Specyfikacja - szczegółowe wymagania techniczne dla karty elektronicznej – blankietu ELS Elektronicznej Legitymacji Studenckiej - ELS/2018

Wymagania techniczno-funkcjonalne dla karty elektronicznej – blankietu ELS

Wstępnie zadrukowany blankiet ELS (Karta) jest **hybrydową elektroniczną kartą procesorową z dwoma niezależnymi układami procesorowymi**: jeden z interfejsem stykowym a drugi z interfejsem bezstykowym:

1. stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM 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® Stadnard Card IC MF1 IC S50 Functional Specification).

Karty wykonane są z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu. Sposób wykonania kart określa załącznik nr 3 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie dokumentacji przebiegu studiów z dnia 16 września 2016 r. (Dz.U. 2016 poz. 1554) wraz z późniejszymi zmianami (Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 19 stycznia 2018 r., Dz.U. 2018 poz. 229).
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).

Wygląd legitymacji

Wygląd blankietu ELS określa załącznik nr 3 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie dokumentacji przebiegu studiów z dnia 16 września 2016 r. (Dz.U. 2016 poz. 1554) wraz z późniejszymi zmianami (Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 19 stycznia 2018 r., Dz.U. 2018 poz. 229).

Blankiety **muszą posiadać nadrukowany numer MIFARE**, niezbędny do zaopatrzenia kart w klucze dostępu umożliwiające kodowanie biletów komunikacji miejskiej.

Wykonawca umieści na blankiecie w sposób trwały, w miejscu przeznaczonym na kod kreskowy, numer karty (odpowiadający numerowi seryjnemu zapisanemu w bloku nr 0 w sektorze nr 0 układu scalonego z interfejsem bezstykowym).

Obowiązuje następujący format nadruku numeru karty:

a. Zawsze 11 cyfr zgrupowanych w dwóch ciągach rozdzielonych odstępem odpowiednio po 3 i 8 cyfr (np. 001 00000001),
b. Grupa 3 pierwszych cyfr odpowiada 8 najbardziej znaczącym bitom 32 bitowego kodu numeru, przyjmuje wartości z przedziału < 000, 255 >,
c. Grupa pozostałych 8 cyfr odpowiada 24 pozostałym bitom 32 bitowego kodu numeru, przyjmuje wartości z przedziału < 00000000,16777215 >,
d. Obowiązuje zasada uzupełniania każdej grupy cyfr nieznaczącymi zerami (z przodu) do osiągnięcia odpowiednio 3 i 8 cyfr (w sumie zawsze 11 cyfr),
e. Cyfry powinny mieć wysokość nie mniejszą niż 2 mm i nie większą niż 3 mm.

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 oraz opcjonalnie ISO/IEC 7816-15.

Blankiet ELS może być stosowany jako komponent techniczny urządzenia do składania podpisu elektronicznego (ustawa z dnia 18 września 2001 r. o podpisie elektronicznym – Dz. U. 2001 nr 130 poz. 1450).

Blankiet ELS musi spełniać następujące wymagania:

1. Układ elektroniczny o pojemności pamięci EEPROM co najmniej 67 kilobajtów z wbudowanym koprocesorem kryptograficznym.
2. Pojemność karty dla danych w systemie plików zgodnym z ISO 7816-4 powinna wynosić co najmniej 10KB (kilobajtów).
3. Układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL4+.
4. Card Management i API zgodne z Global Platform 2.1.1
5. System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.1
6. Blankiet ELS musi posiadać certyfikat Common Criteria Standard według profilu PPSSCD Protection Profile – Secure Signature Creation Device Type 2 and/or 3, version 1.05, EAL4+ (CWA14169).
7. Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).
8. DAP zgodne z Global Platform 2.1 (PK-Based).
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.
14. Generowanie kluczy kryptograficznych o długości do 2048 bitów przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA, obsługa funkcji skrótu SHA-1, SHA-256, obsługa algorytmów DES, 3DES (ECB, CBC), AES.
15. 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.

Oprogramowanie

Do każdej karty oferent dołączy licencję na oprogramowanie Middleware umożliwiające zarządzanie kartą oraz wykorzystanie dodatkowych możliwości karty.

Proponowane Karty muszą być zgodne (kompatybilne) z zainstalowanym na Uczelni systemem OPTIcamp firmy OPTeam S.A.