

**Opinia KIGeIT o projekcie z dnia 7 lutego 2011 r. projektu rozporządzenia
Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań technicznych
dla warstwy elektronicznej dowodu osobistego oraz protokołu komunikacji
elektronicznej z dowodami osobistymi**

KIGeIT dziękuje za zaproszenie do wzięcia udziału w konsultacjach projektu powyższego rozporządzenia przesłanego pismem z dnia 14 lutego 2011 r. nr DP-I-0231-1116/10/AK, które otrzymaliśmy 21 lutego 2011 r.

1. Uwagi ogólne

Uważamy, że jakość obecnego projektu nie kwalifikuje go jeszcze do przyjęcia a zakres modyfikacji to niestety nie tylko poprawki kolejnych akapitów ale przemyślenie całości a zwłaszcza poprzedzenie pisania realnymi pracami analitycznymi, specyfikacją i projektem LUB mocne odchudzenie dokumentu by nie dotyczył kwestii tego „jak” coś ma być realizowane, a raczej skupiło się na części „co i dlaczego” ma być osiągnięte, wg jakich kryteriów, standardów i gdzie będą opublikowane szczegółowe specyfikacje jak już powstaną.

Obecna postać wygląda jak pomieszanie wymagań i opisu ich realizacji, ale sporządzonego przez laików a nie ekspertów z dziedziny, czyli ani nie widać dobrze celu większości wymagań ani jak to ma całościowo funkcjonować, zwłaszcza mając wiedzę na temat tego co jest a co nie jest możliwe, dostępne lub ustandaryzowane w świecie kart elektronicznych i bezpieczeństwa informacji.

2. Wady definicji

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) aktywny punkt zaufania...

Niejasna definicja

2) algorytm RSA...

Wadliwa definicja – czy dowolny algorytm asymetryczny używany do takich celów staje się „algorytmem RSA”?

3) bezpieczny kanał...

Definicja powinna odnosić się bardziej do składowych usług bezpieczeństwa, które są przez ten kanał realizowane dla uzyskania wymaganego efektu ochrony przez czymś (np. usługi poufności, integralności, uwierzytelnienia, autentyczności itp. „Szyfrowane połączenie” jest wskazaniem na sposób realizacji usług poufności, ale już dla „wykrycia zmian tych informacji dokonanych przez osoby trzecie” nie wskazano analogicznego sposobu/mechanizmu służącego do osiągnięcia takiego celu. Nierówna definicja i w detalach nieprecyzyjna a nawet błędna – np. czy na pewno chodzi o wykrycie zmian dokonanych przez „osoby trzecie”, czy może dowolnych modyfikacji? I czy faktycznie bezpieczny kanał wykrywa i rozróżnia zmiany wykonane przez „osoby trzecie”?

5) Centrum Certyfikacji...

Powinna to być raczej logiczna jednostka, formalny zarządca certyfikatów a nie wskazanie, iż jest to „system informatyczny”. To dość oczywiste, że realizacją wielu zadań zajmuje się „system informatyczny”, ale wiązanie zadań funkcjonalnych z ich techniczną realizacją nie w każdym przypadku jest zasadne i właściwe.

6) certyfikat...

Definicja certyfikatu nie objęła w końcu osób fizycznych, czyli w sumie podmiotu najistotniejszego dla dowodu osobistego.

7) certyfikat aktualizacyjny – certyfikat wystawiony przez Centrum Certyfikacji, wskazujący nowy punkt zaufania, weryfikowalny wcześniejszym punktem zaufania;

Jeśli to jest „certyfikat” to wg definicji ma to być zaświadczenie elektroniczne przyporządkowujące dane weryfikacyjne do osoby prawnej lub jednostki organizacyjnej (...) więc warto by wskazać nie tylko to, że wskazuje nowy punkt dostępu ale do kogo te dane weryfikacyjne przyporządkowuje ten certyfikat? I może nie tylko wskazanie nowego punktu zaufania ale ... ZAWIERA nowy punkt zaufania gdyż wg definicji „punktu zaufania” jest właśnie takimi danymi („dane do weryfikacji certyfikatów wystawionych przez Centrum Certyfikacji”).

Certyfikat ma zawierać dane do weryfikacji więc pośrednio, wg takich nieprecyzyjnych definicji wychodzi, że certyfikat aktualizacyjny zawiera punkt dostępu a nie „wskazanie na punkt dostępu”.

8) certyfikat dostępu...

Definicja dubluje część definicji „certyfikatu”, ale niespójnie i np. wprowadza „jednostkę organizacyjną”, jako coś odmiennego od „jednostki organizacyjnej nieposiadającej osobowości prawnej”.

Zmienia się też swobodnie liczbę mnogą z pojedynczą, co może powodować wątpliwości interpretacyjne („certyfikat”... „dla osób” – czy chodzi o jakąś grupę opisywaną jednym certyfikatem?).

9) certyfikat terminala...

Zbyt uproszczona definicja – jak należy rozumieć to „jednoznaczne przypisanie certyfikatu” do „danego terminala”? Zwłaszcza na gruncie definicji samego „certyfikatu”? Czy „wystawiony” jest tożsamy z „opatrzone pieczęcią elektroniczną wystawcy certyfikatu”? A jeśli nawet takie domniemanie jest poprawne, to pieczęcią którego wystawcy certyfikatu albo wystawcy którego certyfikatu? Czy posiadanie dowolnego „certyfikatu dostępu” nadaje uprawnienie do wystawiania dowolnych „certyfikatów terminala”?

Co zawiera certyfikat terminala poza „danymi do weryfikacji pieczęci elektronicznej lub danymi do weryfikacji informacji uwierzytelniającej”?

10) czytnik..

Dla zachowania jakiegoś porządku definicji może lepiej „z warstwą elektroniczną dowodu osobistego” zamiast “z dowodem osobistym”? (patrz definicja 11) finalizacja podpisu...)

11) finalizacja podpisu osobistego...

Czynność Centrum Certyfikacji, która nie została wymieniona w definicji tego co robi system informatyczny mający taką nazwę („Centrum Certyfikacji”) – wymaga rozszerzenia definicji CC lub jej całkowitą zmianę.

12) hasło (PIN)...

W praktyce dotyczącej kart elektronicznych „hasło” i „PIN” to dwa różne nieznacznie pojęcia, które nie są tożsame: hasło niekoniecznie musi być ograniczane do cyfr a PIN, jak sama nazwa wskazuje jest numerem identyfikacyjnym składającym się z cyfr. Nieszczęśliwe wydaje się wskazanie w definicji iż PIN to jest ciąg cyfr ustalanych przez posiadacza dowodu, gdyż zamyka to drogę do nazywania tym określeniem innego kodu o identycznym zastosowaniu ale ustalanego przez kogoś innego niż posiadacz dowodu (np. generowanego losowo przez system IT).

„których znajomość jest niezbędna do wykonania przez warstwę elektroniczną dowodu osobistego niektórych funkcji” – znajomość przez kogo/co? Przez posiadacza, przez sam dowód czy jakąś osobę trzecią?

13) klucz kryptograficzny...

Błędy stylistyczne w definicji (np. „informację”.

Zbędne wprowadzanie nowych pojęć: „cyfrowe podpisywanie”.

Skoro w innej definicji mamy pojęcie „algorytmu kryptograficznego” („algorytm RSA”) to pożądane jest wskazanie w definicji klucza jego związku z algorytmem.

14) kontener...

Niejasna i niekompletna definicja – w treści rozporządzenia mówi się np., że „kontener coś wykonuje” co nie pasuje do tej definicji. Należy ujednoclić podejście: albo kontener zawiera dane wykorzystywane w trakcie wykonywania czegoś albo faktycznie on sam coś wykonuje, ale wtedy nie może to być po prostu „część pamięci...”. Wskazanie EEPROM być może nadmiarowo wskazuje dokładnie rodzaj pamięci, w której kontener może się znajdować a praktyka niektórych rozwiązań może używać różnych rodzajów pamięci dla przechowania różnych informacji mieszczących się pod pojęciem „kontenera”.

15) pieczęć elektroniczna...

W definicji mówi się, że pieczęć to są dane, ... które są powiązane z danymi, do których się odnoszą w taki sposób, że każda późniejsza zmiana danych jest wykrywalna – ale nie jest jednoznacznie jasne, o których danych jest mowa w każdym wystąpieniu pojęcia „dana/dane” w tej definicji.

21) warstwa elektroniczna dowodu osobistego...

Ponieważ rozporządzenie dotyczy również danych znajdujących się w tej „warstwie elektronicznej”, należało by również wymienić „dane” wśród istotnych cech tego co się składa na warstwę elektroniczną, skoro wymienia się np. „oprogramowanie”. W praktyce oprogramowanie jest personalizowane i profilowane przez te dane i zmienia swoje działanie zależnie od wartości „danych” czyli dane w podobny sposób jak „oprogramowanie” wpływają na zachowanie się tej warstwy elektronicznej.

22) weryfikacja certyfikatu...

Część wymagań, które mają być składnikiem „weryfikacji certyfikatu” jest raczej założeniem organizacyjnym, które nie jest łatwe (lub jest niemożliwe) do „weryfikacji” przez podmiot i system wykonujący czynność

weryfikacji certyfikatu. Pod tym względem definicja wydaje się być zbyt uproszczoną i niepraktyczną.

Przez analogię można by też oczekiwać, iż definicji weryfikacji certyfikatu będzie w dużym stopniu podobna do definicji „weryfikacji informacji uwierzytelniającej” a niestety nie jest – np. kto wykonuje to sprawdzenie, o którym jest mowa w definicji „weryfikacji certyfikatu”?

26) zaufany terminal...

Wadliwa konstrukcja mówiąca, że zaufany terminal to... zaufany terminal o pewnych cechach dodatkowych.

3. Ogólne problemy z zakresie definicji:

Nadmiarowość/lokalność definicji – wprowadza się niepotrzebnie własne, lokalne dla rozporządzenia definicje terminów używanych w innych ustawach i rozporządzeniach związanych z informatyzacją administracji (np. ustawą o podpisie elektronicznym) co w szerszej perspektywie powoduje problemy wynikające z różnic definicyjnych. Zgodnie z jednym aktem produkowane są np. certyfikaty, które są „używane” przez systemy i w interakcjach regulowanych przez inne akty prawne, ale w obu aktach powołuje się lokalne definicje dla finalnie tego samego obiektu/relacji, różnice się w szczegółach. Przykładowo definicja „certyfikatu” jest odmienna w różnych aktach prawnych. Podobnie „klucz kryptograficzny”, „pieczęć elektroniczna”, hasło (PIN) itd.

Niektóre definicje niepotrzebnie zawierają ponownie fragmenty innych definicji gdy zawierają pojęcia z tych innych definicji. Np.. W definicji „wewnętrznego datownika” jest „... będącą datą wystawienia certyfikatu terminala przez podmiot posiadający zaufany certyfikat dostępu” a definicja certyfikatu terminala już mówi, że wystawia go podmiot posiadający certyfikat dostępu.

Podobnie w „zaufany certyfikat dostępu” podaje się to komu jest on wydany co jest dublowaniem definicji samego certyfikatu dostępu używanego tutaj już jako pojecie własne.

4. Uwagi do poszczególnych paragrafów:

§ 3. 1 pkt 5)

ISO 7816-7 – w jakim celu/zakresie warstwa elektroniczna ma zawierać implementację SCQL? Nie wynika to z żadnych innych postanowień rozporządzenia lub innych wskazanych standardów dla dowodu. Wymaganie to wydaje się nieuzasadnione a implementacje tej części nowy są na rynku praktycznie nieistniejące.

„14443-2 z komunikacją typu B” – bardzo istotna decyzja, ograniczająca konkurencję w sposób nieuzasadniony. Praktycznie każdy produkowany obecnie czytnik/terminal kart bezstykowych zgodnych z ISO 14443-2 wspiera OBA protokoły (Type A i Type B) więc nie ma uzasadnienia dla ograniczania protokołu komunikacyjnego dowodu wyłącznie do typu B. W warstwie funkcjonalnej, prędkości komunikacji, protokole komunikacyjnym poziomu APDU nie ma różnic pomiędzy tymi odmianami protokołu bezstykowego (Type A i Type B) i warstwa elektroniczna powinna być zgodna ALTERNATYWNIE z dowolnym z obu wariantów komunikacji bezstykowej zgodnej z ISO 14443.

Część druga ISO 14443 nie jest wystarczająca dla zdefiniowania protokołu komunikacyjnego z użyciem interfejsu bezstykowego.

§ 3.6. Ponieważ zgodnie z definicją „kontener” to obszar pamięci EEPROM to niezbyt jasne jest pojęcie jego „aktywacji”. Niejasny jest zakres „niezależnego zarządzania”, choćby w kontekście § 4.1. i min. jednego aktywnego „punktu zaufania” – czy jest on wspólny dla 7 kontenerów? Zagadnienie „niezależnego zarządzania” kontenerami wymaga rozwinięcia.

§ 4.3. Dopiero w tym paragrafie pojawia się informacja, iż certyfikat dostępu zawiera uprawnienia (!) a to jest najistotniejsza cecha tego certyfikatu. Powinna znaleźć się w definicji lub innym punkcie opisującym jego rolę w dowodzie i terminalu dostępu.

§ 4.4. Niepotrzebny punkt – powiela część definicji zaufanego certyfikatu dostępu.

§ 5.1. Warstwa elektroniczna nie może być bezpiecznym urządzeniem wg polskiej ustawy, gdyż tam jest to połączenie komponentu technicznego i aplikacji podpisującej. Całkowicie błędne założenia na gruncie aktualnej ustawy o podpisie el. Oprogramowanie podpisujące i stawiane mu wymagania nie może być zrealizowane w ramach warstwy elektronicznej DO. Prawdopodobna korekta tej regulacji w nadchodzącej nowelizacji ustawy o podpisie el. usunie problem niezgodności definicji „bezpiecznego urządzenia...” w EU i PL.

Warstwa elektroniczna zawiera kontener odpowiedzialny za składanie podpisu bezpiecznego ale wymaganie by cała „warstwa elektroniczna DO” była bezpiecznym urządzeniem jest nadmiarowa, powoduje co najmniej trudności techniczne i formalne (np. konieczność certyfikacji).

Raczej wydzielona część warstwy elektronicznej (jak to wskazano w pkt. 2) może pełnić taką rolę i być „bezpiecznym urządzeniem”. Inne części (kontenery) mają funkcjonalność tak odmienną od bezpiecznego

urządzenia (SSCD), że raczej nie będą spełniały szczegółowych wymagań dla SSCD. Być może zapisy o zgodności wybranych cech warstwy elektronicznej z określonymi precyzyjnie cechami SSCD miałyby tutaj zastosowanie. Np. taki zapis: *"Warstwa elektroniczna dowodu osobistego spełnia wymagania bezpieczeństwa stawiane dla bezpiecznego urządzenia do składania podpisu w rozumieniu art. 18 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.2)."*

§ 5.2. *"Warstwa elektroniczna dowodu posiada wydzielony kontener służący do składania bezpiecznego podpisu elektronicznego..."* – ponieważ definicja kontenera określa go jako „obszar pamięci EEPROM” to niepoprawne wydaje się wskazanie iż kontener „służy do składania podpisu”. Proponowana zmiana „...wydzielony kontener zawierający dane do składania bezpiecznego podpisu...”.

§ 5.3. Warstwa elektroniczna DO nie została wystarczająco precyzyjnie zdefiniowana i nie określono jej granic co stanowi fundament certyfikacji wg wymienionych standardów. Przedmiotem certyfikacji w przypadku kart elektronicznych jest określony zespół sprzętowo-programowy o ściśle zdefiniowanej funkcjonalności i sposobie używania. Najmniejsze odstępstwo od tego zakresu lub scenariusza użycia unieważnia status certyfikacji, więc oczekiwanie certyfikacji dla całej warstwy elektronicznej (globalnie) jest bardzo trudne w utrzymaniu i zarządzaniu gdyż wiele modyfikacji w zakresie dodawania/modyfikacji aplikacji i danych (w ramach poszczególnych kontenerów) będzie naruszało przedmiot certyfikacji i w wielu wypadkach unieważniało certyfikację CALEJ warstwy elektronicznej niezależnie od tego, że tylko wybrana część/kontener będzie podlegał modyfikacji. Zalecane jest precyzyjniejsze zawężenie zakresu objętego certyfikacją i/lub podzielenie warstwy elektronicznej na oddzielne grupy (np. na poziomie kontenerów), które są oddzielnie specyfikowane i certyfikowane zgodnie z wymienionymi standardami.

Norma ISO/IEC 15408 nie określa żadnych konkretnych cech funkcjonalnych i bezpieczeństwa dla produktu/systemu certyfikowanego zgodnie z tą normą. Norma ta wymaga określenie precyzyjnego profilu zabezpieczeń i proces certyfikacji „bada” zgodność i dokładność implementacji założeń tego profilu zabezpieczeń. Wskazywanie jedynie samego poziomu pewności (EAL) oznacza oczekiwanie by produkt realizował „coś” zgodnie z założeniami profilu zabezpieczenia z określonym poziomem pewności, zależnym od dogłębności badań w procesie certyfikacji. Niemniej bez zdefiniowania „co” i wg jakiego profilu ma być certyfikowane jest fundamentalnym błędem specyfikacji gdyż produkty posiadające ten sam certyfikat mogą posiadać diametralnie inne funkcje i sposoby ich realizacji, gdyż każdy z nich może sobie definiować w swoim profilu zabezpieczeń inne metody, cele i środki ich realizacji.

Obejmowanie procesem certyfikacji mgliście zdefiniowanego i bardzo szerokiego zakresu rozwiązania informatycznego bardzo podnosi koszty tego procesu i wydłuża czas certyfikacji.

Zupełnie niezrozumiałym wymaganiem jest posiadanie certyfikatu FIPS 140-2 Level 3 przez warstwę elektroniczną DO, gdyż jest to standard/norma stosowana na rynku amerykańskim i w zakresie SSCD w EU była stosowana przejściowo do czasu zdefiniowania profilu i wymaganego poziomu pewności na bazie normy Common Criteria (ISO/IEC 15408). Oba procesy certyfikacyjne są w zdecydowanej większości podobne co do celu. Wymaganie od warstwy elektronicznej OBU certyfikatów równocześnie nie znajduje potwierdzenia w praktyce obrotu gospodarczego na rynku kart elektronicznych.

Z drugiej strony, oba standardy procesów certyfikacyjnych stosowane są na odmiennych rynkach i dotyczą produktów przygotowywanych dla tych odmiennych rynków co finalnie powoduje, iż produkty certyfikowane pod tymi dwoma standardami zwykle chociaż nieznacznie różnią się między sobą funkcjonalnie, w zakresie dopuszczalnych scenariuszy użycia, dopuszczalnych wartości zmiennych parametrów konfiguracyjnych itd.. lub certyfikowane są w różnych momentach czasu i zawierają nieznaczne różnice w swoich konfiguracjach (np. nowszy model mikroprocesora, nieznacznie poprawiona wersja oprogramowania itp.).

Co do zasadniczych funkcjonalności produkty te są tożsame, ale nawet te drobne różnice powodują, że istniejące na rynku lub przygotowywane produkty posiadające OBA certyfikaty jednocześnie, NIE SĄ w rzeczywistości tym samym produktem i oczekiwanie iż dokładnie TEN SAM produkt posiada oba certyfikaty jest bardzo nietypowe, kosztowne i ograniczające konkurencję.

§ 6. Wskazane w tym paragrafie „wymaganie” jest bardzo niejasne i stosunkowo szybko może przestać być spełniane przez wydane już dokumenty. Nie jest jasno określone iż wymaganie takie dotyczy momentu wydawania dokumentu co z trudem (i wysokim nakładem środków) można jeszcze próbować zapewnić. W kolejnych miesiącach po wydaniu dokumentu, dotyczące go rozporządzenie nakłada w § 6 na warstwę elektroniczną wymagania, które mogą być już nie spełniane – rodzi się pytanie czy DO przestaje wtedy spełniać wymagania rozporządzenia?

§ 7.1. pkt 2. Funkcjonalność dowodu osobistego nie obejmuje tworzenia pieczęci elektronicznej gdyż wg definicji Rozporządzenia jest ona tworzona przez pieczętującego, który jest osobą prawną lub jednostką organizacyjną niemającą osobowości prawnej. Jeśli w świetle niniejszego punktu pieczęć miałaby być tworzona "z użyciem odpowiednich danych zapisanych w dowodzie osobistym" to raczej nie może to być pieczęć

elektroniczna.

§ 7.1. pkt 3 Wskazane założenie może być niepoprawne jedynie jeśli pod pojęciem „innych danych, dostępnych niezależnie od terminala,” będą kryły się odpowiednie sekrety (klucze) zainstalowane w terminalu. Wymaganie wydaje się mieć wewnętrzną sprzeczność gdyż konstrukcja „...wykorzystując wyłącznie dane zarejestrowane...” jest sprzeczna z dalszą częścią wymagania gdzie dodaje się „także przy wykorzystaniu innych danych”. Czyli albo „jedynie” albo „dane z komunikacji + inne dane”. Wykorzystując „inne dane” już nie realizuje się „wykorzystania jedynie danych...”.

Należało by zapis ten zmodyfikować do bardziej konkretnej i poprawnej postaci odwołującej się do wszelkich metod i informacji za wyjątkiem sekretów używanych przez terminal.

§ 8.1. Ponieważ czytnik zdefiniowano jako urządzenie pośredniczące w komunikacji terminala z DO powinno się dopuszczać nawiązywanie bezpiecznego kanału pomiędzy terminalem a DO a nie pomiędzy czytnikiem a DO gdyż wydaje się, iż intencją ustawodawcy jest rozgraniczenie roli czytnika (relatywnie prostego i niezaufanego urządzenia zapewniającego komunikację z DO) i wyposażonego w jakąś logikę, bezpieczeństwo i odpowiedzialne zadania związane z zaufaniem, terminala. W szczególności powinna być dopuszczalna sytuacja gdy bezpieczny kanał jest nawiązywany pomiędzy warstwą elektroniczną DO a systemem informatycznym usługodawcy bez jakichkolwiek pośrednich miejsc gdzie kanał ten jest „przerwany” (tzn. bezpieczeństwo "end-to-end"). Czytnik zwykle jest urządzeniem znajdującym się poza kontrolą posiadacza dowodu, więc nawiązywanie bezpiecznego kanału, który „kończy się na czytniku” w zasadzie pozbawia posiadacza kontroli nad tym czy transmisja poufnych informacji odbywa się w sposób bezpieczny jako, że docelowym adresatem tej transmisji nie jest czytnik ale terminal! Uregulowanie jedynie bezpieczeństwa kanału od DO do czytnika i brak regulacji co do jakości kanału od czytnika do terminala czyni całą wymianę informacji pomiędzy terminalem a DO niezaufaną.

Ponieważ definicja „bezpiecznego kanału” wskazuje iż informacje przesyłane tym kanałem są szyfrowane, to oznacza iż wg § 8.1 czytnik byłby urządzeniem deszyfrującym treść komunikacji, czyli musiałby się posługiwać określonym algorytmem kryptograficznym, kluczami i protokołem formującym kanał – a to wydaje się raczej zadaniem dla bardziej zarządzanego i kontrolowanego uczestnika interakcji z DO jakim jest terminal lub system IT pełniący rolę terminala.

Praktyką rynkową jest, że czytniki są urządzeniami relatywnie prostymi i niepełniącymi ról związanych z bezpieczeństwem komunikacji a jedynie odpowiadają za obsługę interfejsu komunikacyjnego do przesyłania do/z karty określonych jednostek informacyjnych (zwykle tzw. komunikatów ADPU i odpowiedzi na te komunikaty). Nakładanie na czytnik zaawansowanych zadań ochrony komunikacji z DO, faktycznie zaciera różnicę (skądinąd bardzo rozsądną) między czytnikiem a terminalem, gdyż czytnik zaczyna być *de facto*... terminalem.

§ 8.3. Zupełnie niezrozumiałe są wymagania bazujące na alternatywie (LUB) trzech zupełnie odmiennych metod/mechanizmów. W jaki sposób oczekuje się realizacji uwierzytelnienia dowodu „...przez wykorzystanie kodu zawartego w warstwie graficznej dowodu osobistego”? Być może intencją ustawodawcy jest by uwierzytelnienie DO realizowane było pod warunkiem spełnienia pewnych przesłanek – co nie zostało jasno przekazane w niniejszym punkcie.

Czy zapis iż przypadek uwierzytelnienia opisywany w tym punkcie może być „dokonany z wykorzystaniem interfejsu stykowego” należy rozumieć, że nie może on być wykonywany przez interfejs bezstykowy? Czy uprawnione organy „nie mogą” wykorzystywać uwierzytelnienia DO przez taki interfejs czy może dla takiego interfejsu określa się inne wymagania? A jeśli tak to jakie są to wymagania?

§ 8.4. Certyfikat dostępu może być odczytany PO nawiązaniu jakiegoś kanału komunikacyjnego. Jeśli w certyfikacie ma być zawarte wymaganie używania kodu lub hasła a w świetle pkt. 1 do nawiązania bezpiecznego kanału pomiędzy warstwą elektroniczną dowodu osobistego a czytnikiem wymagane jest wykorzystanie kodu zawartego w warstwie graficznej dowodu osobistego lub hasła (PIN), to zdarzenia te wydają się być od siebie uzależnione w sposób niemożliwy do realizacji – odczyt certyfikatu wymaga istnienia jakiegoś kanału komunikacji a samo nawiązanie kanału wymaga... wiedzy czy konieczne jest używanie kodu/hasła, która ta wiedza jest ... w certyfikacie dostępu.

Cały § 8. W sposób niezrozumiały lub niepoprawny łączy i miesza zagadnienie nawiązywania zabezpieczonego kanału i realizacji funkcji uwierzytelniania DO. Jeśli intencją ustawodawcy jest by uwierzytelnianie DO było częścią składową protokołu budowania tego zabezpieczonego kanału to należy przereklamować cały § 8 dla precyzyjnego oddania tych intencji.

Nie jest jasna relacja pomiędzy kodem/hasłem używanym w trakcie zestawiania kanału oraz w trakcie uwierzytelniania DO – czy to ten sam kod czy dwa odrębne kody? Jeśli DO będzie wymagał używania odrębnych kodów/hasel dla realizacji różnych funkcji to należało by to wyraźnie zdefiniować.

Pojęcia bezpiecznego kanału i jego zakresu (czy tylko do czytnika czy dalej do terminala?) również zostały przedstawione nieczytelnie.

§ 10.3 pkt 1. Ze względu na charakter rozporządzenia lepszą formą było by wskazanie iż tożsamość weryfikuje uprawniony organ by łatwiej było modyfikować w przyszłości listę organów, które taką procedurę mogą zrealizować. Jeśli już istnieje potrzeba regulacji w zakresie procedur operacyjnych i uczestników poszczególnych procesów to warto je przenieść do oddzielnego rozdziału i omówić/uregulować spójnie i globalnie dla wszystkich procesów dotyczących obsługi i używania DO.

Dodatkowo § 10.3 pkt 4 wskazuje na użycie „zaufanego terminala”. co samo w sobie pośrednio wskazuje na ograniczoną grupę podmiotów, które taki terminal posiadają, a to w sumie powoduje częściową nadmiarowość § 10.3 pkt 1 gdyż właściwy organ gminy jest wskazany przez wymóg użycia „zaufanego terminala”, który „realizuje zadania związane z wydawaniem dowodów osobistych” (na podstawie definicji zaufanego terminala + posiadacza zaufanego certyfikatu dostępu).

§ 10.4. Wartość 10 000 jest niezrozumiała w kontekście pojęć „średniej liczby prób” i definicji „hasła (PIN)” gdyż matematycznie trudno jest odgadnąć intencje ustawodawcy. Niezrozumiałe jest też dlaczego w ustępie tym jest mowa wyłącznie o „procedurze zmiany hasła lub utworzeniu nowego hasła” – jaki jest związek średniej liczby prób odgadnięcia nowego hasła z procedurą jego zmiany (matematyczny związek)?

§ 11.7. Dowód osobisty określa uprawnienia terminala na podstawie certyfikatu terminala i certyfikatu dostępu. Uprawnienia te są maksymalnymi uprawnieniami, nieprzekraczającymi uprawnień określonych certyfikatem dostępu i certyfikatem terminala.

Powinno być raczej: „*uprawnienia te są maksymalnymi uprawnieniami, nieprzekraczającymi tych uprawnień, która są określone jednocześnie w certyfikacie dostępu i certyfikacie terminala*”, gdyż proponowana postać nie oddaje poprawnie warunku stosowania sumy logicznej (AND) uprawnień pochodzących z obu certyfikatów.

§ 12. Trochę niefortunne miejsce dla tej regulacji gdyż rozdział dotyczy tylko uwierzytelniania terminala. Paragraf ten pośrednio wskazuje na BARDZO ważny aspekt bezpieczeństwa komunikacji z DO, który w minimalnym stopniu został opisany – zawiera on informację, że OBA uwierzytelnienia są warunkiem nawiązania bezpiecznego kanału, ale nie jest jasne czy tylko w takim przypadku powstaje bezpieczny kanał a wykonanie któregokolwiek z uwierzytelnień bez realizacji drugiego nie konstytuuje takiego bezpiecznego kanału.

Czy w ogóle dopuszczalna jest komunikacja z DO lub z terminalem BEZ jednego lub obu uwierzytelnień?

Jaka jest kolejność realizacji obu uwierzytelnień: czy najpierw musi zostać wykonane uwierzytelnienie terminala czy najpierw uwierzytelnienie DO? W drugim przypadku istnieje realne niebezpieczeństwo ujawnienia części informacji z DO dla nieuprawnionego terminala skoro zanim uwierzytelniono jego dane identyfikacyjnych, warstwa elektroniczna pozwoli na wykonywanie uwierzytelniania DO (które jak wiadomo oznacza „udowodnienie” iż przekazane informacje identyfikujące DO są autentyczne i dotyczą tego właśnie egzemplarza DO...).

Paragraf ten dodatkowo wskazuje na powstanie bezpiecznego kanału pomiędzy DO a terminalem co jest odmienne od opisywanego w § 8.1 "bezpiecznego kanału" pomiędzy DO a czytnikiem.

Jakie są zależności między tymi kanałami? Czy jeden kanał znajduje się „wewnątrz” drugiego kanału? Jakimi metodami/protokołami posługują się do budowy tych kanałów strony komunikujące się? Czy określa się i jakie minimalne parametry bezpieczeństwa dla obu tych kanałów (np. minimalne długości kluczy kryptograficznych, rodzaje algorytmów itp.)?

§ 13. Niezrozumiały cel, mechanizm i sposób jego osiągnięcia. Aby potwierdzić zgodność jednych danych z drugimi należało by przekazać oba ich zbiory do weryfikacji. Czy intencją tego paragrafu jest obowiązek/zalecenie odczytu automatycznego danych zawartych w warstwie graficznej i przekazywanie ich do terminala w celu potwierdzenia zgodności z analogicznymi danymi odczytanymi z warstwy elektronicznej? Jaki jest cel takiego potwierdzenia i w jakich kontekstach ma ono występować? Jakie jest cel tego procesu? Kto i kiedy ma go przeprowadzać?

Które dane mają być przekazywane bezpiecznym kanałem do terminala w myśl ostatniego zdania tego paragrafu: dane z której warstwy DO?

§ 14. Zawiera kolejny raz pewnego rodzaju nieczytelną alternatywę używania „albo” interfejsu stykowego „albo”... nieokreślonego interfejsu ale z uwierzytelnieniem DO z pomocą kodu lub hasła (i nieokreślonym wymaganiem dla istnienia lub nie uwierzytelnienia terminala).

Czy w przypadku interfejsu stykowego niewymagane jest uwierzytelnianie DO? Dlaczego w takim przypadku wydaje się, iż ustawodawca domniema autentyczności DO?

Zawarte w § 13 wymaganie na przekazywanie danych w ramach bezpiecznego kanału do terminala, pośrednio już wymusza wykonanie uwierzytelnienia DO jako kroku przygotowawczego do utworzenia bezpiecznego kanału do terminala (wg § 12). Na gruncie takiego szczególnego wskazywania konieczności uwierzytelnienia DO dla przesyłania wybranych danych warstwy graficznej, rodzi się wątpliwość czy dla przesyłania innych danych nie jest wymagane uwierzytelnienie DO? Ale jak wtedy interpretować bezpieczny kanał w myśl § 13?

Wątpliwość generalną budzi zadanie przekazywania (wg § 14) przez dowód osobisty danych, o których mowa a art. 12 ustawy gdyż... w artykule tym ustawa mówi o warstwie graficznej a nie warstwie elektronicznej. Jak sam DO miałby przekazywać, np. interfejsem stykowym wybrane dane z... warstwy graficznej??? Prawdopodobna intencja dotyczy "takich samych danych zawartych w warstwie elektronicznej" ale wymaga to jednoznacznego wskazania a nie domyślania się.

Kolejny problem to oczekiwanie by DO przekazywał wybrane informacje z pominięciem niektórych danych a jednocześnie ustawa w art. 13.1 wskazuje, że warstwa elektroniczna zawiera dane umieszczone w warstwie graficznej wraz z danymi je uwierzytelniającymi. Konsekwencją planowanego przekazywania wybranych danych jest wymaganie by poszczególne dane lub ich grupy posiadały odrębne dane uwierzytelniające gdyż w przypadku objęcia wszystkich danych łączną informację uwierzytelniającą, przesyłanie niekompletnego ich zestawu uniemożliwia poprawne ich uwierzytelnienie a na taki mechanizm bezpieczeństwa wskazuje art. 12.1 ustawy.

Analiza wymagań na uwierzytelnianie jednocześnie DO (wg rozporządzenia) i danych w nim zawartych (wg ustawy) budzi wątpliwości co do oczekiwanego ogólnego modelu bezpieczeństwa w zakresie autentyczności i uwierzytelniania danych pochodzących „z” lub zawartych „w” warstwie elektronicznej DO i ich zgodności z danymi zawartymi w warstwie graficznej. Model ten nie wynika jednoznacznie z postanowień ustawy i rozporządzenia a typowo wg powszechnie stosowanych modelu ochrony powinno bazować w przypadku poszczególnych danych na określonej alternatywie lub koniunkcji:

- a) odczytu uwierzytelnionych danych z dowolnego źródła,
- b) odczytu niewierzytelnionych danych z uwierzytelnionego źródła

Zagadnienie określonych ograniczeń na używanie różnych interfejsów komunikacyjnych, jeśli w ogóle powinno być rozróżniane to wymaga bardziej klarownego i uporządkowanego przedstawienia gdyż takie miejscowe „wyjątki od reguły” wprowadzają bardzo dużą niepewność co do intencji i wymagań ustawodawcy w zakresie różnicowania zakresu dopuszczalności wykonywania różnych funkcji DO za pośrednictwem jednego czy drugiego interfejsu komunikacyjnego.

§ 15. Brakuje definicji „blankietu DO” w sekcji definicji.

§ 15.2. O jakim „podpisie elektronicznym” jest mowa w tym ustępie? Osobistym czy kwalifikowanym? W niniejszym rozporządzeniu nie określono nigdzie specjalnych/odrębnych wymagań ochrony dla „danych do składania podpisu elektronicznego” – jaka więc powinna być ta ochrona?

§ 16.2. W § 11.8 nie ma kryteriów, na które powołuje się ten ustęp – prawdopodobnie błąd numeracji.

§ 16.3. Ustęp ten zawiera pośrednio BARDZO istotną dla całej koncepcji warstwy elektronicznej dowodu osobistego, a nigdzie niewyjaśnioną, wskazówkę iż dla terminali przydzielane są uprawnienia „do poszczególnych kontenerów” i poszczególnych operacji na tych kontenerach. Wymaga to dużo bardziej klarownego zdefiniowania i określenia wymagań a nie tylko wspomnienie iż coś takiego będzie kontrolowane... ale przez kogo, jak, na podstawie jakich informacji, w ramach jakich interakcji z DO itd. itp.?

Rozdział 8. Praktycznie całkowite oderwanie przedstawionych w nim założeń ochrony od standardów i dobrych praktyk stosowanych w przemyśle kartowym obecnie. Konsekwencją jest konieczność przygotowania od początku rozwiązania dedykowanego dla PL.ID co jest procesem bardzo kosztownym i czasochłonnym.

Z postanowień rozporządzenia i ustawy nie wynika nigdzie konieczność stosowania takich dokładnie metod zarządzania zawartością warstwy elektronicznej (danymi i oprogramowaniem) a tym samym przyjęta nietypowa metoda ochrony zapisywania danych i oprogramowania i kontroli uprawnień do takich zapisów nie znajduje uzasadnienia.

§ 19.2. Brakuje choćby minimalnego wyjaśnienia co ustawodawca rozumie przez „potwierdzenie woli posiadacza...” – czy chodzi o jakieś rozwiązanie techniczne czy organizacyjne? Czy wymagane jest późniejsze dowodzenie uzyskania takiego potwierdzenia woli? Jak? Jak definiowane jest pojęcie „bezpośrednio przed zastosowaniem danych do składania podpisu”? Zastosowanie danych poprzedzane jest m.in. transmisją danych do podpisania lub skrótu takich danych, na których ma być podpis składany – czy potwierdzenie woli bezpośrednio przed oznacza moment PO przesłaniu danych do karty? A jeśli tak to w jaki sposób i kto ma wykonać to potwierdzenie: czy chodzi o zadanie dla warstwy elektronicznej, czytnika, terminala czy jakiegoś podmiotu trzeciego? Ustęp ten wymaga rozwinięcia lub wyjaśnienia.

§ 20.1. Z definicji Centrum Certyfikacji nie wynika zasadność przesyłania takich danych akurat do Centrum Certyfikacji, chyba, że finalizacja podpisu osobistego miałaby być „usługą certyfikacyjną” co nie jest oczywiste i wystarczająco wyjaśnione/uzasadnione w treści rozporządzenia ani nie wynika z innych przepisów. Być może warto zmodyfikować definicję Centrum Certyfikacji i rozszerzyć zakres usług świadczonych przez ten system informatyczny?

§ 20.3 pkt 1. Wymaganie to mylnie może sugerować iż dane o których mowa w ust 1 tego paragrafu generalnie można zweryfikować z udziałem Centrum Certyfikacji a faktycznie dane to nie są podpisem osobistym bezwarunkowo i nie mogą być jako taki podpis użyte.

§ 20.4. Zawiera bardzo nietypowe, niesymetryczne względem wcześniejszych ustępów tego paragrafu i trudne w realizacji wymaganie by sfinalizowany podpis był odsyłany bezpiecznym kanałem gdyż:

- a) może to być już trzeci zagnieżdżony bezpieczny kanał do dowodu (pierwsze dwa zakończone są odpowiednio na czytniku i terminalu) od Centrum Certyfikacji,
- b) wytworzenie danych, o których mowa w § 20.1 wymaga użycia mieszanki informacji znajdujących się w DO, w terminalu (lub aplikacji z nim współpracującej) i w Centrum Certyfikacji; przesyłanie takich informacji do DO wymaga odrębnych kanałów lub użycia jednego kanału do przesłania kompletu informacji pozyskanych innymi drogami od pozostałych „uczestników procesu podpisywania”,
- c) końcowym użytkownikiem podpisu osobistego jest prawdopodobnie terminal, więc przesłanie końcowej postaci podpisu do DO jest niezrozumiałe.

Istnienie takiego kolejnego bezpiecznego kanału pośrednio sugeruje § 21.2.

Być może cała koncepcja przebiegu procesu składania podpisu osobistego ma przemyślan model komunikacyjny i bezpieczeństwa, ale trudno go znaleźć w zapisach §19, §20 i §21 w świetle realiów technologii i standardów kart elektronicznych.

§ 22.1 Ponownie niezrozumiała jest koncepcja odczytywania wymagań dla sposobu nawiązania bezpiecznego kanału przed nawiązaniem bezpiecznego kanału.

§ 22.3 Wymaganie określające zmianę hasła (PIN) umieszczone w tym paragrafie, w świetle tego, że zasady modyfikacji hasła określono już wcześniej w § 10, pośrednio wskazują, iż być może intencją ustawodawcy było, żeby były to różne hasła. Jest to na tyle ważne zagadnienie iż zasługuje na odrębne i kompleksowe uregulowanie. Standardem przemysłowym jest rozgraniczanie wymagań i sposobów realizacji uwierzytelniania dokumentu elektronicznego względem systemów zewnętrznych (z użyciem różnych protokołów kryptograficznych klasy „zapytanie-odpowiedź” lub jako część składową protokołów tworzących bezpieczny kanał) ORAZ uwierzytelniania posiadacza dokumentu względem tego dokumentu.

W pierwszym przypadku celem jest udowodnienie iż stosowany jest konkretny i autentyczny dokument, a w drugim przypadku uzyskuje się potwierdzenie iż dokumentem tym posługuje się jego upoważniony posiadacz (dzięki weryfikacji założenia iż tylko posiadacz zna poufne hasło (PIN)).

Obie klasy zadań uwierzytelniania zasługują na wyraźne i spójne uregulowanie, zwłaszcza, że w rozporządzeniu wydaje się iż występuje wiele haseł, wiele akcji uwierzytelniania jakiejś strony względem drugiej oraz wiele bezpiecznych kanałów, które często to bardzo ściśle związane z uwierzytelnianiem, które równie często bywa w praktyce łączone z używaniem haseł posiadacza, zwłaszcza gdy celem przyjętego finalnie rozwiązania jest też optymalizacja czasu realizacji wszystkich zadań cząstkowych.

Cały rozdział 10 wymaga modyfikacji, gdyż z jednej strony jest bardzo złożony co by wskazywało na chęć opisania zagadnienia ograniczonej identyfikacji w sposób umożliwiający jej praktyczne wykorzystanie przez zainteresowane podmioty ale z drugiej strony ilość niejasności, nowych pojęć wcześniej nie zdefiniowanych oraz prawdopodobnych błędów uniemożliwiają weryfikację poprawności całego mechanizmu i jego implementację bez innego, dokładniejszego opisu. Jednak nic nie wskazuje w rozporządzeniu na istnienie lub plan opublikowania takich specyfikacji, więc tylko rozporządzenie i ustawa pozostają jako materiały źródłowe do analizy regulacji co absolutnie nie jest wystarczające i niestety intencje ustawodawcy i skutki regulacji w zakresie ograniczonej identyfikacji nie są możliwe do oceny.

§ 29. Ponieważ funkcjonalność karty ubezpieczenia zdrowotnego została praktycznie niezdefiniowana, niepotrzebne jest regulowanie zagadnienia licznika pieczęci elektronicznych. Znacznie rozsądniejszym wyjściem jest pozostawienie zdefiniowania funkcjonalności tego wyodrębnionego kontenera do osobnego rozporządzenia dotyczącego kompleksowo karty ubezpieczenia zdrowotnego gdyż zakres regulacji w niniejszym rozporządzeniu jest szczątkowy, więc wymaga znacznego rozwinięcia, a taki pojedynczy zapis jak w § 29 tylko utrudnia kompleksowe i spójne zdefiniowanie działania, wydawania, obsługi funkcji karty ubezpieczenia zdrowotnego w oddzielnym dokumencie.

W szczególności wskazanie iż DO samodzielnie dołącza wartość licznika do danych opatrywanych pieczęcią

implikuje praktycznie pełną obsługę sam DO zagadnienia formatów dokumentów opatrywanych taką pieczęcią lub formatów pieczęci i związanych z nią algorytmów, co nie jest typowym oczekiwaniem względem karty elektronicznej i może bardzo komplikować zaprojektowanie faktycznego DO realizującego tak zdefiniowane zadania.

§ 32.1. Może być bardzo trudny do realizacji (lub niemożliwy) na bazie istniejących obecnie technologii kart elektronicznych. Bardziej odpowiednie i symetryczne względem regulacji niniejszego rozporządzenia dotyczących generowania innych danych służących do składania podpisu lub informacji uwierzytelniającej, jest model przyjęty w § 31.1 lub § 31.2 gdzie wskazuje się na ich instalację w warstwie elektronicznej (a nie generowanie przez DO) lub pozostawia się kwestię otwartą odsyłając do spełnienia wymagań jak dla bezpiecznego urządzenia do składania podpisu kwalifikowanego.

Dzięki temu proces generowania i/lub instalacji danych do składania podpisu osobistego może być realizowany na wiele sposobów jeśli tylko spełniają one klarownie wyznaczone cele bezpieczeństwa.

Ze względu na techniczny charakter podpisu osobistego, najwłaściwszą formą dla powstania danych do składania podpisu osobistego jest ich generowanie w ramach współpracy warstwy elektronicznej DO z systemem finalizacji i innymi systemami Centrum Certyfikacji (wg aktualnej definicji z rozporządzenia) gdyż DO i tak nie jest w stanie wygenerować takich informacji samodzielnie bo dane służące do finalizacji podpisu i tak muszą być uzgodnione z systemami zewnętrznymi wobec DO. Wymaganie zawarte w § 32.3 dość jednoznacznie wskazuje, jakie są intencje i oczekiwania ustawodawcy i taki skutek łatwiej jest osiągnąć mając kontrolę nad procesem generowania danych do składania podpisu osobistego a nie oddawanie tego procesu do realizacji przez sam dowód na żądanie posiadacza.

§ 32.2. Można odnieść (być może mylnie, wrażenie), że wskazuje się iż Centrum Certyfikacji generuje dane do składania podpisu po czym wystawia certyfikat...

§ 33.2 Bez równoczesnej analizy przywołanego w tym ustępie opisu protokołu komunikacyjnego, nie można w pełni ocenić poprawności, kompletności i optymalności znacznej części rozporządzenia. Konsultacji powinny być poddawane oba te dokumenty jednocześnie gdyż stanowią nierozdzielny całość.

5. Podsumowanie i generalne zastrzeżenie

Jeśli intencją ustawodawcy jest uregulowanie szczegółowych kwestii technicznych w oddzielnym dokumencie to ok. 1/3 niniejszego projektu należałoby przenieść do tego dokumentu gdyż szczegóły te stanowią całość. W obecnej postaci bardzo wiele postanowień rozporządzenia jest niezrozumiałych, niekompletnych lub budzi wątpliwości, co do możliwości i bezpieczeństwa ich realizacji wg takiego niespójnego i niekompletnego opisu technicznego jaki miejscami pojawia się w rozporządzeniu. Umieszczenie znacznej części szczegółów technicznych w rozporządzeniu może mieć tylko dwa wyjaśnienia:

- a) stanowią one część istniejącej, spójnej i poprawnej koncepcji praktycznej technicznej realizacji funkcjonalności wymaganej od DO i jego bezpośredniego otoczenia, a to oznacza, że są gotowe pozostałe, komplementarne części specyfikacji (np. specyfikacja protokołu komunikacyjnego) i ocenie należy poddać komplet wymagań, koncepcji i specyfikacji,
- b) są pierwszymi i ogólnymi założeniami technicznymi dla części elektronicznej DO i nie istnieją jeszcze inne specyfikacje i koncepcje – ale wtedy wszelkie regulacje, które nie definiują ogólnych wymagań a wskazują już na sposób realizacji innych wymagań powinny zostać usunięte z projektu Rozporządzenia i przeniesione do mocno technicznego, spójnego, kompletnego opisu technicznego DO, który powstanie później.

Aktualna mieszanka zrozumiałych wymagań i regulacji zdefiniowanych w sposób neutralny dla sposobu implementacji oraz fragmentarycznych definicji bezpiecznych protokołów, mechanizmów podpisu i uwierzytelniania i innych szczegółów metod osiągnięcia ogólnych wymagań, jest bardzo daleka od akceptowalnej postaci aktu regulacyjnego, który ma być dokładnie i poprawnie stosowany przez szeroką klasę podmiotów uczestniczących we wszystkich cyklach życia blankietu DO, gotowego DO, w procesach generowania różnych informacji zapisywanych w pamięci DO, projektujących i implementujących składniki otoczenia współpracującego z DO (czytniki, terminale, systemy IT) oraz samych posiadaczy DO, którzy powinni wiedzieć co, jak i dlaczego mogą/powinni/muszą robić by posługiwanie się DO przynosiło im korzyści a nie generowało zagrożenia, powodowało problemy i powiększało frustrację tzw. „elektroniczną administracją”, której niezrozumienie może tworzyć dla nich niebezpieczne sytuacje, za których skutki będą w pełni odpowiedzialni na gruncie prawa.