# Vybudování PKI, SSO a 2FA

Požadována je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro autentizaci uživatelů pomocí čipové karty, v případě VPN pak pomocí mobilní aplikace.

Součástí dodávky budou aplikace a opatření potřebná k zajištění autentizace všech uživatelů pomocí dvou faktorů, přičemž druhým bude hybridní čipová karta (mobilní aplikace pro přístup do VPN), kterou bude možno využít i k dalším účelům, zejména jako bezkontaktní čip pro stravovací systém, průkaz zaměstnance s potiskem po obou stranách a úložiště kvalifikovaných certifikátů pro podepisování zdravotnické dokumentace.

# Požadovaný rozsah dodávky a souvisejících služeb

| # | Položka rozpočtu | Počet | Stručný popis položky |
| --- | --- | --- | --- |
| 1 | Dodávka centrálního systému pro řízení přístupů pracovníků NBV pomocí čipových karet | 1 soubor | Dodávka centrálního systému pro řízení přístupů pracovníků NBV pomocí čipových karet – licence na dobu neurčitou pro 1300 uživatelů, v případě přístupu do VPN pak mobilní aplikaci pro MFA pro 300 uživatelů.  Požadováno je vybudování systému, dodávka systému, instalace do virtuálního prostředí zadavatele, zapojení a konfigurace prvků přístupového systému a zajištění všech nezbytných integrací (napojení na RADIUS server, MS AD, txt export pro stravovací systém, SSO na IS napojené na MS AD atd.). |
| 2 | Vybudování PKI infrastruktury NBV | 1 soubor | Dodávka technologií pro bezpečnostní vrstvu vybudovanou na bázi PKI MS Windows, která je primárně určena pro vydávání klientských karetních a infrastrukturních certifikátů pro zavedení 2FA autentizace. |
| 3 | Čipové karty | 1300 ks | Hybridní čipové karty ve velikosti ID-1 (bankovní karta) s bezkontaktním čipem (Mifare) a funkcí bezpečného zařízení (kvalifikovaný prostředek QSCD) pro ukládání kvalifikovaných  i komerčních certifikátů a vytváření elektronického podpisu (QESCD) v souladu s legislativou.  Čipové karty budou předtištěny podle dodaného designu.  Součástí čipové karty bude vždy předávací protokol (tzv. pinový formulář s bezpečnostním polem). |
| 4 | Čtečky čipových karet | 750 ks | Dodávka USB čteček čipových karet. |
| 5 | Tiskárna na potisk čipových karet | 1 ks | Tiskárna na oboustranný potisk dodávaných čipových karet. |

### Související služby

1. Projektové řízení dodávky řešení.
2. Zpracování návrhu dodávky a konfigurace dodávaných technologií, související konzultace.
3. Dodávka, implementace, instalace, zapojení a konfigurace dodávaných technologií.
4. Ověření funkčnosti dodaných technologií a jejich (sou)částí.
5. Dodávka dokumentace dodaného vybavení a jeho částí (min. administrátorská dokumentace, dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace). Dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace.
6. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
7. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
8. Provedení zkušebního provozu.
9. Poskytnutí záruky na dobu minimálně 2 let .

Dodávkou nebudou negativně dotčeny současné systémy, technologie.

## Požadavky na řešení

### Obecné a společné požadavky

| # | Požadavek |
| --- | --- |
|  | Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR). |
|  | Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi NBV. |
|  | Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií min. po dobu účinnosti servisní smlouvy. |
| Legislativa a další normy | |
|  | Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General data protection regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. |
|  | Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění. |
|  | Soulad s prováděcím nařízením Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný (dále jen „PNK“- Prováděcí nařízení Komise). |
| Ostatní obecné požadavky | |
|  | Zajištění jednotného času na všech technologiích a zařízeních (synchronizace s time serverem) . |

### Dodávka centrálního systému pro řízení přístupů pracovníků NBV pomocí čipových karet

| # | Požadavek |
| --- | --- |
|  | Dodávka centrálního systému pro řízení přístupů pracovníků NBV pomocí čipových karet  Součástí bude vybudování systému, dodávka systému, instalace, zapojení a konfigurace prvků přístupového systému a zajištění všech nezbytných integrací (napojení na RADIUS server, MS AD, txt export pro stravovací sytém, SSO na IS napojené na MS AD atd.). |
| Obecné funkcionality | |
|  | Zjednodušení životního cyklu karet a certifikátů, automatizace procesů životního cyklu karet formou průvodců pro správce životního cyklu i pro držitele certifikátů. Odstínění koncových uživatelů od technologie. |
|  | Podpora činností spojených se správou životního cyklu čipových karet a certifikátů, zastřešení registračního místa doménové CA. |
|  | Webová aplikace, určená správcům certifikátů. Možnost vyhledávat a prohlížet informace o certifikátech, odvolávat certifikáty, generovat a prohlížet reporty. |
|  | Automatizovaná obnova kvalifikovaných i komerčních certifikátů alespoň od tří externích poskytovatelů v ČR. Podpora minimálně I.CA, eIdentity a PostSignum. |
|  | Napojení na dodávanou doménovou CA (viz dále), automatizovaná obnova interních uživatelských certifikátů z doménové CA na čipových kartách. |
|  | Aplikace pro nahrávání certifikátů na dodávané karty, a to jak pro správce, tak pro uživatele v rámci jejich obnovy pro minimálně 3 pracoviště. |
|  | Aplikace pro kvalifikované elektronické pečetění dokumentů prostřednictvím kvalifikovaného certifikátu uloženého na eIDAS ready bezpečnostním prostředku. |
|  | Aplikace, které prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu   * + - 1. Notifikační profil lze konfigurovat podle potřeb, tj. vzhled a textace mailu, pravidla notifikace podle vlastností certifikátu (např. na základě vydavatele certifikátu, šablony certifikátu (pro MS CA), atp.       2. Notifikační zprávu lze zároveň odesílat na mail správců, aby byli informování o blížící   se expiraci certifikátů v organizaci.   * + - 1. Notifikaci lze odeslat nejen při blížící se expiraci certifikátů, ale také při jejich vydání. |
|  | Anonymizace údajů o uživatelích, kteří ukončí pracovní poměr. |
|  | Možnost do dokumentu PDF, Word nebo Excel připojit kvalifikovaný elektronický podpis + pečeť + vodoznak v rámci jednoho kroku |
| Dvoufaktorová autentizace | |
|  | Integrace do domény MS Windows 2019 a vyšší pro dvoufaktorovou autentizaci uživatelů na základě certifikátu a kryptografických operací, kde jako druhý faktor bude sloužit bezpečnostní předmět (karta). |
| Integrace | |
|  | Exporty pro stravovací systém – export karet a jim příslušejících uživatelů a platnosti karet ve formátu TXT.  *Přesná struktura bude poskytnuta v rámci implementační analýzy.* |
|  | Integrace na MS Active Directory:   1. Přebírání seznamu uživatelů a relevantních uživatelských dat. 2. Dvoufaktorová autentizace – viz výše. 3. Přebírání začátku a konce platnosti uživatelských účtů a zneplatnění účtů, karet a certifikátů po ukončení platnosti účtu uživatele. |
|  | Integrace SSO na informační systémy napojené na MS AD.  Nemocniční informační systém NIS AMIS\*H + AMIS\*HD, Laboratorní informační systém TIS, Systém pro řízení workflow firemních dokumentů EISODX, Nefrologický Informační systém NEFRIS, Mailserver, FARMIS, Service Desk, apod. |
|  | Poskytnutí API pro získání seznamu karet, jejich příslušnosti k uživatelům (dle MS AD) a veřejných částí komerčních certifikátů. |
|  | Integrace dvoufaktorové autentizace na RADIUS server pro zajištění vzdálených VPN přístupů v rámci domény MS Windows. Implementace pro VPN / Access přístup pomocí RADIUS serveru (Microsoft NPS) s využíváním atributů protokolu RADIUS pro jednotlivé skupiny uživatelů AD. |
| Dodávka / instalace | |
|  | Instalace, zapojení a konfigurace systému.  *Provozní infrastrukturu poskytne objednatel.* |
|  | Veškerá nastavení a oprávnění musí být v souladu se zákonnými požadavky na ochranu osobních údajů. |
| Potisk / tiskárna | |
|  | Služby pro personalizovaný oboustranný potisk čipových karet z evidence karet/uživatelů na dodávané tiskárně pro potisk čipových karet. |

### Vybudování PKI infrastruktury NBV

| # | Požadavek |
| --- | --- |
|  | Dodávka technologií pro bezpečnostní vrstvu vybudovanou na bázi PKI MS Windows, která je primárně určena pro vydávání klientských karetních a infrastrukturních certifikátů pro zavedení 2FA autentizace.  Z doménového PKI se budou vydávat uživatelské certifikáty na čipové karty za účelem zavedení primárně dvoufaktorové autentizace (náhrada autentizace jménem/heslem). Mimo přihlášení do PC budou z interní CA vydávány případně certifikáty pro přihlášení do VPN a interní elektronický podpis. Interní PKI bude také poskytovat infrastrukturní certifikáty pro interní použití, např certifikáty pro web servery a DC. |
|  | Zpracování návrhu implementace PKI v rámci NBV. Bude využita dvouvrstvá hierarchie CA na OS MS Windows. Privátní klíče všech CA budou hostovány v úložišti OS. |
|  | Implementace zvolené architektury hierarchie PKI, zprovoznění PKI v prostředí objednatele. |
|  | Předání podkladů na implementaci šablon pro vydání certifikátů pro autentizaci uživatelů do domény, případně další uživatelské akce. |
|  | Předání podkladů na implementaci šablon pro vydání technologických certifikátů pro Web server a DC. |
|  | Implementace šablon uživatelských a technologických certifikátů. |
|  | Definice distribučních bodů CRL. |
|  | Ochrana a uložení klíče CA. |
|  | Dodání havarijní a provozní dokumentace k vybudované vrstvě PKI. |
|  | Zálohování dodané doménové CA, aby v případě havárie bylo možno CA obnovit, znovu zprovoznit a provést kompletní obnovu dat |
|  | Instalace, zapojení a konfigurace systému. |
|  | Veškerá nastavení a oprávnění musí být v souladu se zákonnými požadavky na ochranu osobních údajů. |
|  | Všechny vydané certifikáty jsou v reálném čase registrovány a uloženy v databázi. |
|  | Centrální databáze s komplexním zálohováním certifikátů. |
|  | Aplikace nabízí možnost archivovat šifrovací klíče uživatelů v zabezpečené formě v DB s možností jejich pozdější obnovy, např. při ztrátě původního klíče, aniž by bylo možné data rozšifrovat. Organizace také získá řízený přístup k zašifrovaným uživatelským datům (požadavek na audit), zatímco původní klíč již neexistuje. |
|  | Aplikace pro správce – šifrovací klíč uživatele lze obnovit z centrální databáze archivu.  Bezpečnostní algoritmus založený na procesu fragmentace klíče (dešifrovací klíč s více správci). Pro obnovu původního šifrovacího klíče musí být třeba více správců, kteří se sejdou – princip čtyř a více očí. |

### Čipové karty

| # | Požadavek |
| --- | --- |
|  | Hybridní čipové karty ve velikosti ID-1 (bankovní karta) s bezkontaktním čipem (Mifare) pro přístupový systém a funkcí bezpečného zařízení (kvalifikovaný prostředek QSCD) pro ukládání kvalifikovaných i komerčních certifikátů a vytváření elektronického podpisu (QESCD) v souladu s legislativou. |
|  | Karty musí být v souladu (certifikované):   1. s normou ČSN EN ISO 7816, část 1-4 a 2. standardem EN 419 211 a profily:    1. BSI-CC-PP-0059    2. BSI-CC-PP-0075    3. BSI-CC-PP-0071    4. BSI-CC-PP-0072    5. BSI-CC-PP-0076 |
|  | Kompatibilní s centrálním systémem. |
| Kontaktní čip a PKI | |
|  | Možnost uložení elektronických certifikátů X.509 (a generování / uložení příslušných kryptografických klíčů), kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací. |
|  | Všechny operace s privátním klíčem probíhají uvnitř čipu. Privátní klíč uložený na kartě nelze z karty vyexportovat. |
|  | Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS. Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu. |
|  | Podporuje uložení kvalifikovaných certifikátů minimálně od poskytovatele kvalifikovaných  certifikátů. Pro splnění technické podmínky je nutné doložit čestné prohlášení o podpoře od všech  kvalifikovaných poskytovatelů. |
|  | Součástí podpory uložení kvalifikovaných certifikátů na čipovou kartu jsou také moduly pro  ověření původu klíče (důkaz, že privátní klíč vznikl generováním uvnitř čipu kvalifikovaného  prostředku), které je integrované se systémy kvalifikovaných certifikačních autorit. |
|  | Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány |
|  | Vytváření elektronického podpisu na bázi certifikátů ve formě:   1. kvalifikovaného elektronického podpisu, 2. zaručeného elektronického podpisu, 3. uznávaného elektronického podpisu a 4. jiné formy elektronického podpisu. |
|  | Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12. Generování a práce s RSA a ECC klíči v čipu. |
|  | Archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů. |
|  | Podpora minimálních kryptografických algoritmů:   1. Symetrické:, AES 2. Eliptické křivky: P-224, P-256, P-384, P-521 3. RSA: 2048 bitů 4. Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. |
|  | Zablokování bezpečnostního kódu PIN, QPIN resp. PUK po opakovaném chybném zadání PIN, QPIN resp. PUK. Podpora odblokování bezpečnostního kódu PIN pomocí PIN nebo PUK, podpora odblokování bezpečnostního kódu QPIN pomocí QPIN nebo PUK. |
|  | Podpora procesu ověření uživatele manažerem pro obnovu PIN. |
|  | Omezit možnost měnit PUK, aby uživatel mohl měnit pouze PIN. |
|  | Podpora správy PUK administrátorem. |
|  | Zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů) |
|  | Dvoufaktorovou autentizaci na bázi certifikátů X.509 (do PC v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.). |
|  | Hybridní čipová karta musí podporovat získání následného doménového i kvalifikovaného certifikátu  prostřednictvím aplikace pro automatizovanou obnovu certifikátů. V případě kvalifikovaného  certifikátu je požadována podpora minimálně dvou poskytovatelů kvalifikovaných certifikátů. |
|  | Hybridní čipová karta musí podporovat konfigurovatelné množství kontejnerů pro RSA / ECC klíče a  certifikáty, minimálně v rozsahu 10 kontejnerů pro RSA (až do velikosti privátního klíče 4096 b a  10 kontejnerů pro ECC (až do velikosti privátního klíče 521 b). |
| Ovladače do OS a související SW | |
|  | Čipové karty budou dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému. Vlastnosti ovládacího software:   1. Podléhá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší 2. Podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11 3. Použití na MS Windows 10 nebo vyšších verzích; 4. Použití na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11) 5. Instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), RPM, DEB |
|  | Součástí instalačního balíčku ovladačů karet bude aplikace, dostupná pro uživatele i  administrátory a umožňující správu objektů čipové karty, např.   * Změna PIN / PUK * Prohlížení obsahu kontejnerů (klíčů, certifikátů) * Mazání kontejnerů * Import klíčů a certifikátů do čipové karty |
| Stav dodané karty | |
|  | Inicializovaná PKI aplikace s PIN, QPIN a PUK. |
|  | Předání seznamu personalizovaných karet, pro import do evidence Centrálního systému pro řízení přístupů uživatelů. U každé karty uvedeno číslo kontaktního, případně i bezkontaktního čipu. |
|  | Inicializovaná PKI aplikace výchozími hodnotami PIN, QPIN a PUK. Technickými prostředky bude vynuceno, aby si uživatel po přijetí karty změnil hodnotu bezpečnostních kódů. |

### Čtečky čipových karet

| # | Požadavek |
| --- | --- |
|  | Dodávka čteček čipových karet. |
|  | USB propojení (není požadována podpora Bluetooth). |
|  | Podporované operační systému – MS Windows, Linux, MacOS |

### Tiskárna na potisk čipových karet

| # | Požadavek |
| --- | --- |
|  | Dodávka tiskárny na oboustranný potisk dodávaných čipových karet. |
|  | Tisk oboustranného potisku z nástrojů centrálního systému pro řízení přístupů uživatelů. |
|  | Podporovaný operační systém – MS Windows 10 nebo vyšší. |
|  | Instalace, zapojení a konfigurace tiskárny včetně napojení na centrální systém a ověření oboustranného tisku na dodávané karty. |

### Bezpečnostní požadavky

| # | Požadavek |
| --- | --- |
|  | Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému.  Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup. |
|  | Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu. |
|  | Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí. |
|  | Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů. |
|  | Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů. |
|  | Veškeré logy budou dostupné pro externí systém sběru a analýzy logů. |

### Implementační a provozní požadavky

| # | Požadavek |
| --- | --- |
|  | Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop). |
|  | Součástí dodávky musí být i veškeré služby – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele v časech stanovených objednatelem a v českém jazyce.  Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu. |
|  | V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele. |
|  | Zajištění administrátorských aplikací, konzolí pro všechny součástí systému pro zajištění konfiguračního managementu systému anebo jeho součástí. |
|  | Dohled – dodávané systémy a technologie musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení. |
|  | Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém. |

### Servisní podpora

| # | Požadavek |
| --- | --- |
|  | Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop). |
|  | Servisní podpora musí být dostupná formou Service Desku v režimu 5 x 8, jehož provozní doba musí být min. od 8:00 do 16:00 v pracovní dny. |
|  | Požadované reakční doby:  Přijetí požadavku do 2 hodin od nahlášení.  Dočasné řešení do 1 pracovního dne od přijetí požadavku.  Vyřešení požadavku do 5 pracovních dnů od dodání dočasného řešení.  Reakční doby musí být garantovány pro serverové komponenty řešení. |