

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2016/650**z 25. apríla 2016,****ktorým sa stanovujú normy posudzovania bezpečnosti zariadení na vyhotovenie kvalifikovaného podpisu a pečate podľa článku 30 ods. 3 a článku 39 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu****(Text s významom pre EHP)**

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ⁽¹⁾, a najmä na jeho článok 30 ods. 3 a článok 39 ods. 2,

keďže:

- (1) V prílohe II k nariadeniu (EÚ) č. 910/2014 sa stanovujú požiadavky na zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a zariadenia na vyhotovenie kvalifikovanej elektronickej pečate.
- (2) Úlohu vypracovať technické špecifikácie potrebné na výrobu produktov a ich umiestňovanie na trh pri zohľadnení súčasného stavu technológií vykonávajú príslušné organizácie v oblasti normalizácie.
- (3) ISO/IEC (Medzinárodná organizácia pre normalizáciu/Medzinárodná elektrotechnická Komisia) určuje všeobecné pojmy a zásady bezpečnosti IT a špecifikuje všeobecný model posudzovania, ktorý sa použije ako základ pre hodnotenie bezpečnostných vlastností produktov IT.
- (4) Európsky výbor pre normalizáciu (CEN) vyvinul v rámci normalizačného mandátu Komisie M/460 normy pre zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a pečatí, ak sa údaje na vyhotovenie elektronického podpisu alebo údaje na vyhotovenie elektronickej pečate uchovávajú v prostredí, ktoré úplne, ale nie výlučne spravuje používateľ. Tieto normy sa považujú za vhodné na posudzovanie zhody takýchto zariadení s príslušnými požiadavkami uvedenými v prílohe II k nariadeniu (EÚ) č. 910/2014.
- (5) V prílohe II k nariadeniu (EÚ) č. 910/2014 sa stanovuje, že spravovať údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môže výhradne kvalifikovaný poskytovateľ dôveryhodných služieb. Bezpečnostné požiadavky a ich príslušné certifikačné špecifikácie sú rôzne, keď podpisovateľ fyzicky vlastní výrobok a keď v mene poskytovateľa koná poskytovateľ kvalifikovaných dôveryhodných služieb. S cieľom pokryť obidve situácie, ako aj podporiť postupný vývoj produktov a noriem posudzovania prispôbených osobitným potrebám by príloha k tomuto rozhodnutiu mala obsahovať zoznam noriem vzťahujúcich sa na obidve situácie.
- (6) V čase prijatia tohto rozhodnutia Komisia niekoľkí poskytovatelia dôveryhodných služieb už ponúkali riešenia, ktoré im umožňovali spravovať údaje na vyhotovenie elektronického podpisu v mene ich zákazníkov. Certifikačné výrobkov sa v súčasnosti obmedzujú na hardvérové bezpečnostné moduly certifikované podľa rôznych noriem, pričom však ešte nie sú certifikované z hľadiska špecifických požiadaviek týkajúcich sa zariadení na vyhotovenie kvalifikovaných elektronických podpisov a pečatí. Napriek tomu ešte neexistujú uverejnené normy, ako napríklad EN 419 211 (vzťahujúca sa na elektronický podpis vytvorený v prostredí, ktoré úplne, ale nie výlučne spravuje používateľ), pre rovnako dôležitý trh certifikovaných výrobkov používaných na diaľku. Keďže normy, ktoré by mohli byť vhodné na tieto účely, sa v súčasnosti pripravujú, Komisia toto rozhodnutie doplní vtedy, keď budú takéto normy dostupné a z ich posúdenia vyplynie, že sú v súlade s požiadavkami stanovenými v prílohe II k nariadeniu (EÚ) č. 910/2014. Kým nebude určený zoznam takýchto noriem, možno pri posudzovaní súladu takýchto výrobkov na základe podmienok ustanovených v článku 30 ods. 3 písm. b) nariadenia (EÚ) č. 910/2014 používať alternatívny postup.
- (7) V prílohe sa uvádza EN 419 211, ktorá pozostáva z rôznych častí (1 až 6) týkajúcich sa rôznych situácií. V normách EN 419 211 časti 5 a 419 211 časti 6 sa uvádzajú rozšírenia týkajúce sa prostredia, v ktorom

⁽¹⁾ Ú. v. EÚ L 257, 28.8.2014, s. 73.

funguje zariadenie na vytvorenie kvalifikovaného podpisu, ako napríklad komunikácie s aplikáciami na vyhotovenie dôveryhodného podpisu. Výrobcovia produktov môžu voľne uplatňovať takéto rozšírenia. Podľa odôvodnenia 56 nariadenia (EÚ) č. 910/2014 rozsah pôsobnosti certifikácie podľa článkov 30 a 39 uvedeného nariadenia sa obmedzuje na ochranu údajov na vyhotovenie podpisu, kým aplikácie na vyhotovenie podpisu sú vylúčené z rozsahu pôsobnosti certifikácie.

- (8) S cieľom dosiahnuť, aby elektronické podpisy alebo pečate vygenerované zariadením na vyhotovenie kvalifikovaného podpisu alebo pečate boli spoľahlivo chránené proti falšovaniu, ako sa požaduje v prílohe II k nariadeniu (EÚ) č. 910/2014, sú nevyhnutným predpokladom zabezpečenia certifikovaného produktu vhodné kryptovacie algoritmy, dĺžky kľúčov a hašovacie funkcie. Keďže táto otázka nebola harmonizovaná na európskej úrovni, členské štáty by sa mali spoločne dohodnúť na kryptografických algoritmoch, dĺžkach kľúčov a hašovacích funkciách, ktoré sa majú používať v oblasti elektronických podpisov a pečatí.
- (9) Prijatím tohto rozhodnutia sa rozhodnutie Komisie 2003/511/ES ⁽¹⁾ stáva zastaraným. Z toho dôvodu by sa malo zrušiť.
- (10) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru uvedeného v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Normy pre bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu zariadení na vyhotovenie kvalifikovaných elektronických podpisov alebo zariadení na vyhotovenie kvalifikovaných elektronických pečatí podľa článku 30 ods. 3 písm. a) alebo článku 39 ods. 2 nariadenia (EÚ) č. 910/2014, ak sa údaje na vyhotovenie elektronického podpisu alebo údaje na vyhotovenie elektronickej pečate uchovávajú v prostredí, ktoré úplne, ale nie výlučne spravuje používateľ, sú uvedené v prílohe k tomuto rozhodnutiu.

2. Kým Komisia nevytvorí zoznam noriem na bezpečnostné posúdenie produktov informačných technológií, ktoré sa vzťahujú na certifikáciu zariadení na vytvorenie kvalifikovaných elektronických podpisov alebo zariadení na vyhotovenie kvalifikovaných elektronických pečatí v prípadoch, keď kvalifikovaný poskytovateľ dôveryhodných služieb spravuje údaje na vyhotovenie elektronického podpisu alebo údaje na vyhotovenie elektronickej pečate v mene podpisovateľa alebo autora pečate, certifikácia takýchto produktov sa musí zakladať na postupe, ktorý podľa článku 30 ods. 3 písm. b) využíva úroveň bezpečnosti porovnateľnú s úrovňami, aké sa požadujú v článku 30 ods. 3 písm. a), a ktorý sa oznamuje Komisii prostredníctvom verejného alebo súkromného subjektu uvedeného v článku 30 ods. 1 nariadenia (EÚ) č. 910/2014.

Článok 2

Rozhodnutie 2003/511/ES sa týmto zrušuje.

Článok 3

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v Úradnom vestníku Európskej únie.

V Bruseli 25. apríla 2016

Za Komisiu
predseda
Jean-Claude JUNCKER

⁽¹⁾ Rozhodnutie Komisie 2003/511/ES zo 14. júla 2003 o uverejnení referenčných čísel všeobecne uznávaných noriem pre produkty elektronického podpisu v súlade so smernicou Európskeho parlamentu a Rady 1999/93/ES (Ú. v. EÚ L 175, 15.7.2003, s. 45).

PRÍLOHA

ZOZNAM NORIEM UVEDENÝCH V ČLÁNKU 1 ODS. 1

- ISO/IEC 15408 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT, časti 1 až 3 uvedené nižšie:
 - ISO/IEC 15408 – 1:2009 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT. Časť 1. ISO, 2009
 - ISO/IEC 15408 – 2:2008 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT. Časť 2. ISO, 2008
 - ISO/IEC 15408 – 3:2008 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT. Časť 3. ISO, 2008
 - a
 - ISO/IEC 18045:2008 – Informačné technológie. Bezpečnostné techniky. Metodika hodnotenia bezpečnosti IT
 - a
 - EN 419 211 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu, časti 1 až 6, podľa potreby, ako je uvedené nižšie:
 - EN 419211 – 1:2014 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 1: Prehľad
 - EN 419211 – 2:2013 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 2: Zariadenie s generovaním kľúča
 - EN 419211 – 3:2013 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 3: Zariadenie s importovaním kľúča
 - EN 419211 – 4:2013 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 4: Rozšírenie pre zariadenie s generovaním kľúča a dôveryhodným kanálom k aplikácii na generovanie certifikátov
 - EN 419211 – 5:2013 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 5: Rozšírenie pre zariadenie s generovaním kľúča a dôveryhodným kanálom k aplikácii na vyhotovenie podpisu
 - EN 419211 – 6:2014 Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 6: Rozšírenie pre zariadenie s importovaním kľúča a dôveryhodným kanálom k aplikácii na vyhotovenie podpisu
-