Wymagania techniczno-funkcjonalne dla karty elektronicznej – blankietu ELS.

Karta procesorowa

Wstępnie zadrukowany blankiet ELS (Karta) jest hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi):

1. stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności całkowitej pamięci EEPROM co najmniej 390 kilobajtów, w tym dostępnej co najmniej 67 kilobajtów.
2. bezstykowym określonym w normie ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® dla protokołu klasycznego o pojemności pamięci 1 kilobajt (MIFARE® Standard Card IC MF1 IC S50 Functional Specification lub równowazny).

Karty wykonane są z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu. Sposób wykonania kart określa Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego w sprawie studiów z dnia 27 września 2018 (Dz. U. 2018 r. poz. 1861 z późn. zmianami: Dz.U. 2019 r. Poz. 787).

Blankiet może być stosowany jako kwalifikowane urządzenie do składania podpisu elektronicznego zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE – Załącznik II Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego -, na które powołuje się Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579, tekst jednolity Dz.U. 2019 poz. 162).

Wygląd legitymacji

Wygląd blankietu ELS określa załącznik nr 1 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie studiów z dnia 27 września 2018 (Dz. U. 2018 r. poz. 1861 z późn. zmianami: Dz.U. 2019 r. Poz. 787) (blankiety bez napisu „Adres" w poddruku offsetowym).

Część elektroniczna – stykowa

Część stykowa karty jest wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.

Polecenia i odpowiedzi przesyłane podczas komunikacji Karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.

Polecenia realizowane przez Kartę dla operacji kryptograficznych i zarządzania są zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.

Blankiet ELS musi spełniać następujące wymagania:

1. Układ elektroniczny o pojemności pamięci EEPROM o dostępnej pamięci co najmniej 67 kilobajtów z wbudowanym koprocesorem kryptograficznym.
2. Układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+.
3. Card Management i API zgodne z Global Platform 2.1.1
4. System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z roszerzeniami JC 3.0.4 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC)
5. Blankiet ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+ według profilu PP SSCD/QSCD Protection Profile – Qualified Signature Creation Device/Secure Signature Creation Device wg EN 419211 część 1

do 6 (poprzednio publikowane pod kodem EN 14169). Zgodność ze specyfikacją eIDAS.

6. Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).
7. DAP zgodne z Global Platform 2.1.1 (PK-Based).
8. Funkcjonalność PKI zgodna ze standardem minidriver ver. 7.x firmy Microsoft oraz PKCS#11 ver. 2.20. Minidriver dla karty powinien być dostępny na stronach Microsoft Update.
9. Obsługiwane protokoły: T=0, T=1, PPS.
10. Prędkość transmisji czytnik – karta do 230 Kbauds.
11. Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez koprocesor kryptograficzny Karty.
12. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.
13. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem.
14. Blankiet ELS w części stykowej musi pozwalać na zarządzanie pamięcią EEPROM poprzez: usuwanie apletów/pakietów, udostępnianie pamięci zwolnionej po usunięciu apletu/pakietu i defragmentację luk w pamięci EEPROM.
15. Generowanie kluczy kryptograficznych o długości do 2048 bitów (opcjonalnie do 4096 bitów) przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA, generowanie kluczy kryptograficznych ECC o długości do 521 bitów, podpisywanie za pomocą algorytmu ECC, obsługa funkcji skrótu SHA-1, SHA-256, SHA-384, SHA-512, obsługa algorytmów 3DES (ECB, CBC), AES (128, 192, 256 bitów).
16. Karta przystosowana do umieszczenia na niej certyfikatu kwalifikowanego wraz z kluczami kryptograficznymi oraz certyfikatu niekwalifikowanego wraz z kluczami kryptograficznymi; certyfikaty mogą zostać umieszczone w późniejszym czasie.

Część elektroniczna – bezstykowa

Część bezstykowa jest wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.

Sposób komunikacji karty jest zgodny ze standardem przemysłowym MIFARE® dla protokołu klasycznego spełniającym wymagania normy ISO/IEC 14443-1, ISO/IEC 14443-2, ISO/IEC 14443-3 oraz opcjonalnie ISO/IEC 14443-4 (protokół T=CL), przy zachowaniu pełnej antykolizyjności.

Zabezpieczenia na czas dostawy

Dostęp do układów elektronicznych blankietów ELS jest zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej.

Proponowane Karty muszą być zgodne (kompatybilne) z zainstalowanym na Uczelni Systemem USOS.