



Ministerstvo kultury

Maltézské náměstí 1
118 11 Praha 1

telefon: 257 085 111
fax: 224 318 155
e-mail: epodatelna@mkcr.cz

Objednávka č.j. : MK 58081/2022 SOITSS Dodavatel : MONET+, a.s., Za Dvorem 505, Štípa, 763 14 Zlín IČ:26217783	Dne : ... Fakturujte : Ministerstvo kultury Maltézské náměstí 1 118 11 Praha1 – Malá Strana IČO :00023671 DIČ : CZ00023671 Ministerstvo kultury není plátcem DPH
Dodejte do : viz níže Komu: MK Milady Horákové 139, Praha 6 	Č. Ú.: 
Cena s DPH: 360 701 Kč	

Objednáváme:

Dodávku zboží dle níže uvedené specifikace

POLOŽKA	MNOŽSTEVNÍ KATEGORIE	CENA ZA JEDNOTKU V KČ BEZ DPH	CENA CELKEM V KČ BEZ DPH
Čipová karta ProID+Q	300	515	154 500
Licence CMS	Pro max. 350 uživatelů	83 600	83 600
Licence Kartového centra	1 instance	60 000	60 000
Celková cena bez DPH			298 100
Celková cena vč. DPH			360 701

Základní funkce a služby:

- QSCD hybridní čipové karty ve formátu ID-1 (velikost bankovní karty). Kontaktní čipy a aplikace nahraná do kontaktního čipu umožňuje správu kryptografických klíčů určených k vytváření kvalifikovaného elektronického podpisu.
- Dodané karty budou obsahovat i bezkontaktní čip, který Objednatel ve svém prostředí provozuje a to 125kHz a nebo 13MHz
- SW aplikace pro správu hybridních čipových karet a certifikátů s licencí na dobu neurčitou pro 350 uživatelů.
- Pomocí hybridních čipových karet zajistit 2faktorovou autentizaci uživatelů, tak aby byly naplněny podmínky ZoKB.

Technické vlastnosti:

- a) Cílovým požadavkem je:

Umožnit zaměstnancům vytvářet kvalifikovaný elektronický podpis podle nařízení eIDAS pomocí kryptografických klíčů bezpečně chráněných v hardwarovém prostředí – hybridní čipové kartě.

b) Základní požadavky na zařízení:

Hybridní čipové karty a ovladače:

Pro uložení elektronických certifikátů X.509 (a generování / uložení příslušných kryptografických klíčů) budou dodány hybridní čipové karty ve formátu ID-1 (velikost bankovní karty):

- kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací.

Certifikované karty musí být v souladu:

- s normou ČSN EN ISO 7816, část 1-4 a
- 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

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 šifrovaných certifikátů
- Podporované jsou minimálně kryptografické algoritmy:
 - Symetrické: 3DES, AES
 - Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
 - RSA: 1024, 2048 bitů
 - Eliptické křivky: P-224, P-256, P-384, P-521
- 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)
- Dvofaktorovou autentizaci 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.
- Generování a práce s RSA a ECC klíči v čipu
- Hybridní čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů.

Ovládací software karty:

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 O MS Windows 8 nebo vyšších verzích;
- případné použití i na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11)
- instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), 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.

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

- a) Zjednodušení životního cyklu karet a certifikátů
- b) Automatizovaná obnova kvalifikovaných i komerčních certifikátů od externího poskytovatele. Automatizovaná obnova interních certifikátů z doménové CA
- c) Implementace aplikace, které prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu
- d) Implementace aplikace pro podporu činností spojených se správou životního cyklu čipových karet a certifikátů.
- e) Implementace webové aplikace, určené správcům certifikátů. Možnost vyhledávat a prohlížet informace o certifikátech, odvolávat certifikáty, generovat a prohlížet reporty

Termín dodávky do 30ti dní ode dne uveřejnění objednávky v registru smluv.

Celková cena 298 100 Kč bez DPH zahrnuje veškeré náklady na dodávku a je splatná po dodání a převzetí na základě faktury s 30ti denní splatností.

V případě prodloužení s dodávkou o více jak 1 den si bude objednatel účtovat pokutu ve výši 0,5% z celkové ceny za každý den prodloužení.



.....
podepsáno elektronicky

Vyřizuje: [REDACTED]

Potvrzujeme přijetí objednávky.

Datum: [REDACTED] Razítko a podpis:

