Příloha č. 1 Smlouvy

Technické parametry a vlastnosti Díla

1 Technické parametry díla

1.1 Technický popis karty pro tisk průkazů zaměstnance

- plastová duální karta s kontaktním a bezkontaktním čipem
- ISO formát 85 x 54 mm (ID1 plná velikost)

1.1.1 Bezkontaktní část: čip K78C HID

- Frekvence 13,56 MHz, technologie iCLASS, 32 bit
- Velikost a alokace paměti: 32k Bits (4k Bytes) Application areas 16k/2 + 16k/1
- Facility code: 5272
- Programování: formát Cardkey C10001
- Rozsah série nových karet HID (Card Range) musí být od 27000
- Final Part Number 2113PGGNN

1.1.2 Kontaktní část: čip Giesecke & Devrient Starcos 3.7

- kontaktní část musí plně splňovat technické požadavky stanovené Nařízením 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 (nařízení **eIDAS**)
  Kompatibilita se standardy
- ISO/IEC, DIN, EMV

1.2 Základní technické parametry čipu Starcos 3.7

- Velikost paměti karty: 126,9 kB
- Velikost privátního RSA klíče generovaného na kartě: 2048
- Kryptografické funkce: RSA 2048 bits/4096 bits, ECC NIST P-384
- Podpora Hashes: SHA-256 až SHA-512
- Podporované standardy: ISO 7815-4/-8/-9, ISO 14443-1/-2/-3/-4
- Podporované protokoly: ISO 7816-3 T=0 a T=1
- Podporované rozhraní: MS CSP/CNG (minidriver), PKCS 11
- Standard PKCS 12
- Privátní klíč se generuje přímo v kartě a nikdy neopustí kartu
- Počet úložišť pro privátní klíče a certifikáty je variabilní. Možnost vytvoření nového úložiště a uložení dat na kartu je omezena pouze volnou kapacitou karty. Pro uložení klíčů pro kvalifikované certifikáty je vyhrazeno 4x RSA 2048bit nebo 2x RSA 4096bit nebo 4x ECC NIST P-384

Kompatibilita se standardy

- ISO/IEC, DIN, EMV

Další funkčnosti karty

- Prostor pro citlivá data chráněný PINem
- Nativní práce s volným prostorem na kartě
- Tvorba žádosti o obnovu certifikátu bude řešena ve správci karty odkazem na generátor
- PIN management (individuální PIN pro zabezpečená datová úložiště)
- Blokace karty při zadání chybného PIN
- Podpora pro Secure PIN entry
- Nativní podpora pro TWINS

Podpora pro

- OS: Windows Server 2022, Windows 10/11
- MS CAPI (existence Cryptographic Services Provider pro Microsoft) PC/SC rozhraní
- CryptoOKI (modul PKCS11 pro aplikace typu Firefox)

1.3 Personalizace karet

Personalizaci kontaktního čipu provede I.CA. Součástí personalizace je také nahrání mezilehlých a kořenových certifikátů.

1.4 Technologická specifikace čipové karty/čipu Starcos 3.7

- Paměťová kapacita karty je využívána dynamicky, což umožňuje na kartu uložit variabilní počet klíčů, certifikátů a ostatních dat. Toto pravidlo se nevztahuje na kvalifikované certifikáty. Pro uložení klíčů pro kvalifikované certifikáty je vyhrazeno 4x RSA 2048bit nebo 2x RSA 4096bit nebo 4x ECC NIST P-384.
- Karta je využívána i pro bezpečné uložení kořenového certifikátu Certifikační autority. Díky uloženému certifikátu Certifikační autority je možné kartu používat i v neznámém prostředí. Je možné zvolit podporované (důvěryhodné) Certifikační autority, jejichž klientské certifikáty může klient využívat. Jiné klientské certifikáty pak není možné na kartu umístit, čímž se významně omezuje možnost použití karty k nepovoleným operacím.
- Čipová karta má životnost několik let, během života karty si může majitel na kartu nechat vydat několik certifikátů. Životnost karty není aplikací kontrolována.
- Bezpečnostně citlivé operace je na kartě možné vždy realizovat pouze po zadání PIN, jehož délka je **6 – 8 míst**. Po zadání PUK (8 míst) získá klient další pokusy pro zadání PIN, maximální počet použití PUK je omezený. Karta není po personalizaci vybavena PIN a PUK a klient je při prvním použití karty požádán o zvolení PIN a PUK.
- Čip je kvalifikovaným prostředkem pro vytváření elektronických podpisů podle nařízení eIDAS.

2 Typy a počty karet

Objednatel požaduje

Typ čipové karty	Počet kusů
Čipová karta - blank	2000

3 Další podmínky

Objednatel stanovil následující další podmínky pro dodávané čipové karty:

- karty musí být bez inicializace
- karta bude dodána jako duální, tj. s bezkontaktním čipem (viz. bod 1.1.1),
- na karty musí být umožněno nahrání klientského certifikátu, vydaného autoritou SFIF UserCA2 s tím, že root certifikát SZIF UserCA2 nebude nahrán na kartě, ale v souboru. Tento soubor je možné hromadně nakopírovat na všechny stanice, např. přes Group Policy. Soubor bude uložen v cestě C:\ProgramData\I.CA SecureStore.
- na karty musí být umožněno nahrání kvalifikovaného certifikátu pro el. podpis, vydaného autoritou CA I.CA s tím, že root certifikát CA I.CA nebude nahrán na kartě, ale bude v souboru (v cestě C:\ProgramData\I.CA SecureStore), který je součástí instalace I.CA SecureStore.
-

Čipová karta Starcos 3.7 bude dodána s obslužnou aplikací SecureStore I.CA v české, a anglické verzi, která zajistí komfortní práci klienta s čipovou kartou (pro OS WIN v 32b i 64b verzi). Jde o SW pro management karty tj. správu certifikátů, klíčů, přihlašovacích údajů a ostatních údajů na pracovní stanici. Komponenta musí umožňovat použití karty v prostředí internetových prohlížečů, MS Outlook, a dalších aplikacích na platformě Windows a SAP, které využívají standardní rozhraní CryptoAPI.