

Technická špecifikácia pre smart karty - čipové karty pre personalizáciu ePZP

Pre zadefinovanie technickej špecifikácie pre smart karty za účelom obstarania boli použité nasledujúce dokumenty:

- eSO1_x074H Detailný dizajn subsystému IA, časť 1 / 3 – Dizajn technických komponentov
- CMS 5.11.2 Release Notes, zo 18.2.2022, od IDnomic

Čipová karta s vlastným kryptografickým procesorom pre ePZP. Primárnou úlohou čipových kariet pre ePZP je ochrana privátnych kryptografických kľúčov zdravotníckeho pracovníka, ktoré slúžia pri jeho autentifikácii, na zabezpečenie dôvernosti elektronickej komunikácie a na účely elektronickeho podpisu zdravotníckeho pracovníka.

Aby sa predišlo klonovaniu kariet, nesmú byť súkromné kryptografické kľúče z karty exportovateľné, a preto musia byť čipové karty vybavené vlastným procesorom a operačným systémom, ktorý dokáže samostatne vykonávať kryptografické operácie.

Služby čipových kariet sú sprístupňované operačnému systému pomocou middleware. Z pohľadu integrácie so servisným/aktivačným portálom Card Management System (CMS) je dôležité, aby bolo možné využívať karty na operačných systémoch Windows prostredníctvom Microsoft Base Smart Card Crypto Provider.

Karty sú kontaktné a sú čítané pomocou kontaktného rozhrania čítačiek čipových kariet pre zdravotníckych pracovníkov. Tento spôsob zabezpečuje lepší dohľad zdravotníckeho pracovníka nad svojou kartou. Na čítanie kariet zdravotníckych pracovníkov sa používajú štandardné kontaktné jedno-štrbinové čítačky čipových kariet. K dnešnému dňu sa na väčšine pracovísk PZS využívajú čítačky Gemalto ID BRIDGE CT30/31, OMNIKEY 3121, výnimočne aj iný model.

Karty sa personifikujú, potláčajú zariadením Evolis Securion alebo Evolis Primacy. Ako autentifikačný modul sa používa Card Management System OpenTrust od IDnomic.

Pre bezpečnosť operácií s kryptografickými kľúčmi je nutné, aby karta obsahovala vlastný kryptografický procesor s príslušnými bezpečnostnými certifikátami. Magnetické, ani pamäťové karty vlastný kryptografický procesor neobsahujú, preto nemôžu byť predmetom riešenia.

Na karte sa používajú 3 certifikáty, zvyšok do celkového limitu 15 je bezpečnostná rezerva pre potenciálne budúce rozšírenie subsystému. Veľkosť kľúčov 2048 bit RSA je minimom vyžadovaným bezpečnostnými požiadavkami v NZIS.

Životnosť vydananej karty je 25 rokov, čo zahŕňa rezervu pre budúci vývoj technologických platforiem. Splnenie všetkých vyžadovaných štandardov ISO 7816 alebo ekvivalentný, zabezpečuje kompatibilitu kariet čítačkami čipových kariet. Štandard ITU-TX.509 alebo ekvivalentný, popisuje technológiu používaných certifikátov v celom NZIS projekte. Certifikáty v oblasti FIPS – FIPS 140-2 Level 2 alebo 3, prípadne CC EAL5+ alebo ekvivalentné, zabezpečujú splnenie požadovanej úrovne bezpečnosti.

Aktuálne používaný model kariet, kompatibilný pre CMS je Gemalto IDPrime 830.

Obstarávané smart karty musia byť podporované CMS klientom (Card Management System, SW) a samoobslužným portálom tohto SW, podľa priloženého Release Notes k CMS, alebo ekvivalentné, kompatibilné so stávajúcim SW a HW vybavením NCZI pre personalizáciu ePZP.

1. Technické vlastnosti	Hodnota/Charakteristika
Účel	Čipová karta s vlastným kryptografickým procesorom (nie magnetické ani pamäťové karty)
Pamäť	Kapacita aspoň 15 certifikátov a párov kryptografických kľúčov (veľkosť kľúčov 2048 bit RSA)
Rozhranie na komunikáciu OS (middleware)	MS Windows Crypto API CSP (podpora Microsoft Base Smart Card Crypto Provider) version 7PKCS#11 version 2.20.
Podporované platformy	Windows, MAC, Linux

Technická špecifikácia pre smart karty - čipové karty pre personalizáciu ePZP

Životný cyklus	500 000 zápisov
Doba úschovy údajov (data retention)	Aspoň 25 rokov
Komunikačné rozhranie	Kontaktné alebo kontaktná s NFC
Materiál	PET – Pet alebo PVC; farba biela
2. Podporované štandardy / certifikácie	
ISO 7816-1	Identification cards - Integrated circuit(s) cards with contacts – Part 1: Physical characteristics
ISO 7816-2	Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts
ISO 7816-3	Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols
ITU-T X.509	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks
Aspoň jedna z certifikácií :	
FIPS 140-2 Security Requirements for Cryptographic Modules. Alebo CC EAL5+/ PP QSCD	s PKI appletom na karte
Common criteria (CC)	Minimálne na úrovni CC EAL6+ certified on chip level
Full Secure Messaging (SM)	No
3. Kryptografické algoritmy:	
Povinne	RSA up to RSA 2408 bits, On-card asymmetric key pair generation (RSA), RSA OAEP & RSA PSSSHA-1, SHA-256, SHA-384, SHA-512, Generovanie asymetrického páru kľúčov na karte (RSA)
Voliteľne	Eliptické krivky: P-256, P-384, P-521 bits, ECDSA, ECDH Generovanie asymetrického páru kľúčov na karte: (Ellipticcurves)
4. Kompatibilita s použitými riešeniami v procese vydávania kariet:	
Autentifikačný modul	Karta musí byť kompatibilná s verziou CMS OpenTrust – 5.11. a viac.
Potlač a personalizácia kariet	Karta bude obojstranne plnofarebne potlačená (napr termoprint, ofset) podľa zadania objednávateľa a dodaná ako plnofarebná, s následnou možnosťou personalizovať zariadeniami Evolis Securion a Evolis Primacy
Podporované Smart karty/ tokeny a middleware pre CMS klienta a pre Samoobslužný portál na základe CMS 5.11.2 Release Notes, IDnomic <i>(Verejný obstarávateľ na základe Release Notes pre CMS 5.11.2, IDnomic uvádza všetky ekvivalentné smart karty / tokeny)</i>	<ul style="list-style-type: none"> • CardOS with Middleware 5.5.2.1349 • Vasco DIGIPASS KEY with AET SafeSign IC 3.0.101 • G&D STARCOS 3.0 and 3.2 with Cryptovision Middleware 7.0.5 • Gemalto Classic TPC IM (Standard or CC) with Gemalto IDGo 300 6.3 002 (previously Gemalto Classic Client) • Gemalto .Net v2+, SafeNet eToken 5300, IDPrime .Net and IDPrime MD 830, 830B FIPS 140-2 Level 2 and 3, 840, 840B, 3810, 3811, 3840, with SafeNet Authentication Client 10.8 • Thales IDPrime 930 FIPS 140-2 Level 2, 940, 3930 L2, 3940 and 3940 FIDO (Certificates only) with SafeNet Authentication Client 10.8 • Morpho ypsID S2, S3, U3 and Em ccid with ypsID Middleware 7.0.5 • Idemia ypsID S5i with ypsID Middleware 8.0.3

Technická špecifikácia pre smart karty - čipové karty pre personalizáciu ePZP

	<ul style="list-style-type: none">• Oberthur ID-One Cosmo v8.1 R2 and Cosmo v8.2 with AWP 5.3.5• SafeNet eToken 4100/5100/5105 (previously eToken PRO) with SafeNet Authentication Client 10.6• SafeNet eToken 5110/5110+ FIPS with SafeNet Authentication Client 10.6• Gemalto and Idemia cards with "IAS-ECC middleware" 3.1• JCOP3 P60 cards with NXP Athena• Yubikey 5 NFC with Yubikey PIV tools (x86) 2.2.1
--	--