Zestawienie uwag przygotowane na postawie projektu rozporządzenia z dnia 7 lutego 2011 MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI
w sprawie wymagań technicznych dla warstwy elektronicznej dowodu osobistego oraz protokołu komunikacji elektronicznej z dowodami osobistymi

§	pkt.	tekst	uwaga	propozycje
1	2	Odczyt zapis i modyfikacja danych zapisanych w warstwie elektronicznej dowodu osobistego możliwe są **tylko** w sposób określony w niniejszym rozporządzeniu	Każdy zapis, który nie opisuje istniejących technologii powoduje długi i kosztowny proces dostosowywania karty dowodu osobistego do wymagań rozporządzenia	Odczyt zapis i modyfikacja danych muszą spełniać warunki wskazane przez niniejsze rozporządzenie
2	12	hasło (PIN) - ciąg cyfr ustalanych przez posiadacza dowodu osobistego, przechowywanych wyłącznie w warstwie elektronicznej dowodu osobistego, których znajomość jest niezbędna do wykonania przez warstwę elektroniczną dowodu osobistego niektórych funkcji	wymuszenie, że PIN musi być przechowywany w warstwie elektronicznej dowodu osobistego eliminuje rozwiązania bezpieczniejsze, przechowujące skrót z PIN'u. Ograniczenie PIN'u do ciągu cyfr, eliminuje rozwiązania, które dopuszczają stosowanie innych znaków (przy czym należy zauważyć, że PIN to Personal identification **Number**), warto rozważyć wprowadzenie alternatywy do pojęcia hasło. Wprowadzenie do definicji terminu, że PIN ma być ustalany przez posiadacza dowodu osobistego, wyklucza zbudowanie na tej podstawie pojęcia PIN'u transportowego.	hasło/PIN - ciąg znaków, weryfikowany przez warstwę elektroniczną dowodu osobistego w celu wykorzystania chronionych przez niego funkcji
2	19	sektor - zespół podmiotów i jednostek organizacyjnych, wobec których posiadacz dowodu osobistego, korzystając z ograniczonej identyfikacji, jest identyfikowany jako ta sama osoba fizyczna;	definicja sektora nie obejmuje przypadku wydzielonej grupy terminali w ramach organizacji, zespołu podmiotów lub jednostek organizacyjnych	sektor - zespół podmiotów, jednostek organizacyjnych lub terminali wobec których posiadacz dowodu osobistego korzystając z ograniczonej identyfikacji jest identyfikowany jako ta sama osoba fizyczna
2	22	warstwa elektroniczna dowodu osobistego - mikroprocesor umieszczony w dowodzie osobistym, wyposażony w interfejs dualny, wraz z elementami do komunikacji z czytnikami (interfejsami) i oprogramowaniem	Brak precyzji w stwierdzeniu o jakie oprogramowanie chodzi. Można interpretować ten zapis także jako oprogramowanie middleware, które np. nie jest certyfikowane z Common Criteria, czy FIPS. Tego typu zapis może spowodować, że na rynku nie będzie urządzeń spełniających wymagania rozporządzenia.	warstwa elektroniczna dowodu osobistego - mikroprocesor umieszczony w dowodzie osobistym, wyposażony w interfejs dualny, wraz z elementami do komunikacji z czytnikami (interfejsami) i oprogramowaniem zainstalowanym w pamięci mikroprocesora
2	23	weryfikacja certyfikatu - sprawdzenie, czy pieczęć elektroniczna, którą opatrzony jest certyfikat spełnia wymagania wymienione w punkcie 15	w punkcie 15 są wymienione wymagania dla podpisu zaawansowanego. Weryfikacja ich jest nierealna. Przykładowo jak w czasie weryfikacji można stwierdzić, że podmiot mógł mieć dane do składania pieczęci pod swoją wyłączną kontrolą, albo czy dane są jednoznacznie przypisane do pieczętującego (to powinność centrum certyfikacji). Proces weryfikacji certyfikatu jest różny dla różnych jego rodzajów (CVC, X.509). Proponowana definicja jest poprawna dla obu typów certyfikatów	weryfikacja certyfikatu - weryfikacja czy pieczęć elektroniczna, którą opatrzony jest certyfikat jest prawidłowa oraz czy certyfikat został wydany przez zaufanego wydawcę i nie ma przesłanek do stwierdzenia braku jego ważności
2	26	zaufany certyfikat dostępu - certyfikat dostępu wydany osobie prawnej lub jednostce organizacyjnej, realizującej zadania określone w ustawie, związane z wydawaniem dowodów osobistych i określający posiadacza tego certyfikatu jako podmiot zaufany	Definicja bardzo myląca. Z opisu wynika, że chodzi o certyfikat dostępu systemu personalizacji, a nie o certyfikat zaufany każdego systemu. Tego rodzaju definicja może powodować problemy interpretacyjne.	Zaufany certyfikat dostępu - ważny certyfikat dostępu możliwy do zweryfikowania w hierarchii Centrum Certyfikacji

2	27	Zaufany terminal - terminal posiadający ważny certyfikat terminala, określający go jako zaufany terminal, wydany przez podmiot lub jednostkę organizacyjną posiadającą ważny zaufany certyfikat dostępu	Definicja opisuje wyłącznie certyfikaty terminali systemu personalizacji. Nie obejmuje certyfikatów wydanych w innym celu.	Zaufany terminal - terminal posiadający ważny certyfikat dostępu weryfikowany w hierarchii Centrum Certyfikacji
3	1 5)	Warstwa elektroniczna dowodu osobistego spełnia wymagania techniczne określone przez następujące standardy: 5) ISO 7816-7 - w zakresie języka poleceń (SCQL - Structured Card Query Language)	przegląd dostępnych rozwiązań eID nie wykazuje, że wszystkie karty implementują to rozwiązanie; jest to struktura pliku na karcie dla którego w obecnym kształcie rozporządzenia nie widać zastosowania, natomiast może nieuzasadnienie ograniczać konkurencyjność rozwiązań	wykreślić
3	1 8)	Warstwa elektroniczna dowodu osobistego spełnia wymagania techniczne określone przez następujące standardy: 8) ISO 7816-13 - w zakresie zarządzania aplikacjami w środowisku wieloaplikacyjnym	przegląd dostępnych rozwiązań eID nie wykazuje, że wszystkie karty implementują to rozwiązanie; wprowadzenie wymagania zgodności z tą normą może nieuzasadnienie ograniczać konkurencyjność rozwiązań	wykreślić
3	2	sposób zasilania karty i protokół komunikacji z użyciem interfejsu bezstykowego określa standard ISO 14443-2 z komunikacją typu B	Nie ma powodu ograniczania rodzaju komunikacji. Zarówno standardy typu A i B są stosowane w dokumentach eID. Zapis tego rodzaju mógłby być oprotestowany jako ograniczający celowo zakres rozwiązań tym bardziej, że jawnie ogranicza konkurencyjność rozwiązań, co nie ma wy tym przypadku uzasadnienia.	sposób zasilania karty i protokół komunikacji z użyciem interfejsu bezstykowego określa standard ISO 14443-2 z komunikacją typu A lub B
3	3	Protokół komunikacji z użyciem interfejsu stykowego określa standard ISO 7816-3 z protokołem T1	Nie ma powodu ograniczania rodzaju komunikacji. Zarówno komunikacja typu T0 jak i T1 jest stosowana w dokumentach eID. Zapis tego rodzaju mógłby być oprotestowany jako ograniczający celowo zakres rozwiązań, tym bardziej, że jawnie i nieuzasadnienie ogranicza konkurencyjność rozwiązań.	Protokół komunikacji z użyciem interfejsu stykowego określa standard ISO 7816-3 z protokołem T0 lub T1
3	4	Stosowane certyfikaty cyfrowe są zgodne z wersją 3 zaleceń X.509, opracowanych przez organizację ITU-T - International Telecommunication Union - Telecommunication Standarization Sector	Certyfikaty CVC nie spełniają tych zaleceń. Nigdzie nie ma normy opisującej tego rodzaju certyfikaty, a wymaganie stosowanie x.509 powoduje, że nie istnieje technologia realizująca weryfikację certyfikatów terminali przez kartę.	Stosowane certyfikaty cyfrowe są zgodne z wersją 3 zaleceń X.509, opracowanych przez organizację ITU-T - International Telecommunication Union - Telecommunication Standarization Sector albo z formatem certyfikatów CVC opisanym w prEN 14890-1 wydanej przez European Commitee form Standarization
3	5	Do generacji podpisu osobistego i informacji uwierzytelniającej stosowany jest algorytm RSA i klucze kryptograficzne o długości nie mniejszej niż 2048b	nie jest jasne w jakim rozumieniu jest tutaj wskazana "informacja uwierzytelniająca" (certyfikat? - taka definicja znajduje się w rozporządzeniu)	Podpis osobisty jest weryfikowany zgodnie z algorytmem RSA przy użyciu kluczy o długości nie mniejszej niż 2048b.
3	6	W pamięci warstwy elektronicznej dowodu osobistego wydzielonych jest siedem kontenerów, niezależnie zarządzanych i aktywowanych	nie jest jasne co projektant rozporządzenia miał na myśli pod pojęciem zarządzanie. Jeśli chodzi o możliwość niezależnej zmiany zawartości, to wystarczy siedem plików z zapisanymi osobno stanem. W jakim celu jest utworzony ten kontener? Jeżeli kontener jest rozumiany jako aplikacja na karcie to określanie z góry liczby kontenerów może uniemożliwić ustalenie ostatecznego profilu karty.	Warstwa elektroniczna dowodu osobistego umożliwia umieszczanie niezależnie aktywowanego i zarządzanego oprogramowania.

5	1	Warstwa elektroniczna dowodu osobistego jest bezpiecznym urządzeniem do składania podpisu elektronicznego w rozumieniu Dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.	Zapis tego rodzaju powoduje nałożenie na CAŁĄ warstwę elektroniczną wymagań bezpiecznego urządzenia do składania podpisu elektronicznego. W kartach wieloaplikacyjnych z profilem SSCD jest certyfikowany jeden aplet. Wymaganie może powodować konieczność zastosowania jedynie platformy natywnej i jej późniejszą certyfikację jako całośc, co dla wymienionych w rozporządzeniu wymagań uniemożliwia dostarczenie jakiegokolwiek rozwiązania w okresie wymaganym ustawą.	wykreślenie (te same warunki opisuje kolejny punkt) albo zapis "Przestrzeń umożliwiająca zamieszczenie certyfikatu kwalifikowanego, o której mowa w Art 13 ust 1. pkt 3 spełnia wymagania bezpiecznego urządzenia do składania podpisu elektronicznego w rozumieniu Dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisów elektronicznych"
5	3	Warstwa elektroniczna dowodu osobistego posiada certyfikat Common Criteria EAL 4+ określony zgodnie z normą ISO/IEC 15408 **oraz** certyfikat FIPS 140-2 level 3	Zapis tego rodzaju wymusza konieczność certyfikacji WSZYSTKICH apletów umieszczonych na dowodzie osobistym. W przypadku apletów NFZ, podpisu osobistego i niestandardowej aplikacji ograniczonej identyfikacji - oznacza to opóźnienia w dostarczeniu dowodów osobistych. Na moment obecny nie bedzie kart spełniających wymagania. Jednoczesne wymaganie EAL 4+ i FIPS 140-2 level 3 wyklucza z rynku większość dostępnych rozwiązań - producenci zazwyczaj stosują tylko jedną z powyższych certyfikacji ze względu na brak uzasadnienia biznesowego.	**mikroprocesor oraz system operacyjny dowodu osobistego** posiada co najmniej certyfikat Common Criteria EAL 4+ określony zgodnie z normą ISO/IEC 15408 **lub** certyfikat FIPS 140-2 level 3 Dodatkowo, uzupełnienie o zapis: Certyfikacja mikroprocesora oraz systemu operacyjnego umożliwia dodawanie nowych funkcjonalności pod warunkiem ich weryfikacji na zgodność z powyższą certyfikacją.
7	1. 1)	wszelkie dane, z wyjątkiem danych kryptograficznych niezbędnych do nawiązania.....	Niektóre dane niezbędne do nawiązania połączenia nie są danymi kryptograficznymi (np. lista dostępnych aplikacji lub atrybuty związane z kartą)	wszelkie dane, z wyjątkiem danych niezbędnych do rozpoznania mikroprocesora dowodu i nawiązania połączenia .....
7	1. 2)	pełny zapis komunikacji z dowodem osobistym uzupełniony o wszelkie dane dostępne dla terminala, nie umożliwia stwierdzenia przez osoby trzecie autentyczności zapisu, o ile w trakcie komunikacji nie został utworzony podpis osobisty lub bezpieczny podpis elektroniczny lub pieczęć elektroniczna - z użyciem odpowiednich danych zapisanych w dowodzie osobistym	zamknięcie listy mechanizmów, które łamią zasadę potwierdzenia autentyczności zapisu zamyka możliwość wstawienia własnego podpisu przez NFZ i dokonywania jakichkolwiek modyfikacji (np możliwości instalacji na karcie własnych certyfikatów użytkownika)	pełny zapis komunikacji z dowodem osobistym uzupełniony o wszelkie dane dostępne dla terminala, nie umożliwia stwierdzenia przez osoby trzecie autentyczności zapisu, o ile w trakcie komunikacji nie został utworzony podpis elektroniczny lub pieczęć elektroniczna - z użyciem odpowiednich danych zapisanych w dowodzie osobistym
7	1. 3)	Nie można skutecznie zainicjować wymiany danych z dowodem osobistym wykorzystując wyłacznie dane zarejestrowane podczas wcześniejszej komunikacji terminala z warstwą elektroniczną dowodu osobistego, także przy wykorzystaniu innych danych, dostępnych niezależnie od terminala	Taki zapis zakłada, że komunikacja odbywa się wyłącznie przy użyciu mechanizmów EAC. Taki zapis blokuje możliwość złożenia podpisu bezpiecznego przy wykorzystaniu niezaufanego terminala (traktując oprogramowanie na komputerze użytkownika jako system teleinformatyczny). Zapis zakłada, że komunikacja od razu jest obustronnie uwierzytelniona. Wymiana danych musi się także odbywać do uwierzytelniania komunikacji.	Nie można zestawić obustronnie uwierzytelnionego bezpiecznego połączenia pomiędzy dowodem osobistym a terminalem przy wykorzystaniu danych zarejestrowanych podczas wcześniejszej komunikacji.
7	1. 4)	nie można skutecznie zainicjować wymiany danych z terminalem wykorzystując dane zarejestrowane podczas wcześniejszej komunikacji terminala z warstwą elektroniczną dowodu osobistego, także przy wykorzystaniu innych danych dostępnych niezależnie od warstwy elektronicznej dowodu osobistego.	terminal nie jest warstwą elektroniczną dowodu osobistego. Przepis poza delegacją	wykreślić
7	3	brak zapisów	brak zapisów dotyczących nawiązywania komunikacji poprzez interfejs bezstykowy, wymagania zestawienia połączenia za pomocą PIN. Brak takiego wymagania będzie kompensowany przez standardowe metody komunikacji.	Komunikacja za pomocą interfejsu bezstykowego jest możliwa po potwierdzeniu zamiaru nawiązania połączenia przez podanie kodu PIN lub kodu zapisanego w warstwie graficznej dowodu osobistego.

8	1	Rozpoczęcie procedury uwierzytelnienia dowodu osobistego drogą elektroniczną wymaga wykorzystania kodu zawartego w warstwie graficznej dowodu osobistego lub hasła (PIN) do nawiązania bezpiecznego kanału pomiędzy warstwą elektroniczną dowodu osobistego a czytnikiem.	1. Ten element jest związany z ochroną przed skimmingiem (kopiowaniem zawartości karty przy użyciu interfejsu bezstykowego). Chodzi o to, aby nawiązanie komunikacji wymagało podania danych, które nie będą znane osobie próbującej skopiować kartę przez interfejs bezstykowy. Wymaganie to może być niepotrzebne dla interfejsu stykowego, w którym samo włożenie karty do czytnika jest czynnością uniemożliwiającą jej "automatyczne" skopiowanie. Zapis par 7. pkt 3 adresuje wymaganie w wystarczającym zakresie. Nie jest także pewne czy w kolejnych częściach specyfikacji ECC BAC będzie obowiązkowy. 2. Jeśli już powinna być mowa o komunikacji z terminalem	Rozpoczęcie procedury uwierzytelnienia dowodu osobistego drogą elektroniczną wymaga wykorzystania kodu zawartego w warstwie graficznej dowodu osobistego lub hasła (PIN).
8	2	Kod lub hasło (PIN), o których mowa w ust 1, wykorzystywany jest w taki sposób, by nawiązanie komunikacji z wykorzystaniem błędnego kodu lub hasła (PIN) było nieskuteczne oraz by dla kanału komunikacyjnego pomiędzy warstwą elektroniczną dowodu osobistego a czytnikiem były spełnione warunki par. 7. ust 1 - 3 i ust 2.	1. W przypadku akceptacji par 7 pkt 3. przepis jest nadmiarowy 2. jeśli już to można mówić o nawiązaniu komunikacji z terminalem 3. Jeśli par 7 wymienia warunki dla dowolnej wymiany danych to zapis jest zbędny w zakresie spełnienia warunków z wymienionego paragrafu	wykreślić
8	3	Uwierzytelnienie dowodu osobistego przez uprawnione organy, o których mowa w art 11 ust 2 ustawy, może być dokonane z wykorzystaniem interfejsu stykowego lub kodu zawartego w warstwie graficznej dowodu osobistego lub sprawdzenia przez dowód osobisty, że komunikacja nawiązywana jest z uprawnionym terminalem w sposób opisany w par. 11 oraz w par 12.	1. Błąd logiczny - we wskazanym artykule ustawy nie ma wymienionych uprawnionych podmiotów, a jest opis czynności weryfikacji danych zawartych w dowodzie osobistym wraz z wymaganiem potwierdzenia kontroli obywatela nad procesem udostępniania danych.	Kontrola nad czynnością, o której mowa w Art 11, ust 2 Ustawy, może być rozumiana jako świadome wykorzystanie czytnika stykowego, bądź wprowadzenie kodu, o którym mowa w par 7. pkt 3 w przypadku wykorzystania czytnika bezstykowego
8	4	Certyfikat dostępu określa, czy w trakcie uwierzytelnienia dowodu osobistego wymagane jest użycie hasła (PIN) lub kodu, o których mowa w ust 1.	Wymaganie niestandardowe - będzie wymagało zmiany i recertyfikacji dostępnych aplikacji eID realizujących wymagania ECC.	wykreślić
9	1	Uwierzytelnienie dowodu osobistego wymaga zastosowania danych zawartych w certyfikacie dowodu osobistego. Użycie innych danych skutkuje negatywnym wynikiem uwierzytelnienia	Dane w certyfikacie służą do weryfikacji. Nie jest to doprecyzowane. Kolejny punkt opisuje, że uwierzytelnienie jest realizowane przez złożenie podpisu przy użyciu danych nie znajdujących się w certyfikacie.	weryfikacja informacji uwierzytelniającej, o której mowa w par. 9 pkt. 2 jest dokonywana przy użyciu certyfikatu dowodu osobistego.
10	2	Procedura zmiany hasła (PIN) chroni posiadacza przed błędnym wprowadzeniem nowego hasła (PIN)	Sformułowanie jest zbyt ogólne. Zapewne chodzi o powtórne wprowadzenie nowego hasła, ale nie wynika to wprost z zapisu	Procedura zmiany hasła (PIN) wymaga dwukrotnego wprowadzenia nowego hasła (PIN)
10	4	procedury zmiany hasła (PIN) oraz utworzenia nowego hasła (PIN) gwarantują, że nowe hasło (PIN) nie jest możliwe do odgadnięcia przy średniej liczbie prób mniejszej niż 10000, także w przypadku posiadania przez osobę nieuprawnioną dostępu do danych zawartych w warstwie graficznej dowodu.	1. Nie można zagwarantować, że hasło nie zostanie odgadnięte już w pierwszej próbie. Dlatego proponuje się złagodzić przepis. 2. Pin jest ustalany przez użytkownika i nie można zagwarantować, że nie użyje czegoś prostego. Wymuszanie skomplikowanych polityk haseł spowoduje, że PIN będzie noszony na karteczce z dowodem.	procedury zmiany hasła (PIN) oraz utworzenia nowego hasła (PIN) gwarantują, że długość hasła (PIN) nie będzie mniejsza niż 4 znaki

11	"1-8"		W ramach paragrafu została opisana procedura techniczna. Lepszym rozwiązaniem byłoby odwołanie się do normy CEN TS 15480 Identification card systems -- European Citizen Card -- Part 2: Logical data structures and card services annex B.5. (albo od razu do normy prEN 14890-1:2007 rozdział 14.12) Tam proces jest opisany dokładniej i bardziej jednoznacznie.	Procedury uwierzytelniania terminala są przeprowadzane zgodnie ze specyfikacją 14890-1:2007 Application interface for smart cards used as secure signature creation devices.
13	2	brak zapisów	Brak informacji o konieczności weryfikacji autentyczności przekazanych danych za pomocą mechanizmów passive authentication.	Potwierdzenie drogą elektroniczną danych zawartych w warstwie graficznej dowodu osobistego dokonywane jest poprzez przeprowadzenie procesu uwierzytelnienia pasywnego (passive authentication) w sposób opisany w specyfikacji ICAO 9303 part 1. vol 2
14	1	Przekazanie przez dowód osobisty danych wymienionych w art 12 ustawy z wyłączeniem punktu 1 lit g, wymaga użycia interfejsu stykowego albo uwierzytelnienia dowodu osobistego za pomocą kodu zawartego w warstwie graficznej dowodu osobistego za pomocą hasła (PIN)	W specyfikacji BSI Advanced Security Mechanisms for MRTD's (TR 03110 v 1.1) zarówno informacje znajdujące się da dowodzie grupa (DG1) jak i wizerunek twarzy (DG2) są udostępniane bez konieczności używania EAC. Nie ma potrzeby wyróżniania punktu 1. lit. G	Przekazanie przez dowód osobisty danych wymienionych w art 12 Ustawy wymaga użycia interfejsu stykowego albo uwierzytelnienia dowodu osobistego za pomocą kodu zawartego w warstwie graficznej dowodu osobistego za pomocą hasła (PIN)
14	2	Przekazanie przez dowód osobisty danych wymianionych w art 12 punkt 1. lit g ustawy, wymaga uwierzytelnienia dowodu osobistego za pomocą hasła (PIN)	System inspekcyjny powinien mieć możliwość zczytywania twarzy użytkownika.	wykreślenie
15	1	Każdy blankiet dowodu osobistego jest przed personalizacją oznaczony unikalnym identyfikatorem - serią i numerem dowodu osobistego, zapisanym zarówno w warstwie graficznej jak i elektronicznej dowodu osobistego. Zapis w warstwie elektronicznej dowodu osobistego jest opatrzony pieczęcią elektroniczną	Wpisanie, że identyfikator blankietu jest opatrzony pieczęcią elektroniczną budzi od razu pytania, kto wystawił pieczęć? Co jeśli zastosowano inne mechanizmy zabezpieczenia integralności?	Każdy blankiet dowodu osobistego jest przed personalizacją oznaczony unikalnym identyfikatorem - serią i numerem dowodu osobistego, zapisanym zarówno w warstwie graficznej jak i elektronicznej dowodu osobistego.
15	2	Warstwa elektroniczna każdego dostarczonego blankietu dowodu osobistego przechowuje unikalne dane do składania pieczęci elektronicznej - w kontenerze podlegającym ochronie przewidzianej dla danych do składanie podpisu elektronicznego - oraz odpowiadające im dane do weryfikacji pieczęci elektronicznej	niezrozumiałe, o jaką pieczęć chodzi? Kto wystawia dane do weryfikacji? Jaki kontener?	wykreślenie
15	3	Na żądanie zaufanego terminala, dowód osobisty tworzy pieczęć elektroniczną za pomocą danych wymienionych w ust 2. dla danych podanych przez terminal	niezrozumiały cel tego postępowania	wykreślenie

16		§16 1. Dowód osobisty umożliwia zapisanie danych w warstwie elektronicznej dowodu osobistego jedynie po weryfikacji uprawnień terminala, przy użyciu bezpiecznego kanału pomiędzy warstwą elektroniczną dowodu a terminalem. 2. Uprawnienia terminala o których mowa w ust 1, określone są według zasad określonych w §11 ust 8 3. Wymagania, o których mowa w ust. 1 -2 odnoszą się także do zapisu oprogramowania w warstwie elektronicznej dowodu osobistego z dodatkowym zastrzeżeniem, że dowód osobisty nie pozwala na zapisanie przez terminal oprogramowania mającego w stosunku do jakiegokolwiek obszaru warstwy elektronicznej uprawnienia wyższe od uprawnień, jakie w stosunku do tego obszaru posiada terminal. 4. O ile jest to wskazane w certyfikacie dostępu, zapisanie danych lub oprogramowania w warstwie elektronicznej dowodu osobistego wymaga podania hasła przez posiadacza.	Na chwilę obecną certyfikaty CVC nie są wykorzystywane do aktualizacji oprogramowania. Ze względu na fakt, że w tym wypadku mogłaby być konieczna w mechanizmy niskopoziomowe (np. warstwę usługową analogiczną do usług Global Platform) certyfikacja tego rozwiązania mogłabybyć długa i kosztowna	§16 (zapisywanie aplikacji i danych personalizacyjnych przez producenta) 1. Dopuszcza się zapisywanie danych i oprogramowania w trakcie procesu tworzenia karty dowodu osobistego przez producenta karty pod następującymi warunkami: 1) Zakres zapisywanych danych i lista oprogramowania jest ustalana w trakcie zamówienia na zakup kart dowodu osobistego 2) Producent karty zobowiązuje się, że zawartość części elektronicznej dowodu osobistego jest zgodna z uzgodnioną z Ministrem SwiA specyfikacją. 3) Wraz z kartą dowodu osobistego są dostarczane klucze kryptograficzne pozwalające na zarządzanie częścią elektroniczną dowodu osobistego 2. Po zakończeniu procesu tworzenia karty przez producenta dostęp do warstwy elektronicznej dowodu osobistego jest zabezpieczany a dane umożliwiające dostęp przekazane Ministrowi SWiA 3. Minister SWiA zapisuje w części elektronicznej oprogramowanie i dane niezbedne do funkcjonowania warstwy elektronicznej dowodu osobistego po okazaniu danych umożliwiających dostęp do dowodu. 4. Po wykonaniu czynności wymienionych w pkt. 3 Minister SWiA zabezpiecza dostęp do części elektronicznej dowodu osobistego kodem transportowym.
17		§17 1. Zapis w warstwie elektronicznej dowodu osobistego możliwy jest jedynie we wskazanym przez certyfikat dostępu obszarze pamięci dowodu osobistego 2. Dowód osobisty pozwala jedynie na zapisanie oprogramowania opatrzonego pieczęcią elektroniczną, weryfikowaną przy pomocy aktywnego punktu zaufania, zapisanego w dowodzie osobistym. Pieczęć elektroniczna obejmuje oprogramowanie wraz z określeniem jego uprawnień. 3. Pieczęć elektroniczna, o której mowa w ust 2, musi dodatkowo posiadać datę ważności. Nie jest możliwe zapisanie w warstwie elektronicznej oprogramowania z pieczęcią o dacie ważności wcześniejszej, od daty zapisanej w wewnętrznym datowniku dowodu osobistego.	Na chwilę obecną certyfikaty CVC nie są wykorzystywane do aktualizacji oprogramowania. Ze względu na fakt, że w tym wypadku mogłaby być konieczna w mechanizmy niskopoziomowe (np. warstwę usługową analogiczną do usług Global Platform) certyfikacja tego rozwiązania mogłabybyć długa i kosztowna	§17 (zapisywanie aplikacjipo etapie personalizacji) 1. Zapisywanie oprogramowania i danych w warstwie elektronicznej dowodu chronione jest za pomocą mechanizmów DAP opisanych w specyfikacji: Global Platform Card Specification Version 2.1. 2. Minister SWiA zapisuje w warstwie elektronicznej dowodu osobistego dane służące do weryfikacji danych chronionych mechanizmami DAP. 3. Minister SWiA może zapisywać w warstwie elektronicznej dowodu osobistego dane i oprogramowanie z pominięciem technologii wymienionej w pkt. 2. 4. Zapisywane oprogramowanie nie narusza certyfikacji oprogramowania zainstalowanego w części elektronicznej dowodu osobistego.
18		§18 1. Dowód osobisty pozwala zainstalowanemu na nim oprogramowaniu na działanie wyłącznie w ramach uprawnień, o których mowa w §17 ust. 2 2. Uprawnienia oprogramowania uruchomionego przez inne oprogramowanie w dowodzie osobistym to część wspólna uprawnień tych oprogramowań 3. Warstwa elektroniczna dowodu osobistego zapobiega wykonywaniu przez uruchomione oprogramowanie działań, na przeprowadzenie których nie pozwalają uprawnienia tego oprogramowania, określone w ust. 2. Zapobieganie to jest skuteczne także w przypadku błędnej lub złośliwej implementacji uruchomionego oprogramowania.	Na chwilę obecną certyfikaty CVC nie są wykorzystywane do aktualizacji oprogramowania. Ze względu na fakt, że w tym wypadku mogłaby być konieczna w mechanizmy niskopoziomowe (np. warstwę usługową analogiczną do usług Global Platform) certyfikacja tego rozwiązania mogłabybyć długa i kosztowna	§18 (zapis i modyfikacja danych specyficzne dla aplikacji) 1. Dopuszcza się generowanie kluczy kryptograficznych i osadzanie certyfikatu kwalifikowanego przez podmiot świadczący usługę wydawania certyfikatów kwalifikowanych wpisany do rejestru podmiotów kwalifikowanych prowadzonego zgodnie z ustawą o podpisie elektronicznym z dnia 15 listopada 2001 2. Warstwa elektroniczna dowodu osobistego dopuszcza wykonanie czynności wymienionych w ust. 1 wyłącznie jeśli podmiot świadczący usługę wydawania certyfikatów kwalifikowanych posługuje się danymi umożliwiającymi weryfikację uprawnienia do wykonania wymienionych czynności. 3. Dopuszcza się zapisywanie i modyfikację danych w obrębie warstwy elektornicznej dowodu osobistego przez aplikacje w niej umieszczone, w zakresie przydzielonych im uprawnień. 4. Zapis danych i oprogramowania w warstwie elektronicznej dowodu osobistego po dokonaniu czynności aktywacji certyfikatu dowodu osobistego dokonywany zgodnie ze standardami nie posiadającymi ograniczeń licencyjnych.
20	4	Po finalizacji podpisu osobistego Centrum Certyfikacji przesyła do dowodu osobistego sfinalizowany podpis bezpiecznym kanałem	Podpis powinien być przesyłany do aplikacji. Z tego powodu zapis wychodzi poza delegację	wykreślić

21	1. 1)	proces finalizacji podpisu osobistego następuje w tym samym dniu i w czasie nie dłuższym niż określony w polityce certyfikacji dla podpisu osobistego od momentu, w którym utworzone zostały dane, o których mowa w ust 1.	1. nie ma powodu ograniczania procesu finalizacji podpisu do tego samego dnia. Z powodzeniem możnaby pozostawić samą politykę certyfikacji 2. Brak wskazanego artykułu przy ustępie	proces finalizacji podpisu osobistego następuje w czasie nie dłuższym niż określony w polityce certyfikacji dla podpisu osobistego od momentu, w którym utworzone zostały dane, o których mowa w art 20 ust 1.
21	1 2) d)		brak wskazanego artykułu przy ustępie	
21	1 2) e)	finalizacja podpisu osobistego nie narusza warunków polityki certyfikacji właściwych dla podpisującego	bez wskazania tych warunków trudno mówić o ich weryfikacji	nie ma przesłanek do stwierdzenia, że finalizacja podpisu osobistego nie narusza warunków polityki certyfikacji właściwych dla podpisującego
22	1	Ograniczona identyfikacja wymaga użycia interfejsu stykowego lub nawiązania bezpiecznego kanału pomiędzy dowodem osobistym a czytnikiem przy wykorzystaniu kodu zawartego w warstwie graficznej dowodu lub hasła (PIN). Rodzaj wymaganego kodu lub hasła (PIN) jest ustalony dla każdego sektora oddzielnie i określony w certyfikacie dostępu dla tego sektora	1. Trudno mówić o podaniu PIN służącego do nawiązania połączenia po weryfikacji uprawnień, która tego połączenia wymaga. 2. w przypadku zaakceptowania art 7 pkt 3 punkt staje się zbędny	wykreślić (przemodelowania i wyczyszczenia wymaga całość paragrafów dotyczących RI - warunki zostały wyspecyfikowane w paragrafie 25 i to należy pozostawić)
22	2		w przypadku zaakceptowania art 7 pkt 3 - zbędny	wykreślić
22	2		w przypadku zaakceptowania art 7 pkt 3 - zbędny	wykreślić
23	1	§ 23. 1. Dokonując uwierzytelnienia ograniczonej identyfikacji terminal wykorzystuje certyfikat ograniczonej identyfikacji wystawiony dla posiadacza, a w szczególności dane do weryfikacji informacji uwierzytelniającej wskazane tym certyfikatem.	użycie certyfikatu ograniczonej identyfikacji - tego samego dla wszystkich sektorów - powoduje, że ZAWSZE będzie możliwe łączenie sesji pomiędzy sektorami	wykreślić
23	4 1)	4. Uwierzytelnianie ograniczonej identyfikacji nie pozwala na uwierzytelnienie posiadacza w każdym z następujących przypadków: 1) terminal wykorzystuje dane do weryfikacji ograniczonej identyfikacji przypisane do innej osoby lub do innego sektora;	w jaki sposób sektor ma to stwierdzić, skoro nie zna tożsamości osoby?	wykreślić
23	4 3)	3) do utworzenia informacji uwierzytelniającej wykorzystano dane do składania informacji uwierzytelniającej przypisane do innej osoby.	w jaki sposób sektor ma to stwierdzić, skoro nie zna tożsamości osoby?	wykreślić
26	2		to wymaganie dotyczące sektora - poza delegacją	wykreślić
26	2		to wymaganie dotyczące sektora - poza delegacją	wykreślić
27	1	§ 27. Identyfikator posiadacza w sektorze nie ulega zmianie w przypadku wymiany dowodu osobistego tego posiadacza.	co w przypadku gdy karta zostanie skompromitowana? Nawet w przypadku wydania nowej karty, złodziej będzie mógł posługiwać się starą (nie będzie zmieniony identyfikator RI)	wykreślić
28	2	2. Dowód osobisty realizuje funkcje karty ubezpieczenia zdrowotnego wyłącznie po uwierzytelnieniu terminala, o którym mowa w § 11, z zastosowaniem certyfikatu dostępu wystawionego dla ministra właściwego do spraw zdrowia.	Tutaj warto wskazać, że karta ubezpieczenia zdrowotnego ma własne wymagania dotyczące udostępniania danych. Te regulacje powinny być zapisane w odrębnych przepisach. CWA 15974 rozdział 7.3 opisuje funkcje bezpieczeństwa, jakie powinny być realizowane przez kartę ubezpieczenia zdrowotnego. Lista ta może być rozszerzana w szczególności o mechanizmy wymienione w par 28 pkt 2	wykreślić
29	1		nie wiadomo o jaką pieczęć chodzi trzeba doprecyzować. Bez tej wiedzy można tylko wykreślić	wykreślić
31	1	Dane do składania informacji uwierzytelniającej oraz dane do składania informacji uwierzytelniającej ograniczonej identyfikacji są instalowane w warstwie elektronicznej dowodu osobistego w trakcie procesu jego personalizacji	nie jest jasne o jakie dane do składania informacji uwierzytelniającej chodzi (powiązane z certyfikatem dowodu osobistego?, active authentication?)	Dane do składania podpisu weryfikowanego certyfikatem dowodu osobistego oraz dane do składania informacji uwierzytelniającej ograniczonej identyfikacji są instalowane w warstwie elektronicznej dowodu osobistego w trakcie procesu jego personalizacji

32	1	Dane do składania podpisu osobistego są generowane przez dowód osobisty na żądanie posiadacza	Zapis nie jest zgodny z ustawą art 19 ust 4 - ponieważ certyfikat nie może być wydany przed genracją kluczy ani data jego obowiazywania nie może być wcześniejsza niż gneracja kluczy. Dodatkowo genracja w trakcie aktywacji utrudnia proces ochrony tych danych. Przejęcie całego klucza przez użytkownika umożliwia mu składanie podpisów z pominięciemi finalizatora. Z tego względu rozwiązaniem powodującym mniejsze zagrożenia jest ganerowanie kluczy po stronie Centrum Certyfikacji, gdzie procedury i zabezpieczenia gwarantują należyte zabezpieczenie kluczy. Generacja kluczy dla podpisu osobistego wymaga jej przeprowadzenia w bezpiecznym środowisku, które zapewnia poufną wymianę sekretu z systemem centralnym. Generacja kluczy w trakcie aktywacji nie daje możliwośći rzeczywisstej kontroli użytkownika nad tym procesem, jedst działaniem pozornym a jednocześnie bardzo kosztownym.	Dołączyć do § 30 ust 1 generację kluczy podpisu osobistego. § 32 ust 1 uzykuje treść: Centrum Certyfikacji wystawia certyfikat podpisu osobistego po wygenerowaniu danych do składania podpisu osobistego.
32	2	2. Centrum Certyfikacji wystawia certyfikat podpisu osobistego po wygenerowaniu danych do składania podpisu osobistego i dokonuje aktywacji tego certyfikatu.	j.w.	§ 32 ust. 2 uzyskuje treść: Centrum Certyfikacji dokonuje aktywacji certyfikatu podpisu osobistego na żądanie posiadacza.
32	4	4. Protokół realizujący wymagania opisane w § 19 - 21 zapewnia możliwość wykrycia przez Centrum Certyfikacji faktu wygenerowania poza dowodem osobistym danych, o których mowa w § 20 ust. 1. Warunek ten dotyczy w szczególności przypadku ujawnienia danych do składania podpisów osobistych osobom trzecim.	Jakie są konsekwencje ujawnienia takich danych dla administracji publicznej? Należy rozważyć czy ujawnienie tych danych nie jest większym zagrożeniem, od tego że użytkownik posiada skompromitowaną kartę.	wykreślić
34	1	§ 34. 1. Aktywacja certyfikatów dowodu osobistego, certyfikatu ograniczonej identyfikacji oraz certyfikatu podpisu osobistego może być dokonana w dowodzie osobistym jedynie przez zaufany terminal.	zapis narzuca nieimplementowaną w dotychczasowych rozwiązaniach metodę aktywacji.	wyrkeślić
34	3	3. Warstwa elektroniczna dowodu osobistego nie umożliwia wykorzystania określonej funkcji, o ile oprogramowanie dowodu osobistego nie potwierdzi, że dana funkcja jest aktywna.	zapis narzuca niewygodną w realizacji metodę weryfikacji aktywacji. Większość implementacji będzie blokować dostęp do nieaktywnych funkcji, a nie potwierdzać czy dana funkcja jest dostępna	Warstwa elektroniczne dowodu osobistego odmawia wykonania funkcji nieaktywnej
OSR	2	Dodatkowo skierowany zostanie do konsultacji do następujących podmiotów: • Rzecznik Praw Obywatelskich, • Generalny Inspektor Ochrony Danych Osobowych, • Polska Izba Informatyki i Telekomunikacji, • Polskie Towarzystwo Informatyczne.	Wymagane jest skonsultowanie ww. rozporządzenia z samorządzem ze względu na wpływ przedmiotowej regulacji na gminy	
OSR	3	Projektowana regulacja nie pociąga za sobą obciążenia budżetów jednostek samorządu terytorialnego.	Wymaganie - w szczególności zwiazane z generowaniem kluczy podpisu osobistego nakładają bardzo duże wymagania i koszty na jednostki samorządu terytorialnego. Wymagana będą nie tylko inwestycje w infrastrukturę ale także szkolenia persolnelu i przygotowanie jego pod względem procedury bezpiecznej eksploatacji.	