



Požadavky na fyzické nosiče identifikačních údajů a certifikátů

Příloha č. 4 zadávací dokumentace pro zadávací řízení „Nasazení MFA a pořízení nosičů certifikátů“

Obsah

[1 Úvod 3](#_Toc207718723)

[2 Požadavky na fyzické nosiče identifikačních dat a certifikátů 3](#_Toc207718724)

[2.1 Typy fyzických nosičů (karet) 3](#_Toc207718725)

[2.2 Technické požadavky na fyzický nosič typu A 4](#_Toc207718726)

[2.3 Technické požadavky na fyzický nosič typu B 4](#_Toc207718727)

[2.4 Technické požadavky na fyzický nosič typu C 4](#_Toc207718728)

[2.5 Požadavky na jakost fyzického nosiče typu B a typu C 6](#_Toc207718729)

[3 Požadavek na množství dodávaných fyzických nosičů 6](#_Toc207718730)

# Úvod

Tato příloha zadávací dokumentace stanovuje požadavky fyzické nosiče identifikačních údajů, dat a certifikátů pro identifikaci a bezpečnou vícefaktorovou autentizaci zaměstnanců SŽ a uživatelů ICT prostředí SŽ.

# Požadavky na fyzické nosiče identifikačních dat a certifikátů

## Typy fyzických nosičů (karet)

Zadavatel požaduje zajistit dodávku identifikačních a autentizačních prostředků (fyzických nosičů certifikátů), včetně služeb potisku (personalizace) fyzického nosiče v následujících variantách:

* **Typ A**: plastová karta rozměru běžné bankovní platební karty pro vizuální identifikaci (potisk, ochranné prvky);
* **Typ B**: plastová smart karta rozměru běžné bankovní platební karty s vnitřním čipem (bezkontaktní bezdrátová komunikace) pro identifikaci uživatelů, včetně možnosti potisku a ochranných prvků pro vizuální identifikaci jako u typu A;
* **Typ C**: plastová hybridní smart karta rozměru běžné bankovní platební karty s kontaktním (viditelným) čipem pro ukládání uživatelských certifikátů a bezpečnou autentizaci uživatelů a s bezdrátovým čipem pro bezkontaktní identifikaci identické s typem B a možností potisku a ochranných prvků pro vizuální identifikaci jako u typu A;

Zadavatel upozorňuje, že vnitřní čip pro bezkontaktní (bezdrátovou) komunikaci pro identifikaci uživatelů musí být u typu B a typu C shodný.

Zadavatel současně připouští nahrazení fyzického nosiče typu B nosičem typu C (tj. dodávku nosiče typu C místo typu B), pokud to bude ekonomicky výhodné.

Dodávané nosiče musí být personalizovatelné oboustranným barevným potiskem (retransferační technologie tisku), včetně umístění ochranných prvků pro ověření autenticity nosiče (např. hologram) a včetně laminace ochrannou fólii. Požadavky na personalizaci fyzických nosičů jsou uvedeny v příloze č. 1 ZD.

Součástí dodávky fyzických nosičů musí být i průhledný ochranný obal (pouzdro) umožňující snadné umístění i vyjmutí nosiče z obalu a také zavěšení obalu na krk uživatele.

## Technické požadavky na fyzický nosič typu A

|  |  |
| --- | --- |
|  | Požadavek |
| A.1 | Formát nosiče: plastová čipová karta velikosti běžné bankovní karty (85,60 x 53,98mm) |
| A.2 | Karta musí splňovat požadavky na personalizaci oboustranným barevným potiskem (retransferová technologie tisku), včetně možnosti umístění ochranného prvku (hologramu) pro ověření autenticity karty a laminace ochrannou fólií. |

## Technické požadavky na fyzický nosič typu B

Jako fyzický nosiče typu B je požadována platová karta splňující požadavky kladené na nosič typu A (tj. plastová karta formátu běžné bankovní platební karty s možností personalizace).

Karta typu B dále musí obsahovat vnitřní bezkontaktní (bezdrátový) čip splňující minimálně následující požadavky:

|  |  |
| --- | --- |
|  | Požadavek |
| B.1 | podpora MIFARE® DESFire® 8K EV2/EV3 |

## Technické požadavky na fyzický nosič typu C

Jako fyzický nosič typu C je požadována platová karta splňující požadavky kladené na nosič typu A (tj. plastová karta formátu běžné bankovní platební karty s možností personalizace).

Karta typu C dále musí obsahovat jak vnitřní bezkontaktní (bezdrátový) čip identický s typem B a dále kontaktní (viditelný) čip pro ukládání uživatelských certifikátů a bezpečnou autentizaci uživatelů splňující následující požadavky:

|  |  |
| --- | --- |
|  | Požadavek |
| C.1 | Nosič certifikátu musí obsahovat kontaktní i bezkontaktní část (kontaktní a bezkontaktní čipy) - hybridní smart karta. |
| C.2 | Karta musí technicky splňovat požadavky na QSCD (kvalifikovaný prostředek pro vytváření elektronických podpisů) podle eIDAS[[1]](#footnote-2), nemusí však být certifikována u žádné z akreditovaných certifikačních autorit v České republice. |
| C.3 | Privátní PKI klíč uložený na kartě nelze z karty vyexportovat. |
| C.4 | Ke klíčovým párům lze na kartu uložit i příslušné certifikáty X.509. |
| C.5 | PKI aplikace v čipu karty musí splňovat Common Criteria úrovně minimálně EAL4+. |
| C.6 | Podpora vícefaktorové autentizace na bázi certifikátů X.509 do PC (prostředí Microsoft Active Directory / Smartcard Logon), webových služeb, VPN, aplikací apod. |
| C.7 | Možnost uložení certifikátů X.509 různých certifikačních autorit. (tedy nejen certifikáty z interních CA SŽ) |
| C.8 | Uložení minimálně 16 klíčových párů s certifikáty, přičemž lze uložit minimálně 4 certifikáty založené na RSA, 4 certifikáty založené na ECC, případně dynamicky využívat úložný prostor karty pro ukládání klíčových párů certifikátů různých typů. Požadována je možnost případné definice jiného rozdělení před výrobou karty. |
| C.9 | Šifrovací algoritmy RSA: 2048, 3072 a 4096 bitů; RSA OAEP, RSA PSS; včetně generování párů klíčů v čipu |
| C.10 | Šifrovací algoritmy ECC: P-256, P-384 a více, včetně generování párů klíčů v čipu |
| C.11 | Šifrovací algoritmy ECC: P-384 bitů, P-521 bitů, včetně generování párů klíčů v čipu |
| C.12 | Podpora RSA OAEP a RSA PSS |
| C.13 | Hashovací algoritmy: SHA-2: SHA-256, SHA-384, SHA-512; volitelně SHA-3: SHA-265–512 |
| C.14 | Podpora algoritmů ECDSA a ECDH |
| C.15 | Podpora symetrické kryptografie AES (128, 192, 256 bitů) a 3DES (ECB, CBC) |
| C.16 | Import klíčů s certifikáty do čipu, např. ze standardizovaného souboru PKCS#12 |
| C.17 | Podpora možnosti archivace privátních klíčů v procesech vydávání šifrovacích certifikátů |
| C.18 | Podpora PIN; podpora PUK pro odblokování PIN, včetně zablokování PIN, resp. PUK po opakovaném chybném zadání PIN, resp. PUK |
| C.19 | Možnost definice PINových politik před dodáním karty (minimální délka PIN, počty PIN objektů, počty chybných pokusů před zablokováním PIN apod.) |
| C.20 | Uchování dat v paměti min. 10 let |
| C.21 | Přepis paměti: minimálně 500 000 cyklů |

## Požadavky na jakost fyzického nosiče typu B a typu C

Záruka na bezporuchový provoz nosiče (kontaktní i bezkontaktní části) v prostředí Zadavatele minimálně po dobu 24 měsíců od předání nosiče uživateli.

Podmínka bezporuchovosti nosičů bude splněna nepřekročí-li poruchovost nosičů v požadovaném období 24 měsíců 3 % z celkového počtu nosičů předaných uživatelům.

# Požadavek na množství dodávaných fyzických nosičů

Zadavatel požaduje dodávku fyzických nosičů v následující maximálním množství:

|  |  |  |  |
| --- | --- | --- | --- |
| Typ | Počet fyzických nosičů pro pilotní provoz Fáze 6 | Počet pro úvodní dodávku fyzických nosičů (karet), Fáze 6 | Odhadové počty pro průběžnou dodávka fyzických nosičů (karet) Fáze 11 |
| Typ A | 0 | 0 | 400 |
| Typ B | 40 | 1.500 | 5.800 |
| Typ C | 40 | 9.000 | 8.800 |

Při dodávkách fyzických nosičů Zadavatel požaduje:

* **Fáze 6**, dodávka fyzických nosičů pro provedení Fáze 5 (pilotní provoz): fyzické nosiče bez personalizace, bez ochranných prvků a včetně ochranných obalů
* **Fáze 6**, úvodní dodávka fyzických nosičů (mimo pilotní provoz): fyzické nosiče, včetně jejich personalizace, ochranných prvků a ochranných obalů
* **Fáze 11**: fyzické nosiče bez personalizace, včetně ochranných prvků a ochranných obalů

Tabulka určuje maximální objem plnění v dodávkách fyzických nosičů všech typů, jejich ochranných prvků, ochranných obalů a spotřebního materiálu personalizačního pracoviště. Množství fyzických nosičů, poměr jednotlivých typů a množství souvisejících ochranných prvků, obalů a spotřebního materiálu definované tabulkou je nutno vnímat jako maximální a Zadavatel tento rozsah není povinen využít. Dodavatel bere na vědomí, že bez jakékoli sankce či poplatku Zadavatele, nemusí být uvedené množství úplně využito.

U Fáze 6 bude množství a harmonogram dodávek nosičů, jejich personalizace (u dodavatele), ochranných prvků a ochranných obalů upřesněn v předimplementační analýze a může být upravován podle skutečného průběhu plošného nasazení řešení v celé organizaci Zadavatele.

1. Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, popř. Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014 [↑](#footnote-ref-2)