Technická specifikace pro veřejnou zakázku „*Kybernetická bezpečnost ZZS MSK – Multifaktorová autentizace*“ - dodávka prostředí pro multifaktorovou autentizaci a elektronické podepisování

**Zpracoval:** Mgr. Petr Koběrský

**Verze:** 1.0

**K datu:** 31.1.2025

Obsah

[1. Účel veřejné zakázky 3](#_Toc197428788)

[2. Požadované komponenty a funkce systému 4](#_Toc197428789)

[Multifaktorová autentifikace a elektronický podpis za pomocí čipové karty 4](#_Toc197428790)

[Multifaktorová autentizace mobilním telefonem 6](#_Toc197428791)

[Vzdálené elektronické podepisování 7](#_Toc197428792)

[3. Požadované způsoby integrace a autentizace uživatelů jednotlivých IS zadavetele 9](#_Toc197428793)

[4. Povinné součásti dodávky 9](#_Toc197428794)

[5. Běh aplikací, záruka, podpora a služby 10](#_Toc197428795)

## Účel veřejné zakázky

Implementací více faktorové autentizace v prostředí ZZS MSK (dále jen Zadavatel) dojde k naplnění legislativních požadavků uvedených v  § 19 odst. 3 Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), v rozsahu: „Povinná osoba pro ověření identity uživatelů, administrátorů a aplikací využívá autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na více faktorové autentizaci s nejméně dvěma různými typy faktorů“.

Implementace subsystému vícefaktorové autentizace v rozsahu bezheslového přihlašování umožní personálu bezpečné čtení, zápis a změnu dat pod svojí identitou, kdy v rámci implementace souboru technických opatření, bude možné jednoznačně dohledat činnosti jednotlivých identit, jejich jednoznačnou identifikaci v informačních systémech a systémech fyzické bezpečnosti. Systém umožňuje bezpečné přihlašování a odhlašování do/z pracovní stanice a systému. Umožňuje práci na stanici více uživatelům, za dodržení všech bezpečnostních politik.

Uživatelský komfort bude zabezpečen integrací jednotlivých subsystémů do jednoho pracovního nosiče/média, který bude předáván uživateli do užívání při nástupu do zaměstnání, spolu s využitím mobilní aplikace na mobilních telefonech, které budou tvořit záložní řešení a primární řešení pro oblast autentifikace v rámci mobilního zpracování dat.

Systém musí umožnit centrální správu, integraci se zdroji dat jako je identity management (IDM) a adresářová služba Active Directory (AD). Systém musí splňovat požadavky na vysokou dostupnost, centrální správu a reporting. Systém musí být integrován formou rozhraní na dále specifikované systémy a subsystémy. V interních a externích informačních systémech, zajistí integrační platformu a rozhraní, tak aby bylo možné pro všechny procesy bezpečných přístupů a podepisování využívat jednotnou platformu.

Systém bude vyvíjen jako ostrovní systém (on premise) který se instaluje a provozuje přímo na počítačích daného zdravotnického zařízení nebo uživatele. Celý software má tak zdravotnické zařízení „u sebe“ – na vlastním serveru a pracovních stanicích. Ověření mobilním telefonem, které bude provozováno na mobilních zařízeních mimo vnitřní síť a také jako záložní řešení k autentizaci čipovou kartou, může být poskytováno jako cloudová služba.

Pro zajištění rychlé distribuce nových verzí systému musí řešení obsahovat možnost „autoupdate služby“ všech komponent (včetně mobilních aplikací), která zajistí okamžitou automatickou distribuci patchů, hotfixů, aktualizací systému apod. Dodavatel musí neprodleně řešit zranitelnosti CVSS 7 a výše jako vadu systému a zajistit neprodlené odstranění těchto zranitelností pomocí hotfixů a aktualizací.

## Požadované komponenty a funkce systému

Systém musí obsahovat tyto požadované součásti a funkcionality.

Autentizační metody:

* bezheslové přihlašování (passwordless) pomocí FIDO čipů,
* přihlášení certifikátem uloženým na čipové kartě,
* OTP (jednorázová hesla) pro záložní přístup,
* Biometrické ověřování nebo PIN prostřednictvím mobilní aplikace.

Flexibilní konfigurace autentizačních faktorů 1FA, 2FA nebo MFA podle úrovně bezpečnosti a typu přístupu.

Podpora různých prostředí:

* přístup do PC, VPN, Remote Desktop, webových aplikací a dalších systémů,
* možnost připojení libovolné karty s rozhraním ISO/IEC 7816 (ePZP, kvalifikované certifikáty),
* kompatibilita s Microsoft, Apple, Linux, Android.

### Multifaktorová autentifikace a elektronický podpis za pomocí čipové karty

Umožní multifaktorovou autentizaci a vytváření kvalifikovaného elektronického podpisu podle nařízení eIDAS pomocí kryptografických klíčů bezpečně chráněných v hardwarovém prostředku – hybridní čipové kartě.

* Bude dodáno 1400ks kusů QSCD hybridních čipových karet ve formátu maximálně ID-1 (velikost bankovní karty). Kontaktní čipy a aplikace nahraná do kontaktního čipu umožňuje správu kryptografických klíčů určených k vytváření kvalifikovaného elektronického podpisu.
* Bude dodáno 350ks bezdrátových čteček kompatibilních se specifikovanými kartami. Karty musí být připojeny přes UBC (preferován port USB-C) a kompatibilní s Windows 10 a novějšími a aktuální verzí MacOS.
* Součástí dodávky bude SW aplikace pro správu hybridních čipových karet a certifikátů s licencí na dobu neurčitou pro 1400 uživatelů.

Certifikované karty musí být v souladu:

* s normou ČSN EN ISO 7816, část 1-4,
* standardem EN 419 211 a profily:
  + BSI-CC-PP-0059,
  + BSI-CC-PP-0075,
  + BSI-CC-PP-0071,
  + BSI-CC-PP-0072,
  + BSI-CC-PP-0076,
* bezkontaktní čip musí splňovat minimálně standardy - bezkontaktní FIDO, bezkontaktní NXP, Mifare Desfire EV1 8Kb,
* karta musí být dále kompatibilní s přístupovým systémem postaveným na technologii „iCLASS Seos“.

Vlastnosti kontaktního čipu a PKI aplikace:

* všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty,
* 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,
* klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány,
* generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12,
* archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů.

Podporované jsou minimálně kryptografické algoritmy:

* symetrické: AES 256 a vyšší
* hash: SHA-256, SHA-384, SHA-512 a vyšší
* RSA: 3072 bitů a vyšší,
* eliptické křivky: P-384 a vyšší

Dále je požadováno:

* 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,
* zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů),
* dvoufaktorová autentizace na bázi certifikátů X.509 (do PC v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.)

Vytváření elektronického podpisu na bázi certifikátů ve formě:

* kvalifikovaného elektronického podpisu,
* zaručeného elektronického podpisu,
* uznávaného elektronického podpisu a jiné formy elektronického podpisu.

Hybridní čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů. Čipové karty budou dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému.

Vlastnosti ovládacího software:

* + podléhá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší,
  + podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11,
  + použití na OS MS Windows 10 nebo vyšších verzích,
  + použití na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11),
  + podpora obslužné a bezobslužné instalace na Windows, RPM, DEB.

Stav dodané karty:

* inicializovaná PKI aplikace s PIN, QPIN a PUK,
* předání seznamu personalizovaných karet, pro import do evidence CMS. 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.

Požadavky na aplikace pro správu a podporu čipových karet a certifikátů:

* automatizovaná instalace a obnova kvalifikovaných i komerčních certifikátů od externího poskytovatele (min. pro 3 externí autority), instalace a automatizovaná obnova interních certifikátů z doménové CA,
* implementace aplikace, které prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu,
* implementace webové aplikace, určené správcům certifikátů. Možnost vyhledávat a prohlížet informace o certifikátech, odvolávat certifikáty, generovat a prohlížet reporty,
* pro onboarding FIDO2 metody autentizace se využije standardních nástrojů AAD od společnosti Microsoft nebo dodané externí aplikace.

### Multifaktorová autentizace mobilním telefonem

Cílem je použití bezpečné a moderní metody multifaktorové autentizace pomocí mobilního telefonu, kde zaměstnanec další faktor autentizace potvrzuje v autentizační aplikaci. Použití multifaktorové autentizace mobilním telefonem, která bude co nejlépe vyhovovat a zapadat do podmínek, požadavků a scénářů vzešlých z analýzy v rámci implementace.

Povinné technické vlastnosti pro řešení MFA prostřednictvím mobilní aplikace:

* řešení musí být připraveno pro použití jako cloudová služba a onpremise řešení,
* řešení musí podporovat tyto scénáře multifaktorové autentizace pomocí mobilního telefonu:
  + autentizace bez použití hesla (passwordless) do operačního systému MS Windows s použitím certifikátu uživatele,
  + autentizace bez použití hesla (passwordless) do VPN s použitím certifikátu uživatele pomocí PKI,
  + autentizace do interních webových aplikací prostřednictvím standardizovaných autentizačních protokolů OIDC, SAML2.0, OAuth2,
  + autentizace do aplikací prostřednictvím standardizovaného protokolu RADIUS,
  + zaručený elektronický podpis a autorizaci uživatele před podpisem - podpisový certifikát je vydán doménovou certifikační autoritou.
* součástí dodávky musí být autorizační server, kdy autorizace musí probíhat prostřednictvím aplikace v mobilním telefonu,
* povinné metody autorizačního serveru a mobilní aplikace musí být push notifikace, jednorázové heslo OTP nebo SMS,
* řešení musí podporovat metodu dynamického anonymního QR kódu, to znamená uživatel nemusí zadávat uživatelské jméno a naskenuje QR kód (měnící se v čase),
* řešení musí podporovat jako metodu autentizace také HW zařízení (smartkarta s certifikátem),
* řešení musí podporovat minimálně tyto identitní systémy: MS Entra, onpremise AD, Google Cloud Identity Platform,
* řešení musí obsahovat REST API rozhraní pro integraci s ostatními identitními systémy,
* řešení musí mít k dispozici REST rozhraní pro přímou integraci aplikací Zadavatele s autorizačním server pro scénář autorizace/autentizace,
* řešení musí umožnit přizpůsobení obsahu autentizační/autorizační transakce,
* řešení musí umožnit úpravy autentizační login stránky dle firemní identity Zadavatele,
* dostupnost mobilní aplikace musí být pro koncové zařízení iOS, Android,
* mobilní aplikace musí podporovat multitenantní použití,
* mobilní aplikace musí při autentizaci podporovat biometriky - otisk prstu (fingerprint), rozpoznání obličeje (face ID),
* aplikace musí monitorovat podezřelé chování, potencionální nebezpečí a stav mobilního zařízení: Integrita systému, Integrita aplikace, Instalace z důvěryhodného zdroje, Runtime manipulace, Detekce překrytí obrazovky, Zámek zařízení, Zabezpečení biometrikou, Root operačního systému,
* informace z podezřelého chování v rámci mobilního telefonu musí být zobrazeny v náhledu pro administrátora - administrátorská konzole,
* aplikace musí umožnit použití autorizačního SDK pro další mobilní aplikace,
* aktivace mobilní aplikace s identitou uživatele musí být pomocí QR kódu,
* řešení musí umožnit použití více mobilních telefonů pro jednoho uživatele stejně jako využití jednoho mobilního telefonu pro více uživatelů (použití posádkových mobilních telefonů bez nutnosti individuálního zavádění uživatelů do každého telefonu),
* jazyk aplikace minimálně český a anglický s možností přepnutí uživatelem.

### Vzdálené elektronické podepisování

Dodavatel dodá řešení pro kvalifikovaný elektronický podpis a kvalifikovanou elektronickou pečeť na dálku dle nařízení eIDAS.

Cílem je ulehčit svým zaměstnancům práci s kvalifikovanými certifikáty bez nutnosti vazby na fyzický nosič a kvalifikovaně podepsat odkudkoliv ze svého vlastního mobilního zařízení (smartphone, tablet), počítače a stávajících aplikací (např. Zdravotnická dokumentace ZZS, Spisová služba apod.) Dodavatel musí zajistit, aby při dodržení všech bezpečnostních opatření nemohlo dojít ke zneužití certifikátu.

**Povinné technické vlastnosti**

* součástí dodávky musí být certifikovaný SAM dle ČSN EN 419 241-2, který je uveden na QSCD seznamu vedeném EU,
* API rozhraní pro vytváření elektronického podpisu na dálku musí splňovat standard ETSI TS 119 432,
* součástí dodávky musí být HSM moduly, které splňují QSCD certifikaci a jsou uvedeny na EU trust listu nebo obdobné softwarové certifikované řešení se stejnou úrovní zabezpečení jako HSM moduly - redundantní provedení minimálně složeno ze dvou nodů (virtuálních nebo fyzických),
* požadován výkon minimálně 5 vydávaných podpisů/pečetí za sekundu,
* podporované formáty kvalifikovaného elektronického podpisu a elektronické pečeti musí být minimálně tyto: PAdES-B-B, PAdES-B-T, XAdES-B-B, XAdES-B-T, CAdES-B-B, CAdES-B-T, ASiC-S,
* dodavatel musí v rámci plnění předložit certifikát úspěšně absolvovaných ETSI plug-testů   
  pro formáty PAdES, XAdES, CAdES,
* řešení musí umožnit podpis více souborů jedním požadavkem,
* řešení musí podporovat režim podpisu kvalifikovaným dlouhodobým i krátkodobým (“jednorázovým”) certifikátem,
* řešení musí zajistit, že pro jednu identitu uživatele lze použít více certifikátů se stejným nebo obecně jiným účelem,
* dodavatel musí být schopen propojit řešení s Poskytovatelem služeb vytvářejícím důvěru (TSP) pro vydávání kvalifikovaných certifikátů pro elektronický podpis, resp. elektronickou pečeť vybraným Zadavatelem,
* řešení musí zajistit, aby byla vedena auditní stopa vykonávaných operací a změn konfigurace a ta musí být odesílána definovaným protokolem do systému log managementu,
* řešení musí podporovat škálovatelnost a vysokou dostupnost (HA),
* řešení musí podporovat architekturu - HW server pro SAM modul a samostatný HSM nebo obdobné certifikované SW řešení,
* řešení musí obsahovat přehled změn provedených v nastavení služby vytváření elektronických podpisů/pečetí na dálku a odesílání definovaným protokolem do systému log managementu,
* řešení musí zajistit přehled prováděných podpisových operací a jejich výsledek,
* řešení musí zobrazit přehled operací souvisejících s životním cyklem certifikátu – generování klíčů, vydání a obnova certifikátu,
* řešení musí mít přehled stavu jednotlivých komponent – např. HSM, SAM, API, GUI,
* řešení musí zajistit auditní logy pro systémy typu SIEM a log management,
* řešení musí umožnit aktivaci různých typů notifikací v souvislosti s životním cyklem certifikátů,
* součástí dodávky musí být autorizační server pro autorizaci samotného elektronického podpisu - povinná požadavky na autorizační server vycházejí ze stejných požadavků jako u MFA mobilním telefonem (popsáno výše).

## Požadované způsoby integrace a autentizace uživatelů jednotlivých IS zadavatele

* Přihlášení k AD účtu stacionárního PC, VPN, RDP atp.:
  + bezheslové přihlášení bezdrátovou hybridní kartou,
  + alternativní multifaktorová autentizace mobilním telefonem.
* Personální systém Vema:
  + integrované ověření v rámci AD.
* Ekonomický systém Gordic:
  + integrované ověření v rámci AD.
* Systém zdravotnické dokumentace
  + Mobilní zadávání dat:
    - multifaktorová autentizace mobilním telefonem posádky,
    - vzdálené elektronické podepisování pomocí integrace aplikace mobilního zadávání dat ZD.
  + Stacionární webová aplikace:
    - integrované ověření v rámci AD pro přístup z PC v rámci interních sítí,
    - vzdálené elektronické podepisování,
    - bezheslové ověření pomocí hybridní karty,
    - multifaktorová autentizace mobilním telefonem pro přístup z PC mimo doménu (přístup přes VPN, z tabletů posádek apod.).
* Intranetová webová aplikace, webmail apod.
  + přístup ze stacionárních PC v rámci AD pomocí integrace s AD (pokud je podporováno),
  + bezheslové ověření pomocí hybridní karty,
  + alternativně multifaktorové ověření mobilním telefonem.

## Povinné součásti dodávky

Součástí plnění bude zejména:

* Provedení vstupní analýzy
* Vypracování realizačního projektu
* Dodávka a implementace jednotlivých systémů a subsystémů
* Integrace MFA do prostředí zadavatele (včetně dodání dokumentace pro integraci jednotlivých systémů zadavatele)
* Dodávka bezpečnostní dokumentace
* Provedení školení správců systémů
* Předání a akceptace díla
* Zajištění testovacího provozu

Součástí vstupní analýzy bude vypracování návrhu harmonogramu jednotlivých částí, který bude po schválení Zadavatelem zanesen do realizačního projektu.

## Běh aplikací, záruka, podpora a služby

Součástí dodávky bude tříletá záruka na všechna dodaná zařízení a aplikace. Další záruka na HW komponenty bude volitelně řešena Zadavatelem po ukončení záruky.

Aplikace mohou být provozovány v prostředí virtualizace Zadavatele, které je provozováno na platformě Hyper-V, kdy Zadavatel poskytne potřebný počet licencí Windows Server 2022. Pokud je pro běh potřebný jiný operační systém, musí být licence těchto OS součástí dodávky.

Část z dodávky „Multifaktorové autentizace mobilním telefonem“ může dodavatel nabídnout jako službu s provozem v cloudu, za předpokladu, že bude dodržena dostupnost 99,8% v rámci měsíce a nedostupnost služby nebude mít žádný vliv na ostatní služby (zejména MFA pomocí čipových karet). Zodpovědnost za běh aplikací v rámci cloudu, včetně zajištění bezpečnosti běhu přechází na poskytovatele včetně všech případných důsledků. Případné nedodržení dostupnosti bude považováno za porušení sjednané podpory dle smlouvy. Cena provozu v rámci cloudu a poskytování aplikací běžících v cloudu musí být součástí ceny za podporu.

Licence on premise řešení musí být trvalé, tedy nemůže jít o licence, které trvají jen po dobu předplatného nebo podpory. Licence části „Multifaktorové autentizace mobilním telefonem“, pokud budou provozovány jako služba v cloudu, jsou plně na zajištění dodavatelem, tedy po případném ukončení smlouvy a poskytování služeb se nepředpokládá přechod těchto licencí na zadavatele.

V rámci nabídky podpory bude nabídnuta podpora dodaných systémů, a to na dobu neurčitou (s kalkulací ceny na 4 roky pro účely hodnocení nabídek v rámci zadávacího řízení na veřejnou zakázku) s následujícími parametry, podle priority incidentů:

**A – Urgentní**: IS na který je dodavatel povinen poskytovat podporu nebo jeho část je zcela nefunkční, neumožňuje práci uživatelů se systémem (ani alternativní cestou nebo vyřadit), nebo došlo k závažnému bezpečnostnímu incidentu (napadení a prolomení systému).

**B – Závažné**: IS na který je dodavatel povinen poskytovat podporu nebo jeho část je částečně nefunkční, umožňuje částečné poskytování služeb, po přechodnou dobu se sníženým uživatelským komfortem nebo neumožňuje zcela práci minoritní aktuálně zastupitelné části uživatelů, nebo došlo k méně závažnému bezpečnostnímu incidentu (pokus o napadení bez prolomení systému s omezením funkčnosti).

**C – Ostatní**: jakákoliv chyba malého rozsahu nespadající do výše dvou uvedených priorit A, B – nebrání neodkladně užívání IS nebo jeho části, ale nejsou v souladu se stavem předání nebo legislativním rámcem a méně významné bezpečnostní incidenty (prověření bezpečnostního incidentu při podezření o napadení bez vlivu na funkčnost)

**Doba reakce** – doba, která uplyne od přijetí incidentu poskytovatelem služby do potvrzení doby zahájení řešení incidentu poskytovatelem.

**Doba na překlenutí vady** – doba, která uplyne od přijetí incidentu poskytovatelem služby do poskytnutí dočasného řešení zmírňujícího dopady incidentu, tedy do zprovoznění do stavu, kdy je odstraněna akutní nefunkčnost (např. obnoven běh IS restartem služby nebo zařízení, provedením dočasného downgrade nebo přechod na nižší stupeň autentizace, dočasné vyřazení chybující části/služby apod.) a pracuje se na finálním odstranění vady.

**Doba vyřešení incidentu a předání objednateli k ověření vyřešení** – doba, která uplyne od přijetí incidentu po předání řešení k ověření. Doba potřebná na ověření vyřešení ze strany objednatele není započítávána do doby vyřešení. Vyřešením je chápáno i snížení úrovně incidentu v daném čase a tím prodloužení doby pro řešení v souladu s nižší úrovní incidentu.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Priorita A** | **Priorita B** | **Priorita C** |
| **Doba reakce** | 1 hod. | 8 hod. | NBD\* |
| **Doba na překlenutí vady** | 4 hod. | 24 hod. | 48 hod. od reakce |
| **Doba vyřešení** | 48 hod. | 72 hod. | 5 dní od reakce |

\* Nejbližší pracovní den

Za účelem uplatnění podpory poskytne dodavatele Zadavateli přístup k lince podpory (hotline) a dále do helpdesku, kde bude prováděna správa a kontrola způsobu řešení incidentů. Za nahlášení vady se považuje čas ohlášení na linku podpory a následným zanesením do systému helpdesku dodavatele.