Název zakázky: Pořízení a implementace systému pro multifaktorovou autentizaci (MFA)
Číslo zakázky: P25V00000028
Zadavatel: Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

1. Cena dodávky

		Počet ks. / hod.	Cena celkem bez DPH	DPH	Cena celkem včetně DPH
I.	**MFA**	[redacted]	1 514 816,00 Kč	318 111,36 Kč	1 832 927,36 Kč
II.	**Klávesnice se čtečkou ČK**		279 000,00 Kč	58 590,00 Kč	337 590,00 Kč
III.	**Čtečka karet**		15 750,00 Kč	3 307,50 Kč	19 057,50 Kč
IV.	**Čipové karty**		378 292,50 Kč	79 441,43 Kč	457 733,93 Kč
V.	**Hodinová sazba**		1 950,00 Kč	409,50 Kč	2 359,50 Kč

2. Technická specifikace předmětu plnění veřejné zakázky

Předmětem zakázky je pořízení a implementace systému pro multifaktorovou autentizaci uživatelů (MFA), včetně správy digitálních certifikátů, nástroje pro jednotnou správu hesel uživatelů, dodání hybridních čipových karet a klávesnic se čtečkou čipových karet. Dodaný systém musí splňovat legislativní požadavky NIS2, eIDAS 2.0 a zákon o kybernetické bezpečnosti (dále jen všechny legislativní požadavky). Součástí plnění budou veškeré potřebné licence, software, hardware, implementace, technická dokumentace k dodanému řešení a zaškolení IT zaměstnanců objednavatele.

a) Popis prostředí objednavatele

Virtualizační platforma vSphere 8. Pro správu identit využívá objednavatel MS Active Directory, verze OS Windows Server 2022 a identity management AC Identita verze 5.4.2. K evidenci docházky a řízení přístupu pro vstup do jednotlivých objektů a prostor jsou využívány bezkontaktní čipové karty s datovým rozhraním MIFARE, kompatibilní s technologií EM4102 125kHz. V současnosti objednavatel využívá certifikační autoritu První certifikační autorita, a.s. (I.CA). Objednavatel provozuje přibližně 500 koncových stanic (desktop, notebook).

b) Popis požadovaného řešení

Objednavatel očekává od dodaného systému MFA zvýšení kybernetické bezpečnosti a splnění všech legislativních požadavků v rámci kybernetické bezpečnosti. Rovněž zajištění bezpečného a komfortního přihlašování uživatelů do operačního systému, včetně jednotného místa pro bezpečné ukládání a správu jejich hesel. Řešení bude umožňovat automatizovanou správu komerčních a kvalifikovaných certifikátů uživatelů s minimální nutností zásahů administrátorů klientské registrační autority.

Parametr	Požadavek
Systém MFA	• Dodané řešení musí být automaticky synchronizováno s AD/IDM objednavatele, a to zabezpečeným způsobem. Při nástupu nového zaměstnance objednavatele musí systém automaticky

	získat potřebné údaje. Automatická synchronizace identit a všech změn v AD DS. Definice práv na základě členství v AD skupinách, včetně možnosti vytvářet různé kombinace oprávnění. • Řešení umožní uživatelům objednavatele přihlášení do svých pracovních stanic svým doménovým účtem s autentizací prostřednictvím čipových karet s využitím certifikátu X.509 z interní certifikační autority a pinu, případně aplikace mobilního telefonu (podpora Android a iOS). • PIN si bude moci každý uživatel změnit v klientské aplikaci bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním. V klientské aplikaci bude mít uživatel přehled o svých údajích, certifikátech, pinech a heslech. • Zapomenutý nebo uzamčený PIN si budou moci uživatelé resetovat prostřednictvím PUKu bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním. Systém zajistí zabezpečeným způsobem správu PUKu. • Systém umožní více-faktorové ověření uživatelů na bázi certifikátů X.509 při přihlášení do PC, VPN, tak aby byly splněny všechny legislativní požadavky. • Systém musí umožňovat konfiguraci různých typů MFA, včetně biometrických metod a aplikací generujících kódy. • Prostřednictvím dodaného systému bude možno vydávat, prodlužovat, či zneplatňovat interní, kvalifikované a komerční certifikáty dle nařízení eIDAS. Tento proces bude probíhat v takovém režimu, aby objednavatel mohl systém využívat a provozovat pomocí méně kvalifikovaných zaměstnanců. • Prodloužení (obnovení) certifikátů bude probíhat automaticky bez zásahu operátora přímo na klientské stanici v režii samotného uživatele, v souladu s eIDAS a v rámci jednoho systému. Operátor pouze schvaluje (povoluje) žádosti o obnovu. • Recyklace čipové karty bude probíhat v rámci dodaného systému a organizace objednavatele bez využití uživatelského rozhraní třetích stran. Kvalifikovaný prostředek nesmí opustit prostředí organizace. Pro účely recyklace nesmí být používán PIN čipové karty. • Systém zajistí, že vydávání jak interních certifikátů (X.509) tak i certifikátů od akreditovaných CA (komerční, kvalifikované) bude zajištěno ve stejném uživatelském rozhraní, v rámci jednotného systému. • Podporovány musí být minimálně dvě akreditované certifikační autority. • Při blížící se expiraci certifikátu musí být zasílány uživatelům notifikace s možností nastavit časové limity při kterých se notifikace aplikují. Možnost nastavit odesílání těchto notifikací i operátorům. • Požadavkem je synchronizace s CzechPOINT – JIP, minimálně v rámci zápisu sériových čísel certifikátů. • Dodavatel musí zajistit dodávku kvalifikovaných a komerčních certifikátů od certifikační autority v termínu dohodnutém s objednavatelem při předimplementační analýze. • Proces vydání kvalifikovaného certifikátu by měl probíhat bez zbytečných prodlev, zajišťující kontinuitu služby a efektivitu řešení výdejů certifikátů se zachováním všech bezpečnostních a

	legislativních standardů. Vhodná je automatizace těchto procesů a eliminace potřeby lidského faktoru. • Dodaný systém musí poskytovat nástroj pro centrální správu čipových karet, certifikátů a dalších náležitostí pro administrátory a operátory a také klientskou část pro koncové uživatele. • Role operátora bude zajišťovat úkony spojené s vydáváním a správou životního cyklu kvalifikovaných prostředků pro uživatele, přiřazovat karty, vydávání interních certifikátu a ověření identity uživatelů. • Operátor nemůže vydávat čipové karty uživatelům bez vlastního autentizačního prostředku zajišťujícího více-faktorovou autentizaci jeho osoby. • Systém musí uchovávat všechny informace o uživateli a jeho přiřazené čipové kartě tak, aby byl schopen je zprostředkovat dalším systémům v rámci možných integrací. • Systém musí být schopen obsloužit minimálně 500 uživatelů – přiřazení autentizačních prostředků, správa digitálních certifikátů, správa hesel. • Systém bude umožňovat také evidenci a správu serverových a aplikačních certifikátů objednavatele, včetně notifikací ohledně jejich stavu a expirace. Toto funkce musí být dostupná pro všechny infrastrukturní zařízení objednavatele (Servery, Firewall, VPN atd.). • Serverový agent by měl být schopen najít automaticky dostupné certifikáty z konfiguračních souborů nebo databází programů, jako jsou Nginx, Apache, Microsoft Certificate Store (Webhosting,Personal). • Serverový agent musí být propojen se serverem pro evidenci certifikátů a musí zasílat veřejný obsah všech nalezených certifikátů. • Centrální evidence musí obsahovat modul s evidenci serverů a seznamem všech certifikátů s informacemi o jejich expiraci, historii smazaných certifikátů, blížící se expirace, nekomunikujících serverech, případně serverech bez certifikátu. • Centrální evidence serverových certifikátů musí obsahovat možnost notifikací, které budou zasílány určeným osobám nebo skupinám na základě jejich rolí a práv. • Zajištěna musí být podpora provozovaných systému objednavatele, minimálně Linux (RedHat, Debian, Ubuntu), Windows Server 2022.
Čipové karty	• Dodané bezkontaktní hybridní čipové karty musí být kompatibilní s technologií EM4102 s frekvencí 125kHz a v souladu s normou ČSN EN ISO 7816, část 1-4. • Předpokladem je podpora bezheslového a bezdotykového přihlašování. • Hybridní čipové karty budou umožňovat uložení certifikátů (kvalifikované, komerční, doménové), hesel uživatelů a musí obsahovat bezkontaktní čip pro zaznamenávání docházky a vstup uživatelů do určených prostor. • Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS. • Všechny operace s privátním klíčem pro kvalifikovaný elektronický podpis musí probíhat uvnitř čipu, tak aby klíč

	neopustil prostředí čipové karty. Privátní klíč uložený na kartě nelze z karty vyexportovat.
	• Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu, anebo mohou být na kartu importovány.
	• Kryptografický obsah čipové karty musí být logicky oddělen na část pro uložení komerčních certifikátů včetně šifrovacích klíčů a na samostatnou část pro uložení kvalifikovaných certifikátů a jim příslušných šifrovacích klíčů. Tyto dvě části musí být na sobě nezávislé, včetně přístupu k těmto částem.
	• Je vyžadováno, aby čipová karta byla plně v souladu s "Security Target" vydaným výrobcem čipové karty. Cílem tohoto požadavku je vyloučení jakýchkoliv zásahů do obsahu, funkce či nastavení kryptografického čipu třetí stranou, které by mohly potenciálně zpochybnit shodu dodaných čipových karet s kartami výrobce, které prošly certifikací Common Criteria a jsou platně zapsány na evropský seznam QSCD prostředků.
	• Dodané hybridní čipové karty budou ve formátu ID-1 – velikost bankovní karty.
	• Čipová karta musí umožňovat uložení certifikátu z interní certifikační autority založené na produktech Microsoft.
	• Prostřednictvím čipových karet v součinnosti s dalším bezpečnostním faktorem se budou moci uživatelé přihlašovat k pracovním stanicím.
	• Je vyžadováno umožnění recyklace kvalifikované části čipových karet (kvalifikovaný prostředek nesmí opustit organizaci). Po odchodu zaměstnance bude umožněno prostřednictvím centrální aplikace zneplatnění certifikátů (revokace pro interní a kvalifikované certifikáty).
	• Prostřednictvím centrální aplikace bude rovněž umožněno zablokování, či smazání kvalifikované části hybridní čipové karty v případě ztráty, nebo odcizení.
	• Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12.
	• Podporovány jsou minimálně tyto kryptografické algoritmy:
	  ○ Symetrické: 3DES, AES
	  ○ Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
	  ○ RSA: 1024, 2048 bitů
	  ○ Eliptické křivky: P-224, P-256, P-384, P-521
	• Čipové karty musí být kompatibilní s oficiálními běžně používanými ovladači.
	• Objednavatel vyžaduje dodání 600 kusů bezkontaktních čipových karet.

Password manager	• Objednavatel požaduje dodání řešení k uchovávání a správě hesel pro koncové uživatele. Tato funkcionalita musí být přístupná přímo ze systému MFA, dostupná v jedné klientské aplikaci. • Umožnění generování silných hesel a upozornění uživatele v případě zadání vlastního slabého hesla. • Možnost přenést heslo do příslušné aplikace bez nutnosti zobrazení hesla, případně automatické vyplňování hesle ve webových aplikacích.

	• Hesla budou bezpečně uložena v šifrovaném trezoru na čipové kartě uživatele, což bude umožňovat jejich bezpečný přenos a snadný přístup. • Přístup k heslům bude chráněn více-faktorovým ověřením. • Musí být umožněn export hesel z karty, jako záloha pro případ ztráty a podobně.
Klávesnice se čtečkou čipových karet	• Česká lokalizace – QWERTZ. • Integrovaná čtečka čipových karet. • S numerickou části. • Čtení a zápis ze všech mikroprocesorových čipových karet ISO7816-1/1/2/3/4. • Bezdrátová, či kabel USB. • Horizontální směr zasunutí karty do čtečky (vodorovně s podkladem pod klávesnicí), tak aby karta nepřekážela a netrčela do prostoru nad klávesnicí.
Ochrana, bezpečnost a logování	• Zajištění pravidelných aktualizací klientských, operátorských a mobilních aplikací, včetně serverového agenta. • Možnost volby automatických, manuálních, či kombinovaných aktualizací s ohledem na řízení, rozložení zátěže a minimalizaci rizik při nasazení nových verzí. • Řešení musí být nasazeno v režimu vysoké dostupnosti (HA), minimálně v režimu Active-Passive a Disaster Recovery tak, aby citlivá data byla stále vysoce zabezpečená a dostupná. • Obě instance musí běžet v prostředí objednavatele. HA proces musí být plně automatický. • Systém musí zahrnovat řešení pro případ selhání systému – Disaster Recovery, tzn. nouzové scénáře s postupy, jak jednat v situacích s fatálním dopadem na dodaný systém. Toto řešení musí být předáno objednavateli také v textové podobě. • Systém bude kompatibilní s prostředky, které z bezpečnostních důvodů umožňují nastavit hodnoty PUKu pro kvalifikovanou a nekvalifikovanou část samostatně. • Systém musí vytvořit auditní záznam, že proběhla recyklace kvalifikovaného prostředku a byl nastaven nový defaultní PIN a PUK. Recyklace zahrnuje operace revokace certifikátů vydaných systémem a následné vymazání všech certifikátů a datových typů. • Umožnění generovat automaticky měsíční reporty obsahující základní informace, počty vydaných a revokovaných certifikátů, počty uživatelů atp. • Nutnost logovat operace spojené se správou životního cyklu certifikátu a kvalifikovaného prostředku včetně identifikace provádějící osoby. • V centrální aplikaci musí mít operátor, či administrátor přehled o koncových uživatelích, jejich certifikátech a oprávněních.
Licencování	• Objednavatel požaduje dodání systému MFA včetně příslušenství v následujících počtech: o Klientská aplikace pro koncové uživatele v počtu 500 kusů. o Centrální správa pro administrátory a operátory v počtu 10 kusů. o Čipové karty v počtu 600 kusů.

	○ Klávesnice se čtečkou čipových karet v počtu 510 kusů. ○ Čtečka čipových karet v počtu 50 kusů. • Žádná z nabízených technologií nesmí být v okamžiku podání nabídky označena výrobcem jako končící. • Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze dodávaného softwaru. • Součástí dodávky je také dodání všech potřebných SW/HW produktů a licencí, včetně licencí třetích strat, pro bezproblémový provoz navrhovaného řešení.

c) Implementace

Dodavatel musí dodat plně funkční systém, kompletně zprovozněný, nainstalovaný, nakonfigurovaný, integrovaný do prostředí objednavatele (integrace s AD / IDM objednavatele), dle svých nejlepších znalostí a svědomí.

Řešení bude dodáno ve formě HW appliance (19" rack mount) nebo VM appliance, případně v kombinaci tak, aby byla zajištěná vysoká dostupnost, včetně všech licencí nezbytných pro provoz a správu. V případě dodání HW appliance objednavatel požaduje redundantní zapojení do 1/10/25 Gbps switchů včetně potřebných trancieverů a kabelů. Dodavatel umožní instalaci operátorské a klientské aplikace v podobě instalačních balíčků pro koncové zařízení, které musí být podepsány certifikátem, který je akceptován Windows systémem. Aplikace musí běžet na systémech Windows 10 a 11.

Dodané hybridní čipové karty musí být plně otevřeny i jiným systémům, jenž vydávají na takové prostředky obsah, a to s otevřenou dokumentací pro další integrace.

V rámci implementace poskytne dodavatel konzultace a best practices ohledně nasazení sytému. Způsob implementace bude vycházet z před implementační analýzy zpracované dodavatelem před započetím instalace a konfigurace (náklady na provedení před implementační analýzy musí být zahrnuty v nabídkové ceně). Analýza bude obsahovat mimo jiné harmonogram realizace projektu, konkrétní popis postupu nasazení dodaného řešení u objednavatele, upřesnění parametrizace, definování workflow, popis realizace integrace s navazujícími systémy provozovanými v prostředí objednavatele. Před implementační analýza musí být konzultována se zaměstnanci objednavatele z odboru IT a následně odsouhlasena objednavatelem.

d) Technická a servisní podpora

Technická podpora je požadována v délce 60 měsíců. Tato podpora musí zahrnovat update a upgrade, jak softwarového prostředí, tak samotného softwaru, v důsledku samostatné inovační činnosti výrobce, případně z důvodu změny právních předpisů, či zjištěných zranitelností. Zpracování změn a nařízení dle platné legislativy bude vyřešeno nejpozději k datu účinnosti změny. Technologický update a upgrade v důsledku vývoje hardwarových a softwarových prostředků, popřípadě změny technologických postupů objednavatele, které mají vliv na funkčnost dodaného řešení. Záruka na dodaný HW a technická podpora bude poskytnuta přímo výrobcem po dobu min. 60 měsíců s reakční dobou opravy NBD a vyřešením závady do 30 dnů.

Objednavatel požaduje technickou podporu výrobce v režimu 8x5. Objednavatel bude mít permanentní možnost nahlášení závady.

Dodavatel zajistí servisní a provozní podporu s následující klasifikaci hlášení závad souvisejících s provozem dodaného řešení:

Kategorie závad	Popis
Kritická	Úplný výpadek dodaného řešení, případně omezení znemožňující plnohodnotné provozování systému.
Střední	Závada výrazně omezující správnou funkcionalitu dodaného řešení, systém je možné s omezením provozovat.
Nízká	Závada, která nemá na provoz dodaného řešení výrazný vliv. Systém lze provozovat bez výrazného omezení.

Zajištění servisní a provozní podpory dodavatelem garantované v následujících termínech (v režimu 8x5):

Kategorie závad	Zahájení řešení	Doba vyřešení požadavku
Kritická	Neprodleně, nejpozději do 2 hodin od nahlášení	do 1 dne od zahájení řešení
Střední	do 24 hodin od nahlášení	do 5 dnů od zahájení řešení
Nízká	do 3 pracovních dní	do 30 dnů od zahájení řešení

Objednavatel bude mít permanentní možnost kontaktovat servisní a provozní podporu prostřednictvím ticket systému, případně telefonu a emailu.

Nadstandardní požadavky objednavatele, které nespadají pod běžnou technickou podporu výrobce, ani pod servisní a provozní podporu dodavatele, budou účtovány podle hodinové sazby uvedené v bodě 1 tohoto dokumentu. Jedná se o dodatečné práce objednané objednavatelem samostatnými objednávkami.

e) Harmonogram, plán odstávek a termíny

Objednavatel vyžaduje dodání harmonogramu plnění v předimplementační analýze. Dílo musí být předáno do 90 dnů od odsouhlasení předimplementační analýzy. Plnění začíná v čase T, což je datum zveřejnění smlouvy v Registru smluv. Harmonogram musí schválit objednavatel.

Zahájení	T + 0 dní
Předimplementační analýza	T + 14 dní (14 dní)
Implementace + akceptační testy + zkušební provoz + předání díla	T + 90 dní (104 dní)

Bez odstávkové instalace a konfigurace můžou probíhat za provozu. Práce, které vyžadují odstávku je možno provádět po pracovní době. Veškeré práce musí probíhat po předešlé domluvě.

Odstávky je možno provádět po domluvě v těchto časech:

- pondělí a středa od 17:00
- úterý a pátek od 14:00
- čtvrtek od 15:00
- odstávky po 19 hod. a o víkendu je možno realizovat jen po individuální domluvě

f) Akceptační testy a zkušební provoz

Součástí akceptačních testů, které navrhne dodavatel, musí být pro každou jednu část systému minimálně:

- prokázání kompletnosti dodávky a splnění všech povinných požadavků

- prokázání aktivací hardware i software aktivačními nebo jinými klíči či prostředky v případě, že je aktivace potřebná
- před akceptací a předáním díla proběhne 15denní zkušební provoz. Pokud se vyskytnou během testování ve zkušebním provozu závady, dodavatel je povinen závady odstranit do 48 hodin od nahlášení, nejpozději však do konce zkušebního provozu
- dokončením díla se rozumí oboustranné odsouhlasení předávacího protokolu po dokončení testovacího provozu, akceptačních testech a případných úpravách v SW konfiguraci

g) Školení zaměstnanců objednavatele

Dodavatel zajistí školení zaměstnanců objednavatele na veškeré součásti nabízeného řešení

- školení musí probíhat v místě plnění a v rozsahu potřebném pro využívání nabízeného řešení (ukázka, popis, nastavení a vysvětlení jednotlivých součástí systému) minimálně v rozsahu 2 hodin pro administrátory a 2 hodin pro operátory systému
- školení se zúčastní 3 administrátoři a cca 7 operátorů
- k dispozici je školící místnost s prezentační technikou v místě plnění
- náklady na školení musí být zahrnuty v nabídkové ceně
- dodavatel po úspěšné instalaci, konfiguraci a integraci vypracuje a dodá objednavateli veškerou (provozní, technickou a uživatelskou) dokumentaci