

Warszawa, dnia 7 lipca 2022 r.

Poz. 1431

**OBWIESZCZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI**

z dnia 10 czerwca 2022 r.

**w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Spraw Wewnętrznych i Administracji
w sprawie warstwy elektronicznej dowodu osobistego**

1. Na podstawie art. 16 ust. 3 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461) ogłasza się w załączniku do niniejszego obwieszczenia jednolity tekst rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. poz. 400), z uwzględnieniem zmian wprowadzonych rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 września 2021 r. zmieniającym rozporządzenie w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. poz. 1831).

2. Podany w załączniku do niniejszego obwieszczenia tekst jednolity rozporządzenia nie obejmuje odnośników nr 2 i nr 3 oraz § 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 września 2021 r. zmieniającego rozporządzenie w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. poz. 1831), które stanowią:

- „²⁾ Niniejsze rozporządzenie służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się (Dz. Urz. UE L 188 z 12.07.2019, str. 67).
- ³⁾ Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu 16 kwietnia 2021 r. pod numerem 2021/229/PL, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), które wdraża dyrektywę (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241 z 17.09.2015, str. 1).”

„§ 2. Rozporządzenie wchodzi w życie z dniem określonym w komunikacie wydanym na podstawie art. 3a ustawy z dnia 14 kwietnia 2021 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw (Dz. U. poz. 1000 i 1393).”.

Minister Spraw Wewnętrznych i Administracji: *wz. P. Szefermaker*

**ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI¹⁾**

z dnia 26 lutego 2019 r.

w sprawie warstwy elektronicznej dowodu osobistego²⁾

Na podstawie art. 12j ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

- 1) wymagania techniczne dla warstwy elektronicznej dowodu osobistego;
- 2) sposób używania certyfikatów identyfikacji i uwierzytelnienia, podpisu osobistego i potwierdzenia obecności;
- 3) sposób przekazywania i używania kodu umożliwiającego odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego;
- 4) sposób i tryb zawieszania, cofania zawieszenia oraz unieważniania certyfikatów identyfikacji i uwierzytelnienia, podpisu osobistego i potwierdzenia obecności;
- 5) wzór zgłoszenia zawieszenia i cofnięcia zawieszenia certyfikatów identyfikacji i uwierzytelnienia, podpisu osobistego i potwierdzenia obecności;
- 6) wzór zaświadczenia potwierdzającego zgłoszenie zawieszenia lub cofnięcia zawieszenia certyfikatów identyfikacji i uwierzytelnienia, podpisu osobistego i potwierdzenia obecności.

Rozdział 2

Wymagania techniczne dla warstwy elektronicznej dowodu osobistego

§ 2. 1. Warstwa elektroniczna dowodu osobistego:

- 1)³⁾ obsługuje kody o długości minimalnej 4 cyfr, w tym kody z funkcją kodu początkowego dla każdego z kodów, w którego miejsce posiadacz dowodu osobistego ustala własne kody, o których mowa w art. 12b ust. 1 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, zwanej dalej „ustawą”:
 - a) dla certyfikatu identyfikacji i uwierzytelnienia, zwany dalej „kodem PIN1”, oraz
 - b) dla certyfikatu podpisu osobistego, zwany dalej „kodem PIN2”;
- 2) umożliwia zmianę kodu PIN1 i kodu PIN2 za pomocą dotychczasowego kodu PIN1 albo odpowiednio kodu PIN2, albo kodu odblokowującego, o którym mowa w art. 12b ust. 4 ustawy, zwanego dalej „kodem PUK”;

¹⁾ Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej – sprawy wewnętrzne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. poz. 2264).

²⁾ Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu 21 listopada 2018 r. pod numerem 2018/0574/PL, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), które wdraża postanowienia dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie) (Dz. Urz. UE L 241 z 17.09.2015, str. 1).

³⁾ Ze zmianą wprowadzoną przez § 1 pkt 1 lit. a tiret pierwsze rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 września 2021 r. zmieniającego rozporządzenie w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. poz. 1831), które weszło w życie z dniem 7 listopada 2021 r.

- 3) umożliwia odblokowanie kodu PIN1 i kodu PIN2 za pomocą kodu PUK;
- 4) zawiera licznik błędnych prób wprowadzenia kodu PIN1 i kodu PIN2 z możliwością ustawienia parametru liczby błędnych prób powodujących zablokowanie tych kodów;
- 5) w przypadku podania poprawnego kodu PIN1 albo kodu PIN2 zeruje mechanizm licznika, o którym mowa w pkt 4;
- 6) zapewnia komunikację z użyciem interfejsu bezstykowego pozwalającego na bezpieczne, szyfrowane połączenie;
- 7) uniemożliwia odblokowanie kodu PIN1 albo kodu PIN2 po zablokowaniu kodu PUK;
- 8) uniemożliwia odblokowanie kodu PUK;
- 9)⁴⁾ spełnia zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, zwanej dalej „ICAO”, określone w dokumencie – Doc 9303 Machine Readable Travel Documents część 10, 11 i 12 (wersja siódma z 2015 r.);
- 10)⁵⁾ zawiera aplikację zgodną z wymaganiami ICAO umożliwiającą automatyczną odprawę przy przekraczaniu granic państw.

2.⁶⁾ W warstwie elektronicznej dowodu osobistego są wydzielone, niezależnie zarządzane, logiczne części zawierające dane, o których mowa w art. 12a ust. 1 ustawy.

3. Wymagania techniczne dla warstwy elektronicznej dowodu osobistego określa załącznik nr 1 do rozporządzenia.

§ 3.⁷⁾ Nawiązanie połączenia między warstwą elektroniczną dowodu osobistego a urządzeniem lub systemem teleinformatycznym za pośrednictwem czytnika kart wymaga podania numeru dostępowego zamieszczonego na blankiecie dowodu osobistego, zwanego dalej „numerem CAN”.

§ 4. Pierwszy dostęp do przestrzeni umożliwiającej zamieszczenie kwalifikowanego certyfikatu podpisu elektronicznego zgodnego z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE wymaga podania numeru CAN, a następnie użycia kodu PUK.

Rozdział 3

Sposób używania certyfikatów identyfikacji i uwierzytelnienia, podpisu osobistego i potwierdzenia obecności

§ 5. Użycie certyfikatu identyfikacji i uwierzytelnienia wymaga podania numeru CAN oraz czterocyfrowego kodu PIN1, który ustala osobiście posiadacz dowodu osobistego.

§ 6. Użycie podpisu osobistego, weryfikowanego za pomocą certyfikatu podpisu osobistego, wymaga podania numeru CAN oraz sześciocyfrowego kodu PIN2, który ustala osobiście posiadacz dowodu osobistego.

§ 7. 1. Zmiana kodu PIN1 albo kodu PIN2 wymaga podania numeru CAN oraz podania odpowiednio dotychczasowego kodu PIN1 albo kodu PIN2, albo kodu PUK.

2. Trzykrotne wprowadzenie nieprawidłowego kodu PIN1 albo kodu PIN2 powoduje zablokowanie możliwości korzystania odpowiednio z certyfikatu identyfikacji i uwierzytelnienia lub certyfikatu podpisu osobistego.

3. W przypadku, o którym mowa w ust. 2, przywrócenie możliwości korzystania z certyfikatu identyfikacji i uwierzytelnienia lub certyfikatu podpisu osobistego jest możliwe po podaniu numeru CAN, a następnie użyciu kodu PUK i ustaleniu odpowiednio nowego kodu PIN1 albo nowego kodu PIN2.

§ 8. Użycie certyfikatu potwierdzenia obecności wymaga podania numeru CAN.

§ 9. Ponowne podanie numeru CAN w przypadkach, o których mowa w § 5–8, nie jest wymagane, jeśli połączenie nie zostało zakończone.

⁴⁾ W brzmieniu ustalonym przez § 1 pkt 1 lit. a tiret drugie rozporządzenia, o którym mowa w odnośniku 3.

⁵⁾ W brzmieniu ustalonym przez § 1 pkt 1 lit. a tiret trzecie rozporządzenia, o którym mowa w odnośniku 3.

⁶⁾ W brzmieniu ustalonym przez § 1 pkt 1 lit. b rozporządzenia, o którym mowa w odnośniku 3.

⁷⁾ W brzmieniu ustalonym przez § 1 pkt 2 rozporządzenia, o którym mowa w odnośniku 3.

Rozdział 4

Sposób przekazywania i używania kodu PUK

§ 10. Kod PUK jest przekazywany posiadaczowi dowodu osobistego, w którego warstwie elektronicznej zamieszczono certyfikat identyfikacji i uwierzytelnienia lub certyfikat podpisu osobistego. Posiadacz dowodu osobistego, w którego warstwie elektronicznej zamieszczono wyłącznie certyfikat potwierdzenia obecności, nie otrzymuje kodu PUK.

§ 11. Organ gminy przekazuje posiadaczowi dowodu osobistego zabezpieczony dokument z kodem PUK przy odbiorze dowodu osobistego w siedzibie organu gminy lub w każdym czasie po odbiorze dowodu osobistego.

§ 12. 1. W przypadku utraty kodu PUK posiadacz dowodu osobistego, działając osobiście, może przywrócić możliwość korzystania z certyfikatu identyfikacji i uwierzytelnienia lub podpisu osobistego w siedzibie organu dowolnej gminy. Przepis § 7 ust. 3 stosuje się odpowiednio.

2. Przywrócenie możliwości korzystania z certyfikatu identyfikacji i uwierzytelnienia lub podpisu osobistego następuje z wykorzystaniem systemu teleinformatycznego, o którym mowa w § 21, z zachowaniem zasad poufności za pomocą certyfikatu potwierdzenia obecności.

§ 13. Trzykrotne nieprawidłowe wprowadzenie kodu PUK powoduje brak możliwości odblokowania kodu PIN1 i kodu PIN2.

Rozdział 5

Sposób i tryb zawieszania, cofania zawieszenia oraz unieważniania certyfikatów identyfikacji i uwierzytelnienia, podpisu osobistego i potwierdzenia obecności

§ 14. 1. Zgłoszenie zawieszenia lub cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego odbywa się w trybie określonym w art. 32b ust. 1 pkt 3 ustawy, w drodze złożenia w siedzibie organu dowolnej gminy wypełnionego i podpisanego własnoręcznie przez osobę dokonującą zgłoszenia formularza albo w drodze podpisania własnoręcznie przez tę osobę w siedzibie organu dowolnej gminy formularza stanowiącego wydruk sporządzony z wykorzystaniem systemu teleinformatycznego, z którego użyciem prowadzony jest Rejestr Dowodów Osobistych, przez pracownika tego organu na podstawie podanych przez osobę dokonującą zgłoszenia danych oraz danych zawartych w Rejestrze Dowodów Osobistych.

2. Wzór formularza zgłoszenia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego stanowi załącznik nr 2 do rozporządzenia.

3. Wzór formularza zgłoszenia cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego stanowi załącznik nr 3 do rozporządzenia.

§ 15.⁸⁾ Do zgłoszenia zawieszenia lub cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego, dokonanego w trybie określonym w art. 32b ust. 1 pkt 1 ustawy przez pełnomocnika lub opiekuna lub kuratora, dołącza się sporządzone w formie dokumentu elektronicznego pełnomocnictwo szczególne do dokonania takiej czynności lub dokument pozwalający na ustalenie stosunku prawnego istniejącego między wnoszącym zgłoszenie a osobą, w której imieniu zgłoszenie jest wnoszone, a w razie niemożności ich uzyskania – odwzorowanie cyfrowe odpowiednio tego pełnomocnictwa lub dokumentu opatrzone przez osobę dokonującą zgłoszenia za pomocą kwalifikowanego podpisu elektronicznego, podpisu zaufanego albo podpisu osobistego.

§ 16. 1. Organ gminy, do którego zgłoszono zawieszenie lub cofnięcie zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego w trybie określonym w art. 32b ust. 1 pkt 1 i 3 ustawy, ustala zgodność danych posiadacza dowodu osobistego z danymi zawartymi w dostępnych rejestrach publicznych oraz z danymi zawartymi w innych dokumentach tożsamości, jeśli są dostępne.

2. W przypadku zawieszenia lub cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego w trybie określonym w art. 32b ust. 1 pkt 2 ustawy, ustalenie zgodności danych, o których mowa w ust. 1, następuje automatycznie przez porównanie danych przekazywanych przez usługę elektroniczną, za której pomocą zgłoszono zawieszenie lub cofnięcie zawieszenia, z danymi zawartymi w Rejestrze Dowodów Osobistych.

⁸⁾ Ze zmianą wprowadzoną przez § 1 pkt 3 rozporządzenia, o którym mowa w odnośniku 3.

§ 17. Zgłoszenie zawieszenia lub cofnięcia zawieszenia certyfikatów w warstwie elektronicznej dowodu osobistego dokonane w trybie określonym w art. 32b ust. 1 pkt 2 ustawy powoduje automatyczne zawieszenie lub cofnięcie zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego.

§ 18. Organ gminy, do którego zgłoszono zawieszenie lub cofnięcie zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego w trybie określonym w art. 32b ust. 1 pkt 1 i 3 ustawy, dokonuje rejestracji tej czynności w Rejestrze Dowodów Osobistych przez zawieszenie lub cofnięcie zawieszenia dowodu osobistego i wprowadzenie daty i czasu zawieszenia lub daty i czasu cofnięcia zawieszenia.

§ 19. W przypadku zawieszenia lub cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego w trybie określonym w art. 32b ust. 1 pkt 2 ustawy, zaświadczenie, o którym mowa w art. 32b ust. 2 ustawy, jest generowane automatycznie przez usługę elektroniczną, za której pomocą zgłoszono zawieszenie lub cofnięcie zawieszenia.

§ 20. 1. Wzór zaświadczenia potwierdzającego zgłoszenie zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego stanowi załącznik nr 4 do rozporządzenia.

2. Wzór zaświadczenia potwierdzającego zgłoszenie cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego stanowi załącznik nr 5 do rozporządzenia.

§ 21. Dane o zawieszeniu lub cofnięciu zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego są przekazywane z Rejestru Dowodów Osobistych do systemu teleinformatycznego, który obsługuje funkcjonalności warstwy elektronicznej dowodu osobistego, prowadzonego przez ministra właściwego do spraw wewnętrznych, zwanego dalej „ministrem”.

§ 22. Unieważnienie certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego oraz dowodu osobistego z powodu upływu terminu przewidzianego na cofnięcie zawieszenia następuje w sposób automatyczny.

§ 23. 1. Unieważnienia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego na podstawie art. 12g ust. 1 ustawy dokonuje minister w systemie teleinformatycznym, o którym mowa w § 21.

2. Minister przekazuje ministrowi właściwemu do spraw informatyzacji informację o unieważnionych certyfikatach zamieszczonych w warstwie elektronicznej dowodu osobistego w celu aktualizacji statusów warstwy elektronicznej dowodów osobistych w Rejestrze Dowodów Osobistych, a w przypadku przedłużenia ważności dowodu osobistego w zakresie warstwy graficznej – informację o dacie ważności dowodu osobistego.

§ 24. Unieważnienie dowodu osobistego w Rejestrze Dowodów Osobistych powoduje unieważnienie certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego. Dane o unieważnieniu dowodu osobistego są przekazywane z Rejestru Dowodów Osobistych do systemu teleinformatycznego, o którym mowa w § 21.

Rozdział 6

Przepis końcowy

§ 25. Rozporządzenie wchodzi w życie z dniem 4 marca 2019 r.

Załączniki do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r.

Załącznik nr 1⁹⁾

WYMAGANIA TECHNICZNE DLA WARSTWY ELEKTRONICZNEJ DOWODU OSOBISTEGO

- I.**
1. Warstwę elektroniczną dowodu osobistego stanowią:
 - 1) mikroprocesor;
 - 2) biblioteka kryptograficzna;
 - 3) platforma operacyjna, w tym środowisko oprogramowania Java oraz dedykowane oprogramowanie;
 - 4) interfejs bezstykowy zgodny z normą ISO/IEC 14443 typ A lub B;
 - 5) 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), zwanej dalej „ustawą”.
 2. 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.
 3. Warstwa elektroniczna dowodu osobistego wraz z dokumentacją ją opisującą stanowi łącznie przedmiot oceny w rozumieniu normy PN ISO/IEC 15408 lub normy równoważnej.
- II.**
1. Warstwa elektroniczna dowodu osobistego podlega ocenie bezpieczeństwa i certyfikacji zgodnie z wymaganiami normy PN ISO/IEC 15408 lub normy równoważnej.
 2. 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.
 3. 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.
- III.**
1. Profil zabezpieczeń, o którym mowa w pkt II. 2, jest dokumentem publicznie dostępnym, publikowanym przez niezależne od producenta warstwy elektronicznej jednostki zajmujące się certyfikacją.
 2. Specyfikacja techniczna warstwy elektronicznej dowodu osobistego jest zgodna z profilem zabezpieczeń, o którym mowa w pkt 1, jeśli ten profil zabezpieczeń został opracowany.
 3. 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).
- IV.**
1. 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.
 2. 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.

⁹⁾ Ze zmianami wprowadzonymi przez § 1 pkt 4 rozporządzenia, o którym mowa w odnośniku 3.

V.

1. Ocena bezpieczeństwa mikroprocesora jest dokonywana na poziomie uzasadnionego zaufania do zgodności z wymaganiami na poziomie nie niższym niż EAL5, rozszerzonym o komponenty uzasadnienia zaufania zgodnie z normą PN-ISO/IEC 14508-3 lub równoważną, obejmujące co najmniej AVA_VAN.5, ALC_DVS.2, ASE_TSS.2.
2. Ocena bezpieczeństwa platformy operacyjnej jest dokonywana na poziomie uzasadnionego zaufania do zabezpieczeń nie niższym niż poziom EAL5, rozszerzonym o odpowiednie komponenty AVA_VAN.5, ALC_DVS.2, ALC_FLR.1, ASE_TSS.2.
3. Ocena bezpieczeństwa apletu jest dokonywana na poziomie uzasadnionego zaufania do zabezpieczeń nie niższym niż poziom EAL4, rozszerzonym o odpowiednie komponenty ALC_DVS.2, ATE_DPT.1, AVA_VAN.5.

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 wyciekami 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 Triple-DES oraz AES;
- 2) obsługuje następujące algorytmy kryptograficzne:
 - a) symetryczne: AES, DES,
 - b) asymetryczne: RSA, ECDSA, w tym generowania lub obliczania par kluczy,
 - c) wymianę kluczy: DHKE,
 - d) 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:
 - a) przechowywania, tzn. zapewnienia ochrony tych danych przed nieuprawnioną modyfikacją lub manipulacją,
 - b) wymiany danych między apilem a dostawcą usługi zewnętrznej, po uwierzytelnieniu terminala oraz warstwy elektronicznej dowodu osobistego;
 - 2) zapewnia autentyczność:
 - a) danych użytkownika oraz danych służących do realizacji funkcji bezpieczeństwa podczas przechowywania, przez umożliwienie weryfikacji ich autentyczności po stronie terminala,
 - b) danych użytkownika podczas ich wymiany między apilem a dostawcą usługi zewnętrznej, po uwierzytelnieniu terminala oraz warstwy elektronicznej dowodu osobistego;
 - 3) zapewnia poufność danych użytkownika oraz danych służących do realizacji funkcji bezpieczeństwa:
 - a) przez nadanie praw do odczytu jedynie poprawnie uwierzytelnionym terminalom, z określonym poziomem ich autoryzacji,
 - b) podczas wymiany danych między apilem 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:
 - a) zmanipulowania lub ujawnienia danych użytkownika lub danych służących do realizacji funkcji bezpieczeństwa, przechowywanych w warstwie elektronicznej dowodu osobistego,
 - b) 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:
 - a) monitorowania i analizy poprawności operacji na poziomie sygnałowym, zarówno w odniesieniu do operacji wewnętrznych, jak i na interfejsach zewnętrznych,
 - b) wymuszania niepoprawnego działania funkcji w warunkach wykrycia ataku,
 - c) 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:
 - a) pomiarze napięcia lub natężenia prądu na stykach galwanicznych powierzchni układu scalonego, z wyłączeniem obwodów połączonych (z użyciem standardowych narzędzi pomiaru napięcia lub natężenia prądu),
 - b) wykorzystaniu innych rodzajów fizycznego współdziałania ładunków elektrycznych,
 - c) 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.

WZÓR

Rzeczpospolita
Polska oznaczenie organu

DO/ZA/1

Zgłoszenie zawieszenia certyfikatów w dowodzie osobistym**Instrukcja wypełniania w dwóch krokach**

1. WYPEŁNIAJ WIELKIMI LITERAMI

2. Wypełniaj kolorem czarnym lub niebieskim

*Przykład wypełnionego wniosku znajdziesz na stronie internetowej prowadzonej przez Ministerstwo Spraw Wewnętrznych i Administracji.***1. Informacje o zawieszeniu certyfikatów w dowodzie osobistym**

Seria i numer dowodu

*ⓘ Jeśli nie znasz tych danych, pozostaw puste pole.**ⓘ Certyfikaty w dowodzie osobistym można zawiesić na 14 dni kalendarzowych. Jeśli w tym terminie zawieszenie nie zostanie cofnięte, dowód wraz z certyfikatami zostanie unieważniony.***2. Dane posiadacza dowodu osobistego**

Numer PESEL

Nazwisko

Imię (imiona)

3. Dane osoby, która zgłasza zawieszenie certyfikatów w dowodzie osobistym

Nazwisko

Imię (imiona)

Nazwa, seria i numer
dokumentu tożsamości**4. Podpis osoby, która zgłasza zawieszenie certyfikatów w dowodzie osobistym**

Data

 - - *ⓘ dd-mm-rrrr*Własnoręczny
czytelny podpis**Adnotacje urzędowe (wypełnia urzędnik)**

WZÓR

Rzeczpospolita
Polska

oznaczenie organu

DO/ZA/2

Zgłoszenie cofnięcia zawieszenia certyfikatów w dowodzie osobistym**Instrukcja wypełniania w dwóch krokach**

1. WYPEŁNIAJ WIELKIMI LITERAMI

2. Wypełnij kolorem czarnym lub niebieskim

*Przykład wypełnionego wniosku znajdziesz na stronie internetowej prowadzonej przez Ministerstwo Spraw Wewnętrznych i Administracji.***1. Informacje o cofnięciu zawieszenia certyfikatów w dowodzie osobistym**

Seria i numer dowodu

*ⓘ Jeśli nie znasz tych danych, pozostaw puste pole.**ⓘ Zawieszenie certyfikatów w dowodzie osobistym można cofnąć tylko w ciągu 14 dni od zawieszenia. Po cofnięciu zawieszenia certyfikaty i dowód osobisty są ważne i można się nimi posługiwać.***2. Dane posiadacza dowodu osobistego**

Numer PESEL

Nazwisko

Imię (imiona)

3. Dane osoby, która zgłasza cofnięcie zawieszenia certyfikatów w dowodzie osobistym

Nazwisko

Imię (imiona)

Nazwa, seria i numer
dokumentu tożsamości**4. Podpis osoby, która zgłasza cofnięcie zawieszenia certyfikatów w dowodzie osobistym**

Data

 - - *ⓘ dd-mm-rrrr*Własnoręczny
czytelny podpis**Adnotacje urzędowe (wypełnia urzędnik)**

WZÓR



Rzeczpospolita oznaczenie organu
Polska

DO/ZA/3

Zaświadczenie o zgłoszeniu zawieszenia certyfikatów w dowodzie osobistym

1. Informacje o zawieszeniu certyfikatów w dowodzie osobistym

Data i godzina zawieszenia

Seria i numer dowodu osobistego

2. Dane posiadacza dowodu osobistego

Imię (imiona)

Nazwisko

Numer PESEL

3. Dane osoby, która zgłasza zawieszenie certyfikatów w dowodzie osobistym

Imię (imiona)

Nazwisko

Nazwa, seria i numer
dokumentu tożsamości

4. Informacje dodatkowe

- ⓘ Zawieszone certyfikaty i dowód osobisty zostaną unieważnione, jeśli do zawieszenie nie zostanie cofnięte.

5. Informacje o zaświadczeniu

Data wydania:

Podstawa prawna:
art. 32b ust. 2 ustawy z dnia 6 sierpnia 2010 r.
o dowodach osobistych.

6. Podpis urzędnika i pieczęć okrągła organu

- ⓘ Pieczęć nie jest wymagana w przypadku zaświadczenia wydanego w postaci elektronicznej.

WZÓR



Rzeczpospolita oznaczenie organu
Polska

DO/ZA/4

Zaświadczenie o zgłoszeniu cofnięcia zawieszenia certyfikatów w dowodzie osobistym

1. Informacje o cofnięciu zawieszenia certyfikatów w dowodzie osobistym

Data i godzina cofnięcia zawieszenia

Seria i numer dowodu osobistego

2. Dane posiadacza dowodu osobistego

Imię (imiona)

Nazwisko

Numer PESEL

3. Dane osoby, która zgłasza cofnięcie zawieszenia certyfikatów w dowodzie osobistym

Imię (imiona)

Nazwisko

Nazwa, seria i numer
dokumentu tożsamości

4. Informacje o zaświadczeniu

Data wydania:

Podstawa prawna:
art. 32b ust. 2 ustawy z dnia 6 sierpnia 2010 r.
o dowodach osobistych.

5. Podpis urzędnika i pieczęć okrągła organu

 Pieczęć nie jest wymagana w przypadku zaświadczenia
wydanego w postaci elektronicznej.