РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА КОМИСИЯТА

от 14 октомври 2013 година

за изменение на Решение 2009/767/ЕО във връзка със създаването, поддържането и публикуването на доверителни списъци на доставчици на удостоверителни услуги, които се намират под надзора или са акредитирани от държавите членки

(нотифицирано под номер C(2013) 6543)

(текст от значение за ЕИП)

(2013/662/ЕС)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива 2006/123/ЕО на Европейския парламент и на Съвета от 12 декември 2006 г. относно услугите на вътрешния пазар ([1]), и по-специално член 8, параграф 3 от нея,

като има предвид, че:

(1) 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 ([2]) задължава държавите членки да предоставят информацията, необходима за валидиране на усъвършенствани електронни подписи, поддържани от квалифицирано удостоверение. Тази информация следва да се представя по стандартизиран начин, като се използват така наречените доверителни списъци, съдържащи данни за доставчиците на удостоверителни услуги, които издават 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 ([3]) и които се намират под надзора или са акредитирани от държавите членки.

(2) Практическото прилагане на Решение 2009/767/ЕО от страна на държавите членки показа, че са необходими някои подобрения, за да се използват доверителните списъци по най-рационален начин. Освен това Европейският институт за стандарти в далекосъобщенията (ETSI) публикува нови технически спецификации за доверителни списъци (TS 119 612), които се основават на спецификациите, включени понастоящем в приложението към решението, като същевременно внасят редица подобрения в съществуващите спецификации.

(3) Поради това Решение 2009/767/ЕО следва да бъде изменено, за да включи както позоваване на техническите спецификации 119 612 на ETSI, така и промени, които се считат за необходими, за да се подобри и улесни прилагането и използването на доверителни списъци.

(4) С цел да се даде възможност на държавите членки да осъществят изискваните технически изменения в своите сегашни доверителни списъци, уместно е настоящото решение да се прилага от 1 февруари 2014 г.

(5) Мерките, предвидени в настоящото решение, са в съответствие със становището на Комитета по Директивата за услугите,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Изменения на Решение 2009/767/ЕО

Решение 2009/767/ЕО се изменя, както следва:

1) Член 2 се изменя, както следва:

а) Параграфи 1, 2 и 2а се заменят със следното:

„1. Всяка държава членка създава, поддържа и публикува в съответствие с определените в приложението технически спецификации доверителен списък, съдържащ минималната изисквана информация по отношение на намиращите се под неин надзор и притежаващи нейна акредитация доставчици на удостоверителни услуги, издаващи квалифицирани удостоверения за потребители.

2. Държавите членки създават и публикуват доверителен списък в машинно обработваема форма в съответствие с определените в приложението технически спецификации. Ако държава членка реши да публикува своя доверителен списък в четима от човек форма, тази форма на доверителния списък съответства на спецификациите в приложението.

2а. Държавите членки подписват по електронен път машинно обработваемата форма на своя доверителен списък, за да гарантират нейната автентичност и цялост. Ако държава членка публикува своя доверителен списък в четима от човек форма, тя гарантира, че тази форма на доверителния списък съдържа същите данни, каквито съдържа машинно обработваемата форма, и я подписва по електронен път със същото удостоверение, което се използва при машинно обработваемата форма.“

([1]) ОВ L 376, 27.12.2006 г., стр. 36.
([2]) ОВ L 274, 20.10.2009 г., стр. 36.
([3]) ОВ L 13, 19.1.2000 г., стр. 12.

б) Вмъква се следният параграф 2б:

„2б. Държавите членки гарантират, че машинно обработваемата форма на техните доверителни списъци е достъпна в мястото си на публикуване по всяко време без прекъсване, освен за целите на поддръжката“.

в) Параграф 3 се заменя със следното:

„3. Държавите членки съобщават на Комисията следната информация:

а) органа или органите, отговарящи за създаването, поддържането и публикуването на машинно обработваемата форма на доверителния списък;

б) мястото на публикуване на машинно обработваемата форма на доверителния списък;

в) 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 могат да се използват за подписване на машинно обработваемата форма на доверителния списък по електронен път;

г) всички промени в информацията по букви а), б) и в).“

г) Вмъква се следният параграф 3а:

„3а. Ако държава членка публикува доверителния списък в четима от човек форма, информацията по параграф 3 се съобщава и по отношение на четимата от човек форма.“

2) Приложението се заменя с приложението към настоящото решение.

Член 2

Прилагане

Настоящото решение се прилага от 1 февруари 2014 г.

Член 3

Адресати

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 14 октомври 2013 година.

За Комисията

Michel BARNIER

Член на Комисията

ПРИЛОЖЕНИЕ

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОБЩ ОБРАЗЕЦ НА ДОВЕРИТЕЛЕН СПИСЪК НА ПОДНАДЗОРНИ/АКРЕДИТИРАНИ ДОСТАВЧИЦИ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

ОБЩИ ИЗИСКВАНИЯ

1. **Въведение**

С общия образец на доверителен списък на поднадзорни/акредитирани доставчици на удостоверителни услуги се цели създаването на общ формат, в който държавите членки да предоставят информация за състоянието на надзора/акредитацията на удостоверителните услуги, предлагани от доставчици на удостоверителни услуги ([1]) (ДУУ), намиращи се под техен надзор/акредитация по отношение на съответствието с разпоредбите на Директива 1999/93/ЕО. Това включва предоставянето на информация за състоянието на надзора/акредитацията на поднадзорните/акредитираните удостоверителни услуги през минали периоди.

Тази информация е предназначена преди всичко да подпомогне валидирането на квалифицирани електронни подписи (КЕП) и усъвършенствани електронни подписи (УЕП) ([2]), поддържани от квалифицирано удостоверение (КУ) ([3]) ([4]).

Задължителната информация в доверителния списък трябва да включва минималната необходима информация за поднадзорните/акредитираните ДУУ, издаващи квалифицирани удостоверения (КУ) ([5]) в съответствие с разпоредбите на Директива 1999/93/ЕО (член 3, параграф 2, член 3, параграф 3 и член 7, параграф 1, буква а), в това число — когато това не е част от КУ — информация за КУ, поддържащи електронен подпис, както и дали подписът е или не е създаден с помощта на устройство за създаване на защитени електронни подписи (Secure Signature Creation Device — SSCD) ([6]).

Допълнителна информация за други ДУУ, които не издават КУ, но предлагат услуги, свързани с електронни подписи (напр. ДУУ, предлагащи услуги за времеви печати (Time Stamping Services) и издаващи времеви маркери (Time Stamp Tokens); ДУУ, издаващи неквалифицирани удостоверения и т.н.), може да бъде включена на доброволна основа в доверителния списък на национално ниво, при условие че те са акредитирани/поднадзорни подобно на ДУУ, издаващи КУ, или са одобрени съгласно различна национална схема за одобрение. Възможно е в някои държави членки националните схеми за одобрение да се различават по отношение на приложимите изисквания и/или отговарящата организация от схемите за надзор или доброволна акредитация, които се прилагат за ДУУ, издаващи КУ. В настоящите спецификации понятията „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, в това число пояснение за евентуалните разлики спрямо схемите за надзор/акредитация, които се прилагат за ДУУ, издаващи КУ.

Общият образец се основава върху техническата спецификация TS 119 612 v1.1.1 ([7]) на ETSI (наричана по-долу „ETSI TS 119 612“), в която се разглеждат създаването, публикуването, мястото на публикуване, достъпът, удостоверяването и интегритетът на такива списъци.

2. **Структура на общия образец за доверителен списък**

Общият образец за доверителен списък на държава членка е структуриран съгласно ETSI TS 119 612 по следните категории информация:

1. таг за доверителен списък, даващ възможност за идентифициране на доверителния списък при електронно търсене;

2. информация за доверителния списък и неговата схема на издаване;

3. поредица от полета, съдържащи информация за еднозначно идентифициране на всеки ДУУ под надзор/акредитация по схемата (тази поредица е незадължителен елемент, т.е. когато тя не е използвана, се предполага, че списъкът е празен, т.е. в съответната държава членка няма поднадзорни или акредитирани ДУУ в обхвата на доверителния списък);

4. за всеки включен в списъка ДУУ — данните за неговите специфични удостоверителни услуги, чието актуално състояние се отразява в доверителния списък, се предоставят като поредица от полета, еднозначно идентифициращи предлаганите от ДУУ поднадзорни/акредитирани удостоверителни услуги и тяхното актуално състояние (тази поредица трябва да има поне един елемент);

([1]) Както е определено в член 2, параграф 11 от Директива 1999/93/ЕО.
([2]) Както е определено в член 2, параграф 2 от Директива 1999/93/ЕО.
([3]) За УЕП, поддържан от КУ, в настоящия документ се използва съкращението $УЕП_{КУ}$.
([4]) Трябва да се отбележи, че съществуват редица електронни услуги на базата на прости УЕП, чието трансгранично използване също ще бъде улеснено, при положение че поддържащите ги удостоверителни услуги (напр. издаване на неквалифицирани удостоверения) са част от поднадзорните/акредитираните услуги, включени от дадена държава членка в частта за доброволна информация в нейния доверителен списък.
([5]) Както е определено в член 2, параграф 10 от Директива 1999/93/ЕО.
([6]) Както е определено в член 2, параграф 6 от Директива 1999/93/ЕО.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) — Electronic Signatures and Infrastructures (ESI); Trusted Lists (Електронни подписи и инфраструктури (ЕПИ): Доверителни списъци).

5. за всяка включена в списъка поднадзорна/акредитирана удостоверителна услуга — информацията за историята на състоянието (когато това е приложимо);

6. подписа, използван за доверителния списък.

В контекста на ДУУ, издаващи КУ, структурата на доверителния списък, и по-специално елементът с информация за услугата (съгласно точка 4 по-горе), дава възможност допълнителната информация в разширената информация за услугата да компенсира ситуациите, при които в квалифицираното удостоверение липсва достатъчно (машинно обработваема) информация относно неговото квалифицирано състояние, евентуалната му поддръжка от SSCD, и особено да реши проблема, произтичащ от факта, че повечето (търговски) ДУУ използват един единствен издаващ удостоверяващ орган (УО) за издаването на няколко типа потребителски удостоверения — както квалифицирани, така и неквалифицирани.

В контекста на услугите на УО за генериране на удостоверение броят на вписванията в списъка на услуги за ДУУ може да бъде намален, ако съществуват една или повече услуги на УО на по-високо ниво в рамките на PKI на ДУУ (напр. в контекста на йерархичната верига на УО, свързваща един базов УО с издаващи УО), като в списъка се впишат услугите на УО от по-високо ниво, а не услугите на УО, издаващи потребителски удостоверения (напр. като се впишат само услугите на базовия УО за ДУУ). Въпреки това в тези случаи информацията за състоянието се прилага за цялата йерархия на услугите на УО, спадащи под вписаната в списъка услуга, като трябва да бъде спазен и гарантиран принципът за осигуряване на еднозначна връзка между удостоверителната услуга на $ДУУ_{КУ}$ и набора от удостоверения, които трябва да се идентифицират като КУ.

2.1. *Описание на информацията във всяка категория*

1. Таг за доверителен списък

2. Информация за доверителния списък и неговата схема на издаване

В тази категория се включва следната информация:

— **идентификатор за версията на формàта** на доверителния списък,

— **пореден номер (номер на версията)** на доверителния списък,

— **информация за типа** на доверителния списък (напр. за установяване на факта, че доверителният списък дава информация за състоянието на надзор/акредитация на удостоверителни услуги на ДУУ, които са под надзора/акредитацията на съответната държава членка по отношение на съответствието им с разпоредбите на Директива 1999/93/ЕО),

— **информация за оператора (собственика) на схемата** на доверителния списък (напр. име, адрес, контактни данни и т.н. на органа на съответната държава членка, натоварен със създаването, сигурното публикуване и поддръжката на доверителния списък),

— **информация за базовите схеми на надзор/акредитация**, с които е свързан доверителният списък, която включва, но не се ограничава до:

  — държавата, в която те се прилагат,

  — указание за или препратка към мястото, където може да бъде намерена информация за схемите (модел на схемата, правила, критерии, засегната група, тип и т.н.),

  — период на съхраняване на данни (за минали периоди),

— **политика и/или правен коментар, задължения, отговорности във връзка** с доверителния списък,

— **дата и час на издаване** на доверителния списък,

— **следващо планувано актуализиране** на доверителния списък.

3. Еднозначна информация за идентифициране на всеки ДУУ, който е поднадзорен/акредитиран съгласно схемата

Този пакет от информации включва най-малко следното:

— наименование на организацията на ДУУ, както се използва при формални правни регистрации (включително UID на организацията на ДУУ в зависимост от практиката в държавата членка),

— адрес и контактни данни на ДУУ,

— допълнителна информация за ДУУ, включена непосредствено или чрез препратка към адрес, откъдето може да бъде изтеглена.

4. За всеки включен в списъка ДУУ — поредица от полета, съдържащи информация за еднозначно идентифициране на удостоверителна услуга, предлагана от ДУУ и попадаща под надзор/акредитация по смисъла на Директива 1999/93/ЕО

Този пакет от информации включва най-малко следното за всяка удостоверителна услуга, предлагана от включен в списъка ДУУ:

— идентификатор на типа на услугата: идентификатор на типа на удостоверителната услуга (напр. идентификатор, указващ, че поднадзорната/акредитираната удостоверителна услуга на ДУУ представлява удостоверяващ орган, който издава КУ),

— (търговско) име на услугата: (търговско) име на удостоверителната услуга,

— цифрова идентификация на услугата: еднозначен уникален идентификатор на удостоверителната услуга,

— актуално състояние на услугата: идентификатор на актуалното състояние на услугата,

— начални дата и час на актуалното състояние,

— разширена информация за услугата, когато е приложимо: допълнителна информация за услугата (напр. включена непосредствено или чрез препратка към адрес, откъдето може да бъде изтеглена): информация за определението на услугата, предлагана от оператора на схемата, достъп до информация във връзка с услугата, информация за определението на услугата, предлагана от ДУУ, и разширена информация за услугата. За услуги от тип УО/КУ — незадължителна поредица от кортежи от данни, като всеки кортеж включва:

  — критерии за допълнително идентифициране (филтриране) в рамките на идентифицираната доверителна услуга, които определят точен набор от резултати от услугата (напр. набор от (квалифицирани) удостоверения), за която се изисква/предлага допълнителна информация, с оглед на установяване на нейното състояние, наличието на поддръжка от SSCD и/или издаване на юридическо лице, както и

  — свързани „квалификатори“, даващи информация дали наборът от резултати от услугата идентифицира удостоверенията, които трябва да се считат за квалифицирани, и/или дали идентифицираните квалифицирани удостоверения от тази услуга се поддържат от SSCD или не, и/или дали тези КУ се издават на юридическо лице (в общия случай се предполага, че те се издават на физически лица).

5. За всяка включена в списъка услуга — история на състоянието

6. Компютърно генериран подпис за целите на удостоверяването за всички полета на ДС, с изключение на самата стойност на подписа

3. **Насоки за редактиране на данни в доверителния списък**

3.1. *Единен списък с информация за състоянието на поднадзорните/акредитираните удостоверителни услуги и техните доставчици*

Доверителният списък на дадена държава членка означава „Списък на състоянието на надзор/акредитация на удостоверителните услуги, предлагани от доставчици на удостоверителни услуги под надзор на/акредитирани от посочената държава членка по отношение на съответствието им с разпоредбите на Директива 1999/93/ЕО“.

Този доверителен списък е единен инструмент, който съответната държава членка използва, за да предоставя информация за състоянието на надзор/акредитация на удостоверителни услуги и техните доставчици:

— **всички доставчици на удостоверителни услуги**, както е определено в член 2, параграф 11 от Директива 1999/93/ЕО, т.е. „организация, юридическо или физическо лице, което издава удостоверения или предоставя други услуги, свързани с електронните подписи“,

— **които са под надзор/акредитирани** по отношение на съответствието им с разпоредбите на Директива 1999/93/ЕО.

Съгласно определенията и разпоредбите на Директива 1999/93/ЕО, по-конкретно по отношение на съответните ДУУ и техните системи за надзор/доброволна акредитация, могат да бъдат разграничени два вида ДУУ, а именно ДУУ, които издават КУ на потребители ($ДУУ_{КУ}$), и ДУУ, които не издават КУ на потребители, но предлагат „други (спомагателни) услуги, свързани с електронните подписи“:

— **ДУУ, които издават КУ**:

  — Те трябва да бъдат под надзора на държавата членка, в която са установени (ако са установени в държава членка), и могат също да бъдат акредитирани по отношение на съответствието им с разпоредбите на Директива 1999/93/ЕО, в това число разпоредбите на приложение I (изисквания към КУ) и разпоредбите на приложение II (изисквания към ДУУ, издаващи КУ). ДУУ, издаващи КУ, които са акредитирани в дадена държава членка, трябва независимо от това да са включени в адекватна система за надзор на държавата членка, освен ако не са установени в тази държава членка.

— Приложимата система за „надзор“ (съответно системата за „доброволна акредитация“) е определена и трябва да отговаря на съответните изисквания на Директива 1999/93/ЕО, по-специално на съдържащите се в член 3, параграф 3, член 8, параграф 1, член 11, съображение 13 (съответно член 2, параграф 13, член 3, параграф 2, член 7, параграф 1, буква а), член 8, параграф 1, член 11, съображения 4, 11, 12 и 13).

— **ДУУ, които не издават КУ**:

— Те могат да бъдат включени в система за „доброволна акредитация“ (както е определено в Директива 1999/93/ЕО и съгласно нея) и/или в определена национална „призната схема за одобрение“, осъществяваща на национална основа надзор за съответствие с разпоредбите на директивата и евентуално с национални разпоредби по отношение на предоставянето на удостоверителни услуги (по смисъла на член 2, параграф 11 от Директива 1999/93/ЕО).

— Някои от физическите или двоичните (логическите) обекти, генерирани или издадени в резултат на предоставянето на удостоверителна услуга, могат да притежават специални „квалификации“, основаващи се на съответствие с разпоредбите и изискванията на национално ниво, но значението на тези „квалификации“ вероятно ще бъде ограничено единствено до национално ниво.

Всяка държава членка трябва да създаде и да поддържа един-единствен доверителен списък, указващ състоянията на надзор/акредитация на удостоверителните услуги на ДУУ под неин надзор/акредитация. Доверителният списък включва като минимум доставчиците на удостоверителни услуги, които издават квалифицирани удостоверения. Доверителният списък може да указва също и състоянието на други удостоверителни услуги под надзор/акредитация в рамките на определена схема за одобрение на национално равнище.

3.2. *Единен набор от стойности за състоянието на надзор/акредитация*

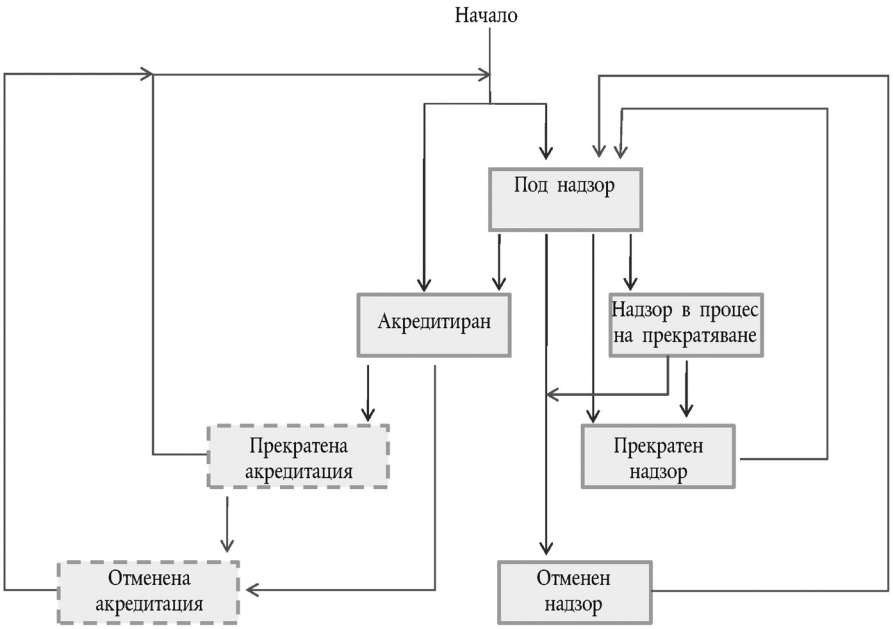
В доверителния списък фактът, че услугата към момента е „под надзор“ или „акредитирана“, се определя от стойността на нейното актуално състояние. Освен това състоянието на надзор или акредитация може да бъде положително („under supervision“ — „под надзор“; „accredited“ — „акредитирана“; „supervision in cessation“ — „надзор в процес на преустановяване“), преустановено („supervision ceased“ — „преустановен надзор“; „accreditation ceased“ — преустановена акредитация“) или отменено („supervision revoked“ — „отменен надзор“; „accreditation revoked“ — „отменена акредитация“), като се обозначава със съответната стойност. В рамките на своето съществуване една удостоверителна услуга може да преминава от режим на надзор в режим на акредитация и обратно ([1]).

Графика 1 показва очакваните промени на възможните състояния на надзор/акредитация на дадена удостоверителна услуга:

([1]) Напр. доставчик на удостоверителни услуги, установен в дадена държава членка, който предлага удостоверителна услуга, намираща се първоначално под надзора на държавата членка (надзорния орган), може след известно време да реши да се подложи на доброволна акредитация за удостоверителната услуга, намираща се понастоящем под надзор. Обратно, доставчик на удостоверителни услуги в друга държава членка може да реши да не прекратява предлагането на дадена акредитирана удостоверителна услуга, а да я прехвърли от състояние на акредитация в състояние на надзор, напр. поради търговски и/или икономически причини.

Графика 1

Очаквани промени в състоянието на надзор/акредитация на услуга, предлагана от ДУУ



Легенда:

Преходно състояние, ако има свързан модел на надзор (напр. за ДУУ, издаващ КУ под надзор/акредитация в държавата членка, в която е установен).
Възможно актуално състояние, ако липсва свързан модел на надзор (напр. ДУУ, акредитиран в държава членка, в която не е установен).

Възможно актуално състояние

Когато е установена в държава членка, удостоверителната услуга, издаваща КУ, трябва да бъде под надзор (от страна на държавата членка, в която е установена) и може да бъде доброволно акредитирана. Стойността за състоянието на такава услуга, когато е включена в доверителния списък, трябва да бъде обозначена с една от горепосочените „стойности за актуалното състояние“ в съответствие с актуалното ѝ състояние и, ако е приложимо, да се променя съгласно горепосочените промени в състоянието. „Accreditation ceased“(„преустановена акредитация“) и „accreditation revoked“ („отменена акредитация“) обаче трябва да бъдат стойности за „преходно състояние“, когато съответната услуга на $ДУУ_{КУ}$ е включена в доверителния списък на държава членка, в която е установена, тъй като такива услуги трябва да са поднадзорни по подразбиране (дори когато не са акредитирани или вече не са акредитирани); когато съответната услуга е включена в списък (акредитирана) в държава членка, различна от държавата, в която е установена, тези стойности могат да бъдат окончателни.

Държавите членки, които създават или са създали определени в национален мащаб „признати схеми за одобрение“, използвани на национална основа за надзор по отношение на съответствието на услугите на ДУУ, които **не** издават КУ, с разпоредбите на Директива 1999/93/ЕО и с евентуални национални разпоредби относно предлагането на удостоверителни услуги (по смисъла на член 2, параграф 11 от Директива 1999/93/ЕО), трябва да категоризират такива схеми за одобрение в една от следните две категории:

— „доброволна акредитация“, както е определена и регламентирана в Директива 1999/93/ЕО (член 2, параграф 13, член 3, параграф 2, член 7, параграф 1, буква а), член 8, параграф 1, член 11, съображения 4, 11, 12, и 13),

— „надзор“, както е определен в Директива 1999/93/ЕО и приложен в национални разпоредби и изисквания в съответствие с националното законодателство.

По същия начин удостоверителна услуга, която не издава КУ, може да бъде поднадзорна или доброволно акредитирана. Стойността за състоянието на такава услуга, когато е включена в доверителния списък, трябва да бъде обозначена с една от горепосочените стойности за състоянието като „стойност за актуалното състояние“ (вж. графика 1) в съответствие с актуалното ѝ състояние и, ако е приложимо, да се променя съгласно горепосочените преходи в състоянието.

Доверителният списък трябва да съдържа информация за базовите схеми за надзор/акредитация, по-конкретно:

— информация за системата на надзор, приложима за всеки ДУУ$_{КУ}$,

— информация, когато е уместно, за националната схема за „доброволна акредитация“, приложима за всеки ДУУ$_{КУ}$,

— информация, когато е уместно, за системата на надзор, приложима за всеки ДУУ, който не издава КУ,

— информация, когато е уместно, за националната схема за „доброволна акредитация“, приложима за всеки ДУУ, който не издава КУ.

Последните два пакета от информация са от ключово значение, за да могат доверяващите се страни да оценят качеството и нивото на сигурност на такива системи за надзор/акредитация, прилагани на национално ниво към ДУУ, които не издават КУ. Когато в доверителния списък се предоставя информация за състоянието на надзор/акредитация по отношение на услугите на ДУУ, които не издават КУ, гореспоменатите пакети от информация се предоставят на ниво доверителен списък, като се използват „URI за информация за схемата (Scheme information URI)“ (клауза 5.3.7 — информация, предоставяна от държавите членки), „Тип/общност/правила на схемата (Scheme type/community/rules)“ (клауза 5.3.9, като се използват общи за всички държави членки формулировки и незадължителна, предоставяна от държавата членка, специфична информация) и „Политика/правен коментар на ССДУ (TSL policy/legal notice)“ (клауза 5.3.11 — обща за всички държави членки формулировка, позоваваща се на Директива 1999/93/ЕО, и възможност за всяка държава членка да добави специфични национални формулировки или позовавания).

Допълнителна информация за „квалификацията“ на нивото на националните системи за надзор/акредитация на ДУУ, които не издават КУ, може да се предоставя на нивото на услугата, ако е уместно и необходимо (напр. за да се различават отделните нива на качество/сигурност), като се използва разширението „additionalServiceInformation“(„допълнителна информация за услугата“ (клауза 5.5.9.4) като част от „Service information extension“ („разширена информация за услугата) (клауза 5.5.9). Допълнителна информация за съответните технически спецификации се предоставя в подробните спецификации в глава I.

Въпреки възможността надзорът и акредитацията на удостоверителни услуги в дадена държава членка да се осъществяват от различни органи, очаква се за дадена удостоверителна услуга да се използва само едно вписване и нейното състояние на надзор/акредитация да се актуализира съответно.

3.3. *Вписвания в доверителния списък с цел улесняване на валидирането на КЕП и УЕП$_{КУ}$*

Най-критичната част от създаването на доверителния списък е установяването на задължителната му част, а именно на „Списъка на услугите“ на всеки ДУУ, издаващ КУ, с цел да се отрази коректно състоянието на всяка такава услуга за издаване на КУ и да се гарантира, че предоставената във всяко вписване информация е достатъчна за валидирането на КЕП и УЕП$_{КУ}$ (когато се комбинира със съдържанието на потребителското КУ, издадено от ДУУ в рамките на удостоверителната услуга, посочена в даденото вписване).

Изискваната информация може да включва и информация, различна от тази в „Service digital identity“ („цифрова идентификация на услугата“) на даден (базов) УО, по-специално информация относно състоянието на КУ на удостоверенията, издадени чрез услугата за УО, и информация за това дали поддържаните подписи са или не са създадени чрез SSCD. Органът на държавата членка, натоварен със създаването, актуализирането и поддръжката на доверителния списък, трябва следователно да вземе предвид актуалния профил и съдържанието на удостоверението за всяко КУ, издадено от ДУУ$_{КУ}$, който е включен в доверителния списък.

В идеалния случай всяко издадено КУ следва да съдържа определената от ETSI декларация QcCompliance [1], когато е обявено като КУ, и да съдържа определената от ETSI декларация QcSSCD, когато се твърди, че то се поддържа от SSCD при генерирането на електронни подписи и/или всяко издадено КУ включва един от обектните идентификатори (OID) на политиката за сертифициране QCP/QCP+, определени в ETSI EN 319 411-2 [2]. Използването на различни стандарти от страна на ДУУ, издаващи КУ, голямата свобода на интерпретация, която тези стандарти позволяват, както и липсата на осведоменост относно наличието и приоритета на някои технически спецификации или стандарти са довели до разлики в действителното съдържание на издаваните понастоящем КУ (напр. относно използването или не на определените от ETSI декларации) и съответно не позволяват на получателя просто да разчита на удостоверението на подписващата страна (и свързаната с него верига от удостоверения) при извършването на оценка (най-малкото на машинна такава) дали удостоверението, поддържащо електронен подпис, е обявено за КУ и дали то е или не е свързано със SSCD, чрез което е бил създаден електронният подпис.

[1] За справка вж ETSI EN 319 412-5 — Electronic Signatures and Infrastructures (ESI): Profiles for Trust Service Providers issuing certificates. Part 5: Extension for Qualified Certificate profile) for the definition of such a statement (Електронни подписи и инфраструктури (ЕПИ): Профили за доставчици на доверителни услуги, които издават удостоверения. Част 5: Разширение за профил на квалифицирано удостоверение).

[2] ETSI TS 319 411-2 — Electronic Signatures and Infrastructures (ESI): Policy and security requirements for Trust Service Providers issuing certificates. Part 2: Policy requirements for certification authorities issuing qualified certificates (Електронни подписи и инфраструктури (ЕПИ): Политика и изисквания за сигурност за доставчици на доверителни услуги, които издават удостоверения. Част 2: Изисквания към политиката за удостоверяващи органи, които издават квалифицирани удостоверения).

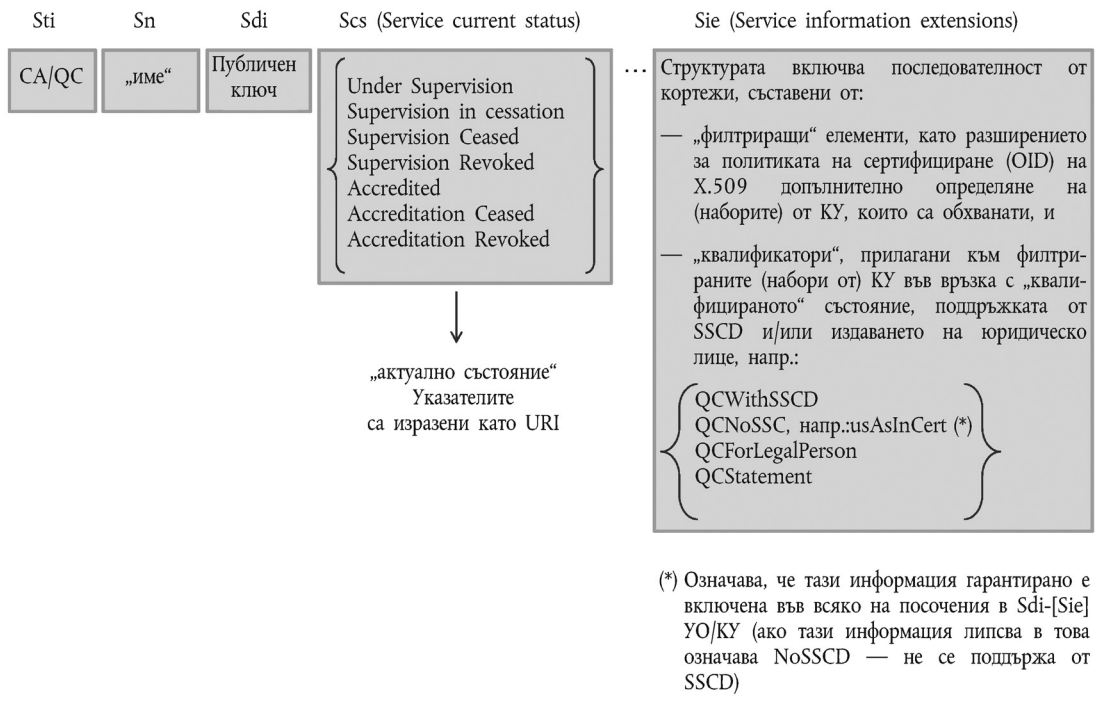
При вписване на услуга в доверителния списък попълването на полетата „Service type identifier“ („Sti“ — „Идентификатор на типа на услугата“), „Service name“ („Sn“ — „Име на услугата“) и „Service digital identity“ („Sdi“ — „Цифрова идентификация на услугата“) с информация, предоставена в полето „Service information extensions“ („Sie“ — „Разширена информация за услугата“), дава възможност да се определи напълно специфичният тип квалифицирано удостоверение, издадено от удостоверяваща услуга на включен в списъка ДУУ, издаващ КУ, и да се предостави информация дали то се поддържа от SSCD или не (когато такава информация липсва в издаденото КУ). С това вписване е свързана специфична информация в полето „Service current status“ („Scs“ — „Актуално състояние на услугата“). Това е показано на графика 2 по-долу.

Включването в списъка на услуга, за която се предоставя само „Sdi“ на (базовия) УО ще означава, че е гарантирано (от ДУУ, издаващ КУ, но и от надзорния/акредитиращия орган, отговарящ за надзора/акредитацията на този ДУУ), че всяко потребителско удостоверение, издадено в рамките на йерархията на този (базов) УО, съдържа достатъчно определена от ETSI и обработваема машинно информация, за да може да бъде преценено дали то е или не е КУ и дали се поддържа от SSCD. Когато например последното твърдение не е вярно (т.е. в КУ липсва стандартизирана от ETSI и машинно обработваема информация дали то се поддържа от SSCD), то въз основа само на „Sdi“ на (базовия) УО ще може единствено да се предположи, че КУ, издадени от тази йерархична верига на (базов) УО, не се поддържат от SSCD. За да се обозначи, че такива КУ трябва да се считат за поддържани от SSCD, следва да се използва полето „Sie“ (това означава също, че коректността на информацията се гарантира от ДУУ, издаващ КУ и намиращ се под надзора/акредитацията съответно на надзорен или акредитиращ орган).

Графика 2

Вписване на услуга за услуга на ДУУ, който издава КУ и е включен в доверителния списък

Основни принципи – правила за редактиране – вписвания за ДУУ$_{КУ}$ (включени в списъка услуги)



(*) Означава, че тази информация гарантирано е включена във всяко на посочения в Sdi-[Sie] УО/КУ (ако тази информация липсва в това означава NoSSCD — не се поддържа от SSCD)

Настоящите технически спецификации на общ образец за доверителен списък позволяват във вписването за услугата да се използва комбинация от пет основни елемента на информацията:

— идентификатор на типа на услугата в полето „Service type identifier“ („Sti“), напр. за да се идентифицира УО, издаващ КУ („CA/QC“ — „УО/КУ“),

— име на услугата в полето „Service name“ („Sn“),

— информация в полето „Service digital identity“ („Sdi“), идентифицираща услуга от списъка, напр. публичния ключ (като минимум) на УО, издаващ КУ,

— за услуги от типа УО/КУ — незадължителна информация в полето „Service information extension“ („Sie“), позволяваща включването на определен брой специфични за услугата позиции във връзка с отмяна на изтекли удостоверения, допълнителни характеристики на КУ, поглъщане на ДУУ от друг ДУУ и друга допълнителна информация за услугата. Например допълнителните характеристики на КУ се представят чрез поредица от един или повече кортежи, като всеки кортеж включва:

— критерии за допълнително идентифициране (филтриране) в рамките на идентифицираната в полето „Sdi“ удостоверителна услуга, които определят набора от квалифицирани удостоверения, за които се изисква/предлага допълнителна информация, с цел обозначаване на „квалифицирано“ състояние, поддръжка от SSCD и/или издаване на юридическо лице; както и

— свързана информация („квалификатори“), указваща дали този набор от квалифицирани удостоверения трябва да се счита за квалифициран, дали се поддържа или не от SSCD и дали тази свързана информация е част от КУ в стандартизиран формат, позволяващ машинна обработка, и/или информация дали такива КУ се издават и на юридически лица (по подразбиране те се издават само на физически лица);

— информацията за „актуалното състояние“ на тази вписана услуга изяснява:

— дали услугата е под надзор или акредитирана, и

— какво е състоянието на надзора/акредитацията.

3.4. *Насоки за редактиране и използване на вписвания на услуги, предлагани от ДУУ$_{КУ}$*

Основните насоки за редактиране са:

1. Ако е сигурно (гаранция от страна на ДУУ$_{КУ}$, който е под надзор/акредитация на надзорен орган (НО)/акредитиращ орган (АО), че за вписана в списъка услуга, идентифицирана чрез „Sdi“, всяко КУ, поддържано от SSCD, съдържа определената от ETSI декларация QcCompliance и декларацията QcSSCD и/или идентификатора QCP + Object Identifier (OID), то използването на подходяща „Sdi“ е достатъчно и полето „Sie“ може да се използва по желание, като не е необходимо да съдържа информация за поддръжката от SSCD.

2. Ако е сигурно (гаранция от страна на ДУУ$_{КУ}$, който е под надзор/акредитация на НО/АО), че за вписана в списъка услуга, идентифицирана чрез „Sdi“, всяко КУ, което не се поддържа от SSCD, съдържа декларацията QcCompliance и/или QCP OID и не съдържа декларацията QcSSCD или QCP + OID, то използването на подходяща „Sdi“ е достатъчно и полето „Sie“ може да се използва по желание, като не е необходимо да съдържа информация за поддръжката от SSCD (което означава, че не се поддържа от SSCD).

3. Ако е сигурно (гаранция от страна на ДУУ$_{КУ}$, който е под надзор/акредитация на НО/АО), че за вписана в списъка услуга, идентифицирана чрез „Sdi“, всяко КУ съдържа декларацията QcCompliance, като някои от тези КУ се поддържат от SSCD, а други не (това може да бъде указано напр. чрез различни специфични за ДУУ OID на политиката за сертифициране или чрез друга специфична за ДУУ информация в КУ, пряко или непряко, в машинно обработваем формат или не), но удостоверенията, които не се поддържат от SSCD, не съдържат НИТО декларацията QcSSCD, НИТО определения от ETSI идентификатор QCP(+) OID, то използването на подходяща „Sdi“ може да не бъде достатъчно И полето „Sie“ трябва да се използва за предоставяне на изрична информация относно поддръжката от SSCD, както и на възможна разширена информация за идентифициране на обхванатия набор от удостоверения. Това вероятно ще изисква включването на различни „стойности, характеризиращи поддръжката от SSCD“ за една и съща информация в полето „Sdi“, когато се използва полето „Sie“.

4. Ако е сигурно (гаранция от страна на ДУУ$_{КУ}$, който е под надзор/акредитация на НО/АО), че за вписана в списъка услуга, идентифицирана чрез „Sdi“, нито едно КУ не съдържа декларацията QcCompliance, QCP OID, декларацията QcSSCD или QCP(+) OID, но е сигурно, че някои от тези потребителски удостоверения, издадени с тази „Sdi“, са предвидени да бъдат КУ и/или да се поддържат от SSCD, а други не (това може да бъде указано напр. чрез различни специфични за ДУУ$_{КУ}$ OID на политиката за сертифициране или чрез друга специфична за ДУУ информация в КУ, пряко или непряко, в машинно обработваем формат или не), то използването на подходяща информация в „Sdi“ няма да бъде достатъчно И полето „Sie“ трябва да се използва за включване на изрична информация относно квалификацията. Това вероятно ще изисква включването на различни „стойности, характеризиращи поддръжката от SSCD“ за една и съща информация в полето „Sdi“, когато се използва полето „Sie“.

Основен принцип по подразбиране е, че при вписаните в доверителния списък ДУУ трябва да има едно вписване за услуга за всеки публичен ключ за удостоверителна услуга от типа УО/КУ, т.е. удостоверяващ орган, издаващ (пряко) КУ. При някои изключителни обстоятелства и грижливо контролирани условия надзорният/акредитиращият орган на държавата членка може да реши да използва като „Sdi“ за едно вписване в списъка с услуги от включен в списъка ДУУ публичния

ключ на базов УО или УО от по-високо ниво в рамките на PKI на ДУУ (напр. в контекста на йерархична верига на УО на ДУУ, свързваща един базов УО с няколко издаващи УО), вместо да вписва всички подчинени услуги на издаващи УО (т.е. включване на удостоверяващ орган, който не издава пряко потребителски КУ, но сертифицира йерархични вериги от УО до нивото на УО, издаващи потребителски КУ). Последствията (предимства и недостатъци) от използването на публичния ключ на такъв базов УО или УО от по-високо ниво като стойност в „Sdi“ при вписване на услуги в доверителен списък трябва да бъдат добре премислени, когато се прилагат от държавите членки. Освен това, когато се прилага това разрешено изключение от основния принцип, държавите членки трябва да осигурят необходимата документация, даваща възможност за конструиране и проверка на удостоверителната верига. Например в контекста на $ДУУ_{КУ}$, използващи един базов УО, в чиято йерархична верига различни УО издават квалифицирани и неквалифицирани удостоверения, но чиито КУ съдържат само декларацията QcCompliance без информация относно поддръжката от SSCD, вписването на „Sdi“ само на базовия УО ще означава (съгласно правилата, обяснени по-горе), че никое КУ, издадено от йерархичната верига на този базов УО, не се поддържа от SSCD. Ако са налице КУ, които в действителност се поддържат от SSCD, но удостоверенията не съдържат машинно обработваема декларация, указваща такава поддръжка, настоятелно се препоръчва в издаваните в бъдеще квалифицирани удостоверения да се използва декларацията QcSSCD. Междувременно (до изтичане на срока на валидност на последното УО, което не съдържа тази информация) в доверителния списък следва да се използва полето „Sie“ и свързаното разширение „Qualifications Extension“, напр. филтриране на информация за идентифициране на набор(и) от удостоверения чрез специфични определени от $ДУУ_{КУ}$ OID, които евентуално се използват от $ДУУ_{КУ}$ за разграничаване на различните видове КУ (поддържани от SSCD или не), и съдържащи изрична „информация за поддръжката от SSCD“ с оглед на набора (наборите) от удостоверения, идентифицирани (филтрирани) въз основа на „квалификатори“.

Основните насоки за използване на приложения за електронни подписи, услуги или продукти, ползващи доверителния списък в съответствие с настоящите технически спецификации, са следните:

Стойност „CA/QC“ („УО/КУ“) в полето „Sti“ (по подобен начин това важи за стойност „CA/QC“ („УО/КУ“), квалифицирана допълнително като базова (RootCA/QC) чрез полето „Sie“ (additionalServiceInformation Extension)

— указва, че всички издадени от идентифицирания чрез „Sdi“ УО (по същия начин това важи за базовия УО, указан в „Sdi“ при йерархична верига) потребителски удостоверения са КУ, **при условие** че са декларирани като такива в удостоверението с помощта на подходяща машинно обработваема декларация от тип QcStatement (т.е. QcCompliance) и/или определени от ETSI QCP(+) OID, като това се гарантира от надзорен/акредитиращ орган (вж. по-горе „Основните насоки за редактиране“)

Забележка: ако в полето „Sie“ липсва информация за „Qualifications Extension“ („разширени квалификации“) или ако потребителско удостоверение, което е обявено за КУ, не е идентифицирано допълнително чрез свързани „Qualifications Extension“ („разширени квалификации“) в поле „Sie“, то машинно обработваемата информация, която се съдържа в КУ, се приема за коректна въз основа на факта, че е под надзор/акредитирана. Това означава, че се гарантира, че употребата (или не) на подходящи декларации от тип QcStatements (т.е. QcCompliance, QcSSCD) и/или определени от ETSI QCP(+) OID е в съответствие с това, което се твърди от $ДУУ_{КУ}$

— **и КОГАТО** в полето „Sie“ е налице информация за „Qualifications Extension“ („разширени квалификации“), в допълнение към горното принципно правило за тълкуване на удостоверенията, то удостоверенията, идентифицирани чрез употребата на информация за „Qualifications Extension“ в „Sie“, изградена на принципа на последователност от филтри за допълнително идентифициране на набор от удостоверения, трябва да се разглеждат в съответствие със съответните квалификатори, предоставящи допълнителна информация относно квалифицираното състояние, „поддръжката от SSCD“ и/или „юридическо лице като субект“ (напр. удостоверенията, съдържащи специфично OID в разширението за политиката на сертифициране, и/или разполагащи със специфична схема за използване на ключа, и/или филтрирани въз основа на наличието на специфична стойност в определено поле или разширение на удостоверението и т.н.). Тези квалификатори са част от следния набор от „квалификатори“, компенсиращи липсата на информация в съдържанието на съответното КУ, и се използват съответно:

— за да се укаже квалифицираното състояние: стойност на квалификатора „QCStatement“, която означава, че идентифицираното(ите) удостоверение(я) е(са) квалифицирани,

И/ИЛИ

— за да се укаже характерът на поддръжката от SSCD

— стойност на квалификатора „QCWithSSCD“, която означава „КУ се поддържа от SSCD“, или

— стойност на квалификатора „QCNoSSCD“, която означава „КУ не се поддържа от SSCD“, или

— стойност на квалификатора „QCSSCDStatusAsInCert“, която означава, че при всяко КУ информацията относно УО/КУ в полетата „Sdi“-„Sie“ гарантирано се придружава от информация относно поддръжката от SSCD;

И/ИЛИ

— за да се укаже издаването на юридическо лице:

— стойност на квалификатора „QCForLegalPerson“, която означава „удостоверението е издадено на юридическо лице“

3.5. *Услуги, които поддържат услуги от типа „УО/КУ“, но в „Sdi“ не са обозначени като „УО/КУ“*

Услугите по проверка на валидността на удостоверенията, които са свързани с КУ и за които информацията за проверката на валидността на удостоверенията (напр. CRL списъци и OCSP отговори) се подписва от субект, чийто частен ключ не е сертифициран съгласно удостоверителна верига, водеща до включен в списъка УО, издаващ КУ („CA/QC“ — „УО/КУ), се включват в доверителния списък, като тези услуги по проверка на валидността на удостоверенията се вписват като такива в ДС (т.е. чрез тип на услугата съответно „OCSP/QC“ или „CRL/QC“), тъй като тези услуги могат да се считат за част от поднадзорните/акредитираните „квалифицирани“ услуги, свързани с предлагането на удостоверителни услуги с КУ. Разбира се, издаващите OCSP отговори или CR списъци, чиито удостоверения са подписани от УО в йерархичната верига на вписана в списъка услуга от тип УО/КУ, следва да се приемат за „валидни“ и съответстващи на стойността на състоянието на вписана в списъка услуга от тип УО/КУ.

Подобна разпоредба може да се приложи към удостоверителните услуги, издаващи неквалифицирани удостоверения (услуги от тип „CA/PKC“).

Доверителният списък включва услуги по проверка на валидността на удостоверенията, когато съответната информация за местоположението на такива услуги липсва в потребителските удостоверения, за които се прилагат услугите по проверка на валидността на удостоверенията.

4. **Определения и съкращения**

За целите на настоящия документ се прилагат следните определения и съкращения:

Термин	Съкращение	Определение
Доставчик на удостоверителни услуги (Certification Service Provider)	ДУУ (CSP)	Както е определено в член 2, параграф 11 от Директива 1999/93/ЕО.
Удостоверяващ орган (Certification Authority)	УО (CA)	1) доставчик на удостоверителни услуги, който създава и присвоява удостоверения за публичен ключ; или 2) услуга за генериране на техническо удостоверение, използвана от доставчик на удостоверителни услуги, който създава и присвоява удостоверения за публичен ключ. *ЗАБЕЛЕЖКА*: За допълнително обяснение на понятието „удостоверяващ орган“ вж. клауза 4 от EN 319 411-2 ([1]).
Удостоверяващ орган, издаващ квалифицирани удостоверения	УО/КУ (CA/QC)	УО, който отговаря на изискванията, посочени в приложение II към Директива 1999/93/ЕО, и издава квалифицирани удостоверения, които отговарят на изискванията, посочени в приложение I към Директива 1999/93/ЕО.
Удостоверение (Certificate)	Удостоверение	Както е определено в член 2, параграф 9 от Директива 1999/93/ЕО.
Квалифицирано удостоверение (Qualified Certificate)	КУ (QC)	Както е определено в член 2, параграф 10 от Директива 1999/93/ЕО.
Подписваща страна (Signatory)	Подписваща страна	Както е определено в член 2, параграф 3 от Директива 1999/93/ЕО.
Надзор (Supervision)	Надзор	„Надзор“ се използва в смисъла на член 3, параграф 3 от Директива 1999/93/ЕО. Директива 1999/93/ЕО изисква държавите членки да създадат подходяща система за надзор над ДУУ, установени на тяхна територия и издаващи потребителски квалифицирани удостоверения, която да осигури надзора по отношение на съответствието с разпоредбите на директивата.
Доброволна акредитация (Voluntary Accreditation)	Акредитация	Както е определено в член 2, параграф 13 от Директива 1999/93/ЕО.
Доверителен списък (Trusted List)	ДС (TL)	Представлява списък, указващ състоянието на надзор/акредитация на удостоверителни услуги, предлагани от доставчици на удостоверителни услуги, които са под надзор/акредитация на съответната държава членка по отношение на съответствието им с разпоредбите на Директива 1999/93/ЕО.

Термин	Съкращение	Определение
Списък на състоянието на доверителни услуги (Trust-service Status List)	ССДУ (TSL)	Вид подписан списък, на базата на който се представя информация за състоянието на доверителни услуги съгласно спецификациите на ETSI TS 119 612.
Доверителна услуга (Trust Service)		Услуга, увеличаваща доверието и увереността при използването на електронни трансакции (обикновено, но не непременно, с помощта на криптографски технологии или доверителен материал) (ETSI TS 119 612). *ЗАБЕЛЕЖКА*: Този термин се използва в по-широк смисъл, отколкото удостоверителни услуги, издаващи удостоверения или предоставящи други услуги, свързани с електронни подписи.
Доставчик на доверителни услуги (Trust Service Provider)	ДДУ (TSP)	Организация, предоставяща една или повече (електронни) доверителни услуги (този термин се използва в по-широк смисъл от ДУУ).
Токен на доверителна услуга (Trust Service Token)	ТДУ (TrST)	Физически или двоичен (логически) обект, генериран или издаден в резултат на използването на доверителна услуга. Примери за двоични ТДУ са удостоверения, списъци на отменени удостоверения (Certificate Revocation Lists — CRL), времеви маркери (Time Stamp Tokens — TST) и отговори на онлайн протокол за състояние на удостоверение (Online Certificate Status Protocol — OCSP).
Квалифициран електронен подпис (Qualified Electronic Signature)	КЕП (QES)	Усъвършенстван електронен подпис (УЕП), поддържан от КУ и създаден с помощта на устройство за създаване на защитени подписи съгласно определението в член 2 от Директива 1999/93/ЕС.
Усъвършенстван електронен подпис (Advanced Electronic Signature)	УЕП (AdES)	Както е определено в член 2, параграф 2 от Директива 1999/93/ЕО.
Усъвършенстван електронен подпис, поддържан от квалифицирано удостоверение	$УЕП_{КУ}$ ($AdES_{QC}$)	Електронен подпис, отговарящ на изискванията към УЕП и поддържан от КУ съгласно определението в член 2 от Директива 1999/93/ЕС.
Механизъм (устройство) за създаване на защитени подписи (Secure Signature Creation Device)	SSCD	Както е определено в член 2, параграф 6 от Директива 1999/93/ЕО.

([1]) EN 319 411-2: Electronic Signatures and Infrastructures (ESI) (Електронни подписи и инфраструктури): Policy and security requirements for Trust Service Providers issuing certificates (Политика и изисквания за сигурност за доставчици на доверителни услуги, които издават удостоверения). Част 2: Policy requirements for certification authorities issuing qualified certificates (Изисквания към политиката за удостоверяващи органи, които издават квалифицирани удостоверения).

В следващите глави от документа ключовите думи „ТРЯБВА“, „НЕ ТРЯБВА/ТРЯБВА ДА НЕ“, „ЗАДЪЛЖИТЕЛЕН“, „СЛЕДВА“, „НЕ СЛЕДВА“, „БИ ТРЯБВАЛО“, „НЕ БИ ТРЯБВАЛО“, „ПРЕПОРЪЧИТЕЛЕН“, „МОЖЕ“ и „НЕЗАДЪЛЖИТЕЛЕН“ следва да се интерпретират в съответствие с термините на английски, описани в RFC 2119 ([1]).

ГЛАВА I

ПОДРОБНИ СПЕЦИФИКАЦИИ ЗА ОБЩИЯ ОБРАЗЕЦ ЗА ДОВЕРИТЕЛЕН СПИСЪК НА ПОДНАДЗОРНИТЕ/АКРЕДИТИРАНИТЕ ДОСТАВЧИЦИ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

Настоящите спецификации се основават на спецификациите и изискванията, определени в ETSI TS 119 612 v1.1.1 (наричани по-долу „ETSI TS 119 612“).

Когато в настоящите спецификации липсва конкретно изискване, ТРЯБВА изцяло да се прилагат изискванията на клаузи 5 и 6 от ETSI TS 119 612. Когато в настоящите спецификации съществуват конкретни изисквания, те ТРЯБВА да заместят съответните изисквания на ETSI TS 119 612. В случай на противоречия между настоящите спецификации и спецификациите от ETSI TS 119 612, ТРЯБВА да са меродавни настоящите спецификации.

Scheme operator name (име на оператора на схемата) (клауза 5.3.4)

Това поле Е ЗАДЪЛЖИТЕЛНО и ТРЯБВА да съответства на спецификациите в клауза 5.3.4 от TS 119 612.

([1]) IETF RFC 2119: Key words for use in RFCs to indicate Requirements Levels (Ключови думи, използвани в документация от тип RFC за обозначаване на различните нива на изискванията).

Дадена държава МОЖЕ да има различни надзорни и акредитиращи органи, и дори допълнителни органи за сродни оперативни дейности. Всяка държава членка определя оператора на схемата на своя доверителен списък. Очаква се надзорният орган, акредитиращият орган и операторът на схемата (когато са отделни органи) да имат свои собствени отговорности и задължения.

Всяка ситуация, в която различни органи отговарят за надзор, акредитиране или оперативни аспекти, ТРЯБВА да се отразява и обозначава надлежно като такава в информацията за схемата като част от доверителния списък, в това число специфичната информация за схемата, указана в „Scheme information URI“ (клауза 5.3.7).

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 ТРЯБВА да се използва следното име:

„EN_name_value“ = „списък на състоянието на надзор/акредитация на удостоверителните услуги, предлагани от доставчици на удостоверителни услуги, които са под надзор/акредитация на оператора на схемата на съответната държава членка по отношение на съответствието им с разпоредбите на Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните подписи“.

Scheme information URI (URI 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 за „подходящата информация за схемата“ ТРЯБВА да включва като минимум:

— Обща за всички държави членки уводна информация относно обхвата и контекста на доверителния списък, както и за базовите схеми за надзор/акредитация. Общият текст, които трябва да се използва, е поместеният по-долу текст, в който символният низ „[*име на съответната държава членка*]“ ТРЯБВА да се замени с името на съответната държава членка:

„The present list is the „Trusted List of supervised/accredited Certification Service Providers“ providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List at a national level on a voluntary basis.“

— Специфична информация за базовите схеми за надзор/акредитация, по-конкретно ([1]):

  — информация за системата на надзор, приложима за всеки ДУУ$_{КУ}$,

  — информация, когато е уместно, за националната схема за доброволна акредитация, приложима за всеки ДУУ$_{КУ}$,

  — информация, когато е уместно, за системата на надзор, приложима за всеки ДУУ, който не издава КУ,

  — информация, когато е уместно, за националната схема за доброволна акредитация, приложима за всеки ДУУ, който не издава КУ.

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

  — общо описание,

  — информация за следваната както от надзорния/акредитиращия орган, така и от страна на ДУУ процедура за осъществяване на надзор/акредитация,

  — информация за критериите, по отношение на които се осъществява надзор/акредитация на ДУУ.

— Специфична информация, когато е приложимо, за специфичните „квалификации“, които някои от физическите или двоичните (логическите) обекти, генерирани или издадени в резултат на предоставянето на удостоверителна услуга, могат да придобият въз основа на своята съвместимост с разпоредбите и изискванията на национално ниво, включително и значението на тези „квалификации“ и съответните национални разпоредби и изисквания.

Допълнителна специфична за държавата членка информация за схемата МОЖЕ да се предоставя на доброволна основа и да включва:

— информация за критериите и правилата, прилагани при избора на надзорни/одиторски органи и определящи как те осъществяват надзора (контрола)/акредитацията (одита) на ДУУ,

— друга контактна и обща информация, която засяга работата на схемата.

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

Това поле Е ЗАДЪЛЖИТЕЛНО, то ТРЯБВА да съответства на спецификациите в клауза 5.3.9 от TS 119 612 и ТРЯБВА да включва най-малко два URI:

— Общ за доверителните списъци на всички държави членки URI, насочващ към описателен текст, който ТРЯБВА да се прилага за всички доверителни списъци:

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

  Описателен текст:

  „*Participation in a scheme*

  Each Member State must create a „Trusted List of supervised/accredited Certification Service Providers“ providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

  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

  The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

([1]) Последните два пакета от информация са от ключово значение, за да могат доверяващите се страни да оценят качеството и нивото на сигурност на такива системи за надзор/акредитация, прилагани към ДУУ, които не издават КУ. Тези пакети от информация се предоставят на ниво доверителен списък, като се използват „Scheme information URI“ (клауза 5.3.7 — информация, предоставяна от държавите членки), „Scheme type/community/rules“ (клауза 5.3.9, като се използват общи за всички държави членки формулировки) и „TSL policy/legal notice“ (клауза 5.3.11 — обща за всички държави членки формулировка, позоваваща се на Директива 1999/93/ЕО, и възможност за всяка държава членка да добави специфични национални формулировки или позовавания). Допълнителна информация за националните системи за надзор/акредитация на ДУУ, които не издават КУ, 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).

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a 'voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined „recognised approval scheme" implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Article 2(11) of Directive 1999/93/EC). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific „qualification" on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a „qualification" is likely to be limited solely to the national level.

Interpretation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] are as follows:

A „CA/QC" „Service type identifier" („Sti") entry (similarly a CA/QC entry further qualified as being a „RootCA/QC" through the use of „Service information extension" („Sie") additionalServiceInformation Extension)

— indicates that from the „Service digital identifier" („Sdi") identified CA (similarly within the CA hierarchy starting from the „Sdi" identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no „Sie" „Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related „Sie" „Qualifications Extension" information, then the „machine-processable" information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF** „Sie" „Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie" „Qualifications Extension" information, which is constructed on the principle of a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing some additional information regarding the qualified status, the „SSCD support" and/or „Legal person as subject" (e.g. those 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.). Those qualifiers are part of the following set of „Qualifiers" used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the qualified status: „QCStatement" meaning the identified certificate(s) is(are) qualified;

AND/OR

— to indicate the nature of the SSCD support:

— „QCWithSSCD“ qualifier value meaning „QC supported by an SSCD“, or

— „QCNoSSCD“ qualifier value meaning „QC not supported by an SSCD“, or

— „QCSSCDStatusAsInCert“ qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the „Sdi“-„Sie“ provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— „QCForLegalPerson“ qualifier value meaning „Certificate issued to a Legal Person“.

The general interpretation rule for any other „Sti“ type entry is that the listed service named according to the „Sn“ field value and uniquely identified by the „Sdi“ field value has a current supervision/accreditation status according to the „Scs“ 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 Technical specifications for a Common Template for the „Trusted List of supervised/accredited Certification Service Providers“ in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the Member States' Trusted Lists.“ “

— Специфичен за доверителния списък на всяка държава членка идентификатор (URI), насочващ към описателен текст, който ТРЯБВА да се прилага за доверителния списък на тази държава членка:

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

— където потребителите могат да намерят специфичните за съответната държава членка политика/правила, съгласно които включените в списъка услуги ТРЯБВА да се оценяват в съответствие с подходяща система за надзор и схеми за акредитация на държавата членка,

— където потребителите могат да намерят специфично за дадената държава членка описание как да използват и тълкуват съдържанието на доверителния списък по отношение на удостоверителните услуги, които не са свързани с издаването на КУ. То може да се използва за обозначаване на потенциална степен на неоднородност между националните системи за надзор/акредитация по отношение на ДУУ, които не издават 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 идентификатори (URI) на базата на горепосочения специфичен за държавата членка идентификатор (т.е. адреси, попадащи в йерархията на този специфичен адрес).

TSL policy/legal notice (Политика/правен коментар на 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 доверителният списък, ТРЯБВА да бъде многоезичен символен низ (неформатиран текст), състоящ се от две части:

1. Първа, задължителна част, обща за доверителните списъци на всички държави членки (задължително на английски (EN UK) и евентуално на един или повече национални езици), указваща, че приложимата законова рамка е Директива 1999/93/ЕО и съответната ѝ реализация в законодателството на държавата членка, посочена в полето „Scheme Territory“ („Територия на схемата“).

Английска версия на общия текст:

The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

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

Текст на националния език (националните езици) на държавата членка: Текст на български език [превод на горния английски текст]: Приложимата законова рамка за настоящата ССДУ реализация на доверителния списък на поднадзорните/акредитираните доставчици на удостоверителни услуги от [име на съответната държава членка] е Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните подписи и нейната реализация в законодателството на [име на съответната държава членка].

2. Втора, незадължителна част, специфична за всеки доверителен списък (задължително на английски (EN UK) и евентуално на един или повече национални езици), включваща препратки към специфични приложими национални законови рамки (напр. конкретно във връзка с национални схеми за надзор/акредитация на ДУУ, които не издават КУ).

ГЛАВА II

НЕПРЕКЪСНАТОСТ НА ДОВЕРИТЕЛНИТЕ СПИСЪЦИ

Удостоверенията, за които Комисията се уведомява съгласно член 3, буква в) от настоящото решение, ТРЯБВА да се издават по такъв начин, че:

— между датите им на валидност да има минимум три месеца,

— да са създадени по нови двойки ключове, тъй като вече използвани двойки ключове не могат да бъдат удостоверени повторно.

В случай на разкриване или на прекратяване на използването на ЕДИН от частните ключове, съответстващ на публичен ключ, който би могъл да се използва за валидиране на подписа на доверителния списък и за който Комисията е била уведомена и го е публикувала в централните си списъци с указатели, държавите членки ТРЯБВА:

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

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

В случай на разкриване или на прекратяване на използването на ВСИЧКИ частни ключове, съответстващи на публични ключове, които биха могли да се използват за валидиране на подписа на доверителния списък и за които Комисията е била уведомена и ги е публикувала в централните си списъци с указатели, държавите членки ТРЯБВА:

— да генерират нови двойки ключове, които биха могли да се използват за подписване на доверителния списък, и съответстващите им удостоверения за публичен ключ,

— незабавно да издадат нов доверителен списък, който е подписан 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 публичен ключ, съответстващи на частните ключове, които биха могли да се използват за подписване на доверителния списък.

ГЛАВА III

СПЕЦИФИКАЦИИ ЗА ЧЕТИМАТА ОТ ЧОВЕК ФОРМА НА ДОВЕРИТЕЛНИЯ СПИСЪК

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

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

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

— Всяко налично поле СЛЕДВА да е изобразено и да съдържа:

  — наименование на полето (напр. „Service type identifier“),

  — стойност на полето (напр. „CA/QC“),

  — значение (описание) на стойността на полето, когато е уместно (напр. „Удостоверяващ орган, който издава удостоверения за публичен ключ.“),

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

[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).

— В четимата от човек форма на доверителния списък СЛЕДВА да бъдат изобразени като минимум следните полета и съответни стойности на цифровите удостоверения, посочени в полето „Service digital identity“:

  — Версия

  — Сериен номер

  — Сигнатурен алгоритъм

  — Издател

  — Валидно от

  — Валидно до

  — Предмет

  — Публичен ключ

  — Политики на удостоверението

  — Идентификатор на ключа на субекта

  — Точки на разпространение на CR списъци

  — Идентификатор на ключа на органа

  — Употреба на ключа

  — Основни ограничения

  — Алгоритъм на електронния отпечатък

  — Електронен отпечатък

— Четимата от човек форма СЛЕДВА да може да се разпечатва лесно.

— Четимата от човек форма ТРЯБВА да бъде подписана от оператора на схемата съгласно базовия профил за подписи PAdES ([1]).

([1]) ETSI TS 103 172 (март 2012 г.) — Electronic Signatures and Infrastructures (ESI): PAdES Baseline Profile.