**RAPORT Z KONSULTACJI**

**projektu rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie warstwy elektronicznej dowodu osobistego**

**Nr w Wykazie prac legislacyjnych Ministra Spraw Wewnętrznych i Administracji: 1102**

**1. Informacje ogólne**

Zgodnie z § 36 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – *Regulamin pracy Rady Ministrów* (M.P. z 2022 r. poz. 348), projekty ustaw lub projekty rozporządzeń przedstawia się do konsultacji publicznych, w tym konsultacji z organizacjami społecznymi lub innymi zainteresowanymi podmiotami albo instytucjami w celu przedstawienia ich stanowiska. Niniejszy dokument stanowi wypełnienie obowiązku, o którym mowa w § 51 ust. 1 Regulaminu, zgodnie z którym organ wnioskujący sporządza raport z konsultacji obejmujący omówienie wyników przeprowadzonych konsultacji publicznych i opiniowania.

Projekt został udostępniony w Biuletynie Informacji Publicznej na stronie Rządowego Centrum Legislacji w zakładce „Rządowy Proces Legislacyjny” zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – *Regulamin pracy Rady Ministrów* oraz stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. *o działalności lobbingowej w procesie stanowienia prawa* (Dz. U. z 2017 r. poz. 248).

**2. Przebieg konsultacji i opiniowania**

Projekt rozporządzenia został skierowany **do konsultacji publicznych** do następujących podmiotów:

Polskie Towarzystwo Informatyczne (PTI), Polska Izba Informatyki i Telekomunikacji (PIIT), Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT), Stowarzyszenie Instytut Informatyki Śledczej, Polska Izba Komunikacji Elektronicznej, Rada Główna Instytutów Badawczych (RGIB), Związek Banków Polskich, Izba Gospodarki Elektronicznej, Polska Izba Informatyki Medycznej, Ogólnopolskie Porozumienie Organizacji Samorządowych, Konfederacja Lewiatan, Fundacja Panoptykon, Fundacja Moje Państwo.

Projekt rozporządzenia został skierowany **do opiniowania** do następujących podmiotów:

Rzecznik Praw Obywatelskich, Prezes Urzędu Ochrony Danych Osobowych, Prezes Polskiego Komitetu Normalizacyjnego, Wojewodowie.

Projekt został również przekazany do zaopiniowania przez Komisję Wspólną Rządu   
i Samorządu Terytorialnego.

**3. Omówienie wyników przeprowadzonych konsultacji publicznych i opiniowania**

Stanowiska i opinie do projektu przedstawili:

Federacja Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie”, Izba Gospodarki Elektronicznej, Związek Banków Polskich, Wojewoda Kujawsko-Pomorski, Wojewoda Lubelski, Wojewoda Małopolski, Wojewoda Podkarpacki, Wojewoda Świętokrzyski, Wojewoda Wielkopolski, Prezes Urzędu Ochrony Danych Osobowych, Polski Komitet Normalizacyjny oraz Komitet Techniczny nr 182 ds. Ochrony informacji w systemach teleinformatycznych.

Federacja Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie”, Izba Gospodarki Elektronicznej oraz ww. Wojewodowie poinformowali o braku uwag do projektu.

Uwagi do projektu wnieśli: Związek Banków Polskich (ZBP), Prezes Urzędu Ochrony Danych Osobowych (UODO), Polski Komitet Normalizacyjny (PKN) oraz Komitet Techniczny nr 182   
ds. Ochrony informacji w systemach teleinformatycznych (KT nr 182).

**ZBP** zgłosił propozycję przeniesienia wymagań dotyczących sposobu używania certyfikatów zawartych w warstwie elektronicznej dowodu osobistego, ich odblokowywania i zawieszania do polityki usługi zgodnej z normą PN-ETSI EN 319 411-1 i wprowadzenie tej polityki jako załącznika do projektowanego rozporządzenia. Przedmiotowa uwaga nie została uwzględniona. Zagadnienia związane z wykorzystaniem dowodu osobistego z warstwą elektroniczną zostały spójnie określone w ustawie z dnia 6 sierpnia 2010 r. *o dowodach osobistych* (Dz. U. z 2022 r. poz. 671, z późn. zm.), dalej: *„ustawa”,* aktach wykonawczych do tej ustawy oraz właśnie   
w *„Polityce świadczenia usług dla dowodu osobistego z warstwą elektroniczną”,* zwanej dalej: *„Polityką”.* Wymóg określenia i opublikowania takiej polityki wynika wprost z art. 12i ustawy, który m. in. wskazuje organ odpowiedzialny za jej określenie i opublikowanie tej polityki (minister właściwy do spraw wewnętrznych), miejsce jej publikacji (Biuletyn Informacji Publicznej ww. ministra), jak również *expressis verbis* definiuje jej zakres przedmiotowy (techniczne i organizacyjne rozwiązania dotyczące sposobu, zakresu oraz warunków tworzenia, wydawania i używania certyfikatów). Odwołanie do polityki znajduje się również w treści samych certyfikatów, co wynika z art. 12e ustawy. W efekcie w BIP na stronie podmiotowej MSWiA jest opublikowana ww. Polityka, która została opracowana zgodnie z wymaganiami normy ETSI EN 319 411‐1, i zawiera deklarację zgodności ze wskazaną normą (rozdział 1. Wstęp). Zagadnienia związane z zasadami używania certyfikatu i pary kluczy, zawieszenie, cofnięcie zawieszenia i unieważnienie certyfikatu są opisane w Polityce w stosownych rozdziałach (4.5-5.0), uwzględniając fakt związania wydanych certyfikatów z dowodem osobistym i jego statusem ważności. Tym samym określanie na poziomie rozporządzenia kolejnej polityki nie wydaje się zasadne.

Większość ze zgłoszonych uwag odnosiła się do uregulowań zawartych w § 2 projektu, który dotyczy ogólnych wymogów dla warstwy elektronicznej dowodu osobistego. Część z tych uwag została uwzględniona, np. w zakresie wątpliwości **UODO** oraz **KT nr 182** co do użytego w § 2 ust. 1 pkt 6 projektu sformułowania: *„szyfrowane połączenie”,* wprowadzone zostały stosowne zmiany w projekcie. Pozostałe uwagi nie zostały uwzględnione, tj.:

* postulat **UODO oraz KT nr 182** przywrócenia górnego limitu cyfr dla długości kodu PIN1 oraz PIN2

Realizacja tej propozycji byłaby kierunkowo sprzeczna z rozwiązaniami przyjętymi na gruncie obecnie obowiązującego rozporządzenia, którego kształt uległ zmianie wskutek jego nowelizacji w 2021 r. Pierwotnie rozporządzenie Ministra Spraw Wewnętrznych   
i Administracji z dnia 26 lutego 2019 r. *w sprawie warstwy elektronicznej dowodu osobistego* (Dz. U. z 2022 r. poz. 1431) w § 2 ust. 1 pkt 1 zawierało zapis: *„1) obsługuje kody o długości od 4 do 8 cyfr(…)”.* Niemniej rozporządzeniem Ministra Spraw Wewnętrznych i Administracji   
z dnia 29 września 2021 r. *zmieniającym rozporządzenie w sprawie warstwy elektronicznej dowodu osobistego* (Dz. U. z 2021 r. poz. 1831), opis długości kodu PIN dla poszczególnych funkcjonalności został zmieniony przez wskazanie wyłącznie ich minimalnej długości,   
co wynikało ze zmiany funkcjonalności dowodu osobistego. Ponadto ograniczenie związane  
z maksymalną długością kodów PIN zostało przeniesione do warstwy aplikacji obsługującej   
e-dowód z dwiema cechami biometrycznymi z poziomu użytkownika, zaś przedmiotowe wartości zostały odwzorowane w dokumentacji technicznej. Brak określenia maksymalnej długości kodów PIN dotyczących samej warstwy elektronicznej nie wpływa na bezpieczeństwo rozwiązania, o którym decyduje minimalna wartość długości kodu PIN.

* propozycja **KT nr 182** uzupełnienia sformułowania: *„długości minimalnej 4 cyfr”* (§ 2 ust. 1 pkt 1 projektu) o zwrot: *„dziesiętnych”*

Postulat ma charakter *stricte* formalno-prawny i z uwagi na spójności systemu prawa   
w obszarze wydawania dowodów osobistych nie został uwzględniony. Już obecnie w ustawie jest odwołanie do cyfr bez odwoływania do systemu dziesiętnego (art. 2 ust. 1 pkt 6). Ponadto powszechne jest wykorzystywanie cyfry z katalogu znaków arabskich, służące do zapisu liczb w systemie dziesiętnym.

* postulat **UODO** doprecyzowania § 2 ust. 1 pkt 4 projektu poprzez określenie maksymalnej liczby błędnych prób wprowadzenia kodu PIN1 i kodu PIN2 (na wzór § 7 ust. 2 projektu)

Zmiana w tym zakresie została uznana za bezzasadną. Kwestionowany przepis odwołuje się do ogólnego mechanizmu zabezpieczeń dotyczących ustalenia limitu wykonania prób,   
a przywołany przepis § 7 ust. 2 projektu stanowi w istocie rozwinięcie ogólnej regulacji zawartej w ww. § 2, ustanawiając dla mechanizmu licznika dopuszczalność trzykrotnego podania nieprawidłowego kodu.

* propozycja **ZBP** wprowadzenia do projektu przepisów ustalających sposób publikacji certyfikatów umożliwiających weryfikację warstwy ICAO oraz list unieważnień tychże certyfikatów, w szczególności przepisów ustalających miejsce publikacji certyfikatów, pozwalających na ich weryfikację oraz status ważności.

Przedmiotowa uwaga nie została uwzględniona, jej uwzględnienie stanowiłoby przekroczenie upoważnienia ustawowego określonego w art. 12j ustawy.

**ZBP** przedstawił propozycję alternatywnego użycia kodu MRZ w operacjach opisanych w § 4, § 5, § 7 pkt 1. i 3, § 8 oraz § 9 projektu. Uwaga nie została uwzględniona. Długość postulowanego kodu MRZ to kilkadziesiąt znaków, zaś długość kodu CAN, do którego odnoszą się ww. przepisy, wynosi 6 znaków. Wprowadzenie zatem dodatkowego wymagania, którego implementacja skutkowałaby koniecznością wprowadzenia zmian do aplikacji wspomagającej, niezależnie od możliwości realizacji tego wymagania na wybranych platformach wykorzystywanych w warstwie elektronicznej e-dowodu, jest niezasadne.

**ZBP** przedstawił propozycję nadania nowego brzmienia § 5 projektu, uwzględniającego sposób i warunki użycia profilu osobistego, jak też dopuszczającego użycie profilu osobistego w celu identyfikacji elektronicznej w systemie udostępnionym przez Ministra Cyfryzacji lub w innym systemie spełniającym normy ETSI TS 119 461, argumentując to m. in. tym, iż dostęp do certyfikatu identyfikacji i uwierzytelnienia nie jest uzależniony od użycia kodu PIN. Przedmiotowa uwaga nie została uwzględniona. Kwestionowany przepis w projektowanym brzmieniu stanowi powtórzenie dotychczasowych rozwiązań zawartych w obecnie obowiązującym rozporządzeniu 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 pozostają skorelowane z przepisami ustawy (art. 12b). Przepisy dotyczące wykorzystania certyfikatów nie powinny być natomiast interpretowane w oderwaniu od określonych funkcjonalności e-dowodu opisanych w art. 10a ust. 3 ustawy. Użyte w rozporządzeniu sformułowanie: *„użycie certyfikatu”,* jest związane z faktycznym wykorzystaniem klucza prywatnego skojarzonego w parze z kluczem publicznym zawartym w certyfikacie.

Ponadto należy zaznaczyć, że kwestie związane z wykorzystaniem profilu osobistego jako Środka Identyfikacji Elektronicznej (ŚIE) regulują odrębne przepisy, w tym ustawa z dnia   
17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*(Dz. U. z 2024 r. poz. 307),która m. in. przewiduje, że minister właściwy do spraw informatyzacji odpowiada za funkcjonowanie systemu teleinformatycznego, zapewniającego obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany jest profil osobisty,   
jak też ustawa z dnia 5 września 2016 r. *o usługach zaufania oraz identyfikacji elektronicznej*(Dz. U. z 2024 r. poz. 422). Zgodnie z obowiązującymi przepisami, wykorzystanie profilu osobistego jest obecnie możliwe wyłącznie poprzez Węzeł Krajowy, w którym w Systemie Identyfikacji Elektronicznej (SIE) udostępniany jest Środek Identyfikacji Elektronicznej (ŚIE)   
w postaci profilu osobistego. Zmiana tego wymagania, postulowana w proponowanym nowym brzmieniu § 5 projektu, byłaby sprzeczna z warunkami użycia profilu osobistego, jak również   
z jego oceną w procesie zakończonej pozytywnie notyfikacji. Wskazanie na możliwość użycia profilu osobistego w innym systemie niż SIE, w którym udostępniony jest obecnie profil osobisty (zgodnie ze schematem Węzła Krajowego), wykracza poza zakres upoważnienia ustawowego.

Pozostałe uwagi dotyczyły załącznika nr 1 do projektu, który określa wymagania techniczne dla warstwy elektronicznej dowodu osobistego. Część zgłoszonych uwag została uwzględniona, np. w zakresie: wykreślenia z pkt II.1 zwrotu: *„certyfikacji”* **(KT nr 182),** uzupełnienia pkt II.3   
o Europejski schemat certyfikacji cyberbezpieczeństwa zgodny z Common Criteria (EUCC) **(KT nr 182),** błędnego odwołania do normy ISO/IEC 14508-3 **(PKN),** rezygnacji z odwołania do komponentów ASE TSS.2 (pkt V.1 i V.2), ALC FLR.1 (pkt V.2), ATE DPT.1 (pkt V.3) **(KT nr 182)** oraz do algorytmu Triple-DES w pkt VII.1 **(UODO oraz KT nr 182)** oraz DES w pkt VII.2 lit. a **(KT nr 182)**, wprowadzone zostały stosowne zmiany w projekcie. Inne uwagi nie zostały uwzględnione. Główną intencją projektodawcy jest bowiem dalsze dostosowanie obszaru dowodów osobistych do zmian, jakie w tej sferze wprowadziła ustawa z dnia 26 maja 2023 r.   
*o aplikacji mObywatel* (Dz. U. z 2023 r. poz. 1234). Wobec powyższego, bez uwzględnienia zasadniczo pozostały następujące uwagi:

* dotyczące norm, do których odwołuje się projekt załącznika nr 1 **(KT nr 182)**

Przedmiotowa grupa uwag zasadniczo zawierała propozycje uzupełnienia przywołanych w załączniku norm o odwołania do poszczególnych lub wszystkich części tych norm (pkt I.3, II.1, V) oraz odwołania się do dodatkowej normy PN-EN ISO/IEC 18045 w pkt II.1. Uwagi te co do zasady zostały odrzucone. W ocenie projektodawcy, należy pozostawić odwołanie do normy PN-EN ISO/IEC 15408 rozumianego jako standardu rozwiązań, a nie do konkretnej części dokumentu, określonego datą i częścią (zeszytem) i nadać temu odwołaniu charakter odwołania niedatowanego. Tego typu odwołanie wydaje się neutralne dla procesu produkcji, oceny bezpieczeństwa i certyfikacji rozwiązań zawartych w dowodzie osobistym. Ponadto przedmiotem projektowanego rozporządzenia jest określenie wymogów dla wymagań technicznych warstwy elektronicznej dowodu osobistego. Wymagania dotyczące bezpieczeństwa produktu opisane zostały w normie PN-EN ISO/IEC 15408. Norma PN-EN ISO/IEC 18045 jest natomiast normą techniczną, która stanowi dokument towarzyszący dla kryteriów oceny zabezpieczeń informatycznych zdefiniowanych w normie PN-EN ISO/IEC 15408. Innymi słowy, norma PN-EN ISO/IEC 18045 zawiera regulację stanowiącą o tym, jakie minimalne działania należy podjąć, aby właściwie przeprowadzić ocenę zgodnie   
z normą PN-EN ISO/IEC 15408. W efekcie projekt został skorygowany pod tym kątem.

* sugestia **PKN** stosowania zapisu: *„co najmniej zgodnie z normą”* lub *„co najmniej zgodnie   
  z wymaganiami normy”* oraz **UODO** dotycząca uzupełnienia sformułowania: *„normy równoważnej”* o sformułowanie: „*w rozumieniu przepisów ustawy z dnia 12 września 2002 r.   
  o normalizacji”* albo zastąpienia go zwrotem: *„lub normy zastępującej powołaną normę”*

Przedmiotowe propozycje nie zostały uwzględnione. Sugerowane zmiany przepisów mogą budzić ryzyko związane z ich wykonalnością bądź funkcjonalnością. W obecnym brzmieniu przepisy mają już ustaloną praktykę stosowania. Z uwagi na pilny charakter projektu, przegląd treści rozporządzenia pod kątem wskazanej terminologii, należy traktować jako uwagę *de lege ferenda.*

* **KT nr 182** dotycząca braku precyzyjności zwrotu: *„dedykowane oprogramowanie”* (pkt I.1.3)

W ocenie projektodawcy, ww. sformułowanie należy uznać za prawidłowe. Nie jest możliwe wskazanie konkretnie nazwy oraz wersji (dedykowanego) oprogramowania, ponieważ oprogramowanie zależy od wykorzystanego mikroprocesora (w ID mogą być stosowane mikroprocesory różnych producentów) i platformy operacyjnej, która jest ściśle związana   
z mikroprocesorem. Użycie zwrotu *„dedykowanego oprogramowania”* wskazuje oprogramowanie właściwe dla wykorzystanego mikroprocesora, a nie dowodu osobistego.

* propozycja uzupełnienia pkt IV.1.5 o sformułowanie: *„testów niefunkcjonalnych produktu złożonego, które wpływają na jego wydajność, użyteczność, bezpieczeństwo”* **(UODO)**

Istniejący wykaz wyczerpuje zakres zagadnienia zgodnie z: *„Composite product evaluation for Smart Cards and similar devices”* v\_1.5.1, https://sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.5.1., w związku   
z czym nie zachodzi potrzeba uzupełnienia.

* propozycja **KT nr 182** wprowadzenia w pkt V nowego podpunktu dotyczącego zagadnienia ALC\_FLR i schematu certyfikacji cyberbezpieczeństwa (EUCC)

Propozycja nie została uwzględniona, z uwagi na brak jednoznacznego ustalenia wpływu wdrażanego schematu EUCC na wskazane w uwadze wymagania.

* dokonanie analizy wymagań bezpieczeństwa dla mikroprocesora oraz biblioteki kryptograficznej określonych w pkt VI i VII pod kątem ich poprawności, kompletności   
  i weryfikowalności oraz zmianazapisów pkt IX.3.8 poprzez odwołanie do metod testowania określonych w normie ISO/IEC 17825 (**KT nr 182)**

W ocenie projektodawcy, pkt V projektu załącznika Nr 1 wskazuje normy dla oceny bezpieczeństwa mikroprocesora, platformy operacyjnej oraz apletu. Spełnienie norm wskazanych w pkt V prowadzi do spełniania przez mikroprocesor, platformę operacyjną czy aplet wymagań z pkt VI i VII. Wymogi dotyczące bezpieczeństwa weryfikowane są   
w procesie ewaluacji i certyfikacji rozwiązania na podstawie przyjętych standardów Common Criteria. Ponadto dokonanie postulowanej analizy wiąże się z długim horyzontem czasowym. Z uwagi więc na pilny charakter projektu, determinowany terminem wejścia   
w życie projektowanego rozporządzenia, który został skorelowany z wydaniem przez ministra właściwego do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw wewnętrznych komunikatu określonego w art. 75 ust. 1 pkt 3 ustawy z dnia   
26 maja 2023 r. *o aplikacji mObywatel*, jak również uwzględniając, iż projektowane rozwiązania stanowią powtórzenie dotychczasowych rozwiązań, przedmiotowe uwagi   
w chwili obecnej zostaną potraktowane jako postulaty *de lege ferenda*.

* wskazanie specyfikacji zestawu krzywych eliptycznych w pkt VII.2 lit. b **(KT nr 182)**

Szczegółowa specyfikacja zestawu wspieranych krzywych eliptycznych, na poziomie rozporządzenia nie jest uzasadniona, ponieważ dla zachowania spójności, należałoby odpowiednie parametry zdefiniować w odniesieniu do wszystkich algorytmów związanych z funkcjonowaniem warstwy elektronicznej e-dowodu. Stosowne parametry zestawu krzywych eliptycznych zostały uwzględniane na poziomie Projektu Technicznego sporządzonego dla projektu eDO 2.0, w którym bezpieczeństwo poszczególnych algorytmów i ich parametrów jest weryfikowane z aktualnie obowiązującymi standardami.

* uszczegółowienie zapisów pkt VII.2 lit. c **(KT nr 182)**

Przedmiotowa uwaga nie została uwzględniona, gdyż kwestionowany zapis – wskazując na ogólny mechanizm ustalenia klucza oparty na protokole Diffiego-Hellmana – nie wymaga uszczegółowienia. Konkretne algorytmy wraz z parametrami zostały wyspecyfikowane na poziomie ww. Projektu Technicznego.

* nieprecyzyjne sformułowanie *„przed podatnościami znanymi w momencie wykonania oceny bezpieczeństwa”* **(KT nr 182)**

Przedmiotowa uwaga nie została uwzględniona. Proces oceny bezpieczeństwa w ramach certyfikacji produktu jest niezależnym procesem realizowanym przez niezależne podmioty umocowane do jego przeprowadzenia według właściwych dla tych procesów standardów.

Stworzenie natomiast na poziomie rozporządzenia katalogu podatności poprzez odwołanie się w treści rozporządzenia do konkretnego dokumentu, wymagałoby poprzedzenia oddzielną analizą, dotyczącą możliwości uznania takiego katalogu za aktualny i wiążący, względem pojawiających się informacji o potencjalnych podatnościach i możliwości czasowej, systematycznej aktualizacji takiego katalogu. Mając na uwadze, że kwestie będące przedmiotem tej uwagi nie mają bezpośredniego wpływu na poprawność zdefiniowanych wymagań, jak też pilny charakter projektu, zgłoszona uwaga została potraktowana jako   
*de lege ferenda.*

**Komisja Wspólna Rządu i Samorządu Terytorialnego** w dniu 13 lutego 2024 r. pozytywnie zaopiniowała projekt rozporządzenia.

**3. Przedstawienie wyników zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym**

Projekt rozporządzenia nie wymaga przedłożenia go właściwym instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu w celu uzyskania opinii, dokonania konsultacji lub uzgodnienia.

Projektowana regulacja zawiera przepisy techniczne w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 roku *w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych* (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), zatem podlega notyfikacji zgodnie z powołanym rozporządzeniem.

**4. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa, wraz ze wskazaniem kolejności dokonania zgłoszeń albo informację o ich braku**

Nie odnotowano zgłoszeń zainteresowanych podmiotów w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.