Załączniki do rozporządzenia Ministra Spraw Wewnętrznych i Administracji

z dnia ……. (Dz. U. ..….)

**Wymagania techniczne dla warstwy elektronicznej dowodu osobistego**

**I.**

1. Warstwę elektroniczną dowodu osobistego stanowią:
   1. mikroprocesor;
   2. biblioteka kryptograficzna;**Załącznik nr 1**

**II.**

**III.**

**IV.**

* 1. platforma operacyjna, w tym środowisko oprogramowania Java oraz dedykowane oprogramowanie;
  2. interfejs bezstykowy zgodny z normą ISO/IEC 14443 typ A lub B;
  3. aplet lub aplety Java, odpowiadające za funkcjonalności określone w art. 12a ustawy   
     z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671 oraz z 2023 r. poz. 1234 i 1941), zwanej dalej „ustawą”.

1. Warstwa elektroniczna dowodu osobistego może być zbudowana z komponentów w innej konfiguracji niż określona w pkt 1, które łącznie spełniają takie same wymagania bezpieczeństwa i poziomu uzasadnienia zaufania.
2. Warstwa elektroniczna dowodu osobistego wraz z dokumentacją ją opisującą stanowi łącznie przedmiot oceny w rozumieniu normy PN-EN ISO/IEC 15408 lub normy równoważnej.
3. Warstwa elektroniczna dowodu osobistego podlega ocenie bezpieczeństwa zgodnie z wymaganiami zawartymi w normie PN-EN ISO/IEC 15408 lub normie równoważnej.
4. Oceny bezpieczeństwa i certyfikacji dokonuje się na zgodność z profilem zabezpieczeń (ang. Protection Profile) lub na zgodność ze specyfikacją techniczną (ang. Security Target) warstwy elektronicznej dowodu osobistego.
5. Certyfikacji dokonuje jednostka certyfikująca, która zapewnia uznanie certyfikatu zgodnie   
   z porozumieniami międzynarodowymi: Porozumieniem o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA lub umową w sprawie uznawania certyfikatów Common Criteria - SOGIS-MRA lub Europejskim schematem certyfikacji cyberbezpieczeństwa zgodnym z Common Criteria (EUCC).
6. Profil zabezpieczeń, o którym mowa w [pkt II. 2,](#_bookmark1) jest dokumentem publicznie dostępnym, publikowanym przez niezależne od producenta warstwy elektronicznej jednostki zajmujące się certyfikacją.
7. Specyfikacja techniczna warstwy elektronicznej dowodu osobistego jest zgodna z profilem zabezpieczeń, o którym mowa w pkt 1, jeśli ten profil zabezpieczeń został opracowany.
8. Specyfikacja techniczna warstwy elektronicznej dowodu osobistego w części, w której opisano szczegółowy sposób realizacji wymagań bezpieczeństwa, może stanowić tajemnicę przedsiębiorstwa w rozumieniu przepisu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r.   
   o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233).
9. W przypadku gdy ocena bezpieczeństwa warstwy elektronicznej prowadzona jest jako ocena złożona (ang. Composite Evaluation), wymagane jest, aby specyfikacja techniczna zawierała opisy:
   1. spójności polityki bezpieczeństwa produktu złożonego;
   2. sposobu integracji poszczególnych komponentów tego produktu;
   3. procedur dostaw poszczególnych komponentów;
   4. spójności wewnętrznej projektu produktu złożonego;
   5. testów funkcjonalnych produktu złożonego;
   6. oceny podatności na zagrożenia.
10. Dopuszcza się, że poszczególne komponenty warstwy elektronicznej dowodu osobistego będącego przedmiotem oceny bezpieczeństwa mogą mieć certyfikaty uprzednio wydane przez jednostkę certyfikującą, o której mowa w pkt II. 3.

**V.**

1. Ocena bezpieczeństwa mikroprocesora jest dokonywana na poziomie uzasadnionego zaufania do zgodności z wymaganiami na poziomie nie niższym niż EAL5, zgodnie z normą PN-EN ISO/IEC 15408 lub normą równoważną, rozszerzonym o komponenty uzasadnienia zaufania zgodnie   
   z normą PN-EN ISO/IEC 15408 lub normą równoważną, obejmujące co najmniej AVA\_VAN.5, ALC\_DVS.2.
2. Ocena bezpieczeństwa platformy operacyjnej jest dokonywana na poziomie uzasadnionego zaufania do zabezpieczeń nie niższym niż poziom EAL5, zgodnie z normą PN-EN ISO/IEC 15408 lub normą równoważną, rozszerzonym o komponenty uzasadnienia zaufania zgodnie z normą PN-EN ISO/IEC 15408 lub normą równoważną, obejmujące co najmniej AVA\_VAN.5, ALC\_DVS.2.
3. Ocena bezpieczeństwa apletu jest dokonywana na poziomie uzasadnionego zaufania do zabezpieczeń nie niższym niż poziom EAL4, zgodnie z normą PN-EN ISO/IEC 15408 lub normą równoważną, rozszerzonym o komponenty uzasadnienia zaufania zgodnie z normą PN-EN ISO/IEC 15408 lub normą równoważną, obejmujące co najmniej AVA\_VAN.5, ALC\_DVS.2.

**VI.**

Mikroprocesor spełnia następujące minimalne wymagania:

1. utrzymanie integralności danych użytkownika, które są przetwarzane i przechowywane   
   w pamięci mikroprocesora;
2. utrzymanie poufności danych użytkownika, które są przetwarzane i przechowywane   
   w pamięci mikroprocesora;
3. zapewnienie poprawności wszystkich funkcji bezpieczeństwa realizowanych przez mikroprocesor;
4. zapewnienie losowego generowania liczb w celu realizacji funkcji kryptograficznych;
5. zapewnienie ochrony przed wyciekiem informacji wynikającym zarówno z realizacji wewnętrznych operacji mikroprocesora, jak i umyślnych działań atakującego;
6. zapewnienie ochrony przed fizyczną ingerencją umożliwiającą odczytanie danych użytkownika przechowywanych w pamięci mikroprocesora;
7. zapewnienie wykrywania prób wymuszenia realizacji operacji mikroprocesora oraz przeciwdziałania takim próbom w sytuacjach, w których niezawodność i bezpieczeństwo tych operacji nie były testowane lub udowodnione;
8. zapewnienie ochrony przed fizycznymi manipulacjami wpływającymi na operacje mikroprocesora, w tym na oprogramowanie mikroprocesora, dane wykorzystywane do realizacji funkcji bezpieczeństwa oraz dane użytkownika;
9. zapewnienie ochrony przed nieuprawnionym użyciem funkcji dedykowanych do testowania mikroprocesora oraz innych komponentów, blokowanych po zakończeniu fazy testowania urządzenia;
10. zapewnienie identyfikacji mikroprocesora, tzn. umieszczenie danych inicjujących oraz danych przed personalizacją w nieulotnej pamięci mikroprocesora.

**VII.**

Mikroprocesor lub mikroprocesor wraz z implementacją bibliotek kryptograficznych spełnia następujące wymagania:

1. realizuje sprzętowe funkcje szyfrowania AES;
2. obsługuje następujące algorytmy kryptograficzne:
   1. symetryczne: AES,
   2. asymetryczne: RSA, ECDSA, w tym generowania lub obliczania par kluczy,
   3. wymianę kluczy: DHKE,
   4. funkcję skrótu: SHA-224, SHA-256, SHA-384, i SHA-512;
3. w odniesieniu do algorytmów kryptograficznych ECDSA i RSA – zapewnia składanie   
   i weryfikację podpisu;
4. realizuje funkcje kryptograficzne wymagające kopiowania, porównywania, powtórnego użycia określonych obszarów pamięci operacyjnej, zapewnia ochronę przed podatnościami znanymi w momencie wykonania oceny bezpieczeństwa;
5. zapewnia środki bezpieczeństwa przed pozostawieniem informacji szczątkowych w pamięci operacyjnej po zrealizowaniu funkcji kryptograficznej.

**VIII.**

Platforma operacyjna warstwy elektronicznej dowodu osobistego spełnia wymagania funkcjonalne   
i wymagania bezpieczeństwa określone w profilu zabezpieczeń, zawarte w dokumencie „Java Card Protection Profile - Open Configuration, Version 3.0, May 2012” (ANSSI-PP-2010/03-M01) lub nowszym, z zastrzeżeniem pkt I. 2.

**IX.**

1. Aplet w części realizującej funkcję bezpiecznego urządzenia do składania kwalifikowanego podpisu elektronicznego albo urządzenia do składania podpisu osobistego spełnia wymagania bezpieczeństwa określone w normie PN-EN 419211-2 albo w normie PN-EN 419211-3 lub normach je zastępujących.
2. Aplet w części realizującej funkcję dokumentu uznawanego zgodnie z odrębnymi przepisami za dokument podróży spełnia wymagania bezpieczeństwa określone w profilu zabezpieczeń BSI-CC-PP-0068-V2-2011, Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP); BSI-CC-PP-0056-V2-2012.
3. Aplet w części realizującej funkcje wskazane w art. 12a ust. 1 pkt 2–5 ustawy spełnia następujące wymagania bezpieczeństwa lub korzysta ze środków ochrony zapewnianych przez inne komponenty warstwy elektronicznej dowodu osobistego w celu spełnienia tych wymagań:
   1. zapewnia integralność danych użytkownika oraz danych służących do realizacji funkcji bezpieczeństwa podczas:
      1. przechowywania, tzn. zapewnienia ochrony tych danych przed nieuprawnioną modyfikacją lub manipulacją,
      2. wymiany danych między apletem a dostawcą usługi zewnętrznej, po uwierzytelnieniu terminala oraz warstwy elektronicznej dowodu osobistego;
   2. zapewnia autentyczność:
      1. danych użytkownika oraz danych służących do realizacji funkcji bezpieczeństwa podczas przechowywania, przez umożliwienie weryfikacji ich autentyczności po stronie terminala,
      2. danych użytkownika podczas ich wymiany między apletem a dostawcą usługi zewnętrznej, po uwierzytelnieniu terminala oraz warstwy elektronicznej dowodu osobistego;
   3. zapewnia poufność danych użytkownika oraz danych służących do realizacji funkcji bezpieczeństwa:
      1. przez nadanie praw do odczytu jedynie poprawnie uwierzytelnionym terminalom,   
         z określonym poziomem ich autoryzacji,
      2. podczas wymiany danych między apletem a dostawcą usługi zewnętrznej, po uwierzytelnieniu terminala oraz warstwy elektronicznej dowodu osobistego;
   4. zapewnia ochronę przed śledzeniem identyfikatora warstwy elektronicznej dowodu osobistego za pośrednictwem monitorowania interfejsu bezstykowego, w sytuacji gdy nie posiadał uprzednio informacji o poprawnych wartościach współdzielonych kodów (minimum CAN lub MRZ);
   5. zapewnia terminalowi, z którym nawiązywane jest połączenie, możliwość weryfikacji swojej autentyczności jako całego urządzenia dostarczonego przez wydawcę warstwy elektronicznej dowodu osobistego, za pomocą kryptograficznie potwierdzanych danych;
   6. zapewnia ochronę funkcji, które nie są używane w fazie operacyjnej, przed ich nadużywaniem w celu:
      1. zmanipulowania lub ujawnienia danych użytkownika lub danych służących do realizacji funkcji bezpieczeństwa, przechowywanych w warstwie elektronicznej dowodu osobistego,
      2. zmanipulowania (obejścia, zablokowania lub zmodyfikowania) funkcji bezpieczeństwa realizowanych programowo;
   7. zapewnia ochronę przed ujawnieniem danych użytkownika oraz danych służących do realizacji funkcji bezpieczeństwa, przechowywanych lub przetwarzanych, za pomocą:
      1. monitorowania i analizy poprawności operacji na poziomie sygnałowym, zarówno   
         w odniesieniu do operacji wewnętrznych, jak i na interfejsach zewnętrznych,
      2. wymuszania niepoprawnego działania funkcji w warunkach wykrycia ataku,
      3. wykrywania i reakcji na próby fizycznej manipulacji;
   8. zapewnia poufność i integralność danych użytkownika, danych służących do realizacji funkcji bezpieczeństwa oraz wbudowanego oprogramowania warstwy elektronicznej dowodu osobistego przed naruszeniem bezpieczeństwa fizycznego przez zastosowanie środków chroniących przed atakami polegającymi na:
      1. pomiarze napięcia lub natężenia prądu na stykach galwanicznych powierzchni układu scalonego, z wyłączeniem obwodów połączonych (z użyciem standardowych narzędzi pomiaru napięcia lub natężenia prądu),
      2. wykorzystaniu innych rodzajów fizycznego współdziałania ładunków elektrycznych,
      3. kontrolowanej manipulacji zawartością pamięci w celu pozyskania danych użytkownika lub danych służących do realizacji funkcji bezpieczeństwa

- bazując na uprzednim wykonaniu inżynierii wstecznej uzyskanego kodu binarnego.