Официален вестник L 235

на Европейския съюз

Издание на български език

Законодателство

Година 58

9 септември 2015 г.

Съдържание

[1] Текст от значение за ЕИП

[1] Текст от значение за ЕИП

II

(Незаконодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1501 НА КОМИСИЯТА

от 8 септември 2015 година

относно рамката за оперативна съвместимост съгласно член 12, параграф 8 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 12, параграф 8 от него,

като има предвид, че:

(1) Съгласно член 12, параграф 2 от Регламент (ЕС) № 910/2014 следва да се създаде рамка за оперативна съвместимост с цел оперативна съвместимост на националните схеми за електронна идентификация, за които е извършено уведомяване съгласно член 9, параграф 1 от същия регламент (наричани по-долу „нотифицирани схеми“).

(2) Възлите играят централна роля във взаимното свързване на схемите за електронна идентификация на държавите членки. Тяхната роля е обяснена в документацията относно Механизма за свързване на Европа, създаден с Регламент (ЕС) № 1316/2013 на Европейския парламент и на Съвета ([2]), включително функциите и компонентите на „възел eIDAS“.

(3) Когато държава членка или Комисията предоставя софтуер, който позволява удостоверяване на автентичността във възел, функциониращ в друга държава членка, субектът, който предоставя и актуализира софтуера, използван за механизма за удостоверяване на автентичността, може да се споразумее със страната, която получава софтуера, за това как ще се управлява функционирането на този механизъм. Подобно споразумение не трябва да налага несъразмерни технически изисквания или разходи (включително за поддръжка, отговорности, хостинг и други разходи) на получаващата страна.

(4) Доколкото това е оправдано от прилагането на рамката за оперативна съвместимост, Комисията би могла да разработи, в сътрудничество с държавите членки, допълнителни технически спецификации, съдържащи подробности за техническите изисквания, посочени в настоящия регламент, като по-специално вземе предвид становищата на мрежата за сътрудничество, посочени в член 14, буква г) от Решение за изпълнение (ЕС) 2015/296 на Комисията ([3]). Тези спецификации следва да бъдат разработени като част от инфраструктурите за цифрови услуги съгласно Регламент (ЕС) № 1316/2013, който определя средствата за практическото осъществяване на градивен елемент за електронна идентификация.

([1]) ОВ L 257, 28.8.2014 г., стр. 73.

([2]) Регламент (ЕС) № 1316/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. за създаване на Механизъм за свързване на Европа, за изменение на Регламент (ЕС) № 913/2010 и за отмяна на регламенти (ЕО) № 680/2007 и (ЕО) № 67/2010 (ОВ L 348, 20.12.2013 г., стр. 129).

([3]) Решение за изпълнение (ЕС) 2015/296 на Комисията от 24 февруари 2015 г. за определяне на процедурни условия за сътрудничество между държавите членки по отношение на електронната идентификация съгласно член 12, параграф 7 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (ОВ L 53, 25.2.2015 г., стр. 14).

(5) Техническите изисквания, посочени в настоящия регламент, следва да са приложими независимо от каквито и да било промени в техническите спецификации, които може да бъдат разработени в съответствие с член 12 от настоящия регламент.

(6) Широкомащабният пилотен проект STORK, включително разработените по него спецификации, както и принципите и понятията, залегнали в Европейската рамка за оперативна съвместимост за европейските обществени услуги, бяха взети изцяло под внимание при изготвянето на разпоредбите на рамката за оперативна съвместимост, формулирана в настоящия регламент.

(7) Резултатите от сътрудничеството между държавите членки бяха взети изцяло под внимание.

(8) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 48 от Регламент (ЕО) № 910/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет

С настоящия регламент се определят техническите и оперативните изисквания на рамката за оперативна съвместимост, за да се гарантира оперативната съвместимост на схемите за електронна идентификация, нотифицирани от държавите членки на Комисията.

Тези изисквания включват по-специално:

а) минимални технически изисквания във връзка с нивата на осигуреност и категоризирането на националните нива на осигуреност на нотифицираните средства за електронна идентификация, издадени съгласно нотифицирани схеми за електронна идентификация по член 8 от Регламент (ЕС) № 910/2014, както е посочено в членове 3 и 4;

б) минимални технически изисквания за оперативна съвместимост, както е посочено в членове 5 и 8;

в) минималния набор от данни за идентификация на лица, представляващ по уникален начин дадено физическо или юридическо лице, както е посочено в член 11 и в приложението;

г) общи оперативни стандарти за сигурност, както е посочено в членове 6, 7, 9 и 10;

д) механизми за уреждане на спорове, както е посочено в член 13.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

(1) „възел“ означава точка на свързване, която е част от архитектурата за оперативна съвместимост на електронната идентификация и участва в трансграничното удостоверяване на автентичността на лица, като е в състояние да разпознава и обработва или препраща предавания на данни към други възли, с което дава възможност на националната инфраструктура за електронна идентификация на една държава членка да се свързва с националната инфраструктура за електронна идентификация на други държави членки;

(2) „оператор на възел“ означава субекта, който е отговорен за осигуряването на правилно и надеждно функциониране на възела като точка на свързване.

Член 3

Минимални технически изисквания във връзка с нивата на осигуреност

Минималните технически изисквания във връзка с нивата на осигуреност са определени в Регламент за изпълнение (ЕС) 2015/1502 на Комисията ([1]).

Член 4

Категоризиране на националните нива на осигуреност

Категоризирането на националните нива на осигуреност на нотифицираните схеми за електронна идентификация се извършва съгласно изискванията, определени в Регламент за изпълнение (ЕС) 2015/1502 на Комисията. Комисията се уведомява за резултатите от категоризирането, като се използва образецът за уведомление, предвиден в Решение за изпълнение (ЕС) 2015/1505 на Комисията ([2]).

Член 5

Възли

1. Възел в една държава членка трябва да е в състояние да се свързва с възли в други държави членки.

2. Възлите трябва да са в състояние да правят разграничение чрез технически средства между органите от обществения сектор и други доверяващи се страни.

3. Прилагането от една държава членка на техническите изисквания, посочени в настоящия регламент, не трябва да налага несъразмерни технически изисквания и разходи за други държави членки, за да постигнат те оперативна съвместимост с прилагането, възприето от тази държава членка.

Член 6

Защита и поверителност на данните

1. Осигурява се защитата на правото на личен живот и поверителността на обменените данни, както и запазването на целостността на предаваните между възлите данни, като се използват най-добрите налични технически решения и практики за защита.

2. Във възлите не се съхраняват никакви лични данни освен за целта, определена в член 9, параграф 3.

Член 7

Цялостност и автентичност на предаваните данни

При предаването на данни между възлите трябва да се осигури тяхната цялостност и автентичност, за да се гарантира, че всички запитвания и отговори са автентични и не са били манипулирани. За тази цел във възлите трябва да се използват решения, които са били успешно приложени в трансграничната оперативна работа.

([1]) Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 г. за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (вж. страница 7 от настоящия брой на Официален вестник).

([2]) Решение за изпълнение (ЕС) 2015/1505 на Комисията от 8 септември 2015 г. за определяне на техническите спецификации и форматите на доверителните списъци съгласно член 22, параграф 5 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (вж. страница 26 от настоящия брой на Официален вестник).

Член 8

Формат на съобщенията за комуникациите

Като синтаксис във възлите се използват общи формати на съобщенията въз основа на стандарти, които вече са употребявани нееднократно между държави членки и са с доказана приложимост в оперативна среда. Синтаксисът трябва да дава възможност за:

а) надлежна обработка на минималния набор от данни за идентификация на лица, представляващи по уникален начин дадено физическо или юридическо лице;

б) надлежна обработка на нивото на осигуреност на средствата за електронна идентификация;

в) разграничаване между органите от обществения сектор и другите доверяващи се страни;

г) гъвкавост, за да се задоволят нуждите от допълнителни специфични данни, свързани с идентификацията.

Член 9

Управление на информацията и метаданните във връзка със сигурността

1. Операторът на възела съобщава по сигурен и надежден начин метаданните за управление на възела в стандартизирана, пригодена за машинна обработка форма.

2. Най-малко параметрите, свързани със сигурността, се извличат автоматично.

3. Операторът на възела съхранява данни, които в случай на инцидент дават възможност да се възстанови последователността на обмен на съобщения, за да се определят мястото и естеството на инцидента. Данните се съхраняват за определен период от време в съответствие с националните изисквания и се състоят, като минимум, от следните елементи:

а) идентификатор на възела;

б) идентификатор на съобщенията;

в) дата и час на съобщенията.

Член 10

Стандарти за осигуреност и сигурност на информацията

1. Операторът на възел, предоставящ удостоверяване на автентичността, доказва, че спрямо възлите, участващи в рамката за оперативна съвместимост, този възел отговаря на изискванията на стандарт ISO/IEC 27001 чрез сертифициране или по равностойни методи за оценка, или в съответствие с националното законодателство.

2. Операторите на възли извършват без излишно забавяне актуализациите, които са от критично значение за сигурността.

Член 11

Данни за идентификация на лица

1. Минималният набор от данни за идентификация на лица, представляващ по уникален начин дадено физическо или юридическо лице, трябва да отговаря на изискванията, посочени в приложението, когато се използва в трансграничен контекст.

2. Минималният набор от данни за дадено физическо лице, представляващо юридическо лице, трябва да съдържа комбинация от специфичните данни, които са изброени в приложението, за физически и юридически лица, когато се използва в трансграничен контекст.

3. Данните се предават с оригиналните писмени знаци, а ако е целесъобразно — и с транслитерация на латиница.

Член 12

Технически спецификации

1. Когато това е оправдано от процеса на въвеждане на рамката за оперативна съвместимост, мрежата за сътрудничество, създадена с Решение за изпълнение (ЕС) 2015/296, може да приема становища съгласно член 14, буква г) от него относно необходимостта от разработване на технически спецификации. Тези технически спецификации предоставят допълнителни подробности относно техническите изисквания, посочени в настоящия регламент.

2. Съгласно становището, посочено в параграф 1, Комисията, в сътрудничество с държавите членки, разработва техническите спецификации като част от инфраструктурите за цифрови услуги по Регламент (ЕС) № 1316/2013.

3. Мрежата за сътрудничество приема становище в съответствие с член 14, буква г) от Решение за изпълнение (ЕС) 2015/296, в който тя оценява дали и до каква степен техническите спецификации, разработени съгласно параграф 2, отговарят на нуждите, установени в посоченото в параграф 1 становище, или на изискванията, определени в настоящия регламент. Тя може да препоръча на държавите членки да се съобразяват с техническите спецификации, когато прилагат рамката за оперативна съвместимост.

4. Комисията предоставя примерно тълкуване на прилагането на техническите спецификации. Държавите членки могат да прилагат това примерно тълкуване или да го използват като образец при изпробването на други прилагания на техническите спецификации.

Член 13

Разрешаване на спорове

1. По възможност всички спорове относно рамката за оперативна съвместимост следва да се разрешават от самите засегнати държави членки чрез преговори.

2. Ако не се постигне решение в съответствие с параграф 1, мрежата за сътрудничество, създадена съгласно член 12 от Решение за изпълнение (ЕС) 2015/296, е компетентна да се произнесе по спора в съответствие със своя процедурен правилник.

Член 14

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 8 септември 2015 година.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

Изисквания относно минималния набор от данни за идентификация на лица, представляващ по уникален начин дадено физическо или юридическо лице, посочен в член 11

1. **Минимален набор от данни за физическо лице**

Минималният набор от данни за физическо лице трябва да съдържа всички изброени по-долу задължителни специфични данни:

а) настоящо фамилно име (или имена);

б) настоящо собствено име (или имена);

в) дата на раждане;

г) уникален идентификатор, създаден от изпращащата държава членка в съответствие с техническите спецификации за целите на трансграничната идентификация, който да остава непроменен, колкото е възможно по-дълго време.

Минималният набор от данни за физическо лице може да съдържа допълнителни специфични данни по една или повече от следните позиции:

а) собствено име (или имена) и фамилно име (или имена) по рождение;

б) място на раждане;

в) настоящ адрес;

г) пол.

2. **Минимален набор от данни за юридическо лице**

Минималният набор от данни за юридическо лице трябва да съдържа всички изброени по-долу задължителни специфични данни:

а) настоящо юридическо наименование;

б) уникален идентификатор, създаден от изпращащата държава членка в съответствие с техническите спецификации за целите на трансграничната идентификация, който да остава непроменен, колкото е възможно по-дълго време.

Минималният набор от данни за юридическо лице може да съдържа допълнителни специфични данни по една или повече от следните позиции:

а) настоящ адрес;

б) регистрационен номер по ДДС;

в) данъчен номер;

г) идентификационен код съгласно член 3, параграф 1 от Директива 2009/101/ЕО на Европейския парламент и на Съвета ([1]);

д) идентификационен код на правния субект (ИКПС), посочен в Регламент за изпълнение (ЕС) № 1247/2012 на Комисията ([2]);

е) идентификационен номер на икономически оператор (EORI номер), посочен в Регламент за изпълнение (ЕС) № 1352/2013 на Комисията ([3]);

ж) акцизен номер, предвиден в член 2, параграф 12 от Регламент № 389/2012 на Съвета ([4]).

([1]) Директива 2009/101/ЕО на Европейския парламент и на Съвета от 16 септември 2009 г. за координиране на гаранциите, които държавите-членки изискват от дружествата по смисъла на член 48, втора алинея от Договора, за защита на интересите на членовете и на трети лица с цел тези гаранции да станат равностойни (ОВ L 258, 1.10.2009 г., стр. 11).

([2]) Регламент за изпълнение (ЕС) № 1247/2012 на Комисията от 19 декември 2012 г. за установяване на технически стандарти за изпълнение по отношение на формата и периодичността на отчетите за трансакциите, предавани на регистрите на трансакции съгласно Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета относно извънборсовите деривати, централните контрагенти и регистрите на трансакции (ОВ L 352, 21.12.2012 г., стр. 20).

([3]) Регламент за изпълнение (ЕС) № 1352/2013 на Комисията от 4 декември 2013 г. за установяване на формулярите, предвидени в Регламент (ЕС) № 608/2013 на Европейския парламент и на Съвета относно защитата на правата върху интелектуалната собственост, осъществявана от митническите органи (ОВ L 341, 18.12.2013 г., стр. 10).

([4]) Регламент (ЕС) № 389/2012 на Съвета от 2 май 2012 г. относно административното сътрудничество в областта на акцизите и за отмяна на Регламент (ЕО) № 2073/2004 (ОВ L 121, 8.5.2012 г., стр. 1).

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1502 НА КОМИСИЯТА

от 8 септември 2015 година

за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 8, параграф 3 от него,

като има предвид, че:

(1) Съгласно член 8 от Регламент (ЕС) № 910/2014 за всяка схема за електронна идентификация, за която е извършено уведомяване съгласно член 9, параграф 1, (наричана по-долу „нотифицирана схема"), трябва да се определят нива на осигуреност „ниско", „значително" и „високо" за средствата за електронна идентификация, издадени по тази схема.

(2) Определянето на минималните технически спецификации, стандарти и процедури е от съществено значение, за да се гарантира общоприето разбиране на данните за нивата на осигуреност, както и да се гарантира оперативната съвместимост при категоризирането на националните нива на осигуреност на нотифицираните схеми за електронна идентификация спрямо нивата на осигуреност съгласно член 8, както е предвидено в член 12, параграф 4, буква б) от Регламент (ЕС) № 910/2014.

(3) Спецификациите и процедурите, посочени в настоящия акт за изпълнение, са съобразени с международния стандарт ISO/IEC 29115, тъй като той е основният международен стандарт в областта на нивата на осигуреност за средствата за електронна идентификация. Съдържанието на Регламент (ЕС) № 910/2014 обаче се различава от този международен стандарт, по-специално по отношение на изискванията за доказване и проверка на самоличността, както и в начина, по който са взети под внимание различията между разпоредбите на държавите членки за самоличността и съществуващите инструменти в ЕС за същата цел. Поради това приложението следва да се основава на този международен стандарт, но без позоваване към конкретно съдържание на ISO/IEC 29115.

(4) Настоящият регламент беше разработен по основан на резултатите подход като най-подходящ за целта, което се отразява и в определенията за термини и понятия. Те са съобразени с целта на Регламент (ЕС) № 910/2014 по отношение на нивата на осигуреност на средствата за електронна идентификация. Поради това широкомащабният пилотен проект STORK, включително разработените по него спецификации, както и определенията и понятията в ISO/IEC 29115, следва да бъдат взети под особено внимание при установяването на спецификациите и процедурите, посочени в настоящия акт за изпълнение.

(5) В зависимост от контекста, в който трябва да бъде проверен даден аспект на доказателството за самоличността, достоверните източници могат да са в множество различни форми, включително регистри, документи и органи. Достоверните източници могат да се различават в зависимост от държавата членка дори в сходен контекст.

(6) Изискванията за доказване и проверка на самоличността следва да са съобразени с различните системи и практики, като същевременно се гарантира достатъчно висока осигуреност, за да се установи необходимото доверие. Поради това приемането на процедури, използвани преди за цел, различна от издаването на средства за електронна идентификация, следва да бъде обвързано с условия за потвърждение, че тези процедури отговарят на изискванията, предвидени за съответното ниво на осигуреност.

([1]) ОВ L 257, 28.8.2014 г., стр. 73.

(7) Обикновено за удостоверяване на автентичността се използват някои фактори като споделени тайни, физически устройства и физически характеристики. Следва да се насърчава обаче използването на по-голям брой фактори за удостоверяване на автентичността — особено на фактори от различни категории, за да да се повиши сигурността на процеса на удостоверяване на автентичността.

(8) Настоящият регламент не следва да засяга правата за представителство на юридически лица. Въпреки това в приложението следва да са предвидени изисквания за обвързването между средствата за електронна идентификация на физически и юридически лица.

(9) Следва да се отчете значението на системите за информационна сигурност и за управление на услуги, както и важността на използването на общоприети методики и на прилагането на принципите, заложени в стандарти като ISO/IEC 27000 и тези от серията ISO/IEC 20000.

(10) Добрите практики във връзка с нивата на осигуреност в държавите членки също следва да бъдат взети предвид.

(11) Сертифицирането на сигурността на информационните технологии (ИТ) на базата на международни стандарти е важен инструмент за проверка на това дали по отношение на сигурността продуктите отговарят на изискванията на настоящия акт за изпълнение.

(12) Комитетът, посочен в член 48 от Регламент (ЕС) № 910/2014, не е представил становище в срока, определен от неговия председател,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

1. Нивата на осигуреност „ниско“, „значително“ и „високо“ за средствата за електронна идентификация, издадени по нотифицирана схема за електронна идентификация, се определят с позоваване на спецификациите и процедурите, посочени в приложението.

2. Спецификациите и процедурите, посочени в приложението, се използват за установяване на нивото на осигуреност на средствата за електронна идентификация, издадени по нотифицирана схема за електронна идентификация, като се определят надеждността и качеството на следните елементи:

а) вписването, както е посочено в раздел 2.1 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, буква а) от Регламент (ЕС) № 910/2014;

б) управлението на средствата за електронна идентификация, както е посочено в раздел 2.2 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, букви б) и е) от Регламент (ЕС) № 910/2014;

в) удостоверяването на автентичността, както е посочено в раздел 2.3 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, буква в) от Регламент (ЕС) № 910/2014;

г) управлението и организацията, както е посочено в раздел 2.4 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, букви г) и д) от Регламент (ЕС) № 910/2014.

3. Когато средството за електронна идентификация, издадено по нотифицирана схема за електронна идентификация, отговаря на изискване, посочено за по-високо ниво на осигуреност, тогава се счита, че средството изпълнява равностойното изискване за по-ниско ниво на осигуреност.

4. Освен ако е указано друго в съответната част на приложението, за съответствие със заявеното ниво на осигуреност трябва да са налице всички елементи, изброени в приложението за определено ниво на осигуреност на средствата за електронна идентификация, издадени по нотифицирана схема за електронна идентификация.

Член 2

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 8 септември 2015 година.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

Технически спецификации и процедури за нивата на осигуреност „ниско“, „значително“ и „високо“ за средства за електронна идентификация, издадени по нотифицирана схема за електронна идентификация

1. **Приложими определения**

За целите на наістоящото приложение се прилагат следните определения:

1) „достоверен източник“ означава който и да е източник, независимо от неговата форма, на който може да се разчита за получаването на точни данни, информация и/или факти, които могат да бъдат използвани, за да се докаже самоличността;

2) „фактор за удостоверяване на автентичността“ означава фактор, потвърден като свързан с дадено лице, който попада в една от следните категории:

   а) „фактор въз основа на притежание“ означава фактор за удостоверяване на автентичността, когато от субекта се изисква да докаже притежанието си върху него;

   б) „фактор въз основа на познаване“ означава фактор за удостоверяване на автентичността, когато от субекта се изисква да докаже познаването му;

   в) „присъщ фактор за удостоверяване на автентичността“ означава фактор, който се основава на физически атрибут на физическо лице и от субекта се изисква да докаже, че притежава този физически атрибут;

3) „динамично удостоверяване на автентичността“ означава електронен процес, при който се използва криптография или друга техника, която осигурява начин за създаване по заявка на електронно потвърждение, че субектът контролира или притежава данните за идентификация, и който се променя с всяко удостоверяване на автентичността между субекта и системата, проверяваща самоличността на субекта;

4) „система за управление на информационната сигурност“ означава набор от процеси и процедури, предназначени за управление до приемливи нива на рисковете, свързани с информационната сигурност.

2. **Технически спецификации и процедури**

Елементите на техническите спецификации и процедури, описани в настоящото приложение, се използват, за да се определи по какъв начин изискванията и критериите съгласно член 8 от Регламент (ЕС) № 910/2014 да се прилагат за средствата за електронна идентификация, издадени по схема за електронна идентификация.

2.1. *Вписване*

2.1.1. Заявяване и регистриране

Ниво на осигуреност	Необходими елементи
Ниско	1. Уверяване, че заявителят е запознат с реда и условията във връзка с използването на средствата за електронна идентификация. 2. Уверяване, че заявителят е запознат с препоръчаните предпазни мерки за сигурност във връзка със средствата за електронна идентификация. 3. Събиране на съответните данни за самоличност, изисквани за доказване и проверка на самоличността.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.1.2. Доказване и проверка на самоличността (физическо лице)

Ниво на осигуреност	Необходими елементи
Ниско	1. Може да се приеме, че лицето разполага с доказателство, което е признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, и удостоверява заявената самоличност. 2. Доказателството може да се приеме за неподправено или за съществуващо съгласно достоверен източник и изглежда да е валидно. 3. От достоверен източник е известно, че заявената самоличност съществува, и може да се приеме, че лицето, което претендира за тази самоличност, съвпада с нея.
Значително	Трябва да бъдат изпълнени изискванията за нивото „ниско“, плюс една от алтернативите, изброени в точки 1—4: 1. Лицето е било проверено, че разполага с доказателство, което е признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, и удостоверява заявената самоличност; както и доказателството се проверява, за да се определи дали е неподправено; или, съгласно достоверен източник, е известно, че съществува и се отнася за действително лице; както и са били предприети стъпки, за да се сведе до минимум рискът самоличността на лицето да не съответства на заявената самоличност, като се отчита например рискът доказателството да е загубено, откраднато, с прекратена валидност, отменено или с изтекъл срок; или 2. По време на процеса на регистрация е представен документ за самоличност, издаден в същата държава членка, и документът изглежда се отнася за представилото го лице; както и са били предприети стъпки, за да се сведе до минимум рискът самоличността на лицето да не съответства на заявената самоличност, като се отчита например рискът документът да е загубен, откраднат, с прекратена валидност, отменен или с изтекъл срок; или 3. Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.2 за нивото „значително“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета [1], или от равностоен орган; или 4. Когато средствата за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „значително“ или „високо“, като се вземат под внимание рисковете от промяна в данните за идентификация на лицето, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „значително“ или „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган.

Ниво на осигуреност	Необходими елементи
Високо	Трябва да бъдат изпълнени изискванията или на точка 1, или на точка 2: 1. Трябва да бъдат изпълнени изискванията за нивото „значително“ плюс една от алтернативите, изброени в букви от а) до в): а) Когато лицето е проверено, че притежава снимково или биометрично доказателство за идентификация, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, и удостоверява заявената самоличност, доказателството се проверява, за да се установи дали то е валидно според достоверен източник; както и заявителят е идентифициран със заявената самоличност чрез сравняване на една или повече физически характеристики на лицето с достоверен източник; или б) Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.2 за нивото „високо“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; както и са предприети стъпки, за да се покаже, че резултатите от по-ранните процедури остават валидни; или в) Когато средства за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „високо“, като се вземат под внимание рисковете от промяна в данните за идентификация на лицето, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; както и са предприети стъпки, за да се покаже, че резултатите от тази предходна процедура на издаване на нотифицирано средство за електронна идентификация остават валидни. ИЛИ 2. Когато заявителят не представи признато снимково или биометрично доказателство за идентификация, за получаване на такова признато снимково или биометрично доказателство за идентификация се прилагат абсолютно същите процедури, използвани на национално равнище в държавата членка на субекта, отговорен за регистрацията.

([1]) Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).

2.1.3. Доказване и проверка на самоличността (юридическо лице)

Ниво на осигуреност	Необходими елементи
Ниско	1. За заявената самоличност на юридическото лице се показва доказателство, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация.

Ниво на осигуреност	Необходими елементи
	2. Доказателството изглежда валидно и може да се приеме, че е неподправено или съществуващо съгласно достоверен източник, когато включването на юридическо лице в достоверния източник е доброволно и се урежда чрез договореност между юридическото лице и достоверния източник. 3. Не е известно от достоверен източник юридическото лице да се намира в състояние, което би го възпрепятствало да действа в това си качество.
Значително	Трябва да бъдат изпълнени изискванията за нивото „ниско“, плюс една от алтернативите, изброени в точки 1—3: 1. За заявената самоличност на юридическото лице се показва доказателство, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, включващо наименованието на юридическото лице, правната му форма и (ако е приложимо) неговия регистрационен номер; и доказателството се проверява, за да се определи дали то е неподправено или е известно като съществуващо съгласно достоверен източник, когато за дейността на юридическото лице в съответния сектор се изисква включването му в достоверния източник; както и са били предприети стъпки, за да се сведе до минимум рискът самоличността на юридическото лице да не съответства на заявената самоличност, като се отчита например рискът съответните документи да са загубени, откраднати, с прекратена валидност, отменени или с изтекъл срок; или 2. Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.3 за нивото „значително“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; или 3. Когато средства за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „значително“ или „високо“, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „значително“ или „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган.
Високо	Трябва да бъдат изпълнени изискванията за нивото „значително“, плюс една от алтернативите, изброени в точки 1—3: 1. За заявената самоличност на юридическото лице се представя доказателство, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, включващо наименованието на юридическото лице, правната му форма и най-малко един уникален идентификатор, представляващ юридическото лице и използван в национален контекст; и доказателството се проверява, за да се определи дали то е валидно съгласно достоверен източник; или

Ниво на осигуреност	Необходими елементи
	2. Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.3 за нивото „високо“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; и са предприети стъпки, за да се покаже, че резултатите от тази предходна процедура остават валидни; или 3. Когато средства за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „високо“, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; и са предприети стъпки, за да се покаже, че резултатите от тази предходна процедура на издаване на нотифицирано средство за електронна идентификация остават валидни.

2.1.4. Свързване между средствата за електронна идентификация на физически и на юридически лица

Когато е приложимо, за свързването между средствата за електронна идентификация на физическо лице и средствата за електронна идентификация на юридическо лице (наричано по-долу „свързването“) са в сила следните условия:

1) Трябва да е възможно да се прекрати временно и/или отмени свързването. Жизненият цикъл на свързването (например активиране, временно спиране, подновяване, отмяна) се управлява съгласно национално признати процедури.

2) Физическото лице, чието средство за електронна идентификация е свързано със средство за електронна идентификация на юридическото лице, може да делегира упражняването на свързването с друго физическо лице въз основа на национално признати процедури. Делегиращото физическо лице обаче продължава да носи отговорността.

3) Свързването се извършва по следния начин:

Ниво на осигуреност	Необходими елементи
Ниско	1. Проверява се дали доказването на самоличността на физическото лице, действащо от името на юридическото лице, е било извършено на ниво „ниско“ или по-високо. 2. Свързването е било осъществено въз основа на национално признати процедури. 3. Не е известно от достоверен източник физическото лице да се намира в състояние, което би го възпрепятствало да действа от името на юридическото лице.
Значително	Като точка 3 за ниво „ниско“, плюс: 1. Проверява се дали доказването на самоличността на физическото лице, действащо от името на юридическото лице, е било извършено на ниво „значително“ или „високо“.

Ниво на осигуреност	Необходими елементи
	2. Свързването е било осъществено въз основа на национално признати процедури, което е довело до регистриране на свързването в достоверен източник. 3. Свързването е било проверено въз основа на информация от достоверен източник.
Високо	Като точка 3 за ниво „ниско“ и точка 2 за ниво „значително“, плюс: 1. Проверява се дали доказването на самоличността на физическото лице, действащо от името на юридическото лице, е било извършено на ниво „високо“. 2. Свързването е било проверено въз основа на уникален идентификатор, представляващ юридическото лице и използван в националния контекст; и въз основа на информация от достоверен източник, представляваща по уникален начин физическото лице.

2.2. *Управление на средствата за електронна идентификация*

2.2.1. Характеристики и структура на средствата за електронна идентификация

Ниво на осигуреност	Необходими елементи
Ниско	1. При средството за електронна идентификация се използва най-малко един фактор за удостоверяване на автентичността. 2. Средството за електронна идентификация се проектира така, че издателят да предприема подходящи мерки, за да проверява, че то се използва само под контрола или във притежанието на лицето, на което принадлежи.
Значително	1. При средството за електронна идентификация се използват най-малко два фактора от различни категории за удостоверяване на автентичността. 2. Средството за електронна идентификация се проектира така, че да може да се приеме, че то се използва само под контрола или във притежанието на лицето, на което принадлежи.
Високо	Както за ниво „значително“, плюс: 1. Средството за електронна идентификация защитава срещу дублиране и подправяне, както и срещу нападатели с голям потенциал за атаки. 2. Средството за електронна идентификация е проектирано така, че лицето, на което принадлежи, да може да го защити надеждно срещу използване от други лица.

2.2.2. Издаване, предоставяне и активиране

Ниво на осигуреност	Необходими елементи
Ниско	След издаването му средството за електронна идентификация се предоставя по начин, за който може да се приеме, че гарантира получаване единствено от лицето, за което е предназначено.
Значително	След издаването на средството за електронна идентификация то се предоставя по начин, за който може да се приеме, че гарантира получаване единствено от лицето, на което принадлежи.
Високо	В процеса на активиране се проверява дали средството за електронна идентификация е било получено единствено от лицето, на което принадлежи.

2.2.3. Временно спиране на действието, отнемане и повторно активиране

Ниво на осигуреност	Необходими елементи
Ниско	1. Възможно е по своевременен и ефективен начин да се прекрати временно действието на дадено средство за електронна идентификация и/или то да се отнеме. 2. Наличието на мерки, предприети за предотвратяване на неразрешено временно спиране на действието, отнемане и/или повторно активиране. 3. Повторно активиране се извършва само ако продължава спазването на същите изисквания за осигуреност, както установените преди временното спиране на действието или отнемането.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.2.4. Подновяване и замяна

Ниво на осигуреност	Необходими елементи
Ниско	Като се вземат предвид рисковете от промяна в данните за идентификация на лицето, подновяването или замяната трябва да отговарят на същите изисквания за осигуреност, както първоначалното доказване и проверка на самоличността, или да се основава на валидно средство за електронна идентификация със същото или по-високо ниво на осигуреност.
Значително	Същите, както за нивото „ниско“.
Високо	Както за ниво „ниско“, плюс: Когато подновяването или замяната се основава на валидно средство за електронна идентификация, данните за самоличността се проверяват чрез достоверен източник.

2.3. *Удостоверяване на автентичността*

Настоящият раздел е посветен на заплахите, свързани с използването на механизма за удостоверяване на автентичността, и се изброяват изискванията за всяко ниво на осигуреност. За контролните мерки по настоящия раздел се подразбира, че те трябва да бъдат съизмерими с рисковете за даденото ниво.

2.3.1. Механизъм за удостоверяване на автентичността

В таблицата по-долу са посочени изискванията за отделните нива на осигуреност по отношение на механизма за удостоверяване на автентичността, чрез който физическото или юридическото лице използва средството за електронна идентификация, за да потвърди своята самоличност пред доверяваща се страна.

Ниво на осигуреност	Необходими елементи
Ниско	1. Разкриването на данни за идентификацията на лицето се предхожда от надеждна проверка на средството за електронна идентификация и неговата валидност. 2. Когато данните за идентификация на лица се съхраняват като част от механизма за удостоверяване на автентичността, тази информация се защитава срещу загуба и срещу компрометиране, включително анализ офлайн. 3. Механизмът за удостоверяване на автентичността осъществява контролни мерки за сигурност за проверката на средството за електронна идентификация, така че е много малко вероятно нападател с повишен базов потенциал за атака да може чрез дейности като налучкване, подслушване, възпроизвеждане или манипулиране на комуникацията да злоупотреби с механизма за удостоверяване на автентичността.

Ниво на осигуреност	Необходими елементи
Значително	Както за ниво „ниско“, плюс: 1. Разкриването на данни за идентификацията на лицето се предхожда от надеждна проверка на средството за електронна идентификация и неговата валидност чрез динамично удостоверяване на автентичността. 2. Механизмът за удостоверяване на автентичността осъществява контролни мерки за сигурност за проверката на средството за електронна идентификация, така че е много малко вероятно нападател с умерен потенциал за атака да може чрез дейности като налучкване, подслушване, възпроизвеждане или манипулиране на комуникацията да злоупотреби с механизма за удостоверяване на автентичността.
Високо	Както за ниво „значително“, плюс: Механизмът за удостоверяване на автентичността осъществява контролни мерки за сигурност за проверката на средството за електронна идентификация, така че е много малко вероятно нападател с голям потенциал за атака да може чрез дейности като налучкване, подслушване, възпроизвеждане или манипулиране на комуникацията да злоупотреби с механизма за удостоверяване на автентичността.

2.4. *Управление и организация*

Всички участници, предоставящи услуга, свързани с електронната идентификация в трансграничен контекст (наричани по-долу „доставчици“), трябва да разполагат с документирани практики и политики за управление на информационната сигурност, подходи за управление на риска и други признати контролни мерки, така че да предоставят гаранции пред компетентните органи по управление за схеми за електронна идентификация в съответните държави членки, че са налице ефективни практики. За всички изисквания/елементи в целия раздел 2.4 се подразбира, че те трябва да бъдат съизмерими с рисковете за даденото ниво.

2.4.1. Общи разпоредби

Ниво на осигуреност	Необходими елементи
Ниско	1. Доставчикът, предоставящ оперативна услуга, попадаща в обхвата на настоящия регламент, е държавен орган или правен субект, признат като такъв от националното право на държава членка, с установена организация и дейност във всички области, които имат отношение към предоставянето на услугата. 2. Доставчиците спазват всички правни изисквания, приложими за тях, във връзка с изпълнението и предоставянето на услугата, включително по отношение на видовете информация, в които може да се търси, как се извършва доказването на самоличността, каква информация може да бъде запазена и за какъв период от време. 3. Доставчиците са в състояние да докажат способността си да поемат риска от възникване на отговорност за причинени щети, както и да притежават достатъчно финансови ресурси за непрекъснато изпълнение и предоставяне на услугите. 4. Доставчиците носят отговорност за изпълнението на всички задължения, възложени на друг субект, и за спазването на политиката за схемата, все едно че те самите са изпълнявали задълженията. 5. За схемите за електронна идентификация, които не са учредени съгласно националното право, трябва да е налице ефективен план за прекратяването им. Такъв план трябва да включва надлежно прекратяване на услугата или продължаване от друг доставчик; начина, по който се информират за това съответните органи и крайните потребители, както и подробности относно начина, по който записите следва да бъдат защитени, запазени и унищожени в съответствие с политиката за схемата.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.2. Публикувани известия и информация за потребителите

Ниво на осигуреност	Необходими елементи
Ниско	1. Наличието на публикувано определение за услугата, което включва всички приложими условия, ред и такси, както и всички ограничения за нейното използване. Определението за услугата трябва да включва политика за защита на правото на личен живот. 2. Трябва да бъдат въведени подходяща политика и процедури, за да се гарантира, че ползвателите на услугата са информирани по своевременен и надежден начин за всяка промяна в определението за посочената услуга и във всички приложими условия, ред и политика за защита на личния живот във връзка с тази услуга. 3. Трябва да бъдат въведени подходяща политика и процедури, които да осигуряват пълни и правилни отговори на исканията за информация.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.3. Управление на информационната сигурност

Ниво на осигуреност	Необходими елементи
Ниско	За управлението и контрола на рисковете, свързани със сигурността на информацията, съществува ефективна система за управление на информационната сигурност.
Значително	Както за ниво „ниско“, плюс: Системата за управление на информационната сигурност е съобразена с изпитани стандарти или принципи за управление и контрол на рисковете, свързани със сигурността на информацията.
Високо	Същите, както за нивото „значително“.

2.4.4. Водене на отчетност

Ниво на осигуреност	Необходими елементи
Ниско	1. Записване и съхраняване на значима информация посредством ефективна система за управление на записите, като се вземат предвид приложимото законодателство и добрите практики по отношение на защитата и запазването на данните. 2. Запазване, доколкото това е разрешено от националното законодателство или други национални административни разпоредби, и защита на записите за срок, съобразен с нуждите на одита, разследването на пробиви в сигурността и съхранението на данни, след което записите се унищожават по сигурен начин.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.5. Съоръжения и персонал

В следващата таблица са посочени изискванията по отношение на съоръженията и персонала и, ако е приложимо, подизпълнителите, които поемат задължения, обхванати от настоящия регламент. Спазването на всяко от изискванията трябва да е пропорционално на степента на рисковете, свързани с предоставяното ниво на осигуреност.

Ниво на осигуреност	Необходими елементи
Ниско	1. Наличието на процедури, с които се гарантира, че персоналът и подизпълнителите са достатъчно обучени, квалифицирани и опитни за уменията, необходими за изпълнението на своите роли. 2. Наличието на достатъчен персонал и подизпълнители за адекватно изпълнение и поддържане на услугата съгласно политиките и процедурите за нея. 3. Съоръженията, използвани за предоставянето на услугата, са под непрекъснато наблюдение за предпазване от щети, причинени от екологични инциденти, неразрешен достъп и други фактори, които могат да повлияят на сигурността на услугата. 4. Съоръженията, използвани за предоставянето на услугата, осигуряват ограничаването до оправомощени служители или подизпълнители на достъпа до зоните за съхранение или обработка на лична, криптографска или друга чувствителна информация.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.6. Технически проверки

Ниво на осигуреност	Необходими елементи
Ниско	1. Наличието на пропорционални технически проверки за управление на рисковете за сигурността на услугите с цел с цел защита на обработваната информация по отношение на нейната поверителност, цялостност и разполагаемост. 2. Електронните канали за комуникация, които се използват за обмен на лична или чувствителна информация, са защитени срещу подслушване, манипулиране и възпроизвеждане. 3. Достъпът до чувствителен криптографски материал, ако се използва такъв за издаване на средства за електронна идентификация и за удостоверяване на автентичност, е ограничен до роли и приложения, за които този достъп е абсолютно необходим. Трябва да се гарантира, че такъв материал никога не се съхранява продължително време като некодиран текст. 4. Съществуват процедури, за да се гарантира постоянно поддържане на сигурността, а също е налице способност да се реагира на промени в нивата на риска, инциденти и пробиви в сигурността. 5. Всички носители, съдържащи лична, криптографска или друга чувствителна информация, се съхраняват, транспортират и унищожават по сигурен и безопасен начин.
Значително	Същите, както за нивото „ниско“, плюс: Ако за издаване на средства за електронна идентификация и за удостоверяване на автентичност се използва чувствителен криптографски материал, той е защитен срещу подправяне.
Високо	Същите, както за нивото „значително“.

2.4.7. Спазване и одит

Ниво на осигуреност	Необходими елементи
Ниско	Наличие на периодични вътрешни одити, обхващащи всички части, които са от значение за предоставянето на услугите, за да се гарантира спазването на съответната политика.

Ниво на осигуреност	Необходими елементи
Значително	Наличие на периодични независими вътрешни или външни одити, обхващащи всички части, които са от значение за предоставянето на услугите, за да се гарантира спазването на съответната политика.
Високо	1. Наличие на периодични независими външни одити, обхващащи всички части, които са от значение за предоставянето на услугите, за да се гарантира спазването на съответната политика. 2. Когато дадена схема се управлява пряко от държавен орган, одитът за нея се извършва в съответствие с националното законодателство.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1503 НА КОМИСИЯТА

от 8 септември 2015 година

за установяване на стандартни стойности при внос с цел определяне на входната цена на някои плодове и зеленчуци

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 1308/2013 на Европейския парламент и на Съвета от 17 декември 2013 г. за установяване на обща организация на селскостопанските пазари и за отмяна на регламенти (ЕИО) № 922/72, (ЕИО) № 234/79, (ЕО) № 1037/2001 и (ЕО) № 1234/2007 ([1]),

като взе предвид Регламент за изпълнение (ЕС) № 543/2011 на Комисията от 7 юни 2011 г. за определяне на подробни правила за прилагането на Регламент (ЕО) № 1234/2007 на Съвета по отношение на секторите на плодовете и зеленчуците и на преработените плодове и зеленчуци ([2]), и по-специално член 136, параграф 1 от него,

като има предвид, че:

(1) В изпълнение на резултатите от Уругвайския кръг на многостранните търговски преговори в Регламент за изпълнение (ЕС) № 543/2011 са посочени критериите, по които Комисията определя стандартните стойности при внос от трети държави за продуктите и периодите, посочени в приложение XVI, част А от същия регламент.

(2) Стандартната стойност при внос се изчислява за всеки работен ден съгласно член 136, параграф 1 от Регламент за изпълнение (ЕС) № 543/2011, като се вземат под внимание променливите данни за всеки ден. В резултат на това настоящият регламент следва да влезе в сила в деня на публикуването му в *Официален вестник на Европейския съюз*,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Стандартните стойности при внос, посочени в член 136 от Регламент за изпълнение (ЕС) № 543/2011, са определени в приложението към настоящия регламент.

Член 2

Настоящият регламент влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 8 септември 2015 година.

За Комисията,

от името на председателя,

Jerzy PLEWA

Генерален директор на генерална дирекция „Земеделие и развитие на селските райони“

([1]) ОВ L 347, 20.12.2013 г., стр. 671.
([2]) ОВ L 157, 15.6.2011 г., стр. 1.

ПРИЛОЖЕНИЕ

Стандартни стойности при внос за определяне на входната цена на някои плодове и зеленчуци

(EUR/100 kg)

Код по КН	Код на трета държава ([1])	Стандартна стойност при внос
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)

Код по КН	Код на трета държава (1)	Стандартна стойност при внос
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Номенклатура на държавите, определена с Регламент (ЕС) № 1106/2012 на Комисията от 27 ноември 2012 година за прилагане на Регламент (ЕО) № 471/2009 на Европейския парламент и на Съвета относно статистиката на Общността за външната търговия с трети страни по отношение на актуализиране на номенклатурата на държавите и териториите (ОВ L 328, 28.11.2012 г., стр. 7). Код „ZZ“ означава „с друг произход“.

РЕШЕНИЯ

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1504 НА КОМИСИЯТА

от 7 септември 2015 година

за предоставяне на дерогации на определени държави членки във връзка с предаването на статистически данни по реда на Регламент (ЕО) № 1099/2008 на Европейския парламент и на Съвета относно статистиката за енергийния сектор

(нотифицирано под номер C(2015) 6105)

(само текстовете на гръцки, естонски, нидерландски, словашки и френски език са автентични)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕО) № 1099/2008 на Европейския парламент и на Съвета от 22 октомври 2008 г. относно статистиката за енергийния сектор ([1]), и по-специално член 5, параграф 4 и член 10, параграф 2 от него,

като има предвид, че:

(1) В съответствие с член 5, параграф 4 от Регламент (ЕО) № 1099/2008, при надлежно обосновано искане на държава членка, могат да се предоставят дерогации по отношение на онези части от националните статистически данни, чието събиране би довело до прекалено натоварване на респондентите.

(2) Белгия, Естония, Кипър и Словакия внесоха искания за получаване на дерогации по отношение на предоставянето на подробни статистически данни за потреблението на енергия в домакинствата по видове крайно потребление за някои референтни години.

(3) Информацията, предоставена от тези държави членки, дава основания да бъдат предоставени дерогации.

(4) Мерките, предвидени в настоящото решение, са в съответствие със становището на Комитета на Европейската статистическа система,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Предоставят се следните дерогации от разпоредбите на Регламент (ЕО) № 1099/2008:

(1) На Белгия се предоставя дерогация от предоставяне на резултати за референтната 2015 година по точка 1.2.3, позиции 4.2.1 — 4.2.5, точка 2.2.3, позиции 4.2.1 — 4.2.5, точка 3.2.3, позиции 3.1 — 3.6, точка 4.2.3, позиции 7.2.1 — 7.2.5 и точка 5.2.4, позиции 4.2.1 — 4.2.5 от приложение Б относно подробните статистически данни за потреблението на енергия в домакинствата по видове крайно потребление (както е определено в точка 2.3, позиция 26 „Други сектори — Жилищен сектор“ от приложение А).

([1]) ОВ L 304, 14.11.2008 г., стр. 1.

(2) На Естония се предоставя дерогация от предоставяне на резултати за референтните 2015, 2016 и 2017 години по точка 1.2.3, позиции 4.2.1 — 4.2.5, точка 2.2.3, позиции 4.2.1 — 4.2.5, точка 3.2.3, позиции 3.1 — 3.6, точка 4.2.3, позиции 7.2.1 — 7.2.5 и точка 5.2.4, позиции 4.2.1 — 4.2.5 от приложение Б относно подробните статистически данни за потреблението на енергия в домакинствата по видове крайно потребление (както е определено в точка 2.3, позиция 26 „Други сектори — Жилищен сектор“ от приложение А).

(3) На Кипър се предоставя дерогация от предоставяне на резултати за референтните 2015, 2016 и 2017 години по точка 1.2.3, позиции 4.2.1 — 4.2.5, точка 2.2.3, позиции 4.2.1 — 4.2.5, точка 3.2.3, позиции 3.1 — 3.6 и точка 5.2.4, позиции 4.2.1 — 4.2.5 от приложение Б относно подробните статистически данни за потреблението на енергия в домакинствата по видове крайно потребление (както е определено в точка 2.3, позиция 26 „Други сектори — Жилищен сектор“ от приложение А).

(4) На Словакия се предоставя дерогация от предоставяне на резултати за референтните 2015 и 2016 години по точка 1.2.3, позиции 4.2.1 — 4.2.5, точка 2.2.3, позиции 4.2.1 — 4.2.5, точка 3.2.3, позиции 3.1 — 3.6, точка 4.2.3, позиции 7.2.1 — 7.2.5 и точка 5.2.4, позиции 4.2.1 — 4.2.5 от приложение Б относно подробните статистически данни за потреблението на енергия в домакинствата по видове крайно потребление (както е определено в точка 2.3, позиция 26 „Други сектори — Жилищен сектор“ от приложение А).

Член 2

Адресати на настоящото решение са Кралство Белгия, Република Естония, Република Кипър и Словашката република.

Съставено в Брюксел на 7 септември 2015 година.

За Комисията

Marianne THYSSEN

Член на Комисията

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1505 НА КОМИСИЯТА

от 8 септември 2015 година

за определяне на техническите спецификации и форматите на доверителните списъци съгласно член 22, параграф 5 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 22, параграф 5 от него,

като има предвид, че:

(1) Доверителните списъци са от съществено значение за изграждането на доверие между пазарните участници, тъй като отразяват статута на доставчика на услуги към момента на осъществяване на надзор.

(2) Трансграничното използване на електронни подписи беше улеснено с Решение 2009/767/ЕО на Комисията ([2]), съгласно което държавите членки са задължени да създадат, поддържат и публикуват доверителни списъци, включващи информация за доставчиците на удостоверителни услуги, издаващи квалифицирани удостоверения за потребители в съответствие с Директива 1999/93/ЕО на Европейския парламент и на Съвета ([3]), и които са под надзора на държавите членки и са акредитирани от тях.

(3) Съгласно член 22 от Регламент (ЕС) № 910/2014 държавите членки са задължени да създадат, поддържат и публикуват по сигурен начин доверителни списъци, които са подписани и подпечатани по електронен път във форма, подходяща за автоматизирана обработка, и да уведомят Комисията за органите, отговорни за изготвянето на националните доверителни списъци.

(4) Даден доставчик на удостоверителни услуги и удостоверителните услуги, които той предоставя, следва да се считат за квалифицирани, когато за доставчика е отбелязан квалифициран статут в доверителния списък. С оглед да се гарантира, че другите задължения, произтичащи от Регламент (ЕС) № 910/2014, и по-конкретно тези, които са определени в членове 27 и 37, са лесно изпълними от доставчиците на услуги от разстояние и по електронен път, и за да се отговори на оправданите очаквания на други доставчици на удостоверителни услуги, които не издават квалифицирани удостоверения, но предлагат услуги, свързани с електронни подписи съгласно Директива 1999/93/ЕО, и са вписани до 30 юни 2016 г., държавите членки следва да имат възможност да добавят удостоверителни услуги, различни от квалифицираните в доверителните списъци, на доброволна основа на национално равнище, при положение че се посочва ясно, че те не са квалифицирани в съответствие с Регламент (ЕС) № 910/2014.

(5) В съответствие със съображение 25 от Регламент (ЕС) № 910/2014 държавите членки могат да добавят други видове удостоверителни услуги, определени на национално равнище, които са различни от определените в член 3, точка 16 от Регламент (ЕС) № 910/2014, при положение че се посочва ясно, че те не са квалифицирани в съответствие с Регламент (ЕС) № 910/2014.

(6) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден съгласно член 48 от Регламент (ЕО) № 910/2014,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Държавите членки създават, публикуват и поддържат доверителни списъци, съдържащи информация за надзираваните от тях квалифицирани доставчици на удостоверителни услуги, както и информация за предоставяните от тези доставчици квалифицирани удостоверителни услуги. Тези списъци трябва да съответстват на техническите спецификации, посочени в приложение I.

([1]) ОВ L 257, 28.8.2014 г., стр. 73.

([2]) Решение 2009/767/ЕО на Комисията от 16 октомври 2009 г. за определяне на мерки, улесняващи прилагането на процедури с помощта на електронни средства чрез „единични звена за контакт“ в съответствие с Директива 2006/123/ЕО на Европейския парламент и на Съвета относно услугите на вътрешния пазар (ОВ L 274, 20.10.2009 г., стр. 36).

([3]) Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните подписи (ОВ L 13, 19.1.2000 г., стр. 12).

Член 2

Държавите членки могат да включват в доверителните списъци информация за неквалифицираните доставчици на удостоверителни услуги заедно с информация за предоставяните от тези доставчици неквалифицирани удостоверителни услуги. В списъците ясно се посочва кои доставчици на удостоверителни услуги и предоставяните от тях удостоверителни услуги не са квалифицирани.

Член 3

1. Съгласно член 22, параграф 2 от Регламент (ЕС) № 910/2014 държавите членки подписват или подпечатват по електронен път своя доверителен списък във форма, подходяща за автоматизирана обработка, в съответствие с техническите спецификации, посочени в приложение I.

2. Ако държава членка публикува по електронен път своя доверителен списък в четима от човек форма, тя гарантира, че тази форма на доверителния списък съдържа същите данни, както подходящата за автоматизирана обработка форма, и я подписва или подпечатва по електронен път в съответствие с техническите спецификации, посочени в приложение I.

Член 4

1. Държавите членки съобщават на Комисията информацията, посочена в член 22, параграф 3 от Регламент (ЕС) № 910/2014, като използват образеца в приложение II.

2. Информацията, посочена в параграф 1, трябва да включва две или повече удостоверения за публичен ключ на оператора на схемата, чиито срокове на валидност се различават с най-малко три месеца и съответстват на частните ключове, които са използваеми за подписване или подпечатване по електронен път на доверителния списък във формата, подходяща за автоматизирана обработка, както и на четимата от човек форма, когато се публикува.

3. Съгласно член 22, параграф 4 от Регламент (ЕС) № 910/2014 Комисията предоставя на обществеността, чрез сигурен канал към уебсървър с удостоверена автентичност, посочената в параграфи 1 и 2 информация, както е съобщена от държавите членки, в подписана и подпечатана форма, подходяща за автоматизирана обработка.

4. Комисията може да предоставя на обществеността, чрез сигурен канал към уебсървър с удостоверена автентичност, посочената в параграфи 1 и 2 информация, както е съобщена от държавите членки, в подписана и подпечатана четима от човек форма.

Член 5

Настоящото решение влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящото решение е задължително в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 8 септември 2015 година.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ I

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОБЩ ОБРАЗЕЦ ЗА ДОВЕРИТЕЛНИ СПИСЪЦИ

ГЛАВА I

ОБЩИ ИЗИСКВАНИЯ

Доверителните списъци включват както актуалната, така и цялата предходна информация за статута на вписаните удостоверителни услуги от датата на включването на техния доставчик в доверителните списъци.

В настоящите спецификации понятията „одобрени“, „акредитирани“ и/или „поднадзорни“ обхващат също така националните схеми за одобрение, като държавите членки ще предоставят в доверителните си списъци допълнителна информация относно характера на националните схеми, включително пояснение за евентуалните разлики спрямо схемите за надзор, които се прилагат за квалифицираните доставчици на удостоверителни услуги и за предоставяните от тях квалифицирани удостоверителни услуги.

Информацията, предоставяна в доверителния списък, служи преди всичко да подпомогне валидирането на токените за квалифицирани удостоверителни услуги, т.е. физическите или двоичните (логически) обекти, създадени или издадени в резултат на използването на квалифицирана удостоверителна услуга, а именно например квалифицирани електронни подписи/печати, усъвършенствани електронни подписи/печати, подкрепяни от квалифицирано удостоверение, квалифицирани времеви печати, квалифицирани доказателства за доставяне по електронен път и т.н.

ГЛАВА II

ПОДРОБНИ ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОБЩИЯ ОБРАЗЕЦ ЗА ДОВЕРИТЕЛНИ СПИСЪЦИ

Настоящите спецификации се основават на спецификациите и изискванията, определени в ETSI TS 119 612 v2.1.1 (наричани по-долу „ETSI TS 119 612“).

Когато в настоящите спецификации липсва специално изискване, се прилагат изискванията на клаузи 5 и 6 от ETSI TS 119 612 в тяхната цялост. Когато в настоящите спецификации са дадени специални изисквания, те подменят съответните изисквания от ETSI TS 119 612. В случай на противоречия между настоящите спецификации и спецификациите от ETSI TS 119 612 са меродавни настоящите спецификации.

Scheme name („Име на схемата“) (клауза 5.3.6)

Това поле е задължително и трябва да съответства на спецификациите в клауза 5.3.6 от TS 119 612, като за схемата се използва следното име:

„EN_name_value“ = „Доверителен списък, включващ информация за квалифицираните доставчици на удостоверителни услуги, които са под надзора на издаващата държава членка, заедно с информация за предоставяните от тях квалифицирани удостоверителни услуги, в съответствие с приложимите разпоредби, определени в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО.“

Scheme information URI (URI, т.е. унифициран идентификатор на ресурси, за информация за схемата) (клауза 5.3.7)

Това поле е задължително и трябва да съответства на спецификациите в клауза 5.3.7 от TS 119 612, като „подходящата информация за схемата“ трябва да включва като минимум:

а) Обща за всички държави членки уводна информация относно обхвата и контекста на доверителния списък, базовата схема за надзор и, ако е приложимо, националните схеми за одобряване (напр. за акредитация). Общият текст, който трябва да се използва, е посоченият по-долу текст, в който символният низ „[*име на съответната държава членка*]“ се заменя с името на съответната държава членка:

> „Настоящият списък е доверителният списък, включващ информация за квалифицираните доставчици на удостоверителни услуги, които са под надзора на [*име на съответната държава членка*], заедно с информация за предоставяните от тях квалифицирани удостоверителни услуги, в съответствие с приложимите разпоредби, определени в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО.

Трансграничното използване на електронни подписи беше улеснено с Решение 2009/767/ЕО на Комисията от 16 октомври 2009 г., съгласно което държавите членки са задължени да създадат, поддържат и публикуват доверителни списъци с информация за доставчиците на удостоверителни услуги, издаващи квалифицирани удостоверения за потребители в съответствие с Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните подписи, и които са под надзора на държавите членки и акредитирани от тях. Настоящият доверителен списък е продължение на доверителния списък, установен с Решение 2009/767/ЕО.“

Доверителните списъци са важни елементи за изграждането на доверие между участниците на електронните пазари, като дават възможност на потребителите да установят дали доставчиците на удостоверителни услуги и предоставяните от тях услуги са със квалифициран статут и какъв е бил техният статут в миналото.

Доверителните списъци на държавите членки, включват като минимум информацията, посочена в членове 1 и 2 от Решение за изпълнение (ЕС) 2015/1505 на Комисията.

Държавите членки могат да включват в доверителните списъци информация за неквалифицираните доставчици на удостоверителни услуги заедно с информация за предоставяните от тези доставчици неквалифицирани удостоверителни услуги. Ясно се указва, че те не са квалифицирани съгласно Регламент (ЕС) № 910/2014.

Държавите членки могат да включат в доверителните списъци информация относно други видове удостоверителни услуги, определени на национално равнище, които са различни от определените по член 3, точка 16 от Регламент (ЕС) № 910/2014. Ясно се указва, че те не са квалифицирани съгласно Регламент (ЕС) № 910/2014.

б) Конкретна информация относно базовата схема за надзор и ако е приложимо, националните схеми за одобряване (например за акредитация), и по-специално ([1]):

1) информация относно националната система за надзор, приложима към квалифицираните и неквалифицираните доставчици на удостоверителни услуги и към квалифицираните и неквалифицираните удостоверителни услуги, които те предоставят съгласно Регламент (ЕС) № 910/2014;

2) информация, когато е уместно, относно националните схеми за доброволна акредитация, приложими към доставчиците на удостоверителни услуги, издали квалифицирани удостоверения съгласно Директива 1999/93/ЕО;

За всяка от базовите схеми, изброени по-горе, тази специфична информация трябва да включва най-малко следното:

1) общо описание;

2) информация относно процедурата, следвана за националната система за надзор и, ако е приложимо, за одобряването по национална схема за одобряване;

3) информация относно критериите, по които се осъществява надзорът или, ако е приложимо, одобряването на доставчиците на удостоверителни услуги;

4) информация относно критериите и правилата, използвани за избор на надзорни/одиторски органи и за оценяване на доставчиците на удостоверителни услуги и предоставяните от тях удостоверителни услуги;

5) ако е уместно — друга контактна и обща информация, която засяга функционирането на схемата.

Scheme type/community/rules („Тип/общност/правила на схемата“) (клауза 5.3.9)

Това поле е задължително и трябва да съответства на спецификациите в клауза 5.3.9 от TS 119 612.

То включва само URI на британски английски.

([1]) Тези пакети от информация са от ключово значение за оценяването от доверяващите се страни на качеството и нивото на сигурност на такива системи. Тези пакети от информация се предоставят на ниво доверителен списък, като се използват задължителните полета„Scheme information URI“ (клауза 5.3.7 — информация, предоставяна от държавите членки), „Scheme type/community/rules“ (клауза 5.3.9, като се използва обща за всички държави членки формулировка) и „TSL policy/legal notice“ (клауза 5.3.11 — обща за всички държави членки формулировка и възможност за всяка държава членка да добави специфични национални формулировки или позовавания). Допълнителна информация за такива системи за неквалифицирани удостоверителни услуги и за (квалифицирани) удостоверителни услуги, определени на национално равнище, може да се предоставя на нивото на услугата, ако е уместно и необходимо (напр. за да се разграничават отделните нива на качество/сигурност), като се използва „Scheme service definition URI“ (клауза 5.5.6).

То включва най-малко два URI:

1) общ URI за доверителните списъци на всички държави членки, насочващ към описателен текст, който да е приложим за всички доверителни списъци, както следва:

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

Описателен текст:

„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) Специфичен за доверителния списък на всяка държава членка идентификатор (URI), насочващ към описателен текст, който се отнася за доверителния списък на тази държава членка:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, където CC = двубуквеният код на държавата по ISO 3166-1 [1], използван в полето „Scheme territory“ („Територия на схемата“) (клауза 5.3.10).

— Там потребителите могат да намерят специфичните за съответната държава членка политика/правила, съгласно които се оценяват включените в списъка услуги в съответствие с нейния режим за надзор и, когато е приложимо, схема за одобряване.

— Там потребителите могат да намерят специфично за дадената държава членка описание как да използват и тълкуват съдържанието на доверителния списък по отношение на вписаните неквалифицирани удостоверителни услуги и/или удостоверителните услуги, определени на национално равнище. То може да се използва за указване на евентуална нееднородност в националната система за одобряване по отношение на доставчици на удостоверителни услуги (ДУУ), които не издават квалифицирани удостоверения (КУ), както и на начина, по който „Scheme service definition URI“ (клауза 5.5.6) и полето „Service information extension“ (клауза 5.5.9) се използват за тази цел.

Държавите членки МОГАТ да определят и използват допълнителни URI, разширяващи горепосочения специфичен за държавата членка URI (т.е. URI, попадащи в йерархията на този специфичен URI).

TSL policy/legal notice („Политика/правен коментар за списъка за статута на доверителните услуги — ССДУ“) (клауза 5.3.11)

Това поле е задължително и трябва да съответства на спецификациите в клауза 5.3.11 от TS 119 612, в които правният коментар относно правния статут на схемата или правните изисквания, на които схемата трябва да отговаря в рамките на юрисдикцията, в която е установена, и/или евентуални ограничения и условия, при които се поддържа и публикува

[1] ISO 3166-1:2006: Кодове за представяне на наименованията на държавите и техните подразделения. Част 1: Кодове на държавите.

доверителният списък, трябва да бъде последователност от многоезични символни низове (вж. клауза 5.1.4), предоставящи на британски английски като задължителен език и по избор — на един или няколко национални езици, конструираният по следния начин актуален текст за тази политика или коментар:

1) Първа задължителна част, обща за доверителните списъци на всички държави членки, в която се указва приложимата правна рамка и чиято версия на английски език е следната:

   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.

   Текст на националния език или езици на държавата членка:

   Приложимата правна рамка за настоящия доверителен списък е Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО.

2) Втора, незадължителна част, специфична за всеки доверителен списък, включваща препратки към специфични приложими национални правни рамки.

Service current status („Настоящ статут на услугата“) (клауза 5.5.4)

Това поле е задължително и трябва да съответства на спецификациите в клауза 5.5.4 от TS 119 612.

Миграцията на стойността на „Service current status“ за услугите, вписани в доверителния списък на държавите — членки на ЕС, към деня преди датата, от която се прилага Регламент (ЕС) № 910/2014 (т.е. 30 юни 2016 г.), се извършва в деня, от който се прилага този регламент (т.е. 1 юли 2016 г.), както е посочено в приложение J към ETSI TS 119 612.

ГЛАВА III

ВРЕМЕВА НЕПРЕКЪСНАТОСТ НА ДОВЕРИТЕЛНИТЕ СПИСЪЦИ

Удостоверенията, за които трябва да се уведоми Комисията в съответствие с член 4, параграф 2 от настоящото решение, трябва да отговарят на изискванията на клауза 5.7.1 от ETSI TS 119 612 и да се издават по такъв начин, че:

— да има най-малко три месеца разлика в крайната им дата на валидност („не по-късно от“),

— да са създадени въз основа на нови двойки ключове. Вече използвани двойки ключове не трябва да бъдат сертифицирани повторно.

В случай на изтичане на валидността на едно от удостоверенията за публичен ключ, което би могло да се използва за валидиране на подписа или печата на доверителния списък и за което Комисията е била уведомена, като тя го е публикувала в централния си списък с указатели, държавите членки трябва:

— в случай че актуалният публикуван доверителен списък е бил подписан или подпечатан с частен ключ, валидността на чието удостоверение за публичен ключ е изтекла — незабавно да издадат нов доверителен списък, който е подписан или подпечатан с частен ключ, валидността на чието удостоверение за публичен ключ не е изтекла;

— да генерират при поискване нови двойки ключове, които биха могли да се използват за подписване или подпечатване на доверителния списък, и да се заемат със създаването на съответстващите им удостоверения за публичен ключ;

— незабавно да уведомят Комисията за новия списък на удостоверения за публични ключове, съответстващи на частните ключове, които биха могли да се използват за подписване или подпечатване на доверителния списък.

В случай на разкриване или на прекратяване на използването на един от частните ключове, съответстващ на едно от удостоверенията за публичен ключ, което би могло да се използва за валидиране на подписа или печата на доверителния списък и за което Комисията е била уведомена, като тя го е публикувала в централния си списък с указатели, държавите членки трябва:

— незабавно да издадат нов доверителен списък, подписан или подпечатан с неразкрит частен ключ, в случай че публикуваният доверителен списък е бил подписан или подпечатан с частен ключ, който е разкрит или чието използване е прекратено;

— да генерират при поискване нови двойки ключове, които биха могли да се използват за подписване или подпечатване на доверителния списък, и да се заемат със създаването на съответстващите им удостоверения за публичен ключ;

— незабавно да уведомят Комисията за новия списък на удостоверения за публични ключове, съответстващи на частните ключове, които биха могли да се използват за подписване или подпечатване на доверителния списък.

В случай на разкриване или на прекратяване на използването на всички частни ключове, съответстващи на удостоверенията за публични ключове, които биха могли да се използват за валидиране на подписа на доверителния списък и за които Комисията е била уведомена, като тя ги е публикувала в централния си списък с указатели, държавите членки трябва:

— да генерират нови двойки ключове, които биха могли да се използват за подписване или подпечатване на доверителния списък, и да се заемат със създаването на съответстващите им удостоверения за публичен ключ;

— незабавно да издадат нов доверителен списък, който е подписан или подпечатан с един от тези нови частни ключове и за чието удостоверение за публичен ключ трябва да се уведоми;

— незабавно да уведомят Комисията за новия списък на удостоверения за публични ключове, съответстващи на частните ключове, които биха могли да се използват за подписване или подпечатване на доверителния списък.

ГЛАВА IV

СПЕЦИФИКАЦИИ ЗА ЧЕТИМАТА ОТ ЧОВЕК ФОРМА НА ДОВЕРИТЕЛНИЯ СПИСЪК

Ако доверителният списък е съставен и публикуван в четима от човек форма, той се предоставя като документ във формат Portable Document Format (PDF) в съответствие с ISO 32000 ([1]), който е форматиран съгласно профила PDF/A (ISO 19005 ([2])).

Съдържанието на четимата от човек форма на доверителния списък на базата на PDF/A трябва да отговаря на следните изисквания:

— Структурата на четимата от човек форма на доверителния списък да отразява логическия модел, описан в TS 119 612.

— Всяко налично поле да е изобразено и да съдържа:

  — наименованието на полето (напр. „Service type identifier“);

  — стойността на полето (напр. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC}“);

  — значението (описание) на стойността на полето, когато е уместно (напр. „Услуга за създаване и подписване на квалифицирани удостоверения въз основа на идентификационните и други данни, проверени от съответните регистрационни служби.“);

  — няколко езикови версии на естествени езици в съответствие с доверителния списък, когато е уместно.

— В четимата от човек форма на доверителния списък трябва да бъдат изобразени като минимум следните полета и съответни стойности на цифровите удостоверения ([3]), ако фигурират в полето „Service digital identity“:

  — Версия

  — Сериен номер на удостоверението

  — Сигнатурен алгоритъм

  — Издател — всички съответни полета за отличително име

  — Период на валидност

  — Издател — всички съответни полета за отличително име

([1]) ISO 32000-1:2008: Document management – Portable document format – Part 1: PDF 1.7.
([2]) ISO 19005-2:2011: Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).
([3]) Препоръка ITU-T X.509 | ISO/IEC 9594-8: Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate frameworks („Информационни технологии. Взаимосвързване на отворени системи. Справочник: Структура за установяване на автентичност“) (вж. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509)

— Публичен ключ

— Идентификатор на ключа на органа

— Идентификатор на ключа на субекта

— Употреба на ключа

— Разширена употреба на ключа

— Политики за удостоверението — всички идентификатори и квалификатори за политиката

— Категоризации на политиката

— Алтернативно име на субекта

— Справочни данни за субекта (Subject directory attributes)

— Основни ограничения

— Ограничения на политиката

— Точки на разпространение на списъци на отменени удостоверения (Certificate Revocation Lists — CRL) ([1])

— Достъп до информация за органа

— Достъп до информация за субекта

— Декларации за квалифицирано удостоверение ([2])

— Алгоритъм за хеширане

— Хеш-стойност на удостоверението

— За четимата от човек форма се изисква да може лесно да се разпечатва.

— Четимата от човек форма трябва да бъде подписана или подпечатана от оператора на схемата съгласно усъвършенствания електронен подпис във формат PDF, посочен в членове 1 и 3 от Решение за изпълнение (ЕС) 2015/1505 на Комисията.

([1]) RFC 5280: Internet X.509 PKI Certificate and CRL Profile
([2]) RFC 3739: Internet X.509 PKI: Qualified Certificates Profile

ПРИЛОЖЕНИЕ II

ОБРАЗЕЦ ЗА УВЕДОМЛЕНИЯТА НА ДЪРЖАВИТЕ ЧЛЕНКИ

Информацията, която трябва да се съобщава от държавите членки в съответствие с член 4, параграф 1 от настоящото решение, трябва да съдържа следните данни, както и всякакви промени в тях:

1) Държавата членка, като се използва двубуквеният код по ISO 3166-1 ([1]) със следните изключения:

   а) кодът на Обединеното кралство е „UK“;

   б) кодът на Гърция е „EL“.

2) Органът или органите, отговорен/отговорни за създаването, поддържането и публикуването на доверителните списъци във форма, подходяща за автоматизирана обработка, и в четима от човек форма:

   а) Scheme operator name („Име на оператора на схемата“): предоставената информация трябва да съвпада точно, включително и по отношение на регистъра на буквите, със стойността в полето „Scheme operator name“ за всички използвани езици в доверителния списък.

   б) Незадължителна информация за вътрешна употреба от Комисията само в случай че се наложи установяване на контакт със съответния орган (тази информация няма да се публикува в съставения от Комисията общ списък на доверителните списъци):

      — адрес на оператора на схемата;

      — координати за връзка с отговорното лице или лица (име, телефон, адрес за електронна поща).

3) Мястото, където е публикуван доверителният списък във форма, подходяща за автоматизирана обработка (*място, където е публикуван актуалният доверителен лист*).

4) Мястото, където евентуално е публикуван доверителният списък в четима от човек форма (*място, където е публикуван актуалният доверителен лист*). Ако доверителният списък вече не се публикува в четима от човек форма, това се посочва.

5) Удостоверенията за публични ключове, съответстващи на частните ключове, които могат да се използват за подписване или подпечатване по електронен път на доверителните списъци във форма, подходяща за автоматизирана обработка, както и в четима от човек форма: тези удостоверения следва да се предоставят като кодирани по Privacy Enhanced Mail Base 64 DER удостоверения. Уведомява се с допълнителна информация за промяна, ако конкретно удостоверение в списъка на Комисията трябва да бъде заменено с ново удостоверение и ако към съществуващите удостоверения трябва да бъде добавено нотифицирано удостоверение, без да заменя някое от тях.

6) Дата на подаване на данните, съобщени по точки 1—5.

Данните, съобщени съгласно точка 1, точка 2, буква а) и точки 3, 4 и 5, трябва да бъдат включени в съставения от Комисията общ списък на доверителните списъци, заменяйки съобщената преди това информация, включена в този общ списък.

([1]) ISO 3166-1: „Кодове за представяне на наименованията на държавите и техните подразделения. Част 1: Кодове на държавите.“

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 НА КОМИСИЯТА

от 8 септември 2015 година

за определяне на спецификации, отнасящи се до форматите на усъвършенствани електронни подписи и усъвършенствани печати, които трябва да бъдат признати от органите от публичния сектор съгласно член 27, параграф 5 и член 37, параграф 5 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 27, параграф 5 и член 37, параграф 5 от него,

като има предвид, че:

(1) Държавите членки трябва да въведат необходимите технически средства, позволяващи им да обработват електронно подписани документи, които се изискват при използване на онлайн услуга, предлагана пряко от орган от публичния сектор или от негово име.

(2) Регламент (ЕС) № 910/2014 задължава държавите членки, изискващи усъвършенстван електронен подпис или печат за използване на онлайн услуга, предлагана от или от името на орган от публичния сектор, да признават усъвършенстваните електронни подписи и печати, както и усъвършенстваните електронни подписи и печати, основани на квалифицирано удостоверение, а също и квалифицираните електронни подписи и печати в специфични формати, или алтернативни формати, които са валидирани в съответствие със специфични референтни методи.

(3) При определянето на специфичните формати и референтни методи следва да се вземат предвид съществуващите практики, стандарти и правни актове на Съюза.

(4) С Решение за изпълнение 2014/148/ЕС на Комисията ([2]) са определени някои от обичайните формати на усъвършенствани електронни подписи, които трябва да бъдат технически поддържани от държавите членки, когато за онлайн административна процедура се изискват усъвършенствани електронни подписи. Установяването на референтни формати има за цел улесняване на трансграничното валидиране на електронните подписи и подобряване на трансграничната оперативна съвместимост на електронните процедури.

(5) Стандартите, изброени в приложението към настоящото решение, са съществуващите стандарти за формати на усъвършенствани електронни подписи. Тъй като понастоящем органите по стандартизация преразглеждат дългосрочните архивни форми на посочените формати, от обхвата на настоящото решение са изключени стандартите относно дългосрочното архивиране. Когато бъде налице новата версия на посочените стандарти, позоваванията на стандартите и на клаузите за дългосрочно архивиране ще бъдат актуализирани.

(6) Усъвършенстваните електронни подписи и усъвършенстваните електронни печати са сходни от техническа гледна точка. Поради това стандартите за формати на усъвършенстваните електронни подписи следва да се прилагат *mutatis mutandis* по отношение на форматите на усъвършенстваните електронни печати.

(7) Когато форматът на използваните за подписване или подпечатване електронни подписи или печати е различен от тези, които обикновено се поддържат технически, следва да бъдат предоставени средства за валидиране, които да дават възможност за трансгранична проверка на електронните подписи и печати. С оглед да се гарантира на получаващите държави членки, че могат да разчитат на тези средства за валидиране на друга държава членка, е необходимо да се предоставя лесно достъпна информация относно тези средства за валидиране чрез включването на информацията в електронните документи, в електронните подписи или в носителите на електронните документи.

([1]) ОВ L 257, 28.8.2014 г., стр. 73.

([2]) Решение за изпълнение 2014/148/ЕС на Комисията от 17 март 2014 г. за изменение на Решение 2011/130/ЕС за установяване на минимални изисквания за трансграничната обработка на документи, подписани електронно от компетентните органи съгласно Директива 2006/123/ЕО на Европейския парламент и на Съвета относно услугите на вътрешния пазар (ОВ L 80, 19.3.2014 г., стр. 7).

(8) Когато за обществените услуги в държавата членка са налице подходящи за автоматизирана обработка възможности за валидиране на електронни подписи или печати, такива възможности за валидиране следва да бъдат създадени и предоставени на получаващата държава членка. Независимо от това настоящото решение не следва да възпрепятства прилагането на член 27, параграфи 1 и 2, както и на член 37, параграфи 1 и 2 от Регламент (ЕС) № 910/2014, когато автоматизираната обработка на възможностите за валидиране не е възможна за алтернативни методи.

(9) С цел да се осигури сходство на изискванията за валидиране и да се повиши доверието във възможностите за валидиране, предоставяни от държавите членки за електронни подписи или печати във формати, различни от тези, които обикновено се поддържат технически, изложените в настоящото решение изисквания за средствата за валидиране са въз основа на изискванията за валидирането на квалифицирани електронни подписи и печати, посочени в членове 32 и 40 от Регламент (ЕС) № 910/2014.

(10) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден съгласно член 48 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Държавите членки, които изискват усъвършенстван електронен подпис или усъвършенстван електронен подпис, основан на квалифицирано удостоверение, както е предвидено в член 27, параграфи 1 и 2 от Регламент (ЕС) № 910/2014, признават усъвършенствани електронни подписи във формати XML, CMS или PDF на нива на съответствие B, T или LT, или използващи свързан с подписа носител, когато тези подписи съответстват на техническите спецификации, посочени в приложението.

Член 2

1. Държавите членки, които изискват усъвършенстван електронен подпис или усъвършенстван електронен подпис, основан на квалифицирано удостоверение, както е предвидено в член 27, параграфи 1 и 2 от Регламент (ЕС) № 910/2014, признават други формати на електронни подписи, различни от тези, посочени в член 1 от настоящото решение, при условие че държавата членка, в която е установен доставчикът на удостоверителната услуга, използвана от титуляря на електронния подпис, предлага на други държави членки възможности за валидиране на подписа, които по възможност са подходящи за автоматизирана обработка.

2. Възможностите за валидиране на подписа трябва:

а) да позволяват на други държави членки да валидират получените електронни подписи онлайн, безплатно и по начин, разбираем за лицата, за които съответният език не е роден;

б) да са посочени в подписания документ, в електронния подпис или в носителя на електронния документ; и

в) да потвърждават валидността на даден усъвършенстван електронен подпис, при условие че:

1) удостоверението в подкрепа на усъвършенстваният електронен подпис е било валидно към момента на подписването, а когато усъвършенстваният електронен подпис е подкрепен от квалифицирано удостоверение, това квалифицирано удостоверение е отговаряло към момента на подписването на изискванията съгласно приложение I към Регламент (ЕС) № 910/2014 и е било издадено от доставчик на квалифицирани удостоверителни услуги;

2) данните от валидирането на подписа съответстват на данните, предоставени на доверяващата се страна;

3) уникалният набор от данни, представляващ титуляря на електронния подпис, е надлежно предаден на доверяващата се страна;

4) ако към момента на подписването е бил използван псевдоним, то това е ясно указано на доверяващата се страна;

5) когато усъвършенстваният електронен подпис е създаден от устройство за създаване на квалифициран електронен подпис, използването на такова устройство е ясно указано на доверяващата се страна;

6) цялостността на подписаните данни не е застрашена;

7) изискванията по член 26 от Регламент (ЕС) № 910/2014 са били изпълнени към момента на подписването;

8) системата, използвана за валидиране на усъвършенстваният електронен подпис, предоставя на доверяващата се страна правилния резултат от процеса на валидиране и ѝ позволява да открие евентуални проблеми, свързани със сигурността.

Член 3

Държавите членки, които изискват усъвършенстван електронен печат или усъвършенстван електронен печат, основан на квалифицирано удостоверение, както е предвидено в член 37, параграфи 1 и 2 от Регламент (ЕС) № 910/2014, признават усъвършенствани електронни печати във формати XML, CMS или PDF на нива на съответствие B, T или LT, или използващи свързан с печата носител, когато те съответстват на техническите спецификации, посочени в приложението.

Член 4

1. Държавите членки, които изискват усъвършенстван електронен печат или усъвършенстван електронен печат, основан на квалифицирано удостоверение, както е предвидено в член 37, параграфи 1 и 2 от Регламент (ЕС) № 910/2014, признават други формати на електронни печати, различни от тези, посочени в член 3 от настоящото решение, при условие че държавата членка, в която е установен доставчикът на удостоверителната услуга, използван от създателя на печата, предлага на други държави членки възможности за валидиране на печата, които по възможност са подходящи за автоматизирана обработка.

2. Възможностите за валидиране на печата трябва:

а) да позволяват на други държави членки да валидират получените електронни печати онлайн, безплатно и по начин, разбираем за лицата, за които съответният език не е роден;

б) да са посочени в подпечатания документ, в електронния печат или в носителя на електронния документ;

в) да потвърждават валидността на даден усъвършенстван електронен печат, при условие че:

1) удостоверението в подкрепа на усъвършенстваният електронен печат е било валидно към момента на подпечатването, а когато усъвършенстваният електронен печат е подкрепен от квалифицирано удостоверение, това квалифицирано удостоверение е отговаряло към момента на подпечатването на изискванията съгласно приложение III към Регламент (ЕС) № 910/2014 и е било издадено от доставчик на квалифицирани удостоверителни услуги;

2) данните от валидирането на печата съответстват на данните, предоставени на доверяващата се страна;

3) уникалният набор от данни, представляващ създателя на печата, е надлежно предаден на доверяващата се страна;

4) ако към момента на подпечатването е бил използван псевдоним, то това е ясно указано на доверяващата се страна;

5) когато усъвършенстваният електронен печат е създаден от устройство за създаване на квалифициран електронен печат, използването на такова устройство е ясно указано на доверяващата се страна;

6) цялостността на подпечатаните данни не е застрашена;

7) изискванията по член 36 от Регламент (ЕС) № 910/2014 са били изпълнени към момента на подпечатването;

8) системата, използвана за валидиране на усъвършенстваният електронен печат, предоставя на доверяващата се страна правилния резултат от процеса на валидиране и ѝ позволява да открие евентуални проблеми, свързани със сигурността.

Член 5

Настоящото решение влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящото решение е задължително в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 8 септември 2015 година.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

Списък на техническите спецификации за усъвършенствани електронни подписи във формат XML, CMS или PDF и за свързания с подписа носител

Усъвършенстваните електронни подписи, посочени в член 1 от решението, трябва да съответстват на една от следните технически спецификации на ETSI с изключение на клауза 9 от тях:

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

Свързаният с подписа носител, посочен в член 1 от решението, трябва да съответства на следните технически спецификации на ETSI:

Базов профил на свързания с подписа носител	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

Списък на техническите спецификации за усъвършенствани електронни печати във формат XML, CMS или PDF и за свързания с печата носител

Усъвършенстваните електронни печати, посочени в член 3 от решението, трябва да съответстват на една от следните технически спецификации на ETSI с изключение на клауза 9 от тях:

Базов профил XAdES	ETSI TS 103171 v.2.1.1
Базов профил CAdES	ETSI TS 103173 v.2.2.1
Базов профил PAdES	ETSI TS 103172 v.2.2.2

Свързаният с печата носител, посочен в член 3 от решението, трябва да съответства на следните технически спецификации на ETSI:

Базов профил на свързания с печата носител	ETSI TS 103174 v.2.2.1

ISSN 1977-0618 (електронно издание)
ISSN 1830-3617 (печатно издание)

Служба за публикации на Европейския съюз
2985 Люксембург
ЛЮКСЕМБУРГ

BG