**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 5.9.2 Release Notes, zo 17.9.2021, 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 elektronického 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.

Karty sa personifikujú, potláčajú a laminujú zariadením Evolis Securion Printer. Ako autentifikačný modul sa používa Card Management System OpenTrust.

Pre bezpečnosť operácií s kryptografickými kľúčmi je nutné, aby karta obsahovala vlastný kryptografický procesor s príslušnými bezpečnostnými certifikáciami. 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 vydanej karty je 25 rokov, čo zahŕňa rezervu pre budúci vývoj technologických platforiem. Splnenie všetkých vyžadovaných štandardov ISO 7816 zabezpečuje kompatibilitu kariet čítačkami čipových kariet. Štandard ITU-TX.509 popisuje technológiu používaných certifikátov v celom NZIS projekte. Certifikáty v oblasti FIPS a Common criteria zabezpečujú splnenie požadovanej úrovne bezpečnosti.

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

K dnešnému dňu sa na väčšine pracovísk PZS využívajú čítačky Gemalto ID BRIDGE CT30/31, OMNIKEY 3121, výnimočne aj iný model.

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**
 |  |
| 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 |
| Čip | Infineon, SLE78CFX3009P |
| 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, Android, iOS |
| Životný cyklus | 500 000 zápisov |
| Doba úschovy údajov (data retention) | Aspoň 25 rokov |
| Komunikačné rozhranie | Kontaktné alebo kontaktná s NFC |
| Materiál | Plast / PET, farba biela, bez potlače |
| 1. **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 forCryptographic Modules. | Úroveň 3 s PKI appletom na karte. |
| Common criteria | Minimálne na úrovni EAL 5+ CC EAL5+ Protection Profile Secure Signature Creation Device |
| 1. **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,ECDHGenerovanie asymetrického páru kľúčov na karte: (Ellipticcurves) |
| 1. **Kompatibilita s použitými riešeniami v procese vydávania kariet:**
 |  |
| Autentifikačný modul | Karta musí byť kompatibilná s aktuálnou verziou CMS OpenTrust – 4.9.x a viac. |
| Potlač a personalizácia kariet | Karta sa musí dať personalizovať zariadeniami Evolis Securion |
| **Podporované Smart karty/ tokeny a middleware pre CMS klienta a pre Samoobslužný portál cez Internet Explorer** | * Gemalto IDPrime MD 830, 830B FIPS 140-2 Level 2 and 3, 840B, 3810, 3840, with SafeNet Authentication Client 10.8
* Morpho ypsID S2, S3, U3 and Em ccid with ypsID Middleware 7.0.5
* SafeNet eToken 4100/5100/5105 (previously eToken PRO) with SafeNet Authentication Client 10.6
 |