IZVEDBENI SKLEP KOMISIJE (EU) 2016/650

z dne 25. aprila 2016

o določitvi standardov za oceno varnosti naprav za ustvarjanje kvalificiranega elektronskega podpisa in žiga v skladu s členoma 30(3) in 39(2) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES [1] ter zlasti členov 30(3) in 39(2) Direktive,

ob upoštevanju naslednjega:

(1) Priloga II k Uredbi (EU) št. 910/2014 določa zahteve v zvezi z napravami za ustvarjanje kvalificiranega elektronskega podpisa in napravami za ustvarjanje kvalificiranega elektronskega žiga.

(2) Tehnične specifikacije za izdelavo izdelkov in njihovo dajanje na trg pripravijo organizacije, pristojne za standardizacijo, pri čemer upoštevajo trenutno tehnološko stanje.

(3) ISO/IEC (Mednarodna organizacija za standardizacijo/Mednarodna elektrotehniška komisija) določa splošne koncepte in načela za varnost IT in podrobno določa splošni model za ocenjevanje, ki se uporabi kot podlaga za evalvacijo varnostnih lastnosti izdelkov IT.

(4) Evropski odbor za standardizacijo (CEN) je na podlagi pooblastila za standardizacijo M/460 Komisije razvil standarde za naprave za ustvarjanje kvalificiranega elektronskega podpisa in žiga, kadar se podatki za ustvarjanje elektronskega podpisa ali žiga v celoti, a ne nujno izključno, hranijo v okolju, ki ga upravlja uporabnik. Ti standardi se štejejo kot ustrezni za oceno skladnosti takih naprav z zadevnimi zahtevami iz Priloge II k Uredbi (EU) št. 910/2014.

(5) Priloga II k Uredbi (EU) št. 910/2014 določa, da lahko le ponudnik kvalificiranih storitev zaupanja upravlja podatke za ustvarjanje elektronskega podpisa v imenu podpisnika. Varnostne zahteve in njihove zadevne certifikacijske specifikacije so drugačne, kadar ima podpisnik izdelek fizično v posesti ali kadar ponudnik kvalificiranih storitev zaupanja deluje v imenu podpisnika. Za obravnavo obeh primerov in spodbujanje postopnega razvoja standardov za izdelke in ocenjevanje, ki ustrezajo posebnim potrebam, bi morali biti v prilogi k temu sklepu navedeni standardi, ki zajemajo oba primera.

(6) V času sprejetja tega sklepa Komisije je več ponudnikov storitev zaupanja že ponujalo rešitve, s katerimi upravljajo podatke za ustvarjanje elektronskega podpisa v imenu svojih strank. Certificiranje izdelkov je trenutno omejeno na varnostne module strojne opreme, ki so certificirani v skladu z različnimi standardi, vendar še niso posebej certificirani v skladu z zahtevami za naprave za ustvarjanje kvalificiranega podpisa in žiga. Vendar objavljeni standardi, kot je EN 419 211 (ki se uporabljajo za elektronski podpis, ki je ustvarjen v okolju, ki ga v celoti, a ne nujno izključno, upravlja uporabnik) še ne obstajajo za enako pomemben trg certificiranih daljinskih izdelkov. Ker so standardi, ki bi lahko bili ustrezni za take namene, trenutno še v pripravi, bo Komisija dopolnila ta sklep, ko bodo taki standardi razpoložljivi in ocenjeni kot skladni z zahtevami iz Priloge II k Uredbi (EU) št. 910/2014. Dokler ni sestavljen seznam takih standardov, se lahko uporabi alternativni postopek za oceno skladnosti takih izdelkov na podlagi pogojev iz točke (b) člena 30(3) Uredbe (EU) št. 910/2014.

(7) Priloga navaja EN 419 211, ki je sestavljen iz različnih delov (1–6), ki zajemajo različne okoliščine. Del 5 EN 419 211 in del 6 EN 419 211 navajata razširitve v zvezi z okoljem naprave za ustvarjanje kvalificiranega

[1] UL L 257, 28.8.2014, str. 73.

podpisa, kot je npr. komunikacija z aplikacijami zaupanja za ustvarjanje podpisa. Proizvajalci izdelkov lahko prosto uporabljajo takšne razširitve. V skladu z uvodno izjavo 56 Uredbe (EU) št. 910/2014 je področje uporabe certificiranja na podlagi členov 30 in 39 navedene uredbe omejeno na zaščito podatkov za ustvarjanje podpisa in so aplikacije za ustvarjanje podpisa izključene iz področja uporabe certificiranja.

(8) Da se zagotovi, da so elektronski podpisi ali žigi, ki jih ustvari naprava za ustvarjanje kvalificiranega elektronskega podpisa ali žiga, zanesljivo zaščiteni pred ponarejanjem, kot se zahteva v Prilogi II k Uredbi (EU) št. 910/2014, so ustrezni kriptografski algoritmi, dolžine ključev in zgoščevalne funkcije predpogoj za varnost certificiranega izdelka. Ker to področje ni usklajeno na evropski ravni, bi morale države članice sodelovati, da se doseže dogovor o kriptografskih algoritmih, dolžinah ključev in zgoščevalnih funkcijah, ki se uporabljajo na področju elektronskih podpisov in žigov.

(9) S sprejetjem tega sklepa Odločba Komisije 2003/511/ES ([1]) zastara. Zato bi jo bilo treba razveljaviti.

(10) Ukrepi iz tega sklepa so v skladu z mnenjem odbora iz člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJI SKLEP:

Člen 1

1. Standardi za oceno varnosti izdelkov informacijske tehnologije, ki se uporabljajo za certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa ali naprav za ustvarjanje kvalificiranega elektronskega žiga v skladu s točko (a) člena 30(3) ali členom 39(2) Uredbe (EU) št. 910/2014, kadar se podatki za ustvarjanje elektronskega podpisa ali podatki za ustvarjanje elektronskega žiga hranijo v okolju, ki ga v celoti, a ne nujno izključno, upravlja uporabnik, so navedeni v Prilogi k temu sklepu.

2. Dokler Komisija za oceno varnosti izdelkov informacijske tehnologije ne vzpostavi seznama standardov, ki se uporabljajo za certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa ali naprav za ustvarjanje kvalificiranega elektronskega žiga, kadar ponudnik kvalificiranih storitev zaupanja upravlja podatke za ustvarjanje elektronskega podpisa ali podatke za ustvarjanje elektronskega žiga v imenu podpisnika ali ustvarjalca žiga, certificiranje takih izdelkov temelji na postopku, ki v skladu s členom 30(3)(b) uporablja ravni varnosti, ki so primerljive s tistimi, ki jih zahteva člen 30(3)(a), in ki ga Komisiji uradno sporoči javni ali zasebni organ iz odstavka 1 člena 30 Uredbe (EU) št. 910/2014.

Člen 2

Odločba 2003/511/ES se razveljavi.

Člen 3

Ta sklep začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

V Bruslju, 25. aprila 2016

Za Komisijo
Predsednik
Jean-Claude JUNCKER

([1]) UL L 175, 15.7.2003, str. 45.

PRILOGA

SEZNAM STANDARDOV IZ ČLENA 1(1)

— ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security, spodaj navedeni deli 1–3:

  — ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1. ISO, 2009

  — ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2. ISO, 2008

  — ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3. ISO, 2008

  in

— ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation

  in

— EN 419 211 – Protection profiles for secure signature creation device, spodaj navedeni deli 1–6, kakor je ustrezno:

  — EN 419211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview

  — EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation

  — EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import

  — EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application

  — EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application

  — EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application