Ministerstwo
Spraw Wewnętrznych

Centrum Certyfikacji
Ministerstwa Spraw Wewnętrznych

Specyfikacja kart kryptograficznych dla pl.ID

Certyfikacji MSW wykorzystuje obecnie w pl.ID następujące karty:

I. Athena IDProtect Duo v1

II. Gemalto ID Prime 3810

1. Karta kryptograficzna ma być zgodna ze standardem ISO w częściach: 7816-1, 7816-2, 7816-3, 7816-4, 7816-5, 7816-6, 7816-8.
2. Karta kryptograficzna ma być wyposażona w interfejs zgodny z normami: ISO 7816, ISO 14443.
3. Karta kryptograficzna ma być wyposażona w procesor o pojemności min 32 kb.
4. Karta kryptograficzna ma być zgodna ze standardem Java Card 2.2.1.
5. Napięcie zasilania karty kryptograficznej musi mieścić się w zakresie 1,62 - 5,5 V.
6. Karta kryptograficzna ma być pozbawiona nadruków.
7. Gwarantowana ilość cykli zapisu/kasowania karty kryptograficznej nie może być mniejsza niż 500 000.
8. Karta kryptograficzna ma być wspierana przez następujące algorytmy kryptograficzne i szyfrujące: AES (128, 192, 256), RSA (2048 bit), SHA-1, SHA-256, SHA-512.
9. Karta kryptograficzna ma generować klucze kryptograficzne: AES (128, 192, 256), RSA (2048 bit), SHA-1, SHA-256, SHA-512.
10. Karta kryptograficzna ma posiadać wsparcie dla: MS terminal Services, logowania w domenie, pracy wieloaplikacyjnej.
11. Karta kryptograficzna ma zapewniać wsparcie dla polityki haseł (PIN'ów).
12. Karta kryptograficzna ma zapewniać wsparcie dla szyfrowania komunikacji między kartą a komponentami systemu.
13. Karta kryptograficzna ma zapewniać wsparcie dla różnych kodów PIN, PUK.

14. Karta kryptograficzna ma zapewniać wsparcie dla historii PIN'ów.

15. Karta kryptograficzna ma zapewniać wsparcie dla konfigurowalnej polityki PIN i PUK.

16. Karta kryptograficzna ma zapewniać wsparcie dla PKCS #11 dla systemów Windows w wersji językowej polskiej lub angielskiej, 32 lub 64 bity (XP SP2 lub SP3, Server, Vista, Windows 7, Windows 8) oraz Unix /Linux 32 lub 64 bity.

17. Karta kryptograficzna ma zapewniać wsparcie dla CSP dla systemu operacyjnego Windows w wersji językowej polskiej lub angielskiej, 32 lub 64 bity (XP SP2 lub SP3, Server, Vista, Windows 7, Windows 8).