SMLOUVA – ŘEŠENÍ PRO MULTIFAKTOROVOU AUTENTIZACI

MONET+, a.s.
zapsána u Krajského soudu v Brně, spisová značka B 3351
se sídlem: Za Dvorem 505, 763 14 Zlín - Štípa
IČ: 26217783 DIČ: CZ26217783
zastoupena: Ing. Břetislavem Endrysem, předsedou představenstva a Ing. Janem Vavrysem, členem představenstva
bankovní spojení: xxxxx
číslo účtu: xxxxx

jako **dodavatel** na straně jedné (dále jen „dodavatel")

a

Všeobecná fakultní nemocnice v Praze
se sídlem: U Nemocnice 499/2, 128 08 Praha 2
IČ: 000 64 165 DIČ: CZ00064165
zastoupena: prof. MUDr. Davidem Feltlem, Ph.D., MBA, ředitelem
bankovní spojení: xxxxx
číslo účtu: xxxxx

jako **objednatel** na straně druhé (dále jen „objednatel")

uzavírají dnešního dne na základě výsledku **nadlimitní veřejné zakázky** s názvem „**Multifaktorová autentizace uživatelů AD**", **vyhlášené otevřeným řízením** dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „z. č. 134/2016 Sb.") a zveřejněné ve Věstníku veřejných zakázek. pod ev. č. Z2023-058174 ze dne 18.12.2023 **a v Úředním věstníku Evropské unie pod č. oznámení o zahájení zadávacího řízení 2023/S 247 – 780006 ze dne 18.12.2023** (dále jen „veřejná zakázka"), v souladu s ustanovením § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, (dále jen „zákon č. 89/2012 Sb."), tuto smlouvu (dále jen „smlouva")

Preambule

Realizace předmětu plnění je spolufinancována Evropskou unií z prostředků Nástroje pro oživení a odolnost (RRF) prostřednictvím Národního plánu obnovy ČR z výzvy č. 25 (předem definovaný projekt, komponenta 1. 2 Digitální systémy veřejné správy, Investice 3: Kybernetická bezpečnost). Financováno Evropskou unií – NextGeneration EU.

I. Předmět smlouvy

1. Předmětem plnění dle této smlouvy je dodání řešení multifaktorové autentizace uživatelů v Active Directory (dále také „AD") v prostředí Všeobecné fakultní nemocnice v Praze (dále také „řešení MFA" nebo „předmět plnění").

Součástí předmětu plnění je:

a) dodání časově neomezených užívacích práv (serverová licence) k SW pro centrální správu životního cyklu čipových karet pro minimálně 50 souběžně pracujících uživatelů pro min. 10 000 karet včetně napojení inicializačních pracovišť a aplikací na koncových stanicích v souladu s funkčními požadavky objednatele na server objednatele.

b) dodání HW/SW klientské části pro 4 200 počítačů:
- časově neomezená užívací práva ke klientskému SW (včetně případných licencí do centrální správy),
- kontaktní/bezkontaktní čtečka (RFID) připojitelná přes USB,
- kabeláž a upevnění nebo zajištění neklouzavé spodní části (např. oboustranná lepenka, přísavka nebo suchý zip),

c) dodání HW/SW klientské části pro 3 počítače inicializačních pracovišť pro výdej a nastavení karet:
- časově neomezená užívací práva k inicializačnímu SW (včetně případných licencí do centrální správy),
- 2 ks kontaktní/bezkontaktní čtečky karet (RFID) připojená přes USB,
- kabeláž a upevnění nebo zajištění neklouzavé spodní části (např. oboustranná lepenka, přísavka nebo suchý zip),

d) dodání 6 900 kusů hybridních kontaktních/bezkontaktních čipových karet včetně potisku karet (potisk karet obdobou kvality barevného potisku při použití barev Fargo HDP color ribbon, které se budou používat na následnou výrobu karet pro nové zaměstnance) na základě databáze uživatelů a jejich přednastavení, což znamená nahrání kompletní struktury karty včetně komunikačních a privátních klíčů, karta bude připravená k výdeji, bude potřeba pouze aktivace karty.

e) dodávka 1 000 kusů hybridních kontaktních/bezkontaktních čipových karet bez potisku.

f) implementace řešení:

Objednatel předá dodavateli před začátkem implementace řešení plán distribuce karet. Implementací řešení nesmí být narušena možnost stávajícího přihlášení do systému (přihlášení heslem, PINem apod.).

Dodavatel v rámci implementace zajistí:

- dodání HW komponent 3 inicializačních a 25 koncových stanic na vybraná pracoviště (v rámci hlavního areálu nemocnice) podle plánu distribuce nasazení (následný rollout na ostatní koncové stanice bude proveden objednatelem),
- instalaci řešení serverové části včetně jejich konfigurace v režimu vysoké dostupnosti (dále také HA),
- instalaci a konfiguraci 3 inicializačních pracovišť, kde jsou pracoviště pro výdej a nastavení karet,
- instalaci a konfiguraci testovacího vzorku koncových stanic (cca 25),
- konfiguraci řešení,
- dodání hybridních kontaktních/bezkontaktních čipových karet QSCD - eIDAS Compliant s následujícími kroky:
  - objednatel dodá soubory k výrobě karet, obsahující:
    - grafickou podobu karty a grafický manuál,
    - strukturovaná data uživatelských karet (údaje k vyplnění do šablon karet),
  - dodavatel předá dle plánu (cca v sedmi rozložených dávkách) potištěné a iniciované karty na stanovené jedno pracoviště objednatele. Jednotlivé dávky budou seřazeny/setříděny dle názvů pracoviště,
  - objednatel distribuuje karty na vybrané pracoviště kliniky, ústavu, úseku nebo odboru,
  - výměna karty uživatele za starou je v režii vybraného pracoviště objednatele,
  - aktivace karty je provedena uživatelem, který provede aktivaci při prvním přiložení karty na koncovou stanici spolu s nastavením PINu, případně dojde k nastavení alternativních možností přihlášení,
  - případné reklamace v prokazatelných chybách potisku či nefungování karty:
    - do 1 % z každé dávky budou řešeny objednatelem a dodavatel dodá náhradní nepotištěné karty,
    - při překročení 1 % z každé dávky bude požadována výměna chybných karet dodavatelem,
- zprovoznění HW/SW komponent 3 inicializačních pracovišť a 25-ti koncových stanic pro testovací provoz,
- dodání technické a provozní/administrátorské dokumentace,
- školení administrátorů a pracovníků inicializačních pracovišť,
- spuštění testovacího provozu,
- odstranění případných zjištěných nedostatků z testovacího provozu,
- spolupráce na spuštění testovacího provozu,
- akceptační testy,
- součinnost při akceptačních testech,
- součinnost při spuštění produkčního prostředí.

g) dodání technické, provozní/administrátorské dokumentace

Dodavatel vypracuje a předá podrobnou dokumentaci k řešení MFA v českém jazyce, zahrnující popis nebo postupy minimálně pro tyto oblasti:

- Technická dokumentace – popis architektury, systémů, konfigurací, nastavení a integrace řešení,
- Procesní dokumentace – nastavení postupů a procesů pro zavedení a správu karet,
- Provozní dokumentace – návody a postupy k správě řešení od její údržby, přes zálohování a záchranné mechanismy až po postupy obnovy při havárii,
- Uživatelská příručka a příručka pro správce.

h) zaškolení administrátorů a pracovníků inicializačních pracovišť

Zajištění proškolení administrátorů a pracovníků inicializačních pracovišť v rozsahu provozní a administrátorské dokumentace pro zaměstnance VFN (min. 10 zaměstnanců objednatele):

- na procesy a postupy zavedení a správy karet,
- na procesy a postupy inicializačních pracovišť,
- na údržbu a správu celého řešení,
- postupy práce na koncových stanicích.

i) akceptační testy

Akceptační testy budou provedeny dle objednatelem připravených testovacích scénářů. Akceptační testy pokrývají požadované funkčnosti definované v požadavcích na řešení MFA. Úspěšná akceptace je podmíněna následujícími podmínkami (kritéria):

- výsledky scénářů nesmí obsahovat žádné vady – Akceptace bez výhrad
- výsledky scénářů obsahují vady – Akceptace s výhradou

  - žádné podstatné vady typu A
  - maximálně 2 vady méně závažného typu B
  - maximálně 7 vad ostatního typu C
- při překročení jakékoli z vad typu A nebo B anebo C uvedených v předchozím bodě (Akceptace s výhradou) nebude řešení akceptováno.

Vada typu A:
- způsobuje, že systém neposkytuje některou z kritických funkcionalit systému (systém nesplňuje účel, pro který byl vytvořen, nebo uživatelé nemohou používat všechny používané funkcionality) nebo/a zároveň,
- činí zcela nefunkčním některou z komponent řešení MFA,
- způsobuje, že systém vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,
- systém vykazuje nedostatek, kdy implementační projekt zjevně neobsahuje části sjednané smlouvou nebo zadávací dokumentací, či zcela chybí podstatná část řešení.

Vada typu B:
- způsobuje, že je systém schopen omezeného provozu nebo neposkytuje některou z nekritických funkcionalit (systém splňuje účel, pro který byl vytvořen; uživatelé mohou používat všechny klíčové funkcionality) nebo/a zároveň,
- způsobuje, že některá z funkcionalit systému není plně činná nebo ztěžuje užívání u některého koncového uživatele, avšak tento stav má jen zanedbatelné dopady na provoz u objednatele.

Vada typu C:
- jsou ostatní závady/incidenty, které nejsou typu „A" ani „B".

j) Záruku a zajištění poskytování záručního servisu
Způsob poskytování záruky a záručního servisu je blíže specifikován v článku III. této smlouvy.

k) Služby na vyžádání
- Služby na vyžádání technického specialisty nad rámec předmětu plnění, který je uveden v čl. I. odst. 1 a) až j) této smlouvy budou realizovány v průběhu plnění této smlouvy na základě dílčích písemných objednávek objednatele, které budou zaslány na e-mailovou adresu kontaktní osoby dodavatele. Za písemnou formu se považuje rovněž její elektronická forma. Rozsah těchto služeb je sjednán na maximálně 50 MD po dobu platnosti záruky a záručního servisu v hodinové sazbě stanovené touto smlouvou.
- Služby na vyžádání budou hrazeny dle ceníku (vysoutěžená hodinová sazba).
- Služby na vyžádání jsou poskytované zpravidla v místě objednatele, služby mohou být po dohodě poskytnuty i vzdáleně. Z poskytnutých služeb je vždy vypracována zpráva o realizaci.
- Forma akceptace poskytnutých služeb je realizována oboustranně potvrzeným akceptačním protokolem.
- Služby na vyžádání zahrnují zejména:
  - konzultační a analytické služby zaměřené na požadovanou oblast,
  - poskytování systémových, programátorských a vývojových prací,
  - realizace požadavků na novou funkcionalitu nad rámec poptávaného řešení.

Bližší specifikace předmětu plnění je uvedena v Příloze č. 1 této smlouvy.

2. Dodavatel bere na vědomí, že v době uzavření smlouvy nesmí být dodávané technické nebo programové prostředky označeny NÚKIB jako hrozba. Následně poskytované služby nesmí být provozované na technických nebo programových prostředcích označených NÚKIB jako hrozba.
3. Dodavatel je povinen prostřednictvím dodavatelem určené odpovědné osoby neprodleně informovat objednatele: Manažera kybernetické bezpečnosti, e-mail: xxxxx, o kybernetických bezpečnostních incidentech souvisejících s implementací nebo při zajištění záručního servisu dodávaného řešení.
4. Součástí předmětu plnění dle této smlouvy je rovněž zajištění záruky na dodaný předmět plnění dle podmínek uvedených v čl. III smlouvy.
5. Dodavatel se zavazuje dodat předmět plnění dle čl. I a Přílohy č. 1 této smlouvy a objednatel se zavazuje uhradit dodavateli cenu specifikovanou v čl. IV. této smlouvy.

II. Dodání předmětu plnění

1. Dodavatel se zavazuje dodat objednateli předmět plnění dle čl. I., odst. 1 písm. a) až j) a Přílohy č. 1 této smlouvy **nejpozději do 180 kalendářních dnů od uzavření této smlouvy.**
2. HW a karty jež jsou součástí předmětu plnění budou dodány do sídla objednatele.
3. Dodavatel bude informovat objednatele o přesném termínu dodávky HW i dalších částí plnění, a to nejméně 3 pracovní dny před realizací dodávky. Při předání a převzetí HW bude pověřenými osobami obou smluvních stran podepsán dodací list.

Kontaktní a odpovědná osoba za objednatele: xxxxx,
Za převzetí HW: xxxxx,
Za akceptaci předmětu plnění: xxxxx,
xxxxx, a
xxxxx,
K nahlašování požadavků na záruční servis: xxxxx,
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy:
manažer KB, xxxxx

Za ochranu osobních údajů: Pověřenec, xxxxx

Kontaktní a odpovědná osoba za dodavatele: xxxxx,

Za předání HW: xxxxx,
Za akceptaci předmětu plnění: xxxxx,
K poskytování záručního servisu: xxxxx,
Za identifikaci případného kybernetického útoku v průběhu plnění předmětu plnění dle této smlouvy: xxxxx,

Za ochranu osobních údajů: xxxxx,

4. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí HW (je nedílnou součástí akceptačního protokolu).
5. Okamžikem protokolárního předání a převzetí HW přechází na objednatele vlastnické právo HW a nebezpečí škody na HW. Objednatel není povinen převzít HW či jeho část, která je poškozena nebo která jinak nesplňuje podmínky této smlouvy, zejména pak jakost zařízení.
6. Dodavatel odpovídá za dodržení přepravních podmínek po dobu přepravy HW k objednateli, tak aby nebylo zařízení znehodnoceno. Předmět plnění (HW) bude dopraven do místa plnění na vlastní náklady a nebezpečí dodavatele.
7. Dodávka se považuje podle této smlouvy za splněnou, pokud:
    - předmět plnění (HW i SW) byl řádně doručen a naimplementován,
    - bylo provedeno zaškolení administrátorů a pracovníků inicializačních pracovišť objednatele,
    - byla předána veškerá potřebná dokumentace,
    - byly provedeny akceptační testy,
    - předmět plnění byl řádně předán a převzat způsobem sjednaným níže,
    - byla provedena akceptace řádného předání a převzetí předmětu plnění.
8. Po splnění a předání celého předmětu plnění vystaví dodavatel akceptační protokol, který bude obsahovat níže uvedené náležitosti:
    - název a sídlo dodavatele a objednatele,
    - číslo smlouvy,
    - datum řádného předání/převzetí předmětu plnění,
    - stav HW a SW v okamžiku jeho předání a převzetí,
    - akceptace či výhrady,
    - jiné náležitosti důležité pro předání a převzetí dodaného předmětu plnění.
9. Dodací list podepíší a opatří otisky razítek oprávnění zaměstnanci obou smluvních stran. Takto opatřený dodací list slouží jako doklad o řádném předání a převzetí zboží (HW) (je nedílnou součástí akceptačního protokolu).
10. Objednatel není povinen akceptovat řádné předání a převzetí předmětu plnění v případě, že předmět plnění bude vykazovat vady a nedodělky. Pokud vada nebo nedodělek nebrání převzetí předmětu plnění smlouvy, musí být vždy uveden v akceptačním protokolu s uvedením data odstranění. Nebude-li objednatelem akceptováno řádné předání a převzetí předmětu plnění z důvodů vad a nedodělků, bude o této skutečnosti sepsán zápis s výčtem zjištěných vad nebo nedodělků, které zjistil objednatel včetně způsobu a lhůt k jejich odstranění. Tento zápis bude současně podepsán zástupci obou smluvních stran.
11. Dodavatel je při plnění dle této smlouvy povinen postupovat v souladu s vnitřními předpisy objednatele se kterými byl prokazatelně seznámen, zejména SM-UI-02 Používání sítě VFN externími uživateli.

III. Způsob poskytování záruky a záručního servisu

1. Dodavatel se zavazuje zajistit záruku včetně záručního servisu u dodaného předmětu plnění dle čl. I., odst. 1 a přílohy č. 1 této smlouvy po dobu 60 měsíců (nevztahuje na kontaktní/bezkontaktní karty) ode dne předání a převzetí celého předmětu plnění. Záruka na kontaktní/bezkontaktní karty je jeden rok od jejich předání objednateli.

2. Záruční servis předmětu plnění obsahuje:
    - odstraňování vad, součinnost s výrobcem,
    - poskytování aktualizací programových prostředků (nové verze, opravné verze, bezpečnostní záplaty),
    - soulad se zákony a normativy ČR a EU,
    - odstranění zjištěných zranitelností (penetrační testy, hrozba nebo opatření NÚKIB, výrobce nebo veřejně zdokumentovaných),
    - pomoc při řešení provozních problémů,
    - podpora na místě při implementaci aktualizací programových prostředků, a to na základě výzvy objednatele,
    - záruční servis v režimu 24x7 s reakční dobou uvedenou v čl. III odst. 4 této smlouvy,
    - exitová součinnost.

3. K zajištění elektronické komunikace mezi objednatelem a dodavatelem je určen helpdeskový nástroj objednatele ServiceDesk VFN. V tomto nástroji budou probíhat hlášení událostí, které bude dodavatel řešit podle kategorie, závažnosti a úrovni dostupnosti služeb (SLA). Za tímto účelem bude určeným pracovníkům dodavatele zřízen přístup do ServiceDesku objednatele. Pokud má dodavatel k dispozici svůj interní helpdeskový nástroj, je také možné provést jeho integraci s nástrojem objednatele.
   V případě technických potíží, které zabraňují objednateli komunikovat s dodavatelem prostřednictvím ServiceDesku objednatele dle předchozího odstavce, lze požadavky odeslat formou elektronické pošty na určenou emailovou adresu dodavatele xxxxx. Tato komunikace má z hlediska úrovně služeb stejnou váhu jako komunikace v ServiceDesku objednatele. Pro operativní komunikaci mezi objednatelem a dodavatelem bude zřízena telefonní Hot Line dodavatele na určeném telefonním čísle xxxxx.

4. Součástí záručního servisu je funkčnosti provozu systému v režimu 24 hodin denně, 7 dní v týdnu (dále též „24x7") při dostupnosti 99,5 % s následujícími parametry služby:

Úroveň závady	Parametry služby		
	Provozní doba služby Hot-line	**Maximální reakční doba od nahlášení požadavku:**	**Maximální doba odstranění závady**
Havárie*	7:00 – 16:30 HotLine – 9,5x5 HelpDesk – 9,5x5	do 2 hodin	do 24 hodin
Porucha**	7:00 – 16:30 HotLine – 9,5x5 HelpDesk – 9,5x5	do 24 hodin	do 48 hodin
Chyba***	7:00 – 16:30 HotLine – 9,5x5 HelpDesk – 9,5x5	do 48 hodin	do 15 pracovních dní

Maximální reakční doba na odstranění závady se počítá od okamžiku zadání hlášení závady objednatelem do systému Helpdesk objednatele.
Do doby na odstranění závady se nezapočítává doba, po kterou jsou dodávány doplňující či upřesňující informace nutné pro řešení objednatelem.
Řešení chyb a provozních problémů není omezeno počtem hodin / měsíc.

Kategorie incidentů/závad

Za závadu nebo incident je považována jakákoliv událost, která narušuje nebo by mohla narušit funkčnost dodaného plnění. Tyto události jsou reprezentovány servisním záznamem se stanovenou závažností. Za incident se nepovažuje porucha způsobená vyšší mocí, tj. živelnou pohromou, válečným konfliktem nebo teroristickým útokem anebo jinými podobnými událostmi, jež nastaly nezávisle na vůli dodavatele a brání mu ve splnění jeho povinností, jestliže nelze rozumně předpokládat, že by dodavatel tuto překážku nebo její následky odvrátil nebo překonal a dále, že by v době vzniku závazku tuto překážku předvídal.
Za závadu nebo incident se nepovažuje výpadek systému způsobený závadou HW objednatele.

Pro účely této smlouvy jsou definovány následující úrovně závad:

***Havárie:** Havárií se rozumí stav, který:
- způsobuje, že systém neposkytuje některou z kritických funkcionalit řešení (nesplňuje účel, pro který byl vytvořen, nebo uživatelé nemohou používat všechny používané funkcionality) nebo/a zároveň,
- činí zcela nefunkčním některou z komponent řešení u nadpolovičních většiny inicializačních či koncových stanic nebo/a zároveň,
- způsobuje, že řešení vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,
- řešení vykazuje nedostatek, kdy implementační projekt zjevně neobsahuje části sjednané smlouvou nebo zadávací dokumentací, či zcela chybí podstatná část řešení.

****Porucha:** Poruchou se rozumí stav, který:
- způsobuje, že řešení je schopno omezeného provozu nebo neposkytuje některou z nekritických funkcionalit (řešení splňuje účel, pro který byl vytvořen; uživatelé mohou používat všechny klíčové funkcionality) nebo/a zároveň,
- způsobuje, že některá z funkcionalit řešení není plně činná nebo ztěžuje užívání u některého koncového uživatele, avšak tento stav má jen zanedbatelné dopady na provoz u objednatele.

*****Chyba**: Chybou se rozumí stav, kdy:
- jsou ostatní závady/incidenty, které nespadají do kategorie „Havárie" ani „Porucha".

Záruční servis předmětu plnění obsahuje:

- Reakce na nahlášené chyby, problémy a požadavky.
- Analytická podpora řešení problémů zadaných do Helpdesku objednatele.
- Oprava vad, chyb a zranitelností.
- Řešení bezpečnostní chyby, hackerské/kybernetické útoky a zjištěné zranitelnosti řešení.
- Zajištění souladu se zákony a normativy ČR a EU.
- Reakce na dotazy oprávněných osob objednatele a metodická podpora při rutinním používání řešení.
- Obnova provozu řešení po výpadcích.
- Služby migrace řešení – převod řešení na vyšší verzi databázového prostředí a operačního systému.
- Služby zahrnující nastavení monitoringu, zálohování a auditingu/logování.
- Instalace oprav a nových verzí SW produktů, které byly dodány jako součást řešení, které jsou vyžadovány pro zajištění bezpečnosti řešení nebo rozvojových aktivit, včetně zajištění funkčnosti celého řešení po provedeném upgradu.
- Aktualizace dokumentace (změny řešení, nové verze).
- Ostatní nevyjmenované práce nutné pro zajištění funkčnosti řešení.

5. Exitová součinnost: Při ukončení záruky (smlouvy) dodavatel poskytne za účelem řádného a plynulého převedení všech činností spojených se zárukou řešení a to především:
   - poskytne náležitou a nezbytnou součinnost pro takové převedení,
   - poskytne veškeré nezbytné informace a dokumentaci,
   - předá objednateli data způsobem a formátem odsouhlaseným objednatelem.

6. Záruka se nevztahuje na poruchy, které byly způsobeny neodbornou obsluhou a údržbou, živelnou pohromou, nedodržením návodu od výrobce, nedodržením provozních podmínek nebo jiným způsobem než obvyklým provozem.
7. Po dobu záruční lhůty je objednatel povinen využívat dodaná zařízení dle pokynů dodavatele, popřípadě dle pokynů výrobce MONET+ výlučně v souladu s jejich posláním a příslušnými technickými podmínkami. Případná technická zlepšení nebo úpravy může vykonat jen na základě písemného souhlasu dodavatele nebo výrobce.
8. V případě zjištění nebo podezření na probíhající kybernetický útok v průběhu poskytování služeb (záruky) dodavatele, musí být provedeny nezbytné kroky dodavatelem k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě za VFN (viz kontaktní osoby), která rozhodne, zda budou práce ukončeny nebo bude v pracích pokračováno a za jakých podmínek.

IV. Cena a platební podmínky

1. Cena za předmět plnění dle čl. I., odst. 1 a) až j) této smlouvy byla sjednána ve výši:

Celková cena bez DPH	**9.879.200 Kč**
DPH	**2.074.632 Kč**
Cena vč. DPH	**11.953.832 Kč**

   (dále jen „cena")
2. Celková cena je stanovena jako konečná a zahrnuje cenu za celý předmět plnění a veškeré náklady dodavatele na plnění dle této smlouvy.
3. Cena služby technického specialisty poskytnuté objednateli na základě jeho emailových požadavků (objednávek) dle čl. I., odst. 1 k) této smlouvy činí 11.500 Kč bez DPH za 1 MD, což činí 1.437,50 Kč bez DPH za 1 hodinu práce dodavatele.
4. Objednatel se zavazuje zaplatit cenu uvedenou v čl. IV. odst. 1 této smlouvy na základě faktury vystavené dodavatelem. Dodavatel předá fakturu objednateli spolu s akceptačním protokolem, jehož součástí bude dodací list, popřípadě ho zašle objednateli do 14 dnů po řádném předání a převzetí předmětu plnění. Fakturována může být pouze celá dodávka předmětu plnění. Na faktuře budou rozepsány jednotlivé položky dle předmětu plnění.
5. Cena za poskytované služby dle čl. IV. odst. 3. této smlouvy bude objednatelem hrazena pouze po předchozí akceptaci každé jednotlivé realizace na základě objednávky. Přílohou jednotlivé faktury za jednotlivou realizaci služeb na vyžádání bude akceptační protokol příslušné fakturované realizace, který bude podepsán oběma smluvními stranami.
6. Faktura musí dále obsahovat všechny údaje uvedené v § 29 odst. 1 zákona č. 235/2004 Sb., o dani z přidané hodnoty a dle zákona č. 563/1991 Sb., o účetnictví. Splatnost faktury činí 60 dnů od jejího doručení objednateli. Faktura může být zaslána elektronicky ve formátu PDF nebo ISDOC na e-mailovou adresu: xxxxx nebo poštou ve dvou vyhotoveních na Ekonomický úsek objednatele, odbor účetnictví. K faktuře bude přiložena kopie řádně opatřeného dodacího listu způsobem sjednaným výše v čl. II. V případě zaslání faktury elektronicky bude dodací list přiložen v naskenované podobě.
7. V případě, že dodavatelem vystavená faktura bude obsahovat nesprávné či neúplné údaje, je právem objednatele takovou fakturu do 15 dnů od jejího převzetí vrátit dodavateli. Ten podle charakteru nedostatků fakturu opraví anebo vystaví novou. U opravené nebo nové faktury běží nová lhůta splatnosti.
8. Platby budou probíhat výhradně v CZK a rovněž veškeré cenové údaje budou v této měně.
9. Faktura musí obsahovat registrační čísla projektu. CZ.31.1.01/MV/23_50/0000050 a CZ.31.2.0/0.0/0.0/22_054/0007984 a musí obsahovat informaci, že se jedná o projekt financovaný z NPO, tzn. faktura musí obsahovat větu „Financováno Evropskou unií – Next Generation EU".
10. Faktury se platí bankovním převodem na účet druhé smluvní strany uvedený na faktuře. Povinnost objednatele zaplatit dodavateli vyúčtovanou dohodnutou cenu je splněna dnem odeslání platby z účtu objednatele.

V. Odstoupení od smlouvy

1. Kterákoliv ze smluvních stran je oprávněna od této smlouvy odstoupit v případě jejího podstatného porušení druhou smluvní stranou. Pro účely této smlouvy se za podstatné porušení smluvních povinností považuje takové porušení, u kterého strana porušující smlouvu měla nebo mohla předpokládat, že při takovémto porušení smlouvy, s přihlédnutím ke všem okolnostem, by druhá smluvní strana neměla zájem smlouvu uzavřít; zejména:
   - na straně objednatele nezaplacení ceny plnění podle této smlouvy ve lhůtě delší 60 dní po dni splatnosti příslušné faktury, přestože byl dodavatelem na neplnění této smlouvy písemně upozorněn,
   - na straně dodavatele zejména jednání uvedená v čl. VI. odst. 2 této smlouvy, tj. jestliže nedodá řádně a včas předmět plnění, pokud dodavatel nezjednal nápravu, přestože byl objednatelem na neplnění této smlouvy písemně upozorněn.
2. Odstoupení od smlouvy musí být provedeno písemným oznámením o odstoupení, které musí obsahovat důvod odstoupení a musí být doručeno druhé smluvní straně. Účinky odstoupení nastanou okamžikem doručení písemného vyhotovení odstoupení druhé smluvní straně.

VI. Sankce

1. Pro případ prodlení objednatele s úhradou ceny dle čl. IV. této smlouvy má dodavatel nárok na zaplacení úroku z prodlení ze strany objednatele ve výši 0,01 % z částky, s jejíž platbou je objednatel v prodlení, za každý den takového prodlení. Smluvní strany se dohodly, že dodavatel je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti.
2. V případě dodání jiného předmětu plnění než objednaného a při nedodržení dodací lhůty je kupující oprávněn požadovat zaplacení jednorázové smluvní pokuty ve výši 50.000,- Kč. Dále je objednatel oprávněn požadovat zaplacení další smluvní

pokuty ve výši 0,1 % z ceny plnění dle čl. IV. odst. 1 smlouvy bez DPH za každý započatý den prodlení s dodáním předmětu plnění, jestliže se s objednatelem nedohodne jinak. Objednatel je dále v těchto případech oprávněn odstoupit od smlouvy.

3. Za nedodržení termínu uvedeného ve čl. III. odst. 4 smlouvy, tzn. odstranění závady v úrovni „Havárie", má objednatel právo účtovat smluvní pokutu ve výši 2.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
4. Za nedodržení termínu uvedeného ve čl. III. odst. 4 smlouvy, tzn. odstranění závady v úrovni „Porucha", má objednatel právo účtovat smluvní pokutu ve výši 1.000,- Kč za každý započatý pracovní den za jednotlivý případ.
5. Za nedodržení termínu uvedeného ve čl. III. odst. 4 smlouvy, tzn. odstranění závady v úrovni „Chyba", má objednatel právo účtovat smluvní pokutu ve výši 1.000,- Kč za každou započatou hodinu prodlení za jednotlivý případ.
6. V případě prodlení dodavatele s dodržením termínů odstranění vad předmětu plnění, jsou-li uvedeny v akceptačním protokolu o předání a převzetí předmětu plnění dle čl. II. odst. 10 smlouvy, je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové ceny předmětu plnění bez DPH za každý i započatý den prodlení.
7. V případě nedodržení některé z povinností dodavatele stanovených v čl. VIII. odst. 2-4 smlouvy má objednatel právo účtovat smluvní pokutu ve výši 10.000,- Kč.
8. Za nedodržení povinností uvedených v čl. I. odst. 2 a 3 nebo v čl. III. odst. 8 nebo čl. VII, má objednatel právo účtovat smluvní pokutu ve výši 200.000,- Kč za každé jednotlivé porušení povinnosti.
9. V případě nedodržení některé z povinností dodavatele stanovených v čl. VIII. odst. 7 a 8 smlouvy má objednatel právo účtovat dodavateli smluvní pokutu ve výši sankce uložené objednateli Vlastníkem komponenty NPO (Ministerstvem vnitra ČR) za nedodržení povinností stanovených v Podmínkách rozhodnutí o poskytnutí dotace nebo ve výši zkrácení dotace z téhož důvodu.
10. V případě nedodržení povinnosti stanovené v čl. VIII. odst. 5 smlouvy má objednatel právo účtovat smluvní pokutu ve výši pohledávky, která byla postoupena v rozporu s touto smlouvu. Objednatel má zároveň právo odstoupit od smlouvy.
11. Smluvní pokuta bude vyúčtovaná samostatným daňovým dokladem a její splatnost činí 30 dní ode dne doručení daňového dokladu. Zaplacením smluvní pokuty není dotčeno právo na náhradu škody vzniklé smluvní straně požadující zaplacení smluvní pokuty.

VII. Mlčenlivost

1. Dodavatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o objednateli, jeho zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Dodavatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen „Osobní údaje") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen GDPR) a příslušnými ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů.
2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.
3. Pokud dodavatel přijde při plnění Smlouvy do styku s Osobními údaji a bude v postavení zpracovatele ve smyslu GDPR a Zákona o zpracování osobních údajů, zavazuje se nakládat s Osobními údaji pouze za účelem splnění závazků z této smlouvy a žádným jiným způsobem, a to v souladu příslušnými ustanoveními GDPR a Zákona o zpracování osobních údajů v rozsahu nezbytném pro plnění smlouvy a po dobu nezbytnou k plnění smlouvy. Zpracovávání Osobních údajů v rozsahu údajů poskytnutých objednatelem a týkajících se zdravotnické dokumentace pacientů, jimž jsou objednatelem poskytovány zdravotní služby, a dále v rozsahu Osobních údajů zaměstnanců objednatele dodavatelem může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů zjištěných při poskytování služeb dle této smlouvy, může také zahrnovat zlepšování funkcí informačních systémů, vyhledávání hrozeb uživatelům a ochrany uživatelů informačních systémů. Osobní údaje nebudou použity k jinému účelu, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely. Dodavatel se zavazuje za účelem ochrany osobních údajů objednatele a jeho pacientů a zaměstnanců před neoprávněným přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou uplatňovat technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů zajišťující splnění všech povinností dle GDPR a Zákona o ochraně osobních údajů, zejména zajistit, aby data obsažená ve zdravotnické dokumentaci byla šifrována způsobem, který znemožní nahlížení do těchto údajů neoprávněným osobám.
4. Dodavatel se zavazuje zajistit informovanost svých pracovníků (včetně poddodavatelů) o povinnostech vyplývajících z této Smlouvy. Dodavatel se zavazuje zajistit, aby jeho pracovníci, kteří budou přicházet do styku s osobními údaji, byli smluvně vázáni povinností mlčenlivosti ve smyslu GDPR a Zákona o zpracování osobních údajů a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich smluvního vztahu k objednateli. Toto ujednání je sjednáno ve smyslu ustanovení čl. 28 GDPR. Dodavatel se zavazuje informovat své poddodavatele o povinnosti mlčenlivosti dle této smlouvy. V případě porušení mlčenlivosti za strany poddodavatele, odpovídá dodavatel objednateli za vzniklou škodu, jako kdyby povinnost porušil sám.
5. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu, k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle prvé věty tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání.
6. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie informací či jiné záznamy nad rámec plnění dle této smlouvy, a nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.
7. Smluvní strany se zavazují pro případ, že se v průběhu plnění dle této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývajícími z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani jinak nepoškodit, neztratit či neznehodnotit.
8. Dodavatel se zavazuje plně respektovat bezpečnostní požadavky objednatele k zajištění ochrany Osobních údajů pacientů a zaměstnanců objednatele.
9. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících Osobní údaje trvá bez časového omezení.

10. Smluvní strany vylučují povinnosti jim uložené ve smyslu čl. VIII., a to za předpokladu plnění povinností jim uložených platnými právními předpisy, především, nikoliv však výlučně zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále též „**registr smluv**").

VIII. Ostatní ujednání

1. Dodavatel bere na vědomí, že objednatel je povinen dle ustanovení § 219 odst. 1 zákona č. 134/2016 Sb., a dle zákona č. 340/2015 Sb., o registru smluv uveřejnit tuto smlouvu včetně případných dodatků, zákonem stanoveným způsobem.
2. Dodavatel je povinen v souladu s ustanovením § 105 z. č. 134/2016 Sb. předložit do 10 pracovních dnů od doručení oznámení o výběru dodavatele objednateli seznam, ve kterém uvede, jaké části předmětu plnění a v jakém rozsahu bude plnit prostřednictvím poddodavatele, spolu s identifikací poddodavatele a uvedením rozsahu jeho plnění, pokud mu jsou známi. Poddodavatelé, kteří nebyli tímto způsobem identifikováni a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni dodatečně, a to nejpozději před zahájením plnění veřejné zakázky tímto poddodavatelem.
3. Dodavatel je povinen mít v platnosti a udržovat pojištění odpovědnosti za škodu způsobenou objednateli či třetím osobám při výkonu podnikatelské činnosti, která je předmětem této smlouvy, s limitem pojistného plnění v minimální výši 1.000.000,- Kč.
4. Dodavatel je povinen udržovat výše uvedené pojištění po celou dobu trvání smlouvy. V případě porušení této povinnosti je objednatel oprávněn od smlouvy, která bude uzavřena na základě výsledku tohoto zadávacího řízení odstoupit. Na žádost objednatele je dodavatel povinen předložit objednateli dokumenty prokazující, že pojištění v požadovaném rozsahu a výši trvá. Pokud by v důsledku pojistného plnění nebo jiné události mělo dojít k zániku pojištění, k omezení rozsahu pojištěných rizik, ke snížení stanovené min. výše pojistného plnění, nebo k jiným změnám, které by znamenaly zhoršení podmínek oproti původnímu stavu, je dodavatel povinen učinit příslušná opatření tak, aby pojištění bylo udrženo tak, jak je požadováno v tomto ustanovení.
5. Dodavatel je oprávněn postoupit pohledávku vyplývající z plnění dle této smlouvy na třetí osobu pouze s předchozím písemným souhlasem objednatele.
6. Dodavatel se zavazuje dodržovat nařízení objednatele, kterým je zakázáno kouření ve všech prostorách i plochách areálu objednatele s výjimkou vyhrazených míst.
7. Dodavatel je povinen uchovávat veškeré doklady související s realizací plnění předmětu smlouvy (způsobem dle zákona o účetnictví) včetně účetních dokladů minimálně do konce roku 2036 nebo po dobu nejméně 10 let ode dne poslední platby za provedené práce, přičemž závazná je lhůta, která je delší. Dále je povinen zajistit, aby také všichni jeho poddodavatelé, partneři, dodavatelé partnerů uchovávali veškeré dokumenty související s prováděním plnění předmětu této smlouvy.
8. Minimálně do konce roku 2036 resp. ve lhůtách dle předchozího odstavce je dodavatel povinen poskytovat požadované informace a dokumentaci související s realizací projektu objednateli, zaměstnancům nebo zmocněncům pověřených orgánů (MV ČR, MZ ČR, MPO ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů veřejné správy), a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout jim při provádění kontroly součinnost a být fyzicky přítomen kontrolám v místě plnění.

IX. Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem podpisu smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
2. Veškeré právní vztahy založené, resp. vyplývající z této smlouvy, které zde nejsou výslovně upravené, včetně eventuálních řešení vzájemných sporů, se řídí ustanoveními příslušných právních předpisů České republiky. Změny a doplnění této smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, vzestupně číslovaných dodatků této smlouvy podepsanými jejich statutárními zástupci.
3. Tato smlouva včetně příloh je vyhotovena ve 2 stejnopisech, z nichž každá strana obdrží po jednom vyhotovení. Obě vyhotovení jsou rovnocenná a mají platnost originálu.
4. Autentičnost této smlouvy potvrzují smluvní strany svými vlastnoručními podpisy.

Přílohy:
Příloha č. 1 – Technická a funkční specifikace předmětu plnění
Příloha č. 2 – Minimální technické a funkční požadavky objednatele
Příloha č. 3 – Položkový ceník
Příloha č. 4 - Používání sítě VFN externími uživateli

V Praze dne:

---

prof. MUDr. David Feltl, Ph.D., MBA
ředitel Všeobecné fakultní nemocnice v Praze

Ve Zlíně dne:

Ing. Břetislav Endrys, předseda představenstva
Ing. Jan Vavrys, člen představenstva

Příloha č. 1 smlouvy

Technická a funkční specifikace plnění
Čipové karty ProID a čtečky
ProID+ Q jsou 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; v doménovém prostředí je to nejčastěji doménová certifikační autorita na platformě MS Windows Server – multifaktorová autentizace uživatele. Karty však mohou hostovat certifikáty, vydané z libovolných certifikačních autorit, např. akreditovaných poskytovatelů certifikačních služeb – eIdentity a PostSignum.
Karty ProID+ Q jsou procesorové čipové karty, s implementovanou asymetrickou kryptografií na kontaktním čipu, umožňují bezpečné uložení privátních klíčů a z toho vyplývající výhody:

- 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.

Kontaktní část čipových karet reprezentuje čip od společnosti Thales. Tento typ čipu splňuje mezinárodní kryptografické standardy. Jedná se o nejnovější dodávaný typ čipu.
ProID+ je v souladu s Smart Card Minidriver Specification; lze jej použít v řadě aplikací, které podporují kryptografické standardy Microsoft CryptoAPI, Cryptography Next Generation, PKCS#11 nebo TokenD.
Nabízená čipová karta je ve formátu ID-1, což odpovídá přesným rozměrům a velikosti bankovní karty.
Karta ProID+ Q disponuje certifikací QSCD. Čip společně s aplikací nahranou v čipu karty ProID+ Q podléhá certifikaci QSCD a podporuje vydání certifikátů pro kvalifikovaný elektronický podpis v režimu eIDAS.
Jedna karta na všechno – bezpečnost, bezkontaktní čip a držitelské údaje na těle karty. Taková karta nabízí držiteli integraci hned několika funkcí a nejlépe zapadá do pracovního prostředí.
Karta je kromě kontaktního také osazena bezkontaktním čipem: bezkontaktní FIDO, bezkontaktní NXP, Mifare Desfire EV1 8Kb.
Kontaktní/bezkontaktní čtečky splňující interoperabilní čtení a zápis podporující:

- kontaktní čtečka splňující ukládání kvalifikovaného elektronického podpisu splňující nařízení eIDAS, většiny technologií bezkontaktních čipových karet,
- NFC,
- FIDO2,
- ovladače CCID,
- standardy ISO 14443 A/B a ISO 15693,
- USB 2.0/3.0 rozhraní,

Manažer ProID
Manažer ProID+ zajišťuje snadné ovládání procesů spojených s kartami a certifikáty v organizaci. Jeho funkce jsou do organizace implementovány prostřednictvím samostatných aplikací. Následující podkapitoly popisují funkce jednotlivých aplikací. ProID+ manažer podporuje jak karty ProID+ tak ProID+Q.
1.1.1Card Management System ProID
Pro evidenci a správu karet bude implementován Card Management System ProID+ (CMS ProID+). CMS je základním modulem pro evidenci a podporu karet v organizaci. Mezi hlavní funkce CMS ProID+ patří:

- evidence karet, používaných v rámci organizace;
- evidence držitelů karet a
- evidence dat na kartách (certifikáty, uživatelská data).

Evidence CMS dává komplexní a aktuální obraz o kartách, používaných v rámci organizace. Umožňuje provádět efektivní správu, včetně podpory a sledování životního cyklu karet.

Data karty
CMS eviduje kompletní informace o kartách:

- identifikátor karty,
- typ karty,
- 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) a
- data na kartě (certifikáty a další data, včetně historie dat na kartě).

Integrace CMS do domény MS Windows
Card Management System ProID+ je velmi těsně integrován do domény MS Windows:

- CMS využívá doménová Active Directory jako zdroj informací o uživatelích / držitelích karet,
- CMS akceptuje nastavení doménových bezpečnostních politik,
- uživatelské role CMS jsou mapovány na doménové skupiny (domain groups),
- CMS definuje oprávnění na úrovni doménových skupin,
- CMS podporuje využití integrované autentizace domény MS Windows (Single Sign On).

Centrální úložiště dat CMS ProID+
Evidence CMS je striktně centralizovaná, veškerá data CMS jsou uložena v jedné MS SQL databázi.
Pro přístup do centrální evidence se využívá doménové infrastruktury:

- K centrální evidenci lze přistupovat po síti. Využívá se sítových propojení, nad kterými běží i komunikační mechanismy domény.

- Při přístupu k datům se využívá integrovaná autentizace MS Windows. Doménoví uživatelé nemusí při přístupu k datům zadávat žádné autentizační údaje; je akceptováno doménové pověření uživatele.
- Přístupová oprávnění k jednotlivým typům dat jsou řízena na úrovni doménových skupin. Správa přístupových oprávnění je pak integrována do Active Directory, oprávnění jsou přidělována běžnými nástroji MS Windows, resp. automaticky Identity Management Systemem.

Přístup k datům přes webové rozhraní
Běžní uživatelé ani operátoři nepřistupují přímo do centrální databáze CMS. S databází CMS komunikují prostřednictvím webového serveru CMS.
K prohlížení dat CMS nepotřebují mít na svém počítači instalován žádný specifický program, používají webový prohlížeč.
Díky tomu jsou data CMS dostupná z libovolného počítače v rámci domény: uživatel se může přihlásit k libovolnému počítači v doméně, spustit prohlížeč a vyhledat data.
Uživatel se při přístupu k webu CMS nemusí speciálně autentizovat. Web CMS akceptuje uživatelský účet (resp. pověření), jímž se uživatel přihlásil do domény (integrovaná autentizace, Single Sign On).
Uživatel může prohlížet a manipulovat pouze s daty, k nimž má přístupová oprávnění. Přístupová oprávnění jsou definována na úrovni doménových skupin. (Uživatel musí být členem příslušné doménové skupiny.)
CMS spolupracuje s dalšími podpůrnými programovými moduly technologie ProID+ (např. Kartové centrum atd.). Tyto moduly čtou a zapisují data do centrální evidence CMS.
Podobně jako uživatelé, ani moduly ProID+ nepřistupují do centrální databáze přímo, nýbrž prostřednictvím webového serveru, resp. webových služeb (web services).

Podpora životního cyklu karet
CMS eviduje stavy jednotlivých karet např. nová, používaná, ztracená, skartovaná atd.
CMS také spolupracuje s dalšími moduly technologie ProID+, které pracují s čipovými kartami. Tyto moduly zasílají informace o provedených operacích do CMS. Změny stavů i informace o držitelích jsou tak automaticky promítány do centrální evidence. Díky tomu jsou údaje vždy aktuální. Centrální evidence poskytuje komplexní obraz nad daty a událostmi jednotlivých karet.
Úpravy životního cyklu karet se řeší v průběhu přípravy implementace CMS do interních systémů organizace.
Architektura CMS ProID+
Systém CMS tvoří dva základní stavební kameny:
- MS SQL databáze, která obsahuje data o kartách.
- Webový server, jehož prostřednictvím mohou klienti číst a zapisovat data z/do centrální evidence.

WWW server zprostředkovává přístup k centrální databázi karet:
- uživatelům umožňuje nahlížet do centrální evidence prostřednictvím webových formulářů,
- správcům umožňuje pomocí webového prohlížeče modifikovat evidovaná data,
- modulům technologie ProID+ dává možnost zapisovat údaje přes webové služby (web services),
- externím systémům umožňuje čerpat informace o kartách prostřednictvím webových služeb.

Sledování dat na kartě
Data čipových karet jsou modifikována lokálně na počítači uživatele, příp. na počítačích správců (např. Kartové centrum). Pro organizaci (a pro správce) je výhodné sledovat datové změny na provozovaných čipových kartách a mít tak evidovaný kompletní datový obraz karet.

Centrální evidence dat na kartách přináší tyto výhody:
- Správce systému má přehled nad kartami a elektronickými identitami uživatelů domény.
- Správce může snadno zjistit, zda uživatel má na své kartě elektronické identity, které tam má mít (zda mu nějaká nechybí a zda na kartě nemá identity, které by mít neměl).
- Správce může snadno zjistit, v jakém stavu jsou elektronické identity na kartě uživatele: zda jsou platné, jak dlouho ještě budou platné atd.
- Informace lze využít např. při ztrátě karty: certifikáty uložené na kartě je třeba odvolat.
- Informace lze z evidence exportovat do návazných systémů.

Centrální evidenci dat na kartách realizuje modul Card Content Monitor (CCM):
- Klientský modul CCM je instalován na všechny klientské počítače. (Je integrován do obslužného software čipové karty, který je instalován na klientské počítače.) Klientský modul CCM monitoruje veškeré operace prováděné s čipovou kartou. Pokud jsou na kartě provedeny datové změny, klientský modul CCM je automaticky zapíše do centrální evidence.
- Centrální evidence dat obsahuje datové struktury pro evidenci dat na kartách.
- Webová služba CCM je instalována na webovém serveru CMS. Prostřednictvím webové služby odesílá klientský modul CCM do centrální evidence informace o datových změnách.

Je třeba zdůraznit, že systém CCM eviduje pouze veřejná data, jako jsou:
- čísla karet,
- názvy kontejnerů na kartách,
- certifikáty (s veřejnými klíči),
- veřejné datové objekty.

Privátní klíče nelze z čipových karet přečíst, nejsou uvedeny v centrální evidenci. Předpokládá se však, že každý evidovaný kontejner obsahuje privátní klíč.
CCM také do evidence nezapisuje hodnoty PIN / PUK, případně QPIN.

Webové stránky CSM ProID+
Součástí implementace CMS je webový server. Hostuje webové stránky a prostřednictvím jich lze:
- prohlížet data evidovaná v CMS,
- modifikovat (některá) data CMS a

- generovat reporty s informacemi o kartách.

Navigace v datech CMS využívá běžných webových odkazů, menu a grafických symbolů. Ovládání webových stránek je intuitivní. Po krátkém zaškolení zvládne obsluhu stránek i méně zkušený uživatel.

Informace o uživatelích

CMS nevede vlastní evidenci uživatelů, čerpá data o uživatelích z Active Directory (AD). V databázi CMS je evidován pouze identifikátor (SID) uživatele AD. Veškeré další informace o uživatelích jsou v případě potřeby vyhledána v AD.

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

Pro vyhledání informací o uživatelích musí mít webový server CMS přístup (pro čtení) do AD.

Předpokládá se, že všichni uživatelé CMS (správcové karet i držitelé karet) jsou doménovými uživateli.

Kartové centrum

Aplikací pro centrální personalizaci a správu čipových karet je Kartové centrum ProID.

Kartové centrum ProID je implementováno jako tlustý klient a bude instalováno na počítači správců karet. Provoz 3 instancí aplikace.

Kartové centrum ProID formou intuitivního grafického rozhraní podporuje řadu scénářů, každý scénář je určen pro jinou situaci v rámci životního cyklu karty:

- **Vydání nové (trvalé) karty.** Obsluha zvolí uživatele a pomocí kartového centra pro něj připravuje kartu: vydává na každou kartu jeden či více doménových certifikátů (podle zvoleného „profilu"). Uživatel, který vlastní kartu, zadá hodnotu PIN a autentizuje se ke kartě. Uživatel, který obdrží novou kartu, si bude volit hodnotu PIN, QPIN a PUK. Výsledkem procesu jsou karty, připravené pro použití v doménovém prostředí, které lze distribuovat pracovníkům a ti je mohou ihned začít používat a nechat si na ně vydat certifikáty z akreditované CA. Součástí procesu vydání karty jsou kontroly, např. zda daná karta náleží danému uživateli anebo zda jde o správný typ karty.
- **Vydání dočasné karty.** Obsluha zvolí uživatele a poté mu na dočasnou kartu vydává jeden či více doménových certifikátů, obvykle se zkrácenou dobou platnosti. Uživatel si v rámci procesu vydání karty nastaví nové hodnoty PIN QPIN a PUK. Scénář slouží pro řešení situace, kdy je třeba pracovníkovi operativně vydat kartu s doménovými certifikáty; např. pro řešení situace zapomenutí karty, ztráty karty, nových zaměstnanců. Předpokládá se, že dočasná karta překlene období, než se pracovníkovi vydá trvalá karta.
- **Obnova doménových certifikátů na kartě.** Obsluha obnoví sadu certifikátů, uloženou na kartě jiného pracovníka. Držitel karty autorizuje operaci zadáním PIN (musí být přítomen operaci). Po obnově jsou z karty odstraněny nepotřebné certifikáty a klíče.
- **Odvolání doménových certifikátů na kartách.** Obsluha může vyhledat jednu či více karet a odvolat certifikáty, které jsou evidovány k jednotlivým kartám.
- **Evidence ztráty či zničení karty.** Obsluha může vyhledat jednu či více karet, označit ji v evidenci jako ztracenou či zničenou / skartovanou; aplikace zároveň odvolá doménové certifikáty, evidované k vybraným kartám.
- **Import informací o nových kartách.** Informace o nově dodaných kartách se importují do centrální evidence. Jsou spárovány s evidovanými držiteli. Importované informace o bezkontaktním čipu mohou být propagovány do návazných (bezkontaktních) systémů.

Kartové centrum ProID+ provádí bezpečnostně citlivé operace. Informace o prováděných operacích jsou (pro zpětnou kontrolu) auditovány.

Oprávnění k použití Kartového centra

Pro použití aplikace Kartové centrum ProID+ se předpokládá využití integrované doménové autentizace: Kartové centrum ProID+ akceptuje doménová pověření obsluhy.

Obsluha musí mít tato oprávnění

- Pro vydávání certifikátů musí být držitelem certifikátu typu enrollment agent
- Pro schvalování žádostí a odvolávání certifikátů musí mít vůči CA oprávnění Issue and Manage Certificates
- Pro čtení / zápis dat do CMS musí mít oprávnění správce karet CMS

Požadovaná oprávnění budou operátorům přidělena prostřednictvím členství v definované doménové skupině.

ACEx

Obnova certifikátu na čipovou kartu může být pro méně zkušeného uživatele komplikovaný proces. Proto je na počítače uživatelů instalována aplikace ACEx (Authentication Certificate Exchange), která

- pravidelně kontroluje certifikáty na kartě a v případě potřeby automaticky vyzve uživatele k obnově certifikátů.
- provádí uživatele celým procesem vydání nového certifikátu.

Úkolem ACEx je především

- Kontrolovat obsah karty a rozhodnout, kdy je třeba obnovit na kartě certifikát.
- Postarat se o úspěšnou obnovu certifikátu na kartě.

ACEx je tedy jednoduchý grafický průvodce procesem obnovy certifikátu. Po úspěšném dokončení práce aplikace ACEx by uživatel měl mít na kartě obnovené certifikáty, použitelné v dalším období v rámci budovaného prostředí.

Jedním z úkolů aplikace ACEx je, pravidelně kontrolovat obsah karty, resp. blížící se konec platnosti certifikátu. Pro zajištění pravidelné kontroly je ACEx spouštěn vždy po přihlášení uživatele. Uživatel spuštění aplikace ACEx nezaznamená: aplikace funguje na pozadí, bez grafického rozhraní. Pouze v případě potřeby provést obnovu certifikátu zobrazí okno s výzvou k započetí procesu. Aplikace ACEx žurnáluje svoji činnost pro usnadnění detekce a řešení případných chybových stavů. Žurnál je vytvářen během analýzy karet i během vydávání certifikátu.

Služby ProID

Návrh životního cyklu karet:

Před implementací karet a aplikací bude vypracován dokument s návrhem životního cyklu karet v organizaci. V rámci dokumentu budou řešena témata:

- Role uživatelů pro správu a použití karet
- Způsob distribuce karet uživatelům
- Vydání a obnova certifikátů na kartách

- Podporované stavy karet a jejich vlastnosti
- Řešení nestandardních stavů karet (zapomenutí, ztráta, zničení, …)
- Aplikační scénáře (podklady pro konfiguraci dodávaných aplikací)

Postup zpracování návrhu životního cyklu

Zpracování návrhu životního cyklu se předpokládá následujícím způsobem:
Před zpracováním dokumentu proběhne telekonference, kde se zástupci MONET+ dohodnou se zákazníkem na obsahu dokumentu.
Následně vznikne dokument „Návrh životního cyklu karet", který bude přesně popisovat dodávku pro zákazníka.
Dokument bude předán k revizím a schválení zákazníkem v editovatelné podobě ve formátu MS Word prostřednictvím e-mailu.
Případné vypořádání revizí a komentářů bude řešeno telekonferenčně.
Na základě schváleného dokumentu Návrh životního cyklu karet bude provedena implementace u zákazníka. Nabízené řešení bude v souladu s přílohou č. 2 této Smlouvy.

Doménová certifikační autorita:

Nejsnazší cestou k certifikátům v doméně je aktivace doménové certifikační služby a vydávání certifikátů z takto vytvořené doménové certifikační autority (dále jen „CA"). Takto získané certifikáty jsou pro organizaci zdarma. Tyto certifikáty nelze použít pro kvalifikovaný elektronický podpis.
MONET+ tímto způsobem vytvořil doménový PKI systém v řadě projektů.

- Kořenová certifikační autorita v módu enterprise (=vydávající CA)
  - Klíč CA chráněn v operačním systému
  - CRL publikován do intranetu přes Active Directory a přes WWW server
  - Základní sada šablon certifikátů (Domain Controller, WWW server, Enrollment Agent, Smartcard User)
  - Bude dodána specifická dokumentace havarijní plány a provozní dokumentace CA.
  - Nejsou dodávány certifikační politiky ani certifikační prováděcí směrnice

Implementace aplikací pro správu karet a školení:

Podkladem pro implementaci a konfiguraci aplikací budou odsouhlasené dokumenty:

- Dokument s návrhem životního cyklu karet a certifikátů
- Dokument s návrhem bezpečnostního konceptu PKI
- Dokument s přehledem šablon certifikátů

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

- Vydání nové karty a doménového certifikátu
- Autentizace do domény
- Podepsání dat
- Vyhledání a přehled informací o kartě v systému CMS
- Obnova doménového certifikátu pomocí aplikace ACEx

2 Multifaktorová autentizace uživatelů AD

2.1 Popis prostředí objednatele

Prostředí objednatele se skládá z virtuálních serverů na platformě VMware ESX, několika fyzických serverů, které není možné či vhodné z jejich podstaty virtualizovat z fyzických a virtuálních pracovních stanic, síťových prvků v topologii hvězda, tj. s centrálním přepínačem, a dalších zařízení. Uvedené servery jsou umístěny ve dvou geograficky oddělených datových centrech z důvodu zajištění vysoké dostupnosti (HA - High Availability) provozovaných IS.

Servery s datovými úložišti komunikují prostřednictvím SAN Fibre Channel sítě vybavené redundantními Cisco MDS přepínači. Maximální, a současně preferovaná, linková rychlost je 16 Gbit.

Fyzické pracovní stanice jsou vybaveny operačním systémem a Windows 10 (omezeně Windows 7).

U informačních systémů objednatele je v maximální efektivní míře implementována funkce Single Sign-On s využitím služby Microsoft Active Directory (autentizační protokol Kerberos). Uživatel se autentizuje pouze do domény a při spuštění aplikace již není zadávání jména/hesla zpravidla nutné.

2.2 Požadavky na řešení multifaktorové autentizace uživatelů AD

Řešení multifaktorové autentizace uživatelů AD musí splňovat následující požadavky a technické parametry:

- V souladu s normami/standardy:
  - ČSN EN ISO 7816, část 1-4 Identifikační karty – Karty s integrovanými obvody,
  - ISO/IEC 14443, část 2-3 Identifikační karty – Bezkontaktní karty s integrovanými obvody – Karty s vazbou na blízko,
  - EN 419 211 Profil ochrany pro zařízení vytvářející bezpečný podpis,
  - ČSN ETSI EN 302 190 V1.1.1 Komunikace v blízkém poli – Rozhraní a protokol (NFCIP-1),
- hybridní kontaktní/bezkontaktní čipové karty QSCD - eIDAS Compliant (dále také karta) ve formátu ID-1 (velikost bankovní karty) pro multifaktorové přihlašování do doménového prostředí MS Windows, podpora bezpečnostního standardu na ukládání přihlašovacích údajů a kvalifikovaných certifikátů (např. FIDO2, eIDAS), NXP a RFID,
- centralizovaná správa životního cyklu karet pro cca 10 tis. karet, instalace SW a základní konfigurace v režimu vysoké dostupnosti (HA),
- MFA ověření na koncových zařízeních,
- inicializační pracoviště pro výrobu karet,
- Kontaktní/bezkontaktní čtečky splňující interoperabilní čtení a zápis podporující:
  - kontaktní čtečka splňující ukládání kvalifikovaného elektronického podpisu splňující nařízení eIDAS,
  - většiny technologií bezkontaktních čipových karet,
  - NFC,
  - FIDO2,
  - ovladače CCID,
  - standardy ISO 14443 A/B a ISO 15693,
  - USB 2.0/3.0 rozhraní,

  v textu dále uváděna jako „kontaktní/bezkontaktní čtečka (RFID) připojitelná přes USB",
- musí umožňovat využívání ověřovacích metod pro multifaktorové přihlášení s využitím bezkontaktní karty a návaznost na Windows Hello (bezkontaktní karta podporuje ověření přes Windows Hello prostřednictvím FIDO2 přes Azure AD),
- propojení a synchronizace s Active Directory,
- podpora Windows Single Sign On.
- Dodané hybridní kontaktní/bezkontaktní čipové karty (6900 kusů) musí splňovat:
  a) Kontaktní čip splňující ukládání kvalifikovaného elektronického podpisu odpovídající nařízení eIDAS,
  b) bezkontaktní FIDO, bezkontaktní NXP, Mifare Desfire EV1 8Kb,

2.3 Funkční požadavky na řešení

V následujících podkapitolách jsou definovány požadavky na funkce SW nebo komponent v návaznosti na zajištění interně definovaných procesů.

2.3.1 Centrální správa karet

Požadavky na centrální správu karet z pohledu zajištění životního cyklu karet:

- zavedení nové karty do správy,

- změny údajů a vlastností aktivních/zneplatněných karet,
- odebrání/zneplatnění karty,
- vyhledání a filtrování množiny karet dle zadaných parametrů (jméno, osobní číslo, číslo karty, aktivní/odebraná/zneplatněná apod.,
- možnost hromadného nahrání čísel karet včetně inicializačních parametrů do správy,
- možnost exportu čísel karet a základní údajů o uživateli (např. jméno, osobní číslo),
- napojení na inicializační pracoviště k možnosti inicializace karet a ověření nastavených parametrů ve správě karet,
- možnost zálohování a obnovy databáze správy karet,
- řízení přístupu k správě přes AD skupiny.

2.3.2 Inicializace karet

Požadavky na inicializační pracoviště karet:

- inicializaci nové karty,
- opakovaná (přepis) inicializace karty,
- změny údajů a vlastností aktivních/zneplatněných karet,
- odebrání/zneplatnění karty,
- vyčtení údajů z centrální správy karet,
- reset PINu karty.

2.3.3 Klientská stanice

Požadavky na klientské stanici:

- MFA ověření prostřednictvím bezkontaktní čipové karty,
- aktivace nové karty,
- změna PINu na kartě,
- kompatibilita s Windows Hello.

Příloha č. 3 – Položkový ceník

Předmět plnění VZ	Množství	Jednotka	Nabídková cena/jednotka		Nabídková cena celkem		
			(bez DPH)	(s DPH)	(bez DPH)	Samostatně DPH (základní sazba)	(s DPH)
Řešení multifaktorové autentizace uživatelů v Active Directory (AD) v souladu se zadávacími podmínkami a s návrhem smlouvy							
Časově neomezená užívací práva k SW pro centrální správu životního cyklu čipových karet dle čl. I., odst. 1 a) návrhu smlouvy včetně instalace a konfigurace v režimu vysoké dostupnosti, záruky a záručního servisu **(60 měsíců)**	2	serverová licence	1 532 500,00 Kč	1 854 325,00 Kč	3 065 000,00 Kč	643 650,00 Kč	3 708 650,00 Kč
HW/SW klientské části pro 4200 počítačů dle čl. I., odst. 1 b) návrhu smlouvy včetně záruky a záručního servisu (60 měsíců):							
• **Časově neomezená užívací práva ke klientskému SW (včetně případných licencí do centrální správy) včetně instalace a konfigurace**	4200	klientská licence	59,00 Kč	71,39 Kč	247 800,00 Kč	52 038,00 Kč	299 838,00 Kč
• **Kontaktní/bezkontaktní čtečka (RFID) připojitelná přes USB**	4200	ks	545,00 Kč	659,45 Kč	2 289 000,00 Kč	480 690,00 Kč	2 769 690,00 Kč
• **Štítek a upevnění nebo zajištění neklouzavé spodní části (např. oboustranná lepenka, přísavka nebo suchý zip)**	4200	ks	5,00 Kč	6,05 Kč	21 000,00 Kč	4 410,00 Kč	25 410,00 Kč
HW/SW klientské části pro 3 počítače inicializačních pracovišť dle čl. I., odst. 1 c) návrhu smlouvy včetně záruky a záručního							
• **Časově neomezená užívací práva k inicializačnímu SW (včetně případných licencí do centrální správy) včetně instalace a**	3	klientská licence	96 250,00 Kč	116 462,50 Kč	288 750,00 Kč	60 637,50 Kč	349 387,50 Kč
• **2 ks kontaktní/bezkontaktní čtečky karet (RFID) připojená přes USB,**	3	ks	545,00 Kč	659,45 Kč	1 635,00 Kč	343,35 Kč	1 978,35 Kč
• **Štítek a upevnění nebo zajištění neklouzavé spodní části (např. oboustranná lepenka, přísavka nebo suchý zip)**	3	ks	5,00 Kč	6,05 Kč	15,00 Kč	3,15 Kč	18,15 Kč
Hybridní kontaktní/bezkontaktní čipové karty QSCD včetně potisku dle čl. I., odst. 1 d) návrhu smlouvy včetně záruky a záručního servisu (12 měsíců):	6900	ks	495,00 Kč	598,95 Kč	3 415 500,00 Kč	717 255,00 Kč	4 132 755,00 Kč
Hybridní kontaktní/bezkontaktní čipové karty QSCD bez potisku dle čl. I., odst. 1 e) návrhu smlouvy včetně záruky a záručního servisu (12 měsíců):	1000	ks	445,00 Kč	538,45 Kč	445 000,00 Kč	93 450,00 Kč	538 450,00 Kč
Dodání technické a provozní/administrátorské dokumentace dle čl. I., odst. 1 g) návrhu smlouvy	1	různé	90 000,00 Kč	108 900,00 Kč	90 000,00 Kč	18 900,00 Kč	108 900,00 Kč
Zaškolení administrátorů a pracovníků inicializačních pracovišť objednatele dle čl. I., odst. 1 h) návrhu smlouvy.	1	různé	15 500,00 Kč	18 755,00 Kč	15 500,00 Kč	3 255,00 Kč	18 755,00 Kč
Služby technického specialisty nad rámec předmětu plnění VZ dle čl. I., odst. 1, písm. k) návrhu smlouvy.	50	MD (Man Day)	11 500,00 Kč	13 915,00 Kč	575 000,00 Kč	120 750,00 Kč	695 750,00 Kč
Celková nabídková cena za celý předmět plnění bez DPH *					10 454 200,00 Kč		

*) Hodnotící kritérium dle bodu 18 ZP
**) Množství doplní dodavatel dle nabízeného řešení

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

Obsah

1 Účel a oblast platnosti dokumentu 2
2 Pojmy a zkratky 2
3 Odpovědnosti a pravomoci 2
4 Postup (popis činností) 3
4.1 Procesy externího přístupu 3
4.1.1 Podmínky schvalování 3
4.1.2 Postup zřízení přístupu 3
4.1.3 Zrušení přístupu 4
4.2 Povinnosti, pravidla a restrikce 4
4.2.1 Povinnosti externích uživatelů 4
4.2.2 Požadavky na připojené zařízení 4
4.2.3 Bezpečnostní incident nebo kybernetický útok 4
4.2.4 Zakázané činnosti 5
4.2.5 Monitoring činností 5
4.2.6 Porušení pravidel a povinností 5
4.3 Revize externího připojení 5
5 Závěrečná ustanovení 6
6 Vznikající dokumenty a údaje 6
7 Související dokumenty 6
8 Přílohy 6
Příloha č. 1 – Povinnosti při připojování zařízení do sítě VFN 6
Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN 6
Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku 6

Zpracovatel:	Účinnost dokumentu od:	Schválil:
[redacted]	23. 7. 2020	[redacted]
Garant:	**První vydání dne:**	**Dne:**
[redacted] Vedoucí odboru správy ICT	1. 1. 2008	23. 7. 2020

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POUŽÍVÁNÍ SÍTĚ VFN EXTERNÍMI UŽIVATELI

1 Účel a oblast platnosti dokumentu

Účelem této směrnice je stanovení podmínek pro používání sítě VFN externími uživateli včetně životního cyklu přístupu a povinností, pravidel a restrikcí vztahující se na externí uživatele přistupující do VFN.

2 Pojmy a zkratky

AD	Active Directory
Externí uživatel	Osoba využívající prostředky ICT VFN, která není v pracovně právním poměru k VFN
Garant	Zaměstnanec VFN, který zodpovídá za přístup a práci externího uživatele v síti VFN.
ICT	Informační a komunikační technologie
ISE	Cisco Identity Services Engine
OSICT	Odbor správy ICT
ServiceDesk	Nástroj na zaznamenání, evidenci a sledování stavu incidentů nebo požadavků zaměstnanců VFN a pracovníků externích dodavatelských firem řešených Úsekem informatiky a digitální transformace.
ÚI	Úsek informatiky a digitální transformace
VFN	Všeobecná fakultní nemocnice v Praze
VPN	Virtual Private Network – vzdálený zabezpečený přístup do lokální sítě

3 Odpovědnosti a pravomoci

Garant – zodpovídá za přístup, rozsah oprávnění a práci externího uživatele v síti VFN.

Externí uživatel – externí pracovník, kterému je na základě smluvního vztahu zřízen externí přístup, který je schválen garantem externího přístupu ve VFN (Garant). Výkon práce provádí v souladu se smluvním ujednáním a v souladu s náležitostmi dodržovat povinnosti, pravidla a zákazy uvedené v kap. 4.2.

Pracoviště Dispečinku ÚI (Odbor podpory uživatelů) – zodpovídá za ověření externího uživatele, schválení požadavku Garantem a za zadání požadavku do ServiceDesku.

OSICT – zodpovídá za zpracování a řešení požadavku o VPN přístup.

4 Postup (popis činností)

4.1 PROCESY EXTERNÍHO PŘÍSTUPU

4.1.1 Podmínky schvalování

Externí uživatel musí vyplnit formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN, kde je uveden garant externího přístupu za VFN (dále jen Garant), na jehož základě dojde k ověření identity žadatele a o schválení validity požadovaného přístupu a rozsahu přístupu Garantem. Po splnění těchto podmínek je možné zřízení účtu externího uživatele.

4.1.2 Postup zřízení přístupu

4.1.2.1 Externí uživatel

Detailní postup pro zřízení účtu externího uživatele je uveden v příloze (Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN) a zároveň dostupný na webové stránce https://www.vfn.cz/externista. Pokud je součástí externího přístupu i požadavek o zřízení vzdáleného přístupu je postupováno dle kapitoly 4.1.2.2 (Vzdálený přístup - VPN). Platnost externího účtu je max. 1 rok od zřízení, pokud nebyl zřizován na dobu určitou. Žadatel bude 1 měsíc před expirací upozorněn na kontaktní e-mail uvedený v žádosti, obdobně i Garant bude upozorněn na svůj pracovní mail 1 měsíc před. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

4.1.2.2 Vzdálený přístup - VPN

Externí pracovníci se mohou do sítě VFN připojit pomocí VPN TLS tunelu s multifaktorovou autentizaci. Detailní postup pro žadatele je na stránce https://www.vfn.cz/vpn. O VPN přístup žádá Garant prostřednictvím požadavku do ServiceDesku, kde musí být uvedeno:

- jméno a příjmení externisty,
- účet externisty ve VFN,
- firma,
- telefon,
- e-mail,
- oblast činnosti ve vztahu k VFN,
- na které zařízení (modality, servery) má mít externí uživatel přístup a v jakém rozsahu (IP, porty),
- doba platnosti VPN přístupu, pokud má být na dobu určitou.

Požadavek dále zpracuje pracovník správy sítí OSICT v následujících krocích:

- předá ke schválení vedoucímu OSICT,
- předá na externí firmu Simac, která podle něj nastaví profil v ISE,
- předá na správu serverů OSICT.

Požadavek dále zpracuje pracovník správy serverů OSICT v následujících krocích:

- nastaví profil v AD,
- pošle informace o vytvoření VPN přístupu externímu uživateli,
- ukončí požadavek Garanta v ServiceDesku (čímž dojde k vygenerování a zaslání notifikačního emailu Garantovi).

4.1.3 Zrušení přístupu

Ke zrušení externího účtu nebo VPN přístupu může dojít za následujících podmínek:

- v oprávněných případech, kdy externí uživatel porušil pravidla a povinnosti uvedené v příloze č. 1, Povinnosti při připojování zařízení do sítě VFN,
- pokud je podezření na zavinění bezpečnostního nebo provozního incidentu či byl jakýmkoliv způsobem zapojen do kybernetického útoku na VFN,
- uplynula stanovená doba externího účtu nebo VPN přístupu (výchozí je 1 rok) nebo Garant nepotvrdil prodloužení externího účtu (čímž zanikne i související VPN přístup)
- nebo byl zadán požadavek na zrušení/ukončení externího účtu anebo VPN přístupu,
- požadavek je zpracován pracovníkem OSICT, který odebere členství v odpovídající AD skupině a následně předá na externí firmu Simac, která zruší profil v ISE.

4.2 POVINNOSTI, PRAVIDLA A RESTRIKCE

4.2.1 Povinnosti externích uživatelů

Uživatel v rámci připojení do sítě VFN:

- smí používat připojení pouze k účelům souvisejícím s výkonem smluvní činnosti v takovém rozsahu, který odpovídá potřebám uživatele pro výkon této činnosti,
- je povinen používat své připojení takovým způsobem, který nenaruší funkci sítě, informačních systémů a jejich dat ani práva ostatních uživatelů,
- je povinen chránit svá hesla před vyzrazením a v případě podezření, že heslo zná jiná osoba, heslo musí změnit přes portál http://www.office.com a tuto situaci neprodleně nahlásit jako incident dle bodu 4.2.1.1,
- je povinen zabránit využití či zneužití jeho vzdáleného připojení (VPN) třetí osobou,
- v případě podezření na bezpečnostní incident, nestandardní chování připojení nebo informačních systémů či jakékoliv náznaku na kybernetický útok neprodleně nahlásit toto podezření dle bodu 4.2.1.1,
- je povinen chovat se v souladu s dobrými mravy a právním řádem České republiky.

4.2.1.1 Nahlášení incidentu

V pracovní dny:

- od 7:00 do 16:00 na Dispečink ÚI na tel. [redacted]
- od 16:00 do 7:00 na Pohotovost ÚI na tel. [redacted]

O víkendu a svátcích na Pohotovost ÚI na tel. - [redacted]

4.2.2 Požadavky na připojené zařízení

Požadavky a povinnosti vztahující se na zařízení, které je používáno pro externí nebo VPN přístup, jsou uvedeny v příloze č. 1 (Povinnosti při připojování zařízení do sítě VFN) tohoto dokumentu.

4.2.3 Bezpečnostní incident nebo kybernetický útok

V případě bezpečnostní hrozby nebo kybernetického útoku má VFN právo zrušit povolení přístupu externího uživatele anebo VPN přístupu na dobu nezbytnou k analyzování hrozby nebo útoku a zabránění jakéhokoliv ohrožení sítě, informačních systémů a dat VFN. Pokud externí uživatel vykonává nebo má práva správce nebo

administrátora IS VFN, je povinen konat bezodkladně a zajistit dostatek důkazního materiálu dle povinností uvedených v příloze (Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku).

4.2.4 Zakázané činnosti

Externí uživatel připojený do sítě VFN nesmí:

- v žádném případě poskytovat informace o přístupu, postupech, přístupová hesla, certifikáty, další citlivé informace a ani jejich části třetím osobám,
- umožnit přístup do sítě jiným osobám (např. umožnit přihlášení pod svým jménem),
- se jakýmkoliv způsobem angažovat při rozesílání a distribuci protiprávních, pomlouvačných, hanlivých, reklamních, agitačních a jiných zpráv,
- v žádném případě předávat jakékoli důvěrné informace získané tímto přístupem třetím osobám (osobní údaje, číselníky, databáze, atd.),
- v síti VFN vyhledávat důvěrné nebo jinak citlivé informace, snažit se získat neautorizovaný přístup k souborům a informacím,
- jakýmkoliv způsobem narušit funkci sítě, informačních systémů a dostupnost jejich dat,
- omezit práva uživatelů/správců ICT nebo získat práva nad rámec svých činností a oprávnění,
- v rámci VFN instalovat nebo ukládat jakýkoli neautorizovaný, nelegální nebo škodlivý software.

4.2.5 Monitoring činností

Veškeré činnosti externího připojení do sítě VFN jsou monitorovány a logovány a pravidelně vyhodnocovány architektem kybernetické bezpečnosti nebo jiným pověřeným zaměstnancem ÚI.

4.2.6 Porušení pravidel a povinností

Externímu uživateli, který poruší pravidla, nedodrží povinnosti nebo provádí zakázané činnosti (viz kap. 4.2):

- bude právo přístupu do sítě VFN neprodleně odebráno,
- porušení může být posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Externí uživatel připojený do sítě VFN:

- plně zodpovídá za škody vzniklé v důsledku zneužití jeho přístupu zaviněného nedbalostí, nebo poskytnutím přístupu do sítě VFN třetí osobě,
- je plně zodpovědný za obsah svého datového prostoru.

4.3 REVIZE EXTERNÍHO PŘIPOJENÍ

Za oprávněnost, platnost a rozsah externího připojení odpovídá Garant, který v případě jakékoliv změny (zrušení, odebrání/přidání práv, apod.) zadá tuto změnu formou požadavku do ServiceDesku.

V rámci kontrolních mechanizmů je minimálně 1x ročně prováděna kontrola povolených externích uživatelů a připojení VPN v rámci pravidelných auditů KB prováděné auditorem KB nebo jiným pověřeným subjektem.

5 Závěrečná ustanovení

Tato směrnice je závazná pro všechny výše uvedené zaměstnance a externí subjekty v kap. 3 Odpovědnosti a pravomoci.

Porušení této směrnice bude posuzováno jako závažné porušení povinností vyplývajících z právních předpisů a smluvního vztahu vztahujících se k externímu uživateli vykonávané práci a jednání v rozporu se zájmy VFN a uzavřeného smluvního vztahu.

Tato směrnice podléhá revizi nejméně jednou ročně. Za provedení revize dokumentu odpovídá zpracovatel této směrnice.

6 Vznikající dokumenty a údaje

Název	Uchovává	Doba uchování

7 Související dokumenty

RD-VFN-11 Řád používání informačních systémů

F-VFN-463 Formulář: Žádost o zřízení přístupu externího uživatele do sítě VFN

8 Přílohy

Příloha č. 1 – Povinnosti při připojování zařízení do sítě VFN

Příloha č. 2 – Postup zřízení přístupu externímu uživateli do počítačové sítě VFN

Příloha č. 3 – Povinnost administrátora v případě bezpečnostního incidentu nebo kybernetického útoku

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POVINNOSTI PŘI PŘIPOJOVÁNÍ ZAŘÍZENÍ DO SÍTĚ VFN

Povinnosti při připojování zařízení do sítě VFN:

1) Připojení každého zařízení do LAN sítě VFN musí být předem konzultováno s Odborem správy ICT Úsekem informatiky a digitální transformace (dále jen ÚI) VFN.
2) Instalace a provozování jakéhokoli software v síti VFN musí být předem konzultováno s Odborem vývoje a správy SW ÚI VFN.
3) Je zakázáno svévolně zapojovat zařízení do LAN sítě a jakkoli měnit LAN síť VFN.
4) Je zakázáno měnit, instalovat a nahrávat jakýkoli softwarový obsah na zařízení VFN.
5) Je zakázáno jakýmkoli způsobem měnit a zasahovat do hardware vybavení VFN.
6) Je zakázáno využívat pro vzdálený přístup na připojovaná zařízení jiných než ÚI VFN schválených metod - viz níže.
7) Při umisťování IT zařízení (server, PC) do sítě VFN je vlastník IT zařízení povinen na své náklady, pokud není ve smlouvě uvedeno jinak, udržovat toto zařízení:
   a. v aktuálním (aktualizace operačního systému, aktualizace antivirového programu)
   b. v bezpečném (nemožnost jednoduše zneužít, používání silných přístupových hesel...) stavu.

   ÚI provádí náhodné testy zneužitelnosti zařízení. V případě zjištění hrozeb nebo nedostatků je vlastník IT zařízení povinen na své náklady zjištěné hrozby a nedostatky neprodleně odstranit.
8) Vlastník IT zařízení je povinen, na vyžádání ÚI, předložit ke kontrole konfiguraci IT zařízení. V situaci, kdy připojené zařízení způsobuje jakékoliv bezpečnostní anebo technické problémy v síti VFN, má VFN možnost takovéto zařízení bez předchozího upozornění odpojit od sítě VFN a externí účet (včetně VPN připojení) zablokovat nebo i zrušit.

Případné dotazy, požadavky nebo problémy je možné řešit na:

- od 7:00 do 16:00 Dispečink ÚI na tel. [redacted]

Metoda vzdáleného přístupu

K připojovaným zařízením je možné, pokud tomu nebrání další důvody, zřídit vzdálený přístup typu VPN připojení (IPSec tunel nebo jeho obdoba). Je nutná instalace Cisco VPN klienta.

Info: https://www.vfn.cz/vpn nebo Pohotovosti ÚI: [redacted] (mimo pracovní hodiny Dispečinku ÚI).

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POSTUP ZŘÍZENÍ PŘÍSTUPU EXTERNÍMU UŽIVATELI DO POČÍTAČOVÉ SÍTĚ VFN

Postup

Postup žádosti o povolení přístupu do počítačové sítě VFN:

- Žadatel si stáhne, vytiskne a vyplní formulář F-VFN-463.
- Žadatel se dostaví s vyplněným a NEPODEPSANÝM formulářem na Dispečink Úseku informatiky a digitální transformace (dále jen Dispečink ÚI) ve VFN (Budova ředitelství A5, pracovní dny 7:00 – 16:00).
- Pracovník Dispečinku ÚI ověří identitu žadatele (OP, pas). Žadatel podepíše formulář.
- Pracovník Dispečinku ÚI zašle na uvedeného Garanta e-mail s žádostí o schválení validity požadovaného přístupu a rozsahu přístupu. V případě požadavku na VPN připojení, je Garant upozorněn.
- Po obdržení potvrzení od Garanta bude vytvořen přístupový účet externího uživatele a případně VPN přístup.
- Žadatel bude o schválení a zřízení přístupového účtu informován e-mailem.
- Žadatel se dostaví na Dispečink ÚI a vyzvedne si uživatelské jméno a heslo. Heslo je doporučeno si na místě změnit.
- Expirace přístupového účtu je max. po 1 roce od zřízení. Žadatel i Garant bude 1 měsíc před expirací upozorněn na zadaný e-mail. O prodloužení přístupového účtu žádá Garant e-mailem – jako odpověď na e-mail s upozorněním na expiraci.

Upozornění: *Přístup do počítačové sítě VFN se nezřizuje na počkání!*

Povinnosti, pravidla a omezení

Po dobu platnosti účtu externího uživatele je externí uživatel povinen dodržovat následující:

- stanovené povinnosti, pravidla a případné restrikce v kap. 4.2 Řádu používání sítě VFN externími uživateli (SM-UI-02),
- při používání VPN přístupu:
  - stanovené povinnosti pro připojování zařízení do sítě VFN definované v příloze č. 1 (SM-UI-02),
  - návody a postupy pro VPN připojení do sítě VFN uvedené na webových stránkách https://www.vfn.cz/vpn,
- aktuální informace uvedená na webových stránkách https://www.vfn.cz/externista.

Dokumenty ke stažení

- Formulář F-VFN-463 Žádost o zřízení přístupu externího uživatele do sítě VFN
- Řád používání sítě VFN externími uživateli (SM-UI-02)

Kontakt

Dispečink ÚI

- Všeobecná fakultní nemocnice v Praze, U Nemocnice 499/2, 128 08 Praha 2
- Telefon: [redacted]
- E-mail: [redacted]

VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | www.vfn.cz, http://intranet.vfn.cz

POVINNOST ADMINISTRÁTORA V PŘÍPADĚ BEZPEČNOSTNÍHO INCIDENTU NEBO KYBERNETICKÉHO ÚTOKU

Povinnosti administrátora

V případě podezření či probíhajícím bezpečnostním incidentu nebo kybernetickém útoku je povinností správce nebo administrátora konat bezodkladně a zajistit dostatek důkazního materiálu:

- k identifikaci zdroje nebo příčiny,
- k čemu došlo nebo jak se projevuje,
- důsledkům a možným dopadům,

u tohoto incidentu či útoku je vždy povinen:

- zajistit kopie logů nebo transakčních záznamů, pokud by to nezpůsobilo jejich poškození nebo smazání,
- iniciovat nebo pozastavit šíření či poškození, zamezit incidentu nebo útoku,
- nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení VFN, Policie ČR nebo NÚKIB,
- nahlásit toto podezření neodkladně na Pohotovost ÚI jako bezpečnostní nebo kybernetický incident:
  - v pracovní dny:
    - od 7:00 do 16:00 na Dispečink ÚI na tel. [redacted]
    - od 16:00 do 7:00 na Pohotovost ÚI na tel. [redacted]
  - o víkendu a svátcích na Pohotovost ÚI na tel. [redacted]