RZECZPOSPOLITA POLSKA

Szef
Agencji Bezpieczeństwa Wewnętrznego
Krzysztof Bondaryk

P-~~AO78~~/2011/887MG/NR

Warszawa, 24 lutego 2011 r.

Egz. nr 3

Pan Piotr Kołodziejczyk

Podsekretarz Stanu
Ministerstwo Spraw Wewnętrznych
i Administracji

W odpowiedzi na pismo z dnia 14 lutego 2011 r., znak: DP-I-0231-1116/10/AK, Agencja Bezpieczeństwa Wewnętrznego pragnie zgłosić następujące uwagi do *projektu rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań technicznych dla warstwy elektronicznej dowodu osobistego oraz protokołu komunikacji elektronicznej z dowodami osobistymi:*

I. Uwagi merytoryczne:

- w § 3 ust. 1 projektowanego rozporządzenia określone zostały normy, które powinna spełniać warstwa elektroniczna dowodu osobistego. Ustęp 2 tego paragrafu stanowi, iż: „protokół komunikacji z użyciem interfejsu bezstykowego określa standard ISO 14443-2 z komunikacją typu B". W ocenie ABW zasadnym jest wprowadzenie zapisu w następującym brzmieniu: „protokół komunikacji z użyciem interfejsu bezstykowego określa standard ISO 14443-2 z komunikacją typu A lub typu B". Zastosowanie zapisu w wersji zaproponowanej w rozporządzeniu nie jest uzasadnione technicznie i ogranicza konkurencję.
- w rozdziale 2 rozporządzenia **„Wymagania bezpieczeństwa dla warstwy elektronicznej"** nie nałożono na producenta dowodu osobistego obowiązku spełnienia wymogów Dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych

(Dz. U.UE.L z 2000 nr 13, poz. 12). W związku z powyższym ABW proponuje odpowiednie uzupełnienie zapisów projektu rozporządzenia w tym zakresie.

- w § 5 ust. 3 rozporządzenia ograniczono krąg potencjalnych wytwórców dowodów osobistych do podmiotów posiadających na swój produkt równocześnie certyfikat Common Criteria EAL4+ oraz FIPS 140-2 Level 3, co w opinii ABW jest podejściem błędnym, gdyż nie precyzuje się profilu zabezpieczeń (*ang. Protection Profile*), w oparciu o który należy przeprowadzić procedurę certyfikacji Common Criteria, a co za tym idzie producenci mogą dostarczyć produkt niezgodny z wymaganiami określonymi w rozporządzeniu. Ponadto takie sformułowania podważają autorytet unijnych jednostek certyfikujących. Podkreślenia wymaga również fakt, iż do rzadkości należy certyfikowanie inletów stosowanych w dokumentach elektronicznych w oparciu o dwie procedury (FIPS i Common Criteria) jednocześnie. W ocenie ABW zasadna jest więc rezygnacja z obowiązku łącznego spełnienia obydwu wymagań.
- w rozdziale 8 projektu rozporządzenia **„Zapisywanie danych i oprogramowania w warstwie elektronicznej dowodu osobistego"** określone zostały procedury związane z zapisywaniem danych i aplikacji w warstwie elektronicznej dowodu osobistego. Z powyższych przepisów wynika, iż możliwe będzie umieszczanie w warstwie elektronicznej dowodu osobistego nowych danych i aplikacji po zakończeniu procesu personalizacji. Taki mechanizm wydaje się nadmiarowy, z uwagi na fakt konieczności ponownej certyfikacji warstwy elektronicznej dowodu osobistego każdorazowo po przeprowadzeniu aktualizacji, lub umieszczeniu w warstwie elektronicznej dowodu osobistego nowej aplikacji. W ocenie ABW wątpliwe wydaje się również uzyskanie wskazanego w treści rozporządzenia certyfikatu Common Criteria EAL4+ na rozwiązanie umożliwiające dodawanie nowych aplikacji po sfinalizowaniu procesu personalizacji dokumentu. Należy dodatkowo nadmienić, iż może to spowodować ograniczenie bezpieczeństwa dokumentu.
- obecne brzmienie § 28 ust. 2 projektu rozporządzenia może spowodować znaczny wzrost kosztów systemu teleinformatycznego dedykowanego do obsługi warstwy elektronicznej i brak możliwości korzystania z dowodu osobistego jako Karty Ubezpieczenia Zdrowotnego w wersji off-line. W świetle przytoczonych powyżej zapisów § 29 rozporządzenia jest zbędny, gdyż wszelkie operacje z wykorzystaniem Karty Ubezpieczenia Zdrowotnego będą realizowane w wersji on-line.
- § 30 ust. 1 rozporządzenia stanowi, iż „dowód osobisty umożliwia wykorzystanie go jako dokumentu uprawniającego do przekraczania granic (...) przy użyciu

elektronicznych protokołów wymiany danych, przyjętych w Unii Europejskiej" z jednoczesnym zastrzeżeniem ustępu 2, iż nie może to naruszać warunków określonych w § 8-9 (uwierzytelnianie dowodu) i w § 11-12 (uwierzytelnianie terminala). Łączne zastosowanie w/w wymagań wskazuje na zastosowanie do tego celu mechanizmu EAC (*ang. Extended Access Control –Rozszerzona Kontrola Dostępu*) w wersji 2.0. Wydaje się to być niezgodne z art. 11 ust. 2 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. Nr 167, poz. 1131), gdzie dostęp do tych danych jest również możliwy przy zapewnieniu kontroli obywatela nad dostępem do tych danych, co sugeruje raczej wprowadzenie mechanizmu BAC (*ang. Basic Access Control – Podstawowa Kontrola Dostępu*), który wykorzystuje się w dokumentach podróży nie zawierających danych biometrycznych. W tym miejscu należy wskazać, iż zastosowanie mechanizmu EAC w wersji 2.0 wymaga, przed przekazaniem jakichkolwiek danych, przeprowadzenia procedury uwierzytelnienia terminala. Jest to sprzeczne z zapisami § 13 rozporządzenia, zgodnie z którymi przekazanie tych danych do terminala „odbywa się po uwierzytelnieniu dowodu osobistego", czyli nie wymaga uwierzytelnienia terminala. ABW proponuje w tym zakresie jednoznaczne wskazanie warunków, które muszą być spełnione w celu uzyskania przez państwa Unii Europejskiej dostępu do zapisanych w warstwie elektronicznej dowodu danych z warstwy graficznej wraz z danymi je uwierzytelniającymi.

- zgodnie z § 32 rozporządzenia „dane do składania podpisu osobistego są generowane przez dowód osobisty na życzenie posiadacza". Przytoczony powyżej zapis jest sprzeczny z art. 13 ust. 1 pkt 2 ustawy o dowodach osobistych, który w stanowi, iż „Warstwa elektroniczna dowodu osobistego zawiera (...) dane służące do składania podpisu osobistego". W związku z powyższym dane służące do składania podpisu osobistego winny znajdować się w warstwie elektronicznej dowodu osobistego już w momencie zakończenia procesu personalizacji, niezależnie od żądania posiadacza, a na jego żądanie aktywowany będzie jedynie certyfikat podpisu osobistego.

II. Uwaga formalno - prawna:

W ocenie ABW nie jest zasadne stwierdzenie zawarte w ostatnim akapicie uzasadnienia do projektu rozporządzenia, iż nie jest wymagana w tym przypadku notyfikacja Komisji Europejskiej. Przedmiotowe rozporządzenie reguluje kwestie stricte techniczne dotyczące społeczeństwa informacyjnego i winno być przedmiotem notyfikacji na gruncie Dyrektywy 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998r. ustanawiającej procedurę udzielenia informacji w dziedzinie norm i przepisów

technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. U. UE.L. z 1998 nr 204, poz. 37).

(-) Krzysztof Bondaryk

Do wiadomości:
- Pan Jacek Cichocki, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów, Sekretarz Kolegium do Spraw Służb Specjalnych.