Wymagania techniczno-funkcjonalne dla karty elektronicznej – blankietu ELS

Przedmiotem zamówienia jest zakup wstępnie zadrukowanych blankietów ELS.
Karty muszą być wykonane z materiału laminowanego nieulegającemu odkształceniu i rozwarstwieniu o wymiarach i właściwościach fizycznych zgodnych z wymaganiami dla kart identyfikacyjnych formatu ID-1 określonymi w normie ISO/IEC 7810, a jego właściwości i odporność muszą być potwierdzone badaniami przeprowadzonymi zgodnie z wieloczęściową normą ISO/IEC 10373.
Blankiety nie mogą być wygięte, zniekształcone, porysowane oraz sklejone. Laminat po obydwu stronach karty płynnie przykrywa wszystkie zniekształcenia powierzchni – zwłaszcza w miejscu wprasowywania chipów.

Wygląd legitymacji

Wygląd blankietu ELS określa załącznik nr 3 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16 września 2016 r. w sprawie dokumentacji przebiegu studiów (Dz. U. 2016 nr poz. 1554).
Białe pole po stronie rewersowej jest położone w stosunku do brzegów karty z dokładnością +/- 0,5 mm w poziomie i 23,5 mm w pionie.

Karta procesorowa:

Elektroniczna hybrydowa karta procesorowa o pojemności pamięci nieulotnej EEPROM, co najmniej 24 kilobajtów z dwoma interfejsami:

I. Stykowym:
   1) określonym w normach ISO/IEC 7816-1, ISO/IEC 7816-2 i ISO/IEC 7816-3,
   2) polecenia i odpowiedzi przesyłane podczas komunikacji Karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4,
   3) polecenia realizowane przez Kartę dla operacji kryptograficznych i zarządzania muszą być zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9 oraz ISO/IEC 7816-15;

II. Bezstykowym:
   1) 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),
   2) spełniającym wymagania normy ISO/IEC 14443-1, ISO/IEC 14443-2, ISO/IEC 14443-3 przy zachowaniu pełnej antykolizyjności,
   3) polecenia i odpowiedź przesyłane podczas komunikacji karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z określoną w normie ISO/IEC 14443 - 4 oraz umożliwiać realizację poleceń APDU ze zbioru określonego dla interfejsu stykowego (protokół T = CL).

Układ procesorowy:

1) Preinstalowane aplety:
   a. Card Management i API zgodne z Global Platform w wersji 2.1 lub wyższej,

   b. system plików ISO IEC 7816,
   c. funkcjonalność PKCS #11.
2) Karta musi pozwalać na zarządzanie pamięcią EEPROM poprzez:
   usuwanie apletów/pakietów;
   udostępnianie pamięci zwolnionej po usunięciu apletu/pakietu;
   defragmentację luk w pamięci EEPROM.
3) Generowanie kluczy kryptograficznych o długości do 2048 bitów (co najmniej 1024 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.
4) Karta przystosowana do założenia instancji i utworzenia w ramach tej instancji struktury umożliwiającej umieszczenia na niej certyfikatu kwalifikowanego wraz z kluczami kryptograficznymi oraz certyfikatu niekwalifikowanego wraz z kluczami kryptograficznymi; certyfikaty mogą zostać umieszczone w późniejszym czasie. Ilość certyfikatów możliwych do umieszczenia na Karcie ograniczona jest jedynie pojemnością Karty.
5) Karta przystosowana do zapewnia niezależnej i oddzielnej realizacji operacji:
   a. składania podpisu elektronicznego z wykorzystaniem certyfikatu umieszczonego na karcie: kwalifikowanego lub niekwalifikowanego (MS CSP, PKCS#11);
   b. sprzętowego zabezpieczenia komputera (za pomocą osobnej aplikacji): wyjęcie karty z czytnika – zablokowanie dostępu do komputera, włożenie karty do czytnika i podanie kodu PIN - odblokowanie dostępu do komputera.
6) Dostęp do klucza prywatnego zapisanego na karcie możliwy jest wyłącznie przez koprocesor kryptograficzny karty. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane są na karcie. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika.
7) Dostęp do każdej z operacji wymienionych w powyższych punktach zabezpieczony oddzielnymi kodami PIN i PUK, blokada kodu PIN po trzykrotnym kolejnym błędnym podaniu tego kodu, blokada kodu PUK po trzykrotnym kolejnym błędnym podaniu tego kodu.

Kompatybilność

Zamawiający wymaga, żeby blankiety współpracowały z posiadanymi przez Zamawiającego drukarkami Evolis Securion SMART & CONTACTLESS.

Karta ma być obsługiwana przez system USOS oraz powinna posiadać aplety takie same jak użytkowane obecnie przez Uczelnię (aplet PKI GEMSAFE oraz aplet systemu operacyjnego MPCOS). Lista kart obsługiwanych przez system USOS zawarta jest w załączniku 2B do SIWZ.

Dokumentacja

Dostawca Karty udostępnia Zamawiającemu, w ciągu 7 dni od daty zawarcia umowy, dokumentację umożliwiającą programowanie karty.

Zabezpieczenia na czas dostawy

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