý i započatý kalendářní den prodlení po termínu splatnosti.

5. Ujednáním o smluvní pokutě není dotčeno právo dotčené/poškozené smluvní strany domáhat se na druhé smluvní straně/škůdci náhrady škody, a to i v části, v níž výše škody přesahuje smluvní pokutu.

6. Zaplacením smluvní pokuty nezaniká nárok poškozené strany na náhradu způsobené škody, a to v plném rozsahu, např. znemožnění čerpání dotace z důvodu nesplnění smluvních podmínek na straně dodavatele.

6. Právo fakturovat smluvní pokutu vzniká oprávněné straně kdykoli poté, co nastala skutečnost, s níž je spojen vznik práva na smluvní pokutu. Smluvní pokuta je splatná bezhotovostně na účet uvedený ve faktuře vystavené oprávněnou stranou a v den, který je jako den splatnosti ve faktuře uveden, jinak 30-tého dne po prokazatelném doručení faktury povinné smluvní straně. Tuto smluvní pokutu má objednatel právo započítat na částku uvedenou v konečné faktuře.

**čl. XIV**

**odstoupení od smlouvy**

1. Od smlouvy lze odstoupit, stanoví-li tak smlouva či občanský zákoník. Odstoupení musí být písemné a musí být doručeno prokazatelně druhé smluvní straně. Účinky odstoupení nastávají dnem doručení písemného oznámení o odstoupení smluvní straně, jíž je určeno.
2. Objednatel a dodavatel jsou oprávněni odstoupit od smlouvy z těchto důvodů:
3. podstatného porušení smluvních povinností druhou smluvní stranou, v případech stanovených touto smlouvou a v případě, je-li v insolvenčním řízení příslušným soudem pravomocně rozhodnuto o úpadku dodavatele nebo je-li insolvenční návrh ve věci dodavatele v postavení dlužníka zamítnut pro nedostatek majetku. Za podstatné porušení smluvních povinností se považuje neplnění sjednaných termínů a dalších rozhodujících závazků vyplývajících z této smlouvy;
4. dodavatel již třikrát porušil jakoukoliv svou povinnost vyplývající z této smlouvy a na toto porušení byl upozorněn;

c) neprovádí-li dodavatel předmět plnění řádně kvalitně nebo jinak porušuje smluvní povinnosti, je objednatel oprávněn odstoupit od této smlouvy v případě, že dodavatel nesplní jakékoli své povinnosti vyplývající ze smlouvy ani v dodatečně přiměřené lhůtě, která mu k tomu byla poskytnuta, přičemž však tato lhůta nesmí být kratší než 14 kalendářních dnů.

1. Smluvní strany se zavazují spolupracovat v maximální možné míře a učinit veškerá okolnostem případu přiměřená opatření ke zmenšení škody, která by případně odstoupením od smlouvy mohla vzniknout některé z nich. Na případné předání neúplné dodávky předmětu plnění se přiměřeně použijí ustanovení této smlouvy upravující předání. Veškeré náklady spojené s odstoupením od této smlouvy jdou k tíži strany, která porušila povinnost, v důsledku čehož druhá smluvní strana od smlouvy odstoupila.
2. Smluvní strany se zavazují bezprostředně po odstoupení od smlouvy některou z nich provést následující kroky:
3. Dodavatel provede finanční ocenění dodaného IT vybavení, a to v souladu s cenovou nabídkou dodavatele z předmětného zadávacího řízení a zpracuje konečnou fakturu případné neúplné dodávky předmětu plnění; tato částka nesmí být vyšší, než kolik by činilo ocenění dle cenové nabídky dodavatele.
4. Dodavatel případně vyzve objednatele k převzetí neúplné dodávky předmětu plnění a objednatel je povinen do 15 kalendářních dnů od obdržení vyzvání zahájit přejímací řízení.
5. Společně s neúplnou dodávkou předmětu plnění předá dodavatel objednateli i veškerou dokumentaci, kterou má či je povinen mít k dispozici, jakož i veškeré věci, které od objednatele převzal v souvislosti s realizací plnění dle této smlouvy.

5. Dojde-li k účinnému odstoupení od smlouvy, je objednatel povinen uhradit dodavateli pouze to, o co se prováděním předmětu plnění obohatil. Nedojde-li k dohodě o hodnotě tohoto obohacení, bude oceněno znaleckým posudkem na náklady dodavatele.

6. Objednateli budou uhrazeny dodavatelem vícenáklady vzniklé z titulu přerušení prací z důvodů na straně dodavatele, a tím pádem nutnosti dokončení předmětu plnění jiným dodavatelem, a vlivem nedodržení termínu dokončení předmětu plnění.

7. Zánikem smlouvy nejsou dotčeny nároky účastníků na náhradu škody a jiné sankce, které za trvání smlouvy vznikly.

**čl. XV**

**závěrečná ujednání**

1. Dodavatel je oprávněn změnit poddodavatele, pomocí něhož v zadávacím řízení prokazoval kvalifikaci jen na základě předchozího souhlasu objednatele a za subjekt, který splňuje kvalifikaci minimálně ve stejném rozsahu. Objednatel se zavazuje tento souhlas bezdůvodně neodepřít.
2. Tam, kde nejsou práva a závazky smluvních stran výslovně upraveny, platí ustanovení občanského zákoníku.
3. Smluvní strany si sjednávají, že § 564 občanského zákoníku se nepoužije, tzn. měnit nebo doplňovat text smlouvy je možné pouze formou písemných dodatků v elektronické podobě opatřených elektronickým podpisem obou smluvních stran. Za písemnou formu se pro tento účel nebude považovat výměna e-mailových či jiných elektronických zpráv. Neplatnost smlouvy pro nedodržení formy lze namítnout kdykoliv, a to i když již bylo započato s plněním.
4. Dodavatel není oprávněn bez souhlasu Objednatele postoupit jakoukoli svou tvrzenou pohledávku za Objednatelem třetí osobě.
5. Dodavatel není oprávněn jednostranně započíst jakoukoli svou tvrzenou pohledávku za Objednatelem na pohledávku objednatele za dodavatelem.
6. Práva a povinnosti vyplývající z této smlouvy přecházejí i na případné právní nástupce obou smluvních stran.
7. Dodavatel prohlašuje, že je plně způsobilý ke splnění všech závazků, které na sebe podpisem této smlouvy převezme.
8. S ohledem na povinnost vést písemnou komunikaci elektronicky dle § 211 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, je tato smlouva vyhotovena pouze v jednom elektronickém vyhotovení s platností originálu.
9. Tato smlouva obsahuje úplné ujednání o předmětu smlouvy a všech náležitostech, které smluvní strany měly a chtěly ve smlouvě ujednat, a které považují za důležité pro závaznost této smlouvy. Žádný projev smluvních stran učiněný při jednání o této smlouvě ani projev učiněný po uzavření této smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními této smlouvy a nezakládá žádný závazek žádné ze stran.
10. Kdykoli Smlouva vyžaduje vyhotovení nebo vystavení souhlasů, osvědčení, svolení, rozhodnutí, oznámení a žádostí jakoukoli osobou, tato sdělení musejí být vyhotovena písemně či elektronicky a doručena dle jejich charakteru osobně, zaslána e-mailem, datovou schránkou, prostřednictvím kurýrní služby nebo doporučenou poštou oproti doručence.
11. Smluvní Strany pro vyloučení pochybností výslovně sjednávají, že sdělení budou doručena, zaslána nebo přenesena zástupcům Smluvních Stran (tj. podle okolností zástupci objednatele nebo zástupci dodavatele uvedeným v úvodních ustanovení Smlouvy, ledaže (i) příjemce oznámí změnu kontaktních údajů v předstihu deseti (10) pracovních dnů; sdělení budou poté doručena podle zmíněných kontaktních údajů, nebo (ii) v případě, že příjemce neuvede při žádosti o schválení nebo souhlas jinak, může být sdělení zasláno na adresu, z níž byla žádost odeslána. Smluvní Strany se zavazují udržovat své kontaktní údaje vůči druhé Smluvní Straně aktuální a zajistit na nich přebírání komunikace zasílané dle této Smlouvy.
12. Strany si nepřejí, aby nad rámec výslovných ustanovení této smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.
13. Smluvní strany tuto smlouvu přečetly, prohlašují, že je projevem jejich svobodné a vážné vůle, že nebyla sjednána v tísni za nápadně nevýhodných podmínek a na důkaz souhlasu doplňují zástupci obou smluvních stran elektronické podpisy.
14. Tuto smlouvu lze změnit nebo upřesnit pouze písemným ujednáním nazvaným „Dodatek ke smlouvě“ v elektronické podobě a očíslovaným podle pořadových čísel, který bude potvrzen a odsouhlasen smluvními stranami a prohlášen za nedílnou součást této smlouvy.
15. Odpověď smluvní strany podle § 1740 odst. 3 občanského zákoníku, s dodatkem nebo odchylkou, není přijetím nabídky na uzavření této smlouvy, ani když podstatně nemění podmínky nabídky.
16. Smluvní strany se dohodly, že Objednatel bezodkladně po uzavření této smlouvy odešle smlouvu k řádnému uveřejnění do registru smluv spravovaného Digitální a informační agenturou . O uveřejnění smlouvy Objednatel bezodkladně informuje druhou smluvní stranu, nebyl-li kontaktní údaj této smluvní strany uveden přímo do registru smluv jako kontakt pro notifikaci o uveřejnění.
17. Smlouva nabývá platnosti dnem jejího elektronického podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv spravovaném Digitální a informační agenturou v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění.
18. Smluvní strany berou na vědomí, že nebude-li smlouva zveřejněna ani do tří měsíců ode dne jejího uzavření, je následujícím dnem zrušena od počátku s účinky případného bezdůvodného obohacení.
19. Smluvní strany prohlašují, že žádná část smlouvy nenaplňuje znaky obchodního tajemství (§ 504 zákona č. 89/2012 Sb., občanský zákoník).

Doložka dle § 41 zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů

Schváleno usnesením Rady města Pardubice ze dne 12.2.2025 č. usnesení R/4950/2025.

Příloha č. 1: Dodavatelem nabízené řešení předmětu plnění

Příloha č. 2: Specifikace předmětu plnění - oceněný nabídkový list

      V Pardubicích 26.03.2025                                                                             V Ostravě 11.03.2025

                      Za objednatele                                                                                 Za dodavatele

        .................................................                                                    .................................................

                  Bc. Jan Nadrchal                                                                   Jaroslav Dvořák, člen představenstva

primátor města

6. Specifikace nabízeného řešení

VZ: Kybernetická bezpečnost Pardubice - posílení informačních systémů

(IS) v rámci zabezpečení kyberbezpečnosti Příloha č. 1

Specifikace funkčních požadavků - pro ČÁST 1: Identity management systém (IDM - IAM)

IDM -IAM Funkční požadavky

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parametr** | **Popis povinného parametru** | **Splňuje**  **ANO /NE** | **Dodavatel popíše detailní návrh způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| Licence | Poskytnutá licence umožní nasazení a provoz systému bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.).  Předpokládaný počet uživatelů je do 880. | ANO | Poskytnutá licence IDM Aricoma ID umožní nasazení a provoz systému bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Neobsahu-je žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Škálovatelnost | Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. Data systému budou uchovávána v databázi. Systém musí podporovat režim ve vysoké dostupnosti. | ANO | Systém umožňuje zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. Data systému jsou uchovávána v databázi. Systém podporuje režim ve vysoké dostupnosti. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3. Práce s informačním systémem IDM |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Uživatelské role | Integrovaná správa aplikačních rolí včetně zařazení uživatele do odpovídající role v příslušných IS. V rámci dané role bude možné definovat jemné členění různých významů role. Například roli „editor webu“ bude možné rozšířit o významy odpovídající jednotlivým oddělením, pro které jsou části webu určené. Tyto rozšiřující významy rolí bude možné přímo přiřazovat systematizovaným místům, skupinám, organizačním jednotkám, uživatelům spravovaných v systému.  Systém umožní správu zákazových rolí. Zákazová role přiřazená systematizovanému místu, skupině, organizační jednotce nebo přímo uživateli zajistí odebrání této role v synchronizovaných systémech. | ANO | Idm obsahuje správu aplikačních rolí včetně zařazení uživatele do odpovídající role v příslušných IS a aplikacích. V rámci dané role bude možné definovat jemné členění různých významů role. Například i roli „editor webu“ bude možné rozšířit o významy odpovídající jednotlivým oddělením, pro které jsou části webu určené. Tyto rozšiřující významy rolí je možné přímo přiřazovat systematizovaným místům, skupinám, organizačním jednotkám, uživatelům spravovaných v systému.  Systém umožňuje správu zákazových rolí. Zákazová role přiřazená systematizovanému místu, skupině, organizační jednotce nebo přímo uživateli zajistí odebrání této role v synchronizovaných systémech. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.7 Číselník Aplikační role, 5.4.3.1 Zakázání specifikace aplikační role uživatelskému účtu, 5.4.3.4 Delegace aplikačních rolí |
|  | Systém umožní delegaci aplikačních rolí. Při delegaci jsou aplikační role předány na nového uživatele s možností nastavení platnosti, do kdy je delegace platná. Následně jsou role vráceny delegujícímu uživateli a odebraný delegovanému. |  | Systém umožňuje delegaci aplikačních rolí. Při delegaci jsou aplikační role předány na nového uživatele s možností nastavení platnosti, do kdy je delegace platná. Po skončení platnosti jsou role vráceny delegujícímu uživateli a odebraný delegovanému. |  |
| Historizace | Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti. | ANO | Idm obsahuje detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytuje data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.7 Historie |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Automatizace | Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě kombinace libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). Provádění vyhodnocení pravidel bude mít stejné vlastnosti jako jiné synchronizační procesy systému. Ruční vs plánované spuštění, historii běhů, simulační režim, atd. | ANO | Idm obsahuje podporu intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě kombinace libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). Provádění vyhodnocení pravidel má stejné vlastnosti jako jiné synchronizační procesy systému. Ruční vs plánované spuštění, historii běhů, simulační režim, atd. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 13. Pravidla |
| Logování SIEM | Systém bude exportovat auditní logy pro systémy typu SIEM ve formátu CSV nebo XML. | ANO | Systém Idm exportuje auditní logy pro systémy typu SIEM ve formátu CSV nebo XML. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Logování systému | Systém obsahuje 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) * odeslané notifikace a upozornění (notifikační log) | ANO | Systém obsahuje 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) * odeslané notifikace a upozornění (notifikační log) | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Systematizovan á místa | Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. | ANO | Systém pracuje s principem systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. V systému Idm je systemizované místo uváděno jako pracovní pozice | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.9 Číselník Pracovní pozice (Systemizovaná místa) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Podpora elDAS | Systém 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. | ANO | Systém umožňuje 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. | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Požadavky na portál - obecné | Systém bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. | ANO | Systém obsahuje webový portál, který slouží jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Požadavky na portál - přístup | Správa systému musí být implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole musí být přístupná výhradně protokolem https. | ANO | Správa systému je implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole je přístupná výhradně protokolem https. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Podpora mobilních zařízení | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno). | ANO | Portál je implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno). | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Správa referenčních objektů | Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, certifikát. | ANO | Portál umožňuje přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, certifikát. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 8. Modul nastavení |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Referenční objekty | Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Systém bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě. | ANO | Systém umožňuje přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Systém je v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 8. Modul nastavení |
| Zabezpečení referenčních objektů | Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů | ANO | Systém umožňuje nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 8.4 Oprávnění IDM |
| Rozšiřující atributy | Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IAM. | ANO | Systém umožňuje dodatečné rozšiřování identit a referenčních objektů o další atributy a zajišťuje publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IAM. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 8. Modul nastavení |
| Přehledné zobrazení | Systém bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v systému bude zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury bude možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky. | ANO | Systém Idm obsahuje grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v systému je zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury je možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 6. Modul Organizační struktura, 3.6 Vyhledávání a filtrování v aplikaci IDM |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vyhledávání - diakritika | Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Novak vyhledává i Novák apod.) | ANO | Portál umožňuje vyhledávat i bez diakritiky (např. zadání Novak vyhledává i  Novák apod.) | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.6 Vyhledávání a filtrování  v aplikaci IDM |
| Správa certifikátů | Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti. | ANO | Správa uživatelů (identit) umožňuje i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech je možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožňuje automatické zneplatnění uložených certifikátů po vypršení data platnosti. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.17 Číselník Uživatelské  certifikáty |
| Obrázky | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie. | ANO | Systém umožňuje k jednotlivým účtům (identitám) přikládat obrázky - fotografie. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 5.2.1.1 Záložka osoba |
| Přesun identit | Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními. | ANO | Systém umožňuje přesun identit mezi jednotlivými organizacemi či jejich odděleními. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 4.1 Profil uživatele |
| Kopírování rolí | Systém umožní kopírovaní aplikačních rolí, mezi jednotlivými systematizovanými místy. | ANO | Systém umožňuje kopírovaní aplikačních rolí, mezi jednotlivými systematizovanými místy. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 14.1.1 Zkopírování práv z jiného  oprávnění |
| Ochrana proti chybám | Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). | ANO | Systém obsahuje mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.11 Funkce Automatické spouštění synchronizací, 11.3.7 Záložka Synchronizace  objektů |
| Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem | ANO | Systém obsahuje přehled uživatelů aktuálně pracujících s Portálem - přihlášení uživatelé. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.4 Modul Centrálního  dashboardu |
| Slučování identit | Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. | ANO | Systém umožňuje sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.9 Funkce sjednocení osob |
| Export údajů | Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu | ANO | Systém Idm obsahuje vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.7.1 Historie záznamů |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Filtrování | Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití. | ANO | Idm systém obsahuje vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů a možnost uložení filtrů pro opakované použití. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.6 Vyhledávání a filtrování  v aplikaci IDM |
| Správa oprávnění | Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) | ANO | Idm obsahuje víceúrovňovou správu administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 14.2 Nastavování detailních  práv oprávnění |
| Editor oprávnění | Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému, reporty, workflow, správa webových služeb IAM atd.) Dále bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět. | ANO | Systém Idm obsahuje editor oprávnění. V rámci editoru administrátor definuje oprávnění do Systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění je definováno pro jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému, reporty, workflow, správa webových služeb IAM atd.) Dále je oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů je možnost definovat akce, které může uživatel s entitami a v rámci systému provádět. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 14.2 Nastavování detailních  práv oprávnění |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kontextový výběr organizační jednotky | Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, systematizovaných míst dostupných pro identity z dané organizační jednotky. | ANO | V rámci systému Idm je na úrovní organizační jednotky možnost pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, systematizovaných míst dostupných pro identity z dané organizační jednotky. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 15. Funkce Dědění |
| Správa licencí | Systém umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IAM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. | ANO | Systém Idm umožňuje spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí IAM obsahuje workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.3 Modul Workflow |
| Časová omezení | Systém bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení systém roli přiřazenému objektu automaticky odebere. | ANO | Systém Idm umožňuje přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení systém roli přiřazenému objektu automaticky odebere. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.7 Číselník Aplikační role |
| Vícenásobné vazby | Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v systému evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. | ANO | Systém Idm má možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v systému evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.9.1 Přiřazení uživatelů  pracovní pozici |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Přehled rolí | Systém bude zajišťovat zobrazení přidělených rolí a jejich rozšiřujících významům k jednotlivým identitám s rozdělením na role navázané na systemizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity musí být evidován a v systému souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.). | ANO | Systém Idm zajišťuje zobrazení přidělených rolí a jejich rozšiřujících významům k jednotlivým identitám s rozdělením na role navázané na systemizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity je evidován a v systému souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.). | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.9 Číselník Pracovní pozice  (Systemizovaná místa) |
| Skupiny | Systém bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. | ANO | Systém obsahuje správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 7.11 Číselník Skupiny uživatelů |
| Zastupitelnost | Systém bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. | ANO | Systém Idm obsahuje správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 5.4.3.4 Delegace aplikačních rolí |
| Delegování oprávnění | Možnost delegování administrátorských práv. | ANO | Systém Idm má možnost delegování administrátorských práv. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 5.4.3.4 Delegace aplikačních rolí |
| Obnovení hesla | Systém bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. v systému musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu). | ANO | Systém Idm obsahuje samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele má možnost provádět pomocí SMS (tj. v systému musí být možné na SMS bránu či službu napojit). Rozhraní umožňuje i běžnou změnu hesla (bez resetu). | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.1 Funkce Reset hesla |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Žádosti | IAM 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. | ANO | Systém Idm obsahuje 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. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.3 Modul Workflow |
| Kontextový výběr | Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. | ANO | Samoobslužné rozhraní umožňuje na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.3 Modul Workflow |
| Individualizace | Systém umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně | ANO | Systém umožňuje uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.6.1 Zobrazení sloupců |
| Workflow | Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky:   * Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným * Možnost sledování stavu svých požadavků uživateli * E-mailové upozornění schvalovatele na požadavek ke schválení * Přehled úloh ke schválení pro každého schvalovatele * Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění * Podpora vícekrokového schvalování * Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) * Správce IAM může pracovat se všemi úlohami * Možnost větvení pro ošetření výjimek vzniklých při schvalování | ANO | Idm obsahuje integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Obsahuje tyto funkční požadavky:   * Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným * Možnost sledování stavu svých požadavků uživateli * E-mailové upozornění schvalovatele na požadavek ke schválení * Přehled úloh ke schválení pro každého schvalovatele * Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění * Podpora vícekrokového schvalování * Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) * Správce IAM může pracovat se všemi úlohami * Možnost větvení pro ošetření výjimek vzniklých při schvalování | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.3 Modul Workflow |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * Řešení zastupitelnosti * Eskalace - upozornění při překročení termínu splnění * Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů |  | * Řešení zastupitelnosti * Eskalace - upozornění při překročení termínu splnění * Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů |  |
| Workflow - sledování | Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate | ANO | Průběh workflow je možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram je v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.3 Modul Workflow |
| Upozornění | Systém zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravován přímo v Portálu systému. | ANO | Systém Idm zajišťuje zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. Mechanismus správy notifikací včetně náhledu na odeslané notifikace jet spravován přímo v Portálu systému. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 9. Modul Správa notifikací |
| Včasná upozornění | Portál bude obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu. | ANO | Portál bude obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 9. Modul Správa notifikací |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Šablony upozornění | 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. | ANO | Šablony upozornění umožňují definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám je možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony umožňují vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 9. Modul Správa notifikací |
| Kontext upozornění | U notifikací ve vazbě na identity a referenční objekty musí být možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně musí být možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále musí být možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributu identity a referenčních objektů. (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo, atd.). V Portálu musí být možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IAM změnu identity nebo referenčního objektu provedly. | ANO | U notifikací ve vazbě na identity a referenční objekty je možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně je možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále je možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributu identity a referenčních objektů. (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo, atd.). V Portálu je možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IAM změnu identity nebo referenčního objektu provedly. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 9. Modul Správa notifikací |
| Logování | Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IAM 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 IAM. Záznam v logu bude obsahovat původní i novou hodnotu. | ANO | Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IAM jsou provedeny transakčně. Jsou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IAM. Záznam v logu obsahuje původní i novou hodnotu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.7 Historie |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Důvěryhodnost logování | Veškeré požadavky na změny v IAM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IAM. | ANO | Veškeré požadavky na změny v IAM je možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IAM. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.7 Historie |
| Auditní report | IAM umožní export auditního reportu z údajů o identitách uložených v IAM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IAM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. | ANO | IAM umožňuje export auditního reportu z údajů o identitách uložených v IAM a to i historických. Auditní reporty jsou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IAM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Auditní report - výběr | IAM bude obsahovat editor pro vyhledávání identit a referenčních objektů v systému IAM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IAM evidovány včetně přidružených referenčních objektů. | ANO | IAM obsahuje editor pro vyhledávání identit a referenčních objektů v systému IAM pro vytvoření reportu. Do filtru je možné zadat libovolné atributy identity, které jsou v systému IAM evidovány včetně přidružených referenčních objektů. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Reporty uživatelů | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. | ANO | Systém Idm obsahuje vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů.  Reporty jsou exportovatelný do CSV souboru. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Reporty - zasílání | IAM bude obsahovat možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatického zasílání reportu emailem. | ANO | IAM obsahuje možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatického zasílání reportu emailem. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Karta uživatele | IAM bude obsahovat report, který do formátu PDF vygeneruje kartu uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů, atd. | ANO | IAM obsahuje report, který do formátu PDF vygeneruje kartu uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů, atd. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. | ANO | Idm obsahuje automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Reporty - porovnání | Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. | ANO | Idm obashuje snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Dashboard | IAM bude obsahovat centrální dashboard, který bude  obsahovat následující údaje:   * Synchronizační úlohy v   chybě   * chyby běhu synchronizací * chyby při generování a   odesílání notifikací   * chyby volaní metod   rozhraní webových služeb IMD(např. pokus o přístup k metodě, na kterou nemám oprávnění)   * chyby plánovaných úloh   (agentů)   * nově vytvořené poznámky * workflow v chybě * neúspěšné akce systému   v systému IAM  Záznamy v dashboard se budou načítat za počet dnů definovaných v konfiguraci IAM | ANO | IAM obsahuje centrální dashboard, který bude obsahovat následující údaje:   * Synchronizační úlohy v chybě * chyby běhu synchronizací * chyby při generování a odesílání   notifikací   * chyby volaní metod rozhraní   webových služeb IMD(např. pokus o přístup k metodě, na kterou nemám oprávnění)   * chyby plánovaných úloh (agentů) * nově vytvořené poznámky * workflow v chybě * neúspěšné akce systému v systému   IAM  Záznamy v dashboard se budou načítat za počet dnů definovaných v konfiguraci IAM | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.4 Modul Centrálního dashboardu |
| Webové služby (WS) | IAM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. | ANO | IAM poskytuje rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 10. Modul Správa rozhraní |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Standardy WS | Webové služby IAM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. V rámci povahy předávaných identitních údajů (včetně osobních údajů) je požadováno zajistit maximální zabezpečení a zajištění spolehlivosti volání webových služeb minimálně v rozsahu specifikací WS-Security, WS- SecurityPolicy, WS- ReliableMessaging, WS- AtomicTransactions. | ANO | Webové služby lAMjsou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. V rámci povahy předávaných identitních údajů (včetně osobních údajů) je požadováno zajistit maximální zabezpečení a zajištění spolehlivosti volání webových služeb minimálně v rozsahu specifikací WS- Security, WS-SecurityPolicy, WS- ReliableMessaging, WS- AtomicTransactions. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 10. Modul Správa rozhraní |
| Bezpečnost WS | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. | ANO | Konfigurace webových služeb umožňuje konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 10. Modul Správa rozhraní |
| Logování WS | Volání webových služeb bude logováno na úrovni databáze a bude možné je zobrazit v prostředí Portálu | ANO | Volání webových služeb je logováno na úrovni databáze a bude možné je zobrazit v prostředí Portálu | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 10. Modul Správa rozhraní |
| Služby rozhraní  WS | Rozhraní bude poskytovat minimálně následující služby:   * Načtení   organizační struktury   * Načtení   hierarchie systematizovaných míst   * Načtení   seznamu identit   * Načtení   nadřízené osoby pro daného zaměstnance   * Načtené   seznamu aplikační rolí   * Načtení   seznamu uživatelů dané aplikace   * Zápis   seznamu aplikačních rolí do IAM   * Zápis   certifikátů do IAM   * Zápis a změna   uživatelů a osob   * Zabezpečená   služba pro přihlášení aplikace k IAM   * Zabezpečená   služba pro přihlášení uživatele k IAM   * Přidání a   odebrání uživatele do/z skupiny   * Přidání a   odebrání aplikační role a jejího rozšiřujícího významu na/z uživatele, organizační jednotku, systematizované místo nebo skupinu | ANO | Rozhraní poskytuje všechny požadované služby. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 10. Modul Správa rozhraní |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | - Přidání a  odebrání agendové role na uživatele nebo systematizované místo |  |  |  |
| Synchronizace | Ruční i automatické spuštění synchronizací s propojenými systémy. | ANO | Systém Idm obsahuje ruční i automatické spuštění synchronizací s propojenými systémy. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 11. Modul Synchronizace |
| Synchronizace - simulace | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. | ANO | Systém Idm obsahuje spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy jsou zobrazitelné v Portálu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 11. Modul Synchronizace |
| Simulace - průběh | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. | ANO | Zobrazení jednotlivých stavů průběhu synchronizace je k dispozici v přehledné grafické podobě. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 11. Modul Synchronizace |
|  | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IAM umožní IAM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): |  | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IAM umožňuje IAM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): |  |
|  | - Plná synchronizace - prochází všechny objekty v IAM a synchronizuje je s objekty daného systému |  | - Plná synchronizace - prochází všechny objekty v IAM a synchronizuje je s objekty daného systému |  |
| Synchronizace - režimy | - Změnová synchronizace - synchronizuje vždy jen změny od poslední spuštěné synchronizace. | ANO | - Změnová synchronizace - synchronizuje vždy jen změny od poslední spuštěné synchronizace. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 11. Modul Synchronizace |
|  | - Okamžitá synchronizace konkrétní identity na vyžádání - synchronizuje okamžitě pouze vybranou identitu. |  | - Okamžitá synchronizace konkrétní identity na vyžádání - synchronizuje okamžitě pouze vybranou identitu. |  |
|  | - Rekonciliační synchronizace - synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IAM vs. nastavení identit a oprávnění přímo v připojeném systému. |  | - Rekonciliační synchronizace - synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IAM vs. nastavení identit a oprávnění přímo v připojeném systému. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | - Simulační synchronizace - synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. |  | - Simulační synchronizace - synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. |  |
|  | - Historie běhu synchronizací - |  |  |  |
|  | jednotlivé běhy synchronizací budou zaznamenány v databázi a dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci |  | - Historie běhu synchronizací - jednotlivé běhy synchronizací budou zaznamenány v databázi a dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno  v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. |  |
| vyvolala. |
|  | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, |  | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, závislostí mezi synchronizacemi, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž umožněno, aby bylo možné vybírat organizace, které se mají z IAM synchronizovat s danými systémy. Správa je součástí Portálu. |  |
| Synchronizace - | závislostí mezi synchronizacemi, nastavení časového intervalu | ANO | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM |
| správa | spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IAM synchronizovat s danými systémy. Správa bude součástí Portálu. | P, kapitola 11. Modul Synchronizace |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Synchronizace - sekvence | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM sekvenční spouštění (za předpokladu podpory napojovaných systémů) a to tak, aby jednotlivé synchronizace mohli být spouštěny po sobě v sekvencích. Navazující synchronizované systémy v sekvenci bude možno definovat dle požadavků a spouštět nebo zastavovat automaticky i ručně. | ANO | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožňuje IDM sekvenční spouštění (za předpokladu podpory napojovaných systémů) a to tak, aby jednotlivé synchronizace mohli být spouštěny po sobě v sekvencích. Navazující synchronizované systémy v sekvenci je možno definovat dle požadavků a spouštět nebo zastavovat automaticky i ručně. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 11. Modul Synchronizace |
| Agenti | Pro plánované úlohy umožní IDM definici agentů a jejich plánovaných spouštění na základě akcí a triggerů v systému. Spouštění je možné definovat i pro požadované intervaly, definovat omezení a další. Agenty bude možné importovat do systému IDM minimálně ve formátu JSON. | ANO | Pro plánované úlohy umožňuje IDM definici agentů a jejich plánovaných spouštění na základě akcí a triggerů v systému. Spouštění je možné definovat i pro požadované intervaly, definovat omezení a další. Agenty je možné importovat do systému IDM minimálně ve formátu JSON. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 12. Modul Agenti |
| Agenti - simuilace | Systém IDM umožní spouštění agentů také v režimu simulace. | ANO | Systém IDM umožňuje spouštění agentů také v režimu simulace. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 12. Modul Agenti |
| Správa aktiv | V rámci systému bude možné spravovat evidenci aktiv s klasifikací dle zákona o kybernetické bezpečnosti.  V systému bude možné spravovat evidenci primárních, podpůrných a technických aktiv. Technická aktiva budou dále rozdělena na datová, softwarová, hardwarová aktiva, informační služby. Jednotlivá aktiva je možné členit do hierarchie aktiv. | ANO | V rámci systému je možné spravovat evidenci aktiv s klasifikací dle zákona o kybernetické bezpečnosti. V systému je možné spravovat evidenci primárních, podpůrných a technických aktiv. Technická aktiva jsou dále rozdělena na datová, softwarová, hardwarová aktiva, informační služby. Jednotlivá aktiva je možné členit do hierarchie aktiv. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.7 Modul aktiv |
| Rozsah aktiv | Minimální rozsah evidovaných dat:  Základní údaje:   * ID Aktiva - identifikátor * Název aktiva - označení   aktiva   * Popis aktiva - popis aktiva * Typ aktiva - typ aktiva * Kategorizace aktiva -   kategorizace aktiva   * Organizace - označení   organizace daného aktiva | ANO | Systém Idm a jeho modul aktiv obsahuje rozsah požadovaných evidovaných dat. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.7 Modul aktiv |

* Stav aktiva - stav daného aktiva
* Kód ISVS - číselný kód přidělený informačnímu systému veřejné správy
* Datum identifikace aktiva
* Lokalizace aktiva
* Vazby na jiná aktiva

Analýza rizik

* Požadavky na dostupnost

aktiva

* Požadavky na důvěrnost

aktiva

* Požadavky na integritu

aktiva

* Celkové hodnocení aktiva
* číselné hodnocení aktiva
* Popis zabezpečení aktiva -

popis způsobu zabezpečení aktiva

* Frekvence přístupu -

hodnota frekvence použití aktiva

* Nedostupnost - popis

hodnocení maximální doby nedostupnosti a definice náhradních postupů v případě nedostupnosti

Ochrana v rámci zpracování osobních údajů:

* Klasifikace - klasifikace osobních údajů
* Zdroj dat - popis získání osobních údajů
* Aktualizace - popis způsobu aktualizace osobních údajů
* Skartace - popis skartace dat
* Zpracování - popis způsobu zpracování osobních údajů
* Registrace - popis registrace zpracování osobních údajů na Úřad pro ochranu osobních údajů
* Kategorie - kategorie osobních údajů
* Účel zpracování - účel zpracování osobních údajů
* Zpracovatel - informace o

zpracovateli osobních údajů

* Příjemce - informaci o

příjemci osobních údajů v případě, že jsou předávány

* Legislativa - popis legislativy vztahující se k danému aktivu.

Garanti aktiv:

* Vlastník - vlastník aktiva
* Správce aktiva - správce

aktiva (například dané aplikace)

* Zástupce - zástupce správce aktiva

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * Uživatelé - seznam   uživatelů daného aktiva.  Uživatele bude možné slučovat do rolí a skupin  Technické údaje (týkající se technických aktiv):   * Technické prostředky   (servery, databáze) - odkaz na technické prostředky, pro provoz a aktiva  Zálohování - popis způsobu a frekvence zálohování |  |  |  |
| Správa osob | Systém obsahovat správu osob, organizační strukturu, rolí. Tuto evidenci bude možné synchronizovat s personálním systémem a navázat na správu aktiv. | ANO | Systém obsahuje správu osob, organizační strukturu, rolí. Tuto evidenci je možné synchronizovat s personálním systémem a navázat na správu aktiv. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.7 Modul aktiv |
| Tiskové výstupy | Systém bude obsahovat  funkcionalitu pro generování následujících reportů:   * Přehled aktiv s možností   filtrování a třídění podle všech dostupných polí   * Karta aktiva se všemi   navázanými údaji   * Zobrazení vazeb mezi   aktivy   * Možnost definice vlastních   sestav   * Přehled žádostí o přidělení   aktiva aktivních a dokončených Přehled oprávnění a přístupů k danému aktivu | ANO | Systém Idm obsahuje funkcionalitu pro generování požadovaných reportů. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.7 Modul aktiv |
| Schvalovací workflow | Systém bude obsahovat  implementaci následujících  workflow:   * Žádost o přístup k aktivu   směrovaná na seznam Garantů jako schvalovatele žádosti   * Periodická revize aktiv   jednotlivými garanty   * Periodická revize stavu   evidence garantem z oblasti řízení bezpečnosti  Funkční požadavky na workflow:   * Zadávání požadavků uživatelů na změny v evidenci * Možnost sledování stavu svých požadavků uživateli * E-mailové upozornění schvalovatele na požadavek ke schválení * Přehled úloh ke schválení pro každého schvalovatele * Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění * Podpora vícekrokového schvalování * Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) | ANO | Systém Idm obsahuje implementaci požadovaných workflow. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.3 Modul Workflow |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti * Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate |  |  |  |
| Vícefaktorová autentizace | Systém bude napojen na systém řízení autentizace uživatelů | ANO | Systém umožňuje napojení na systém řízení autentizace uživatelů | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Požadavky na portál - obecné | Systém bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci systému. | ANO | Systém obsahuje webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci systému. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Požadavky na portál - přístup | Správa systému musí být implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole musí být přístupná výhradně protokolem https. | ANO | Správa systému je implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole musí být přístupná výhradně protokolem https. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Podpora mobilních zařízení | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno). | ANO | Portál je implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno). | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Rozšiřující atributy | Systém umožní dodatečné konfigurační rozšiřování evidence o další atributy | ANO | Systém umožňuje dodatečné konfigurační rozšiřování evidence o další atributy | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 8. Modul nastavení |
| Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem | ANO | Systém obsahuje přehled uživatelů aktuálně pracujících s Portálem | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.4 Modul Centrálního  dashboardu |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Správa oprávnění | Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé části systému (aktiva, uživatelé aktiva, konfigurace notifikací, konfigurace systému, reporty, workflow, správa rozhraní atd.) Oprávnění bude definováno až na konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět. | ANO | Systém obsahuje editor oprávnění. V rámci editoru může administrátor definovat oprávnění do systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění je definováno pro jednotlivé části systému (aktiva, uživatelé aktiva, konfigurace notifikací, konfigurace systému, reporty, workflow, správa rozhraní atd.) Oprávnění je definováno až na konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů je možnost definovat akce, které může uživatel s entitami a v rámci systému provádět. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 14.2 Nastavování detailních  práv oprávnění |
| Logování | Veškeré změny vyvolané požadavky uživatelem systému budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v evidenci. Záznam v logu bude obsahovat původní i novou hodnotu. | ANO | Veškeré změny vyvolané požadavky uživatelem systému jsou provedeny transakčně. Jsou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v evidenci. Záznam v logu obsahuje původní i novou hodnotu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.7 Historie |
| Důvěryhodnost logování | Veškeré požadavky na změny v systému bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů. | ANO | Veškeré požadavky na změny v systému je možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.7 Historie |
| Synchronizace software aktiv | Systém poskytne rozhraní pro pravidelnou synchronizaci softwarových aktiv a jim přidělených uživatelům. | ANO | Systém poskytne rozhraní pro pravidelnou synchronizaci softwarových aktiv a jim přidělených uživatelům. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 18.7 Modul aktiv |
| Obecné konektory | Vestavěné obecné skriptovatelné (javascript, groovy) konektory pro správu identit v napojených systémech: | ANO | Systém Idm obsahuje vestavěné obecné skriptovatelné (javascript, groovy) konektory pro správu identit v napojených systémech: | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 11.3 Konektory |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * konektor pro spouštění CMD a powershell příkazů, SSH * konektor pro práci s CSV soubory * konektor pro práci s databázi Microsoft SQL, Oracle * konektor pro napojení na SOAP webové služby * konektor pro napojení na REST webové služby   U jednotlivých konektorů je možné dynamicky měnit transformační logiku pro nutnou komunikaci s danými typy rozhraní. |  | * konektor pro spouštění CMD a powershell příkazů, SSH * konektor pro práci s CSV soubory * konektor pro práci s databázi Microsoft SQL, Oracle * konektor pro napojení na SOAP webové služby * konektor pro napojení na REST webové služby   U jednotlivých konektorů je možné dynamicky měnit transformační logiku pro nutnou komunikaci s danými typy rozhraní. |  |
| Zdrojový systém | IAM bude napojeno na personální systém VEMA. Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IAM sloužit jako zdrojové | ANO | IAM bude napojeno na personální systém VEMA. Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IAM sloužit jako zdrojové | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor na  VEMA | IAM musí obsahovat konektor umožňující napojení na VEMA s následující funkcionalitou:   * inicializační   načtení dat   * správa   lokálních identit   * správa   oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | IAM bude obsahovat konektor umožňující napojení na VEMA s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor na Active Directory | IAM musí obsahovat konektor umožňující napojení na Microsoft Active Directory s následující funkcionalitou:   * komplexní   správu účtů, kontaktů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)   * založení   domovského adresáře včetně nastavení oprávněná | ANO | IAM bude obsahovat konektor umožňující napojení na Microsoft Active Directory s následující funkcionalitou:   * komplexní správu   účtů, kontaktů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)   * založení domovského   adresáře včetně nastavení oprávněná | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * správu účtů a   jejich certifikátů včetně inicializačního načtení z AD   * správu skupin   a členství ve skupinách včetně inicializačního načtení z AD   * správu   organizačních jednotek včetně inicializačního načtení z AD |  | * správu účtů a jejich   certifikátů včetně inicializačního načtení z AD   * správu skupin a   členství ve skupinách včetně inicializačního načtení z AD   * správu organizačních   jednotek včetně inicializačního načtení z AD |  |
| Konektor na GINIS | IAM musí obsahovat konektor na umožňující napojení na IS Ginis s následující funkcionalitou:   * inicializační   načtení dat   * správu   životního cyklu lokálních identit   * správu   oprávnění pro jednotlivé uživatele na moduly IS (správa konfiguračních skupin)   * správu   funkčních míst a organizačních jednotek | ANO | IAM bude obsahovat konektor na umožňující napojení na IS Ginis s následující funkcionalitou:   * inicializační načtení   dat   * správu životního cyklu   lokálních identit   * správu oprávnění pro   jednotlivé uživatele na moduly IS (správa konfiguračních skupin)   * správu funkčních míst   a organizačních jednotek | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor na Cityware Geovap | IAM musí obsahovat konektor umožňující napojení na Cityware Geovap s následující funkcionalitou:   * inicializační   načtení dat   * správa   lokálních identit   * správa   oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | IAM bude obsahovat konektor umožňující napojení na Cityware Geovap s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor Vita | Konektor IAM musí umožnit napojení na Vita s následující funkcionalitou:  • inicializační  načtení dat | ANO | Konektor IAM musí umožnit napojení na Vita s následující funkcionalitou:  • inicializační načtení  dat | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | • správa  lokálních identit  • správa  oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |  | * správa lokálních   identit   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí |  |
| Konektor MS PowerApps | Konektor IAM musí umožnit napojení na MS PowerApps s následující funkcionalitou:   * inicializační   načtení dat   * správa   lokálních identit   * správa   oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | Konektor IAM umožní napojení na MS PowerApps s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor MS  0365 | Konektor IAM musí umožnit napojení na MS O365 s následující funkcionalitou:   * inicializační   načtení dat   * správa   lokálních identit   * správa   oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | Konektor IAM umožní napojení na MS O365 s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor WEB (GIANT) | Konektor IAM musí umožnit napojení na Giant s následující funkcionalitou:  • inicializační  načtení dat  • správa  lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | Konektor IAM umožní napojení na Giant s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Konektor IAM musí umožnit napojení na RPP a IAM musí obsahovat aktuální evidenci matice práv a rolí dle informačního systému základních registrů (ISZR-RPP) matice RPP určenou (automaticky předfiltrovanou) pro zadavatele tak: |  | Konektor IAM musí umožnit napojení na RPP a IAM musí obsahovat aktuální evidenci matice práv a rolí dle informačního systému základních registrů (ISZR-RPP) matice RPP určenou (automaticky předfiltrovanou) pro zadavatele tak: |  |
|  | • aby vedoucí  pracovníci mohli zadávat k jednotlivým činnostem konkrétní uživatele a obráceně (tedy u uživatelů mohli zadávat jednotlivé činnosti) |  | • aby vedoucí pracovníci  mohli zadávat k jednotlivým činnostem konkrétní uživatele a obráceně (tedy u uživatelů mohli zadávat jednotlivé činnosti) |  |
|  |  |  |  | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor RPP | • přidělování a  odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systematizovaná místa | ANO | • přidělování a  odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systematizovaná místa |  |
|  | • udržování a  poskytování přehledu o oznámených působnostech, jejich stavech, kontrole registrace a změnách |  | • udržování a  poskytování přehledu o oznámených působnostech, jejich stavech, kontrole registrace a změnách |  |
|  | • evidence  přehledu legislativy včetně vazby na jednotlivé činnosti/agendy |  | • evidence přehledu  legislativy včetně vazby na jednotlivé činnosti/agendy |  |
|  | • Napojení na  RPP |  | • Napojení na RPP |  |
| Konektor Gemos | Konektor IAM musí umožnit napojení na Gemos s následující funkcionalitou:  • inicializační  načtení dat | ANO | Konektor IAM umožní napojení na  Gemos s následující funkcionalitou:  • inicializační načtení  dat | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
|  | • správa  lokálních identit |  | • správa lokálních  identit |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | • správa  oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |  | • správa oprávnění pro  jednotlivé uživatele ve formě přiřazení skupin nebo rolí |  |
| Konektor RŽP | Konektor IAM musí umožnit napojení na RŽP následující funkcionalitou:   * inicializační   načtení dat   * správa   lokálních identit a organizační struktury   * správa   oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | Konektor IAM umožní napojení na RŽP následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit a organizační struktury   * správa oprávnění pro   jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor ICA | Konektor IAM musí umožnit napojení na ICA s následující funkcionalitou:  • inicializační  načtení dat  • správa  lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | ANO | Konektor IAM umožní napojení na ICA s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Externí IDM | IAM bude obsahovat samostatnou část Portál pro správu externích uživatelů. Tato externí část IAM bude obsahovat konektor/rozhraní pro správu identit ze strany externích organizací. | ANO | IAM bude obsahovat samostatnou část Portál pro správu externích uživatelů. Tato externí část IAM bude obsahovat konektor/rozhraní pro správu identit ze strany externích organizací. | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Konektor App  Jednání (Shp) | Konektor IAM musí umožnit napojení na Sharepoint aplikaci App Jednání s následující funkcionalitou:  • inicializační  načtení dat  • správa  lokálních identit | ANO | Konektor IAM umožní napojení na Sharepoint aplikaci App Jednání s následující funkcionalitou:   * inicializační načtení   dat   * správa lokálních   identit | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |  | správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |  |
| Konektor JIP | Konektor IAM musí umožnit napojení na JIP s následující funkcionalitou:   * obousměrné   synchronizace s JIP   * automatické   pravidelné načítání informací z JIP do IDM   * automatické   předávání změněných údajů identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IDM do JIP včetně certifikátů   * automatické   předgenerování informací u nového uživatele, minimálně v rozsahu: přenesené celé jméno v potřebné struktuře, login složený z loginu použitého v AD plus prefix kupa\_ (tedy např. kupa\_novak1, kdy v AD je uživatel veden jako novakl - ne novak a ne novak2, přenesená pracovní emailová adresa, přenesené označení systemizovaného místa včetně čísla, je-li vyžadováno | ANO | Konektor IAM umožní napojení na JIP s následující funkcionalitou:   * obousměrné   synchronizace s JIP   * automatické   pravidelné načítání informací z JIP do IDM   * automatické   předávání změněných údajů identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IDM do JIP včetně certifikátů   * automatické   předgenerování informací u nového uživatele, minimálně v rozsahu: přenesené celé jméno v potřebné struktuře, login složený z loginu použitého v AD plus prefix kupa\_ (tedy např. kupa\_novak1, kdy v AD je uživatel veden jako novak1 - ne novak a ne novak2, přenesená pracovní emailová adresa, přenesené označení systemizovaného místa včetně čísla, je-li vyžadováno | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |

možnosti změny hesla uživatele v JIP prostřednictvím webového portálu IDM

možnosti změny hesla uživatele v JIP prostřednictvím webového portálu IDM

IDM - IAM řízení autentizace - funkční požadavky

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Parametr** | **Popis povinného parametru** | **Splňuje**  **ANO / NE** | **Uchazeč popíše detailní návrh způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| Licence | Poskytnutá licence umožní nasazení a provoz bez omezení na počet uživatelů, spravovaných uživatelů a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). | ANO | Poskytnutá licence umožňuje nasazení a provoz bez omezení na počet uživatelů, spravovaných uživatelů a napojených systémů. Neobsahuje žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Škálovatelnost | Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů. Systém bude podporovat režimu běhu ve vysoké dostupnosti. | ANO | Systém umožní zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů. Systém podporuje režimu běhu ve vysoké dostupnosti. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16. Authentication Module  (Autentizační brána) |
| SSO | Systém bude obsahovat službu autentizace pro napojené systémy formou jednotného webového přihlášení Single Sign On. Systém bude řídit připojení třetích aplikací pro federovanou autentizaci a autorizaci  (komunikace mezi  poskytovatelem identity (IdP) a poskytovatelem služeb (SeP)) pomocí SAML 2.0 protokolu a OpenID Connect. | ANO | Systém obsahuje službu autentizace pro napojené systémy formou jednotného webového přihlášení Single Sign On. Systém řídí připojení třetích aplikací pro federovanou autentizaci a autorizaci (komunikace mezi poskytovatelem identity (IdP) a poskytovatelem služeb (SeP)) pomocí SAML 2.0 protokolu a OpenID Connect. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16. Authentication Module  (Autentizační brána) |
| Autentizace | Autentizační brána musí umožnit autentizaci uživatelů v  integrovaných aplikacích. | ANO | Autentizační brána umožňuje autentizaci uživatelů v integrovaných aplikacích. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16. Authentication Module  (Autentizační brána) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NIA | Systém zprostředkuje ověření identity vůči externím  poskytovatelům identit NIA. Systém bude schopen fungovat v režimu IdP vůči poskytovatelů služeb (SeP). Systém bude dále vystupovat v režimu SeP vůči NIA. | ANO | Systém zprostředkuje ověření identity vůči externím poskytovatelům identit NIA. Systém je schopen fungovat v režimu IdP vůči poskytovatelů služeb (SeP). Systém bude dále vystupovat v režimu SeP vůči NIA. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.5 Poskytovatelé identit (IDP) |
| Vícefaktorová autentizace | Systém bude obsahovat modul pro zprostředkování autentizace přes a Active Directory a přes MFA systém. | ANO | Systém obsahuje modul pro  zprostředkování autentizace přes a Active Directory a přes MFA systém. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 3.1 Přihlášení do aplikace IDM  a MFA |
| Logování SIEM | Systém bude obsahovat logy o úspěšně i neúspěšně  přihlášených uživatelích. Logy bude možné předat do systému typu SIEM. | ANO | Systém obsahuje logy o úspěšně i neúspěšně přihlášených uživatelích. Logy bude možné předat do systému typu SIEM. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Historie | Autentizační brána musí  obsahovat historii a seznam všech sessions (komunikací) uživatelů a seznam všech requests - požadavků a response - odpovědí, které brána posílá na IdP nebo vrací do SeP. Tyto seznamy musí obsahovat informace o IdP, SeP, vazbě na konkrétní session a identifikaci uživatele. | ANO | Autentizační brána obsahuje historii a seznam všech sessions (komunikací) uživatelů a seznam všech requests - požadavků a response - odpovědí, které brána posílá na IdP nebo vrací do SeP. Tyto seznamy musí obsahovat informace o IdP, SeP, vazbě na konkrétní session a identifikaci uživatele. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitolac 16.11 Session,  16.10 Požadavky (Request) |
| Reporty a statistiky | Autentizační brána musí  obsahovat reporty a statistiky, minimálně přehled session, seznam request, seznam  response. Každý report musí umožnit volbu zobrazených sloupců a musí být  exportovatelný minimálně v těchto formátech - CSV, PDF, RTF, XSLX, HTML, XML. Tyto reporty a statistiky musí být možné importovat a zobrazit v městském IDM. | ANO | Autentizační brána obsahuje reporty a statistiky, minimálně přehled session, seznam request, seznam response. Každý report musí umožnit volbu zobrazených sloupců a musí být exportovatelný minimálně v těchto formátech - CSV, PDF, RTF, XSLX, HTML, XML. Tyto reporty a statistiky musí být možné importovat a zobrazit v městském IDM. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 17. Reporty |
| Uživatelé | Autentizační brána musí  obsahovat seznam uživatelů. | ANO | Autentizační brána obsahuje seznam uživatelů. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.12 Uživatelé |
| Přihlášení | Přihlašování přes autentizační bránu musí podporovat webové, mobilní a desktopové aplikace. | ANO | Přihlašování přes autentizační bránu podporuje webové, mobilní a desktopové aplikace. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16. Authentication Module  (Autentizační brána), 3.1 Přihlášení do  aplikace IDM a MFA |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Platnost přihlášení | Systém zajistí dle nastavení parametru v konfigurace  platnost tokenu pro přihlášení Single Sign On pro napojené aplikace. Po vypršení tohoto časového intervalu bude nutné se opět autentizovat. | ANO | Systém zajistí dle nastavení parametru v konfigurace platnost tokenu pro přihlášení Single Sign On pro napojené aplikace. Po vypršení tohoto časového intervalu bude nutné se opět autentizovat. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.5 Poskytovatelé identit (IDP) |
| Odhlášení | Autentizační brána musí  umožňovat odhlášení uživatele. Při odhlášení z libovolné aplikace nebo z autentizační brány dojde i k automatickému odhlášení ze všech aplikací, ve kterých je uživatel přihlášen za  předpokladu, že aplikace toto podporují. Brána bude obsahovat implementace odhlašování front­channel a back-channel pro protokoly SAML2 a OIDC. | ANO | Autentizační brána umožňuje odhlášení uživatele. Při odhlášení z libovolné aplikace nebo z autentizační brány dojde i k automatickému odhlášení ze všech aplikací, ve kterých je uživatel přihlášen za předpokladu, že aplikace toto podporují. Brána bude obsahovat implementace odhlašování front-channel a back-channel pro protokoly SAML2 a OIDC. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM  P, kapitola 16.4.1 Konfigurace poskytovatelů služeb |
| Integrace IDM | Autentizační brána bude  integrována na IDM zadavatele a přebírat evidenční a autorizační data uživatelů. | ANO | Autentizační brána je integrována na IDM zadavatele a přebírat evidenční a autorizační data uživatelů. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.12 Uživatelé |
| Integrace IdP | Autentizační brána bude  umožňovat napojení na tyto Identity providery (IdP):   * e-identita (NIA) * Datové schránky * LDAP | ANO | Autentizační brána bude umožňovat napojení na tyto Identity providery (IdP):   * e-identita (NIA) * Datové schránky * LDAP | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |
| Podpora elDAS | Systém 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. | ANO | Systém umožňuj 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. | Nab\_Aricoma\_MMP\_IDM, kapitola 5.1 Popis jednotlivých požadavků |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rozcestník autentizace | Systém obsahuje rozcestník pro výběr vhodného poskytovatele identit a autentizačního  prostředku. Pro jednotlivé poskytovatele služeb (SeP) bude možné v platformě konfigurovat seznam povolených  poskytovatelů identit (IdP) a úrovní autentizace (LoA). Seznam povolených IdP pro SeP musí být řízen pomocí vazby SeP - IdP. Vytvořením vazby dojde k povolení daného poskytovatele identit pro poskytovatele služeb a brána musí umožnit určit pořadí, v jakém se budou IdP nabízet pro SeP na straně rozcestníku identitní brány při autentizaci uživatele. | ANO | Systém obsahuje rozcestník pro výběr vhodného poskytovatele identit a autentizačního prostředku. Pro jednotlivé poskytovatele služeb (SeP) je možné v platformě konfigurovat seznam povolených poskytovatelů identit (IdP) a úrovní autentizace (LoA). Seznam povolených IdP pro SeP musí být řízen pomocí vazby SeP - IdP. Vytvořením vazby dojde k povolení daného poskytovatele identit pro poskytovatele služeb a brána musí umožnit určit pořadí, v jakém se budou IdP nabízet pro SeP na straně rozcestníku identitní brány při autentizaci uživatele. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.7 Vazba SEP a IDP |
| Perzistence dat | Systém využije pro perzistenci dat diskové úložiště a databázový systém | ANO | Systém využije pro perzistenci dat diskové úložiště a databázový systém. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16. Authentication Module  (Autentizační brána) |
| Úroveň autentizace - Level of Assurance  (LoA) | Jednotlivá uživatelská data poskytnutá přes autentizační bránu musí obsahovat informaci Level of Assurance (LoA).  Autentizační brána musí podporovat úrovně Level of Assurance (LoA) definovaných pomocí standardu ISO/IEC 29115. Úroveň LoA identifikuje zabezpečení a spolehlivost uložených hodnot, atributů a uživatelských údajů.  Autentizační brána musí evidovat informace o stupni LoA u každé uložené hodnoty a údaje.  Při získání nových hodnot jednotlivých údajů uživatele se zjistí, s jakou LoA se nové hodnoty získaly. Pokud nové hodnoty budou mít vyšší nebo stejnou úroveň LoA než předchozí uložené údaje, systém si tyto nové údaje uchová místo původních. | ANO | Jednotlivá uživatelská data poskytnutá přes autentizační bránu obsahují informaci Level of Assurance (LoA).  Autentizační brána podporuje úrovně Level of Assurance (LoA) definovaných pomocí standardu ISO/IEC 29115. Úroveň LoA identifikuje zabezpečení a spolehlivost uložených hodnot, atributů a uživatelských údajů. Autentizační brána musí evidovat informace o stupni LoA u každé uložené hodnoty a údaje.  Při získání nových hodnot jednotlivých údajů uživatele se zjistí, s jakou LoA se nové hodnoty získaly. Pokud nové hodnoty budou mít vyšší nebo stejnou úroveň LoA než předchozí uložené údaje, systém si tyto nové údaje uchová místo původních. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.8 Úrovně přístupu, 16.12.1 Konfigurace uživatelů |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Když si externí aplikace vyžádá přihlášení uživatele a získání jeho údajů s určitou úrovní LoA, autentizační brána zkontroluje, zdali všechny odpovídající údaje má k dispozici s požadovanou úrovní.  Pokud má uživatel na autentizační bráně již existující session, ale některý z požadovaných údajů chybí nebo má nedostatečné LoA, systém vyzve uživatele k novému přihlášení a nabídnuté IdP omezí pouze na ty, která mají dostatečné LoA.  Při vyžádání atributů s určitou LoA úrovní bude autentizační brána požadovat existenci těchto údajů s alespoň požadovanou úrovní a bude od uživatele požadovat přihlášení s daným LoA. |  | Když si externí aplikace vyžádá přihlášení uživatele a získání jeho údajů s určitou úrovní LoA, autentizační brána zkontroluje, zdali všechny odpovídající údaje má k dispozici s požadovanou úrovní.  Pokud má uživatel na autentizační bráně již existující session, ale některý z požadovaných údajů chybí nebo má nedostatečné LoA, systém vyzve uživatele k novému přihlášení a nabídnuté IdP omezí pouze na ty, která mají dostatečné LoA.  Při vyžádání atributů s určitou LoA úrovní bude autentizační brána požadovat existenci těchto údajů s alespoň požadovanou úrovní a bude od uživatele požadovat přihlášení s daným LoA. |  |
| Režimy ukládání dat | Systém autentizační brány bude možné provozovat v několika režimech rozdělených podle rozsahu ukládaných dat o identitě uživatele v rámci interní databáze. Volba režimu bude konfigurovatelná na úrovni vazby IdP - SeP, kde bude určen rozsah předávaných a ukládaných údajů. Součástí logiky provozovaných režimů je mechanismus na automatizaci promazávání  uživatelských účtů dlouhodobě nečinných nebo neaktivních uživatelů. Délku tohoto  parametru bude možné  konfigurovat.  Transparentní mód | ANO | Systém autentizační brány je možné provozovat v několika režimech rozdělených podle rozsahu ukládaných dat o identitě uživatele v rámci interní databáze. Volba režimu bude konfigurovatelná na úrovni vazby IdP - SeP, kde bude určen rozsah předávaných a ukládaných údajů. Součástí logiky provozovaných režimů je mechanismus na automatizaci promazávání  uživatelských účtů dlouhodobě nečinných nebo neaktivních uživatelů. Délku tohoto parametru bude možné konfigurovat.  Transparentní mód | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.7 Vazba SEP a IDP |

V transparentním módu nebudou ukládána žádná osobní data uživatelů. V tomto režimu vznikne pouze překladová databáze identifikátorů mezi různými identity providery (tj. mapovací tabulka uživatel - IdP). V tomto módu bude podpora LoA závislá na typu primárního poskytovatele identit. Pokud primární Identity provider

nepodporuje LoA, nebude možné informaci o LoA atributů

uživatele v tomto módu

poskytovat připojeným

aplikacím.

V transparentním módu nebudou ukládána žádná osobní data uživatelů. V tomto režimu vznikne pouze překladová databáze identifikátorů mezi různými identity providery (tj. mapovací tabulka uživatel - IdP). V tomto módu bude podpora LoA závislá na typu primárního poskytovatele identit. Pokud primární Identity provider nepodporuje LoA, nebude možné informaci o LoA atributů uživatele v tomto módu poskytovat připojeným aplikacím.

Plně perzistentní mód

Plně perzistentní mód

V tomto módu se po každé autentizaci uživatele na straně IdP provede kontrola a případná aktualizace dat o identitě uživatele, tj. uloží se kopie dat z IdP systému do interní databáze brány. Rozsah ukládaných metadat uživatelů bude konfigurovatelný správcem systému. V tomto režimu bude také možné aplikovat koncept LoA na data, která pochází i ze systémů, které LoA. K autentizaci uživatele na straně IdP dojde tehdy, pokud v databázi brány dosud není pro uživatele a IdP záznam nebo vypršela časová platnost evidovaných dat o identitě uživatele a nelze tedy použít data uložená v identitní bráně.

Hybridní mód

V tomto módu se po každé autentizaci uživatele na straně IdP provede kontrola a případná aktualizace dat o identitě uživatele, tj. uloží se kopie dat z IdP systému do interní databáze brány. Rozsah ukládaných metadat uživatelů bude konfigurovatelný správcem systému. V tomto režimu bude také možné aplikovat koncept LoA na data, která pochází i ze systémů, které LoA. K autentizaci uživatele na straně IdP dojde tehdy, pokud v databázi brány dosud není pro uživatele a IdP záznam nebo vypršela časová platnost evidovaných dat o identitě uživatele a nelze tedy použít data uložená v identitní bráně.

Hybridní mód

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Tento režim bude kombinací transparentního a plně  persistentního módu. V tomto režimu bude brána poskytovat identitu připojeným aplikacím obohacenou o některá data udržovaná v interní databázi systému. Např. doplní identitu o ověřené informace o uživateli z informačního systému IDM města či z jiného autoritativního zdroje a tyto informace poskytne integrovaným aplikacím. Na straně brány bude možné konfigurovat, zda pro daný IdP a SeP dojde k získání dat z externího systému, rozsah ukládaných dat do brány. |  | Tento režim bude kombinací  transparentního a plně persistentního módu. V tomto režimu bude brána poskytovat identitu připojeným aplikacím obohacenou o některá data udržovaná v interní databázi systému. Např. doplní identitu o ověřené informace o uživateli z informačního systému IDM města či z jiného autoritativního zdroje a tyto informace poskytne integrovaným aplikacím. Na straně brány bude možné konfigurovat, zda pro daný IdP a SeP dojde k získání dat z externího systému, rozsah ukládaných dat do brány. |  |
| Lokální účty | Autentizační brána bude  umožňovat evidenci lokálních účtů, prostřednictvím lokálního účtu je možné provést přihlášení do aplikací (SeP). Pro přihlášení lokálním účtem je možné nastavit druhý faktor (email nebo SMS s využitím SMS brány zadavatele). Pomocí druhého faktoru je realizován proces zapomenutého hesla.  Pro jednotlivé SeP bude možné zapínat/vypínat druhý faktor při autentizaci. | ANO | Autentizační brána umožňuje evidenci lokálních účtů, prostřednictvím lokálního účtu je možné provést přihlášení do aplikací (SeP). Pro přihlášení lokálním účtem je možné nastavit druhý faktor (email nebo SMS s využitím SMS brány zadavatele). Pomocí druhého faktoru je realizován proces zapomenutého hesla.  Pro jednotlivé SeP bude možné zapínat/vypínat druhý faktor při autentizaci. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.12 Uživatelé |
| Integrace SeP | Autentizační brána musí umožnit integrace na systémy úřadu (SeP) v rámci rozvoje autentizační brány bez jakýchkoliv omezení včetně licenčních. | ANO | Autentizační brána umožňuje integrace na systémy úřadu (SeP) v rámci rozvoje autentizační brány bez jakýchkoliv omezení včetně licenčních. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.4 Poskytovatelé služeb (SEP) |
| SeP | Autentizační brána bude  obsahovat seznam SeP a v tomto seznamu, stejně jako v ostatních seznamech v autentizační bráně, musí umožnit řazení, filtrování, vyhledávání a možnost přidat nebo odebrat sloupce seznamu a dále musí umožnit export do různých formátů včetně XML , CSV. | ANO | Autentizační brána obsahuje seznam SeP a v tomto seznamu, stejně jako v ostatních seznamech v autentizační bráně, musí umožnit řazení, filtrování, vyhledávání a možnost přidat nebo odebrat sloupce seznamu a dále musí umožnit export do různých formátů včetně XML , CSV. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.4 Poskytovatelé služeb (SEP) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rozšiřitelnost | Autentizační brána musí  umožňoval rozšiřitelnost o moduly pro přihlášení přes další poskytovatele identit (IdP), externí IdM nebo o moduly napojení na další systémy poskytující doplňující informace o uživateli.  Autentizační brána musí umožnit rozšíření atributů o další parametry poskytovatele služeb (SeP), o další parametry poskytovatele identit (IdP) a musí umožnit správu certifikátů pro podepisování nebo šifrování. Certifikáty musí umožnit přidat ručním zápisem nebo importem z metadat SeP nebo IdP. | ANO | Autentizační brána umožňuje  rozšiřitelnost o moduly pro přihlášení přes další poskytovatele identit (IdP), externí IdM nebo o moduly napojení na další systémy poskytující doplňující informace o uživateli.  Autentizační brána umožňuje rozšíření atributů o další parametry poskytovatele služeb (SeP), o další parametry poskytovatele identit (IdP) a musí umožnit správu certifikátů pro podepisování nebo šifrování. Certifikáty musí umožnit přidat ručním zápisem nebo importem z metadat SeP nebo IdP. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.4 Poskytovatelé služeb (SEP), 16.5 Poskytovatelé identit (IDP) |
| Rozhraní | Autentizační brána musí  obsahovat rozhraní pro správu uživatelů a jejich rolí a správu oprávnění, které musí být dostupné přes GUI a volitelně i přes API. Každý uživatel může mít více rolí zároveň. | ANO | Autentizační brána obsahuje rozhraní pro správu uživatelů a jejich rolí a správu oprávnění, které musí být dostupné přes GUI a volitelně i přes API. Každý uživatel může mít více rolí zároveň. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.12 Uživatelé |
| Správa | Každá aplikace může mít sadu vlastních dostupných rolí uložených v autentizační bráně. Autentizační brána musí umožnit tyto role přebírat z městského IDM, spravovat ručně přes GUI a volitelně i přes API. | ANO | Každá aplikace může mít sadu vlastních dostupných rolí uložených v autentizační bráně. Autentizační brána musí umožnit tyto role přebírat z městského IDM, spravovat ručně přes GUI a volitelně i přes API. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.13 Role |
| Správa | Autentizační brána musí  umožňovat aplikacím  specifikovat, které způsoby přihlášení lze pro autentizaci v aplikaci použít. | ANO | Autentizační brána umožňuje aplikacím specifikovat, které způsoby přihlášení lze pro autentizaci v aplikaci použít. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.7 Vazba SEP a IDP |
| Správa souhlasů | Autentizační brána musí  vynucovat udělení souhlasu uživatelem před předáním uživatelských dat (např. jméno a příjmení). Zároveň musí mít uživatel možnost souhlas kdykoliv odvolat.  Při založení uživatelského účtu musí být vynucen souhlas se smluvním vztahem (smluvními podmínkami) s vedením historie změn včetně ukončení smluvního vztahu. | ANO | Autentizační brána umí vynucovat udělení souhlasu uživatelem před předáním uživatelských dat (např. jméno a příjmení). Zároveň má uživatel možnost souhlas kdykoliv odvolat.  Při založení uživatelského účtu musí být vynucen souhlas se smluvním vztahem (smluvními podmínkami) s vedením historie změn včetně ukončení smluvního vztahu. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.17 Souhlasové formuláře |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Systém musí umožňovat  přeskočení fáze pro vyžadování  souhlasů (podmínek užití) na základě užitého Identity  providera. |  | Systém musí umožňovat přeskočení fáze pro vyžadování souhlasů (podmínek užití) na základě užitého Identity providera. |  |
| Správa souhlasů | Přihlašovací obrazovka,  obrazovka souhlas s předáním údajů a obrazovka pro odsouhlasení (souhlas)  podmínek užití dané služby musí být součástí autentizační brány.  Pro každou aplikaci bude možné definovat vlastní seznam dokumentů pro odsouhlasení podmínek užití včetně jejich obsahu.  V bráně se bude zobrazovat stránka odsouhlasení podmínek užití dané služby pro předání údajů do SeP až v okamžiku, kdy se uživatel úspěšně přihlásí. Stránka se tedy bude zobrazovat pouze úspěšně autentizovaným uživatelům za předpokladu, že již v minulosti nedošlo  k odsouhlasení podmínek užití dané služby případně podmínky nebyly aktualizovány.  Tyto dokumenty musí být zároveň v bráně verzovány, aby v případě aktualizace podmínek užití dané služby byl uživatel vyzván k udělení nového  souhlasu s novou verzí  dokumentu. Obecně lze souhlasy udělovat jednorázově nebo trvale. U každého trvalého souhlasu bude mít uživatel možnost ho následně odvolat, pomocí centrálního přehledu souhlasů. Při udělení trvalého souhlasu je při příštím přístupu uživatele obrazovka se souhlasy vynechána. Udělení souhlasů se provádí pro každou připojenou aplikaci zvlášť. | ANO | Přihlašovací obrazovka, obrazovka souhlas s předáním údajů a obrazovka pro odsouhlasení (souhlas) podmínek užití dané služby je součástí autentizační brány.  Pro každou aplikaci je možné definovat vlastní seznam dokumentů pro odsouhlasení podmínek užití včetně jejich obsahu.  V bráně se zobrazuje stránka odsouhlasení podmínek užití dané služby pro předání údajů do SeP až v okamžiku, kdy se uživatel úspěšně přihlásí. Stránka se tedy zobrazuje pouze úspěšně autentizovaným uživatelům za  předpokladu, že již v minulosti nedošlo k odsouhlasení podmínek užití dané služby případně podmínky nebyly aktualizovány.  Tyto dokumenty jsou zároveň v bráně verzovány, aby v případě aktualizace podmínek užití dané služby byl uživatel vyzván k udělení nového souhlasu s novou verzí dokumentu. Obecně lze souhlasy udělovat jednorázově nebo trvale. U každého trvalého souhlasu bude mít uživatel možnost ho následně odvolat, pomocí centrálního přehledu souhlasů. Při udělení trvalého souhlasu je při příštím přístupu uživatele obrazovka se souhlasy vynechána. Udělení souhlasů se provádí pro každou připojenou aplikaci zvlášť. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.17 Souhlasové formuláře |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| API | Autentizační brány musí  obsahovat zabezpečené  zdokumentované webové  rozhraní API na REST architektuře. Zabezpečení API bude provedeno pomocí přístupového tokenu, který uživatel získá při přihlášení. | ANO | Autentizační brány obsahuje zabezpečené zdokumentované webové rozhraní API na REST architektuře. Zabezpečení API je provedeno pomocí přístupového tokenu, který uživatel získá při přihlášení. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16. Authentication Module  (Autentizační brána) |
| Registrace | Rozhraní autentizační brány musí obsahovat správu profilu uživatele, kde je možné párovat profily pro jednotlivé  poskytovatele identit. | ANO | Rozhraní autentizační brány obsahuje správu profilu uživatele, kde je možné párovat profily pro jednotlivé poskytovatele identit. | Aricoma\_ID\_ACIdentitaUzivatelskaPrirucka\_MM P, kapitola 16.12 Uživatelé |

Požadovaná podpora v následujícím rozsahu:

poskytování služby servisní a technické podpory řešení v délce 5 let od spuštění ostrého provozu s následujícími parametry:

garance reakční doby a řešení incidentů do úrovně obnovy funkčnosti v původním stavu, hlášení požadavků v HelpDesku Zhotovitele v režimu 7 x 24, komunikace v českém jazyce, hlášení požadavků telefonicky v režimu 5 x 12, komunikace v českém jazyce, pravidelný report čerpání podpory a řešených incidentů (součást faktury), technická podpora zahrnuje podporu produktu výrobcem i servisní podporu, cena za tyto podpory je společná, údržba systému (profylaxe) jednou za měsíc v rozsahu 4 hodin, konzultace a rozvoj řešení v rozsahu 4 hodin za měsíc, nevyčerpané hodiny v rámci měsíce, lze vyčerpat nejpozději do jednoho roku od jeho uplynutí, nárok na opravy (patche) odstraňující známé chyby nebo zranitelnosti včetně jejich nasazení, nárok na nové verze systému.

Kategorie závady

Kategorie A

IDM-IAM, nebo jeho část/služba není použitelná ve svých základních funkcích a parametrech nebo se vyskytuje funkční závada znemožňující činnost a řádné užití systému nebo jeho části/služby. Tento stav ohrožuje nebo znemožňuje běžný provoz, případně může Objednateli nebo dalším subjektům způsobit větší finanční nebo jiné škody. Tento stav může ohrozit běžný provoz Objednatele a nelze jej dočasně řešit organizačním opatřením.

Kategorie B

Funkčnost IDM -IAM nebo jeho části/služby nebo rozsah služeb Objednatele je ve svých funkcích a parametrech degradována tak, že tento stav omezuje běžný provoz systému nebo omezuje řádné užití nebo jeho části/služby a nebo služeb Objednatele. Existuje náhradní pracovní postup pro obejití závady, případně organizační opatření.

Kategorie C

Ostatní - drobné závady, které nespadají do kategorie A a/nebo B.

Zařazení vady do jednotlivých kategorií určuje Objednatel.

Parametry SLA

Kategorie vady - Reakční lhůty v pracovní době, Doba odstranění vady na produkčním prostředí

A - Vysoká - 4 hodiny, Do 8 hodin

B - Střední - 8 hodin, Do 48 hodin C - Nízká - 16 hodin, Best effort

Reakční lhůtou se rozumí doba od zahájení požadavku do doby potvrzení zahájení jeho řešení. Reakční lhůta a doba na odstranění vady běží pouze v pracovní době.

3. Nabídková cena

VZ: Kybernetická bezpečnost Pardubice - posílení informačních systémů (IS) v rámci zabezpečení kyberbezpeč Příloha č. 2

Specifikace - nabídkový list - pro ČÁST 1: Identity management systém (IDM - IAM)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Licence** | **Počet** | **Jednotková cena v Kč bez DPH** | **Cena celkem bez DPH** | **Cena celkem vč.**  **DPH** |
| SW IDM | 1 | 220 000,00 Kč | 220 000,00 Kč | 266 200,00 Kč |
| Konektor Vema | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor AD | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor VITA | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor GEMOS | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor GINIS | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor Cityware Geovap | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor App Jednání (Shp) | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor MS PowerApps | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor MS O365 | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor WEB (GIANT) | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor RPP | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor JIP | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor ICA | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Konektor RŽP | 1 | 40 000,00 Kč | 40 000,00 Kč | 48 400,00 Kč |
| Authentizační brána | 1 | 220 000,00 Kč | 220 000,00 Kč | 266 200,00 Kč |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nabídková cena** | **Počet** |  | **Cena celkem bez DPH** | **Cena celkem vč.**  **DPH** |
| Implementace, konfigurace, zaškolení, dokumenta | 1 | 2 132 000,00 Kč | 2 132 000,00 Kč | 2 579 720,00 Kč |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nabídková cena** | **Počet roků** | **Cena na 1 rok/Kč bez DPH** | **Cena celkem za 5 let/ Kč bez DPH** | **Cena celkem za 5 let/ Kč vč. DPH** |
| Podpora a servis | 5 | 360 000,00 Kč | 1 800 000,00 Kč | 2 178 000,00 Kč |

REKAPITULACE

|  |  |  |
| --- | --- | --- |
| **Celková cena** | **Cena celkem bez DPH** | **Cena celkem vč.**  **DPH** |
| Licence+implementace, konfigurace, zaškolení, dokumentace+podpora a servis na 5 le | 4 932 000,00 Kč | 5 967 720,00 Kč |