Projekt z dnia 17 maja 2024 r.

etap: Komitet Rady Ministrów do Spraw Cyfryzacji

ROZPORZĄDZENIE

Ministra spraw Wewnętrznych i Administracji[[1]](#footnote-1))

z dnia r.

w sprawie warstwy elektronicznej dowodu osobistego[[2]](#footnote-2)), [[3]](#footnote-3))

Na podstawie art. 12j 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) 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 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) 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”;

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 połączenie, gwarantujące, za pomocą technik kryptograficznych, poufność i integralność danych oraz uwierzytelnienie stron komunikacji;

7) uniemożliwia odblokowanie kodu PIN1 albo kodu PIN2 po zablokowaniu kodu PUK;

8) uniemożliwia odblokowanie kodu PUK;

9) spełnia zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, zwanej dalej „ICAO”, określone w dokumencie – Doc 9303 Machine Readable Travel Documents część 10, 11 i 12 (wersja ósma z 2021 r.);

10) zawiera aplikację zgodną z wymaganiami ICAO umożliwiającą automatyczną odprawę przy przekraczaniu granic państw.

2. 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. 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.

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 albo w miejscu pobytu osoby w przypadkach określonych w art. 30c ust. 1 ustawy, 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. Zgłoszenie zawieszenia lub cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego w trybie określonym w art. 32b ust. 1 pkt 3 ustawy, odbywa się na podstawie danych podanych przez osobę dokonującą zgłoszenia oraz danych zawartych w Rejestrze Dowodów Osobistych.

§ 15. 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, opiekuna lub kuratora, dołącza się:

1) pełnomocnictwo szczególne do dokonania zgłoszenia sporządzone na piśmie utrwalonym w postaci elektronicznej, opatrzonym przez posiadacza dowodu osobistego kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, albo dokument pozwalający na ustalenie stosunku prawnego istniejącego między wnoszącym zgłoszenie a osobą, w której imieniu zgłoszenie jest wnoszone, sporządzony na piśmie utrwalonym w postaci elektronicznej, albo

2) odwzorowanie cyfrowe dokumentu, o którym mowa w pkt 1, opatrzone przez osobę dokonującą zgłoszenia kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

§ 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.

§ 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 2 do rozporządzenia.

2. Wzór zaświadczenia potwierdzającego zgłoszenie cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego stanowi załącznik nr 3 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 określonym w komunikacie wydanym na podstawie art. 75 ust. 1 pkt 3 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234).[[4]](#footnote-4))

Minister Spraw Wewnętrznych I administracji

w porozumieniu:

MinistER Cyfryzacji

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 16 maja 2024 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. poz. 738). [↑](#footnote-ref-1)
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). [↑](#footnote-ref-2)
3. ) Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu … pod numerem …, 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 (ujednolicenie) (Dz. Urz. UE L 241 z 17.09.2015, str.1). [↑](#footnote-ref-3)
4. ) Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 26 lutego 2019 r. w sprawie warstwy elektronicznej dowodu osobistego (Dz. U. z 2022 r. poz. 1431), które traci moc z dniem określonym w komunikacie wydanym na podstawie art. 75 ust. 1 pkt 3 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234) w związku z wejściem w życie art. 37 pkt 1 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel. [↑](#footnote-ref-4)