DECYZJA WYKONAWCZA KOMISJI (UE) 2016/650

z dnia 25 kwietnia 2016 r.

ustanawiająca normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE [1], w szczególności jego art. 30 ust. 3 i art. 39 ust. 2,

a także mając na uwadze, co następuje:

(1) W załączniku II do rozporządzenia (UE) nr 910/2014 określono wymagania dotyczące kwalifikowanych urządzeń do składania podpisu elektronicznego oraz kwalifikowanych urządzeń do składania pieczęci elektronicznej.

(2) Zadanie sporządzania specyfikacji technicznych niezbędnych do produkcji i wprowadzania do obrotu produktów, z uwzględnieniem aktualnego stanu technologii, jest realizowane przez organizacje właściwe w dziedzinie normalizacji.

(3) ISO/IEC (Międzynarodowa Organizacja Normalizacyjna/Międzynarodowa Komisja Elektrotechniczna) ustanawia ogólne pojęcia i zasady bezpieczeństwa informatycznego oraz określa ogólny model oceny stosowany jako podstawa oceny właściwości bezpieczeństwa produktów informatycznych.

(4) Na podstawie wydanego przez Komisję zlecenia normalizacji M/460 Europejski Komitet Normalizacyjny (CEN) opracował normy dotyczące kwalifikowanych urządzeń do składania podpisu elektronicznego i pieczęci elektronicznej w sytuacji gdy dane służące do składania podpisu elektronicznego i pieczęci elektronicznej są przechowywane w środowisku zarządzanym w pełni, ale niekoniecznie wyłącznie, przez użytkownika. Normy te zostały uznane za odpowiednie do oceny zgodności takich urządzeń z odpowiednimi wymaganiami określonymi w załączniku II do rozporządzenia (UE) nr 910/2014.

(5) Zgodnie z załącznikiem II do rozporządzenia (UE) nr 910/2014 jedynie kwalifikowany dostawca usług zaufania może zarządzać w imieniu podpisującego danymi służącymi do składania podpisu elektronicznego. Wymogi bezpieczeństwa oraz odpowiadające im specyfikacje certyfikacji różnią się w zależności od tego, czy podpisujący fizycznie posiada produkt, czy też kwalifikowany dostawca usług zaufania działa w imieniu podpisującego. Aby odnieść się do obu sytuacji, a także sprzyjać przyszłemu rozwojowi produktów i norm odpowiadających szczególnym potrzebom, w załączniku do niniejszej decyzji należy wymienić normy obejmujące oba przypadki.

(6) W chwili przyjęcia niniejszej decyzji Komisji kilku dostawców usług zaufania już oferuje rozwiązania w zakresie zarządzania w imieniu klientów danymi służącymi do składania podpisu elektronicznego. Certyfikacja produktów obecnie ogranicza się do sprzętowych modułów bezpieczeństwa certyfikowanych na podstawie różnych norm. Moduły te nie są jednak jeszcze certyfikowane konkretnie w odniesieniu do wymogów dotyczących kwalifikowanych urządzeń do składania podpisu i pieczęci. Niemniej jednak nie istnieją jeszcze opublikowane normy, takie jak EN 419 211 (właściwa dla podpisów elektronicznych tworzonych w środowisku zarządzanym w pełni, ale niekoniecznie wyłącznie, przez użytkownika), które miałyby zastosowanie do równie ważnego rynku certyfikowanych produktów zdalnych. Ponieważ trwają prace nad normami, które mogą być odpowiednie do takich celów, Komisja uzupełni niniejszą decyzję, gdy takie normy będą dostępne i zostaną ocenione jako zgodne z wymogami określonymi w załączniku II do rozporządzenia (UE) nr 910/2014. Do czasu gdy zostanie ustanowiony wykaz takich norm, do oceny zgodności takich produktów można stosować alternatywną procedurę na warunkach określonych w art. 30 ust. 3 lit. b) rozporządzenia (UE) nr 910/2014.

(7) W załączniku wymieniono normę EN 419 211, która składa się z różnych części (1–6) obejmujących różne sytuacje. W częściach 5 i 6 normy EN 419 211 przewidziano rozszerzenia dla środowiska kwalifikowanych urządzeń do składania podpisu, m.in. dotyczące komunikacji z bezpiecznymi aplikacjami służącymi do składania

[1] Dz.U. L 257 z 28.8.2014, s. 73.

podpisu. Producenci mogą swobodnie decydować o stosowaniu takich rozszerzeń. Zgodnie z motywem 56 rozporządzenia (UE) nr 910/2014 zakres certyfikacji na podstawie art. 30 i 39 tego rozporządzenia ogranicza się do ochrony danych służących do składania podpisu, natomiast aplikacje służące do składania podpisu są wyłączone z zakresu certyfikacji.

(8) Aby zagwarantować skuteczną ochronę przed sfałszowaniem podpisów elektronicznych lub pieczęci elektronicznych generowanych przez kwalifikowane urządzenie do składania podpisów lub pieczęci, jak wymaga tego załącznik II do rozporządzenia (UE) nr 910/2014, odpowiednie algorytmy kryptograficzne, długości kluczy oraz funkcje skrótu są warunkiem wstępnym bezpieczeństwa produktów certyfikowanych. Kwestia ta nie jest zharmonizowana na szczeblu europejskim, zatem państwa członkowskie powinny współpracować w celu uzgodnienia algorytmów kryptograficznych, długości kluczy oraz funkcji skrótu stosowanych w dziedzinie podpisów elektronicznych i pieczęci elektronicznych.

(9) Przyjęcie niniejszej decyzji sprawia, że decyzja Komisji 2003/511/WE [1] staje się nieaktualna. Należy zatem ją uchylić.

(10) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu, o którym mowa w art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. W załączniku do niniejszej decyzji wymienia się normy dotyczące oceny bezpieczeństwa produktów informatycznych stosowanych do certyfikacji kwalifikowanych urządzeń do składania podpisu elektronicznego lub kwalifikowanych urządzeń do składania pieczęci elektronicznej zgodnie z art. 30 ust. 3 lit. a) lub art. 39 ust. 2 rozporządzenia (UE) nr 910/2014, jeżeli dane służące do składania podpisu elektronicznego lub pieczęci elektronicznej są przechowywane w środowisku zarządzanym w pełni, ale niekoniecznie wyłącznie, przez użytkownika.

2. Do czasu ustanowienia przez Komisję wykazu norm dotyczących oceny bezpieczeństwa produktów informatycznych stosowanych do certyfikacji kwalifikowanych urządzeń do składania podpisu elektronicznego lub kwalifikowanych urządzeń do składania pieczęci elektronicznej, w sytuacji gdy kwalifikowany dostawca usług zaufania zarządza w imieniu podpisującego lub podmiotu składającego pieczęć danymi służącymi do składania podpisu elektronicznego lub pieczęci elektronicznej, certyfikacja tych produktów opiera się na procedurze, w której, zgodnie z art. 30 ust. 3 lit. b), stosuje się poziomy bezpieczeństwa porównywalne z poziomami wymaganymi w art. 30 ust. 3 lit. a), oraz która została zgłoszona Komisji przez podmiot publiczny lub prywatny, o którym mowa w art. 30 ust. 1 rozporządzenia (UE) nr 910/2014.

Artykuł 2

Niniejszym uchyla się decyzję 2003/511/WE.

Artykuł 3

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 25 kwietnia 2016 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

[1] Decyzja Komisji 2003/511/WE z dnia 14 lipca 2003 r. w sprawie publikacji numerów referencyjnych dla powszechnie uznanych norm dotyczących produktów podpisu elektronicznego zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE (Dz.U. L 175 z 15.7.2003, s. 45).

ZAŁĄCZNIK

WYKAZ NORM, O KTÓRYCH MOWA W ART. 1 UST. 1

— ISO/IEC 15408 – Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych, części 1–3 wymienione poniżej:

  — ISO/IEC 15408-1:2009 – Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1. ISO, 2009.

  — ISO/IEC 15408-2:2008 – Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 2. ISO, 2008.

  — ISO/IEC 15408-3:2008 – Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 3. ISO, 2008

  oraz

— ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation (Technika informatyczna – Techniki zabezpieczeń – Metodyka oceny zabezpieczeń informatycznych),

  oraz

— EN 419 211 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu, wymienione poniżej części 1–6, w zależności od przypadku:

  — EN 419211-1: 2014 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 1: Przegląd

  — EN 419211-2: 2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 2: Urządzenie z generowaniem kluczy

  — EN 419211-3: 2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 3: Urządzenie z generowaniem kluczy

  — EN 419211-4: 2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 4: Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją generującą certyfikaty

  — EN 419211-5: 2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 5: Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją podpisującą

  — EN 419211-6: 2014 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 6: Rozszerzenie dla urządzenia z importem kluczy i bezpiecznym kanałem z aplikacją podpisującą