

Opinia Polskiej Izby Informatyki i Telekomunikacji

o warstwie elektronicznej oraz innych rozwiązaniach informatycznych zawartych w projekcie ustawy o dowodach osobistych (druk sejmowy 2917)

Przedłożony projekt ustawy zawiera znaczącą część opisującą wprowadzenie do dowodu osobistego warstwy elektronicznej (informatycznego nośnika danych) zawierającego dane osobowe w postaci cyfrowej oraz dane do składania podpisu osobistego i inne dane. Jest to nowe rozwiązanie w polskim ustawodawstwie, przy istnieniu równoległej ustawy o podpisie elektronicznym. Zrozumiałe jest, że zapisy te są trudne do opracowania i procedowania.

Dobrze by też było skonfrontować zapisy z tej ustawy z zapisami istniejącej ustawy o podpisie elektronicznym, projektem jej nowelizacji aktualnie procedowanym przez Komisję „Przyjazne Państwo” oraz z nowym projektem ustawy o podpisach elektronicznych (chyba aktualnie kierowanym przez Rząd do Sejmu).

Poniżej przedstawiamy szereg uwag natury generalnej oraz szczegółowej wraz z propozycjami poprawienia niektórych zapisów, co powinno poprawić jakość merytoryczną tej ustawy. Uwag tych jest wiele i wydaje się konieczne, aby w trakcie procedowania było możliwe ich objaśnianie.

Uwagi generalne:

1. Pojęcia „warstwy graficznej” i odpowiednio „warstwy elektronicznej” są interesujące, ale też nie są zdefiniowane w tej ani w innej ustawie. W polskim ustawodawstwie używa się pojęcia: **informatyczny nośnik danych** - materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej” (zdefiniowany w Art. 3. pkt. 1 w ustawie o informatyzacji podmiotów publicznych realizujących zadania publiczne¹) oraz wykorzystywany już w kilku innych ustawach. Odpowiednio do tego na użytek tej ustawy trzeba by było pewnie zdefiniować: **graficzny nośnik danych** – materiał służący do zapisu danych w postaci wizualnej. Konieczne do zmiany w całym tekście ustawy.
2. **Wyłączenie** z tej ustawy, **ustawy o podpisie elektronicznym** uniemożliwia zastosowanie już przyjętych w prawie polskim i europejskim mechanizmów zaufania wobec podpisu elektronicznego. W ten sposób brakuje też definicji niektórych pojęć – np. *dane do składania podpisu osobistego (elektronicznego)* , *dane do weryfikacji podpisu osobistego (elektronicznego)* , a które są zdefiniowane ustawie o podpisie elektronicznym.
3. **„Wprowadzenie numeru PIN”** – opisuje technologie – co nie powinno mieć miejsca w ustawie. Należy w przepisie ustawy zamiast korzystania z PIN (i jego definicji) wpisać „... lub w sposób zapewniający kontrolę obywatela nad udostępnianiem danych”. Warunki udostępniania danych z dowodu osobistego mogą być treścią delegacji ustawowej zaś szczegółowe warunki techniczne powinny być zawarte w rozporządzeniu. Przy okazji zwracamy tutaj uwagę na brak zasad procedury „odzyskiwania numeru PIN” w przypadku

¹ Tekst jednolity opracowano na podstawie Dz.U. z 2005 r. Nr 64, poz. 565, z 2006 r. Nr 12, poz.65, Nr 73, poz. 501, z2008 r. Nr 127, poz.817, z 2009 r. Nr 157,poz. 1241, Dz. U. z2010 r. Nr 40, poz.230.

jego zapomnienia, co się często zdarza przy bankowości kartowej (banki mają taką procedurę – być może warto z niej skorzystać).

4. Nie istnieje technologia **ograniczonej identyfikacji oparta o certyfikaty**, natomiast istnieje kilka technologii opartych o techniki kryptograficzne. Zawarcie w ustawie wymagań na certyfikat ograniczonej identyfikacji uniemożliwia rzeczywistą implementację mechanizmu ograniczonej identyfikacji. Wobec braku uzasadnienia do stosowania ograniczonej identyfikacji (patrz uzasadnienie do ustawy) **proponujemy zrezygnować z tego mechanizmu w tej ustawie**. Jednocześnie należy podkreślić, iż nie są obecnie znane mechanizmy ograniczonej identyfikacji (lub pokrewne) korzystające z certyfikatów. Nie widać w opiniowanej ustawie zapisów prawnych związanych ze skutkami prawnymi ograniczonej identyfikacji. Dodatkowo wątpliwość budzi zapis o skutkach prawnych ograniczonej identyfikacji. Przewidywane podobnie zastosowanie tego rozwiązania do głosowania w trackie wyborów, wobec braku jednoznacznego pomysłu na sposób głosowania elektronicznego, jest dalece przedwcześnie. Niezależnie od wybranej technologii do realizacji mechanizmów ograniczonej identyfikacji - nie widać praktycznej możliwości realizacji zapisów tego punktu.

Uwagi szczegółowe:

Art.2.1

pkt.1 *certyfikat dowodu osobistego – elektroniczne zaświadczenie przyporządkowujące dane do weryfikacji informacji uwierzytelniającej do dowodu osobistego; [niestety nie wiadomo do czego przyporządkowujące – może numeru dowodu osobistego?]*

pkt. 2 *certyfikat ograniczonej identyfikacji - usunąć zgodnie z Uwagą 4 – nie istnieje technologiczna implementacja opisanego definicją mechanizmu.*

pkt.3 *certyfikat podpisu osobistego – elektroniczne zaświadczenie przyporządkowujące dane do weryfikacji podpisu osobistego do posiadacza dowodu osobistego; [niestety nie wiadomo do czego przyporządkowujące – może do numeru PESEL lub jakiegoś zbioru danych?]*

pkt 8 *numer PIN – usunąć zgodnie z Uwagą 3 a w Rozporządzeniu można zdefiniować jako: „osobisty numer identyfikacyjny posiadacza dowodu osobistego stanowiący poufny ciąg 4 cyfr umożliwiający kontrolę obywatela nad udostępnieniem danych” ;*

pkt 9 *ograniczona identyfikacja – usunąć zgodnie z Uwagą 4 – nie jest zrozumiały cel takiego mechanizmu uwierzytelnienia.*

pkt.10 *personalizacja dowodu osobistego – wprowadzenie danych przyszłego posiadacza dowodu osobistego na nośnik graficzny i informatyczny danych dowodu osobistego dokonywane przez ministra właściwego do spraw wewnętrznych; [ale to chyba nie wszystkie dane, które są potem wprowadzone na informatyczny nośnik danych?]*

pkt.12 *Zapis w tym punkcie implikuje pośrednio wniosek, że te same dane zwarte w nieważnym dowodzie już nie mogą być podstawą podpisu osobistego – ale od strony podmiotu ufającego nie można tego rozróżnić czy dane pochodziły z ważnego czy nieważnego dowodu. Finalny podpis może być nieważny z innych przyczyn ale nie takiej jak pośrednio wskazuje się w tej definicji.*

Art.3.

Patrz Uwaga 2. Nie należy odłączać tej ustawy od ustawy o podpisie elektronicznym, a rozbieżności można rozwiązać poprzez dopisanie w tym Art.3 wyjątków od zasady niestosowania poprzez wskazanie tych przepisów ustawy o podpisie elektronicznym, które mają zastosowanie, a w tym część definicji.

Art. 11. Proponowana nowa wersja zapisu art. zgodna z uwagami generalnymi:

1. Dowód osobisty posiada graficzny i informatyczny nośnik danych.
2. Dowód osobisty potwierdza prawdziwość danych zawartych na nośniku graficznym oraz po udostępnieniu, danych zawartych na nośniku informatycznym. Udostępnienie następuje na żądanie uprawnionych organów lub za zgodą obywatela. **[Patrz też DODATEK do DYSKUSJI!]**
3. Dowód osobisty umożliwia uwierzytelnienie go w systemach teleinformatycznych podmiotów publicznych, uwierzytelnienie jego posiadacza w systemach teleinformatycznych podmiotów publicznych oraz przy dostępie do rejestrów publicznych.

Art. 13. Poprawiona wersja Art. 13.

1. **Informatyczny nośnik danych** dowodu osobistego zawiera:

- 1) dane zamieszczone na **nośniku graficznym** dowodu osobistego zapisane elektronicznie wraz z danymi je uwierzytelniającymi; [powstaje pytanie jak ma być zamieszczony wizerunek twarzy – zdjęcie czy cechy biometryczne? – patrz też poniżej w - Do dyskusji]
 - 1) dane służące do składania informacji uwierzytelniającej **weryfikowane za pomocą certyfikatu dowodu osobistego, dane służące do składania podpisu osobistego weryfikowane przy pomocy certyfikatu podpisu osobistego**; [usunięto identyfikację ograniczoną – patrz Uwaga 4; Proponujemy też zmienić słowo „opatrzonej”, słowem odpowiednio „weryfikowane przy pomocy”, gdyż Certyfikat (dokładniej klucz publiczny znajdujący się w certyfikacie stosowany jest podczas weryfikowania, a nie podczas tworzenia podpisu, informacji uwierzytelniającej, itp.]
 - 2) przestrzeń umożliwiającą zamieszczenie **certyfikatu kwalifikowanego wraz z danymi do składania bezpiecznego podpisu elektronicznego** na podstawie ustawy z dnia 18 września 2001 r. o podpisie elektronicznym; [to trzeba będzie zweryfikować z treścią zmian w ustawie o podpisie elektronicznym]
 - 3) przestrzeń na zamieszczenie danych służących do wykorzystania dowodu osobistego jako karty ubezpieczenia zdrowotnego w rozumieniu ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2008 r. Nr 164, poz. 1027, z późn. zm.).
2. Dowód osobisty wydany osobie, która nie ukończyła 5 roku życia, nie zawiera danych służących do składania podpisu osobistego opatrzonego certyfikatem podpisu osobistego.[usunięto „...ograniczonej identyfikacji].

Do dyskusji: W zapisie pkt.1 brakuje określenia czy dane uwierzytelniające dotyczą ZESTAWU danych czy poszczególnych informacji oddzielnie. Występuje tu zagrożenie dla prywatności posiadaczy gdyż jest niebezpieczeństwo iż w celu uwierzytelnienia informacji z warstwy elektronicznej NIEZBEDNE jest ujawnienie WSZYSTKICH danych z informatycznego nośnika

danych (warstwy elektronicznej) gdyż tylko wtedy możliwa będzie realizacja funkcji uwierzytelnienia NAWET jeśli ujawnieniu co do ma podlegać tylko wybrana informacja (np. tylko imię i nazwisko). Dla realizacji uwierzytelnienia DANYCH niezbędne jest ich CAŁOŚCIOWE ujawnienie (!) Poprawne i powszechnie stosowane rozwiązanie alternatywne to uwierzytelnienia karty i KANAŁU komunikacyjnego w ramach którego odczytywane są wyłącznie WYBRANE dane z warstwy elektronicznej dowodu. Wtedy dane są uwierzytelnione pośrednio przez fakt pobrania ich z uwierzytelnionej karty a nie przez proponowany tutaj mechanizm uwierzytelnienia SAMYCH DANYCH.

Art. 14. Poprawiona wersja Art.:

1. *Zabezpieczenia informatycznego nośnika danych dowodu osobistego uniemożliwiają utworzenie funkcjonującej jego kopii przy zastosowaniu technologii dostępnych w momencie personalizacji dowodu osobistego.* [Uzasadnienie: Obecne brzmienie punktu zawiera niezrozumiałe stwierdzenie dotyczące "elektronicznego uwierzytelniania" bez podania czego uwierzytelnienie dotyczy.]
2. *Dane posiadacza zapisane na informatycznym nośniku danych dowodu osobistego w trakcie procesu personalizacji są zabezpieczone w sposób umożliwiający stwierdzenie, że ich treść została utworzona w trakcie personalizacji dowodu osobistego.* [Uzasadnienie: Obecne sformułowanie w praktyce wykluczałoby możliwość dodawania danych do warstwy elektronicznej po zakończeniu personalizacji, co jest wymagane dla użycia dowodu jako karty ubezpieczenia zdrowotnego.]

Art. 15. Poprawiona treść Art.:

Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wymagania techniczne dla informatycznego nośnika danych dowodu osobistego oraz protokołu komunikacji elektronicznej z dowodami osobistymi, kierując się potrzebą zapewnienia bezpieczeństwa funkcjonowania dowodów osobistych oraz zapewnienia ochrony interesów posiadaczy dowodów osobistych.

Art. 16.

Naszym zdaniem błędna jest koncepcja zawarta w tym art. 16 ust. 1 dotycząca skutków prawnych podpisu osobistego a mianowicie taka ,że jest on równoważny własnoręcznemu tylko jeśli dokument został skierowany do podmiotu publicznego(lub gdy strony wyrażą wolę). Czynności prawne jednostronne nie muszą być do nikogo kierowane w momencie podpisania np. oświadczenia. Przepisy prawa wymagają zaś często składania własnoręcznie podpisanych oświadczeń. Czy oświadczenia takie będąc podpisywane podpisem osobistym będą równoważne podpisowi własnoręcznemu czy też nie? Sprawa ma zasadnicze znaczenie jeśli zamierzamy znacząco odbiurokratyzować działanie administracji i zastępować zaświadczenia oświadczeniami. Przepis ten może budzić zasadnicze wątpliwości interpretacyjne i być zupełnie niezrozumiały dla społeczeństwa.

Art. 17.2

Polityka certyfikacji oraz polityka podpisu powinny zostać określone i ogłoszone w przepisach szczegółowych (rozporządzenie). Obie polityki stanowią zobowiązanie zarówno posiadacza dowodu osobistego posługującego się częścią elektroniczną, gminy biorącej udział w procesie wydania, MSWiA świadczącego usługi certyfikacyjne a także wszystkich ufających mechanizmom zawartym w warstwie elektronicznej. W punkcie tym wprowadzono różne urządzenia, dla których brakuje definicji.

Art.18.1

Do dyskusji: Wg uzasadnienia uwierzytelnienia dowodu odbywa się bez dodatkowej zgody posiadacza: „*Do złożenia informacji uwierzytelniającej nie będzie wymagana ingerencja posiadacza dowodu, tzn. dowód będzie składał informację uwierzytelniającą na każde żądanie, po połączeniu z czytnikiem*”. Czyli każdy system informatyczny otrzyma na tym etapie treść certyfikatu dowodu osobistego = serię i numer dowodu osobistego! Jest to informacja umożliwiająca jednoznaczną identyfikację posiadacza czyli wyklucza sens stosowania ograniczonej identyfikacji gdyż na etapie uwierzytelniania dowodu już przekazano (bez ograniczeń!) JEDNOZNACZNĄ identyfikację posiadacza przez pozostawienia jego numeru dowodu osobistego w systemie informatycznym, który wykonywał uwierzytelnianie dowodu osobistego. Przy połączeniu tego założenia z bezstykowym interfejsem komunikacyjnym powstaje kompletny system śledzenia aktywności obywateli!

Art. 19.2

Pojęcie „aktywacji certyfikatu” jest mylne, niezgodne z techniczną stroną modelu PKI i wprowadza istotne zagrożenia gdyż w systemach PKI ochronie i kontroli posiadacza podlega wyłącznie klucz prywatny a certyfikat klucza publicznego jest informacją publiczną, która nie posiada statusu „aktywny/nieaktywny” a jedynie ważny/nieważny/zawieszony.

Nie przewiduje się pojęcia „deaktywacji certyfikatu” a jedynie zawieszenie.

Art. 19.4

Niepotrzebne i BARDZO niepraktyczne założenie gdyż implikuje bardzo długie przechowywanie na lisach CRL informacji o unieważnionym certyfikacie (np. przez 9 lat). Co prowadzi to bardzo dużego przyrostu ich wielkości. Podobnie inne metody walidacji certyfikatów muszą przechowywać i przetwarzać bardzo duże zbiory danych tylko dlatego, że certyfikat nie podlega naturalnemu usunięciu z obiegu wraz z zakończeniem jego ważności.

Postęp w krypto-analizie może powodować konieczność wydania certyfikatów dla innych algorytmów lub innych długości klucza. Gdyby okres był krótszy to można by kolejny certyfikat wydać dla dłuższych kluczy lub innego algorytmu.

Nie ma też unieważnienia certyfikatu.

Art. 19.9

Złożenie podpisu osobistego powinno być realizowane w sposób zapewniający kontrolę jego aktywacji przez posiadacza dowodu osobistego. Sposób kontroli aktywacji określa rozporządzenie.

Nie powinno się natomiast wpisywać technologii jaką jest „PIN” – patrz Uwaga 3.

Art. 20 – do usunięcia – patrz Uwaga 4

Art. 21. Pkt 2

Zapis może sugerować posiadaczowi dowodu osobistego, że umieszczenie w dowodzie osobistym danych służących do składania podpisu kwalifikowanego odbywa się na jego ryzyko i stąd może to być ryzykowna operacja. W praktyce ryzyko powinien ponosić tylko i wyłącznie podmiot kwalifikowany. Stąd proponujemy taki zapis:

„Odpowiedzialność za ewentualne uszkodzenia funkcjonalności dowodu osobistego, powstałe w wyniku zamieszczenia przez podmiot kwalifikowany w dowodzie osobistym danych służących do składania bezpiecznego podpisu elektronicznego weryfikowanego za pomocą kwalifikowanego certyfikatu, o których mowa w ust. 1, ponosi podmiot kwalifikowany.”

Art. 22

Sugeruje się zmianę punktu 4. Proponuje się zastosowanie zapisu umożliwiającego po ustaniu powodu dla którego wyłączono możliwość korzystania z funkcjonalności informatycznego nośnika danych, ponowne jej włączenie.

Art. 29.

Proponuje się zastosować zapisy analogiczne do tych, które określają wymagania dla zdjęć w paszportach (spełniają wymagania ICAO).

Art. 33 pkt.2

Usunąć, gdyż jest nadmiarowy, bo małoletni nie ma pełnej zdolności do czynności prawnych.

Art. 35.

W tym opisie wniosku nie wiadomo kto jest wnioskodawcą – osoba mająca być właścicielem certyfikatu, czy jego pełnomocnik?

W pkt.3 nie powinno być wysyłania PINu (lub danych aktywacyjnych) na adres wnioskodawcy, ale powinien on być wręczany bezpośrednio przy wydawaniu dowodu osobistego i jego aktywacji. Pkt.3 można skreślić.

Art. 47

Wpisanie w ustawie „wzory formularzy” – jest niezgodne z ustawą o informatyzacji, która wskazuje na wzory pism, podań, wniosków – które także powinny mieć postać elektroniczną.

Art. 51

Zapis uniemożliwia realizację zgłoszenia elektronicznie. Propozycja aby był zapis „*Zgłoszenie utraty lub uszkodzenia dowodu zawiera:*”;

Art. 58

Wskazuje się dane przechowywane w Rejestrze Dowodów Osobistych. W szczególności w punkcie 5) mowa o danych dotyczących danych zapisywanych w warstwie elektronicznej dowodu osobistego. Wymieniony katalog danych nie jest pełny, gdyż nie wskazano szeregu innych danych technicznych

(np. wersji aplikacji zapisanej w warstwie elektronicznej). Jednocześnie wydaje się, iż Rejestr Dowodów Osobistych nie jest odpowiednim miejscem do przechowywania takich danych. Zasadne jest przechowywanie ich w systemach pomocniczych, związanych z Rejestrem Dowodów Osobistych (np. systemach odpowiedzialnych za wydawanie certyfikatów cyfrowych, czy systemach odpowiedzialnych za zarządzanie zawartością karty elektronicznej dowodu osobistego- jeśli takowe planuje się wdrażać).

Art 59.

Proponuje się ze względów bezpieczeństwa ograniczenie dostępu do danych organom gmin jedynie do tych danych, które są niezbędne w realizowanych przez nie procesach.

Art. 60,

Proponujemy usunąć, gdyż nie widać podstaw dla prowadzenia gminnych rejestrów dowodów osobistych (sprawy związane z wydawaniem dowodów osobistych wymagają w myśl projektu ustawy pracy z rejestrem centralnym). Utrzymywanie kopii wycinka (lub całości) Rejestru Dowodów Osobistych w gminach jest niewskazane ze względów bezpieczeństwa. Zniesienie bytu "Gminny rejestr dowodów osobistych" powoduje konieczność modyfikacji dodatkowych artykułów ustawy (m.in. 62, 78).

Rozdział 8 Uwaga ogólna:

Zasady udostępniania, wzorowane zresztą na Ustawie o ewidencji ludności (Rejestr PESEL), są zbyt restrykcyjne. Utrudniają, np. zastosowanie dowodu osobistego do uwierzytelniania posiadacza w systemach opieki zdrowotnej, w systemach bankowych, ogólnie w sieci. O ile w przypadku rejestru PESEL można takie restrykcje jeszcze zrozumieć, to o tyle w przypadku Rejestru Dowodów Osobistych jest to niezrozumiałe i przeczy idei społeczeństwa informacyjnego, w którym elementem podstawowym jest konieczność weryfikacji tożsamości obywateli w sieci. Elektroniczny dokument powinien wspomagać weryfikację tożsamości obywatela, ale obostrzenia określone w Art. 69 i dalszych role taką ograniczają jedynie do kontaktów z wybranymi urzędami publicznymi i rządowymi. Proponowany dowód osobisty nie będzie więc pełnić roli jedynego elektronicznego identyfikatora tożsamości obywatela. Poddajemy to Komisji pod rozwagę.

Art 67.

Proponuje się zmienić zapis mówiący o zakresie udostępnianych danych. Niewskazane jest w szczególności przekazywanie danych służących do aktywacji certyfikatów, czy odblokowujące funkcjonalności elektronicznej warstwy dowodu (Art. 58 pkt. 5 lit. e oraz g).

Art. 68.

Dlaczego nie udostępnia się informacji o zawieszeniu i wznowieniu pozostałych typów certyfikatów? Pomyłka?

Art. 69

W tym art. mówi się o trybie pełnej, ograniczonej teletransmisji oraz o trybie jednostkowym udostępniania danych, nie precyzując znaczenia tych terminów. Niezależnie od znaczenia tych terminów, nie widać uzasadnienia dla udostępniania jakimkolwiek podmiotowi danych technicznych związanych z certyfikatami oraz warstwą elektroniczną dowodu osobistego.

Uwagi dodatkowe poza tematem ekspertyzy.

Poddajemy też pod rozważenie Komisji następujące uwagi dotyczące treści ustawy:

Art. 2 pkt.2

Zapis ten chyba powinien być w Art. 4 pkt 1a.

2. Ilekroć w ustawie jest mowa o organie gminy, należy przez to rozumieć wójta, burmistrza lub prezydenta miasta.

Art. 6.

W pkt.1 można chyba opuścić listę państw, gdyż mogą się pojawić szybko nowe (np. Ukraina) , które zaakceptują nasz nowy dowód osobisty. Pkt. 2 jest chyba też nadmiarowy. Propozycja uproszczonego zapisu.

Dowód osobisty jest dokumentem potwierdzającym tożsamość i obywatelstwo polskie osoby na terytorium i granicach Rzeczypospolitej Polskiej oraz innych państw uznających ten dokument za uprawniający do przekraczania ich granic oraz potwierdzania tożsamości.

Art. 9a

Chyba w ustawie należy wpisać możliwość wydawania dowodów osobistych z „drugą tożsamością” dla służb specjalnych oraz świadków koronnych i innych osób z odesłaniem do rozporządzenia (może już niejawnego) o trybie i zasadach takich procedur oraz sposobie kontroli. Co prawda zasady te są wpisane do innych ustaw (o ABW i Policji oraz ...) , ale warto to zweryfikować przy tej okazji.

Art. 12 pkt.2a,

Przy „serii i numerze dowodu osobistego,” warto może zaznaczyć, aby Minister projektując graficzny nośnik danych skorzystał z większych niż obecnie czcionek, gdyż seria i numer są często używane , a obecnie są trudne do odczytania!!!

Art. 29

Chyba logicznie pkt 11 i 12 powinny zostać zamienione miejscami.

Art. 84.

Zgodnie ze standardami konstytucyjnego Państwa prawa niedopuszczalne jest karanie za nieposiadanie dowodu osobistego. Dowód osobisty jest ,co prawda, dokumentem obowiązkowym dla obywateli zamieszkałych w kraju. Nie ma żadnego uzasadnienia karanie za jego nieposiadanie jeżeli można ustalić tożsamość obywatela lub jeżeli obywatel posiada inny równoważny dokument tożsamości - paszport. Raczej rynek i funkcje które za pośrednictwem dowodu osobistego można będzie realizować „zmusi” osoby do występowanie o jego wydanie niż groźba sankcji karnej.

Dodatek dotyczący Art. 11.2 do DYSKUSJI.

Obecny zapis:

*„Dowód osobisty potwierdza prawdziwość danych zawartych w warstwie graficznej przez udostępnienie tych danych zamieszczonych w warstwie elektronicznej. **Udostępnienie następuje na żądanie uprawnionych organów lub za zgodą obywatela wyrażoną przez wprowadzenie numeru PIN.**”*

Proponowany zapis Art. 11.2:

Dowód osobisty potwierdza prawdziwość danych zawartych w warstwie graficznej przez udostępnienie tych danych zamieszczonych w warstwie elektronicznej, przy zastosowaniu mechanizmów bezpieczeństwa określonych w drodze rozporządzenia przez Ministra właściwego do spraw wewnętrznych. Udostępnienie następuje na za zgodą obywatela wyrażoną przez wprowadzenie numeru PIN. [bez uwzględnienia uwagi 3].

GŁOS 1:

Umożliwienie odczytu danych elektronicznych na żądanie uprawnionych organów przy braku zgody obywatela oznacza w praktyce konieczność użycia mechanizmu Extended Access Control (EAC) tak jak w przypadku odcisków palców w paszportach biometrycznych, przy czym z uwagi na specyfikę dowodu osobistego niezbędne będzie zbudowanie ogromnego systemu PKI do obsługi EAC na potrzeby Policji i innych uprawnionych organów (znacznie większa skala systemu PKI niż w przypadku paszportów biometrycznych).

Zapis wyróżniony powyżej jest wzorowany na wymaganiach niemieckiego dowodu osobistego, który w warstwie elektronicznej będzie zawierał odciski palców, co zgodnie z wytycznymi ICAO uzasadnia zastosowanie mechanizmu EAC, analogicznie do odczytu odcisków palców w paszportach biometrycznych.

W polskim dowodzie osobistym z uwagi na:

- a. brak odcisków palców,***
- b. ten sam zakres danych obywatela zawartych w warstwie elektronicznej i graficznej dokumentu (odczyt danych z warstwy graficznej możliwy „gotym okiem” i w żaden sposób nie ograniczony)***

nie ma uzasadnienia dla stosowania mechanizmu EAC, gdyż oznaczałoby to wdrożenie bardzo kosztownego rozwiązania dla odczytu danych elektronicznych pomimo udostępnienia wszystkich tych danych do swobodnego odczytu z warstwy graficznej dokumentu (dane naniesione na awers i rewers karty w procesie personalizacji).

Wymóg zastosowania mechanizmu EAC w dowodach osobistych wpływa na wydłużenie czasu produkcji blankietów, oraz znacząco zwiększa koszty wdrożenia projektu elektronicznych dowodów osobistych (co najmniej 45 mln zł netto w okresie 5 lat). Na koszty te składają się przede wszystkim:

- a. wyższe koszty zakupu mikroprocesorów (koszty modułu oprogramowania EAC wraz z certyfikatem Common Criteria EAL4+)
- b. koszty budowy i serwisowania skomplikowanej infrastruktury PKI o znacznie większej niż w przypadku paszportów biometrycznych liczbie terminali umożliwiających odczyt danych elektronicznych poprzez mechanizm EAC.

Obecny zapis Art. 11.2 projektu ustawy faworyzuje firmy niemieckie, które na dzień dzisiejszy jako jedyne przygotowały i są w trakcie certyfikacji wg Common Criteria EAL 4+

oprogramowania mikroprocesorów spełniającego wymagania niemieckiego dowodu osobistego wraz z mechanizmem EAC.

GŁOS 2:

Dowód osobisty jako dokument podróży wewnątrz granic unijnych powinien w zakresie mechanizmów dotyczących bezpiecznego udostępniania danych zawartych w warstwie elektronicznej wzorować się na rozwiązaniach paszportowych. W szczególności zasadne wydaje się wykorzystanie mechanizmów EAC oraz PACE. Z racji na konieczność stosowania drogich czytników – nie zalecane jest wykorzystywanie mechanizmu BAC korzystającego z odczytu optycznego strefy MRZ dokumentu.

Porównywanie udostępniania danych z warstwy graficznej (np. okazanie dokumentu osobie uprawnionej do jego kontroli) z udostępnianiem danych z warstwy elektronicznej (pełna, potwierdzona kopia wszystkich danych z warstwy graficznej) jest nieuprawnione. Nie sposób zgodzić się ze stwierdzeniem, że dane z warstwy graficznej dokumentu są "udostępniane do swobodnego odczytu".

Wprowadzenie mechanizmu EAC do nowego dowodu osobistego wymaga rozbudowy infrastruktury PKI używanej dla potrzeb paszportów lub rozbudowania planowanego środowiska PKI koniecznego do wydawania certyfikatów zawartych w dowodzie.

O ile niemieckie podmioty przygotowujące karty pod wymagania niemieckiego dowodu tożsamości nie są w kontekście wymagań na polski dowód osobisty faworyzowane, gdyż wdrożenie polskiego dowodu odbędzie się istotnie później niż niemieckiego. Daje to czas pozostałym producentom na przygotowanie odpowiedniego oprogramowania i jego certyfikację. Ponadto należy zauważyć, iż dowody nie będą wydawane jednorazowo, a stopniowo, przez wiele lat. Daje to instytucjom zamawiającym karty swobodę w wyborze dostawców w trakcie tego procesu.

Niezależnie od problemu odczytywania danych z warstwy elektronicznej, mechanizm może być użyty do delegowania uprawnień do modyfikacji zawartości karty. W szczególności podmiotom wydającym certyfikaty kwalifikowane mogą być wydane stosowne certyfikaty, które umożliwią osadzenie na karcie certyfikatu kwalifikowanego. Infrastruktura centralna dla potrzeb tego mechanizmu jest zatem konieczna niezależnie od sposobu udostępniania danych z warstwy elektronicznej dowodu osobistego.