Opis przedmiotu zamówienia

Załącznik nr 2

Wymagania techniczno-funkcjonalne dla karty elektronicznej – blankietu ELS

Karta procesorowa

Wstępnie zadrukowany blankiet ELS jest elektroniczną hybrydową kartą procesorową o pojemności pamięci nieulotnej typu EEPROM, co najmniej 36 kilobajtów z dwoma interfejsami:

1. stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3,
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).

Karty wykonane są z materiału laminowanego nieulegającemu odkształceniu i / lub 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.

Wygląd legitymacji

Wygląd blankietu ELS określa załącznik nr 3 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 02 listopada 2006 r. w sprawie dokumentacji przebiegu studiów (Dz. U. 2006 nr 224 poz. 1634).

Białe pole po stronie rewersowej jest położone w stosunku do brzegów karty z dokładnością +/- 0,5 mm. Blankiety nie mogą być wygięte, zniekształcone, porysowane oraz sklejone. Laminat po obydwu stronach karty płynnie przykrywa wszystkie zniekształcenia powierzchni – zwłaszcza w miejscu wprasowywania chipów.

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.

System operacyjny z maszyną wirtualną Java (*JavaCard*) w wersji 2.1 lub wyższej, zapewniający wieloaplikacyjność, obsługujący interfejs stykowy, a w przypadku Karty dualnej – również interfejs bezstykowy, umożliwiający wprowadzanie obiektów (tzn. aplikacji, plików) w bezpiecznym środowisku. Card Management i API zgodne z Global Platform 2.0.1' lub wyższą.

Blankiet ELS jest gotowy do stosowania 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, rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego – Dz. Ustaw 2002 nr 128 poz. 1094), w szczególności posiadać co najmniej jeden z niżej wymienionych certyfikatów zgodności:

1. 1. ITSEC v 1.2 dla poziomu E3 z minimalną siłą mechanizmów zabezpieczających, określoną jako „wysoka", albo poziomu bezpieczniejszego, lub
2. norma FIPS PUB 140 Security Requirements for Cryptographic Modules, wydana przez National Institute of Standards and Technology dla poziomu 3 albo bezpieczniejszego, lub
3. norma ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security, wydaną przez International Organization for Standardization dla poziomu EAL4 albo bezpieczniejszego.

Blankiet ELS musi spełniać następujące wymagania:

1. Układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard, EAL5+.

2. W przypadku zgodności z normą ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security Karta musi posiadać certyfikat Common Criteria Standard według profilu PPSSCD Protection Profile – Secure Signature Creation Device Type 2 and/or 3, version 1.05, dla poziomu EAL4+ (CWA14169).
3. W przypadku zgodności z normą ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security Karta musi być zgodna ze standardem funkcjonalności E-Sign K (CWA14890).
4. DAP zgodne z Global Platform 2.1 (PK-Based).
5. Obsługiwane protokoły: T=0, T=1, PPS.
6. Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez wbudowany koprocesor kryptograficzny Karty.
7. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na Karcie.
8. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika.
9. Blankiet ELS musi pozwalać na zarządzanie pamięcią EEPROM poprzez: usuwanie apletów/pakietów, udostępnianie pamięci zwolnionej po usunięciu apletu/pakietu i defragmentację luk w pamięci EEPROM.
10. Generowanie kluczy kryptograficznych o długości co najmniej 1024 bitów przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA, obsługa funkcji skrótu SHA-1, szyfrowanie i deszyfrowanie za pomocą algorytmu RSA, obsługa algorytmów DES, 3DES (ECB, CBC).
11. Karta przystosowana do założenia instancji i utworzenia w ramach tej instancji struktury umożliwiającej na niej 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.
12. Karta przystosowana według pkt 11 zapewnia niezależne i oddzielne realizacje operacji:
    - składania podpisu elektronicznego z wykorzystaniem certyfikatu niekwalifikowanego (MS CSP, PKCS#11);
    - składania podpisu elektronicznego z wykorzystaniem certyfikatu kwalifikowanego;
    - 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.
13. 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.

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.

Kompatybilność
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).

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.