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 (Dz.U. z 2021 r. poz. 661 t.j.)
      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 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. Dokumentacja
   2.1. specyfikacja techniczna karty,
   2.2. dokumentacja techniczna preinstalowanych pakietów i apletów, w szczególności zawierająca opis realizowanych poleceń i odpowiedzi APDU,
   2.3. dokumentacja techniczna oprogramowania dostarczanego z kartą,
   2.4. potwierdzenie producenta karty o spełnieniu wymagań dla podmiotu, którego przedmiotem działalności jest wytwarzanie blankietów dokumentów i druków zabezpieczonych, które spełniają wymagania dotyczące bezpieczeństwa wytwarzania blankietów dokumentów publicznych kategorii trzeciej,
   2.5. potwierdzenie producenta karty o spełnianiu przez blankiet minimalnych wymagań dla dokumentów publicznych kategorii trzeciej.

3. Oprogramowanie
   3.1. 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.

4. Zabezpieczenia na czas dostawy
   4.1. Każda partia kart jest dostarczana z ustalonymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej (dostęp do układu procesorowego).

Załącznik nr 1a

Wyciąg z rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz. U. z 2021 r. poz. 661 t.j.)

ZAŁĄCZNIK Nr 1

WZÓR LEGITYMACJI STUDENCKIEJ

Opis:

1. Elektroniczna legitymacja studencka jest elektroniczną kartą procesorową z interfejsem stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3. Elektroniczna legitymacja studencka może zawierać również inne interfejsy, w tym interfejs bezstykowy.
2. Blankiet elektronicznej legitymacji studenckiej jest wykonany z materiału laminowanego 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.
3. Poddruk blankietu elektronicznej legitymacji studenckiej wykonany w technice offsetowej w standardzie 5 + 4 (CMYK i Pantone 5555 na awersie oraz CMYK na rewersie) jest chroniony zewnętrzną folią laminacyjną. W procesie zadrukowywania blankietu (poddruk offsetowy) są nanoszone następujące elementy:
   1) tło z elementami grafiki rastrowej w kolorach CMYK;
   2) zabezpieczające elementy wykonane techniką giloszową w formie stylizowanego, powtarzalnego ornamentu geometrycznego wydrukowanego linią o grubości 0,075 pkt w kolorze Pantone 5555 umieszczone na pasie o szerokości 22,7 mm przebiegającym wzdłuż prawego boku legitymacji w odległości 3,8 mm od krawędzi, na całej jej wysokości, włącznie z polem przeznaczonym pod druk zdjęcia;
   3) napis "LEGITYMACJA STUDENCKA" wykonany w technice mikrodruku, na białym pasku o szerokości 1 mm przebiegającym poziomo w odległości 1,7 mm od dolnej krawędzi legitymacji, w kolorze czarnym;
   4) wizerunek orła ustalony dla godła Rzeczypospolitej Polskiej o wysokości 8,5 mm i napis "RZECZPOSPOLITA POLSKA" wykonany krojem Palm Springs Bold o wielkości 5 pkt, w kolorze czarnym;
   5) napisy:
      a) "LEGITYMACJA STUDENCKA" wykonany krojem Aura Ibis o wielkości 12,5 pkt, w kolorze granatowym (C100, M70, Y25, K20),
      b) "STUDENT CARD" wykonany krojem Aura Ibis o wielkości 9,7 pkt, w kolorze granatowym (C100, M70, Y25, K20),
      c) "Wydana:", "Nr albumu:", "PESEL:", "Legitymacja ważna do:" wykonane krojem Arial Narrow o wielkości 7 pkt, w kolorze czarnym,
      d) "Poświadcza uprawnienia do 50% ulgi przy przejazdach środkami komunikacji miejskiej, a także uprawnienia do korzystania - do ukończenia 26 roku życia - z ulgowych przejazdów środkami publicznego transportu zbiorowego

autobusowego i kolejowego na podstawie odrębnych przepisów." wykonany krojem Arial Narrow Bold o wielkości 6 pkt, w kolorze czarnym;

6) biały obszar przeznaczony na zdjęcie posiadacza legitymacji o wymiarach 20 mm x 25 mm, w odległości 5 mm w poziomie i 23,5 mm w pionie;
7) 12 pól o wymiarach 8 mm x 9 mm, oznaczonych kolejno liczbami od 1 do 12 wykonanymi krojem Arial o wielkości 5 pkt, w kolorze czarnym;
8) biały obszar o wymiarach 30 mm x 21 mm przeznaczony na naniesienie kodu kreskowego - jeżeli w uczelni kod kreskowy nie jest stosowany, obszar może być wykorzystany w sposób określony przez uczelnię.

4. W procesie personalizacji elektronicznej legitymacji studenckiej są nanoszone w sposób zapewniający trwałe i bezpieczne użytkowanie następujące dane:
   1) kolorowe zdjęcie posiadacza legitymacji o wymiarach 20 mm x 25 mm w rozdzielczości co najmniej 300 dpi;
   2) nazwa uczelni wykonana krojem Arial Narrow Bold o wielkości 7 pkt, w dwóch lub trzech wierszach, do 30 znaków w wierszu, wyjustowana do prawej strony; notacja: **"Pierwsze Litery Wielkie";** pozycjonowanie: 27,2 mm w poziomie, licząc od prawej krawędzi bloku tekstu, 6,2 mm w pionie, licząc od górnej krawędzi bloku tekstu, w kolorze czarnym;
   3) imię do 24 znaków oraz nazwisko w dwóch wierszach, do 28 znaków każdy, wykonane krojem Arial Narrow o wielkości 8 pkt, wyjustowane centralnie; notacja: **"Pierwsze Litery Wielkie";** pozycjonowanie: oś pionowa tekstu 43,6 mm w poziomie i 24 mm w pionie, licząc od górnej krawędzi bloku tekstu, w kolorze czarnym;
   4) data wydania wykonana krojem Arial Narrow o wielkości 7 pkt, w kolorze czarnym;
   5) nr albumu wykonany krojem Arial Narrow o wielkości 7 pkt, w kolorze czarnym;
   6) numer PESEL (dla obcokrajowców data urodzenia w formacie rrmmdd00000, kodowanie tysięcy i setek lat zgodnie z zasadami systemu PESEL) wykonany krojem Arial Narrow o wielkości 7 pkt, w kolorze czarnym;
   7) kod kreskowy (opcjonalnie) w kolorze czarnym.
5. Wszystkie parametry pozycjonowania liczone są do prawego górnego rogu karty.
6. Podczas etapu personalizacji graficznej dane są zapisywane w układzie scalonym karty.
7. Struktura danych zawartych w układzie scalonym elektronicznej legitymacji studenckiej jest zgodna z normą ISO/IEC 7816-4.
8. Polecenia i odpowiedzi przesyłane podczas komunikacji karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
9. Elektroniczna legitymacja studencka zawiera w pamięci obowiązkowo plik DF.SELS oraz dwa pliki potomne: EF.CERT i EF.ELS. Plik DF.SELS jest dostępny za pomocą polecenia SELECT FILE bezpośrednio po resecie karty. Plik DF.SELS może także zawierać plik potomny EF.PHOTO o dwubajtowym identyfikatorze, którego wartość jest wskazana w polu efPhotoId struktury opisanej w ust. 12 pkt 2 lit. b, zawierający cyfrowy zapis w formacie JPG fotografii umieszczonej podczas procesu personalizacji na awersie elektronicznej legitymacji studenckiej.
10. Dane związane z elektroniczną legitymacją studencką powinny być zlokalizowane w pliku dedykowanym DF.SELS, którego nazwa jest zarejestrowanym w Polskim Komitecie Normalizacyjnym identyfikatorem aplikacji określonym zgodnie z normą ISO/IEC 7816-5+A1. Własne rozszerzenie identyfikatora aplikacji (PIX) dla elektronicznej legitymacji studenckiej jest równe "01 01" (zapis w systemie szesnastkowym).

11. Plik DF.SELS musi być dostępny bezpośrednio po resecie karty elektronicznej za pomocą polecenia wyboru, którego parametrem jest pełna nazwa tego pliku (AID wraz z rozszerzeniem).
12. Obligatoryjnymi potomnymi plikami elementarnymi dla pliku DF.SELS są dwa pliki o przezroczystej strukturze binarnej:
    1) plik EF.CERT o dwubajtowym identyfikatorze "00 01" (zapis w systemie szesnastkowym), zawierający kwalifikowany certyfikat podpisu elektronicznego albo kwalifikowany certyfikat pieczęci elektronicznej, w którym:
        a) w polu "właściciel certyfikatu" znajdują się następujące atrybuty: "nazwa organizacji", "nazwa województwa", "nazwa miejscowości" i "adres", które dotyczą uczelni,
        b) w przypadku kwalifikowanego certyfikatu podpisu elektronicznego w polu "właściciel certyfikatu" w atrybucie "nazwa powszechna" zawarto sformułowanie: "osoba upoważniona do wystawiania legitymacji studenckiej";
    2) plik EF.ELS o dwubajtowym identyfikatorze "00 02" (zapis w systemie szesnastkowym) zawierający wiadomość w formacie zgodnym z normą europejską ETSI EN 319 122-1, opatrzoną kwalifikowanym podpisem elektronicznym albo kwalifikowaną pieczęcią elektroniczną, przy czym:
        a) format podpisanej wiadomości to "podpis bazowy w formacie CAdES o poziomie B-B", w którym eContentType wewnątrz struktury SignedData zawiera id-SELSInfo o następującym identyfikatorze obiektu:
        1d-SELSInfo OBJECT IDENTIFIER::= iso(1) member-body(2) pl(616) organization(1) gov(101) moneas(4) pki(1) sels(1) 1,
        b) podpisywane dane (SELSInfo) są umieszczone w eContent wewnątrz struktury SignedData i mają następującą składnię:

SELSInfo::= SEQUENCE

wersja	**INTEGER v1(1)**
numerSeryjnyUkladu	**PrintableString (SIZE (8..16)),**
nazwaUczelni	**UTF8String (SIZE (1..128)),**
nazwiskoStudenta	**SEQUENCE OF UTF8String (SIZE (1..28)),**
imionaStudenta	**SEQUENCE OF UTF8String (SIZE (1..24)),**
numerAlbumu	**PrintableString (SIZE (1..16)),**
numerEdycji	**PrintableString (SIZE (1)),**
numerPesel	**PrintableString (SIZE (11)),**
dataWaznosci	**GeneralizedTime,**

albo:

SELSInfo::= SEQUENCE

wersja	**INTEGER v2(2),**
numer SeryjnyUkladu	**PrintableString (SIZE (8..16)),**
nazwaUczelni	**UTF8String (SIZE (1..128)),**
nazwiskoStudenta	**SEQUENCE OF UTF8String (SIZE (1..28)),**
imionaStudenta	**SEQUENCE OF UTF8String (SIZE (1..24)),**

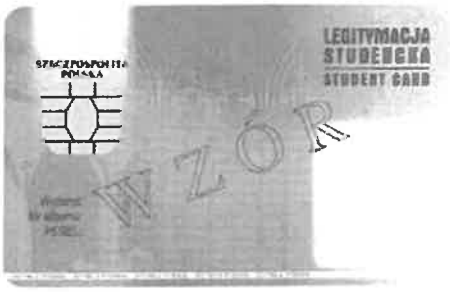
numerAlbumu	**PrintableString (SIZE (1..16)),**
numerEdycji	**PrintableString (SIZE (1)),**
numerPesel	**PrintableString (SIZE (11)),**
dataWaznosci	**GeneralizedTime,**
dataWydania	**GeneralizedTime,**
urlUniewaznienia	**UTF8String (SIZE (1..128)),**
funkcjaSkrotu	**OBJECT IDENTIFIER,**
skrotZdjecia	**BIT STRING,**
efPhotoId	**OCTET STRING**

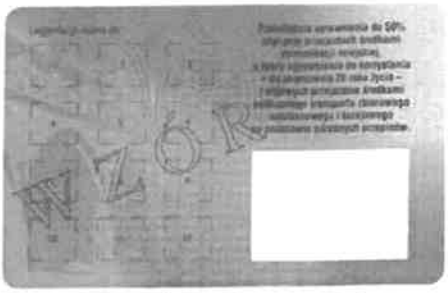
określoną za pomocą notacji ASN.1 opisanej w normie ISO/IEC 8824; poszczególne pola należy interpretować następująco:

- wersja zawiera numer wersji struktury podpisywanych danych; pole to umożliwi łatwe rozpoznawanie ewentualnych nowych wersji struktur danych zawartych w elektronicznej legitymacji studenckiej,
- numerSeryjnyUkladu to unikatowy numer nadawany przez producenta układu scalonego zapisany w formacie heksadecymalnym; podczas zapisywania danych w układzie elektronicznym karty aplikacja dokonująca zapisu weryfikuje jego zgodność z numerem seryjnym odczytanym z karty,
- nazwaUczelni to oficjalnie zarejestrowana nazwa uczelni,
- nazwisko Studenta to dane zgodne z informacją wpisaną do dowodu osobistego lub paszportu studenta,
- imionaStudenta to dane zgodne z informacją wpisaną do dowodu osobistego lub paszportu studenta,
- numerAlbumu, to nadany studentowi numer, o którym mowa w § 14 ust. 1 rozporządzenia,
- numerEdycji to literowe oznaczenie egzemplarza legitymacji o tym samym numerze albumu; pierwszy egzemplarz jest oznaczony literą A, kolejne literami B, C, D...,
- numerPesel to numer studenta z Powszechnego Elektronicznego Systemu Ewidencji Ludności,
- dataWaznosci to data, po upływie której elektroniczna legitymacja studencka traci ważność; jest modyfikowana co semestr przez umieszczenie w kolejno oznaczonych polach legitymacji hologramu określonego w załączniku nr 2 do rozporządzenia,
- dataWydania to data wydania legitymacji, zgodna z datą, która została umieszczona na awersie elektronicznej legitymacji studenckiej w procesie personalizacji,
- urlUniewaznienia to adres umożliwiający sprawdzenie czy legitymacja została unieważniona; dane odczytane z tego adresu dla legitymacji unieważnionej muszą być równe ciągowi znaków "UNIEWAZNIONA", np. https://nazwaSerwisu.domenaUczelni/numerSeryjnyUkladu; w przypadku legitymacji ważnych może być zwrócony ciąg znaków "WAZNA" lecz nie jest to obligatoryjne; adres urlUniewaznienia nie musi przedstawiać informacji o legitymacjach ważnych; w adresie urlUniewaznienia do identyfikacji elektronicznej legitymacji studenckiej może być wykorzystany jedynie numerSeryjnyUkladu;
- funkcjaSkrotu to identyfikator obiektu wskazującego funkcję skrótu, która została użyta do wyliczenia wartości zapisanej w skrotZdjecia, np. dla SHA-

256 joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1),
- skrotZdjecia to wartość skrótu z pliku EF.PHOTO wyliczona za pomocą algorytmu wskazanego w funkcjaSkrotu,
- efPhotoId to dwubajtowy identyfikator pliku potomnego EF.PHOTO np. "00 04" (zapis w systemie szesnastkowym),

c) w formacie podpisywanej wiadomości zostaną umieszczone, jako podpisane atrybuty:
- atrybuty obligatoryjne według normy europejskiej ETSI EN 319 122-1,
- atrybut "deklarowany czas złożenia podpisu" (ang. signing-time), zawierający czas złożenia podpisu kodowany zgodnie z typem GeneralizedTime; czas ten nie może być wcześniejszy niż 9 miesięcy od daty zawartej w polu dataWaznosci, o którym mowa w lit. b,
- atrybut "rodzaj zobowiązania" zawierający identyfikator obiektu: commitmentType OBJECT IDENTIFIER::= iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 16 6 5,
wskazujący, że podpisujący zaaprobował podpisywane dane.





ZAŁĄCZNIK Nr 1

WZÓR ELEKTRONICZNEJ LEGITYMACJI STUDENCKIEJ

Wyciąg z rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz. U. z 2021 r. poz. 661 t.j.)