Příloha č. 1

ke kupní smlouvě evid. č. u prodávajícího: 798/2018

Specifikace předmětu plnění

Předmětem plnění je pořízení 80 ks multifunkčních čipových karet, také dodávka 70 ks adekvátních čteček čipových karet, SW licence, služby spojené s implementací dodávky, provedení zaškolení kompetentních pracovníků, základní servis nabízeného řešení, který musí zahrnout podporu po dobu jednoho roku ode dne podpisu předávacího protokolu.

Čipové karty

- Musí se jednat o prostředek pro uložení certifikátu pro kvalifikovaný elektronický podpis podle nařízení Evropské unie č. 910/2014 eIDAS. Nařízení eIDAS prostřednictvím české legislativy vyžaduje přechod na samosprávy právě na takový podpis.
- Musí splnit požadavek na dvoufaktorovou autentizaci do pracovních počítačů. Silná autentizace splňuje kritéria zákona o kybernetické bezpečnosti v oblasti autentizace a zajišťuje ochranu osobních údajů související s nařízením Evropské unie GDPR.
- Do těla karty musí být integrován bezkontaktní čip pro použití v bezkontaktních systémech – docházkový systém, případně tiskové řešení, fyzické přístupy atd. Zaměstnanec pro pohyb po budovách úřadu použije jeden prostředek.
- Karta musí podporovat práci s certifikáty z doménové i akreditované certifikační autority PostSignum.
- Je potřeba provést a nastavit službu aktivace doménové certifikační autority, která zajistí zejména vydání certifikátů pro autentizaci doménových pracovních stanic. Případně šifrovacích a technologických certifikátů.
- Kupující požaduje aplikační podporu pro podrobnou evidenci karet a certifikátů a řešení problémových stavů. Evidence musí podporovat jednotlivé stavy karet a certifikátů. Zobrazuje aktuální data o kartách uložených certifikátech. Platí pro doménovou i akreditovanou CA.
- Kupující požaduje aplikaci pro automatizovanou obnovu certifikátů. Automatizovaná obnova certifikátů musí zároveň podporovat i obnovu certifikátů z doménové certifikační autority.

Čtečky čipových karet

- Pro práci s čipovou kartou je potřeba dodat čtečky Gemalto, typ CT30.

Návrh životního cyklu karet

Před implementací karet a aplikací musí být vypracován dokument s návrhem životního cyklu karet na MÚ Rýmařov a odsouhlasený před implementací karet. K jeho zpracování bude třeba diskuse s kupujícím. V rámci dokumentu musí být řešena témata:

- Role uživatelů pro správu a použití karet.
- Způsob distribuce karet uživatelům.
- Vydání a obnova certifikátů na kartách.
- Způsob aplikačního využití karet (operace, využívaná aplikační rozhraní).
- Podporované stavy karet a jejich vlastnosti.
- Řešení nestandardních stavů karet (zapomenutí, ztráta, zničení, …).
- Aplikační scénáře (podklady pro konfiguraci dodávaných aplikací).
- Návrh tiskových protokolů.

Doménová certifikační autorita

K certifikátům v doméně je potřeba provést aktivaci doménové certifikační služby a vydávání certifikátů z takto vytvořené doménové certifikační autority (dále jen „CA“). Takto získané certifikáty budou pro MÚ zdarma. Tyto certifikáty nelze použít pro kvalifikovaný elektronický podpis.

CA na platformě MS Windows Server nabízí značnou variabilitu budovaného řešení.

- Klíč CA bude chráněn v operačním systému.
- CRL bude publikován do intranetu přes Active Directory.
- Bude dodána základní sada šablon certifikátů.
- CA se musí pravidelně zálohovat.
- Musí být dodána provozní dokumentace pro správu a provoz, spolu s havarijním plánem.

Čipové karty

Musí se jednat o karty pro ochranu soukromých klíčů, spojených s elektronickými certifikáty. Pro jejich použití je proto nutno mít v čipu uložen alespoň jeden pár klíčů s certifikátem.

Certifikát musí vydat certifikační autorita. Karty budou schopny hostovat certifikáty, vydané z certifikační autority České pošty, s.p. - akreditovaného poskytovatele certifikačních služeb – PostSignum. Karty mohou hostovat certifikáty, vydané z libovolných certifikačních autorit, např. akreditovaných poskytovatelů certifikačních služeb.

Musí se jednat o prostředek pro uložení certifikátu pro kvalifikovaný elektronický podpis podle nařízení Evropské unie č. 910/2014 eIDAS. Nařízení eIDAS prostřednictvím české legislativy vyžaduje přechod na samosprávy právě na takový podpis.

Musí se jednat o procesorové čipové karty, s implementovanou asymetrickou kryptografií na kontaktním čipu, které umožňují bezpečné uložení privátních klíčů.

Důvod:

- Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty.
- Privátní klíč uložený na kartě nelze z karty vyexportovat.
- Klíče mohou být generovány v čipu anebo mohou být na kartu importovány.
- K párům klíčů lze na kartu uložit i příslušné certifikáty.
- Po vytažení karty se čtečky se automaticky uzamkne PC nebo přeruší komunikace s aplikací. Čipová karta **ProID+Q** musí být ve formátu ID-1, což odpovídá přesným rozměrům a velikosti bankovní karty. Karty ve formátu ID-1 musí být – kromě kontaktního čipu – osazeny také **bezkontaktním čipem EM 4102**, 125 kHz (v konfiguraci dodané výrobcem), který bude MÚ Rýmařov využívat v rámci bezkontaktních systémů – docházkový systém. Bude se jednat o **hybridní kartu** (kontaktní a bezkontaktní čip), **bílou bez potisku, bez příbalového materiálu, s výchozími nastavenými hodnotami QPIN, PIN a PUK.**

Musí splnit požadavek na dvoufaktorovou autentizaci do pracovních počítačů. Silná autentizace splňuje kritéria zákona o kybernetické bezpečnosti v oblasti autentizace a zajišťuje ochranu osobních údajů související s nařízením Evropské unie GDPR.

Součástí čipové karty je s ní svázaná SW licence ProID+Q, časově neomezená (na dobu životnosti karty), která pokrývá používání jak software implementovaného v PKI čipu, tak middleware instalovaného v uživatelském počítači. Počet instalací middleware je tak libovolný.

Čtečky čipových karet

Je nutno dodat kvalitní čtečky, které budou mít krátké doby odezvy a minimální výpadky spojení s operačním systémem. Čtečka musí být připojena do počítače přes standardní USB port. Jde o čtečku standardu PC/SC, výrobce Gemalto, typ CT30.

SW pro centrální personalizaci a správu čipových karet (CMS)

pro snadné ovládání procesů spojených s kartami a certifikáty. Funkce budou implementovány prostřednictvím aplikace, či aplikací.

- **Vydání nové (trvalé) karty**

  Vydání na každou kartu jeden či více certifikátů (podle zvoleného „profilu“), vygenerování nové hodnoty PIN, resp. PUK karty, tisk nově nastavené hodnoty PIN/PUK na PIN-formulář.

  Výsledkem procesu bude kompletně připravená karta, která bude předána pracovníkům. Součástí procesu vydání karty budou kontroly, např. zda daná karta náleží danému uživateli anebo zda jde o správný typ karty.

- **Vydání dočasné karty**

  Musí být možnost vydání dočasné kartu, na které může být jeden či více certifikátů.

  Tyto budou sloužit zejména pro řešení situace, kdy je třeba pracovníkovi operativně vydat kartu s certifikáty; např. pro řešení situace zapomenutí karty, ztráty karty, nových zaměstnanců. Předpoklad je, že dočasná karta překlene období, než se pracovníkovi vydá trvalá karta.

- **Obnova doménových certifikátů na kartě**

  Musí být možnost obnovení sady certifikátů, uložených na kartě jiného pracovníka. Držitel karty musí autorizovat operaci zadáním PIN (musí být přítomen operaci). Po obnově musí být z karty odstraněny nepotřebné certifikáty a klíče.

- **Odvolání doménových certifikátů na kartách**

  Nutnost vyhledání jedné či více karet, včetně odvolání certifikátů, které jsou evidovány k jednotlivým kartám.

- **Evidence ztráty či zničení karty**

  Nutnost vyhledání jedné či více karet s možností označit ji v evidenci jako ztracenou či zničenou / skartovanou; včetně volby, zda mají být zároveň odvolány certifikáty, evidované k vybraným kartám.

- **Evidence požadavků na nové karty**

  Jedná se o zavedení požadavku do centrální evidence na dodání nové karty konkrétnímu pracovníkovi.

- **Import informací o nových kartách**

  Informace o nově dodaných kartách se musí importovat do centrální evidence. Budou spárovány s evidovanými držiteli.

Bude se jednat o modul **Card management systém ProID+ (CMS)** pro evidenci a podporu karet.

Základní požadavky:

- Evidence karet, používaných na MÚ.
- Evidence držitelů karet.
- Evidence dat na kartách (certifikáty, uživatelská data).

Cílem je provádět efektivní správu, včetně podpory a sledování životního cyklu karet.

Je potřeba sledovat min. následující údaje:

- Identifikátor karty (kontaktního čipu i bezkontaktního čipu).
- Typ karty (kontaktní, bezkontaktní, hybridní…).
- Druh karty (uživatelská, administrační, operátorská…).
- Stav karty (nová, používaná, skartovaná…).
- Historii karty (datum zavedení do evidence, vydání uživateli, recyklace…).
- Držitele karty (aktuálního držitele i všechny předchozí držitele).
- Data na kartě (certifikáty a další data, včetně historie dat na kartě).

SW licence pro jednu instalaci CMS v prostředí kupujícího, pro objem 1-300 uživatelů, časově neomezená.

Integrace CMS do domény MS Windows

CMS je nutné integrovat do domény MS Windows

- CMS musí využívat doménovou Active Directory jako zdroj informací o uživatelích / držitelích karet.
- CMS bude akceptovat nastavení doménových bezpečnostních politik.
- Uživatelské role CMS budou mapovány na doménové skupiny (domain groups).
- CMS bude definovat oprávnění na úrovni doménových skupin.
- CMS musí podporovat využití integrované autentizace domény MS Windows (Single Sign On).
- Evidence CMS bude centralizovaná, veškerá data CMS budou uložena v jedné MS SQL databázi.
- Pro přístup do centrální evidence se bude využívat doménová infrastruktura.
- K centrální evidenci se bude přistupovat po síti.
- Při přístupu k datům se využije integrovaná autentizace MS Windows. Doménoví uživatelé nebudou muset při přístupu k datům zadávat žádné autentizační údaje; bude akceptováno doménové pověření uživatele.
- Přístupová oprávnění k jednotlivým typům dat musí být řízena na úrovni doménových skupin.
- Správa přístupových oprávnění bude integrována do Active Directory, oprávnění budou přidělována běžnými nástroji MS Windows.

Informace o uživatelích

CMS nepovede vlastní evidenci uživatelů, data o uživatelích bude přebírat z Active Directory (AD). V databázi CMS bude evidován pouze identifikátor (SID) uživatele AD. Veškeré další informace o uživatelích budou v případě potřeby vyhledána v AD.

Správa uživatelů v systému bude jednotná, nebude třeba řešit problematiku dvojí evidence a synchronizace dat. Změní-li se v AD informace o uživateli (např. jméno, příjmení, …) musí se tyto změny automaticky promítnout i do formulářů CMS.

Kartové centrum ProID+ (KC)
je aplikací pro centrální personalizaci a správu čipových karet. Je implementována jako tlustý klient a instalována na počítači správce karet. Kartové centrum formou intuitivního grafického rozhraní podporuje požadovanou řadu scénářů, kdy každý scénář je určen pro jinou situaci v rámci životního cyklu karty. Kartové centrum akceptuje doménová pověření obsluhy.

SW licence pro jednu instalaci v prostředí kupujícího, časově neomezená.

Aplikace pro obnovu certifikátů (ACEx)

Obnova certifikátu na čipovou kartu je povětšinou komplikovaný proces. Kupující vyžaduje dodat komponentu, které bude uživatelsky přívětivá a provede koncového uživatele celým procesem vydání nového certifikátu.

Komponenta musí pravidelně kontrolovat certifikáty na kartě a v případě potřeby automaticky vyzvat uživatele k obnově certifikátů. Následně automatizovaně provede uživatele obnovou certifikátů. Obnova certifikátu proběhne pouze na základě zadání PINu, pokud nejsou třeba měnit uživatelské údaje v certifikátu.

Software ACEx (Authentication Certificate Exchange) není v tomto případě centrální, ale distribuovaný SW, určený pro instalaci v uživatelském počítači. ACEx je jednoduchý grafický průvodce procesem obnovy certifikátu. Po úspěšném dokončení práce SW aplikace ACEx by uživatel měl mít na kartě obnovené certifikáty, použitelné v dalším období. Obnova doménových certifikátů bude funkční po instalaci ACEx, obnova certifikátů od kvalifikované certifikační autority bude funkční do 12 měsíců od vydání produkčního kvalifikovaného certifikátu.
SW multilicence pro prostředí kupujícího, k instalaci až pro 300 uživatelů, časově neomezená.

Implementace aplikací pro správu karet a školení

Dodavatel musí provést všechny služby spojené s úspěšnou implementací dodávky a provedení zaškolení kompetentních pracovníků.

Podkladem pro implementaci a konfiguraci aplikací bude:

- Dokument s návrhem životního cyklu.

Po dokončení implementace budou funkční všechny aplikace a procesy, spojení se správou karet a životním cyklem certifikátů. Součástí implementace je ověření fungování karet, certifikátů a nainstalovaných aplikací.

Servisní podpora

Základní servis nabízeného řešení zahrnuje podporu po dobu jednoho roku ode dne podpisu předávacího protokolu (servisní podpora počíná běžet dnem následujícím po dni podpisu). Delší podpora je volitelná a zadavatel ji nemusí využít.
Jde o základní servis nabízeného řešení, který zahrnuje podporu na OS na klientských stanicích Windows 7 až 10, na serverových OS Windows Server 2008 R2 a vyšších, dostupnost verzí middleware čipových karet ProID+ Q do konce jejich životnosti, podporu dodané čtečky standardu PC/SC, podporu dodaných SW modulů pro správu životního cyklu karet a certifikátů KC, CMS, ACEx a dodaného middleware. Podpora bude poskytována formou Service Desku v režimu 5 x 8, jehož provozní doba bude od 8:00 – 16:00 v pracovní dny.
Reakční doba a doby řešení jsou garantovány pro serverové komponenty řešení (KC, CMS) a týkají se jejich podstatných vad. Pro koncové stanice bude vyvinuto ze strany dodavatele maximální úsilí pro rychlé vyřešení vzniklého incidentu, kde je důvodem heterogenní prostředí na vrstvě aplikační i na operačních systémech. Celková definice podoby prostředí kupujícího, do něhož jsou jednotlivé SW moduly úspěšně nasazeny, je podchycena v dodané dokumentaci při akceptaci dodávky.

Kontaktní údaje prodávajícího: support@monetplus.cz tel. +420 739 685 921

Reakční doby servisní podpory

Potvrzení přijetí požadavku	do 2 hodin od nahlášení
Dodání dočasného řešení	do 1 pracovního dne od přijetí požadavku
Vyřešení požadavku	do 3 pracovních dnů od dodání dočasného řešení

Položkový rozpočet plnění

Celková kupní cena dle článku V., odst. 1 smlouvy, je tvořena součtem níže vyčíslených položek, zahrnuje i cenu za dodání na místo určení.

	Cena bez DPH	Částka DPH	Cena vč. DPH
Návrh životního cyklu karet	28.000 Kč	5.880 Kč	33.880 Kč
Doménová CA, havarijní a provozní dokum.	58.000 Kč	12.180 Kč	70.180 Kč
Čipové karty	36.000 Kč	7.560 Kč	43.560 Kč
Čtečky čipových karet	22.400 Kč	4.704 Kč	27.104 Kč
SW pro centr. pers. a spr. karet: KC, ACEx	105.000 Kč	22.050 Kč	127.050 Kč
Integrace CMS do domény MS Windows	je zahrnuto v ceně implementace		
Aplikace pro správu karet: CMS	57.000 Kč	11.970 Kč	68.970 Kč
Implementace	105.000 Kč	22.050 Kč	127.050 Kč
Servisní podpora – paušální částka na 1 rok	47.760 Kč	10.030 Kč	57.790 Kč
Školení	10.500 Kč	2.205 Kč	12.705 Kč
CELKEM	**469.660 Kč**	**98.629 Kč**	**568.289 Kč**