Úradný vestník Európskej únie

L 235

Zväzok 58

Slovenské vydanie

Právne predpisy

9. septembra 2015

Obsah

[1] Text s významom pre EHP

SK

Akty, ktoré sú vytlačené obyčajným písmom, sa týkajú každodennej organizácie poľnohospodárskych záležitostí a sú spravidla platné len obmedzený čas.

Názvy všetkých ostatných aktov sú vytlačené tučným písmom a je pred nimi hviezdička.

[1] Text s významom pre EHP

II

(Nelegislatívne akty)

NARIADENIA

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2015/1501

z 8. septembra 2015

o rámci interoperability podľa článku 12 ods. 8 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 12 ods. 8,

keďže:

(1) V článku 12 ods. 2 nariadenia (EÚ) č. 910/2014 sa stanovuje povinnosť zaviesť rámec interoperability na účely interoperability vnútroštátnych schém elektronickej identifikácie oznámených podľa článku 9 ods. 1 uvedeného nariadenia.

(2) Ústrednú úlohu pri prepájaní schém elektronickej identifikácie členských štátov zohrávajú uzly. Ich prínos vrátane funkcií a komponentov „uzla eIDAS“ je vysvetlený v dokumentácii k Nástroju na prepájanie Európy ustanovenému nariadením Európskeho parlamentu a Rady (EÚ) č. 1316/2013 ([2]).

(3) Ak členský štát alebo Komisia poskytnú softvér s cieľom umožniť autentifikáciu uzlu prevádzkovanému v inom členskom štáte, strana, ktorá softvér používaný na mechanizmus autentifikácie dodala a aktualizuje, sa môže so stranou, ktorá softvér hosťuje, dohodnúť na tom, ako sa bude prevádzka mechanizmu identifikácie riadiť. Z takejto dohody by pre hostiteľskú stranu nemali vyplynúť neprimerané technické požiadavky alebo náklady (vrátane podpory, zodpovedností, hosťovania a iných nákladov).

(4) Do tej miery, ako si to bude vyžadovať realizácia rámca interoperability, by mohla Komisia v spolupráci s členskými štátmi vypracovať ďalšie technické špecifikácie obsahujúce podrobnosti o technických požiadavkách stanovených v tomto nariadení, najmä so zreteľom na stanoviská siete spolupráce uvedené v článku 14 písm. d) vykonávacieho rozhodnutia Komisie (EÚ) 2015/296 ([3]). Tieto špecifikácie by sa mali vypracovať ako súčasť infraštruktúr digitálnych služieb uvedených v nariadení (EÚ) č. 1316/2013, v ktorom sa stanovujú spôsoby týkajúce sa praktickej realizácie stavebných blokov elektronickej identifikácie.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1316/2013 z 11. decembra 2013 o zriadení Nástroja na prepájanie Európy, ktorým sa mení nariadenie (EÚ) č. 913/2010 a zrušujú sa nariadenia (ES) č. 680/2007 a (ES) č. 67/2010 (Ú. v. EÚ L 348, 20.12.2013, s. 129).

([3]) Vykonávacie rozhodnutie Komisie (EÚ) 2015/296 z 24. februára 2015, ktorým sa stanovujú procedurálne opatrenia týkajúce sa spolupráce medzi členskými štátmi v oblasti elektronickej identifikácie podľa článku 12 ods. 7 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 53, 25.2.2015, s. 14).

(5) Technické požiadavky stanovené v tomto nariadení by mali byť uplatniteľné napriek všetkým prípadným zmenám technických špecifikácií, ktoré by mohli byť vypracované v súlade s článkom 12 tohto nariadenia.

(6) Pri stanovení pravidiel rámca interoperability uvedených v tomto nariadení sa v maximálnej možnej miere zohľadnil rozsiahly pilotný projekt STORK vrátane špecifikácií vypracovaných v rámci tohto projektu, ako aj zásady a koncepcie európskeho rámca interoperability pre európske verejné služby.

(7) V maximálnej možnej miere sa zohľadnili aj výsledky spolupráce medzi členskými štátmi.

(8) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru, ktorý bol zriadený článkom 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

Článok 1

Predmet úpravy

Týmto nariadením sa stanovujú technické a prevádzkové požiadavky na rámec interoperability s cieľom zabezpečiť interoperabilitu schém elektronickej identifikácie, ktoré členské štáty oznamujú Komisii.

Tieto požiadavky zahŕňajú najmä:

a) minimálne technické požiadavky týkajúce sa úrovní zabezpečenia a mapovanie vnútroštátnych úrovní zabezpečenia oznámených prostriedkov elektronickej identifikácie vydaných v rámci oznámených schém elektronickej identifikácie podľa článku 8 nariadenia (EÚ) č. 910/2014 uvedené v článkoch 3 a 4;

b) minimálne technické požiadavky týkajúce sa interoperability uvedené v článkoch 5 a 8;

c) minimálny súbor osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú alebo právnickú osobu uvedený v článku 11 a v prílohe;

d) spoločné normy prevádzkovej bezpečnosti uvedené v článkoch 6, 7, 9 a 10;

e) mechanizmy na riešenie sporov uvedené v článku 13.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „uzol“ je miesto pripojenia, ktoré je súčasťou architektúry interoperability elektronickej identifikácie a je zapojené do cezhraničnej autentifikácie osôb a ktoré je schopné rozoznať a spracovať alebo prenášať signály s údajmi na iné uzly tým, že vnútroštátnej infraštruktúre elektronickej identifikácie jedného členského štátu umožní vzájomné zosúladenie s vnútroštátnymi infraštruktúrami elektronickej identifikácie ostatných členských štátov;

2. „uzlový operátor“ je subjekt zodpovedný za zabezpečenie toho, aby uzol správne a spoľahlivo vykonával svoje funkcie ako miesto pripojenia.

Článok 3

Minimálne technické požiadavky týkajúce sa úrovní zabezpečenia

Minimálne technické požiadavky týkajúce sa úrovní zabezpečenia sú stanovené vo vykonávacom nariadení Komisie (EÚ) 2015/1502 ([1]).

Článok 4

Mapovanie vnútroštátnych úrovní zabezpečenia

Mapovanie vnútroštátnych úrovní zabezpečenia oznámených schém elektronickej identifikácie musí spĺňať požiadavky ustanovené vo vykonávacom nariadení Komisie (EÚ) 2015/1502. Výsledky mapovania sa oznámia Komisii, pričom sa použije vzorové oznámenie stanovené vo vykonávacom rozhodnutí Komisie (EÚ) 2015/1505 ([2]).

Článok 5

Uzly

1. Uzol v jednom členskom štáte musí byť schopný spojenia s uzlami iných členských štátov.

2. Uzly musia byť schopné pomocou technických prostriedkov rozlišovať medzi subjektmi verejného sektora a ďalšími závislými stranami.

3. Z realizácie technických požiadaviek stanovených v tomto nariadení jedným členským štátom nesmú pre iné členské štáty vyplynúť nijaké neprimerané technické požiadavky ani náklady na dosiahnutie interoperability s realizáciou prvého členského štátu.

Článok 6

Ochrana a dôvernosť údajov

1. Ochrana a dôvernosť vymieňaných údajov a zachovanie integrity údajov medzi uzlami sa zabezpečuje pomocou najlepších dostupných technických riešení a ochranných postupov.

2. Uzly nesmú uchovávať žiadne osobné údaje okrem údajov na účely uvedené v článku 9 ods. 3

Článok 7

Integrita a autenticita údajov pri komunikácii

Komunikácia medzi uzlami musí zabezpečovať integritu a autenticitu údajov s cieľom overiť autenticitu všetkých žiadostí a odpovedí a vylúčiť možnosť, že s nimi niekto manipuloval. Na tento účel využívajú uzly riešenia, ktoré sa úspešne použili pri cezhraničnej prevádzke.

([1]) Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Pozri stranu 7 tohto úradného vestníka).

([2]) Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Pozri stranu 26 tohto úradného vestníka).

Článok 8

Formát správ pri komunikácii

Na systemizáciu sa pri uzloch použije spoločný formát správ na základe noriem, ktoré sa medzi členskými štátmi použili už viac ako jedenkrát a v prevádzkovom prostredí sa osvedčili. Systemizácia musí umožniť:

a) riadne spracovanie minimálneho súboru osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú alebo právnickú osobu,

b) riadne spracovanie úrovne zabezpečenia prostriedkov elektronickej identifikácie,

c) rozlišovanie medzi subjektmi verejného sektora a inými závislými stranami,

d) flexibilitu umožňujúcu uspokojenie potrieb dodatočných charakteristík týkajúcich sa identifikácie.

Článok 9

Spravovanie bezpečnostných informácií a metaúdajov

1. Uzlový operátor oznamuje metaúdaje týkajúce sa spravovania uzlov v normalizovanej strojovo spracovateľnej forme a bezpečným a dôveryhodným spôsobom.

2. Prinajmenšom parametre relevantné pre bezpečnosť sa získavajú automaticky.

3. Uzlový operátor uchováva údaje, ktoré by v prípade mimoriadnej udalosti umožnili obnovu postupnosti výmeny správ potrebnú na zistenie miesta a povahy tejto udalosti. Údaje sa uchovávajú na isté časové obdobie v súlade s vnútroštátnymi požiadavkami a pozostávajú minimálne z týchto prvkov:

a) identifikácia uzla;

b) identifikácia správy;

c) dátum a čas správy.

Článok 10

Zabezpečenie informácií a bezpečnostné normy

1. Uzloví operátori poskytujúci autentifikáciu preukážu, že pokiaľ ide o uzly, ktoré spolupracujú v rámci interoperability, daný uzol spĺňa požiadavky normy ISO/IEC 27001, a to certifikáciou alebo rovnocennou metódou posudzovania alebo súladom s vnútroštátnymi právnymi predpismi.

2. Uzloví operátori musia bez zbytočného odkladu inštalovať bezpečnostné kritické aktualizácie.

Článok 11

Osobné identifikačné údaje:

1. Minimálny súbor osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú alebo právnickú osobu musí v prípade, že sa používa v cezhraničnom kontexte, spĺňať požiadavky stanovené v prílohe.

2. Minimálny súbor údajov týkajúcich sa fyzickej osoby, ktorá zastupuje právnickú osobu, musí v prípade, že sa používa v cezhraničnom kontexte, obsahovať kombináciu atribútov uvedených v prílohe pre fyzické osoby a právnické osoby.

3. Údaje sa vysielajú s použitím pôvodných znakov a tam, kde je to potrebné, sa aj transkribujú do latinky.

Článok 12

Technické špecifikácie

1. Ak si to postup realizácie rámca interoperability vyžaduje, sieť spolupráce zriadená vykonávacím rozhodnutím (EÚ) 2015/296 môže prijímať stanoviská podľa článku 14 písm. d) uvedeného vykonávacieho rozhodnutia týkajúce sa potreby vypracovania technických špecifikácií. V týchto technických špecifikáciách sa poskytnú ďalšie podrobnosti o technických požiadavkách stanovených v tomto nariadení.

2. V súlade so stanoviskom uvedeným v odseku 1 Komisia v spolupráci s členskými štátmi vypracuje technické špecifikácie ako súčasť infraštruktúry digitálnych služieb uvedenej v nariadení (EÚ) č. 1316/2013.

3. Sieť spolupráce prijme stanovisko v súlade s článkom 14 písm. d) vykonávacieho nariadenia (EÚ) 2015/296, v ktorom vyhodnotí, či a v akom rozsahu technické špecifikácie vypracované podľa odseku 2 zodpovedajú potrebám zisteným v stanovisku uvedenom v odseku 1 alebo požiadavkám stanoveným v tomto nariadení. Môže odporučiť, aby členské štáty pri vykonávaní rámca interoperability tieto technické špecifikácie zohľadnili.

4. Komisia poskytne referenčnú realizáciu ako príklad výkladu technických špecifikácií. Členské štáty môžu túto referenčnú realizáciu uplatniť alebo ju využiť ako vzor pri testovaní iných spôsobov realizácie technických špecifikácií.

Článok 13

Riešenie sporov

1. Tam, kde je to možné, sa každý spor týkajúci sa rámca interoperability rieši v príslušných členských štátoch prostredníctvom rokovaní.

2. Ak sa nedospeje k riešeniu v súlade s odsekom 1, právomoc na riešenie sporu má sieť spolupráce zriadená v súlade s článkom 12 vykonávacieho rozhodnutia (EÚ) 2015/296 v súlade so svojím rokovacím poriadkom.

Článok 14

Nadobudnutie účinnosti

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

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA

Požiadavky na minimálny súbor osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú alebo právnickú osobu, uvedený v článku 11

1. **Minimálny súbor údajov pre fyzické osoby**

Minimálny súbor údajov pre fyzické osoby musí obsahovať všetky tieto povinné atribúty:

a) súčasné priezvisko(-á),

b) súčasné meno(-á),

c) dátum narodenia,

d) jedinečný identifikátor vytvorený odosielajúcim členským štátom v súlade s technickými špecifikáciami na účely cezhraničnej identifikácie a pokiaľ možno následne nemenený.

Minimálny súbor údajov pre fyzické osoby musí obsahovať jeden alebo viacero týchto povinných atribútov:

a) meno(-á) a priezvisko(-á) pri narodení,

b) miesto narodenia,

c) súčasná adresa,

d) pohlavie.

2. **Minimálny súbor údajov pre právnické osoby**

Minimálny súbor údajov pre právnické osoby musí obsahovať všetky tieto povinné atribúty:

a) súčasný úradný názov (názvy),

b) jedinečný identifikátor vytvorený odosielajúcim členským štátom v súlade s technickými špecifikáciami na účely cezhraničnej identifikácie a pokiaľ možno následne nemenený.

Minimálny súbor údajov pre právnické osoby musí obsahovať jeden alebo viacero týchto povinných atribútov:

a) súčasná adresa,

b) registračné číslo DPH,

c) daňové registračné číslo,

d) identifikátor (identifikačný znak) uvedený v článku 3 ods. 1 smernice Európskeho parlamentu a Rady 2009/101/ES ([1]),

e) identifikátor právneho subjektu (LEI) uvedený vo vykonávacom nariadení Komisie (EÚ) č. 1247/2012 ([2]),

f) číslo registrácie a identifikácie hospodárskych subjektov (EORI) uvedené vo vykonávacom nariadení Komisie (EÚ) č. 1352/2013 ([3]),

g) číslo pre spotrebnú daň stanovené v článku 2 ods. 12 nariadenia Rady č. 389/2012 ([4]).

([1]) Smernica Európskeho parlamentu a Rady 2009/101/ES zo 16. septembra 2009 o koordinácii záruk, ktoré sa od obchodných spoločností v zmysle článku 48 druhého odseku zmluvy vyžadujú v členských štátoch na ochranu záujmov spoločníkov a tretích osôb s cieľom zabezpečiť rovnocennosť týchto záruk (Ú. v. EÚ L 258, 1.10.2009, s. 11).

([2]) Vykonávacie nariadenie Komisie (EÚ) č. 1247/2012 z 19. decembra 2012, ktorým sa stanovujú vykonávacie technické normy, pokiaľ ide o formát a frekvenciu hlásení obchodov archívom obchodných údajov podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 352, 21.12.2012, s. 20).

([3]) Vykonávacie nariadenie Komisie (EÚ) č. 1352/2013 zo 4. decembra 2013, ktorým sa stanovujú formuláre podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 608/2013 o presadzovaní práv duševného vlastníctva colnými orgánmi (Ú. v. EÚ L 341, 18.12.2013, s. 10).

([4]) Nariadenie Rady (EÚ) č. 389/2012 z 2. mája 2012 o administratívnej spolupráci v oblasti spotrebných daní a zrušení nariadenia (ES) č. 2073/2004 (Ú. v. EÚ L 121, 8.5.2012, s. 1).

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2015/1502

z 8. septembra 2015,

ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 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 8 ods. 3,

keďže:

(1) V článku 8 nariadenia (EÚ) č. 910/2014 sa stanovuje, že schéma elektronickej identifikácie oznámená podľa článku 9 ods. 1 musí obsahovať špecifikácie úrovní zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie vydávané v rámci danej schémy.

(2) Určenie minimálnych technických špecifikácií, noriem a postupov je nevyhnutné na zaistenie jednotného chápania podrobných vlastností úrovní zabezpečenia a na zaistenie interoperability pri mapovaní vnútroštátnych úrovní zabezpečenia oznámených schém elektronickej identifikácie na úrovne zabezpečenia podľa článku 8, ako sa uvádza v článku 12 ods. 4 písm. b) nariadenia (EÚ) č. 910/2014.

(3) Pri príprave špecifikácií a postupov stanovených v tomto vykonávacom akte bola ako zásadná medzinárodná norma v oblasti úrovní zabezpečenia prostriedkov elektronickej identifikácie zohľadnená medzinárodná norma ISO/IEC 29115. Obsah nariadenia (EÚ) č. 910/2014 sa však od tejto medzinárodnej normy líši, a to najmä pokiaľ ide o požiadavky na preukazovanie a overovanie totožnosti, ako aj o spôsob, akým sa zohľadňujú rozdiely medzi dojednaniami v oblasti totožnosti v jednotlivých členských štátoch a existujúcimi nástrojmi na rovnaký účel v EÚ. Preto by sa v prílohe nemalo odkazovať na konkrétny obsah normy ISO/IEC 29115, hoci z tejto medzinárodnej normy vychádza.

(4) Toto nariadenie bolo vypracované na základe prístupu založeného na výsledkoch, keďže bol najvhodnejší, čo sa odráža aj vo vymedzeniach použitých na špecifikovanie termínov a pojmov. Berie sa v nich do úvahy cieľ nariadenia (EÚ) č. 910/2014 v súvislosti s úrovňami zabezpečenia prostriedkov elektronickej identifikácie. Preto by sa pri stanovovaní špecifikácií a postupov stanovených v tomto vykonávacom akte mal v najvyššej možnej miere zohľadniť rozsiahly pilotný projekt STORK vrátane špecifikácií, ktoré boli v jeho rámci vyvinuté, ako aj vymedzenia a pojmy uvedené v norme ISO/IEC 29115.

(5) Spoľahlivé zdroje môžu mať v závislosti od kontextu, v ktorom treba overiť nejaký aspekt dôkazu totožnosti, mnoho podôb, ako sú okrem iného registre, doklady a orgány. V rôznych členských štátoch sa môžu spoľahlivé zdroje líšiť, a to dokonca v podobnom kontexte.

(6) V požiadavkách na preukazovanie a overovanie totožnosti by sa mali zohľadňovať rozdielne systémy a postupy a zároveň zaistiť dostatočne vysoký stupeň zabezpečenia s cieľom vytvoriť potrebnú dôveru. Preto by sa akceptovanie postupov, ktoré sa predtým používali na iné účely, než je vydávanie prostriedkov elektronickej identifikácie, malo podmieniť potvrdením toho, že tieto postupy spĺňajú požiadavky stanovené pre príslušnú úroveň zabezpečenia.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73.

(7) Obvykle sa využívajú určité faktory autentifikácie, ako napríklad spoločné tajomstvá, fyzické zariadenia a fyzické vlastnosti. Na zvýšenie bezpečnosti procesu autentifikácie by sa však malo podnecovať používanie väčšieho počtu faktorov autentifikácie, a najmä z rôznych kategórií faktorov.

(8) Toto nariadenie by nemalo mať vplyv na práva právnických osôb na zastúpenie. V prílohe by sa však mali stanovovať požiadavky na prepojenie medzi prostriedkami elektronickej identifikácie fyzických a právnických osôb.

(9) Mal by sa uznať význam systémov riadenia informačnej bezpečnosti a služieb, ako aj význam používania uznávaných metodík a uplatňovania zásad zakotvených v normách, ako sú normy súboru ISO/IEC 27000 a súboru ISO/IEC 20000.

(10) Do úvahy by sa mali brať aj osvedčené postupy týkajúce sa úrovní zabezpečenia v jednotlivých členských štátoch.

(11) Dôležitým nástrojom na overovanie súladu produktov s bezpečnostnými požiadavkami tohto vykonávacieho aktu je bezpečnostná certifikácia IT založená na medzinárodných normách.

(12) Výbor uvedený v článku 48 nariadenia (EÚ) č. 910/2014 nevydal stanovisko v termíne stanovenom jeho predsedom,

PRIJALA TOTO NARIADENIE:

Článok 1

1. Úrovne zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie vydané v rámci oznámenej schémy elektronickej identifikácie sa určujú vzhľadom na špecifikácie a postupy stanovené v prílohe.

2. Na špecifikovanie úrovne zabezpečenia prostriedkov elektronickej identifikácie vydaných v rámci oznámenej schémy elektronickej identifikácie sa použijú špecifikácie a postupy stanovené v prílohe tak, že sa určí spoľahlivosť a kvalita týchto prvkov:

a) prihlásenie, ako sa stanovuje v oddiele 2.1 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. a) nariadenia (EÚ) č. 910/2014;

b) riadenie prostriedkov elektronickej identifikácie, ako sa stanovuje v oddiele 2.2 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. b) a f) nariadenia (EÚ) č. 910/2014;

c) autentifikácia, ako sa stanovuje v oddiele 2.3 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. c) nariadenia (EÚ) č. 910/2014;

d) riadenie a organizácia, ako sa stanovuje v oddiele 2.4 prílohy k tomuto nariadeniu podľa článku 8 ods. 3 písm. d) a e) nariadenia (EÚ) č. 910/2014.

3. Ak prostriedky elektronickej identifikácie vydané v rámci oznámenej schémy elektronickej identifikácie spĺňajú nejakú požiadavku uvedenú pre vyššiu úroveň zabezpečenia, potom sa predpokladá, že spĺňajú aj zodpovedajúcu požiadavku nižšej úrovne zabezpečenia.

4. Pokiaľ nie je v príslušnej časti prílohy uvedené inak, musia byť na dosiahnutie údajnej úrovne zabezpečenia splnené všetky prvky uvedené v prílohe pre konkrétnu úroveň zabezpečenia prostriedkov elektronickej identifikácie vydaných v rámci oznámenej schémy elektronickej identifikácie.

Článok 2

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

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA

Technické špecifikácie a postupy pre úrovne zabezpečenia „nízka“, „pokročilá“ a „vysoká“ pre prostriedky elektronickej identifikácie vydané v rámci oznámenej schémy elektronickej identifikácie

1. Platné vymedzenie pojmov

Na účely tejto prílohy sa uplatňuje toto vymedzenie pojmov:

1. „spoľahlivý zdroj“ je akýkoľvek zdroj bez ohľadu na svoju podobu, pri ktorom sa dá spoľahnúť na to, že poskytuje presné údaje, informácie a/alebo dôkazy, ktoré sa môžu použiť na preukázanie totožnosti;

2. „faktor autentifikácie“ je faktor, pri ktorom sa potvrdilo, že je spojený s osobou, a ktorý patrí do niektorej z týchto kategórií:

   a) „faktor autentifikácie na základe držby“ je faktor autentifikácie, ktorého držbu je osoba povinná preukázať;

   b) „faktor autentifikácie na základe poznania“ je faktor autentifikácie, ktorého poznanie je osoba povinná preukázať;

   c) „inherentný faktor autentifikácie“ je faktor autentifikácie, ktorý je založený na fyzickej vlastnosti fyzickej osoby, pričom osoba je povinná preukázať, že má túto fyzickú vlastnosť;

3. „dynamická autentifikácia“ je elektronický proces využívajúci kryptografiu alebo iné techniky na poskytnutie prostriedkov, ktoré na požiadanie vytvoria elektronický dôkaz o tom, že osoba má kontrolu nad identifikačnými údajmi alebo ich má v držbe, pričom tento proces sa pri každej autentifikácii medzi osobou a systémom, ktorý overuje jej totožnosť, mení;

4. „systém riadenia informačnej bezpečnosti“ je súbor procesov a postupov určených na zmiernenie rizík súvisiacich s informačnou bezpečnosťou na prijateľné úrovne.

2. Technické špecifikácie a postupy

Prvky technických špecifikácií a postupov uvedené v tejto prílohe sa používajú na stanovenie spôsobu, akým sa požiadavky a kritériá uvedené v článku 8 nariadenia (EÚ) č. 910/2014 uplatňujú na prostriedky elektronickej identifikácie vydané v rámci schémy elektronickej identifikácie.

2.1. *Registrácia*

2.1.1. Žiadosť a prihlásenie

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Zabezpečenie toho, aby žiadateľ poznal podmienky týkajúce sa používania prostriedkov elektronickej identifikácie. 2. Zabezpečenie toho, aby žiadateľ poznal odporúčané bezpečnostné opatrenia týkajúce sa prostriedkov elektronickej identifikácie. 3. Zhromaždenie relevantných údajov o totožnosti požadovaných na preukázanie a overenie totožnosti.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.1.2. Preukazovanie a overovanie totožnosti (fyzická osoba)

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Možno predpokladať, že daná osoba má v držbe dôkaz označujúci údajnú totožnosť, uznaný členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva. 2. Možno predpokladať, že dôkaz je pravý alebo že podľa spoľahlivého zdroja existuje, a podľa všetkého je platný. 3. Spoľahlivému zdroju je známe, že údajná totožnosť existuje, a možno predpokladať, že osoba hlásiaca sa k nejakej totožnosti, je jedna a tá istá.
Pokročilá	Úroveň „nízka“ a zároveň musí byť splnená jedna z alternatív uvedených v bodoch 1 až 4: 1. Bolo overené, že osoba má v držbe dôkaz označujúci údajnú totožnosť, uznaný členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a dôkaz je skontrolovaný, aby sa zistilo, či je pravý, alebo je podľa spoľahlivého zdroja známe, že existuje a viaže sa na skutočnú osobu, a boli podniknuté kroky na minimalizáciu rizika, že totožnosť danej osoby nie je údajná totožnosť, pričom sa bralo do úvahy napríklad riziko, že dôkaz sa stratil, bol odcudzený, jeho platnosť bola pozastavená alebo zrušená alebo uplynula, alebo 2. sa predloží doklad totožnosti počas procesu registrácie v členskom štáte, v ktorom sa doklad vydal, a tento doklad sa zjavne viaže na osobu, ktorá ho predkladá, a podnikli sa kroky na minimalizáciu rizika, že totožnosť danej osoby nie je údajná totožnosť, pričom sa bralo do úvahy napríklad riziko, že doklady sa stratili, boli odcudzené, bola pozastavená alebo zrušená ich platnosť alebo ich platnosť uplynula, alebo 3. ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi stanovenými v oddiele 2.1.2 pre úroveň zabezpečenia „pokročilá“, potom subjekt zodpovedný za registráciu nemusí opakovať už tieto použité postupy za predpokladu, že takéto rovnocenné zabezpečenie potvrdí orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 ([1]) alebo rovnocenný orgán, alebo 4. ak sa prostriedky elektronickej identifikácie vydávajú na základe platného oznámeného prostriedku elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“ alebo „vysoká“, pričom sa berú do úvahy riziká zmeny osobných identifikačných údajov, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „pokročilá“ alebo „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán.

Úroveň zabezpečenia	Potrebné prvky
Vysoká	Musia byť splnené požiadavky uvedené v bode 1 alebo v bode 2: 1. Úroveň „pokročilá“ a zároveň musí byť splnená jedna z alternatív uvedených v písmenách a) až c): a) Ak bolo overené, že daná osoba má v držbe fotografický alebo biometrický identifikačný dôkaz uznaný členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a tento dôkaz označuje údajnú totožnosť, dôkaz je skontrolovaný, aby sa zistilo, či je podľa spoľahlivého zdroja platný, a prostredníctvom porovnania jednej alebo viacerých fyzických vlastností danej osoby so spoľahlivým zdrojom sa identifikuje, že žiadateľ má údajnú totožnosť, alebo b) ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi uvedenými v oddiele 2.1.2 pre úroveň zabezpečenia „vysoká“, potom subjekt zodpovedný za registráciu nemusí opakovať tieto predchádzajúce postupy za predpokladu, že je takéto rovnocenné zabezpečenie potvrdené orgánom posudzovania zhody uvedeným v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenným orgánom, a sú prijaté kroky na preukázanie toho, že výsledky predchádzajúcich postupov sú naďalej platné, alebo c) ak sa prostriedky elektronickej identifikácie vydávajú na základe platných oznámených prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „vysoká“, pričom sa berú do úvahy riziká zmeny osobných identifikačných údajov, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán, a sú prijaté kroky na preukázanie toho, že výsledky predchádzajúceho postupu vydávania oznámených prostriedkov elektronickej identifikácie naďalej platia, alebo 2. ak žiadateľ nepredloží žiadny uznaný fotografický alebo biometrický identifikačný dôkaz, uplatnia sa rovnaké postupy, aké sa na získanie takéhoto uznaného fotografického alebo biometrického identifikačného dôkazu používajú na vnútroštátnej úrovni v členskom štáte subjektu zodpovedného za registráciu.

([1]) Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

2.1.3. Preukazovanie a overovanie totožnosti (právnická osoba)

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Údajná totožnosť právnickej osoby je preukázaná na základe dôkazu uznaného členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva.

Úroveň zabezpečenia	Potrebné prvky
	2. Dôkaz je podľa všetkého platný a možno predpokladať, že je pravý alebo že podľa spoľahlivého zdroja existuje, ak je zahrnutie právnickej osoby do spoľahlivého zdroja dobrovoľné a upravuje ho dohoda medzi právnickou osobou a spoľahlivým zdrojom. 3. Spoľahlivému zdroju nie je známe, že by právnická osoba mala postavenie, ktoré by jej bránilo konať ako daná právnická osoba.
Pokročilá	Úroveň „nízka“ a zároveň musí byť splnená jedna z alternatív uvedených v bodoch 1 až 3: 1. Údajná totožnosť právnickej osoby je preukázaná na základe dôkazu uznaného členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a to vrátane názvu, právnej formy a (prípadne) registračného čísla právnickej osoby, a dôkaz je skontrolovaný, aby sa zistilo, či je pravý, alebo či je podľa spoľahlivého zdroja známe, že existuje, ak sa pre pôsobenie právnickej osoby v jej odvetví vyžaduje, aby bola zahrnutá do spoľahlivého zdroja, a boli podniknuté kroky na minimalizáciu rizika, že totožnosť právnickej osoby nie je údajná totožnosť, pričom sa bralo do úvahy napríklad riziko, že doklady sa stratili, boli odcudzené, bola pozastavená alebo zrušená ich platnosť alebo ich platnosť uplynula, alebo 2. ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi uvedenými v oddiele 2.1.3 pre úroveň zabezpečenia „pokročilá“, potom subjekt zodpovedný za registráciu nemusí opakovať tieto predchádzajúce postupy za predpokladu, že je takéto rovnocenné zabezpečenie potvrdené orgánom posudzovania zhody uvedeným v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenným orgánom, alebo 3. ak sa prostriedky elektronickej identifikácie vydávajú na základe platných oznámených prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“ alebo „vysoká“, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „pokročilá“ alebo „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán.
Vysoká	Úroveň „pokročilá“ a zároveň musí byť splnená jedna z alternatív uvedených v bodoch 1 až 3: 1. Údajná totožnosť právnickej osoby je preukázaná na základe dôkazu uznaného členským štátom, v ktorom sa žiadosť o prostriedok elektronickej identifikácie podáva, a to vrátane názvu právnickej osoby, jej právnej formy a najmenej jedného jedinečného identifikátora používaného na vnútroštátnej úrovni a označujúceho danú právnickú osobu, a dôkaz je skontrolovaný, aby sa zistilo, či je podľa spoľahlivého zdroja platný, alebo

Úroveň zabezpečenia	Potrebné prvky
	2. ak postupy, ktoré v minulosti použil verejný alebo súkromný subjekt v tom istom členskom štáte na iné účely, než je vydanie prostriedku elektronickej identifikácie, poskytujú zabezpečenie rovnocenné s postupmi uvedenými v oddiele 2.1.3 pre úroveň zabezpečenia „vysoká“, potom subjekt zodpovedný za registráciu nemusí opakovať tieto predchádzajúce postupy za predpokladu, že je takéto rovnocenné zabezpečenie potvrdené orgánom posudzovania zhody uvedeným v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenným orgánom, a sú prijaté kroky na preukázanie toho, že výsledky tohto predchádzajúceho postupu sú naďalej platné, alebo 3. ak sa prostriedky elektronickej identifikácie vydávajú na základe platných oznámených prostriedkov elektronickej identifikácie s úrovňou zabezpečenia „vysoká“, nie je potrebné opakovať procesy preukazovania a overovania totožnosti. Ak prostriedok elektronickej identifikácie slúžiaci ako základ nebol oznámený, musí úroveň zabezpečenia „vysoká“ potvrdiť orgán posudzovania zhody uvedený v článku 2 bode 13 nariadenia (ES) č. 765/2008 alebo rovnocenný orgán, a sú prijaté kroky na preukázanie toho, že výsledky predchádzajúceho postupu vydávania oznámených prostriedkov elektronickej identifikácie naďalej platia.

2.1.4. Prepojenie medzi prostriedkami elektronickej identifikácie fyzických a právnických osôb

V príslušných prípadoch platia pre prepojenie medzi prostriedkom elektronickej identifikácie fyzickej osoby a prostriedkom elektronickej identifikácie právnickej osoby (ďalej len „prepojenie“) tieto podmienky:

1. Musí byť možné pozastaviť a/alebo zrušiť prepojenie. Životný cyklus prepojenia (napr. aktivácia, pozastavenie, obnovenie, zrušenie) sa spravuje podľa postupov uznaných na vnútroštátnej úrovni.

2. Fyzická osoba, ktorej prostriedok elektronickej identifikácie je prepojený s prostriedkom elektronickej identifikácie právnickej osoby, môže poveriť uplatňovaním tohto prepojenia inú fyzickú osobu na základe postupov uznaných na vnútroštátnej úrovni. Zodpovednosť však naďalej nesie poverujúca fyzická osoba.

3. Prepojenie sa realizuje takto:

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Je overené, že preukázanie totožnosti fyzickej osoby konajúcej v mene právnickej osoby bolo vykonané na úrovni „nízka“ alebo na vyššej úrovni. 2. Prepojenie bolo vytvorené na základe postupov uznaných na vnútroštátnej úrovni. 3. Spoľahlivému zdroju nie je známe, že by fyzická osoba mala postavenie, ktoré by jej bránilo konať v mene danej právnickej osoby.
Pokročilá	Bod 3 úrovne „nízka“ a zároveň: 1. Je overené, že preukázanie totožnosti fyzickej osoby konajúcej v mene právnickej osoby bolo vykonané na úrovni „pokročilá“ alebo „vysoká“.

Úroveň zabezpečenia	Potrebné prvky
	2. Prepojenie bolo vytvorené na základe postupov uznaných na vnútroštátnej úrovni, ktorých výsledkom bola registrácia prepojenia v spoľahlivom zdroji. 3. Prepojenie bolo overené na základe informácií zo spoľahlivého zdroja.
Vysoká	Bod 3 úrovne „nízka“ a bod 2 úrovne „pokročilá“ a zároveň: 1. Je overené, že preukázanie totožnosti fyzickej osoby konajúcej v mene právnickej osoby bolo vykonané na úrovni „vysoká“. 2. Prepojenie bolo overené na základe jedinečného identifikátora označujúceho právnickú osobu používaného na vnútroštátnej úrovni a na základe informácií zo spoľahlivého zdroja, ktoré jedinečným spôsobom vystihujú fyzickú osobu.

2.2. *Riadenie prostriedkov elektronickej identifikácie*

2.2.1. Vlastnosti a uspôsobenie prostriedkov elektronickej identifikácie

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Prostriedok elektronickej identifikácie využíva najmenej jeden faktor autentifikácie. 2. Prostriedok elektronickej identifikácie je uspôsobený tak, aby vydavateľ mohol prijať primerané kroky na kontrolu toho, či sa používa iba pod kontrolou alebo v držbe osoby, ktorej patrí.
Pokročilá	1. Prostriedok elektronickej identifikácie využíva najmenej dva faktory autentifikácie z rôznych kategórií. 2. Prostriedok elektronickej identifikácie je uspôsobený tak, aby bolo možné predpokladať, že sa používa iba pod kontrolou alebo v držbe osoby, ktorej patrí.
Vysoká	Úroveň „pokročilá“ a zároveň: 1. Prostriedok elektronickej identifikácie chráni proti vyhotovovaniu duplikátov a manipulácii, ako aj proti útočníkom s vysokým útočným potenciálom. 2. Prostriedok elektronickej identifikácie je uspôsobený tak, aby ho osoba, ktorej patrí, mohla spoľahlivo chrániť pred použitím inými osobami.

2.2.2. Vydanie, doručenie a aktivácia

Úroveň zabezpečenia	Potrebné prvky
Nízka	Po vydaní sa prostriedok elektronickej identifikácie doručí prostredníctvom mechanizmu, na základe ktorého sa dá predpokladať, že ho dostane iba určená osoba.
Pokročilá	Po vydaní sa prostriedok elektronickej identifikácie doručí prostredníctvom mechanizmu, na základe ktorého sa dá predpokladať, že bude doručený iba do držby osoby, ktorej patrí.
Vysoká	V procese aktivácie sa overí, že prostriedok elektronickej identifikácie bol doručený iba do držby osoby, ktorej patrí.

2.2.3. Pozastavenie, zrušenie a obnovenie aktivácie

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Prostriedok elektronickej identifikácie je možné pozastaviť a/alebo zrušiť včas a účinným spôsobom. 2. Existujú opatrenia na zabránenie neoprávnenému pozastaveniu, zrušeniu a/alebo obnoveniu aktivácie. 3. K obnoveniu aktivácie dôjde len vtedy, ak sú naďalej splnené rovnaké požiadavky na zabezpečenie ako požiadavky stanovené pred pozastavením alebo zrušením.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.2.4. Obnovenie a výmena

Úroveň zabezpečenia	Potrebné prvky
Nízka	Ak sa vezmú do úvahy riziká zmeny osobných identifikačných údajov, obnovenie alebo výmena musia spĺňať rovnaké požiadavky na zabezpečenie ako pôvodné preukázanie a overenie identity alebo sa zakladajú na platnom prostriedku elektronickej identifikácie rovnakej alebo vyššej úrovne zabezpečenia.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Úroveň „nízka“ a zároveň: Ak sa obnovenie alebo výmena zakladajú na platnom prostriedku elektronickej identifikácie, identifikačné údaje sa overujú podľa spoľahlivého zdroja.

2.3. *Autentifikácia*

Tento oddiel sa zameriava na hrozby spojené s používaním mechanizmu autentifikácie a uvádzajú sa v ňom požiadavky na každú úroveň zabezpečenia. Kontroly sa v tomto oddiele chápu ako kontroly úmerné rizikám na danej úrovni.

2.3.1. Mechanizmus autentifikácie

V nasledujúcej tabuľke sa uvádzajú požiadavky podľa jednotlivých úrovní zabezpečenia, pokiaľ ide o mechanizmus autentifikácie, prostredníctvom ktorého fyzická alebo právnická osoba používa prostriedok elektronickej identifikácie na potvrdenie svojej totožnosti spoliehajúcej sa strane.

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Uvoľneniu osobných identifikačných údajov predchádza spoľahlivé overenie prostriedku elektronickej identifikácie a jeho platnosti. 2. Ak sú osobné identifikačné údaje uložené ako súčasť mechanizmu autentifikácie, tieto informácie sú zabezpečené proti strate a proti vyzradeniu vrátane offline analýzy. 3. V mechanizme autentifikácie sú implementované bezpečnostné kontroly na overenie prostriedku elektronickej identifikácie, takže je veľmi nepravdepodobné, že by činnosti, ako je hádanie, odpočúvanie, reprodukcia alebo manipulácia komunikácie útočníkom s rozšíreným základným útočným potenciálom, mohli rozvrátiť mechanizmus autentifikácie.

Úroveň zabezpečenia	Potrebné prvky
Pokročilá	Úroveň „nízka“ a zároveň: 1. Uvoľneniu osobných identifikačných údajov predchádza spoľahlivé overenie prostriedku elektronickej identifikácie a jeho platnosti prostredníctvom dynamickej autentifikácie. 2. V mechanizme autentifikácie sú implementované bezpečnostné kontroly na overenie prostriedku elektronickej identifikácie, takže je veľmi nepravdepodobné, že by činnosti, ako je hádanie, odpočúvanie, reprodukcia alebo manipulácia komunikácie útočníkom so stredným útočným potenciálom, mohli rozvrátiť mechanizmus autentifikácie.
Vysoká	Úroveň „pokročilá“ a zároveň: V mechanizme autentifikácie sú implementované bezpečnostné kontroly na overenie prostriedku elektronickej identifikácie, takže je veľmi nepravdepodobné, že by činnosti, ako je hádanie, odpočúvanie, reprodukcia alebo manipulácia komunikácie útočníkom s vysokým útočným potenciálom, mohli rozvrátiť mechanizmus autentifikácie.

2.4. *Riadenie a organizácia*

Všetci účastníci, ktorí poskytujú služby súvisiace s elektronickou identifikáciou v cezhraničnom kontexte (ďalej len „poskytovatelia“), musia mať zavedené zdokumentované postupy a politiky riadenia informačnej bezpečnosti, prístupy k riadeniu rizík a iné uznané kontroly, aby príslušným riadiacim orgánom pre schémy elektronickej identifikácie v jednotlivých členských štátoch poskytli záruku, že sa zaviedli účinné postupy. V celom oddiele 2.4 sa všetky požiadavky/prvky chápu ako úmerné rizikám na danej úrovni.

2.4.1. Všeobecné ustanovenia

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Poskytovatelia dodávajúci prevádzkové služby, na ktoré sa vzťahuje toto nariadenie, sú orgány verejnej správy alebo právnické osoby uznané ako také vnútroštátnym právom členského štátu, majú zavedenú organizáciu a sú plne prevádzkyschopné na všetkých úsekoch, ktoré sú relevantné pre poskytovanie týchto služieb. 2. Poskytovatelia spĺňajú všetky právne požiadavky, ktoré sa na nich vzťahujú v súvislosti s prevádzkou a dodávaním služby, vrátane druhov informácií, ktoré možno požadovať, spôsobu vykonávania preukazovania totožnosti, informácií, ktoré sa môžu uchovávať, a času, počas ktorého sa môžu uchovávať. 3. Poskytovatelia dokážu preukázať svoju schopnosť prevziať riziko zodpovednosti za škodu, ako aj to, že majú dostatočné finančné zdroje na pokračovanie činnosti a poskytovanie služieb. 4. Poskytovatelia sú zodpovední za plnenie všetkých záväzkov zadaných externým subjektom a za ich súlad s politikou schémy tak, ako keby tieto úlohy vykonali samotní poskytovatelia. 5. Schémy elektronickej identifikácie, ktoré neboli zriadené na základe vnútroštátneho práva, majú zavedený účinný plán ukončenia činnosti. Takýto plán musí zahŕňať riadne prerušenie služby alebo pokračovanie iným poskytovateľom, spôsob, akým sa informujú príslušné orgány a koncoví používatelia, ako aj podrobnosti o tom, akým spôsobom sa v súlade s politikou schémy majú chrániť, uchovávať a ničiť záznamy.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.2. Uverejnené oznámenia a informácie pre používateľov

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Existencia zverejneného vymedzenia služby, ktoré zahŕňa všetky platné podmienky a poplatky vrátane všetkých obmedzení jej používania. Vymedzenie služby musí obsahovať politiku ochrany osobných údajov. 2. Musí sa zaviesť vhodná politika a postupy, aby sa zabezpečilo, že používatelia služby budú včas a spoľahlivo informovaní o všetkých zmenách vymedzenia služby a akýchkoľvek platných podmienok a politiky ochrany osobných údajov pre uvedenú službu. 3. Musia sa zaviesť vhodné politiky a postupy na zabezpečenie úplných a správnych odpovedí na žiadosti o informácie.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.3. Riadenie informačnej bezpečnosti

Úroveň zabezpečenia	Potrebné prvky
Nízka	Existuje účinný systém riadenia informačnej bezpečnosti na riadenie a kontrolu rizík v oblasti informačnej bezpečnosti.
Pokročilá	Úroveň „nízka“ a zároveň: Systém riadenia informačnej bezpečnosti dodržiava osvedčené normy alebo zásady riadenia a kontroly rizík v oblasti informačnej bezpečnosti.
Vysoká	Rovnaké ako pri úrovni „pokročilá“.

2.4.4. Vedenie záznamov

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Zaznamenávanie a uchovávanie relevantných informácií pomocou účinného systému riadenia záznamov pri zohľadnení platných právnych predpisov a osvedčených postupov v oblasti ochrany a uchovávania údajov. 2. Pokiaľ to povoľujú vnútroštátne právne predpisy alebo iné vnútroštátne správne úpravy, uchovávanie a ochrana záznamov, kým sa vyžadujú na účely auditu a vyšetrovania porušení bezpečnosti a uchovávania údajov, a ich následné bezpečné zničenie.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.5. Zariadenia a personál

V nasledujúcej tabuľke sa uvádzajú požiadavky na zariadenia a personál a prípadne na subdodávateľov, ktorí vykonávajú úlohy, na ktoré sa vzťahuje toto nariadenie. Súlad s každou z požiadaviek musí byť úmerný úrovni rizika spojeného s poskytovanou úrovňou zabezpečenia.

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Existencia postupov, ktoré zabezpečujú, aby personál a subdodávatelia boli dostatočne vyškolení, kvalifikovaní a skúsení, pokiaľ ide o zručnosti potrebné na vykonávanie úloh, ktoré plnia. 2. Existencia dostatočného počtu zamestnancov a subdodávateľov na primeranú prevádzku služby a zaistenie jej zdrojov v súlade s jej politikami a postupmi. 3. Zariadenia používané na poskytovanie služby sa nepretržite monitorujú vzhľadom na škody spôsobené environmentálnymi udalosťami, neoprávnený prístup a iné faktory, ktoré môžu mať vplyv na bezpečnosť služby, a sú pred nimi chránené. 4. Zariadenia používané na poskytovanie služby zabezpečujú, aby bol prístup do priestorov, v ktorých sa uchovávajú alebo spracúvajú osobné, kryptografické alebo iné citlivé informácie, obmedzený na oprávnených zamestnancov alebo subdodávateľov.
Pokročilá	Rovnaké ako pri úrovni „nízka“.
Vysoká	Rovnaké ako pri úrovni „nízka“.

2.4.6. Technické kontroly

Úroveň zabezpečenia	Potrebné prvky
Nízka	1. Existencia primeraných technických kontrol na riadenie rizík ohrozujúcich bezpečnosť služieb a na ochranu dôvernosti, integrity a dostupnosti spracúvaných informácií. 2. Elektronické komunikačné kanály používané na výmenu osobných alebo citlivých informácií sú chránené proti odpočúvaniu, manipulácii a reprodukcii. 3. Ak sa na vydávanie prostriedkov elektronickej identifikácie a autentifikáciu používa citlivý kryptografický materiál, prístup k nemu je obmedzený na úlohy a aplikácie, ktoré si ho bezpodmienečne vyžadujú. Musí sa zabezpečiť, aby sa takýto materiál nikdy trvalo neuchovával ako jednoduchý text. 4. Existujú postupy na zabezpečenie toho, aby sa stále udržiavala bezpečnosť a aby existovala schopnosť reagovať na zmeny úrovní rizika, incidenty a narušenia bezpečnosti. 5. Všetky nosiče obsahujúce osobné, kryptografické alebo iné citlivé informácie sa uchovávajú, prepravujú a odstraňujú bezpečným a zabezpečeným spôsobom.
Pokročilá	Rovnaké ako pri úrovni „nízka“ a zároveň: Ak sa na vydávanie prostriedkov elektronickej identifikácie a na autentifikáciu používa citlivý kryptografický materiál, je chránený pred manipuláciou.
Vysoká	Rovnaké ako pri úrovni „pokročilá“.

2.4.7. Súlad a audit

Úroveň zabezpečenia	Potrebné prvky
Nízka	Existencia pravidelných vnútorných auditov zameraných na pokrytie všetkých úsekov týkajúcich sa dodávania poskytovaných služieb na zabezpečenie súladu s príslušnou politikou.

Úroveň zabezpečenia	Potrebné prvky
Pokročilá	Existencia pravidelných nezávislých vnútorných alebo vonkajších auditov zameraných na pokrytie všetkých úsekov týkajúcich sa dodávania poskytovaných služieb na zabezpečenie súladu s príslušnou politikou.
Vysoká	1. Existencia pravidelných nezávislých vonkajších auditov zameraných na pokrytie všetkých úsekov týkajúcich sa dodávania poskytovaných služieb na zabezpečenie súladu s príslušnou politikou. 2. Ak schému riadi priamo orgán verejnej správy, audit sa uskutočňuje v súlade s vnútroštátnymi právnymi predpismi.

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2015/1503

z 8. septembra 2015,

ktorým sa ustanovujú paušálne dovozné hodnoty na určovanie vstupných cien niektorých druhov ovocia a zeleniny

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 1308/2013 zo 17. decembra 2013, ktorým sa vytvára spoločná organizácia trhov s poľnohospodárskymi výrobkami a ktorým sa zrušujú nariadenia Rady (EHS) č. 922/72, (EHS) č. 234/79, (ES) č. 1037/2001 a (ES) č. 1234/2007 ([1]),

so zreteľom na vykonávacie nariadenie Komisie (EÚ) č. 543/2011 zo 7. júna 2011, ktorým sa ustanovujú podrobné pravidlá uplatňovania nariadenia Rady (ES) č. 1234/2007, pokiaľ ide o sektory ovocia a zeleniny a spracovaného ovocia a zeleniny ([2]), a najmä na jeho článok 136 ods. 1,

keďže:

(1) Vykonávacím nariadením (EÚ) č. 543/2011 sa v súlade s výsledkami Uruguajského kola mnohostranných obchodných rokovaní ustanovujú kritériá, na základe ktorých Komisia stanovuje paušálne hodnoty na dovoz z tretích krajín, pokiaľ ide o výrobky a obdobia uvedené v časti A prílohy XVI k uvedenému nariadeniu.

(2) Paušálne dovozné hodnoty sa vypočítajú každý pracovný deň v súlade s článkom 136 ods. 1 vykonávacieho nariadenia (EÚ) č. 543/2011, pričom sa zohľadnia premenlivé každodenné údaje. Toto nariadenie by preto malo nadobudnúť účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*,

PRIJALA TOTO NARIADENIE:

Článok 1

Paušálne dovozné hodnoty uvedené v článku 136 vykonávacieho nariadenia (EÚ) č. 543/2011 sú stanovené v prílohe k tomuto nariadeniu.

Článok 2

Toto nariadenie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

v mene predsedu

Jerzy PLEWA

generálny riaditeľ pre poľnohospodárstvo a rozvoj vidieka

([1]) Ú. v. EÚ L 347, 20.12.2013, s. 671.
([2]) Ú. v. EÚ L 157, 15.6.2011, s. 1.

PRÍLOHA

Paušálne dovozné hodnoty na určovanie vstupných cien niektorých druhov ovocia a zeleniny

(EUR/100 kg)

Číselný znak KN	Kód tretej krajiny (1)	Paušálna dovozná hodnota
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

Číselný znak KN	Kód tretej krajiny (1)	Paušálna dovozná hodnota
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Nomenklatúra krajín stanovená nariadením Komisie (EÚ) č. 1106/2012 z 27. novembra 2012, ktorým sa vykonáva nariadenie Európskeho parlamentu a Rady (ES) č. 471/2009 o štatistike Spoločenstva o zahraničnom obchode s nečlenskými krajinami, pokiaľ ide o aktualizáciu nomenklatúry krajín a území (Ú. v. EÚ L 328, 28.11.2012, s. 7). Kód „ZZ“ znamená „iného pôvodu“.

ROZHODNUTIA

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2015/1504

zo 7. septembra 2015,

ktorým sa udeľujú výnimky určitým členským štátom, pokiaľ ide o poskytovanie štatistiky podľa nariadenia Európskeho parlamentu a Rady (ES) č. 1099/2008 o energetickej štatistike

[oznámené pod číslom C(2015) 6105]

(Iba estónske, francúzske, grécke, holandské a slovenské znenie je autentické)

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 1099/2008 z 22. októbra 2008 o energetickej štatistike ([1]), a najmä na jeho článok 5 ods. 4 a článok 10 ods. 2,

keďže:

(1) V súlade s článkom 5 ods. 4 nariadenia (ES) č. 1099/2008 sa v prípade riadne odôvodnenej žiadosti členského štátu môžu udeliť výnimky pre tie časti národných štatistík, pre ktoré by zhromažďovanie viedlo k nadmernému zaťaženiu respondentov.

(2) Belgicko, Estónsko, Cyprus a Slovensko podali žiadosti o udelenie výnimiek, pokiaľ ide o poskytovanie podrobnej štatistiky o spotrebe energie v domácnostiach podľa druhu konečného použitia za určité referenčné roky.

(3) Informácie predložené týmito členskými štátmi opodstatňujú udelenie výnimiek.

(4) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom Výboru pre Európsky štatistický systém,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Týmto sa udeľujú tieto výnimky z ustanovení nariadenia (ES) č. 1099/2008:

1. Belgicku sa udeľuje výnimka z predkladania údajov za referenčný rok 2015, pokiaľ ide o bod 1.2.3 položky 4.2.1 až 4.2.5, bod 2.2.3 položky 4.2.1 až 4.2.5, bod 3.2.3 položky 3.1 až 3.6, bod 4.2.3 položky 7.2.1 až 7.2.5, bod 5.2.4 položky 4.2.1 až 4.2.5 prílohy B týkajúcej sa podrobnej štatistiky o spotrebe energie v domácnostiach podľa druhu konečného použitia (ako je vymedzené v bode 2.3 položke 26 „Ostatné sektory – Domácnosti“ prílohy A).

([1]) Ú. v. EÚ L 304, 14.11.2008, s. 1.

2. Estónsku sa udeľuje výnimka z predkladania údajov za referenčné roky 2015, 2016 a 2017, pokiaľ ide o bod 1.2.3 položky 4.2.1 až 4.2.5, bod 2.2.3 položky 4.2.1 až 4.2.5, bod 3.2.3 položky 3.1 až 3.6, bod 4.2.3 položky 7.2.1 až 7.2.5, bod 5.2.4 položky 4.2.1 až 4.2.5 prílohy B týkajúcej sa podrobnej štatistiky o spotrebe energie v domácnostiach podľa druhu konečného použitia (ako je vymedzené v bode 2.3 položke 26 „Ostatné sektory – Domácnosti“ prílohy A).

3. Cypru sa udeľuje výnimka z predkladania údajov za referenčné roky 2015, 2016 a 2017, pokiaľ ide o bod 1.2.3 položky 4.2.1 až 4.2.5, bod 2.2.3 položky 4.2.1 až 4.2.5, bod 3.2.3 položky 3.1 až 3.6, bod 5.2.4 položky 4.2.1 až 4.2.5 prílohy B týkajúcej sa podrobnej štatistiky o spotrebe energie v domácnostiach podľa druhu konečného použitia (ako je vymedzené v bode 2.3 položke 26 „Ostatné sektory – Domácnosti“ prílohy A).

4. Slovensku sa udeľuje výnimka z predkladania údajov za referenčné roky 2015 a 2016, pokiaľ ide o bod 1.2.3 položky 4.2.1 až 4.2.5, bod 2.2.3 položky 4.2.1 až 4.2.5, bod 3.2.3 položky 3.1 až 3.6, bod 4.2.3 položky 7.2.1 až 7.2.5, bod 5.2.4 položky 4.2.1 až 4.2.5 prílohy B týkajúcej sa podrobnej štatistiky o spotrebe energie v domácnostiach podľa druhu konečného použitia (ako je vymedzené v bode 2.3 položke 26 „Ostatné sektory – Domácnosti“ prílohy A).

Článok 2

Toto rozhodnutie je určené Belgickému kráľovstvu, Estónskej republike, Cyperskej republike a Slovenskej republike.

V Bruseli 7. septembra 2015

Za Komisiu

Marianne THYSSEN

členka Komisie

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2015/1505

z 8. septembra 2015,

ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 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 22 ods. 5,

keďže:

(1) Dôveryhodné zoznamy sú nevyhnutné na vybudovanie dôvery medzi trhovými subjektmi, pretože určujú štatút poskytovateľa služieb v čase dohľadu.

(2) Cezhraničné používanie elektronických podpisov bolo uľahčené rozhodnutím Komisie 2009/767/ES ([2]), ktorým sa stanovila povinnosť členských štátov vytvoriť, viesť a uverejňovať zoznamy dôveryhodných informácií vrátane informácií o poskytovateľoch certifikačných služieb, ktorí vydávajú kvalifikované certifikáty verejnosti v súlade so smernicou Európskeho parlamentu a Rady 1999/93/ES ([3]) a ktorí sú pod dohľadom určitého členského štátu alebo sú v ňom akreditovaní.

(3) V článku 22 nariadenia (EÚ) č. 910/2014 sa stanovuje povinnosť členských štátov vytvoriť, viesť a uverejňovať dôveryhodné zoznamy, ktoré sú zabezpečeným spôsobom elektronicky podpísané alebo zapečatené vo forme vhodnej na automatizované spracovanie, a poskytnúť Komisii informácie o orgáne zodpovednom za vytvorenie, vedenie a uverejňovanie národných dôveryhodných zoznamov.

(4) Poskytovateľ dôveryhodných služieb a ním poskytované dôveryhodné služby by sa mali považovať za kvalifikované, ak je kvalifikovaný štatút spojený s poskytovateľom v dôveryhodnom zozname. S cieľom zabezpečiť, aby ostatné povinnosti vyplývajúce z nariadenia (EÚ) č. 910/2014, najmä tie, ktoré sú stanovené v článkoch 27 a 37, mohli poskytovatelia služieb ľahko splniť na diaľku a elektronickými prostriedkami a aby sa splnili oprávnené očakávania ostatných poskytovateľov certifikačných služieb, ktorí nevydávajú kvalifikované certifikáty, ale poskytujú služby súvisiace s elektronickými podpismi v zmysle smernice 1999/93/ES a v zozname sú uvedení do 30. júna 2016, by mali mať členské štáty možnosť pridať do dôveryhodných zoznamov aj iné než kvalifikované dôveryhodné služby, a to dobrovoľne, na vnútroštátnej úrovni, za predpokladu, že sa jasne uvedie, že tieto služby nie sú kvalifikované podľa nariadenia (EÚ) č. 910/2014.

(5) V súlade s odôvodnením 25 nariadenia (EÚ) č. 910/2014 môžu členské štáty pridať iné druhy dôveryhodných služieb na vnútroštátnej úrovni než tie, ktoré sú vymedzené v článku 3 ods. 16 nariadenia (EÚ) č. 910/2014, za predpokladu, že sa jasne uvedie, že tieto služby nie sú kvalifikované podľa nariadenia (EÚ) č. 910/2014.

(6) 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

Členské štáty vytvoria, vedú a uverejňujú dôveryhodné zoznamy vrátane informácií o kvalifikovaných poskytovateľoch dôveryhodných služieb, nad ktorými vykonávajú dohľad, ako aj informácií o nimi poskytovaných kvalifikovaných dôveryhodných službách. Tieto zoznamy musia byť v súlade s technickými špecifikáciami stanovenými v prílohe I.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73.

([2]) Rozhodnutie Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu (Ú. v. EÚ L 274, 20.10.2009, s. 36).

([3]) Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy (Ú. v. ES L 13, 19.1.2000, s. 12).

Článok 2

Členské štáty môžu do týchto dôveryhodných zoznamov zaradiť informácie o nekvalifikovaných poskytovateľoch dôveryhodných služieb spolu s informáciami o nimi poskytovaných nekvalifikovaných dôveryhodných službách. V tomto zozname sa musí jasne označiť, ktorí poskytovatelia dôveryhodných služieb nie sú kvalifikovaní a ktoré nimi poskytované dôveryhodné služby nie sú kvalifikované.

Článok 3

1. Podľa článku 22 ods. 2 nariadenia (EÚ) č. 910/2014 členské štáty elektronicky podpisujú alebo zapečaťujú formu dôveryhodného zoznamu vhodnú na automatizované spracovanie v súlade s technickými špecifikáciami stanovenými v prílohe I.

2. Ak členský štát elektronicky uverejní formu dôveryhodného zoznamu čitateľnú ľudským okom, musí zabezpečiť, aby táto forma dôveryhodného zoznamu obsahovala rovnaké údaje ako forma vhodná na automatizované spracovanie, a elektronicky ju podpíše alebo zapečatí v súlade s technickými špecifikáciami stanovenými v prílohe I.

Článok 4

1. Členské štáty oznamujú Komisii informácie uvedené v článku 22 ods. 3 nariadenia (EÚ) č. 910/2014 podľa vzoru v prílohe II.

2. Informácie uvedené v odseku 1 zahŕňajú dva alebo viac certifikátov s verejným kľúčom prevádzkovateľa schémy s dobou platnosti posunutou aspoň o 3 mesiace, ktoré zodpovedajú súkromným kľúčom, ktoré sa môžu používať na elektronicky podpísanú alebo zapečatenú formu dôveryhodného zoznamu vhodnú na automatizované spracovanie a na formu čitateľnú ľudským okom po uverejnení.

3. Podľa článku 22 ods. 4 nariadenia (EÚ) č. 910/2014 Komisia prostredníctvom zabezpečeného kanálu na overenom webovom serveri sprístupňuje verejnosti informácie oznámené členskými štátmi uvedené v odsekoch 1 a 2 v elektronicky podpísanej alebo zapečatenej forme vhodnej na automatizované spracovanie.

4. Komisia môže prostredníctvom zabezpečeného kanálu na overenom webovom serveri sprístupniť verejnosti informácie oznámené členskými štátmi uvedené v odsekoch 1 a 2 v elektronicky podpísanej alebo zapečatenej forme čitateľnej ľudským okom.

Článok 5

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

Toto rozhodnutie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA I

TECHNICKÉ ŠPECIFIKÁCIE SPOLOČNÉHO VZORU PRE DÔVERYHODNÉ ZOZNAMY

KAPITOLA I

VŠEOBECNÉ POŽIADAVKY

Dôveryhodné zoznamy obsahujú súčasné aj všetky historické informácie o štatúte dôveryhodných služieb uvedených v zoznamoch, datujúce sa od začlenenia poskytovateľa dôveryhodnej služby do dôveryhodných zoznamov.

Pojmy „schválený“, „akreditovaný“ a/alebo „podliehajúci dohľadu“ v súčasných špecifikáciách takisto zahŕňajú vnútroštátne schémy schvaľovania, ale dodatočné informácie o povahe všetkých týchto vnútroštátnych schém poskytnú členské štáty vo svojom dôveryhodnom zozname vrátane objasnenia možných rozdielov oproti schémam dohľadu uplatňovaným na kvalifikovaných poskytovateľov dôveryhodných služieb a nimi poskytované kvalifikované dôveryhodné služby.

Informácie uvedené v dôveryhodnom zozname sú zamerané v prvom rade na podporu validácie tokenov kvalifikovaných dôveryhodných služieb, t. j. fyzických alebo binárnych (logických) objektov vygenerovaných alebo vydaných v dôsledku využitia dôveryhodnej služby, napr. menovite kvalifikovaných elektronických podpisov/pečatí alebo zdokonalených elektronických podpisov/pečatí podporovaných kvalifikovaným certifikátom, kvalifikovaných časových pečiatok, kvalifikovaných elektronických potvrdení o doručení atď.

KAPITOLA II

PODROBNÉ ŠPECIFIKÁCIE SPOLOČNÉHO VZORU PRE DÔVERYHODNÉ ZOZNAMY

Tieto špecifikácie sú založené na špecifikáciách a požiadavkách stanovených v ETSI TS 119 612 v2.1.1 (ďalej len „ETSI TS 119 612“).

Ak sa v týchto špecifikáciách nestanovuje žiadna osobitná požiadavka, uplatňujú sa požiadavky ETSI TS 119 612 časti 5 a 6 v celom rozsahu. Ak sa v týchto špecifikáciách stanovujú osobitné požiadavky, majú prednosť pred zodpovedajúcimi požiadavkami ETSI TS 119 612. V prípade rozdielov medzi týmito špecifikáciami a špecifikáciami ETSI TS 119 612 majú prednosť tieto špecifikácie.

Názov schémy („Scheme name“) (odsek 5.3.6)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.6. normy TS 119 612, v ktorom sa pre schému používa tento názov:

„EN_name_value“ = „Dôveryhodný zoznam vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí sú pod dohľadom členského štátu pôvodu, spolu s informáciami týkajúcimi sa nimi poskytovaných kvalifikovaných dôveryhodných služieb v súlade s príslušnými ustanoveniami uvedenými v nariadení 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.“

URI informácií o schéme („Scheme information URI“) (odsek 5.3.7)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.7. normy TS 119 612, v ktorom „príslušné informácie o schéme“ zahŕňajú minimálne:

a) Úvodné informácie spoločné pre všetky členské štáty o rozsahu a súvislostiach dôveryhodného zoznamu, schéme, ktorá je základom dohľadu, a v prípade potreby aj príslušnú vnútroštátnu schému (príslušné vnútroštátne schémy) schvaľovania (napr. akreditáciu). Spoločný text, ktorý sa má použiť, je ďalej uvedený text, v ktorom sa reťazec znakov „[*názov príslušného členského štátu*]“ nahradí názvom príslušného členského štátu:

> „Tento zoznam je dôveryhodným zoznamom vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb, ktorí sú pod dohľadom [*názov príslušného členského štátu*], spolu s informáciami týkajúcimi sa nimi poskytovaných kvalifikovaných dôveryhodných služieb v súlade s príslušnými ustanoveniami uvedenými v nariadení 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.

Cezhraničné používanie elektronických podpisov bolo uľahčené rozhodnutím Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa stanovila povinnosť členských štátov vytvoriť, viesť a uverejňovať zoznamy dôveryhodných informácií vrátane informácií o poskytovateľoch certifikačných služieb, ktorí vydávajú kvalifikované certifikáty verejnosti v súlade so smernicou Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy a ktorí sú pod dohľadom určitého členského štátu alebo sú v ňom akreditovaní. Súčasný dôveryhodný zoznam je pokračovaním zoznamu dôveryhodných informácií vytvoreného podľa rozhodnutia 2009/767/ES.“

Dôveryhodné zoznamy sú základnými prvkami pri budovaní dôvery medzi elektronickými trhovými subjektmi vďaka tomu, že používateľom umožňujú určiť kvalifikovaný štatút a históriu štatútu poskytovateľov dôveryhodných služieb a ich služieb.

Dôveryhodné zoznamy členských štátov obsahujú prinajmenšom informácie uvedené v článkoch 1 a 2 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1505.

Členské štáty môžu do dôveryhodných zoznamov zaradiť informácie o nekvalifikovaných poskytovateľoch dôveryhodných služieb spolu s informáciami o nimi poskytovaných nekvalifikovaných dôveryhodných službách. Jasne sa musí uviesť, že nie sú kvalifikovaní podľa nariadenia (EÚ) č. 910/2014.

Členské štáty môžu do dôveryhodných zoznamov zaradiť informácie aj o iných druhoch dôveryhodných služieb vymedzených na vnútroštátnej úrovni než tie, ktoré sú vymedzené v článku 3 ods. 16 nariadenia (EÚ) č. 910/2014. Jasne sa musí uviesť, že nie sú kvalifikované podľa nariadenia (EÚ) č. 910/2014.

b) Konkrétne informácie o schéme, ktorá je základom dohľadu, a v prípade potreby aj o príslušnej vnútroštátnej schéme (príslušných vnútroštátnych schémach) schvaľovania (napr. akreditácia), najmä ([1]):

1. Informácie o vnútroštátnom systéme dohľadu, ktoré sa vzťahujú na kvalifikovaných a nekvalifikovaných poskytovateľov dôveryhodných služieb a nimi poskytované kvalifikované a nekvalifikované dôveryhodné služby, ako ich upravuje nariadenie (EÚ) č. 910/2014;

2. Prípadne informácie o vnútroštátnych dobrovoľných akreditačných schémach, ktoré sa týkajú poskytovateľov certifikačných služieb vydávajúcich kvalifikované certifikáty podľa smernice 1999/93/ES;

Tieto konkrétne informácie zahŕňajú pri každej uvedenej základnej schéme minimálne:

1. Všeobecný opis;

2. Informácie o postupe dodržiavanom pre vnútroštátny systém dohľadu a prípadne pre schvaľovanie podľa vnútroštátnej schémy schvaľovania.

3. Informácie o kritériách, podľa ktorých sa vykonáva a v prípade potreby schvaľuje dozor nad poskytovateľmi dôveryhodných služieb.

4. Informácie o kritériách a pravidlách uplatnených pri výbere osôb vykonávajúcich dohľad alebo audítorov a pri vymedzení spôsobu, akým majú posudzovať poskytovateľov dôveryhodných služieb a nimi poskytované dôveryhodné služby.

5. V prípade potreby aj iné kontaktné a všeobecné informácie, ktoré sa týkajú prevádzkovania schémy.

Typ schémy/komunity/pravidlá („Scheme type/community/rules“) (odsek 5.3.9)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.9 normy TS 119 612.

Zahŕňa len URI v britskej angličtine.

([1]) Uvedené súbory informácií sú pre závislé strany mimoriadne dôležité na posúdenie kvality a stupňa bezpečnosti týchto systémov. Uvedené súbory informácií sa uvádzajú na úrovni dôveryhodného zoznamu prostredníctvom súčasných „Scheme information URI“ (odsek 5.3.7 – informácie, ktoré poskytujú členské štáty), „Scheme type/community/rules“ (odsek 5.3.9 – prostredníctvom textu spoločného pre všetky členské štáty) a „TSL policy/legal notice“ (odsek 5.3.11 – text spoločný pre všetky členské štáty spolu s možnosťou doplniť texty/referencie špecifické pre daný členský štát). Dodatočné informácie o takýchto systémoch nekvalifikovaných dôveryhodných služieb a (kvalifikovaných) dôveryhodných služieb definovaných na vnútroštátnej úrovni sa v prípade potreby a ak je to uplatniteľné môžu poskytovať na úrovni služby (napríklad na účely odlíšenia viacerých úrovní kvality/bezpečnosti) pomocou „Scheme service definition URI“ (odsek 5.5.6).

Zahŕňa minimálne dve URI:

1. URI spoločný pre všetky dôveryhodné zoznamy členských štátov, ktorý odkazuje na opisný text uplatniteľný na všetky dôveryhodné zoznamy nasledujúcim spôsobom:

   URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

   Opisný text:

   „Participation in a scheme

   Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

   The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

   Policy/rules for the assessment of the listed services

   Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

   The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

   The trusted lists include both current and historical information about the status of listed trust services.

   Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) schemes) under which the trust service providers and the trust services that they provide are listed.

   Interpretation of the Trusted List

   The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

   The ‚qualified' status of a trust service is indicated by the combination of the ‚Service type identifier' (‚Sti') value in a service entry and the status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'. Historical information about such a qualified status is similarly provided when applicable.

   Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

   A ‚CA/QC' ‚Service type identifier' (‚Sti') entry (possibly further qualified as being a ‚RootCA-QC' through the use of the appropriate ‚Service information extension' (‚Sie') additionalServiceInformation Extension)

   — indicates that any end-entity certificate issued by or under the CA represented by the ‚Service digital identifier' (‚Sdi') CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

     — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

     — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. ‚undersupervision', ‚supervisionincessation', ‚accredited' or ‚granted') for that entry.

— **and IF** ‚Sie' ‚Qualifications Extension' information is present, then in addition to the above default rule, those certificates that are identified through the use of ‚Sie' ‚Qualifications Extension' information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the ‚SSCD support' and/or ‚Legal person as subject' (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‚Key usage' pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of ‚Qualifiers' used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — ‚QCStatement' meaning the identified certificates) is(are) qualified under Directive 1999/93/EC;

    — ‚QCForESig' meaning the identified certificates), when claimed or stated as qualified certificates), is (are) qualified certificates) for electronic signature under Regulation (EU) No 910/2014;

    — ‚QCForESeal' meaning the identified certificates), when claimed or stated as qualified certificates), is (are) qualified certificates) for electronic seal under Regulation (EU) No 910/2014;

    — ‚QCForWSA' meaning the identified certificates), when claimed or stated as qualified certificates), is (are) qualified certificates) for web site authentication under Regulation (EU) No 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — ‚NotQualified' meaning the identified certificates) is(are) not to be considered as qualified; And/or

  — to indicate the nature of the SSCD support:

    — ‚QCWithSSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have their private key residing in an SSCD, or

    — ‚QCNoSSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have not their private key residing in an SSCD, or

    — ‚QCSSCDStatusAsInCert' meaning the identified certificates), when claimed or stated as qualified certificates), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — ‚QCWithQSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have their private key residing in a QSCD, or

    — ‚QCNoQSCD' meaning the identified certificates), when claimed or stated as qualified certificates), have not their private key residing in a QSCD, or

    — ‚QCQSCDStatusAsInCert' meaning the identified certificates), when claimed or stated as qualified certificates), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — ‚QCQSCDManagedOnBehalf' indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; And/or

— to indicate issuance to Legal Person:

— ‚QCForLegalPerson' meaning the identified certificates), when claimed or stated as qualified certificates), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚QCStatement' qualifier, or

— an ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚NotQualified' qualifier,

then the certificate is not to be considered as qualified.

‚Service digital identifiers' are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other ‚Sti' type entry is that, for that ‚Sti' identified service type, the listed service named according to the ‚Service name' field value and uniquely identified by the ‚Service digital identity' field value has the current qualified or approval status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'.

Specific interpretation rules for any additional information with regard to a listed service (e.g. ‚Service information extensions' field) may be found, when applicable, in the Member State specific URI as part of the present ‚Scheme type/community/rules' field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists."

2. URI špecifický pre dôveryhodný zoznam každého členského štátu odkazujúci na opisný text, ktorý je uplatniteľný na dôveryhodný zoznam daného členského štátu:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, kde CC = ISO 3166-1 ([1]) alpha-2 kód krajiny používaný v poli „Scheme territory" (odsek 5.3.10)

— Prostredníctvom tohto URI môžu používatelia získať prístup k osobitným politikám/pravidlám dotknutého členského štátu, podľa ktorých sa dôveryhodné služby na zozname posudzujú v súlade s režimom dohľadu daného členského štátu a v prípade potreby aj jeho schémou schvaľovania.

— Prostredníctvom tohto URI môžu používatelia získať prístup k osobitnému opisu členského štátu týkajúcemu sa toho, ako používať a vykladať obsah dôveryhodného zoznamu vzhľadom na uvedené nekvalifikované dôveryhodné služby a/alebo dôveryhodné služby definované na vnútroštátnej úrovni. Toto sa môže využiť na znázornenie možnej nesúrodosti vnútroštátneho systému schvaľovania súvisiaceho s poskytovateľmi certifikovaných služieb, ktorí nevydávajú kvalifikovaný certifikát, a na vysvetlenie, ako sa na tento účel používajú polia „Scheme service definition URI" (odsek 5.5.6) a „Service information extension" (odsek 5.5.9).

Členské štáty MÔŽU vymedziť a používať dodatočné URI, ktoré je rozšírením uvedeného URI špecifického pre daný členský štát (t. j. URI vymedzené na základe tohto hierarchického špecifického URI).

Politické/právne upozornenie TSL (TSL policy/legal notice) (odsek 5.3.11)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.3.11 normy TS 119 612, keď politické/právne upozornenie týkajúce sa právneho štatútu schémy alebo právnych požiadaviek, ktoré schéma spĺňa, na území, pod ktorého právomoc spadá, a/alebo obmedzenia a podmienky, za ktorých sa zoznam dôveryhodných informácií

([1]) ISO 3166-1:2006: „Kódy názvov krajín a ich častí – 1. časť: Kódy krajín".

o poskytovateľoch vedie a uverejňuje, je sekvencia viacjazyčných reťazcov znakov (pozri odsek 5.1.4) uvádzajúca povinne v britskej angličtine a nepovinne v jednom alebo viacerých národných jazykoch samotný text takejto politiky alebo upozornenia v nasledujúcej podobe:

1. Prvá, povinná časť, spoločná pre dôveryhodné zoznamy všetkých členských štátov, uvádza uplatniteľný právny rámec, ktorého anglické znenie je nasledovné:

   The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

   Znenie v národnom jazyku (národných jazykoch) členského štátu:

   Uplatniteľným právnym rámcom tohto dôveryhodného zoznamu je 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.

2. Druhá, nepovinná časť, špecifická pre každý dôveryhodný zoznam, s odkazmi na osobitné uplatniteľné vnútroštátne právne rámce.

Aktuálny štatút služby (Service current status) (odsek 5.5.4)

Toto pole je prítomné a je v súlade so špecifikáciami odseku 5.5.4 normy TS 119 612.

Migrácia hodnoty „Service current status“ pre služby uvedené v dôveryhodnom zozname VŠEÚ ku dňu predchádzajúcemu dátumu uplatňovania nariadenia (EÚ) č. 910/2014 (t. j. 30. júna 2016) sa vykoná v deň uplatňovania nariadenia (t. j. 1. júla 2016), ako sa uvádza v prílohe J k ETSI TS 119 612.

KAPITOLA III

KONTINUITA DÔVERYHODNÝCH ZOZNAMOV

Certifikáty, ktoré treba oznámiť Komisii v súlade s článkom 4 ods. 2 tohto rozhodnutia, musia spĺňať požiadavky odseku 5.7.1 ETSI TS 119 612 a musia byť vydané tak, aby:

— mali aspoň trojmesačný rozdiel v konečnom dátume platnosti („Not After“),

— boli vytvorené s novými pármi kľúčov. Páry kľúčov používané predtým sa nesmú opätovne certifikovať.

V prípade vypršania platnosti jedného z certifikátov verejného kľúča, ktorý by sa mohol použiť na validáciu podpisu alebo pečate v dôveryhodnom zozname a ktorý bol oznámený Komisii a uverejnený v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— v prípade, ak bol aktuálne uverejnený dôveryhodný zoznam podpísaný alebo zapečatený súkromným kľúčom, ktorého certifikát verejného kľúča stratil platnosť, znovu vydajú, a to bez zdržania, nový dôveryhodný zoznam podpísaný alebo zapečatený súkromným kľúčom, ktorého certifikát verejného kľúča nestratil platnosť,

— na požiadanie vygenerujú nové páry kľúčov, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu, a vygenerujú pre ne príslušné certifikáty verejného kľúča,

— okamžite oznámia Komisii nový zoznam certifikátov verejného kľúča zodpovedajúcich súkromným kľúčom, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu.

V prípade poškodenia alebo vyradenia jedného zo súkromných kľúčov zodpovedajúceho certifikátom verejného kľúča, ktorý by sa mohol použiť na validáciu podpisu alebo pečate v dôveryhodnom zozname a ktorý bol oznámený Komisii a uverejnený v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— znovu vydajú, a to bezodkladne, nový dôveryhodný zoznam podpísaný alebo zapečatený nepoškodeným súkromným kľúčom v prípade, ak bol uverejnený dôveryhodný zoznam podpísaný poškodeným alebo vyradeným súkromným kľúčom,

— na požiadanie vygenerujú nové páry kľúčov, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu, a vygenerujú pre ne príslušné certifikáty verejného kľúča,

— okamžite oznámia Komisii nový zoznam certifikátov verejného kľúča zodpovedajúcich súkromným kľúčom, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu.

V prípade poškodenia alebo vyradenia všetkých súkromných kľúčov zodpovedajúcich certifikátom verejných kľúčov, ktoré by sa mohli použiť na overenie podpisu v dôveryhodnom zozname a ktoré boli oznámené Komisii a uverejnené v centrálnych zoznamoch ukazovateľov Komisie, členské štáty:

— vygenerujú nové páry kľúčov, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu, a vygenerujú pre ne príslušné certifikáty verejného kľúča,

— znovu vydajú, a to bezodkladne, nový dôveryhodný zoznam podpísaný alebo zapečatený jedným z tých nových súkromných kľúčov, ktorých zodpovedajúci certifikát s verejným kľúčom sa má oznámiť,

— okamžite oznámia Komisii nový zoznam certifikátov verejného kľúča zodpovedajúcich súkromným kľúčom, ktoré by sa mohli použiť na podpísanie alebo zapečatenie dôveryhodného zoznamu.

KAPITOLA IV

ŠPECIFIKÁCIE FORMY DÔVERYHODNÉHO ZOZNAMU ČITATEĽNEJ ĽUDSKÝM OKOM

Ak sa stanoví a uverejní forma dôveryhodného zoznamu čitateľná ľudským okom, poskytne sa vo formáte dokumentu PDF podľa ISO 32000 ([1]), ktorý sa naformátuje podľa profilu PDF/A (ISO 19005 ([2])).

Obsah formy dôveryhodného zoznamu čitateľnej ľudským okom vo formáte PDF/A musí spĺňať tieto požiadavky:

— v štruktúre formy čitateľnej ľudským okom by sa mal odrážať logický model opísaný v norme TS 119 612,

— každé zahrnuté pole je zobrazené a uvádza:

  — názov poľa (napríklad „*Service type identifier*“),

  — hodnotu poľa (napríklad „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“),

  — v prípade potreby význam (opis) hodnoty poľa, (napr. „*Služba na vydávanie certifikátov, ktorá vytvára a podpisuje kvalifikované certifikáty na základe identity a ostatných atribútov overených príslušnými registračnými službami*.“),

  — v prípade potreby viacero jazykových verzií, ako sa stanovuje v dôveryhodnom zozname.

— Na forme čitateľnej ľudským okom sa uvedú minimálne tieto polia a zodpovedajúce hodnoty digitálnych certifikátov ([3]), ak sú uvedené v poli „Service digital identity“:

  — Verzia,

  — Sériové číslo certifikátu,

  — Algoritmus podpisu,

  — Vydavateľ – všetky dôležité rozlíšiteľné názvové polia,

  — Doba platnosti,

  — Subjekt – všetky dôležité rozlíšiteľné názvové polia,

([1]) ISO 32000-1:2008: Správa dokumentov – PDF (Portable document format) – 1. časť: PDF 1.7.
([2]) ISO 19005-2:2011: Správa dokumentov – Formát pre dlhodobú archiváciu elektronických textových dokumentov – 2. časť: Používanie normy ISO 32000-1 (PDF/A-2).
([3]) Odporúčanie ITU-T X.509 | ISO/IEC 9594-8: Informačné technológie – prepojenia otvorených systémov – adresár: Certifikačné rámce verejného kľúča a atribútu (pozri http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Verejný kľúč,

— Identifikátor kľúča orgánu,

— Identifikátor kľúča subjektu,

— Používanie kľúča,

— Rozšírené používanie kľúča,

— Certifikačné politiky – všetky identifikátory a kvalifikátory politiky,

— Mapovanie politiky,

— Alternatívny názov subjektu,

— Vlastnosti adresára subjektu,

— Základné obmedzenia,

— Politické obmedzenia,

— Distribučné body CRL ([1]),

— Prístup k informáciám pre orgán,

— Prístup k informáciám pre subjekt,

— Vyhlásenia kvalifikovaného certifikátu ([2]),

— Hašovací algoritmus,

— Hašovacia hodnota certifikátu.

— Forma čitateľná ľudským okom sa musí dať ľahko vytlačiť.

— Formu čitateľnú ľudským okom podpíše alebo zapečatí prevádzkovateľ schémy podľa zdokonalených podpisov PDF vymedzených v článkoch 1 a 3 vykonávacieho rozhodnutia Komisie (EÚ) 2015/1505.

([1]) RFC 5280: Profil certifikátu Internet X.509 PKI a profil CRL.
([2]) RFC 3739: Internet X.509 PKI: Profil kvalifikovaného certifikátu.

PRÍLOHA II

VZOR OZNÁMENÍ ČLENSKÝCH ŠTÁTOV

Informácie, ktoré majú členské štáty oznamovať podľa článku 4 ods. 1 predmetného rozhodnutia obsahujú tieto údaje a akékoľvek ich zmeny:

1. Členský štát, s použitím kódu ISO 3166-1 ([1]) alpha-2 s týmito výnimkami:

   a) Kódom krajiny pre Spojené kráľovstvo je „UK".

   b) Kódom krajiny pre Grécko je „EL".

2. Orgán(-y) zodpovedný(-é) za zostavenie, vedenie a uverejňovanie formy dôveryhodných zoznamov vhodnej na automatizované spracovanie a formy dôveryhodných zoznamov čitateľnej ľudským okom:

   a) Meno prevádzkovateľa schémy: poskytnutá informácia sa musí zhodovať – rozlišujú sa veľké a malé písmená – s menom prevádzkovateľa schémy („Scheme operator name") v zozname dôveryhodných informácií vo všetkých jazykoch, ktoré sa v ňom používajú.

   b) Nepovinné údaje iba na vnútorné účely Komisie v prípadoch, keď je potrebné kontaktovať príslušný orgán (v zozname dôveryhodných zoznamov, ktorý zostavila EK, nebudú tieto informácie uverejnené):

      — adresa prevádzkovateľa schémy;

      — kontaktné údaje o zodpovednej(-ých) osobe(-ách) (meno, telefón, emailová adresa).

3. Lokalita, kde je uverejnený dôveryhodný zoznam vo forme vhodnej na automatizované spracovanie (*lokalita, kde je uverejnený v súčasnosti platný dôveryhodný zoznam*).

4. V prípade potreby lokalita, kde je uverejnený dôveryhodný zoznam vo forme čitateľnej ľudským okom (*lokalita, kde je uverejnený v súčasnosti platný dôveryhodný zoznam*). Ak dôveryhodný zoznam vo forme čitateľnej ľudským okom už nie je uverejnený, je potrebné túto skutočnosť uviesť.

5. Certifikáty verejného kľúča zodpovedajúce súkromným kľúčom, ktoré sa môžu používať na elektronické podpísanie alebo zapečatenie formy dôveryhodných zoznamov vhodnej na automatizované spracovanie a formy dôveryhodných zoznamov čitateľnej ľudským okom: tieto certifikáty sa predkladajú ako certifikáty DER kódované vo formáte Privacy Enhanced Mail Base64. Pri oznamovaní zmeny sa uvedú dodatočné informácie v prípade, keď je v zozname Komisie potrebné nahradiť osobitný certifikát novým certifikátom, a v prípade, keď je k existujúcemu certifikátu alebo certifikátom potrebné pridať oznámený certifikát bez akejkoľvek náhrady.

6. Dátum predloženia údajov oznamovaných v bodoch 1 až 5.

Údaje oznámené podľa bodu 1, bodu 2 písm. a) a bodov 3, 4 a 5 sa musia pridať do zoznamu dôveryhodných zoznamov, ktorý zostavuje EK, namiesto predtým oznámených informácií v uvedenom zozname.

([1]) ISO 3166-1: „Kódy názvov krajín a ich častí – 1. časť: Kódy krajín".

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2015/1506

z 8. septembra 2015,

ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 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 články 27 ods. 5 a 37 ods. 5,

keďže:

(1) Členské štáty musia zaviesť potrebné technické prostriedky, ktoré im umožnia spracúvať elektronicky podpísané dokumenty, ktoré sa vyžadujú pri používaní služieb online ponúkaných prostredníctvom alebo v mene subjektu verejného sektora.

(2) Nariadením (EÚ) č. 910/2014 sa členským štátom, ktoré pri používaní služieb online ponúkaných prostredníctvom alebo v mene subjektu verejného sektora vyžadujú zdokonalený elektronický podpis alebo pečať, ukladá povinnosť uznať zdokonalené elektronické podpisy a pečate, zdokonalené elektronické podpisy a pečate založené na kvalifikovanom certifikáte a kvalifikované elektronické podpisy a pečate v konkrétnych formátoch, alebo alternatívne formáty validované podľa konkrétnych referenčných metód.

(3) Pri vymedzení konkrétnych formátov a referenčných metód by sa mali zohľadniť existujúca prax, normy a právne akty Únie.

(4) Vykonávacím rozhodnutím Komisie 2014/148/EÚ ([2]) sa vymedzilo niekoľko najbežnejších formátov zdokonalených elektronických podpisov, ktoré sa majú technicky podporovať v členských štátoch, kde sa pri administratívnych postupoch online vyžadujú zdokonalené elektronické podpisy. Cieľom zavedenia referenčných formátov je uľahčenie cezhraničnej validácie elektronických podpisov a zlepšenie cezhraničnej interoperability elektronických postupov.

(5) Normy uvedené v prílohe k tomuto rozhodnutiu sú existujúcimi normami pre formáty zdokonalených elektronických podpisov. Vzhľadom na prebiehajúcu revíziu dlhodobých foriem archivovania referenčných formátov, ktorú realizujú normalizačné orgány, sú normy týkajúce sa dlhodobej archivácie vylúčené z rozsahu pôsobnosti tohto rozhodnutia. Keď bude k dispozícii nová verzia referenčných noriem, odkazy na normy a ustanovenia o dlhodobej archivácii sa budú revidovať.

(6) Zdokonalené elektronické podpisy a zdokonalené elektronické pečate sú z technického hľadiska podobné. Preto by sa mali normy upravujúce formáty zdokonalených elektronických podpisov primerane uplatňovať aj na formáty zdokonalených elektronických pečatí.

(7) Ak sa na podpis alebo zapečatenie používajú iné než bežne podporované formáty elektronických podpisov alebo pečatí, je potrebné poskytnúť validačné prostriedky, ktoré umožnia overiť elektronické podpisy alebo pečate cez hranice. S cieľom umožniť, aby sa prijímajúce členské štáty mohli spoľahnúť na uvedené validačné nástroje iného členského štátu, je nevyhnutné poskytnúť ľahko dostupné informácie týkajúce sa týchto validačných nástrojov, a to tým, že sa tieto informácie uvedú v elektronických dokumentoch, v elektronických podpisoch alebo v nosičoch elektronických dokumentov.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73.

([2]) Vykonávacie rozhodnutie Komisie 2014/148/EÚ zo 17. marca 2014, ktorým sa mení rozhodnutie 2011/130/EÚ, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu (Ú. v. EÚ L 80, 19.3.2014, s. 7).

(8) Ak sú možnosti validácie elektronického podpisu alebo pečate vhodné na automatizované spracovanie dostupné vo verejných službách niektorého členského štátu, takéto možnosti validácie by mali byť sprístupnené a poskytnuté aj prijímajúcemu členskému štátu. Napriek tomu by toto rozhodnutie nemalo brániť uplatneniu článku 27 ods. 1 a 2 a článku 37 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, ak takéto automatizované spracovanie možností validácie pre alternatívne metódy nie je možné.

(9) S cieľom zabezpečiť porovnateľné požiadavky na validáciu a zvýšiť dôveru v možnosti validácie, ktoré poskytujú členské štáty pre iné než bežne podporované formáty elektronických podpisov alebo pečatí, vychádzajú požiadavky na nástroje validácie stanovené v tomto rozhodnutí z požiadaviek na validáciu kvalifikovaných elektronických podpisov a pečatí uvedených v článkoch 32 a 40 nariadenia (EÚ) č. 910/2014.

(10) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru, ktorý bol uvedený v článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Členské štáty vyžadujúce zdokonalený elektronický podpis alebo zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, ako sa ustanovuje v článku 27 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, uznajú zdokonalený elektronický podpis XML, CMS alebo PDF na úrovni súladu B, T alebo LT alebo použitie podpisového kontajnera vo formáte ASiC, ak sú tieto podpisy v súlade s technickými špecifikáciami uvedenými v prílohe.

Článok 2

1. Členské štáty vyžadujúce zdokonalený elektronický podpis alebo zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, ako sa ustanovuje v článku 27 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, uznajú iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 tohto rozhodnutia, za predpokladu, že členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkne iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie.

2. Možnosti validácie podpisu musia:

a) umožňovať ostatným členským štátom validovať prijaté elektronické podpisy online, bezplatne a spôsobom, ktorý je zrozumiteľný pre cudzincov;

b) byť uvedené v podpísanom dokumente, v elektronickom podpise alebo na nosiči elektronických dokumentov; a

c) potvrdzovať platnosť elektronického podpisu za predpokladu, že:

1. certifikát, ktorý podporuje zdokonalený elektronický podpis, bol v čase podpísania platný, a ak je zdokonalený elektronický podpis podporovaný kvalifikovaným certifikátom, kvalifikovaný certifikát, ktorý podporuje zdokonalený elektronický podpis, bol v čase podpísania kvalifikovaným certifikátom elektronického podpisu v súlade s prílohou I k nariadeniu (EÚ) č. 910/2014 a bol vydaný kvalifikovaným poskytovateľom dôveryhodných služieb;

2. údaje na validáciu podpisu zodpovedajú údajom poskytnutým spoliehajúcej sa strane;

3. sa jedinečný súbor údajov reprezentujúcich podpisovateľa správne poskytol spoliehajúcej sa strane;

4. sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase podpísania použil pseudonym;

5. ak je zdokonalený elektronický podpis vytvorený pomocou zariadenia na vytvorenie kvalifikovaného elektronického podpisu, použitie každého takého zariadenia sa jasne oznámilo spoliehajúcej sa strane;

6. neporušenosť podpísaných údajov nebola skompromitovaná;

7. v čase podpísania boli dodržané požiadavky stanovené v článku 26 nariadenia (EÚ) č. 910/2014;

8. systém použitý na validáciu zdokonaleného elektronického podpisu poskytuje spoliehajúcej sa strane správny výsledok procesu validácie a umožňuje spoliehajúcej sa strane odhaliť akékoľvek problémy súvisiace s bezpečnosťou.

Článok 3

Členské štáty vyžadujúce zdokonalenú elektronickú pečať alebo zdokonalenú elektronickú pečať založenú na kvalifikovanom certifikáte, ako sa ustanovuje v článku 37 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, uznajú zdokonalenú elektronickú pečať XML, CMS alebo PDF na úrovni súladu B, T alebo LT alebo použitie pečaťového kontajnera vo formáte ASiC, ak sú tieto pečate v súlade s technickými špecifikáciami uvedenými v prílohe.

Článok 4

1. Členské štáty vyžadujúce zdokonalenú elektronickú pečať alebo zdokonalenú elektronickú pečať založenú na kvalifikovanom certifikáte, ako sa ustanovuje v článku 37 ods. 1 a 2 nariadenia (EÚ) č. 910/2014, uznajú iné formáty elektronických pečatí než tie, ktoré sú uvedené v článku 3 tohto rozhodnutia, za predpokladu, že členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný pôvodcom pečate, ponúkne iným členským štátom možnosti validácie pečate, ktoré budú podľa možnosti vhodné na automatizované spracovanie.

2. Možnosti validácie pečate musia:

a) umožniť ostatným členským štátom validovať prijaté elektronické pečate online, bezplatne a spôsobom, ktorý je zrozumiteľný pre cudzincov;

b) byť uvedené v zapečatenom dokumente, v elektronickej pečati alebo na nosiči elektronických dokumentov;

c) potvrdzovať platnosť elektronickej pečate, za predpokladu, že:

1. certifikát, ktorý podporuje zdokonalenú elektronickú pečať, bol v čase zapečatenia platný, a ak je zdokonalená elektronická pečať podporovaná kvalifikovaným certifikátom, kvalifikovaný certifikát, ktorý podporuje zdokonalenú elektronickú pečať, bol v čase zapečatenia kvalifikovaným certifikátom elektronickej pečate v súlade s prílohou III k nariadeniu (EÚ) č. 910/2014 a bol vydaný kvalifikovaným poskytovateľom dôveryhodných služieb;

2. údaje na validáciu pečate zodpovedajú údajom poskytnutým spoliehajúcej sa strane;

3. sa jedinečný súbor údajov reprezentujúcich pôvodcu pečate správne poskytol spoliehajúcej sa strane;

4. sa použitie pseudonymu jasne oznámilo spoliehajúcej sa strane v prípade, že sa v čase zapečatenia použil pseudonym;

5. ak je zdokonalená elektronická pečať vytvorená pomocou zariadenia na vytvorenie kvalifikovanej elektronickej pečate, použitie takých zariadení sa jasne oznámilo spoliehajúcej sa strane;

6. neporušenosť zapečatených údajov nebola skompromitovaná;

7. v čase zapečatenia boli dodržané požiadavky stanovené v článku 36 nariadenia (EÚ) č. 910/2014;

8. systém použitý na validáciu zdokonalenej elektronickej pečate poskytuje spoliehajúcej sa strane správny výsledok procesu validácie a umožňuje spoliehajúcej sa strane odhaliť akékoľvek problémy súvisiace s bezpečnosťou.

Článok 5

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

Toto rozhodnutie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. septembra 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA

Zoznam technických špecifikácií pre zdokonalené elektronické podpisy XML, CMS alebo PDF a pre podpisový kontajner vo formáte ASiC

Zdokonalené elektronické podpisy uvedené v článku 1 rozhodnutia musia byť v súlade s jednou z týchto technických špecifikácií ETSI, s výnimkou ich časti 9:

Základný profil XAdES	ETSI TS 103171 v.2.1.1 ([1])
Základný profil CAdES	ETSI TS 103173 v.2.2.1 ([2])
Základný profil PAdES	ETSI TS 103172 v.2.2.2 ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf.
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.

Podpisový kontajner uvedený v článku 1 rozhodnutia musí byť v súlade s týmito technickými špecifikáciami ETSI:

Základný profil podpisového kontajnera vo formáte ASiC	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf.

Zoznam technických špecifikácií pre zdokonalené elektronické pečate XML, CMS alebo PDF a pre pečaťový kontajner vo formáte ASiC

Zdokonalené elektronické pečate uvedené v článku 3 rozhodnutia musia byť v súlade s jednou z týchto technických špecifikácií ETSI, s výnimkou ich časti 9:

Základný profil XAdES	ETSI TS 103171 v.2.1.1
Základný profil CAdES	ETSI TS 103173 v.2.2.1
Základný profil PAdES	ETSI TS 103172 v.2.2.2

Pečaťový kontajner uvedený v článku 3 rozhodnutia musí byť v súlade s týmito technickými špecifikáciami ETSI:

Základný profil pečaťového kontajnera vo formáte ASiC	ETSI TS 103174 v.2.2.1

ISSN 1977-0790 (elektronické vydanie)
ISSN 1725-5147 (papierové vydanie)

Úrad pre vydávanie publikácií Európskej únie
2985 Luxemburg
LUXEMBURSKO

SK