Název veřejné zakázky: **KYBEZ města Litvínov – Implementace terminálových služeb zabezpečených vícefaktorovým ověřováním – RDS; §25 Aplikační bezpečnost vyhlášky č. 82/2018 o kybernetické bezpečnosti**

systémové číslo: P25V00000111

# Předmět veřejné zakázky

Předmětem veřejné zakázky je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele (dále také jen „dodávka“, „systém“, „řešení“ nebo „technologie“). Dodavatel, se kterým bude uzavřena smlouva na plnění veřejné zakázky, je povinen poskytnout zadavateli dodávky a služby uvedené v následující tabulce a dále specifikované v dalších článcích této přílohy, jakož i takové související plnění, které je nezbytné pro řádné poskytnutí takových dodávek a služeb a funkčnost takových dodávek a služeb v prostředí zadavatele:

| **Zajišťovaná oblast** | **Stručný popis položky** |
| --- | --- |
| Zajištění aplikační bezpečnosti dle § 25 vyhlášky č. 82/2018 Sb. prostřednictvím centralizovaného přístupu k IS pomocí terminálových služeb, které minimalizují rizika manipulace a neoprávněného zásahu na straně klientských zařízení. | * Pořízení SW licencí terminálových služeb. * Pořízení mobilní aplikace umožňující vícefaktorovou autentizaci. * Implementace a související služby. |

Doporučuje se, aby dodavatel při realizaci veřejné zakázky postupoval podle doporučení výrobců dodávaného plnění a dle tzv. nejlepších praktik.

U technických parametrů plnění, u kterých není výslovně uvedeno, že jde o požadovanou minimální či maximální hodnotu, lze nabídnouti řešení „lepší“, tedy řešení přesahující (ve smyslu výhodnějším z pohledu užitné hodnoty) hodnotu stanoveného požadavku, pokud z této přílohy výslovně nevyplývá, že musí být splněna přesně daná hodnota.

# Stávající a cílový stav

Zadavatel provozuje vysoce dostupnou virtualizovanou infrastrukturu založenou na technologiích VMware a Microsoft. Tato infrastruktura je umístěna na třech fyzických serverech se softwarově definovaným úložištěm a disponuje dostatečnou výkonovou rezervou pro plánované rozšíření. Zadavatel má k dispozici licence Windows Server 2022 Datacenter, které umožňují provoz neomezeného počtu virtuálních serverů.

Většina klíčových informačních systémů (např. GINIS, VITA, FLUX, PowerKey) je v současnosti provozována v modelu klient–server, kdy aplikační klienty běží přímo na koncových pracovních stanicích uživatelů.

Zadavatel požaduje vybudování bezpečné a centralizované platformy pro vzdálený přístup zaměstnanců a spolupracujících osob k aplikačním prostředím i celým uživatelským desktopům. „Desktopem“ se v tomto kontextu rozumí buď pracovní plocha uživatele v rámci virtuálního prostředí, nebo samostatný desktopový operační systém provozovaný na serverové infrastruktuře – souhrnně označováno jako VDI (Virtual Desktop Infrastructure).

Technické řešení bude navrženo s maximálním využitím stávajících kapacit – fyzických serverů, úložišť, síťových prvků, zálohovacích a bezpečnostních systémů. Pro provoz systému VDI budou pořízeny nezbytné softwarové licence včetně vícefaktorovoého řešení, které zabezpečí ověřování externích uživatelů.

Pro bezpečný přístup externích uživatelů (např. zaměstnanců pracujících na dálku nebo pracovníků spolupracujících organizací) bude zřízen webový aplikační portál, který umožní přístup ke vzdáleným aplikacím a desktopům prostřednictvím webového rozhraní. Portál bude zabezpečen pomocí hvězdičkového SSL certifikátu vydaného důvěryhodnou certifikační autoritou, přičemž tento certifikát bude zajištěn zadavatelem.

Implementace VDI přinese sjednocení uživatelských pracovních prostředí, sníží nároky na jejich správu a umožní prodloužení životního cyklu koncových zařízení. Přesun uživatelských dat do centrální infrastruktury zároveň významně zvýší úroveň jejich zabezpečení proti ztrátě, poškození či kompromitaci.

Součástí dodávky bude veškeré potřebné licencování pro provoz 70 uživatelských relací v rámci nové virtualizační platformy včetně vícefaktorového ověřování pomocí mobilní aplikace.

# Implementační služby

## Obecné požadavky

Zadavatel požaduje provedení následujících implementačních činností. Rozsah služeb zahrnuje minimálně tyto kroky:

* **Zpracování prováděcí dokumentace**, která musí být před zahájením realizace dodávek schválena zadavatelem. Tato dokumentace bude zahrnovat:
  + předimplementační analýzu,
  + návrh cílového konceptu řešen.
* **Dodávku a implementaci řešení** v souladu se schváleným cílovým konceptem.
* **Zajištění projektového řízení** po celou dobu realizace zakázky.
* **Zpracování školicích materiálů a realizaci školení** pro 3 administrátory v sídle zadavatele v rozsahu 1 pracovního dne.
* **Zajištění zkušebního provozu** v délce minimálně 14 kalendářních dnů. Během tohoto období musí být k dispozici technická podpora alespoň jednoho specialisty na dodané řešení, s maximální dobou reakce 3 hodiny od nahlášení požadavku v pracovních dnech mezi 8:00 a 17:00.
* **Předání systému do ostrého provozu**. Akceptace bude provedena pouze v případě úspěšného ukončení bezproblémového zkušebního provozu.

Veškeré náklady spojené s implementačními službami a školením musí být zahrnuty v nabídkové ceně (neuvádějí se samostatně).

Všechny dodané dokumenty musí být vyhotoveny výhradně v českém jazyce a předány v elektronické podobě ve standardních formátech používaných zadavatelem (např. MS Office).

## Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude vycházet z předimplementační analýzy a bude obsahovat veškeré aktivity nezbytné pro úspěšnou realizaci předmětu plnění.

Předimplementační analýza bude reflektovat aktuální prostředí zadavatele a navrhované řešení dodavatele. Minimálně bude zahrnovat tyto oblasti:

* Analýzu stávající konfigurace a vazeb na související systémy,
* Identifikaci požadované součinnosti ze strany zadavatele.

Na základě této analýzy bude vytvořen cílový koncept, který zohlední výchozí stav i technické parametry nabízeného řešení. Cílový koncept bude obsahovat minimálně:

* podrobný popis cílového stavu a funkcionality jednotlivých částí řešení,
* přehled nutných a doporučených optimalizačních a konfiguračních změn navázaných systémů,
* způsob zajištění jednotlivých dodávek a služeb, včetně časového harmonogramu,
* detailní návrh implementačního postupu,
* způsob zajištění informační bezpečnosti,
* projektový harmonogram s vyznačením klíčových milníků,
* popis vazeb na stávající systémy a jejich konfiguraci,
* návrh akceptačních kritérií a testovacích scénářů,
* specifikaci školení, jejich obsahu a rozsahu,
* přehled a strukturu provozní dokumentace.

V návrhu akceptačních kritérií a testovacích scénářů budou minimálně tyto kritéria:

* Uživatel se registruje do uživatelského portálu vícefaktorového řešení, provede instalaci aplikace na svém mobilním zařízení a před přihlášením k RDS Host serveru se vícefaktorově ověří.
* Uživatel se přihlásí na „celý“ desktop a uvidí kompletní prostředí RDS Host serveru, které odpovídá prostředí desktopového operačního systému Windows.
* Uživateli se spustí pouze publikovaná aplikace, která je graficky plně integrovaná do stávajícího klientského operačního systému nebo zpřístupněna přes webové rozhraní.
* Uživateli má možnost přihlásit se na svou desktopovou stanici přes webový https portál.
* Vybraný uživatel provede testovací tisk.
* Proběhlo zaškolení obsluhy v rozsahu 1 dne na místě pro 3 administrátory.
* V Active Directory existují skupiny pro definic přístupů k plnému desktopu i webovému portálu.

Po předání dokumentace bude mít zadavatel lhůtu 10 pracovních dnů na její připomínkování. Dodavatel je povinen všechny připomínky vypořádat – buď jejich zapracováním, nebo formou písemného a odůvodněného odmítnutí v případě, že je považuje za nevalidní. Zadavatel nebude dokumentaci opravovat, ale pouze vyznačí věcné nebo formální nedostatky.

Prováděcí dokumentace musí být výslovně schválena zadavatelem před zahájením dalších etap plnění.

Po realizaci implementace bude dokumentace aktualizována dle skutečně provedeného stavu, včetně všech konfigurací, nastavení a analytických výstupů. Tato aktualizovaná dokumentace bude nedílnou součástí dokumentace předávané v rámci akceptačního protokolu.

# Požadované parametry technického řešení

## Terminálové služby

Řešení musí být univerzální, modulární a škálovatelné, s možností jednoduchého rozšíření přidáváním RDS hostitelů bez nutnosti zásahu do architektury nebo redesignu systému.

Implementace terminálových služeb bude minimálně v tomto rozsahu:

* Příprava prostředí pro 70 uživatelských relací.
* Testování funkčnosti aplikací, periferních zařízení (např. tiskáren) a jejich chování v terminálovém režimu.
* Instalace a konfigurace standardních aplikací a běžných nástrojů.
* Vyhodnocení testů a identifikace případných potřeb úprav.
* Upřesnění technického návrhu dle výsledků testování.
* Nasazení do ověřovacího provozu pro určenou testovací skupinu uživatelů.
* Zpracování dokumentace skutečného provedení řešení.
* Zaškolení správců a technické obsluhy systému.

Uživatelům bude zpřístupněn webový aplikační portál s možností přístupu k publikovaným aplikacím i kompletním vzdáleným desktopům. Přístupová práva a rozsah oprávnění budou řízena prostřednictvím skupin v Active Directory.

V rámci AD bude vytvořena speciální organizační jednotka (OU) se sadou skupinových politik (GPO), které zajistí transformaci klasických PC do role tenkých klientů. Tato zařízení budou mít uzamčený operační systém a budou sloužit výhradně pro připojení k terminálové infrastruktuře. Tím se prodlouží jejich životní cyklus a výrazně sníží nároky na jejich správu.

Nabízené licence musí splňovat požadavky:

* Kompatibilita s Windows Server 2022 Datacenter nebo kompatibilita s Windows Server 2025 Datacenter s možností downgrade.
* Licence může být i druhotná, musí ale splňovat podmínky pro legální převod vlastnictví:
  + První země použití byla v rámci EU/EHP nebo Švýcarsko.
  + Produkt byl plně uhrazen vlastníkovi autorských práv.
  + Produkt je trvalý a jeho použití není časově omezeno.
  + Produkt již není používán jiným majitelem.
  + Součástí těchto nabízených licencí musí být dodání dokumentace o legálnosti v souladu s výše uvedenými podmínkami, s právními předpisy EU a ČR.
* Licence musí být trvalá (perpetual).
* Licence musí být na uživatele (user).

## Vícefaktorové řešení

Řešení musí být univerzální, modulární a škálovatelné, s možností jednoduchého rozšíření přidáváním uživatelů bez nutnosti zásahu do architektury nebo redesignu systému.

Implementace vícefaktorového řešení bude minimálně v tomto rozsahu:

* Příprava prostředí pro 70 uživatelů.
* Testování funkčnosti vícefaktorového ověřování v terminálovém režimu.
* Vyhodnocení testů a identifikace případných potřeb úprav.
* Upřesnění technického návrhu dle výsledků testování.
* Nasazení do ověřovacího provozu pro určenou testovací skupinu uživatelů.
* Zpracování dokumentace skutečného provedení řešení.
* Zaškolení správců a technické obsluhy systému.

Implementované vícefaktorové řešení bude splňovat technické požadavky minimálně v tomto rozsahu:

* Řešení je připraveno pro použití jako cloudová služba, ale i s možností ostrovního režimu (v případě nedostupnosti cloudové služby z on-prem prostředí musí řešení poskytnout záložní off-line variantu autentizace pomocí jednorázového časového autentizačního kódu, který uživatel vygeneruje v mobilní aplikaci).
* Řešení umožňuje stažení autentizační aplikace z Google Play a Apple Store.
* Řešení podporuje ověření metodou QR kódu bez nutnosti zadávat uživatelské jméno, a to i pokud je zařízení off-line.
* Řešení funguje v těchto scénářích vícefaktorové autentizace:
  + do OS MS Windows,
  + do aplikací s RADIUS protokolem,
  + do RDS Gateway.
* Metody autentizačního serveru a mobilní aplikace musí být:
  + Push notifikace,
  + OTP heslo.
* Řešení obsahuje uživatelský portál pro aktivaci a správu autentizační metody pomocí mobilní aplikace. Portál poskytuje možnosti prohledávání uživatelů a zobrazení jejich detailu. Detail uživatele obsahuje informace o stavu mobilní autentizační metody a zobrazení historie autentizačních požadavků. Onboarding uživatele bez nutnosti interakce s administrátorem.
* Faktory ověření v mobilní aplikaci musí být:
  + Biometrika při autentizaci,
  + 6 místné PIN.
* Řešení musí podporovat identity z Entra ID a zároveň z on-prem Active Directory.
* Mobilní aplikace musí obsahovat ochranu pomocí RASP technologie a zabezpečit detekci:
  + instalace aplikace z nedůvěryhodného zdroje,
  + přebalení aplikace,
  + root/jailbreak OS,
  + napojení na debug nástroje,
  + nástrojů pro odposlouchávání aktivity,
  + využití zámku telefonu a jeho změny.

Licence nabízeného vícefaktorového řešení musí splňovat požadavky:

* Kompatibilita s Windows Server 2022 Datacenter.
* Licence může být i druhotná, musí ale splňovat podmínky pro legální převod vlastnictví:
  + První země použití byla v rámci EU/EHP nebo Švýcarsko.
  + Produkt byl plně uhrazen vlastníkovi autorských práv.
  + Produkt je trvalý a jeho použití není časově omezeno.
  + Produkt již není používán jiným majitelem.
  + Součástí těchto nabízených licencí musí být dodání dokumentace o legálnosti v souladu s výše uvedenými podmínkami, s právními předpisy EU a ČR.
* Licence musí být trvalá (perpetual).
* Licence musí být na uživatele (user).
* Licence musí být pro 70 uživatelů.

# Nabídka uchazeče

|  |  |  |  |
| --- | --- | --- | --- |
| **Zajišťovaná oblast** | **Funkcionalita** | **Účastník splňuje ANO/NE** | **Detail naplnění požadavku (vyplní účastník)** |
| Licence terminálových služeb | Kompatibilita s Windows Server 2022 Datacenter nebo kompatibilita s Windows Server 2025 Datacenter s možností downgrade. |  |  |
| Licence může být i druhotná, musí ale splňovat podmínky pro legální převod vlastnictví:   * První země použití byla v rámci EU/EHP nebo Švýcarsko. * Produkt byl plně uhrazen vlastníkovi autorských práv. * Produkt je trvalý a jeho použití není časově omezeno. * Produkt již není používán jiným majitelem. * Součástí těchto nabízených licencí musí být dodání dokumentace o legálnosti v souladu s výše uvedenými podmínkami, s právními předpisy EU a ČR. |  |  |
| Licence musí být trvalá (perpetual). |  |  |
| Licence musí být na uživatele (user). |  |  |
| Licence musí být pro 70 uživatelů. |  |  |
| Implementace v minimálním rozsahu:   * Příprava prostředí pro 70 uživatelských relací. * Testování funkčnosti aplikací, periferních zařízení (např. tiskáren) a jejich chování v terminálovém režimu. * Instalace a konfigurace standardních aplikací a běžných nástrojů. * Vyhodnocení testů a identifikace případných potřeb úprav. * Upřesnění technického návrhu dle výsledků testování. * Nasazení do ověřovacího provozu pro určenou testovací skupinu uživatelů. * Zpracování dokumentace skutečného provedení řešení. * Zaškolení správců a technické obsluhy systému. * Uživatelům bude zpřístupněn webový aplikační portál s možností přístupu k publikovaným aplikacím i kompletním vzdáleným desktopům. Přístupová práva a rozsah oprávnění budou řízena prostřednictvím skupin v Active Directory. * V rámci AD bude vytvořena speciální organizační jednotka (OU) se sadou skupinových politik (GPO), které zajistí transformaci klasických PC do role tenkých klientů. Tato zařízení budou mít uzamčený operační systém a budou sloužit výhradně pro připojení k terminálové infrastruktuře. Tím se prodlouží jejich životní cyklus a výrazně sníží nároky na jejich správu. |  |  |
| Řešení vícefaktorového ověřování | Řešení je připraveno pro použití jako cloudová služba, ale i s možností ostrovního režimu (v případě nedostupnosti cloudové služby z on-prem prostředí musí řešení poskytnout záložní off-line variantu autentizace pomocí jednorázového časového autentizačního kódu, který uživatel vygeneruje v mobilní aplikaci). |  |  |
| Řešení umožňuje stažení autentizační aplikace z Google Play a Apple Store. |  |  |
| Řešení podporuje ověření metodou QR kódu bez nutnosti zadávat uživatelské jméno, a to i pokud je zařízení off-line. |  |  |
| Řešení funguje v těchto scénářích vícefaktorové autentizace:   * do OS MS Windows, * do aplikací s RADIUS protokolem, * do RDS Gateway. |  |  |
| Metody autentizačního serveru a mobilní aplikace musí být:   * Push notifikace, * OTP heslo. |  |  |
| Řešení obsahuje uživatelský portál pro aktivaci a správu autentizační metody pomocí mobilní aplikace. Portál poskytuje možnosti prohledávání uživatelů a zobrazení jejich detailu. Detail uživatele obsahuje informace o stavu mobilní autentizační metody a zobrazení historie autentizačních požadavků. Onboarding uživatele bez nutnosti interakce s administrátorem. |  |  |
| Faktory ověření v mobilní aplikaci musí být:   * Biometrika při autentizaci, * 6 místné PIN. |  |  |
| Řešení musí podporovat identity z Entra ID a zároveň z on-prem Active Directory. |  |  |
| Mobilní aplikace musí obsahovat ochranu pomocí RASP technologie a zabezpečit detekci:   * instalace aplikace z nedůvěryhodného zdroje, * přebalení aplikace, * root/jailbreak OS, * napojení na debug nástroje, * nástrojů pro odposlouchávání aktivity, * využití zámku telefonu a jeho změny. |  |  |
| Kompatibilita s Windows Server 2022 Datacenter. |  |  |
| Licence může být i druhotná, musí ale splňovat podmínky pro legální převod vlastnictví:   * + První země použití byla v rámci EU/EHP nebo Švýcarsko.   + Produkt byl plně uhrazen vlastníkovi autorských práv.   + Produkt je trvalý a jeho použití není časově omezeno.   + Produkt již není používán jiným majitelem.   + Součástí těchto nabízených licencí musí být dodání dokumentace o legálnosti v souladu s výše uvedenými podmínkami, s právními předpisy EU a ČR. |  |  |
| Licence musí být trvalá (perpetual).  Licence musí být na uživatele (user). |  |  |
| Licence musí být pro 70 uživatelů. |  |  |
| Implementace v minimálním rozsahu:   * Příprava prostředí pro 70 uživatelů. * Testování funkčnosti vícefaktorového ověřování v terminálovém režimu. * Vyhodnocení testů a identifikace případných potřeb úprav. * Upřesnění technického návrhu dle výsledků testování. * Nasazení do ověřovacího provozu pro určenou testovací skupinu uživatelů. * Zpracování dokumentace skutečného provedení řešení. * Zaškolení správců a technické obsluhy systému. |  |  |