Załącznik nr 1

Szczegółowe wymagania dla blankietu elektronicznej legitymacji studenckiej

1. Karta procesorowa
   1.1. Wstępnie zadrukowana elektroniczna karta procesorowa o pojemności pamięci nieulotnej typu EEPROM wynoszącej co najmniej 64 kilobajtów, z dwoma równoważnymi interfejsami układu procesora (karta dualna):
      1.1.1.stykowym:
         1.1.1.1. zgodnym z normą ISO/IEC 7816-1, 7816-2 i 7816-3,
         1.1.1.2. polecenia i odpowiedzi przesyłane podczas komunikacji karty z infrastrukturą informatyczną (APDU) mają strukturę określoną w normie ISO/IEC 7816-4,
         1.1.1.3. karta realizuje polecenia APDU określone w normie ISO/IEC 7816-4,
      1.1.2.bezstykowym:
         1.1.2.1. zgodnym z normą ISO/IEC 14443-1, 14443-2, ISO/IEC 14443-3,
         1.1.2.2. polecenia i odpowiedzi przesyłane podczas komunikacji karty z infrastrukturą informatyczną (APDU) mają strukturę określoną w normie ISO/IEC 14443-4 (protokół T=CL) oraz umożliwiają realizację poleceń APDU ze zbioru określonego dla interfejsu stykowego,
         1.1.2.3. określonym w normie ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® Classic o pojemności pamięci co najmniej 1 kilobajt,
         1.1.2.4. posiadającym stały, nadawany na etapie produkcji identyfikator karty (UID) o długości 4 lub 7 bajtów,
         1.1.2.5. dla którego wszystkie operacje wykonywane przez interfejs stykowy są możliwe do wykonania również przez interfejs bezstykowy,
         1.1.2.6. zgodny z wykorzystywanym w systemie Poznańskiej Elektronicznej Karty Aglomeracyjnej.
   1.2. Poddruk karty
      1.2.1.dla blankietów ELS jest wykonany według wymagań i wzoru określonego w załączniku nr 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (tj. Dz. U. z 2023 r. poz. 2787)
      1.2.2.białe pole po stronie rewersowej jest położone w stosunku do brzegów karty z dokładnością +/- 0,5 mm.
   1.3. Karty wykonane są z materiału laminowanego nieulegającego odkształceniu i rozwarstwieniu o wymiarach i właściwościach fizycznych zgodnych z wymaganiami dla kart identyfikacyjnych formatu ID-1 określonymi w normie ISO/IEC 7810, a ich właściwości i odporność muszą być potwierdzone badaniami przeprowadzonymi zgodnie z wieloczęściową normą ISO/IEC 10373.
      1.3.1.Karty nie mogą być wygięte, zniekształcone, porysowane, sklejone lub zabrudzone. Laminat po obydwu stronach kart płynnie przykrywa wszystkie zniekształcenia powierzchni, szczególnie w miejscu umieszczenia układów elektronicznych.

1.3.2. Producent kart spełnia wymagania ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych dla podmiotu , którego przedmiotem działalności jest wytwarzanie blankietów dokumentów i druków zabezpieczonych, które spełniają wymagania dotyczące bezpieczeństwa wytwarzania blankietów dokumentów publicznych kategorii trzeciej.

1.3.3. Blankiet spełniana minimalne wymagań dla dokumentów publicznych kategorii trzeciej.

1.4. System operacyjny karty:

1.4.1. jest zgodny ze standardem *Global Platform Card Specification* w wersji 2.1.1 lub wyższej,

1.4.2. jest oparty o maszynę wirtualną Java (*JavaCard)* w wersji 2.2 lub wyższej,

1.4.3. zapewnia wieloaplikacyjność,

1.4.4. obsługuje interfejsy stykowy i bezstykowy karty,

1.4.5. umożliwia wprowadzanie obiektów (aplikacji, plików) zapewniając bezpieczną komunikację,

1.4.6. poziom bezpieczeństwa systemu operacyjnego karty zweryfikowany na poziomie ITSEC E3 High lub Common Criteria (CC) EAL4+ lub FIPS 140 - 2 Level 3.

1.5. Bezpieczna komunikacja z kartą jest realizowana przy użyciu protokołu SCP01 lub SCP02.

1.5.1. Dla kart opartych o maszynę wirtualną Java (*JavaCard*) w wersji 2.2.2 i wyższej obsługiwane są podstawowe kanały logiczne (obsługa CLA=C0/D0 jak „proprietary class").

1.6. Na karcie preinstalowane są aplety:

1.6.1. zarządzanie kartą (Card Manager),

1.6.2. (opcjonalnie) system plików zgodny z ISO IEC 7816-4,

1.6.2.1. struktura plików karty jest zgodna z normą ISO/IEC 7816-4,

1.6.2.2. system plików skonfigurowany w taki sposób, że bezpośrednio po resecie karty możliwy jest wybór aplikacji DF.SELS (SELECT FILE DF.SELS),

1.6.3. (opcjonalnie) aplet zapewniający wykorzystanie karty w środowisku infrastruktury klucza publicznego:

1.6.3.1. ochrona obiektów i realizacji funkcji kryptograficznych kodami PIN i PUK,

1.6.3.2. domyślnie blokada kodu PIN po trzykrotnym kolejnym błędnym podaniu tego kodu, domyślnie blokada kodu PUK po dziesięciokrotnym kolejnym błędnym podaniu tego kodu. Karta powinna mieć możliwość zmiany parametrów PIN/PUK w trakcie personalizacji: wartości PIN i PUK, liczby prób dla PIN i PUK, minimalnej i maksymalnej długości,

1.6.3.3. dostęp do kluczy prywatnych zapisanych na karcie jest możliwy tylko po pozytywnej weryfikacji kodu PIN użytkownika chroniącego dany klucz prywatny,

1.6.3.4. możliwa zmiana kodu PIN po podaniu kodu PUK,

1.6.3.5. składanie podpisu elektronicznego z wykorzystaniem certyfikatu niekwalifikowanego (MS CSP, PKCS#11),

1.6.3.6. sprzętowe zabezpieczenie komputera, wyjęcie karty z czytnika powoduje zablokowanie dostępu do komputera, umieszczenie karty w czytniku i podanie kodu PIN powoduje odblokowanie dostępu do komputera,

1.6.4. (opcjonalnie) inne aplety, w tym w szczególności obsługujących płatności realizowane przez międzynarodowe organizacje płatnicze.

1.6.5. Profil karty i ustawienia poszczególnych apletów należy uzgodnić przed dostarczeniem pierwszej partii blankietów.

1.7. Karta zapewnia co najmniej:

1.7.1. generowanie kluczy kryptograficznych o długości co najmniej 2048 bitów przeznaczonych do użycia przez algorytm RSA, generowanie kluczy następuje w oparciu o generator liczb losowych oparty na zjawisku fizycznym,

1.7.2. obsługę funkcji skrótu SHA-1, SHA-256 i SHA-512,

1.7.3. podpisywanie, szyfrowanie i deszyfrowanie przy użyciu algorytmów DES, 3DES, AES o długości klucza do 128 bitów, RSA o długości klucza do 2048 bitów,

1.7.4. obsługę mechanizmu CRC16 wg normy ISO/IEC 3309.

1.8. Dostęp do kluczy prywatnych zapisanych na karcie możliwy jest wyłącznie przez koprocesor kryptograficzny. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego zapisanego na karcie wykonywane muszą być ramach maszyny wirtualnej Java i aplikacji pracujących na karcie.

2. Oprogramowanie

2.1. Dla kart zawierających aplet zapewniający wykorzystanie karty w środowisku infrastruktury klucza publicznego oprogramowanie umożliwiające zarządzanie kartą przez użytkownika, tj.: zmianę wartości PIN/PUK, generowanie kluczy i żądania certyfikacji, import certyfikatów, usunięcie certyfikatów i kluczy.

3. Zabezpieczenia na czas dostawy

3.1. Każda partia kart jest dostarczana z ustalonymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej (dostęp do układu procesorowego).