Uradni list Evropske unije

L 235

Zvezek 58

Slovenska izdaja

Zakonodaja

9. september 2015

Vsebina

II *Nezakonodajni akti*

UREDBE

★ **Izvedbena uredba Komisije (EU) 2015/1501 z dne 8. septembra 2015 o interoperabilnostnem okviru v skladu s členom 12(8) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu** [1] 1

★ **Izvedbena uredba Komisije (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu** [1] 7

Izvedbena uredba Komisije (EU) 2015/1503 z dne 8. septembra 2015 o določitvi standardnih uvoznih vrednosti za določitev uvozne cene za nekatere vrste sadja in zelenjave 21

SKLEPI

★ **Izvedbeni sklep Komisije (EU) 2015/1504 z dne 7. septembra 2015 o odobritvi odstopanj nekaterim državam članicam glede zagotavljanja statističnih podatkov v skladu z Uredbo (ES) št. 1099/2008 Evropskega parlamenta in Sveta o statistiki energetike** *(notificirano pod dokumentarno številko C(2015) 6105)* [1] 24

★ **Izvedbeni sklep Komisije (EU) 2015/1505 z dne 8. septembra 2015 o določitvi tehničnih specifikacij in formatov v zvezi z zanesljivimi seznami v skladu s členom 22(5) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu** [1] 26

[1] Besedilo velja za EGP

SL

★ **Izvedbeni sklep Komisije (EU) 2015/1506 z dne 8. septembra 2015 o določitvi specifikacij v zvezi s formati naprednih elektronskih podpisov in naprednih elektronskih žigov, ki jih priznajo organi javnega sektorja v skladu s členoma 27(5) in 37(5) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu** [1] 37

[1] Besedilo velja za EGP

II

(Nezakonodajni akti)

UREDBE

IZVEDBENA UREDBA KOMISIJE (EU) 2015/1501

z dne 8. septembra 2015

o interoperabilnostnem okviru v skladu s členom 12(8) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 12(8) Uredbe,

ob upoštevanju naslednjega:

(1) Člen 12(2) Uredbe (EU) št. 910/2014 določa, da bi bilo za interoperabilnost nacionalnih shem elektronske identifikacije, priglašene v skladu s členom 9(1) navedene uredbe, treba vzpostaviti interoperabilnostni okvir.

(2) Vozlišča imajo osrednjo vlogo pri medomrežnem povezovanju shem elektronske identifikacije držav članic. Njihov prispevek je pojasnjen v dokumentaciji v zvezi z instrumentom za povezovanje Evrope, vzpostavljenim z Uredbo (EU) št. 1316/2013 Evropskega parlamenta in Sveta ([2]), vključno s funkcijami in sestavnimi deli „vozlišča eIDAS“.

(3) Kadar država članica ali Komisija zagotavlja programsko opremo, s katero vozlišču, ki deluje v drugi državi članici, omogoča avtentikacijo, se lahko stranka, ki dobavlja in posodablja programsko opremo, ki se uporablja za mehanizem avtentikacije, s stranko gostiteljico programske opreme dogovori o načinu upravljanja izvajanja mehanizma avtentikacije. Tak dogovor stranki gostiteljici ne bi smel povzročiti nesorazmernih tehničnih zahtev ali stroškov (vključno s podporo, odgovornostmi, gostovanjem in drugimi stroški).

(4) Če izvajanje interoperabilnostnega okvira to upravičuje, lahko Komisija v sodelovanju z državami članicami razvije dodatne tehnične specifikacije s podrobnostmi o tehničnih zahtevah, kot so določene v tej uredbi, zlasti ob upoštevanju mnenj mreže za sodelovanje iz člena 14(d) Izvedbene uredbe Komisije (EU) 2015/296 ([3]). Take tehnične specifikacije bi morale biti razvite kot del infrastrukture za digitalne storitve iz Uredbe (EU) št. 1316/2013, ki določa sredstva za praktično izvajanje gradnika za elektronsko identifikacijo.

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

([2]) Uredba (EU) št. 1316/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o vzpostavitvi Instrumenta za povezovanje Evrope, spremembi Uredbe (EU) št. 913/2010 in razveljavitvi uredb (ES) št. 680/2007 in (ES) št. 67/2010 (UL L 348, 20.12.2013, str. 129).

([3]) Izvedbeni sklep Komisije (EU) 2015/296 z dne 24. februarja 2015 o določitvi postopkovne ureditve za sodelovanje med državami članicami na področju elektronske identifikacije v skladu s členom 12(7) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (UL L 53, 25.2.2015, str. 14).

(5) Tehnične zahteve iz te uredbe bi bilo treba uporabljati ne glede na morebitne spremembe tehničnih specifikacij, ki bi bile lahko razvite v skladu s členom 12 te uredbe.

(6) Obsežni pilotni projekt STORK, vključno s specifikacijami, ki so bile razvite v njegovem okviru, načela in koncepti evropskega interoperabilnostnega okvira za evropske javne storitve so bili dosledno upoštevani pri oblikovanju ureditve interoperabilnostnega okvira iz te uredbe.

(7) Rezultati sodelovanja med državami članicami so bili dosledno upoštevani.

(8) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predmet urejanja

Ta uredba določa tehnične in operativne zahteve za interoperabilnostni okvir, s katerimi se zagotovi interoperabilnost shem elektronske identifikacije, ki jih države članice priglasijo Komisiji.

Navedene zahteve zlasti vključujejo:

(a) minimalne tehnične zahteve, povezane z ravnmi zanesljivosti in določitvijo nacionalnih ravni zanesljivosti priglašenih sredstev elektronske identifikacije, izdanih na podlagi priglašenih shem elektronske identifikacije na podlagi člena 8 Uredbe (EU) št. 910/2014, kot je določeno v členih 3 in 4;

(b) minimalne tehnične zahteve glede interoperabilnosti v skladu s členoma 5 in 8;

(c) minimalni niz identifikacijskih podatkov osebe, ki enolično predstavljajo fizično ali pravno osebo v skladu s členom 11 in Prilogo;

(d) skupne varnostne standarde delovanja v skladu s členi 6, 7, 9 in 10;

(e) ureditev za reševanje sporov v skladu s členom 13.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

1. „vozlišče“ pomeni priključno točko, ki je del interoperabilnostne arhitekture za elektronsko identifikacijo in se vključuje v postopke čezmejne avtentikacije oseb ter lahko prepozna in obdeluje ali posreduje podatke drugim vozliščem, tako da nacionalni infrastrukturi za elektronsko identifikacijo ene države članice omogoča, da se prek vmesnika poveže z nacionalno infrastrukturo za elektronsko identifikacijo drugih držav članic;

2. „operater vozlišča“ pomeni subjekt, ki je odgovoren za zagotavljanje, da vozlišče kot priključno mesto svoje funkcije opravlja pravilno in zanesljivo.

Člen 3

Minimalne tehnične zahteve, povezane z ravnimi zanesljivosti

Minimalne tehnične zahteve, povezane z ravnmi zanesljivosti, so določene v Izvedbeni uredbi Komisije (EU) 2015/1502 ([1]).

Člen 4

Določitev nacionalnih ravni zanesljivosti

Določitev nacionalnih ravni zanesljivosti priglašenih shem elektronske identifikacije izpolnjuje zahteve iz Izvedbene uredbe (EU) 2015/1502. Rezultati določitve bodo uradno sporočeni Komisiji z uporabo predloge za uradno obveščanje iz Izvedbenega sklepa Komisije (EU) 2015/1505 ([2]).

Člen 5

Vozlišča

1. Vozlišče v eni državi članici se lahko poveže z vozlišči drugih držav članic.

2. Vozlišča imajo sposobnost, da s tehničnimi sredstvi razlikujejo med organi javnega sektorja in drugimi zanašajočimi se strankami.

3. Izvajanje tehničnih zahtev iz te uredbe v posamezni državi članici drugim državam članicam ne povzroča nesorazmernih tehničnih zahtev in stroškov zaradi sodelovanja pri izvajanju interoperabilnosti, ki jo je sprejela prva država članica.

Člen 6

Zasebnost in zaupnost podatkov

1. Varstvo zasebnosti in zaupnosti izmenjanih podatkov ter ohranjanje celovitosti podatkov med vozlišči se zagotavlja z uporabo najboljših razpoložljivih tehničnih rešitev in varstvenih postopkov.

2. Vozlišča ne hranijo osebnih podatkov, razen za namene iz člena 9(3).

Člen 7

Celovitost in avtentičnost podatkov pri prenosu

Pri prenosu podatkov med vozlišči se zagotavljata celovitost in avtentičnost podatkov, s čimer se zagotovi, da so vsi zahtevki in odgovori avtentični ter da se vanje ni nepooblaščeno posegalo. Za ta namen vozlišča uporabljajo rešitve, ki so bile uspešno uporabljene pri čezmejni operativni uporabi.

([1]) Izvedbena uredba Komisije (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (glej stran 7 tega Uradnega lista).

([2]) Izvedbeni sklep Komisije (EU) 2015/1505 z dne 8. septembra 2015 o določitvi tehničnih specifikacij in formatov v zvezi z zanesljivimi seznami v skladu s členom 22(5) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (glej stran 26 tega Uradnega lista).

Člen 8

Format sporočila za prenos podatkov

Vozlišča za sintakso uporabljajo skupne formate sporočil, ki temeljijo na standardih, ki so jih države članice že večkrat uporabile in dokazano delujejo v okolju izvajanja. Sintaksa omogoča:

(a) pravilno obdelavo minimalnega niza identifikacijskih podatkov osebe, ki enolično predstavljajo fizično ali pravno osebo;

(b) pravilno obdelavo ravni zanesljivosti sredstva za elektronsko identifikacijo;

(c) razlikovanje med organi javnega sektorja in drugimi zanašajočimi se strankami;

(d) prožnost v primeru potreb po dodatnih značilnostih v zvezi z identifikacijo.

Člen 9

Upravljanje zaupnih podatkov in metapodatkov

1. Operater vozlišča sporoči metapodatke o upravljanju vozlišča v standardizirani obliki, primerni za strojno obdelavo, na varen in zaupanja vreden način.

2. Najmanj parametri v zvezi z varnostjo se prikličejo samodejno.

3. Operater vozlišča hrani podatke, s katerimi se v primeru incidenta lahko rekonstruira zaporedje izmenjanih sporočil, da se ugotovi kraj in narava incidenta. Podatki se hranijo v časovnem obdobju, ki je v skladu z nacionalnimi zahtevami, in vsebujejo najmanj naslednje elemente:

(a) identifikacijo vozlišča;

(b) identifikacijo sporočila;

(c) datum in uro sporočila.

Člen 10

Informacijska varnost in varnostni standardi

1. Operaterji vozlišč, ki zagotavljajo avtentikacijo, na podlagi izdajanja potrdil ali enakovrednih metod ocenjevanja ali usklajenosti z nacionalno zakonodajo dokažejo, da vozlišče izpolnjuje zahteve standarda ISO/IEC 27001 glede na vozlišča, ki sodelujejo v interoperabilnostnem okviru.

2. Operaterji vozlišč brez nepotrebnega odlašanja izvajajo nujne varnostne posodobitve.

Člen 11

Identifikacijski podatki osebe

1. Kadar se uporablja čezmejno, minimalni niz identifikacijskih podatkov osebe, ki enolično predstavljajo fizično ali pravno osebo, izpolnjuje zahteve iz Priloge.

2. Kadar se uporablja čezmejno, minimalni podatkovni niz za fizično osebo, ki zastopa pravno osebo, vsebuje kombinacijo značilnosti iz Priloge za fizične in pravne osebe.

3. Podatki se prenašajo na podlagi prvotnih znakov in se, kadar je to ustrezno, tudi prečrkujejo v latinico.

Člen 12

Tehnične specifikacije

1. Kadar postopek izvajanja interoperabilnostnega okvira to upravičuje, lahko mreža za sodelovanje, vzpostavljena z Izvedbenim sklepom (EU) 2015/296, v skladu s členom 14(d) Izvedbenega sklepa sprejema mnenja v zvezi s potrebo po razvoju tehničnih specifikacij. Take tehnične specifikacije določajo dodatne podrobnosti glede tehničnih zahtev iz te uredbe.

2. V skladu z mnenjem iz odstavka 1 Komisija v sodelovanju z državami članicami razvije tehnične specifikacije kot del infrastrukture za digitalne storitve iz Uredbe (EU) št. 1316/2013.

3. Mreža za sodelovanje sprejme mnenje v skladu s členom 14(d) Izvedbenega sklepa (EU) 2015/296, v katerem oceni, ali in v kolikšni meri tehnične specifikacije, razvite na podlagi odstavka 2, ustrezajo ugotovljeni potrebi v mnenju iz odstavka 1 ali zahtevam iz te uredbe. Državam članicam lahko priporoči, da upoštevajo tehnične specifikacije pri izvajanju interoperabilnostnega okvira.

4. Komisija zagotavlja referenčno izvajanje kot primer razlage tehničnih specifikacij. Države članice lahko to referenčno izvajanje uporabijo ali pa ga uporabljajo kot predlogo za preskušanje drugih izvajanj tehničnih specifikacij.

Člen 13

Reševanje sporov

1. Kadar je to mogoče, zadevne države članice kakršne koli spore v zvezi z interoperabilnostnim okvirom rešujejo s pogajanji.

2. Če ni dosežena rešitev v skladu z odstavkom 1, je za reševanje spora v skladu s svojim poslovnikom pristojna mreža za sodelovanje, vzpostavljena v skladu s členom 12 Izvedbenega sklepa (EU) 2015/296.

Člen 14

Začetek veljavnosti

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

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo

Predsednik

Jean-Claude JUNCKER

PRILOGA

Zahteve v zvezi z minimalnim nizom identifikacijskih podatkov osebe, ki enolično predstavljajo fizično ali pravno osebo iz člena 11

1. **Minimalni podatkovni niz za fizično osebo**

Minimalni podatkovni niz za fizično osebo vsebuje vse naslednje obvezne značilnosti:

(a) sedanji priimek;

(b) sedanje ime;

(c) datum rojstva;

(d) enolični identifikator, ki ga je ustvarila država članica pošiljateljica v skladu s tehničnimi specifikacijami za namene čezmejne identifikacije in je časovno čim bolj obstojen.

Minimalni podatkovni niz za fizično osebo vsebuje eno ali več naslednjih dodatnih značilnosti:

(a) ime in priimek ob rojstvu;

(b) kraj rojstva;

(c) sedanji naslov;

(d) spol.

2. **Minimalni podatkovni niz za pravno osebo**

Minimalni podatkovni niz za pravno osebo vsebuje vse naslednje obvezne značilnosti:

(a) sedanje pravno ime;

(b) enolični identifikator, ki ga je ustvarila država članica pošiljateljica v skladu s tehničnimi specifikacijami za namene čezmejne identifikacije in je časovno čim bolj obstojen.

Minimalni podatkovni niz za pravno osebo vsebuje eno ali več naslednjih dodatnih značilnosti:

(a) sedanji naslov;

(b) identifikacijsko številko za DDV;

(c) davčno sklicno številko;

(d) identifikator iz člena 3(1) Direktive 2009/101/ES Evropskega parlamenta in Sveta ([1]);

(e) identifikator pravnega subjekta iz Izvedbene uredbe Komisije (EU) št. 1247/2012 ([2]);

(f) registracijsko identifikacijsko številko gospodarskega subjekta (številko EORI) iz Izvedbene uredbe Komisije (EU) št. 1352/2013 ([3]);

(g) trošarinsko številko iz člena 2(12) Uredbe Sveta (EU) št. 389/2012 ([4]).

([1]) Direktiva 2009/101/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o uskladitvi zaščitnih ukrepov za varovanje interesov družbenikov in tretjih oseb, ki jih države članice zahtevajo od gospodarskih družb v skladu z drugim pododstavkom člena 48 Pogodbe, zato da se oblikujejo zaščitni ukrepi z enakim učinkom v vsej Skupnosti (UL L 258, 1.10.2009, str. 11).

([2]) Izvedbena uredba Komisije (EU) št. 1247/2012 z dne 19. decembra 2012 o izvedbenih tehničnih standardih glede oblike in pogostosti poročanja o trgovanju repozitorijem sklenjenih poslov v skladu z Uredbo (EU) št. 648/2012 Evropskega parlamenta in Sveta o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 352, 21.12.2012, str. 20).

([3]) Izvedbena uredba Komisije (EU) št. 1352/2013 z dne 4. decembra 2013 o določitvi obrazcev iz Uredbe (EU) št. 608/2013 Evropskega parlamenta in Sveta o uveljavljanju pravic intelektualne lastnine s strani carinskih organov (UL L 341, 18.12.2013, str. 10).

([4]) Uredba Sveta (EU) št. 389/2012 z dne 2. maja 2012 o upravnem sodelovanju na področju trošarin in o razveljavitvi Uredbe (ES) št. 2073/2004 (UL L 121, 8.5.2012, str. 1).

IZVEDBENA UREDBA KOMISIJE (EU) 2015/1502

z dne 8. septembra 2015

o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 8(3) Uredbe,

ob upoštevanju naslednjega:

(1) Člen 8 Uredbe (EU) št. 910/2014 določa, da mora shema elektronske identifikacije, priglašena v skladu s členom 9(1), določati nizko, srednjo in visoko raven zanesljivosti, dodeljeno sredstvom elektronske identifikacije, izdanim v okviru navedene sheme.

(2) Določitev minimalnih tehničnih specifikacij, standardov in postopkov je bistvena, da se zagotovita skupno razumevanje podrobnih podatkov o ravneh zanesljivosti in interoperabilnost, kadar se določajo nacionalne ravni zanesljivosti priglašenih shem elektronske identifikacije glede na ravni zanesljivosti iz člena 8, kakor določa člen 12(4)(b) Uredbe (EU) št. 910/2014.

(3) Mednarodni standard ISO/IEC 29115 je bil upoštevan kot glavni razpoložljivi mednarodni standard na področju ravni zanesljivosti za sredstva elektronske identifikacije za specifikacije in postopke iz tega izvedbenega akta. Vendar pa se vsebina Uredbe (EU) št. 910/2014 razlikuje od navedenega mednarodnega standarda, zlasti v zvezi z zahtevami glede dokazovanja in preverjanja identitete ter načina, kako se upoštevajo razlike med ureditvijo identitete v državah članicah in obstoječimi instrumenti EU za isti namen. Zato se Priloga kljub opiranju na ta mednarodni standard ne bi smela sklicevati na katero koli posebno vsebino ISO/IEC 29115.

(4) Podlaga za pripravo te uredbe je bil na rezultatih temelječi pristop, ki se je izkazal za najprimernejši, kar se odraža tudi v opredelitvah, ki se uporabljajo za podrobno določanje terminov in pojmov. V njih se upošteva cilj Uredbe (EU) št. 910/2014 glede ravni zanesljivosti sredstev elektronske identifikacije. Zato bi bilo treba pri pripravi specifikacij in postopkov iz tega izvedbenega akta dosledno upoštevati obsežni pilotni projekt STORK, vključno s specifikacijami, ki so bile razvite v njegovem okviru, in opredelitve ter pojme iz ISO/IEC 29115.

(5) Verodostojni viri so lahko glede na okoliščine, v katerih je treba preveriti vidik dokazila o identiteti, v številnih oblikah, kot so med drugim registri, dokumenti in organi. V različnih državah članicah se verodostojni viri lahko razlikujejo celo v podobnih okoliščinah.

(6) Zahteve za dokazovanje in preverjanje identitete bi morale upoštevati različne sisteme in prakse ter hkrati zagotavljati dovolj visoko zanesljivost, da se vzpostavi potrebno zaupanje. Zato bi sprejetje postopkov, ki so se predhodno uporabljali za druge namene, kot je izdajanje sredstev elektronske identifikacije, moralo biti pogojeno s potrditvijo, da navedeni postopki izpolnjujejo zahteve, ki so določene za ustrezno raven zanesljivosti.

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

(7) Navadno se uporabljajo določeni dejavniki avtentikacije, kot so deljene skrivnosti, fizične naprave in fizične značilnosti. Vendar bi bilo treba spodbujati uporabo večjega števila dejavnikov avtentikacije, zlasti iz različnih kategorij dejavnikov, da se poveča varnost postopka avtentikacije.

(8) Ta uredba ne bi smela vplivati na pravice zastopanja pravnih oseb. Vendar bi morale biti v Prilogi določene zahteve za povezavo med sredstvi elektronske identifikacije fizičnih in pravnih oseb.

(9) Priznati bi bilo treba pomen sistemov informacijske varnosti in upravljanja storitev ter pomen uporabe priznanih metodologij in uporabe načel, ki jih vsebujejo standardi serij ISO/IEC 27000 in ISO/IEC 20000.

(10) Upoštevati bi bilo treba tudi dobre prakse glede ravni zanesljivosti v državah članicah.

(11) Izdajanje varnostnih potrdil, kar zadeva informacijsko tehnologijo, na podlagi mednarodnih standardov je pomemben instrument za preverjanje varnostne skladnosti izdelkov z zahtevami iz tega izvedbenega akta.

(12) Odbor iz člena 48 Uredbe (EU) št. 910/2014 ni dal mnenja v roku, ki ga je določil njegov predsednik –

SPREJELA NASLEDNJO UREDBO:

Člen 1

1. Nizka, srednja in visoka raven zanesljivosti sredstev elektronske identifikacije, izdanih v okviru priglašene sheme elektronske identifikacije, se določi s sklicevanjem na specifikacije in postopke, ki so določeni v Prilogi.

2. Specifikacije in postopki iz Priloge se uporabljajo za podrobno določitev ravni zanesljivosti sredstev elektronske identifikacije, izdanih v okviru priglašene sheme elektronske identifikacije, tako da se določi zanesljivost in kakovost naslednjih elementov:

(a) prijava, kakor je določena v oddelku 2.1 Priloge k tej uredbi v skladu s členom 8(3)(a) Uredbe (EU) št. 910/2014;

(b) upravljanje sredstva elektronske identifikacije, kakor je določeno v oddelku 2.2 Priloge k tej uredbi v skladu s členom 8(3)(b) in (f) Uredbe (EU) št. 910/2014;

(c) avtentikacija, kakor je določena v oddelku 2.3 Priloge k tej uredbi v skladu s členom 8(3)(c) Uredbe (EU) št. 910/2014;

(d) upravljanje in organizacija, kakor sta določena v oddelku 2.4 Priloge k tej uredbi v skladu s členom 8(3)(d) in (e) Uredbe (EU) št. 910/2014.

3. Kadar sredstvo elektronske identifikacije, izdano na podlagi priglašene sheme elektronske identifikacije, izpolnjuje zahtevo, navedeno za višjo raven zanesljivosti, se šteje, da izpolnjuje enakovredno zahtevo nižje ravni zanesljivosti.

4. Če ni določeno drugače v ustreznem delu Priloge, morajo biti za doseganje navedene ravni zanesljivosti sredstva elektronske identifikacije, izdanega na podlagi priglašene sheme elektronske identifikacije, izpolnjeni vsi elementi iz Priloge za določeno raven zanesljivosti.

Člen 2

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

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo
Predsednik
Jean-Claude JUNCKER

PRILOGA

Tehnične specifikacije in postopki za nizko, srednjo in visoko raven zanesljivosti sredstev elektronske identifikacije, izdanih na podlagi priglašene sheme elektronske identifikacije

1. Opredelitev uporabljenih pojmov

V tej prilogi se uporabljajo naslednje opredelitve pojmov:

1. „verodostojni vir“ pomeni kateri koli vir v poljubni obliki, ki na zanesljiv način zagotavlja natančne podatke, informacije in/ali dokaze, ki se lahko uporabljajo za dokazovanje identitete;

2. „dejavnik avtentikacije“ pomeni dejavnik, ki je dokazljivo povezan z osebo, in spada v (najmanj) eno izmed naslednjih kategorij:

   (a) „dejavnik avtentikacije, ki temelji na posesti“ pomeni dejavnik avtentikacije, za katerega mora oseba dokazati, da ga ima v posesti;

   (b) „dejavnik avtentikacije, ki temelji na poznavanju“ pomeni dejavnik avtentikacije, za katerega mora oseba dokazati, da ga pozna;

   (c) „inherentni dejavnik avtentikacije“ pomeni dejavnik avtentikacije, ki temelji na fizični značilnosti fizične osebe in v zvezi s katerim mora oseba dokazati, da ima navedeno fizično značilnost;

3. „dinamična avtentikacija“ pomeni elektronski postopek, ki z uporabo kriptografskih ali drugih metod na zahtevo ustvari elektronski dokaz, da ima oseba pod nadzorom ali v posesti identifikacijske podatke, in ki se spremeni z vsako avtentikacijo med osebo in sistemom, ki preverja identiteto osebe;

4. „sistem za upravljanje informacijske varnosti“ pomeni niz procesov in postopkov za upravljanje tveganj v zvezi z informacijsko varnostjo na sprejemljivih ravneh.

2. Tehnične specifikacije in postopki

Elementi tehničnih specifikacij in postopkov iz te priloge se uporabljajo za določanje, kako se zahteve in merila iz člena 8 Uredbe (EU) št. 910/2014 uporabljajo za sredstva elektronske identifikacije, izdana na podlagi sheme elektronske identifikacije.

2.1 *Prijava*

2.1.1 Vloga in registracija

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Zagotovljeno je, da vložnik pozna pogoje v zvezi z uporabo sredstev elektronske identifikacije. 2. Zagotovljeno je, da vložnik pozna priporočene previdnostne varnostne ukrepe v zvezi s sredstvi elektronske identifikacije. 3. Zbirajo se ustrezni identifikacijski podatki za dokazovanje in preverjanje identitete.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.1.2 Dokazovanje in preverjanje identitete (fizična oseba)

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Domneva se lahko, da ima oseba v posesti dokaz, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, in predstavlja identiteto, ki se izkazuje. 2. Domneva se lahko, da je dokaz pristen ali da obstaja v skladu z verodostojnim virom in je domnevno veljaven. 3. Verodostojnemu viru je znano, da izkazana identiteta obstaja in domneva se lahko, da gre za isto osebo, ki izkazuje identiteto.
Srednja	Poleg ravni „Nizka“ mora biti izpolnjena še ena izmed možnosti iz točk 1 do 4: 1. preverjeno je, da ima oseba v posesti dokaz, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, in predstavlja identiteto, ki se izkazuje; in preverja se pristnost dokaza; ali pa je verodostojnemu viru znano, da dokaz obstaja in se nanaša na resnično osebo; ter sprejeti so bili ukrepi za zmanjšanje tveganja, da identiteta osebe ni enaka identiteti, ki se izkazuje, pri čemer je bilo upoštevano na primer tveganje izgube, kraje, začasne razveljavitve, preklica ali izteka veljavnosti dokaza; ali 2. med postopkom registracije je bil predložen identifikacijski dokument v državi članici, ki ga je izdala, in se nanaša na osebo, ki ga je predložila; in sprejeti so bili ukrepi za zmanjšanje tveganja, da identiteta osebe ni enaka identiteti, ki se izkazuje, pri čemer so bila upoštevana na primer tveganja izgube, kraje, začasne razveljavitve, preklica ali izteka veljavnosti dokumentov; ali 3. kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.2 za srednjo raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 Evropskega parlamenta in Sveta ([1]) ali enakovredni organ; ali 4. kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašenega sredstva elektronske identifikacije s srednjo ali visoko ravnjo zanesljivosti in ob upoštevanju tveganj za spremembo identifikacijskih podatkov osebe, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora srednjo in visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ.

Raven zanesljivosti	Zahtevani elementi
Visoka	Izpolnjene morajo biti zahteve iz točke 1 ali 2: 1. poleg ravni „Srednja“ mora biti izpolnjena še ena izmed možnosti iz točk (a) do (c): (a) kadar ima oseba preverjeno v posesti dokaz v obliki fotografije ali biometrične identifikacije, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, in navedeni dokaz predstavlja identiteto, ki se izkazuje, se dokaz preveri, da se ugotovi njegova veljavnost v skladu z verodostojnim virom; in s primerjavo ene ali več fizičnih značilnosti osebe z verodostojnim virom je bila izkazana identiteta vložnika; ali (b) kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.2 za visoko raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ; in sprejeti so bili ukrepi za dokazovanje, da so rezultati predhodnih postopkov še vedno veljavni; ali (c) kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašenega sredstva elektronske identifikacije z visoko ravnjo zanesljivosti in ob upoštevanju tveganj za spremembo identifikacijskih podatkov osebe, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ; in sprejeti so bili ukrepi za dokazovanje, da so rezultati predhodnega postopka za izdajo priglašenega sredstva elektronske identifikacije še vedno veljavni; ALI 2. kadar vložnik ne predloži priznanega dokaza s fotografijo ali biometrično identifikacijo, se uporabljajo enaki postopki za pridobitev takega priznanega dokaza s fotografijo ali biometrično identifikacijo kot na nacionalni ravni v državi članici subjekta, ki je odgovoren za registracijo.

([1]) Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).

2.1.3 Dokazovanje in preverjanje identitete (pravna oseba)

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Identiteta pravne osebe, ki se izkazuje, je dokazana na podlagi dokaza, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije.

Raven zanesljivosti	Zahtevani elementi
	2. Dokaz je domnevno veljaven in lahko se domneva, da je pristen ali da obstaja v skladu z verodostojnim virom, pod pogojem, da je vključitev pravne osebe v verodostojni vir prostovoljna in jo ureja dogovor med pravno osebo in verodostojnim virom. 3. Verodostojnemu viru ni znano, da bi bila pravna oseba v stanju, ki bi ji onemogočalo, da deluje kot navedena pravna oseba.
Srednja	Poleg ravni „Nizka“ mora biti izpolnjena še ena izmed možnosti iz točk 1 do 3: 1. identiteta pravne osebe, ki se izkazuje, je dokazana na podlagi dokaza, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, vključno z imenom pravne osebe, pravno obliko in (kadar se uporablja) registracijsko številko; in preverja se pristnost dokaza, ali je njegov obstoj znan verodostojnemu viru, kadar se zahteva vključitev pravne osebe v verodostojni vir za delovanje znotraj njenega sektorja; in sprejeti so bili ukrepi za zmanjšanje tveganja, da identiteta pravne osebe ni enaka identiteti, ki se izkazuje, pri čemer so bila upoštevana na primer tveganja izgube, kraje, začasne razveljavitve, preklica ali izteka veljavnosti dokaza; ali 2. kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.3 za srednjo raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da tako enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ; ali 3. kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašenega sredstva elektronske identifikacije s srednjo ali visoko ravnjo zanesljivosti, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora srednjo in visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ.
Visoka	Poleg ravni „Srednja“ mora biti izpolnjena še ena izmed možnosti iz točk 1 do 3: 1. identiteta pravne osebe, ki se izkazuje, je dokazana na podlagi dokaza, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, vključno z imenom pravne osebe, pravno obliko in najmanj enim enoličnim identifikatorjem, ki predstavlja pravno osebo, kot se uporablja v nacionalnem kontekstu; in preverja se veljavnost dokaza v skladu z verodostojnim virom; ali

Raven zanesljivosti	Zahtevani elementi
	2. kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.3 za visoko raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da tako enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ; in sprejeti so bili ukrepi za dokazovanje, da so rezultati tega predhodnega postopka še vedno veljavni; ali 3. kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašenega sredstva elektronske identifikacije z visoko ravnjo zanesljivosti, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ; in sprejeti so bili ukrepi za dokazovanje, da so rezultati predhodnega postopka za izdajo priglašenega sredstva elektronske identifikacije še vedno veljavni.

2.1.4 Povezava med sredstvi elektronske identifikacije fizičnih in pravnih oseb

Za povezavo med sredstvi elektronske identifikacije fizične osebe in sredstvi elektronske identifikacije pravne osebe (v nadaljnjem besedilu: povezava) se, kadar je to primerno, uporabljajo naslednji pogoji:

1. Povezavo je mogoče začasno razveljaviti in/ali preklicati. Življenjski cikel povezave (npr. aktiviranje, začasna razveljavitev, podaljšanje, preklic) se upravlja v skladu s priznanimi postopki na nacionalni ravni.

2. Fizična oseba, katere sredstvo elektronske identifikacije je povezano s sredstvom elektronske identifikacije pravne osebe, lahko izvajanje povezave prenese na drugo fizično osebo na podlagi priznanih postopkov na nacionalni ravni. Vendar pa je odgovornost še vedno na strani fizične osebe.

3. Povezava se izvede na naslednji način:

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Dokazovanje identitete fizične osebe, ki deluje v imenu pravne osebe, je preverjeno na ravni „Nizka“ ali višji. 2. Povezava je bila vzpostavljena na podlagi priznanih postopkov na nacionalni ravni. 3. Verodostojnemu viru ni znano, da bi bila fizična oseba v stanju, ki bi ji onemogočalo, da deluje kot navedena pravna oseba.
Srednja	Poleg točke 3 ravni „Nizka“ še: 1. Dokazovanje identitete fizične osebe, ki deluje v imenu pravne osebe, je preverjeno na ravni „Srednja“ ali „Visoka“.

Raven zanesljivosti	Zahtevani elementi
	2. Povezava je bila vzpostavljena na podlagi priznanih postopkov na nacionalni ravni, posledica česar je bila registracija povezave v verodostojnem viru. 3. Povezava je bila preverjena na podlagi informacij iz verodostojnega vira.
Visoka	Poleg točke 3 ravni „Nizka“ in točke 2 ravni „Srednja“ še: 1. Dokazovanje identitete fizične osebe, ki deluje v imenu pravne osebe, je bilo preverjeno na ravni „Visoka“. 2. Povezava je bila preverjena na podlagi enoličnega identifikatorja, ki predstavlja pravno osebo, ki se uporablja v nacionalnem okviru, in na podlagi informacij iz verodostojnega vira, ki enolično predstavljajo fizično osebo.

2.2 *Upravljanje sredstev elektronske identifikacije*

2.2.1 Lastnosti in zasnova sredstev elektronske identifikacije

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Sredstvo elektronske identifikacije uporablja najmanj en dejavnik avtentikacije. 2. Sredstvo elektronske identifikacije je zasnovano tako, da izdajatelj sprejme razumne ukrepe, s katerimi preveri, da se uporablja le pod nadzorom ali v posesti osebe, ki ji pripada.
Srednja	1. Sredstvo elektronske identifikacije uporablja najmanj dva dejavnika avtentikacije iz različnih kategorij. 2. Sredstvo elektronske identifikacije je zasnovano tako, da se lahko domneva, da se uporablja le, kadar je pod nadzorom ali v posesti osebe, ki ji pripada.
Visoka	Poleg ravni „Srednja“ še: 1. Sredstvo elektronske identifikacije varuje pred podvajanjem in nedovoljenim posegom ter napadalci z visokim potencialom za napad. 2. Sredstvo elektronske identifikacije je zasnovano tako, da ga lahko oseba, ki ji pripada, zanesljivo zavaruje pred uporabo drugih oseb.

2.2.2 Izdaja, dostava in aktiviranje

Raven zanesljivosti	Zahtevani elementi
Nizka	Po izdaji se sredstvo elektronske identifikacije dostavi na način, pri katerem je mogoče domnevati, da je doseglo le osebo, ki ji je namenjeno.
Srednja	Po izdaji se sredstvo elektronske identifikacije dostavi na način, pri katerem je mogoče domnevati, da je bilo dostavljeno v posest le osebi, ki ji pripada.
Visoka	V postopku aktiviranja se preverja, da je bilo sredstvo elektronske identifikacije dostavljeno v posest le osebi, ki ji pripada.

2.2.3 Začasna razveljavitev, preklic in ponovno aktiviranje

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Sredstvo elektronske identifikacije je mogoče pravočasno in učinkovito začasno razveljaviti in/ali preklicati. 2. Obstajajo ukrepi za preprečitev nezakonite začasne razveljavitve, preklica in/ali ponovnega aktiviranja. 3. Ponovno aktiviranje se izvede le, če so še vedno izpolnjene enake zahteve glede zanesljivosti kot pred začasno razveljavitvijo ali preklicem.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.2.4 Podaljšanje in zamenjava

Raven zanesljivosti	Zahtevani elementi
Nizka	Ob upoštevanju tveganj za spremembo identifikacijskih podatkov osebe morajo biti za podaljšanje ali zamenjavo izpolnjene enake zahteve glede zanesljivosti kot pri prvotnem dokazovanju in preverjanju identitete oz. morata temeljiti na veljavnem sredstvu elektronske identifikacije z enako ali višjo ravnjo zanesljivosti.
Srednja	Enako kot za raven „Nizka“.
Visoka	Poleg ravni „Nizka“ še: kadar podaljšanje ali zamenjava temelji na veljavnem sredstvu elektronske identifikacije, se podatki o identiteti preverjajo na podlagi verodostojnega vira.

2.3 *Avtentikacija*

Ta oddelek se osredotoča na grožnje, ki so povezane z uporabo mehanizma avtentikacije in navaja zahteve za vsako raven zanesljivosti. V tem oddelku se šteje, da so nadzorni ukrepi sorazmerni tveganjem za dano raven zanesljivosti.

2.3.1 Mehanizem avtentikacije

Naslednja preglednica za vsako raven zanesljivosti določa zahteve glede na mehanizem avtentikacije, prek katerega fizična ali pravna oseba uporablja sredstvo elektronske identifikacije za potrjevanje identitete zanašajoči se stranki.

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Identifikacijski podatki osebe se izdajo po zanesljivem preverjanju sredstva elektronske identifikacije in njegove veljavnosti. 2. Kadar so identifikacijski podatki osebe shranjeni kot del mehanizma avtentikacije, morajo biti zavarovani, da se zaščitijo pred izgubo in zlorabo, vključno z nespletno analizo. 3. V mehanizmu avtentikacije se izvajajo varnostni nadzori za preverjanje sredstva elektronske identifikacije, zato je zelo malo verjetno, da bi napadalci z povečanim osnovnim potencialom za napad lahko z dejavnostmi, kot so ugibanje, prisluškovanje, ponovno predvajanje ali manipulacija s sporočilom, ogrozili mehanizme avtentikacije.

Raven zanesljivosti	Zahtevani elementi
Srednja	Poleg ravni „Nizka“ še: 1. Identifikacijski podatki osebe se izdajo po zanesljivem preverjanju sredstva elektronske identifikacije in njegove veljavnosti z dinamično avtentikacijo. 2. V mehanizmu avtentikacije se izvajajo varnostni nadzori za preverjanje sredstva elektronske identifikacije, zato je zelo malo verjetno, da bi napadalci z zmernim potencialom za napad lahko z dejavnostmi, kot so ugibanje, prisluškovanje, ponovno predvajanje ali manipulacija s sporočilom, ogrozili mehanizme avtentikacije.
Visoka	Poleg ravni „Srednja“ še: v mehanizmu avtentikacije se izvajajo varnostni nadzori za preverjanje sredstva elektronske identifikacije, zato je zelo malo verjetno, da bi napadalci z visokim potencialom za napad lahko z dejavnostmi, kot so ugibanje, prisluškovanje, ponovno predvajanje ali manipulacija s sporočilom, ogrozili mehanizme avtentikacije.

2.4 *Upravljanje in organizacija*

Vsi udeleženci, ki zagotavljajo čezmejne storitve v zvezi z elektronsko identifikacijo (v nadaljnjem besedilu: ponudniki) imajo dokumentirane postopke za upravljanje informacijske varnosti, politike, pristope za upravljanje tveganj in druge priznane nadzorne ukrepe, s katerimi se ustreznim organom upravljanja shem elektronske identifikacije v zadevnih državah članicah zagotavlja, da so vzpostavljeni učinkoviti postopki. V oddelku 2.4. se šteje, da so vse zahteve/elementi sorazmerni tveganjem za dano raven zanesljivosti.

2.4.1 Splošne določbe

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Ponudniki katerih koli operativnih storitev iz te uredbe so javni organ ali pravni subjekt, ki ga kot takega priznava nacionalno pravo države članice in ima vzpostavljeno organizacijo ter je polno operativen v vseh delih, ki so bistveni za opravljanje storitev. 2. Ponudniki izpolnjujejo vse pravne zahteve, ki so jim naložene v zvezi z izvajanjem in zagotavljanjem storitve, vključno s tem, katere vrste informacij se lahko zahtevajo, kako se izvaja dokazovanje identitete, katere informacije se lahko hranijo in kako dolgo. 3. Ponudniki lahko dokažejo, da so sposobni prevzeti škodno odgovornost in da imajo zadostne finančne vire za neprekinjeno delovanje in zagotavljanje storitev. 4. Ponudniki so odgovorni za izpolnjevanje vseh zavez, ki jih prenesejo na zunanje izvajalce, in skladnost s politiko sheme v enaki meri, kot če bi naloge opravili sami. 5. Za sheme elektronske identifikacije, ki niso bile vzpostavljene na podlagi nacionalne zakonodaje, je pripravljen učinkovit načrt prenehanja delovanja. Tak načrt mora vključevati urejeno prekinitev storitve ali nadaljevanje izvajanja prek drugega ponudnika, način obveščanja zadevnih organov in končnih uporabnikov ter podrobnosti o načinu zavarovanja, hrambe in uničenja podatkov v skladu s politiko sheme.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.2 Objavljena obvestila in uporabniške informacije

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Obstaja objavljena opredelitev storitve, ki vključuje vse uporabljene izraze, pogoje in pristojbine, vključno z vsemi omejitvami uporabe. Opredelitev storitve vključuje tudi politiko varstva osebnih podatkov. 2. Vzpostaviti je treba ustrezno politiko in postopke, da se zagotovi pravočasna in zanesljiva obveščenost uporabnikov storitve o vseh spremembah opredelitve storitve in uporabljenih izrazov, pogojev ter politike varstva zasebnosti za zadevno storitev. 3. Vzpostaviti je treba ustrezne politike in postopke, ki zagotavljajo celovite in pravilne odgovore na zahtevke za informacije.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.3 Upravljanje informacijske varnosti

Raven zanesljivosti	Zahtevani elementi
Nizka	Obstaja učinkovit sistem upravljanja informacijske varnosti za upravljanje in nadzor tveganj v zvezi z informacijsko varnostjo.
Srednja	Poleg ravni „Nizka“ še: sistem za upravljanje informacijske varnosti upošteva dokazane standarde ali načela za upravljanje in nadzor tveganj v zvezi z informacijsko varnostjo.
Visoka	Enako kot za raven „Srednja“.

2.4.4 Vodenje evidence

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Vodenje evidence in hramba zadevnih informacij z uporabo učinkovitega sistema za upravljanje evidence ob upoštevanju veljavne zakonodaje in dobrih praks v zvezi z varstvom in hrambo podatkov. 2. Evidence se v dovoljenem obsegu v skladu z nacionalnim pravom ali drugo nacionalno upravno ureditvijo hranijo in varujejo tako dolgo, dokler se potrebujejo za revizijo in preiskovanje kršitev varnosti ter hrambo podatkov, nato se evidence varno uničijo.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.5 Prostori in osebje

Naslednja preglednica vsebuje zahteve v zvezi s prostori, osebjem in, kadar je to primerno, podizvajalci, ki izvajajo naloge iz te uredbe. Skladnost z vsako od zahtev je sorazmerna tveganju, ki je povezano z zagotovljeno ravnjo zanesljivosti.

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Obstajajo postopki, s katerimi se zagotavlja, da so osebje in podizvajalci za naloge, ki jih izvajajo, dovolj usposobljeni, kvalificirani in izkušeni. 2. Na voljo je dovolj osebja in podizvajalcev za ustrezno izvajanje in financiranje storitve v skladu z njenimi politikami in postopki. 3. Prostori, ki se uporabljajo za zagotavljanje storitve, so pod stalnim nadzorom in zavarovani pred škodo, ki jo povzročajo okoljski dogodki, nepooblaščeni dostop in drugi dejavniki, ki bi lahko vplivali na varnost storitve. 4. Prostori, ki se uporabljajo za zagotavljanje storitve, omogočajo, da je dostop do območij, kjer se nahajajo ali obdelujejo osebni, kriptografski ali drugi občutljivi podatki, dovoljen le pooblaščenemu osebju ali podizvajalcem.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.6 Tehnični nadzor

Raven zanesljivosti	Zahtevani elementi
Nizka	1. Obstaja sorazmeren tehnični nadzor za upravljanje tveganj v zvezi z varnostjo storitev, ki varujejo zaupnost, celovitost in razpoložljivost obdelanih informacij. 2. Elektronski komunikacijski kanali, ki se uporabljajo za izmenjavo osebnih ali občutljivih podatkov, so zavarovani pred prisluškovanjem, manipulacijo in ponovnim predvajanjem. 3. Če se občutljivi kriptografski material uporablja za izdajo sredstva elektronske identifikacije in avtentikacijo, je dostop do njega omejen na uporabniške vloge in aplikacije, ki nujno potrebujejo dostop. Zagotavlja se, da se tak material nikoli ne hrani v golem besedilu. 4. Obstajajo postopki, ki zagotavljajo trajnostno vzdrževanje varnosti in zmožnost odgovora na spremembe ravni tveganja, incidente in kršitve varnosti. 5. Vsi mediji, ki vsebujejo osebne, kriptografske ali druge občutljive podatke, se shranjujejo, prevažajo in odstranjujejo na varen in zanesljiv način.
Srednja	Poleg ravni „Nizka“ še: če se občutljiv kriptografski material uporablja za izdajo sredstev elektronske identifikacije in avtentikacijo, je zavarovan pred nedovoljenim posegom.
Visoka	Enako kot za raven „Srednja“.

2.4.7 Skladnost in revizija

Raven zanesljivosti	Zahtevani elementi
Nizka	Obstajajo redne notranje revizije, ki zajamejo vse ustrezne dele za izvajanje zagotovljenih storitev, da se zagotovi skladnost z zadevno politiko.

Raven zanesljivosti	Zahtevani elementi
Srednja	Obstajajo redne neodvisne notranje ali zunanje revizije, ki zajamejo vse ustrezne dele za izvajanje zagotovljenih storitev, da se zagotovi skladnost z zadevno politiko.
Visoka	1. Obstajajo redne neodvisne zunanje revizije, ki zajamejo vse ustrezne dele za izvajanje zagotovljenih storitev, da se zagotovi skladnost z zadevno politiko. 2. Kadar shemo neposredno upravlja vladni organ, se revizija izvaja v skladu z nacionalno zakonodajo.

IZVEDBENA UREDBA KOMISIJE (EU) 2015/1503

z dne 8. septembra 2015

o določitvi standardnih uvoznih vrednosti za določitev uvozne cene za nekatere vrste sadja in zelenjave

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 1308/2013 Evropskega parlamenta in Sveta z dne 17. decembra 2013 o vzpostavitvi skupne ureditve trgov kmetijskih proizvodov in razveljavitvi uredb Sveta (EGS) št. 922/72, (EGS) št. 234/79, (ES) št. 1037/2001 in (ES) št. 1234/2007 ([1]),

ob upoštevanju Izvedbene uredbe Komisije (EU) št. 543/2011 z dne 7. junija 2011 o določitvi podrobnih pravil za uporabo Uredbe Sveta (ES) št. 1234/2007 za sektorja sadja in zelenjave ter predelanega sadja in zelenjave ([2]) ter zlasti člena 136(1) Izvedbene uredbe,

ob upoštevanju naslednjega:

(1) Izvedbena uredba (EU) št. 543/2011 na podlagi izida večstranskih trgovinskih pogajanj urugvajskega kroga določa merila, po katerih Komisija določi standardne vrednosti za uvoz iz tretjih držav za proizvode in obdobja iz dela A Priloge XVI k tej uredbi.

(2) Standardna uvozna vrednost se izračuna vsak delovni dan v skladu s členom 136(1) Izvedbene uredbe (EU) št. 543/2011 ob upoštevanju spremenljivih dnevnih podatkov. Zato bi morala ta uredba začeti veljati na dan objave v *Uradnem listu Evropske unije* –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Standardne uvozne vrednosti iz člena 136 Izvedbene uredbe (EU) št. 543/2011 so določene v Prilogi k tej uredbi.

Člen 2

Ta uredba začne veljati na dan objave v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo

V imenu predsednika

Jerzy PLEWA

Generalni direktor za kmetijstvo in razvoj podeželja

([1]) UL L 347, 20.12.2013, str. 671.
([2]) UL L 157, 15.6.2011, str. 1.

PRILOGA

Standardne uvozne vrednosti za določitev uvozne cene za nekatere vrste sadja in zelenjave

(EUR/100 kg)

Oznaka KN	Oznaka tretje države (1)	Standardna uvozna vrednost
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)

Oznaka KN	Oznaka tretje države (1)	Standardna uvozna vrednost
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Nomenklatura držav, določena v Uredbi Komisije (EU) št. 1106/2012 z dne 27. novembra 2012 o izvajanju Uredbe (ES) št. 471/2009 Evropskega parlamenta in Sveta o statistiki Skupnosti o zunanji trgovini z državami nečlanicami v zvezi s posodabljanjem nomenklature držav in ozemelj (UL L 328, 28.11.2012, str. 7). Oznaka „ZZ“ predstavlja „druga porekla“.

SKLEPI

IZVEDBENI SKLEP KOMISIJE (EU) 2015/1504

z dne 7. septembra 2015

o odobritvi odstopanj nekaterim državam članicam glede zagotavljanja statističnih podatkov v skladu z Uredbo (ES) št. 1099/2008 Evropskega parlamenta in Sveta o statistiki energetike

(notificirano pod dokumentarno številko C(2015) 6105)

(Besedilo v estonskem, francoskem, grškem, nizozemskem in slovaškem jeziku je edino verodostojno)

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (ES) št. 1099/2008 Evropskega parlamenta in Sveta z dne 22. oktobra 2008 o statistiki energetike ([1]) ter zlasti člena 5(4) in člena 10(2) Uredbe,

ob upoštevanju naslednjega:

(1) V skladu s členom 5(4) Uredbe (ES) št. 1099/2008 se lahko na ustrezno utemeljeno zahtevo države članice odobrijo odstopanja za tiste dele zbiranja nacionalnih statističnih podatkov, ki bi dajalce podatkov pretirano obremenili.

(2) Belgija, Estonija, Ciper in Slovaška so vložili zahteve za odobritev odstopanj v zvezi z zagotavljanjem podrobnih statističnih podatkov o porabi energije v gospodinjstvih glede na vrsto končne porabe za nekatera referenčna leta.

(3) Informacije, ki so jih predložile navedene države članice, upravičujejo odobritev odstopanj.

(4) Ukrepi iz tega sklepa so v skladu z mnenjem Odbora za evropski statistični sistem –

SPREJELA NASLEDNJI SKLEP:

Člen 1

Odobrijo se naslednja odstopanja od določb Uredbe (ES) št. 1099/2008:

(1) Belgiji se odobri odstopanje od zagotavljanja podatkov za referenčno leto 2015 za postavke 4.2.1 do 4.2.5 točke 1.2.3, postavke 4.2.1 do 4.2.5 točke 2.2.3, postavke 3.1 do 3.6 točke 3.2.3, postavke 7.2.1 do 7.2.5 točke 4.2.3 in postavke 4.2.1 do 4.2.5 točke 5.2.4 Priloge B o podrobnih statističnih podatkih o porabi energije v gospodinjstvih glede na vrsto končne porabe (kakor je opredeljena v 26. postavki točke 2.3 „Drugi sektorji – gospodinjstva“ Priloge A).

([1]) UL L 304, 14.11.2008, str. 1.

(2) Estoniji se odobri odstopanje od zagotavljanja podatkov za referenčna leta 2015, 2016 in 2017 za postavke 4.2.1 do 4.2.5 točke 1.2.3, postavke 4.2.1 do 4.2.5 točke 2.2.3, postavke 3.1 do 3.6 točke 3.2.3, postavke 7.2.1 do 7.2.5 točke 4.2.3 in postavke 4.2.1 do 4.2.5 točke 5.2.4 Priloge B o podrobnih statističnih podatkih o porabi energije v gospodinjstvih glede na vrsto končne porabe (kakor je opredeljena v 26. postavki točke 2.3 „Drugi sektorji – gospodinjstva“ Priloge A).

(3) Cipru se odobri odstopanje od zagotavljanja podatkov za referenčna leta 2015, 2016 in 2017 za postavke 4.2.1 do 4.2.5 točke 1.2.3, postavke 4.2.1 do 4.2.5 točke 2.2.3, postavke 3.1 do 3.6 točke 3.2.3 in postavke 4.2.1 do 4.2.5 točke 5.2.4 Priloge B o podrobnih statističnih podatkih o porabi energije v gospodinjstvih glede na vrsto končne porabe (kakor je opredeljena v 26. postavki točke 2.3 „Drugi sektorji – gospodinjstva“ Priloge A).

(4) Slovaški se odobri odstopanje od zagotavljanja podatkov za referenčni leti 2015 in 2016 za postavke 4.2.1 do 4.2.5 točke 1.2.3, postavke 4.2.1 do 4.2.5 točke 2.2.3, postavke 3.1 do 3.6 točke 3.2.3, postavke 7.2.1 do 7.2.5 točke 4.2.3 in postavke 4.2.1 do 4.2.5 točke 5.2.4 Priloge B o podrobnih statističnih podatkih o porabi energije v gospodinjstvih glede na vrsto končne porabe (kakor je opredeljena v 26. postavki točke 2.3 „Drugi sektorji – gospodinjstva“ Priloge A).

Člen 2

Ta sklep je naslovljen na Kraljevino Belgijo, Republiko Estonijo, Republiko Ciper in Slovaško republiko.

V Bruslju, 7. septembra 2015

Za Komisijo

Marianne THYSSEN

Članica Komisije

IZVEDBENI SKLEP KOMISIJE (EU) 2015/1505

z dne 8. septembra 2015

o določitvi tehničnih specifikacij in formatov v zvezi z zanesljivimi seznami v skladu s členom 22(5) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 22(5) Uredbe,

ob upoštevanju naslednjega:

(1) Zanesljivi seznami so bistveni za vzpostavljanje zaupanja med udeleženci na trgu, saj je iz njih razviden status ponudnika storitev v trenutku nadzora.

(2) Čezmejno uporabo elektronskih podpisov je pospešila Odločba Komisije 2009/767/ES ([2]), ki državam članicam nalaga obveznost, da vzpostavijo, vzdržujejo in objavijo zanesljive sezname, ki vsebujejo informacije v zvezi z overitelji, ki izdajajo kvalificirana potrdila javnosti v skladu z Direktivo 1999/93/ES Evropskega parlamenta in Sveta ([3]) ter so nadzorovani in akreditirani s strani držav članic.

(3) Člen 22 Uredbe (EU) št. 910/2014 državam članicam nalaga obveznost, da v obliki, primerni za avtomatizirano obdelavo, na varen način sestavijo, vodijo in objavijo elektronsko podpisane ali ožigosane zanesljive sezname in Komisijo uradno obvestijo o organih, ki so pristojni za sestavljanje nacionalnih zanesljivih seznamov.

(4) Ponudnik storitev zaupanja in storitve zaupanja, ki jih zagotavlja, bi se morali šteti za kvalificirane, kadar je ponudniku na zanesljivem seznamu dodeljen kvalificiran status. Da se zagotovi, da lahko ponudniki storitev na daljavo in po elektronski poti brez težav izpolnjujejo druge obveznosti iz Uredbe (EU) št. 910/2014, zlasti tiste iz členov 27 in 37, in da se izpolnijo legitimna pričakovanja drugih overiteljev, ki ne izdajajo kvalificiranih potrdil, vendar pa zagotavljajo storitve v zvezi z elektronskimi podpisi na podlagi Direktive 1999/93/ES in so uvrščeni na seznam do 30. junija 2016, bi moralo biti državam članicam omogočeno, da na nacionalni ravni na zanesljive sezname prostovoljno dodajo storitve zaupanja, ki niso kvalificirane, pod pogojem, da se jasno navede, da te storitve zaupanja niso kvalificirane v skladu z Uredbo (EU) št. 910/2014.

(5) V skladu z uvodno izjavo 25 Uredbe (EU) št. 910/2014 lahko države članice dodajo druge vrste nacionalno opredeljenih storitev zaupanja, ki niso opredeljene v členu 3(16) Uredbe (EU) št. 910/2014, pod pogojem, da je jasno navedeno, da te storitve zaupanja niso kvalificirane v skladu z Uredbo (EU) št. 910/2014.

(6) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJI SKLEP:

Člen 1

Države članice sestavijo, objavijo in vodijo zanesljive sezname, ki vsebujejo informacije o ponudnikih kvalificiranih storitev zaupanja, ki jih nadzorujejo, in informacije o kvalificiranih storitvah zaupanja, ki jih ti zagotavljajo. Navedeni seznami so v skladu s tehničnimi specifikacijami iz Priloge I.

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

([2]) Odločba Komisije 2009/767/ES z dne 16. oktobra 2009 o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo „enotnih kontaktnih točk“ po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu (UL L 274, 20.10.2009, str. 36).

([3]) Direktiva Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (UL L 13, 19.1.2000, str. 12.)

Člen 2

Države članice lahko v zanesljive sezname vključijo informacije o ponudnikih nekvalificiranih storitev zaupanja, skupaj z informacijami o nekvalificiranih storitvah zaupanja, ki jih ti zagotavljajo. Iz zanesljivega seznama je jasno razvidno, kateri ponudniki storitev zaupanja in katere storitve zaupanja, ki jih ti zagotavljajo, niso kvalificirani.

Člen 3

1. V skladu s členom 22(2) Uredbe (EU) št. 910/2014 države članice elektronsko podpišejo ali ožigosajo obliko, primerno za avtomatizirano obdelavo svojega zanesljivega seznama v skladu s tehničnimi specifikacijami iz Priloge I.

2. Če država članica elektronsko objavi zanesljivi seznam v človeku berljivi obliki, zagotovi, da ta oblika zanesljivega seznama vsebuje enake podatke kot oblika, primerna za avtomatizirano obdelavo, ter jo elektronsko podpiše ali ožigosa v skladu s tehničnimi specifikacijami iz Priloge I.

Člen 4

1. Države članice Komisiji uradno sporočijo informacije iz člena 22(3) Uredbe (EU) št. 910/2014 z uporabo predloge iz Priloge II.

2. Informacije iz odstavka 1 vsebujejo dve ali več potrdil javnih ključev upravljavca sheme z najmanj trimesečnimi izmeničnimi obdobji veljavnosti, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za elektronsko podpisovanje ali žigosanje oblike, primerne za avtomatizirano obdelavo zanesljivega seznama, in človeku berljive oblike, kadar se objavi.

3. V skladu s členom 22(4) Uredbe (EU) št. 910/2014 Komisija prek varnega kanala na avtenticiranem spletnem strežniku javnosti da na voljo informacije iz odstavkov 1 in 2, kot so jih uradno sporočile države članice, v podpisani ali ožigosani obliki, primerni za avtomatizirano obdelavo.

4. Komisija prek varnega kanala na avtenticiranem spletnem strežniku javnosti lahko da na voljo informacije iz odstavkov 1 in 2, kot so jih uradno sporočile države članice, v podpisani ali ožigosani človeku berljivi obliki.

Člen 5

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

Ta sklep je v celoti zavezujoč in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo

Predsednik

Jean-Claude JUNCKER

PRILOGA I

TEHNIČNE SPECIFIKACIJE ZA SKUPNO PREDLOGO ZA ZANESLJIVE SEZNAME

POGLAVJE I

SPLOŠNE ZAHTEVE

Zanesljivi seznami vključujejo veljavne in pretekle informacije o statusu navedenih storitev zaupanja od vključitve ponudnika storitev zaupanja v zanesljive sezname.

Izrazi „potrjen“, „akreditiran“ in/ali „nadzorovan“ v teh specifikacijah zajemajo tudi nacionalne sheme potrjevanja, vendar bodo države članice zagotovile dodatne informacije o naravi vsake take nacionalne sheme v svojem zanesljivem seznamu, vključno s pojasnili o mogočih razlikah glede na sheme nadzora, ki se uporabljajo za ponudnike kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih ti zagotavljajo.

Glavni cilj informacij zanesljivega seznama je podpreti potrjevanje veljavnosti žetonov kvalificiranih storitev zaupanja, tj. fizičnih ali binarnih (logičnih) objektov, ki se generirajo ali izdajo ob uporabi kvalificirane storitve zaupanja, in sicer na primer kvalificiranih elektronskih podpisov/žigov, naprednih elektronskih podpisov/žigov, podprtih s kvalificiranim potrdilom, kvalificiranih časovnih žigov, kvalificiranih evidenc elektronske dostave itd.

POGLAVJE II

PODROBNE SPECIFIKACIJE ZA SKUPNO PREDLOGO ZA ZANESLJIVE SEZNAME

Te specifikacije temeljijo na specifikacijah in zahtevah iz ETSI TS 119 612 v 2.1.1 (v nadaljnjem besedilu: ETSI TS 119 612).

Kadar v teh specifikacijah niso navedene posebne zahteve, v celoti veljajo zahteve iz razdelkov 5 in 6 ETSI TS 119 612. Kadar so v teh specifikacijah navedene posebne zahteve, prevladajo nad ustreznimi zahtevami iz ETSI TS 119 612. V primeru neskladij med temi specifikacijami in specifikacijami iz ETSI TS 119 612 prevladajo te specifikacije.

Ime sheme (razdelek 5.3.6)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.6 TS 119 612, v katerem se za shemo uporablja naslednje ime:

„EN_name_value“ = „zanesljivi seznam, ki vsebuje informacije o ponudnikih kvalificiranih storitev zaupanja, ki jih nadzirajo države članice izdajateljice, skupaj z informacijami o kvalificiranih storitvah zaupanja, ki jih ti zagotavljajo, v skladu z ustreznimi določbami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.“

URI za informacije o shemi (razdelek 5.3.7)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.7 TS 119 612, v katerem „ustrezne informacije o shemi“ zajemajo najmanj:

(a) za vse države članice enake uvodne informacije o obsegu in ozadju zanesljivega seznama, osnovni shemi nadzora in, kadar je to primerno, nacionalnih shemah potrjevanja (npr. akreditacijskih). Uporabi se spodnje besedilo, v katerem se znakovni niz „[*ime zadevne države članice*]“ nadomesti z imenom zadevne države članice:

„Ta seznam je zanesljivi seznam, ki vsebuje informacije o ponudnikih kvalificiranih storitev zaupanja, ki jih nadzira [*ime zadevne države članice*], skupaj z informacijami o kvalificiranih storitvah zaupanja, ki jih ti zagotavljajo, v skladu z ustreznimi določbami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.

Čezmejno uporabo elektronskih podpisov je pospešila Odločba Komisije 2009/767/ES z dne 16. oktobra 2009, ki državam članicam nalaga obveznost, da vzpostavijo, vzdržujejo in objavijo zanesljive sezname, ki vsebujejo informacije v zvezi z overitelji, ki izdajajo kvalificirana potrdila javnosti v skladu z Direktivo Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis ter so nadzorovani/akreditirani s strani držav članic. Ta zanesljivi seznam je nadaljevanje zanesljivega seznama, ki je bil vzpostavljen z Odločbo 2009/767/ES."

Zanesljivi seznami so bistveni elementi za vzpostavljanje zaupanja med udeleženci na elektronskem trgu, ki uporabnikom omogočajo, da preverijo, ali imajo ponudniki ter njihove storitve kvalificirani status ter kakšen je bil njihov pretekli status.

Zanesljivi seznami države članice vključujejo najmanj informacije, navedene v členih 1 in 2 Izvedbenega sklepa Komisije (EU) 2015/1505.

Države članice lahko v zanesljive sezname vključijo informacije o nekvalificiranih ponudnikih storitev zaupanja, skupaj z informacijami o nekvalificiranih storitvah zaupanja, ki jih ti zagotavljajo. Jasno mora biti navedeno, da niso kvalificirani v skladu z Uredbo (EU) št. 910/2014.

Države članice lahko v zanesljive sezname vključijo informacije o nacionalno opredeljenih storitvah zaupanja, ki niso opredeljene na podlagi člena 3(16) Uredbe (EU) št. 910/2014. Jasno mora biti navedeno, da niso kvalificirane v skladu z Uredbo (EU) št. 910/2014.

(b) Posebne informacije o osnovni shemi nadzora in, kadar je to primerno, nacionalnih shemah potrjevanja (npr. akreditacije), zlasti ([1]):

1. informacije o nacionalnem sistemu nadzora, ki se uporablja za ponudnike kvalificiranih in nekvalificiranih storitev zaupanja ter kvalificirane in nekvalificirane storitve zaupanja, ki jih ti zagotavljajo, kakor je določeno v Uredbi (EU) št. 910/2014;

2. informacije, kadar je to primerno, o nacionalnih shemah za prostovoljno akreditacijo, ki se uporabljajo za overitelje, ki so izdali kvalificirana potrdila na podlagi Direktive 1999/93/ES.

Te posebne informacije za vsako zgoraj navedeno osnovno shemo vključujejo najmanj:

1. splošni opis;

2. informacije o postopku, ki se upošteva za nacionalni sistem nadzora in, kadar je to primerno, za potrjevanje na podlagi nacionalne sheme potrjevanja;

3. informacije o merilih za nadzor ali, kadar je to primerno, za potrjevanje ponudnikov storitev zaupanja;

4. informacije o merilih in pravilih, ki se uporabljajo za izbiro nadzornikov/revizorjev in za opredelitev, kako naj ocenjujejo ponudnike storitev zaupanja in storitve zaupanja, ki jih ti zagotavljajo;

5. kadar je to primerno, druge kontaktne in splošne informacije, ki se uporabljajo za izvajanje sheme.

Vrsta sheme/skupnost/pravila (razdelek 5.3.9)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.9. TS 119 612.

Vključuje izključno URI v britanski angleščini.

([1]) Navedena podatkovna niza sta za zanašajoče se stranke bistvenega pomena za ocenjevanje ravni kakovosti in varnosti takih sistemov. Ta dva podatkovna niza se zagotavljata na ravni zanesljivega seznama v poljih „Informacije o shemi URI" (razdelek 5.3.7 – informacije, ki jih zagotovi država članica), „Vrsta sheme/skupnost/pravila" (razdelek 5.3.9 – skupno besedilo za vse države članice) in „Politika/pravno obvestilo v zvezi s seznamom o statusu storitev zaupanja" (razdelek 5.3.11 – skupno besedilo za vse države članice, z možnostjo za vsako državo članico, da doda besedilo/sklice, ki so zanjo posebni). Dodatne informacije o takih sistemih za nekvalificirane storitve zaupanja in nacionalno opredeljene (kvalificirane) storitve zaupanja se lahko zagotavljajo na ravni storitve, kadar je to primerno in potrebno (npr. za razlikovanje med več ravnmi kakovosti/varnosti), v polju „URI za opredelitev storitev sheme" (razdelek 5.5.6).

Vključuje najmanj dva URI:

1. URI, ki je skupen vsem zanesljivim seznamom držav članic, z napotilom na opisno besedilo, ki velja za vse zanesljive sezname, in sicer:

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

   Opisno besedilo:

   „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) scheme(s) 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 certificate(s) is(are) qualified under Directive 1999/93/EC;

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

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

— ‚QCForWSA' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is(are) qualified certificate(s) 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 certificate(s) is(are) not to be considered as qualified; and/or

— to indicate the nature of the SSCD support:

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

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

— ‚QCSSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), 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 certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

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

— ‚QCQSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), 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 certificate(s), when claimed or stated as qualified certificate(s), 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, ki je specifičen za zanesljivi seznam vsake države članice, z napotilom na opisno besedilo, ki velja za zanesljivi seznam te države članice:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, pri čemer je CC = ISO 3166-1 ([1]) dvočrkovna oznaka države, ki se uporablja v polju „Država sheme" (razdelek 5.3.10),

— podatki o tem, kje lahko uporabniki najdejo posebne politike/pravila za zadevno državo članico, v skladu s katerimi se storitve zaupanja v zanesljivem seznamu ocenjujejo v skladu s sistemom nadzora države članice in, kadar je to primerno, shemo potrjevanja,

— podatki o tem, kje lahko uporabniki najdejo posebni opis za zadevno državo članico glede načina uporabe in razlage vsebine zanesljivega seznama v zvezi z navedenimi nekvalificiranimi storitvami zaupanja in/ali nacionalno opredeljenimi storitvami zaupanja. Ta opis se lahko uporabi za navedbo morebitne razdrobljenosti v nacionalnih sistemih potrjevanja v zvezi z overitelji, ki ne izdajajo kvalificiranih potrdil, in kako se v ta namen uporabljata polji „URI za opredelitev storitev sheme" (razdelek 5.5.6) in „Razširitve informacij o storitvah" (razdelek 5.5.9).

Države članice LAHKO razširijo zgoraj naveden poseben URI za državo članico, tako da opredelijo in uporabijo dodatne URI (tj. URI, opredeljen na podlagi tega hierarhičnega posebnega URI).

Politika/pravno obvestilo v zvezi s seznamom o statusu storitev zaupanja (razdelek 5.3.11)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.3.11 TS 119 612, v katerem je politika/pravno obvestilo v zvezi s pravnim statusom sheme ali pravnimi zahtevami, ki jih shema izpolnjuje v okviru pristojnosti, v kateri je bila vzpostavljena, in/ali kakršnimi koli omejitvami ter pogoji, na podlagi katerih se zanesljivi seznam vodi in

([1]) ISO 3166-1:2006: „Kode za predstavljanje imen držav in njihovih podrejenih enot – 1. del: Kode držav".

objavi, izražena z zaporedjem večjezikovnih znakovnih nizov (glej razdelek 5.1.4), ki v britanski angleščini kot obveznem jeziku in izbirno v enem ali več nacionalnih jezikih navaja dejansko besedilo take politike ali obvestilo, ki je sestavljeno na naslednji način:

1. prvi obvezni del, skupen vsem zanesljivim seznamom držav članic, v katerem je naveden veljaven pravni okvir v angleščini:

   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.

   Besedilo v nacionalnem jeziku države članice:

   Pravni okvir, ki se uporablja za ta zanesljivi seznam je Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES;

2. drugi, neobvezni del, ki je poseben za vsak zanesljivi seznam in navaja sklicevanje na nacionalni pravni okvir, ki se uporablja.

Trenutni status storitve (razdelek 5.5.4)

To polje mora biti vključeno in v skladu s specifikacijami iz razdelka 5.5.4. TS 119 612.

Migracija vrednosti „Trenutni status storitve“ storitev, ki so uvrščene na zanesljivi seznam držav članic EU od datuma pred začetkom veljavnosti Uredbe (EU) št. 910/2014 (tj. 30. junija 2016), se izvrši na datum začetka uporabe Uredbe (tj. 1. julija 2016), kot je določeno v Prilogi J k ETSI TS 119 612.

POGLAVJE III

NEPREKINJENA VELJAVNOST ZANESLJIVIH SEZNAMOV

Potrdila, ki se uradno sporočijo Komisiji v skladu s členom 4(2) tega sklepa, morajo izpolnjevati zahteve iz razdelka 5.7.1 ETSI TS 119 612 in se izdajo tako, da:

— so do njihovega končnega datuma veljavnosti najmanj trije meseci („NotAfter“),

— so bili generirani na podlagi novih parov ključev. Predhodno uporabljeni pari ključev se ne smejo ponovno potrjevati.

V primeru izteka veljavnosti enega od potrdil javnih ključev, ki se lahko uporabljajo za potrjevanje veljavnosti podpisa ali žiga zanesljivega seznama, ki je bil uradno sporočen Komisiji in je objavljen v osrednjem seznamu kazalcev Komisije, države članice:

— v primeru, da je bil trenutno objavljeni zanesljivi seznam podpisan ali ožigosan z zasebnim ključem, katerega potrdilo javnega ključa je poteklo, brez odlašanja ponovno izdajo nov zanesljivi seznam, podpisan ali ožigosan z zasebnim ključem, katerega uradno sporočeno potrdilo javnega ključa ni poteklo,

— na zahtevo generirajo nove pare ključev, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama, in generirajo ustrezna potrdila javnih ključev,

— nemudoma Komisiji uradno sporočijo nov seznam potrdil javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama.

V primeru, da je kompromitiran ali deaktiviran eden od zasebnih ključev, ki ustreza potrdilu javnega ključa, ki se lahko uporabi za potrjevanje veljavnosti podpisa ali žiga zanesljivega seznama, in ki je bil uradno sporočen Komisiji ter objavljen v osrednjem seznamu kazalcev Komisije, države članice:

— brez odlašanja ponovno izdajo nov zanesljivi seznam, podpisan ali ožigosan z nekompromitiranim zasebnim ključem, če je bil objavljeni zanesljivi seznam podpisan ali ožigosan s kompromitiranim ali deaktiviranim zasebnim ključem,

— na zahtevo generirajo nove pare ključev, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama, in generirajo ustrezna potrdila javnih ključev,

— nemudoma Komisiji uradno sporočijo nov seznam potrdil javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama.

V primeru, da so kompromitirani ali deaktivirani vsi zasebni ključi, ki ustrezajo potrdilom javnega ključa, ki se lahko uporabijo za potrjevanje veljavnosti podpisa zanesljivega seznama, in ki so bili uradno sporočeni Komisiji ter objavljeni v osrednjem seznamu kazalcev Komisije, države članice:

— generirajo nove pare ključev, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama, in generirajo ustrezna potrdila javnih ključev,

— brez odlašanja ponovno izdajo nov zanesljivi seznam, podpisan ali ožigosan z enim od navedenih novih zasebnih ključev, katerega ustrezno potrdilo javnega ključa je treba uradno sporočiti,

— nemudoma Komisiji uradno sporočijo nov seznam potrdil javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za podpisovanje ali žigosanje zanesljivega seznama.

POGLAVJE IV

TEHNIČNE SPECIFIKACIJE ZA ČLOVEKU BERLJIVO OBLIKO ZANESLJIVEGA SEZNAMA

Kadar je pripravljena in objavljena človeku berljiva oblika zanesljivega seznama, se zagotavlja v obliki datoteke Portable Document Format (PDF) v skladu z ISO 32000 ([1]), katere format mora ustrezati profilu PDF/A (ISO 19005 ([2])).

Vsebina zanesljivega seznama v človeku berljivi obliki na podlagi PDF/A mora izpolnjevati naslednje zahteve:

— struktura človeku berljive oblike upošteva logični model, opisan v TS 119 612,

— prikazano je vsako vsebovano polje, ki vključuje:

  — naziv polja (npr. „Identifikator vrste storitve“),

  — vrednost polja (npr. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}“),

  — pomen (opis) vrednosti polja, kadar je to primerno (npr. „Storitev generiranja potrdil, s katero se generirajo in podpisujejo kvalificirana potrdila na podlagi identitete in drugih značilnosti, ki jih preverjajo zadevne registracijske službe.“),

  — kadar je to primerno, več različic v naravnih jezikih, kot so določene v zanesljivem seznamu,

— naslednja polja in ustrezne vrednosti digitalnih potrdil ([3]), če so izpolnjene v polju „Digitalna identiteta storitve“, morajo biti prikazane vsaj v človeku v berljivi obliki:

  — Različica

  — Serijska številka potrdila

  — Algoritem za podpis

  — Izdajatelj – vsa ustrezna polja z razločevalnimi imeni

  — Obdobje veljavnosti

  — Imetnik – vsa ustrezna polja z razločevalnimi imeni

([1]) ISO 32000-1:2008: Upravljanje dokumentov – Portable document format – del 1: PDF 1.7.
([2]) ISO 19005-2:2011: Upravljanje dokumentov – Format datoteke elektronskega dokumenta za dolgotrajno hrambo – del 2: Uporaba ISO 32000-1 (PDF/A-2).
([3]) Priporočilo ITU-T X.509 | ISO/IEC 9594-8: Informacijska tehnologija – Medsebojno povezovanje odprtih sistemov – Register: Strukture potrdil javnih ključev in atributov (glej http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Javni ključ

— Identifikator izdajateljevega ključa

— Identifikator imetnikovega ključa

— Uporaba ključa

— Razširjena uporaba ključa

— Oznaka politike potrdila – vse enolične oznake politike in identifikatorji politike

— Določitve politike

— Alternativno ime imetnika

— Atributi direktorija imetnika

— Osnovne omejitve

— Politične omejitve

— Objava registra preklicanih potrdil ([1])

— Dostop do podatkov o overitelju

— Dostop do podatkov o imetniku

— Izjave, da je potrdilo kvalificirano ([2])

— Zgoščeni algoritem

— Zgoščena vrednost potrdila

— Človeku berljiva oblika mora biti enostavna za tiskanje.

— Človeku berljivo obliko podpiše ali ožigosa upravljavec sheme v skladu z naprednim podpisom PDF, določenim v členih 1 in 3 Izvedbenega sklepa Komisije (EU) 2015/1505.

([1]) RFC 5280: Potrdilo o infrastrukturi javnih ključev internet X. 509 PKI in profil registra preklicanih potrdil.
([2]) RFC 3739 internet X.509 PKI: Profil kvalificiranih potrdil.

PRILOGA II

PREDLOGA ZA URADNA OBVESTILA DRŽAV ČLANIC

Informacije, ki jih morajo države članice uradno sporočiti v skladu s členom 4(1) tega sklepa, vsebujejo naslednje podatke in vse njihove morebitne spremembe:

1. Država članica, ki uporablja kode ISO 3166-1 ([1]) Alpha 2 z naslednjimi izjemami:

   (a) koda države za Združeno kraljestvo je „UK“;

   (b) koda države za Grčijo je „EL“.

2. Organ oz. organi, odgovorni za sestavljanje, vodenje in objavo oblike zanesljivih seznamov, ki je primerna za avtomatizirano obdelavo, in zanesljivih seznamov v človeku berljivi obliki:

   (a) ime upravljavca sheme: zagotovljene informacije morajo biti enake vrednosti polja „Ime upravljavca sheme“ v zanesljivem seznamu, in sicer v vseh jezikih, ki se uporabljajo v zanesljivem seznamu (z ujemanjem velikih oziroma malih črk);

   (b) neobvezne informacije le za interno uporabe Komisije, kadar je treba stopiti v stik z zadevnim organom (informacije ne bodo objavljene na zbirnem seznamu Evropske komisije zanesljivih seznamov):

      — naslov upravljavca sheme,

      — kontaktni podatki odgovornih oseb (ime in priimek, telefon, e-naslov).

3. Kraj, kjer je objavljena oblika, primerna za avtomatizirano obdelavo zanesljivega seznama (*kraj, kjer je objavljen veljavni zanesljivi seznam*).

4. Kraj, kadar je to primerno, kjer je objavljen zanesljivi seznam v človeku berljivi obliki (*kraj, kjer je objavljen veljavni zanesljivi seznam*). Če zanesljivi seznam v človeku berljivi obliki ni več objavljen, se to navede.

5. Potrdila javnih ključev, ki ustrezajo zasebnim ključem, ki se lahko uporabljajo za elektronsko podpisovanje ali žigosanje oblike zanesljivega seznama, primerne za avtomatizirano obdelavo, in človeku berljive oblike zanesljivih seznamov: navedena potrdila se zagotovijo kot potrdila DER, prekodirana na način Base 64 v format PEM (Privacy Enhanced Mail). Ob uradnem obvestilu o spremembi se navedejo dodatne informacije, če se z novim potrdilom zamenja določeno potrdilo na seznamu Komisije in če se uradno sporočeno potrdilo doda k obstoječim, ne da bi se katero potrdilo zamenjalo.

6. Datum predložitve podatkov, ki se uradno sporočijo v točkah 1 do 5.

Podatki, uradno sporočeni v skladu s točkami 1, 2(a), 3, 4 in 5, se vključijo v zbirni seznam Evropske komisije zanesljivih seznamov, ki zamenja predhodno uradno sporočene informacije, vključene v navedeni zbirni seznam.

([1]) ISO 3166-1: „Kode za predstavljanje imen držav in njihovih podrejenih enot – 1. del: Kode držav“.

IZVEDBENI SKLEP KOMISIJE (EU) 2015/1506

z dne 8. septembra 2015

o določitvi specifikacij v zvezi s formati naprednih elektronskih podpisov in naprednih elektronskih žigov, ki jih priznajo organi javnega sektorja v skladu s členoma 27(5) in 37(5) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti členov 27(5) in 37(5) Uredbe,

ob upoštevanju naslednjega:

(1) Države članice morajo vzpostaviti potrebna tehnična sredstva za obdelavo elektronsko podpisanih dokumentov, zahtevanih pri uporabi spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu.

(2) Uredba (EU) št. 910/2014 zavezuje države članice, ki zahtevajo napredni elektronski podpis ali žig za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, da priznajo napredne elektronske podpise in žige, napredne elektronske podpise in žige, ki temeljijo na kvalificiranem potrdilu, ter kvalificirane elektronske podpise in žige v posebnih formatih ali drugih formatih, katerih veljavnost se potrjuje v skladu s posebnimi referenčnimi metodami.

(3) Za opredelitev posebnih formatov in referenčnih metod bi bilo treba upoštevati obstoječe prakse, standarde in pravne akte Unije.

(4) V Izvedbenem sklepu Komisije 2014/148/EU ([2]) je opredeljenih več najpogostejših formatov naprednih elektronskih podpisov, za katere morajo imeti države članice tehnično podporo, kadar se napredni elektronski podpisi zahtevajo za spletne upravne postopke. Namen določitve referenčnih formatov je olajšati čezmejno potrjevanje veljavnosti elektronskih podpisov in izboljšati čezmejno interoperabilnost elektronskih postopkov.

(5) Standardi iz Priloge k temu sklepu so obstoječi standardi za formate naprednih elektronskih podpisov. Zaradi tekočega pregleda v zvezi z oblikami dolgoročnega arhiviranja referenčnih formatov, ki ga izvajajo organi za standardizacijo, so standardi o dolgoročnem arhiviranju izključeni iz področja uporabe tega sklepa. Ko bo na voljo nova različica referenčnih standardov, bo pregledano sklicevanje na standarde in določbe v zvezi z dolgoročnim arhiviranjem.

(6) Napredni elektronski podpisi in napredni elektronski žigi so si s tehničnega vidika podobni. Zato bi se morali standardi za formate naprednih elektronskih podpisov smiselno uporabljati tudi za formate naprednih elektronskih žigov.

(7) Kadar se za podpisovanje ali žigosanje uporabljajo drugi formati elektronskih podpisov ali žigov, ki navadno niso tehnično podprti, bi bilo treba zagotoviti sredstva za potrjevanje veljavnosti, ki omogočajo čezmejno preverjanje elektronskih podpisov ali žigov. Da bi se države članice prejemnice lahko zanesle na navedena orodja za potrjevanje veljavnosti v drugi državi članici, je treba zagotoviti lahko dostopne informacije o navedenih orodjih za potrjevanje veljavnosti, tako da se informacije vključijo v elektronske dokumente, elektronske podpise ali vsebnike elektronskih dokumentov.

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

([2]) Izvedbeni sklep Komisije 2014/148/EU z dne 17. marca 2014 o spremembi Sklepa 2011/130/EU o določitvi minimalnih zahtev glede čezmejne obdelave dokumentov z elektronskim podpisom pristojnih organov v skladu z Direktivo 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu (UL L 80, 19.3.2014, str. 7).

(8) Kadar so v javnih službah države članice na voljo možnosti za potrjevanje veljavnosti elektronskega podpisa ali žiga, ki so primerne za avtomatizirano obdelavo, bi moral biti državi članici prejemnici omogočen dostop do takih možnosti za potrjevanje veljavnosti. Vendar pa ta sklep ne bi smel ovirati uporabe člena 27(1) in (2) ter člena 37(1) in (2) Uredbe (EU) št. 910/2014, kadar avtomatizirana obdelava možnosti za potrjevanje veljavnosti za alternativne metode ni mogoča.

(9) Za zagotovitev primerljivih zahtev za potrjevanje veljavnosti in krepitev zaupanja v možnosti potrjevanja veljavnosti, ki jih zagotavljajo države članice za druge formate elektronskih podpisov ali žigov, ki navadno niso tehnično podprti, zahteve glede orodij za potrjevanje veljavnosti iz tega sklepa izhajajo iz zahtev za potrjevanje veljavnosti kvalificiranih elektronskih podpisov in žigov iz členov 32 in 40 Uredbe (EU) št. 910/2014.

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

SPREJELA NASLEDNJI SKLEP:

Člen 1

Države članice, ki zahtevajo napredni elektronski podpis ali napredni elektronski podpis, ki temelji na kvalificiranem potrdilu iz člena 27(1) in (2) Uredbe (EU) št. 910/2014, priznajo napredne elektronske podpise XML, CMS ali PDF na ravni skladnosti B, T ali LT ali napredne elektronske podpise s pripadajočimi vsebniki podpisov, kadar so navedeni napredni elektronski podpisi v skladu s tehničnimi specifikacijami iz Priloge.

Člen 2

1. Države članice, ki zahtevajo napredni elektronski podpis ali napredni elektronski podpis, ki temelji na kvalificiranem potrdilu iz člena 27(1) in (2) Uredbe (EU) št. 910/2014, priznajo druge formate elektronskih podpisov, ki niso navedeni v členu 1 tega sklepa, če država članica, v kateri ima sedež ponudnik storitev zaupanja, ki ga uporablja podpisnik, drugim državam članicam zagotavlja možnosti za potrjevanje veljavnosti podpisa, ki so, kadar je to mogoče, primerne za avtomatizirano obdelavo.

2. Možnosti za potrjevanje veljavnosti podpisa:

(a) drugim državam članicam omogočajo, da potrjujejo veljavnost prejetih elektronskih podpisov prek spleta, brezplačno in na način, razumljiv tujim govorcem;

(b) so navedene v podpisanem dokumentu, v elektronskem podpisu ali vsebniku elektronskega dokumenta; in

(c) potrjujejo veljavnost naprednega elektronskega podpisa pod pogojem, da:

1. je bilo potrdilo, na katerem temelji napredni elektronski podpis, veljavno v času podpisovanja in, kadar napredni elektronski podpis temelji na kvalificiranem potrdilu, je bilo kvalificirano potrdilo, na katerem temelji napredni elektronski podpis, v času podpisovanja kvalificirano potrdilo za elektronski podpis v skladu s Prilogo I k Uredbi (EU) št. 910/2014 in ga je izdal ponudnik kvalificiranih storitev zaupanja;

2. podatki za potrjevanje veljavnosti podpisa ustrezajo podatkom, predloženim zanašajoči se stranki;

3. je enolični podatkovni niz, ki predstavlja podpisnika, pravilno predložen zanašajoči se stranki;

4. je zanašajoči se stranki jasno sporočeno, če je bil v času podpisa uporabljen psevdonim;

5. kadar je bil napredni elektronski podpis ustvarjen z napravo za ustvarjanje kvalificiranega elektronskega podpisa, je uporaba take naprave zanašajoči se stranki jasno sporočena;

6. celovitost podpisanih podatkov ni ogrožena;

7. so bile v času podpisa izpolnjene zahteve iz člena 26 Uredbe (EU) št. 910/2014;

8. sistem za potrjevanje veljavnosti naprednega elektronskega podpisa zanašajoči se stranki zagotavlja pravilne rezultate postopka potrjevanja veljavnosti in ji omogoča odkrivanje vseh zadevnih varnostnih vprašanj.

Člen 3

Države članice, ki zahtevajo napredni elektronski žig ali napredni elektronski žig, ki temelji na kvalificiranem potrdilu iz člena 37(1) in (2) Uredbe (EU) št. 910/2014, priznajo napredne elektronske žige XML, CMS ali PDF na ravni skladnosti B, T ali LT ali napredne elektronske žige s pripadajočimi vsebniki žigov, kadar so navedeni napredni elektronski žigi v skladu s tehničnimi specifikacijami iz Priloge.

Člen 4

1. Države članice, ki zahtevajo napredni elektronski žig ali napredni elektronski žig, ki temelji na kvalificiranem potrdilu iz člena 37(1) in (2) Uredbe (EU) št. 910/2014, priznajo druge formate elektronskih žigov, ki niso navedeni v členu 3 tega sklepa, če država članica, v kateri ima sedež ponudnik storitev zaupanja, ki ga uporablja ustvarjalec žiga, drugim državam članicam zagotavlja možnosti za potrjevanje veljavnosti žiga, ki so, kadar je to mogoče, primerne za avtomatizirano obdelavo.

2. Možnosti za potrjevanje veljavnosti žiga:

(a) drugim državam članicam omogočajo brezplačno spletno potrjevanje veljavnosti prejetih elektronskih žigov na način, ki je razumljiv tujim govorcem;

(b) so navedene v ožigosanem dokumentu, v elektronskem žigu ali vsebniku elektronskega dokumenta;

(c) potrjujejo veljavnost naprednega elektronskega žiga pod pogojem, da:

1. je bilo potrdilo, ki podpira napredni elektronski žig, veljavno v času žigosanja in, kadar napredni elektronski žig temelji na kvalificiranem potrdilu, je bilo kvalificirano potrdilo, na katerem temelji napredni elektronski žig, v času žigosanja kvalificirano potrdilo za elektronski žig v skladu s Prilogo III k Uredbi (EU) št. 910/2014 in ga je izdal ponudnik kvalificiranih storitev zaupanja;

2. podatki za potrjevanje veljavnosti žiga ustrezajo podatkom, predloženim zanašajoči se stranki;

3. je enolični podatkovni niz, ki predstavlja ustvarjalca žiga, pravilno predložen zanašajoči se stranki;

4. je zanašajoči se stranki jasno sporočeno, če je bil v času žigosanja uporabljen psevdonim;

5. kadar napredni elektronski žig ustvari naprava za ustvarjanje kvalificiranega elektronskega žiga, je uporaba take naprave zanašajoči se stranki jasno sporočena;

6. celovitost žigosanih podatkov ni ogrožena;

7. so bile v času žigosanja izpolnjene zahteve iz člena 36 Uredbe (EU) št. 910/2014;

8. uporabljeni sistem za potrjevanje veljavnosti naprednega elektronskega žiga zanašajoči se stranki zagotavlja pravilne rezultate postopka potrjevanja veljavnosti in ji omogoča odkrivanje vseh zadevnih varnostnih vprašanj.

Člen 5

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

Ta sklep je v celoti zavezujoč in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo
Predsednik
Jean-Claude JUNCKER

PRILOGA

Seznam tehničnih specifikacij za napredne elektronske podpise XML, CMS ali PDF ter pripadajoče vsebnike podpisa

Napredni elektronski podpisi iz člena 1 Sklepa morajo biti skladni z eno od naslednjih tehničnih specifikacij ETSI z izjemo določbe 9 specifikacij:

Osnovni profil XAdES	ETSI TS 103171 v.2.1.1 ([1])
Osnovni profil CAdES	ETSI TS 103173 v.2.2.1 ([2])
Osnovni 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

Pripadajoči vsebnik naprednega elektronskega podpisa iz člena 1 Sklepa mora biti skladen z naslednjimi tehničnimi specifikacijami ETSI:

Osnovni profil pripadajočega vsebnika podpisa	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

Seznam tehničnih specifikacij za napredne elektronske žige XML, CMS ali PDF ter pripadajoče vsebnike žiga

Napredni elektronski žigi iz člena 3 Sklepa morajo biti skladni z eno od naslednjih tehničnih specifikacij ETSI z izjemo določbe 9 specifikacij:

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

Pripadajoči vsebnik naprednega elektronskega žiga iz člena 3 Sklepa mora biti skladen z naslednjimi tehničnimi specifikacijami ETSI:

Osnovni profil pripadajočega vsebnika žiga	ETSI TS 103174 v.2.2.1

ISSN 1977-0804 (elektronska različica)
ISSN 1725-5155 (tiskana različica)

Urad za publikacije Evropske unije
2985 Luxembourg
LUKSEMBURG

SL