



Požadavky na systém řízení životního cyklu certifikátů, nosičů certifikátů a obslužný software

Příloha č. 3 zadávací dokumentace pro zadávací řízení „Nasazení MFA a pořízení nosičů certifikátů“

1. Obsah

[1 Úvod 3](#_Toc207718627)

[2 Požadavky na systém řízení životního cyklu certifikátů 3](#_Toc207718628)

[3 Požadavky na systém správy životního cyklu nosičů certifikátů 4](#_Toc207718629)

[4 Požadavky na obslužný software a middleware pracovních stanic 5](#_Toc207718630)

[4.1 Ovladače pro nosiče certifikátů 6](#_Toc207718631)

[4.2 Obslužný software pro správu certifikátů a jejich nosičů 6](#_Toc207718632)

[4.3 Software pro obnovu uživatelských certifikátů 7](#_Toc207718633)

[4.4 Obecné požadavky na obslužný software a middleware pracovních stanic 7](#_Toc207718634)

# Úvod

Tato příloha zadávací dokumentace stanovuje požadavky na

* Systém řízení životního cyklu certifikátů
* Systém řízení životního cyklu nosičů certifikátů
* Obslužný software a middleware pracovních stanic

Zadavatel připouští možnost neimplementovat uvedené části jako samostatné systémy a připouští jejich sdružení do jednoho nebo více systémů, přičemž výsledné řešení musí splňovat všechny požadované vlastnosti.

# Požadavky na systém řízení životního cyklu certifikátů

Systém správy životního cyklu certifikátů musí splňovat zejména požadavky uvedené v následující tabulce:

|  |  |  |
| --- | --- | --- |
| ID | Požadavek, vlastnost | Požadováno |
| S.1 | Podpora automatizace procesů správy životního cyklu uživatelských certifikátů: vystavení nového certifikátu, vystavení následného certifikátu, zneplatnění kompromitovaných/expirovaných certifikátů apod. | Ano |
| S.2 | Propojenost (integrace) systému se systémem správy životního cyklu nosičů certifikátů (zejména evidence čísel kontaktních i bezkontaktních čipů nosičů certifikátů, stav nosiče apod.) | Ano |
| S.3 | Evidence informací o vydaných certifikátech pro každého uživatele, jejich aktuálním stavu a kompletní historie. | Ano |
| S.4 | Identity držitelů certifikátů musí být navázány na objekty jednoznačné identifikace držitele (uživatele), např. účet v AD, identifikační číslo identity v personálním systému nebo systému typu IDM apod. Konkrétní vazba na jednoznačnou identifikaci bude stanovena v předimplementační analýze. | Ano |
| S.5 | Archivace privátních klíčů v procesu vydávání šifrovacích certifikátů. Privátní klíče šifrovacích certifikátů musí být uloženy (archivovány) v bezpečném hardware (HSM). | Ano |
| S.6 | Podpora vydání certifikátu v zastoupení[[1]](#footnote-2) |  |
| S.7 | Rozšířené operace s certifikáty:   * export certifikátu do souboru (bez exportu privátního klíče certifikátu) * import certifikátu ze souboru standardu PKCS#12 (včetně privátního klíče), smazání importovaných certifikátů |  |
| S.8 | Podpora procesů řešení nestandardních stavů (včetně podporu jejich automatizace), zejména: zapomenutí nosiče certifikátu, ztráta nosiče certifikátu, zničení nosiče certifikátů, zablokování přístupových kódů, kompromitace přístupových kódů, odebrání nosiče certifikátů nebo jednotlivých certifikátů apod.). Návrh procesů a scénářů řešení nestandardních stavů budou výstupem předimplementační analýzy. | Ano |
| S.9 | Podpora schvalovacích procesů a segregace rolí správy certifikátů a jejich nosičů (návrh procesů a segregace rolí je součástí předimplementační analýzy) | Ano |
| S.10 | Notifikace uživatelů o změnách stavů certifikátů a blížící se expiraci vydaných certifikátů včetně instrukcí pro jejich obnovu (vydání následného certifikátu) a opakovaných notifikací | Ano |
| S.11 | Uživatelské rozhraní systému správy životního cyklu certifikátů musí být v českém jazyce, grafické a intuitivní pro obsluhu. | Ano |
| S.12 | Podpora příjmu a evidence informací o změnách dat na nosiči certifikátů zasílaných ovladači nosičů nebo obslužným software (příjem může být zajištěn i systémem správy životního cyklu nosičů certifikátů). |  |

Systém správy životního cyklu certifikátů musí být propojen (integrován) se systémem správy životního cyklu nosičů certifikátů na datové nebo aplikační úrovni, popř. může být implementován jako jeden (modulární) systém a může být zcela nebo zčásti implementován jako webová aplikace.

Prostřednictvím online záznamu změn je v centrální evidenci aktualizován stav certifikátů, uložených na všech nosičích ve správě Zadavatele.

# Požadavky na systém správy životního cyklu nosičů certifikátů

Systém správy životního cyklu nosičů certifikátů musí splňovat zejména požadavky uvedené v následující tabulce:

|  |  |  |
| --- | --- | --- |
| ID | Požadavek, vlastnost | Požadováno |
| S.13 | Centrální evidence a správa životního cyklu nosičů certifikátů a podpory souvisejících procesů včetně vysoké míry automatizace.  Evidence musí obsahovat kompletní informace o nosiči a jeho stavu, zejména:   * typ a druh nosiče, * identifikátory kontaktních a bezkontaktních čipů, * informace o uživatelích (držiteli) nosiče (včetně časových intervalů držitelů nosiče) * stavu nosiče (stav jeho přípravy, stav předání uživateli, stav předání přístupových kódů, nestandardní stavy apod.)   včetně kompletní historie. | Ano |
| S.14 | Systém správy životního cyklu musí být propojen (integrován) se systémem správy certifikátů a evidovat informace o uložených certifikátech a dalších datech na nosiči uložených a zaplněnosti paměťového prostoru nosiče. | Ano |
| S.15 | Systém musí zajistit přípravu nosiče certifikátů bezpečným způsobem, tzn. tak, aby správce neznal přístupové kódy spravovaných nosičů. |  |
| S.16 | Evidence aktualizací systémů využívající nosič certifikátu k identifikaci uživatele, včetně úplné historie | Ano |
| S.17 | Příprava dat pro personalizaci karet a podpora jejich automatizovaného odesílání na personalizační pracoviště a získání informací o stavu přípravy. | Ano |
| S.18 | Evidence stavu přípravy nosiče (sklad, personalizační pracoviště, doprava, předání apod.), stavu přístupových kódů (PIN, PUK), jejich bezpečného tisku a stavu distribuce uživateli, včetně historie. | Ano |
| S.19 | Systém správy nosičů musí podporovat vyhledávání v evidenci, včetně příslušných filtrů a zobrazovat/filtrovat uložené informace, zejména   * informace o typu nosiče a identifikátorech čipů * informace o certifikátech v čipu, podrobnosti o každém certifikátu * seznam kryptografických klíčů v čipu * zaplnění paměťového prostoru nosiče * zjistit a zobrazit stav přístupových kódů (PIN/PUK) * nastavit, odblokovat či změnit některý z přístupových kódů (PIN/PUK) * zobrazit log problematických technických stavů (nesprávné funkce čtečky nosiče, čipu, certifikátů apod.). | Ano |
| S.20 | Uživatelské rozhraní systému správy životního cyklu nosičů certifikátů musí být v českém jazyce, grafické a intuitivní pro obsluhu. | Ano |
| S.21 | Podpora příjmu a evidence informací o změnách dat na nosiči certifikátů zasílaných ovladači nosičů nebo obslužným software (příjem může být zajištěn i systémem správy životního cyklu certifikátů). |  |

Systém správy životního cyklu nosičů certifikátů musí být propojen (integrován) se systémem správy životního cyklu certifikátů na datové nebo aplikační úrovni, popř. může být implementován jako jeden (modulární) systém a může být zcela nebo zčásti implementován jako webová aplikace.

# Požadavky na obslužný software a middleware pracovních stanic

Pro integraci nosičů certifikátů s operačními systémy koncových stanic a aplikacemi je podstatná kvalita ovladačů nosičů[[2]](#footnote-3) tak, aby byla zajištěna požadovaná bezpečnost a interoperabilita.

## Ovladače pro nosiče certifikátů

Dodavatel musí spolu s nosiči certifikátů dodat i příslušné ovladače, pro jednotlivé podporované operační systémy podle následující tabulky:

|  |  |  |
| --- | --- | --- |
| ID | Požadavek, vlastnost | Požadováno |
| M.1 | Microsoft Windows v10 a vyšší:   * Minidriver, kompatibilní s CryptoAPI, resp. Crypto Next Generation[[3]](#footnote-4) * Knihovna PKCS#11 | Ano |
| M.2 | Linux (hlavní distribuce, zejména RedHat/CENTOS a Ubuntu)   * Knihovna #PCKS11 | Ano |
| M.3 | Apple macOS, verze 12+ (Apple Silicon, Intel)   * Knihovna PKCS#11 * CryptoTokenKit[[4]](#footnote-5) | Ano |

Prostřednictvím ovladače budou využívány kryptografické operace nosiče certifikátu. Ovladače pro MS Windows musí podporovat bezpečnou archivaci šifrovacích klíčů[[5]](#footnote-6).

Ovladače nebo další obslužný software musí podporovat zasílání změn dat na nosiči certifikátů do systému správy životního cyklu nosiče nebo certifikátů[[6]](#footnote-7). Zasílány budou pouze informace o certifikátech, nikoli certifikáty samotné.

## Obslužný software pro správu certifikátů a jejich nosičů

Součástí dodávky musí být také software s intuitivním grafickým rozhraním pro využití certifikátů uživatelem a pro uživatelskou správu certifikátů a jejich nosičů.

Obslužný software musí zajišťovat minimálně následující funkce:

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Požadavek, vlastnost | Požadováno | |
| M.4 | Přehledně zobrazovat informace o uložených certifikátech a podrobnosti o každém certifikátu | Ano | |
| M.5 | Podpora importu, popř. smazání certifikátu (i s klíčem) uložených ve souboru podle standardu #PKCS12 | Ano | |
| M.6 | Zobrazit seznam kryptografických klíčů uložených v čipu nosiče, zobrazit zaplnění paměťového prostoru čipu | Ano | |
| M.7 | Zjistit a zobrazit stav přístupových kódů (PIN/PUK) | Ano | |
| M.8 | Nastavit, odblokovat nebo změnit přístupové kódy (PIN/PUK) | Ano | |
| M.9 | Exportovat certifikát z čipu do souboru (bez podpory exportu privátního klíče certifikátu) | Ano | |
| M.10 | Podpora diagnostiky správné funkce čtečky, čipu a stavu certifikátu | Ano | |
| M.11 | Intuitivně umožnit uživateli výběr certifikátu pro prováděnou operaci včetně volitelného intuitivního popisu certifikátu | Ano | |
| M.12 | Rozhraní obslužného software musí být grafické a v českém jazyce |  | |
| M.13 | Software pro správu certifikátů a nosičů musí podporovat minimálně operační systémy:   * Microsoft Windows v10 a vyšší * macOS v13 a vyšší | |  |

## Software pro obnovu uživatelských certifikátů

Součástí dodávky musí být i softwarové řešení pro obnovu uživatelských certifikátů podporovaný technologií autoenrollment. Toto softwarové řešení musí splňovat minimálně následující požadavky:

|  |  |  |
| --- | --- | --- |
| ID | Požadavek, vlastnost | Požadováno |
| M.14 | Intuitivní grafický průvodce obnovou certifikátu pro uživatele. | Ano |
| M.15 | Podporovat komunikaci se systémy pro správu životního cyklu certifikátů a nosičů (centrální evidencí certifikátů a karet), automaticky analyzovat stav certifikátů a nosičů a automaticky nabídnout uživateli k obnově příslušného certifikátu. | Ano |
| M.16 | Průvodce obnovením certifikátu software spustí pouze v případě, že jsou splněny podmínky pro úspěšnou obnovu certifikátu (dostupnost systému pro vydávání certifikátů, ve čtečce je vložen správný nosič certifikátu apod.). Splnění podmínek musí software kontrolovat automaticky. | Ano |
| M.17 | Výzvu uživateli k obnově certifikátu musí software zobrazovat opakovaně, dokud nedojde k úspěšné obnově certifikátu. | Ano |
| M.18 | V případě neúspěšné obnovy certifikátu zaznamenat diagnostické informace pro analýzu příčin neúspěšné obnovy. | Ano |
| M.19 | Software pro obnovu certifikátů musí podporovat minimálně operační systémy:   * Microsoft Windows v10 a vyšší |  |

## Obecné požadavky na obslužný software a middleware pracovních stanic

Ovladače, middleware a další obslužný software musí být dodán v instalačním balíčku, ve formátu běžném pro požadované operační systémy (Windows, macOS, Linux). Minimálně pro operační systém Microsoft Windows musí být dodán instalační balíček ve formátu, umožňující bezobslužnou/vzdálenou instalaci a podporující technologii Microsoft SCCM[[7]](#footnote-8).

1. Podle definice Microsoft pro doménové PKI (Enrollment On Behalf Of). Správce nosičů certifikátů by měl být vybaven certifikátem typu Enrollment Agent, kterým autorizuje žádosti o certifikáty jiných uživatelů. [↑](#footnote-ref-2)
2. Ovladače zajišťují přístup a komunikaci operačního systému a aplikací s kontaktním čipem. [↑](#footnote-ref-3)
3. Minidriver je využíván v aplikacích, které s kartami pracují prostřednictvím kryptografických funkcí MS Windows (např. MS Office, vč. MS Outlook, Adobe Reader, Edge, Chrome apod.). [↑](#footnote-ref-4)
4. Ovladač používaný na novějších verzích macOS, v nativních aplikacích (Mail, Safari apod.). [↑](#footnote-ref-5)
5. Tak jak ji definuje Microsoft (Key Recovery Agent). [↑](#footnote-ref-6)
6. Pokud je koncová stanice připojená do domény. [↑](#footnote-ref-7)
7. Microsoft System Center Configuration Manager [↑](#footnote-ref-8)