Този документ е средство за документиране и не обвързва институциите

►**B** ►**C1** **РЕШЕНИЕ НА КОМИСИЯТА**

от 16 октомври 2009 година

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

(нотифицирано под номер C(2009) 7806)

(текст от значение за ЕИП)

(2009/767/ЕО) ◄

(ОВ L 274, 20.10.2009 г., стр. 36)

Изменено със:

		Официален вестник		
		№	страница	дата
►**M1**	Решение 2010/425/ЕС на Комисията от 28 юли 2010 година	L 199	30	31.7.2010 г.

Поправено със:

►**C1** Поправка, ОВ L 299, 14.11.2009 г., стр. 18 (2009/767/ЕО)

►**C2** Поправка, ОВ L 4, 7.1.2011 г., стр. 6 (2009/767/ЕО)

▼B
▼C1

РЕШЕНИЕ НА КОМИСИЯТА

от 16 октомври 2009 година

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

(нотифицирано под номер C(2009) 7806)

(текст от значение за ЕИП)

(2009/767/ЕО)

КОМИСИЯТА НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската общност,

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) Задълженията за административно опростяване, наложени на държавите-членки в глава II от Директива 2006/123/ЕО, и по-конкретно в членове 5 и 8 от нея, включват задължението да се опростят процедурите и формалностите, приложими към достъпа до и упражняването на дейности по предоставянето на услуги, и задължението да се гарантира, че тези процедури и формалности могат да бъдат лесно изпълнени от разстояние от доставчиците на такива услуги и с помощта на електронни средства чрез „единични звена за контакт“.

(2) Изпълнението на процедурите и формалностите чрез „единични звена за контакт“ трябва да бъде възможно през границите на държавите-членки, както е предвидено в член 8 от Директива 2006/123/ЕО.

(3) За да се спази задължението за опростяване на процедурите и формалностите и да се улесни трансграничното използване на „единичните звена за контакт“, процедурите на базата на електронни средства следва да се основават на прости решения, в това число и по отношение използването на електронния подпис. Ако след подходяща оценка на риска за конкретни процедури и формалности се прецени, че за някои процедури и формалности е необходимо високо ниво на сигурност или еквивалентност на собственоръчния подпис, от доставчиците на услуги могат да бъдат изискани усъвършенствани електронни подписи на базата на квалифицирано удостоверение със или без използването на механизъм (устройство) за създаване на защитени електронни подписи.

([1]) ОВ L 376, 27.12.2006 г., стр. 36.

▼C1

(4) Рамката на Общността за електронни подписи бе създадена с Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните подписи ([1]). За да се улесни трансграничното използване на усъвършенствани електронни подписи на базата на квалифицирано удостоверение, доверието в тези електронни подписи следва да бъде разширено, така че да не зависи от държавата-членка, в която е установен подписващият или доставчикът на удостоверителни услуги, който издава квалифицираното удостоверение. Това може да бъде постигнато, като се улесни достъпът до информацията (в надеждна форма), необходима за валидиране на електронните подписи, по-специално до информацията във връзка с доставчици на удостоверителни услуги, намиращи се под надзора и притежаващи акредитацията на дадена държава-членка, и до услугите, които те предлагат.

(5) Необходимо е да се осигури публикуването на тази информация от държавите-членки чрез общ образец, за да се улесни нейното използване и да се гарантира подходящо ниво на детайлност, позволяващо на приемащата страна да валидира електронния подпис,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Използване и приемане на електронни подписи

1. Когато е оправдано, въз основа на подходящ анализ на съответните рискове и в съответствие с член 5, параграфи 1 и 3 от Директива 2006/123/ЕО, държавите-членки могат да изискат от доставчика на услуги да използва при осъществяването на определени процедури и формалности чрез единичните звена за контакт съгласно член 8 от Директива 2006/123/ЕО усъвършенствани електронни подписи на базата на квалифицирани удостоверения със или без използването на механизъм (устройство) за създаване на защитени електронни подписи, както е определено и регулирано с Директива 1999/93/ЕО.

2. Държавите-членки следва да приемат всеки усъвършенстван електронен подпис на базата на квалифицирано удостоверение със или без използването на механизъм (устройство) за създаване на защитени електронни подписи за осъществяването на процедурите и формалностите, посочени в параграф 1, като това не засяга правото на държавите-членки да ограничат приеманите усъвършенствани електронни подписи до такива на базата на квалифицирано удостоверение с използването на механизъм (устройство) за създаване на защитени електронни подписи, когато това е в съответствие с оценката на риска, посочена в параграф 1.

3. Държавите-членки не поставят при приемането на усъвършенствани електронни подписи на базата на квалифицирани удостоверения със или без използването на механизъм (устройство) за създаване на защитени електронни подписи условия, създаващи пречки за ползването от доставчиците на услуги на процедури с електронни средства чрез единичните звена за контакт.

([1]) ОВ L 13, 19.1.2000 г., стр. 12.

▼C1

4. Параграф 2 не възпира държавите-членки да приемат електронни подписи, различни от усъвършенстваните електронни подписи на базата на квалифицирани удостоверения със или без използването на механизъм (устройство) за създаване на защитени електронни подписи.

Член 2

Създаване, поддържане и публикуване на доверителни списъци

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.

▼M1

2. Държавите-членки създават и публикуват доверителен списък както в четима от човек форма, така и в машинно четима форма в съответствие с определените в приложението технически спецификации.

2а. Държавите-членки подписват по електронен път машинно четимата форма на своя доверителен списък и публикуват поне четимата от човек форма на доверителния списък по сигурен канал, за да гарантират нейната автентичност и цялост.

3. Държавите-членки съобщават на Комисията следната информация:

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

б) мястото на публикуване на четимата от човек форма и на машинно четимата форма на доверителния списък;

в) удостоверението за публичния ключ, използван за осъществяване на сигурния канал, чрез който се публикува четимата от човек форма на доверителния списък, а ако четимият от човек списък е подписан по електронен път — удостоверението за публичния ключ, използван за подписа;

г) удостоверението за публичния ключ, използван за електронно подписване на машинно четимата форма на доверителния списък;

д) всички промени в информацията по букви от а) до г).

4. Комисията предоставя на всички държави-членки чрез сигурен канал към уебсървър с удостоверена автентичност съобщената от държавите-членки информация, посочена в параграф 3, както в четима от човек форма, така и в подписана машинно четима форма.

▼C1

Член 3

Прилагане

Настоящото решение се прилага от 28 декември 2009 г.

Член 4

Адресати

Адресати на настоящото решение са държавите-членки.

▼C1

ПРИЛОЖЕНИЕ

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОБЩ ОБРАЗЕЦ НА „ДОВЕРИТЕЛЕН СПИСЪК НА ДОСТАВЧИЦИ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ ПОД НАДЗОР/АКРЕДИТАЦИЯ“

ПРЕДГОВОР

1. **Обща информация**

С общия образец на „Доверителен списък на доставчици на удостоверителни услуги с акредитация и под надзор“ се цели създаването на общ формат за предоставяне на информация от държавите-членки за състоянието на надзора/акредитацията на намиращите се под техен надзор/акредитация по отношение на съвместимостта със съответните разпоредби на Директива 1999/93/ЕО доставчици на удостоверителни услуги ([1]) (ДУУ). Това включва предоставянето на историческа информация за състоянието на поднадзорните/акредитираните удостоверителни услуги.

Задължителната информация в доверителния списък (ДС) трябва да включва минималната необходима информация за поднадзорните/акредитираните ДУУ, издаващи квалифицирани удостоверения (КУ) ([2]) в съответствие с разпоредбите на Директива 1999/93/ЕО (член 3, параграф 3, член 3, параграф 2 и член 7, параграф 1, буква а), в това число информация за КУ, поддържащи електронен подпис, и дали подписът е създаден с помощта на механизъм (устройство) за създаване на защитени електронни подписи (SSCD) ([3]).

Допълнителна информация за други поднадзорни/акредитирани ДУУ, които не издават КУ, но предлагат услуги, свързани с електронния подпис (например 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.

Тази информация е предназначена преди всичко да подкрепи валидирането на квалифицирани електронни подписи (КЕП) ([4]) и усъвършенствани електронни подписи (УЕП) ([5]) ([6]) с помощта на квалифицирано удостоверение.

Предложеният общ образец е съгласуван с приложение на базата на спецификациите TS 102 231 ([7]) на ETSI, които разглеждат създаването, публикуването, разполагането, достъпа, идентифицирането и удостоверяването на такъв вид списъци.

([1]) Както е определено в член 2, параграф 11 от Директива 1999/93/ЕО.
([2]) Както е определено в член 2, параграф 10 от Директива 1999/93/ЕО.
([3]) Както е определено в член 2, параграф 6 от Директива 1999/93/ЕО.
([4]) Както е определено в член 2, параграф 2 от Директива 1999/93/ЕО.
([5]) За УЕП, поддържан от КУ, в настоящия документ се използва съкращението $УЕП_{КУ}$.
([6]) Трябва да се отбележи, че съществуват многобройни електронни услуги на базата на прости УЕП, чието трансгранично използване също ще бъде улеснено, при положение че поддържащите ги удостоверителни услуги (например издаване на неквалифицирани удостоверения) са част от контролираните услуги, включени от дадена държава-членка в доброволната част на нейния доверителен списък.
([7]) ETSI TS 102 231 — Електронни подписи и инфраструктура (ESI): Предоставяне на хармонизирана информация за състоянието на удостоверителните услуги.

▼C1

2. **Насоки за редактиране на данни в ДС**

2.1. *ДС, насочен към удостоверителни услуги под надзор/акредитация*

Отделен списък за съответните удостоверителни услуги и доставчици на удостоверителни услуги

Доверителният списък на една държава-членка се определя като „Списък на състоянието на надзора и акредитациите на удостоверителните услуги, предлагани от доставчици на удостоверителни услуги под надзор на/-акредитирани от посочената държава-членка относно съвместимостта им със съответните разпоредби на Директива 1999/93/ЕО“.

Такъв доверителен списък трябва да обхваща:

— **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** относно съвместимостта им със съответните разпоредби на Директива 1999/93/ЕО.

Съгласно определенията и разпоредбите, дадени в Директива 1999/93/ЕО, по-конкретно по отношение на съответните ДУУ, 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 (допълнителни) 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 относно съвместимостта им с разпоредбите на Директива 1999/93/ЕО, в това число и разпоредбите на приложение I (изисквания към КУ), и с 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 системата 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 тези, определени 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 и 11—13).

— **ДУУ, които не издават КУ:**

— Те могат да бъдат включени в система за „доброволна акредитация“ (в съответствие с определенията в Директива 1999/93/ЕО) и/или в национална „призната разрешителна схема“, осъществяваща на национална основа надзор за съвместимост с разпоредбите на директивата и евентуално с национални разпоредби по отношение на разпоредбата за предоставяне на удостоверителни услуги (по смисъла на член 2, параграф 11 от директивата).

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

▼C1

Доверителният списък на държавата-членка трябва да предлага минималната необходима информация за поднадзорните/акредитираните ДУУ, издаващи квалифицирани удостоверения за потребители в съответствие с разпоредбите на Директива 1999/93/ЕО (член 3, параграф 3, член 3, параграф 2 и член 7, параграф 1, буква а), информация за КУ, поддържащи електронен подпис, и дали подписът е създаден с помощта на механизъм (устройство) за създаване на защитени електронни подписи.

Допълнителна информация за други поднадзорни/акредитирани услуги на ДУУ, които не издават КУ на потребители (например 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.

Предназначението на доверителния списък е:

— да помества и предлага надеждна информация за състоянието на надзор/акредитация на удостоверителни услуги, предлагани от доставчици на удостоверителни услуги, които са под надзор/-акредитация на държавата-членка, носеща отговорността за създаването и поддържането на списъка, относно съвместимостта им със съответните разпоредби, установени с Директива 1999/93/ЕО;

— да улеснява валидирането на електронните подписи, поддържани от изброените в списъка поднадзорни/акредитирани удостоверителни услуги на изброените ДУУ.

Единен списък на състоянията на надзор/акредитация

Всяка държава-членка трябва да създаде и да поддържа един единствен списък, указващ състоянията на надзор/акредитация на удостоверителните услуги на ДУУ под надзора/акредитацията на държавата-членка.

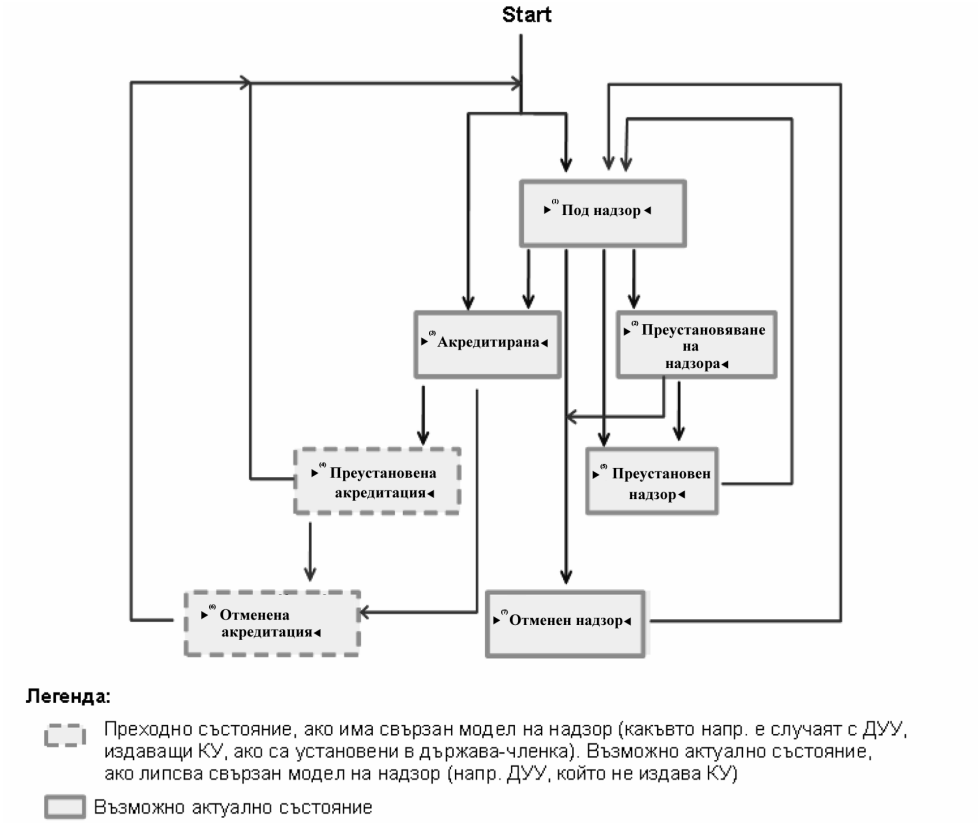
Фактът, че услугата към момента е под надзор или акредитирана, е елемент на нейното актуално състояние. Освен това състоянието на надзор или акредитация може да бъде „текущо“ („ongoing“), „в процес на преустановяване“ („in cessation“), „преустановено“ („ceased“) и дори „отменено“ („revoked“). В рамките на своето съществуване една удостоверителна услуга може да преминава от режим на надзор в режим на акредитация и обратно ([1]).

Фигура 1 показва очакваните преходи на дадена удостоверителна услуга между възможните състояния на акредитация/надзор:

([1]) Напр. един доставчик на удостоверителни услуги 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, един доставчик на удостоверителни услуги в друга държава-членка може да реши да не прекратява предлагането на дадена акредитирана удостоверителна услуга, но да я прехвърли от състояние на акредитация в поднадзорно състояние, напр. поради търговски и/или икономически причини.

▼C1

Очаквани преходи на състоянието на надзор/акредитация на услуга, предлатана от ДУУ



▶(1) (2) (3) (4) (5) (6) (7) C2

Фигура 1

Една удостоверителна услуга, издаваща КУ, трябва задължително да бъде под надзор (ако е установена в държава-членка) и може да бъде доброволно акредитирана. Стойността на състоянието на такава услуга, когато е включена в доверителния списък, може да бъде коя да е от посочените по-горе „актуални стойности на състоянието“. Трябва обаче да се отбележи, че стойностите „преустановена акредитация“ и „отменена акредитация“ трябва да бъдат само „преходни състояния“ при услуги на $ДУУ_{КУ}$, установени в държава-членка, тъй като такива услуги трябва да са поднадзорни по подразбиране (дори когато вече не са акредитирани).

Изисква се държави-членки, които създават или са създали дефинирани в национален мащаб „признати схеми за одобрение“, използвани на национална основа за надзор на съвместимостта 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 директивата), да категоризират такива „схеми за одобрение“ в една от следните две категории:

— „доброволна акредитация“, както е определена и регулирана 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 и 11—13);

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

▼C1

По същия начин, удостоверителна услуга, която не издава КУ, може да бъде под надзор или доброволно акредитирана. Стойността на състоянието на такава услуга, когато е включена в доверителния списък, може да бъде коя да е от посочените по-горе „актуални стойности на състоянието“ (вж. фигура 1).

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

— информация за системата на надзор, достъпна 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 оценяването от доверяващите се страни на качеството и нивото на сигурност на такива системи за надзор/акредитация, приложени на национално ниво към ДУУ, които не издават КУ. Когато в ДС се предлага информация за състоянието на надзора/акредитациите по отношение на ДУУ, които не издават КУ, гореспоменатите пакети от информация се предлагат на ниво ДС, 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, „квалифицираща“ информация на нивото на националните системи за надзор/акредитация на ДУУ, които не издават КУ, може да бъде предложена на нивото на услугата, ако е уместно и необходимо (например за да се различават отделните нива на качество/сигурност), като се използва разширението „additionalServiceInformation“ (клауза 5.8.2) като част от „Service information extension“ (клауза 5.5.9). Допълнителна информация за съответните технически спецификации се предлага в подробните спецификации в глава I.

Въпреки възможността надзорът и акредитацията в дадена държава-членка да се осъществяват от различни органи, се очаква да се използва едно-единствено вписване за дадена удостоверителна услуга (идентифицирана чрез своята „Service digital identity“ (цифрова идентификация на услугата) съгласно ETSI TS 102 231 ([1]) и нейното състояние на надзор/акредитация да се актуализира съответно. Значението на посочените по-горе състояния е разяснено в съответната клауза 5.5.4 на подробните технически спецификации в глава I.

2.2. *Вписвания в ДС с цел улесняване на валидирането на КЕП и УЕП$_{КУ}$*

Най-критичната част от създаването на ДС е установяването на задължителната част на ДС, а именно на „Списъка на услугите“ на всеки ДУУ, издаващ КУ, с цел да се отрази коректно състоянието на издаване 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).

([1]) ETSI TS 102 231 — Електронни подписи и инфраструктура (ESI): Предоставяне на хармонизирана информация за състоянието на удостоверителните услуги.

▼C1

В този смисъл, тъй като не съществува наистина оперативно съвместим и общоприет профил за КУ, изискваната информация може да бъде различна от „Service digital identity“ на даден (базов) УО, по-специално информация относно състоянието на КУ на издаденото удостоверение, както и информация дали поддържаните подписи са били създадени с SSCD. Органът на държавата-членка, натоварен със създаването, актуализирането и поддръжката на ДС (т.е. операторът на схемата съгласно ETSI TS 102 231) трябва следователно да вземе предвид настоящия профил и съдържанието на удостоверението за всяко КУ, издадено от ДУУ$_{КУ}$, който е включен в ДС.

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 удостоверение включва един от обектните идентификатори (OIDs) на политиката за сертифициране QCP/QCP+, определени в ETSI TS 101 456 ([2]). Използването на разнородни 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 подписания (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 свързано с SSCD, чрез което е бил създаден електронният подпис.

Допълването на полетата „Service type identifier“ („Sti“), „Service name“ („Sn“) и „Service digital identity“ („Sdi“) ([3]) с информация, предоставена в полето „Service information extensions“ („Sie“), дава възможност чрез предложения общ образец на ДС да се определи напълно специфичният тип на едно 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, разбира се, е свързана специфична информация в полето „Service current status“ („Scs“). Това е показано на фигура 2 по-долу.

Включването на услуга в списъка, за която се предлага само информацията „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 от този (базов) УО, съдържа достатъчно дефинирана от ETSI и обработваема машинно информация, за да може да бъде оценено дали то е КУ и дали се поддържа от SSCD. Когато например последното твърдение не е вярно (т.е. липсва стандартизирана от ETSI и обработваема машинно информация в КУ дали то се поддържа от SSCD), то въз основа само на информацията „Sdi“ на (базовия) УО ще може единствено да се предположи, че КУ, издадени от тази йерархия на (базови) УО, не се поддържат от SSCD. За да се обозначат тези КУ като поддържани от SSCD, „Sie“ следва да указва този факт (като това ще означава също, че коректността на информацията се гарантира от ДУУ, издаващ КУ и намиращ се под надзора/акредитацията на надзорен или акредитиращ орган съответно).

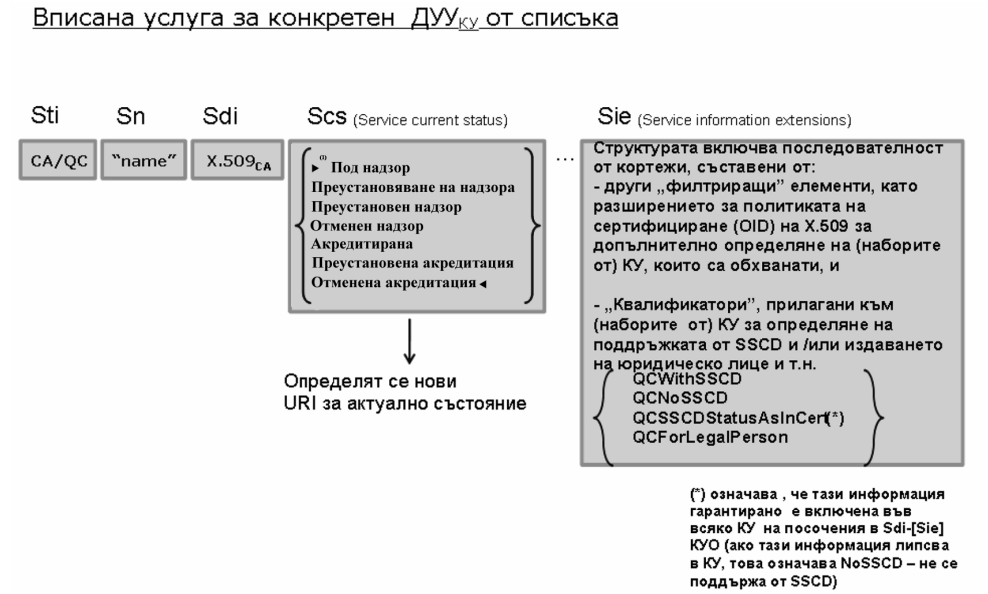
([1]) За справка виж ETSI TS 101 862 — Електронни подписи и инфраструктура (ESI): Профил на квалифицираното удостоверение.

([2]) ETSI TS 101 456 — Електронни подписи и инфраструктура (ESI): Изисквания към политиката за сертифициране на органи, издаващи квалифицирани удостоверения.

([3]) Тоест най-малко удостоверение X.509 v3 на издаващия КУО или на един от предшестващите УО във веригата на удостоверяване.

▼C1

Основни принципи — правила за редактиране — вписани ДУУ$_{КУ}$ (услуги)



►(1) C2

Фигура 2:

Вписване на услуга на регистриран ДУУ, издаващ КУ, в ДС, изпълнен във формат ССДУ (TSL)

Настоящите технически спецификации на общ образец за ДС позволяват използването на комбинация от пет основни елемента на информацията за вписаната услуга:

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

— името на услугата в полето „Service name" („Sn");

— информация в полето „Service digital identity" („Sdi"), идентифицираща услуга от списъка, т.е. най-малко удостоверение от тип X.509v3 на УО, издаващ КУ;

— за услуги от типа УО/КУ, незадължителна информация в полето „Service information extensions" („Sie"), позволяваща включването на един или повече кортежи (кортеж = tuple = подреден списък от елементи), като всеки от тях включва:

  — критерии за допълнително идентифициране (филтриране) на указаната в полето „Sdi" удостоверителна услуга, които определят услуга, за която се изисква/предлага допълнителна информация, с цел установяване наличието на поддръжка от SSCD (и/или предоставяне на юридическо лице); и

  — свързана информация („квалификатори"), указваща дали този допълнително уточнен набор от служебни квалифицирани удостоверения се поддържа 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);

▼C1

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

— дали услугата е под надзор или е акредитирана, и

— какво е състоянието на надзор/акредитация.

2.3. *Насоки за редактиране и използване на вписвания на услуги 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 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 информация в „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$_{КУ}$, която е под надзор/-акредитация на НО/АО), че за вписана услуга, идентифицирана чрез „Sdi“, всяко КУ, което не се поддържа от SSCD, съдържа или определената от ETSI декларация QcCompliance и/или QCP OID и не е предвидено да съдържа декларацията QcSSCD или QCP + OID, то използването на подходяща информация в „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$_{КУ}$, която е под надзор/-акредитация на НО/АО), че за вписана 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 всеки ДУУ информация в КУ, пряко или непряко, в машинно обработваем формат или не), но не съдържат НИТО декларацията QcSSCD, НИТО определения от ETSI идентификатор QCP(+) OID, то използването на подходяща информация в „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, указваща набора от удостоверения, който е покрит. 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$_{КУ}$, която е под надзор/-акредитация на НО/АО), че за вписана 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 КУ и/или 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 всеки 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 поддръжката от SSCD. 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“.

▼C1

Основен принцип по подразбиране е, че при вписаните в доверителния списък ДУУ трябва да има едно вписване за всяка услуга и за всяко отделно удостоверение от тип X.509v3 за удостоверителни услуги от тип УО/КУ (т.е. удостоверителен орган, издаващ (пряко) КУ). В някои внимателно определени ситуации и грижливо контролирани условия надзорният орган/акредитиращият орган на държава-членка може да реши да използва X.509v3 удостоверения на базов УО или такъв от по-високо ниво (например УО, който не издава непосредствено потребителски удостоверения, но сертифицира йерархични вериги от УО до нивото на УО, издаващи потребителски удостоверения) като информация в полето „Sdi“ на отделен елемент от списъка на услугите на вписан ДУУ. Последствията (предимства и недостатъци) от използването на X.509v3 базови УО или УО от по-високо ниво като стойности в полето „Sdi“ на услуги от ДС трябва да бъдат добре премислени от държавите-членки. Освен това, когато се прилага това изключение от основния принцип, държавите-членки трябва да осигурят необходимата документация, даваща възможност за конструиране и проверка на удостоверителната верига.

За онагледяване на основните правила за редактиране служи следният пример: в контекста на $ДУУ_{КУ}$, които използват базов УО, използван от множество УО за издаване на КУ, но чиито КУ съдържат само декларацията QcCompliance без информация относно поддръжката от SSCD, указването на „Sdi“ на базовия УО ще означава единствено (съгласно правилата, обяснени по-горе), че всяко КУ, издадено от йерархичната верига на този базов УО, НЕ се поддържа от SSCD. Препоръчва се настоятелно използването на декларацията QcSSCD в издаваните в бъдеще удостоверения, ако тези КУ в действителност се поддържат от SSCD. Междувременно (до изтичането на срока на валидност на последното УО, което не съдържа тази информация) в ССДУ следва да се използва полето „Sie“ и свързаното разширение „Qualifications“, напр. филтриране на удостоверения чрез специфични дефинирани 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 удостоверенията, филтрирани въз основа на „квалификатори“.

Основните насоки за използване на приложения на електронния подпис, услуги или продукти, ползващи ССДУ реализация на 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 подходящи декларации от тип QcStatements (т.е. QcC, QcSSCD) и/или определени от ETSI QCP(+) OID, като това се гарантира от надзорен/акредитиращ орган (вж. по-горе „Основните насоки за редактиране“)

Забележка: ако липсва информация за „квалификацията“ в „Sie“ или ако едно потребителско удостоверение, което е обявено за КУ, не е „идентифицирано допълнително“ чрез свързано 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. QcC, QcSSCD) и/или определени от ETSI QCP(+) OID е в съответствие с декларацията по въпроса на $ДУУ_{КУ}$.

▼C1

— **а КОГАТО** е налице информация за „квалификацията“ в „Sie“, в допълнение към горното принципно правило за интерпретиране удостоверенията, идентифицирани чрез употребата на информация за „квалификацията“ в „Sie“, изградена на принципа на последователност от филтри за допълнително идентифициране на набор от удостоверения и предоставяне на допълнителна информация относно „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 на използване, и/или филтрирани въз основа на наличието на специфична стойност в определено поле или разширение на удостоверението и т.н.), следва да се разглеждат в съответствие със следния набор от „квалификатори“, компенсиращи липсата на информация в съответното КУ, тоест:

— за да се укаже поддръжка 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 рубриките „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“.

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

Случаите, в които CR списъци (CRL — Certificate Revocation List) и OCSP отговори (OCSP — Online Certificate Status Protocol) са подписани с ключове, различни от тези на УО, издаващ КУ („УО/КУ“), следва също да бъдат обхванати. Това може да стане чрез включване на тези услуги като такива в ССДУ реализацията на ДС (т.е. с „Service type identifier“, квалифициран допълнително чрез разширението „additionalServiceInformation“, декларираще дадена услуга за OCSP или CRL като част от предоставянето на КУ, напр. чрез тип на услугата „OCSP/QC“ или „CRL/QC“ съответно), тъй като тези услуги могат да бъдат считани за част от поднадзорните/акредитираните „квалифицирани“ услуги, свързани с предлагането на удостоверителните услуги с КУ. Разбира се, издаващите OCSP отговори или CR списъци, чиито удостоверения са подписани от УО в йерархичната верига на вписана услуга от тип УО/КУ, следва да се приемат за „валидни“ и съответстващи на състоянието на вписана услуга от тип УО/КУ.

Подобна разпоредба може да се приложи към удостоверителните услуги, издаващи неквалифицирани удостоверения (услуги от тип „CA/PKC“), използващи типовете по подразбиране за OCSP и CRL услуги, съгласно ETSI TS 102 231.

Следва да се отбележи, че ССДУ реализацията на ДС ТРЯБВА да включва услуги за оттегляне на удостоверения, ако подобна информация не е включена в полето AIA на потребителските удостоверения или не е подписана от УО, който е измежду включените в списъка.

2.5. *Създаване на оперативно съвместим профил на КУ*

По принцип целта трябва да бъде възможно най-значително опростяване (намаляване) на броя на вписаните услуги (различни „Sdi“). За сметка на това обаче следва да се идентифицират коректно услугите, които са свързани с издаването на КУ и предоставянето на надеждна информация дали тези КУ се поддържат от SSCD, ако тази информация липсва в издаденото КУ.

▼C1

В идеалния случай употребата на полето „Sie“ и на разширението „Qualification“ следва да бъде (строго) ограничена до специалните случаи, които се решават чрез нея, тъй като КУ следва да съдържат достатъчно информация относно декларираното квалифицирано състояние и декларираното наличие/липса на поддръжка от SSCD.

Доколкото е възможно държавите-членки следва да налагат приемането и употребата на съвместими профили на КУ.

3. **Структура на общия образец за доверителния списък**

Структурата на предложения общ образец за доверителния списък на държава-членка ще съдържа следните категории информация:

1. Информация за доверителния списък и неговата схема на издаване.

2. Поредица от полета, съдържащи еднозначна информация за 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. няма поднадзорни или акредитирани ДУУ в съответната държава-членка в обхвата на доверителния списък).

3. За всеки включен ДУУ, поредица от полета, съдържащи информация за еднозначно идентифициране на поднадзорна/акредитирана удостоверителна услуга, предлагана от ДУУ (тази поредица трябва да има поне един елемент).

4. За всяка включена поднадзорна/акредитирана услуга, идентификация на актуалното състояние на услугата и историята на състоянието.

В контекста на ДУУ, издаващи УО, еднозначната идентификация на поднадзорна/акредитирана удостоверителна услуга, подлежаща на включване в списъка, трябва да вземе предвид случаите, при които липсва достатъчно информация в квалифицираното удостоверение относно неговото „квалифицирано“ състояние, евентуалната му поддръжка от SSCD, и особено да реши проблема, произтичащ от факта, че повечето (търговски) ДУУ използват един единствен издателски квалифициран УО за издаването на множество различни типове потребителски удостоверения — както квалифицирани, така и неквалифицирани.

Броят на вписванията в списъка за един признат ДУУ може да бъде намален, ако съществуват една или повече УО услуги на по-високо ниво, напр. в контекста на търговската йерархична верига на УО, свързваща един базов УО с издаващи УО. Дори и в тези случаи обаче трябва да бъде спазен принципът за осигуряване на еднозначна връзка между удостоверителната услуга на $ДУУ_{КУ}$ и набора от удостоверения, които трябва да се идентифицират като КУ.

1. *Информация за доверителния списък и неговата схема на издаване*

В тази категория ще бъде поместена следната информация:

— **таг** за доверителен списък, даващ възможност за идентифициране на доверителния списък при електронно претърсване и за потвърждаване на неговото предназначение, когато е във форма, позволяваща четене от хора;

— **идентификатор за формата и за версията на формата** на доверителния списък;

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

— **информация за типа** на доверителния списък (например за установяване на факта, че този доверителен списък дава информация за състоянието на надзор/акредитация на удостоверителни услуги на ДУУ, които са под надзора/акредитацията на съответната държава-членка относно тяхната съгласуваност с разпоредбите на Директива 1999/93/ЕО);

▼C1

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

— **информация за схемите на надзор/акредитиране**, с които е свързан доверителният списък, включваща между другото:

  — 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 (исторически) данни.

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

— **дата и час на издаване** на доверителния списък **и следващо планувано актуализиране**.

2. *Еднозначна информация за всеки ДУУ, признат в съответствие със схемата*

Този пакет от информации ще включва най-малко следното:

— наименование на организацията на ДУУ, както е използвано при формални правни регистрации (може да се изисква и 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, от където може да бъде изтеглена.

3. *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 ще включва най-малко следното за всяка удостоверителна услуга, предлагана от включен в списъка ДУУ:

— идентификатор на типа на удостоверителна услуга (например идентификатор, указващ, че поднадзорната/акредитираната удостоверителна услуга на ДУУ представлява удостоверителен орган, издаващ КУ);

— (търговско) име на тази удостоверителна услуга;

— еднозначен уникален идентификатор на удостоверителната услуга;

— допълнителна информация за удостоверителната услуга (например включена непосредствено или чрез препратка към адрес, от където може да бъде изтеглена, информация за достъп до услугата).

— за услуги от тип УО/КУ, незадължителна поредица от кортежи от данни, като всеки кортеж включва:

  i) критерии за допълнително идентифициране (филтриране) на указаната в полето „Sdi“ удостоверителна услуга, които определят услуга, за която се изисква/предлага допълнителна информация, с оглед на установяване наличието на поддръжка за SSCD (и/или предоставяне на юридическо лице); и

  ii) свързани „квалификатори“, даващи информация дали даден набор от квалифицирани удостоверения се поддържа 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).

▼C1

4. *За всяка включена в списъка услуга, идентификация на актуалното състояние на услугата и историята на състоянието*

Този пакет от информации ще включва най-малко следното:

— идентификатор на актуалното състояние;

— начална дата и час на актуалното състояние;

— историческа информация за това състояние.

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)	Един УО е ДУУ и може да използва множество технически частни (за УО) подписващи ключове, на всеки от които е присвоено удостоверение, за да издава потребителски удостоверения. УО е орган, упълномощен от един или повече потребители да издава и присвоява удостоверения. Алтернативно удостоверяващият орган може да създава потребителските ключове [ETSI TS 102 042]. УО се установява по наличната в полето издател (Issuer) на удостоверението на УО информация относно (удостоверяването на) публичния ключ, свързан с частния подписващ ключ на УО, който на практика се използва от УО за издаване на удостоверения. Един УО може да има множество подписващи ключове. Всеки подписващ ключ на УО се идентифицира еднозначно с помощта на уникален идентификатор, който е част от полето Идентификатор на ключа на органа (Authority Key Identifier) на удостоверението на УО.
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 Директива 1999/93/ЕО (член 3, параграф 3). Директивата изисква държавите-членки да създадат подходяща система за надзор на ДУУ, установени на тяхна територия и издаващи потребителски квалифицирани удостоверения, която да осигури надзора относно съвместимостта 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 относно съвместимостта им с разпоредбите на Директива 1999/93/ЕО.

▼C1

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 102 231.
Доверителна услуга (Trust Service)		Услуга, увеличаваща доверието и увереността при използването на електронни транзакции (обикновено, но не непременно, с помощта на криптографски технологии или доверителен материал) (ETSI TS 102 231).
Доставчик на доверителни услуги (Trust Service Provider)	ДДУ (TSP)	Организация, поддържаща 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 логически (двоичен) обект, генериран или издаден в резултат на използването на доверителна услуга. Примери за двоични ТДУ са удостоверения, CRL (Certificate Revocation Lists = списъци на отменени удостоверения), времеви маркери (Time Stamp Tokens) и OCSP отговори (OCSP — Online Certificate Status Protocol).
Квалифициран електронен подпис (Qualified Electronic Signature)	КЕП (QES)	Усъвършенстван електронен подпис (УЕП), поддържан от КУ и създаден с помощта на SSCD съгласно определението в Директива 1999/93/ЕО.
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/ЕО.
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

ГЛАВА I

ПОДРОБНИ СПЕЦИФИКАЦИИ ЗА ОБЩИЯ ОБРАЗЕЦ НА „ДОВЕРИТЕЛЕН СПИСЪК НА ДОСТАВЧИЦИ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ ПОД НАДЗОР/АКРЕДИТАЦИЯ“

В следващата част 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]).

►M1 Настоящите спецификации се основават на спецификациите и изискванията, определени в ETSI TS 102 231 v.3.1.2. Когато в настоящите спецификации липсва конкретно изискване, ТРЯБВА изцяло да се прилагат изискванията на ETSI TS 102 231 v.3.1.2. ◄ Когато в настоящите спецификации съществуват конкретни изисквания, те СЛЕДВА да заместят съответните изисквания на ETSI TS 102 231, като се допълват от форматните спецификации на ETSI TS 102 231. В случай на противоречия между настоящите спецификации и спецификациите от ETSI TS 102 231, настоящите спецификации СЛЕДВА да са меродавни.

([1]) IETF RFC 2119: „Ключови думи, използвани в документация от тип RFC за обозначаване на различните нива на изискванията“.

▼C1

Езикова поддръжка СЛЕДВА да се реализира и предлага най-малко за английски (EN) и евентуално за един или повече национални езици в допълнение.

Индикацията на времето СЛЕДВА да се съгласува с клауза 5.1.4 от ETSI TS 102 231.

Използването на унифицирани идентификатори на ресурси (URI) СЛЕДВА да се съгласува с клауза 5.1.5 от ETSI TS 102 231.

Информация за схемата на издаване на доверителен списък

Tag (маг)

TSL tag (Таг за ССДУ) (клауза 5.2.1)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да се съгласува с клауза 5.2.1 от ETSI TS 102 231.

▼M1

———————

▼C1

Scheme Information (информация за схемата)

TSL version identifier (идентификатор за версията на ССДУ) (клауза 5.3.1)

Това поле е ЗАДЪЛЖИТЕЛНО и стойността му СЛЕДВА да е числото „3“ (като цяло число).

TSL sequence number (пореден номер на ССДУ) (клауза 5.3.2)

▼M1

Това поле е ЗАДЪЛЖИТЕЛНО. То ТРЯБВА да указва поредния номер на TSL. Като започва от „1“ за първото издание на TSL, стойността на това цяло число ТРЯБВА да се увеличава за всяко следващо издание на TSL. Стойността НЕ ТРЯБВА да започва отново от „1“, когато по-горната стойност на „TSL version identifier“ е увеличена.

▼C1

TSL type (тип на ССДУ) (клауза 5.3.3)

▼M1

Това поле е ЗАДЪЛЖИТЕЛНО и указва типа на TSL. То ТРЯБВА да съдържа стойността http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/-TSLType/generic (Generic).

▼C1

Забележка: За да отговарят на клауза 5.3.3 от ETSI TS 102 231 и да указват специфичния тип на ССДУ, като същевременно се съобразяват с правилата за създаване на реализации на доверителни списъци ([1]) на държавите-членки на базата на ССДУ, установени от настоящите спецификации, и да позволят на парсера (parser = синтактичен анализатор) да определи в какъв формат трябва да очаква следващите полета ([2]), тъй като тези полета имат специфично (или алтернативно) значение в зависимост от типа на ССДУ (в настоящия случай това е доверителен списък на една държава-членка), горният URI СЛЕДВА да се регистрира и описва като:

([1]) Тоест „списъкът на състоянието на надзора и акредитациите на удостоверителните услуги, предлагани от доставчици на удостоверителни услуги, които са под надзор/акредитация на съответната държава-членка относно съвместимостта им с разпоредбите на Директива 1999/93/ЕО“ (съкратено „доверителният списък“).

([2]) Значение на полетата, определени от ETSI TS 102 231 — Електронни подписи и инфраструктура (ESI): Осигуряване на хармонизирана информация за доверителни услуги, „пригодена“ от настоящите спецификации за описване на процеса на създаване на доверителни списъци на държавите-членки.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/-TSLType/generic

▼C1

Описание: ССДУ реализацията на списък на състоянието на надзора и акредитациите на удостоверителните услуги, предлагани от доставчици на удостоверителни услуги, намиращи се под пряк надзор/акредитация (доброволно или задължително) на посочената държава-членка, която притежава тази реализация, относно съвместимостта им със съответните разпоредби на Директива 1999/93/ЕО.

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

Това поле е ЗАДЪЛЖИТЕЛНО. То СЛЕДВА да указва името на органа на държавата-членка, отговарящ за създаването, издаването и поддръжката на националния доверителен списък. То СЛЕДВА да указва официалното име, под което работи упълномощеното юридическо лице или упълномощената организация (например държавни административни агенции), която се свързва с този орган. То ТРЯБВА да е името, използвано при формалната юридическа регистрация или оправомощаването, към което следва да се насочва всякакъв вид формална комуникация. То СЛЕДВА да представлява последователност от многоезични символни низове и СЛЕДВА да се реализира задължително на английски (EN) и евентуално на един или повече национални езици.

Забележка: Една държава МОЖЕ да има различни надзорни и акредитиращи органи и дори допълнителни органи за сродни оперативни дейности. ►M1 Всяка държава-членка определя оператора на схемата (Scheme operator) на TSL реализацията 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, СЛЕДВА да се отразява и обозначава надлежно като такава в информацията за схемата като част от ДС, в това число специфичната информация за схемата, указана в „Scheme information URI“ (клауза 5.3.7).

▼M1

Посоченият оператор на схемата (Scheme operator, клауза 5.3.4) е организацията, която подписва TSL.

▼C1

Scheme operator address (адрес на оператора на схемата) (клауза 5.3.5)

Това поле е ЗАДЪЛЖИТЕЛНО. То СЛЕДВА да указва адресите на юридическото лице или упълномощената организация, посочени в полето „Scheme operator name“ (клауза 5.3.4), за пощенски и електронни комуникации. То СЛЕДВА да включва както „PostalAddress“ (т.е. улица, селище, [щат или провинция], [пощенски код] и двубуквен код на държавата по ISO 3166-1) съгласно клауза 5.3.5.1, така и „ElectronicAddress“ (т.е. електронна поща и/или уебсайт) съгласно клауза 5.3.5.2.

Scheme name (име на схемата) (клауза 5.3.6)

Това поле е ЗАДЪЛЖИТЕЛНО и указва името, под което действа схемата. То СЛЕДВА да бъде последователност от многоезични символни низове (реализирани задължително на английски (EN) и евентуално на един или повече национални езици), дефинирана както следва:

▼C1

— Английската версия СЛЕДВА да бъде низ от символи със следната структура:

CC:EN_name_value

където:

— „CC“ = двубуквения код на държавата по ISO 3166-1, използван в полето „Scheme territory“ (клауза 5.3.10);

— „:“ = се използва като разделителен знак;

▼M1

— „EN_name_value“ = „Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws“;

▼C1

— Националната езикова версия на всяка държава-членка СЛЕДВА да бъде символен низ със следната структура:

CC:name_value

където:

— „CC“ = двубуквения код на държавата по ISO 3166-1, използван в полето „Scheme territory“ (клауза 5.3.10);

— „:“ = се използва като разделителен знак;

— „name_value“ = официалния превод на съдържанието на полето „EN_name_value“, посочено по-горе.

Името на схемата е необходимо, за да се идентифицира еднозначното схемата, посочена чрез „Scheme information URI“, а също и за да се гарантира, в случай че операторът на схемата поддържа повече от една схема, че всяка от тези схеми е получила различно име.

Държавите-членки и операторите на схеми СЛЕДВА да гарантират, че когато държава-членка или оператор на схема поддържат повече от една схема, всяка от тях получава различно име.

Scheme information URI (URI за информация за схемата) (клауза 5.3.7)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да посочва идентификатори (URI), чрез които потребителите (доверяващите се страни) могат да получат специфична за схемата информация (като английската езикова версия се предоставя задължително, а евентуално може да съществуват и други национални езикови версии). То СЛЕДВА да бъде последователност от многоезични указатели (реализирани задължително на английски (EN) и евентуално на един или повече национални езици). Указаните URI ТРЯБВА да предлагат адрес за достъп до информация, даваща „подходяща информация за схемата“.

Тази „подходяща информация за схемата“ СЛЕДВА да включва най-малко:

— Принципна уводна информация, обща за всички държави-членки в частта, отнасяща се до обхвата и контекста на доверителния списък, както и схемите за надзор/акредитация, на които той се основава. Общият текст, които трябва да се използва, е следният:

▼C1

„The present list is the TSL implementation of [*name of the relevant Member State*] „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;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including 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 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 Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 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 and the present TSL implementation at a national level on a voluntary basis.“

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

— информация за системата на надзор, приложима за всеки $ДУУ_{КУ}$;

([1]) Последните два пакета от информация са от ключово значение за оценяването от доверяващите се страни на качеството и нивото на сигурност на такива системи за надзор/акредитация. Тези пакети от информация се предлагат на ниво ДС, 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 „Правен/политически коментар към 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 националните системи за надзор/-акредитация на ДУУ, които не издават КУ, може да бъде предложена на нивото на услугата, ако е уместно и необходимо (например за да се различават отделните нивата на качество/сигурност), като се използва разширението „Scheme service definition URI“ (клауза 5.5.6).

▼C1

— 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 СЛЕДВА 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/-акредитиране;

— информация за критериите, по отношение на които се упражнява надзор/акредитиране на ДУУ.

— Специфична информация, когато е уместно, за специфичните „квалификации“, които някои от физическите или двоичните (логически) обекти, генерирани или издавани 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 бъде предоставена на доброволна основа. Тя СЛЕДВА да включва:

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

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

Status determination approach (подход за определяне на състоянието) (клауза 5.3.8)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да съдържа идентификатора на документа, описващ подхода за определяне на състоянието. СЛЕДВА да се използва следният специфичен идентификатор (URI), както е постановено и описано по-долу:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/-appropriate

Описание: Състоянието на изброените услуги се определя от (или от името на) оператор на схемата по подходяща система за съответната държава-членка, която позволява „надзора“ (и когато е уместно, „доброволната акредитация“) на доставчици на удостоверителни услуги, установени на нейна територия (или на територията на трета държава в случай на „доброволна акредитация“) и издаващи квалифицирани удостоверения на потребителите в съответствие с член 3, параграф 3 (съответно член 3, параграф 2 или член 7, параграф 1, буква а) от Директива 1999/93/ЕО, и позволява, когато е уместно, „надзора“/„доброволната акредитация“ на доставчици на удостоверителни услуги, които не издават квалифицирани удостоверения, в съответствие с определени и изградени на национално ниво „признати схеми за одобрение“, прилагани на национална основа за надзор на съвместимостта на услугите на ДУУ, които не издават КУ, с разпоредбите на Директива 1999/93/ЕО и евентуално разширени от национални разпоредби по отношение на предлагането на такива услуги.

▼C1

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

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да съдържа най-малко следните URI:

— Общ за доверителните списъци на всички държави-членки идентификатор, насочващ към описание, което СЛЕДВА да се прилага за всички ДС:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— чрез което се декларира участието на схемата на държава-членка (с помощта на „TSL type“ (клауза 5.3.3) и „Scheme name“ (клауза 5.3.6) в схема от схеми (т.е. ССДУ, съдържащ препратки към всички държави-членки, издаващи и поддържащи ДС под формата на ССДУ);

— където потребителите могат да направят справка за политиката/-правилата, според които СЛЕДВА да се оценяват включените в списъка услуги и от които може да бъде установен типът на ССДУ (виж клауза 5.3.3);

— където потребителите могат да намерят описание как да използват и интерпретират съдържанието на ССДУ реализацията на доверителния списък. Тези правила за употреба СЛЕДВА да бъдат общи за доверителните списъци на всички държави-членки независимо от типа на изброените услуги или на системите за надзор/акредитация.

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 TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their 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 a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 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.

▼C1

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 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 Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 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 and the present TSL implementation 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 Art. 2.11 of the Directive). 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 TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC 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 ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no „Sie“„Qualification“ information is present or if an end-entity certificate that is claimed to be a QC is not „further identified“ through a related „Sie“ entry, 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. QcC, QcSSCD) 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“„Qualification“ information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie“„Qualification“ entry, 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 „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 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 TSL implementation of the Member States' Trusted Lists.“

▼C1

— Специфичен за доверителния списък на всяка държава-членка идентификатор (URI), насочващ към описание, което СЛЕДВА да се прилага за ДС на тази държава-членка:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

където CC = двубуквения код на държавата по ISO 3166-1, използван в полето „Scheme territory“ (клауза 5.3.10)

— където потребителите могат да намерят специфичните за съответната държава-членка политика/правила, съгласно които СЛЕДВА да се оценяват услугите, включени в списъка, в съответствие с подходяща система за надзор и схеми за акредитация на държавата-членка.

— където потребителите могат да са сдобият със специфично за дадената държава-членка описание как да използват и интерпретират съдържанието на ССДУ реализацията на доверителния списък по отношение на удостоверителните услуги, които не са свързани с издаването на КУ. То може да бъде използвано за обозначаване на потенциална степен на детайлност в националните системи за надзор/акредитация по отношение на ДДУ, които не издават КУ, както и на начина, по който „Scheme service definition URI“ (клауза 5.5.6) и полето „Service information extension“ се използват за тази цел.

Държавите-членки МОГАТ да определят допълнителни идентификатори (URI) на базата на горепосочения специфичен за държавата-членка идентификатор (т.е. адреси, попадащи в йерархията на този специфичен адрес).

Scheme territory (територия на схемата) (клауза 5.3.10)

В контекста на настоящите спецификации това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да определя държавата, в която е установена схемата (двубуквен код на държавата по ISO 3166-1).

TSL policy/legal notice (политика/правен коментар към ССДУ) (клауза 5.3.11)

В контекста на настоящите спецификации това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да определя политиката на схемата или предлага коментар относно правния статут на схемата или законовите изисквания, на които тя е подчинена и юрисдикцията, в която тя е установена, и/или ограниченията и условията, при които доверителният списък се поддържа и публикува.

То СЛЕДВА да бъде многоезичен символен низ (неформатиран текст), състоящ се от две части:

— Първа задължителна част, обща за ДС на всички държави-членки (реализирана задължително на английски (EN) и евентуално на един или повече национални езици), указваща, че приложимата законова рамка е Директива 1999/93/ЕО и съответна ѝ реализация в законодателството на държавата-членка, посочена в полето „Scheme Territory“.

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 the 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.

Текст на български език [превод на горния английски текст]:

▼C1

Приложимата законова рамка за настоящата ССДУ реализация на доверителния списък на 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 [име на съответната държава-членка].

— Втора незадължителна част, специфична за всеки ДС (задължително на английски (EN) 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).

Historical information period (период на съхраняване на историческа информация) (клауза 5.3.12)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва продължителността на периода (като цяло число), през който в ССДУ се предоставя историческа информация. Това цяло число посочва броя на дните и в контекста на настоящите спецификации то СЛЕДВА да бъде по-голямо от или равно на 3 653 (т.е. една ССДУ реализация на ДС на държава-членка ТРЯБВА да съдържа историческа информация за период от минимум десет години). По-големите стойности следва да са надлежно съобразени със законовите изисквания на държавата-членка, посочена в „Scheme Territory“ (клауза 5.3.10).

Pointers to other TSLs (препратки към други ССДУ) (клауза 5.3.13)

В контекста на настоящите спецификации това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да съдържа препратка (когато такава е налице) към съобразен с изискванията на ETSI TS 102 231 списък, съставен от Европейската комисия и съдържащ препратки (указатели) към всички ССДУ реализации на доверителни списъци на държавите-членки. Спецификациите на ETSI TS 102 231, клауза 5.3.13 важат при регламентирането на използването на незадължителната цифрова идентификация, представяща посочения издател на ССДУ, във формата, определен в клауза 5.5.3.

Забележка: Това поле НЕ СЛЕДВА да се използва, докато се очаква създаването на съгласувания с ETSI TS 102 231 и съставен от Европейската комисия списък на препратки към ССДУ реализациите на доверителни списъци на държавите-членки.

List issue date and time (дата и час на издаване на списъка) (клауза 5.3.14)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва датата и часа (универсално координирано време, изразено във формат Zulu) на издаване на ССДУ, като стойностите за дата и час отговарят на спецификациите от ETSI TS 102 231, клауза 5.1.4.

Next update (следващо актуализиране) (клауза 5.3.15)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва датата и часа (универсално координирано време, изразено във формат Zulu) на издаване на следващия ССДУ, или е празно, чрез което се указва, че ССДУ е приключен (използваните стойности за дата и час отговарят на спецификациите от ETSI TS 102 231, клауза 5.1.4).

В случай че няма междинни промени в състоянието на включените в схемата ДДУ или услуги, ССДУ ТРЯБВА да бъде преиздаден в момента на изтичане на последния издаден ССДУ.

В контекста на настоящите спецификации разликата между стойностите за дата и час в полето „Next update“ и тези в „List issue date and time“ НЕ СЛЕДВА да надвишава **шест (6)** месеца.

▼C1

Distribution points (точки на разпространение) (клауза 5.3.16)

Това поле е НЕЗАДЪЛЖИТЕЛНО. Ако се използва, то СЛЕДВА да указва адресите, на които е публикувана актуалната ССДУ реализация на ДС и където могат да бъдат намерени актуални версии на настоящия ССДУ. Ако са указани няколко точки на разпространение, те СЛЕДВА да предлагат идентични копия на настоящия ССДУ или на неговата актуализирана версия. Когато се използва, това поле се форматира като непразна последователност от символни низове, всеки от които е съвместим с RFC 3986 ([1]).

Scheme extensions (разширения на схемата) (клауза 5.3.17)

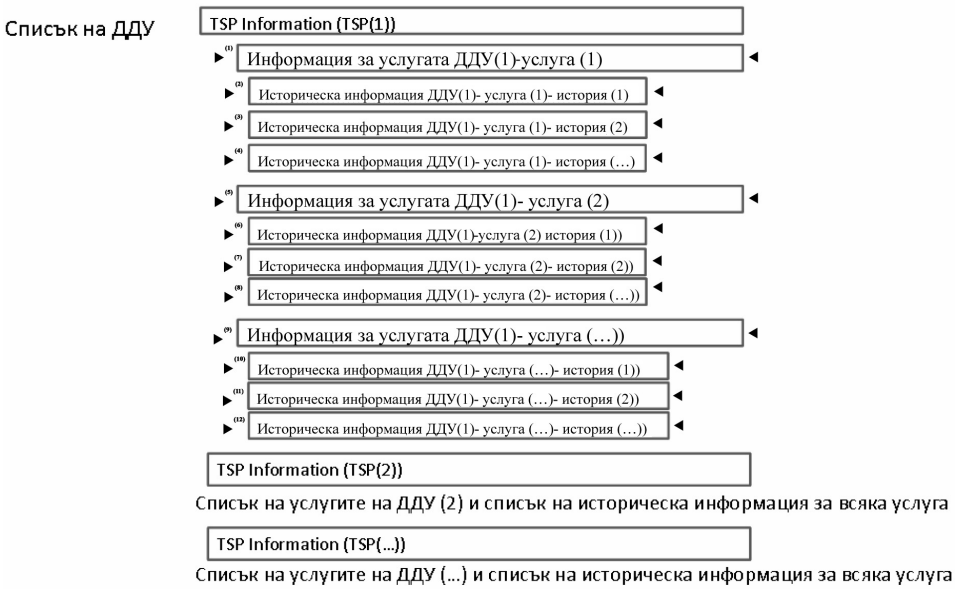
Това поле е НЕЗАДЪЛЖИТЕЛНО и не се използва в контекста на настоящата спецификация.

List of Trust Service Providers (списък на доставчиците на доверителни услуги)

Това поле е НЕЗАДЪЛЖИТЕЛНО.

В случай че няма или не е имало поднадзорни/акредитирани ДУУ в контекста на схемата на държава-членка, това поле НЕ СЛЕДВА да съществува. Има споразумение обаче, че дори ако в дадена държава-членка липсват поднадзорни или акредитирани ДУУ по схемата, държавите-членки СЛЕДВА да създадат ССДУ, в който обаче това поле не съществува. Липсата на ДУУ в списъка СЛЕДВА да се тълкува като липса на поднадзорни/акредитирани ДУУ на територията на държавата, посочена в „Scheme Territory“.

В случай че една или повече услуги на ДУУ са или са били под надзор/-акредитация на схемата, то полето СЛЕДВА да съдържа последователност, идентифицираща всеки ДУУ, предлагащ една или повече от тези поднадзорни/акредитирани услуги, и подробности относно състоянието на надзор/акредитация и история на състоянието на всяка от услугите на ДУУ (на фигурата по-долу ДДУ = ДУУ).



▶(1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) C2

([1]) IETF RFC 3986: „Uniform Resource Identifiers (URI, унифицирани идентификатори на ресурси): Generic syntax (Общ синтаксис)“.

▼C1

На горната фигура е изобразен списък на ДДУ. За всеки ДДУ съществува последователност от полета, съдържащи информация за ДДУ („TSP Information“), следвана от списък на услуги. За всяка от тези изброени услуги съществува последователност от полета, съдържащи информация за услугата („Service Information“), и последователност от полета относно историята на състоянието на одобряване на услугата („Service approval history“).

TSP Information (информация за ДДУ)

TSP(1) (ДДУ(1)

TSP name (име на ДДУ) (клауза 5.4.1)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва името на **юридическото лице**, отговарящо за услугите на ДУУ, които са или са били под надзор/акредитация в рамките на схемата. То представлява последователност от многоезични символни низове (реализирани задължително на английски (EN) и евентуално на един или повече национални езици). Това име ТРЯБВА да е името, използвано при формалната юридическа регистрация, към което следва да се насочва всякакъв вид формална комуникация.

TSP trade name (търговско име на ДДУ) (клауза 5.4.2)

Това поле е НЕЗАДЪЛЖИТЕЛНО и ако съществува, СЛЕДВА да указва алтернативно име, с което един ДУУ се идентифицира в специфичния контекст на предлаганите от него услуги, които могат да бъдат намерени в настоящия ССДУ под неговото име, вписано в полето „TSP name“ (клауза 5.4.1).

Забележка: Когато един ДУУ (едно юридическо лице) предлага услуги под различни търговски имена или в няколко различни специфични контекста, може да съществуват толкова вписвания на ДУУ, колкото специфични контекста има (напр. двойки вписвания име/търговско име). Алтернативно може всеки ДУУ да се вписва само веднъж (юридическо лице), като се дава информация за специфичния контекст в зависимост от услугата. Операторът на схемата на държавата-членка следва да обсъди и постигне споразумение с ДУУ за най-уместния подход.

TSP address (адрес на ДДУ) (клауза 5.4.3)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва адресите на юридическото лице или упълномощената организация, посочени в полето „TSP name“ (клауза 5.4.1), за пощенски и електронни комуникации. То СЛЕДВА да включва както „PostalAddress“ (т.е. улица, селище, [щат или провинция], [пощенски код] и двубуквен код на държавата по ISO 3166-1) съгласно клауза 5.3.5.1, така и „ElectronicAddress“ (т.е. електронна поща и/или уебсайт) съгласно клауза 5.3.5.2.

TSP information URI (URI за информация за ДДУ) (клауза 5.4.4)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва адресите (URI), на които потребителите (доверяващите се страни) могат да получат специфична за ДУУ информация. То СЛЕДВА да бъде последователност от многоезични указатели (реализирани задължително на английски (EN) и евентуално на един или повече национални езици). Указаните URI ТРЯБВА да предлагат адрес за достъп до информация относно общите условия и задължения на ДУУ, неговата практика, юридически въпроси, неговата политика спрямо клиентите и друга основна информация, която засяга всички негови услуги, изброени в рамките на неговото вписване в ССДУ.

Забележка: Когато един ДУУ (юридическо лице) предлага услуги под различни търговски имена или в няколко различни специфични контекста и това е отразено чрез наличието на толкова вписвания на ДУУ, колкото контекста съществуват, това поле СЛЕДВА да съдържа информация, свързана със специфичния набор от услуги, изброени в рамките на вписването за конкретната двойка име/търговско име на ДУУ.

▼C1

TSP information extensions (разширена информация за ДДУ) (клауза 5.4.5)

Това поле е НЕЗАДЪЛЖИТЕЛНО и ако съществува, МОЖЕ да бъде използвано от оператора на схемата в съответствие със спецификациите ETSI TS 102 231 (клауза 5.4.5), за поместване на специфична информация, която се интерпретира съгласно правилата на специфичната схема.

List of Services (списък на услуги)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да съдържа последователност, описваща всяка от признатите услуги на ДУУ и нейното състояние (и историята на това състояние) на одобрение. В списъка трябва да е включена поне една услуга (дори ако информацията за нея е изцяло историческа).

Тъй като съхраняването на историческа информация за изброените услуги е ЗАДЪЛЖИТЕЛНО според настоящите спецификации, тази историческа информация ТРЯБВА да бъде запазена, дори ако настоящото състояние на услугата не налага непременно включването ѝ в списъка (напр. ако тя е оттеглена). Следователно даден ДУУ ТРЯБВА да бъде включен в списъка, дори ако единствената негова включена в списъка услуга е в състояние, което налага включване в списъка единствено с цел запазване на информацията.

Service Information (информация за услугата)

TSP(1) Service(1) (ДДУ(1) услуга(1)

Service type identifier (идентификатор на типа на услугата) (клауза 5.5.1)

▼M1

Това поле е ЗАДЪЛЖИТЕЛНО и ТРЯБВА да указва идентификатора на типа на услугата в съответствие с типа на настоящите спецификации за TSL (т.е. „/eSigDir-1999-93-EC-TrustedList/TSLType/generic“).

▼C1

Ако посочената услуга е свързана с издаването на квалифицирани удостоверения, то указаният URI СЛЕДВА да бъде http://uri.etsi.org/TrstSvc/Svctype/CA/QC (удостоверителен орган, издаващ квалифицирани удостоверения).

Ако посочената услуга е свързана с издаването на токени на доверителни услуги, които не са КУ и не спомагат за издаването на КУ, указаният URI СЛЕДВА да бъде един от определените и посочени в клауза D.2 на ETSI 102 231 идентификатори, отнасящи се до това поле. Това правило СЛЕДВА да се прилага дори за онези токени на доверителни услуги, които са под надзор/акредитация относно съвместимостта с някои специфични изисквания съгласно националните законодателства на държавите-членки (напр. квалифицирани времеви маркери в Германия или Унгария), като посочените URI СЛЕДВА да бъдат измежду определените в спецификацията ETSI 102 231 и изброени в нейната клауза D.2 идентификатори, отнасящи се до това поле (напр. TSA за определени на национална основа квалифицирани времеви маркери). Когато е уместно, такава специфична национална квалификация на токени на доверителни услуги МОЖЕ да бъде включена във вписването на доверителната услуга, като за тази цел СЛЕДВА да се използват полетата „additionalServiceInformation extension“ (клауза 5.8.2) и „Service information extension“ (клауза 5.8.2).

▼C1

Основен принцип по подразбиране е, че СЛЕДВА да има по едно вписване за всяко отделно удостоверение от тип X.509v3 (напр. за удостоверителни услуги от тип УО/КУ) сред вписаните удостоверителни услуги на включен в доверителния списък ДУУ (напр. удостоверителен орган, издаващ (непосредствено) КУ). В някои внимателно определени ситуации и грижливо контролирани условия надзорният орган/акредитиращият орган на държава-членка МОЖЕ да реши да използва X.509v3 удостоверения на базов УО или такъв от по-високо ниво (например УО, който не издава непосредствено потребителски удостоверения, но сертифицира йерархични вериги от УО, достигащи до нивото на УО, издаващи потребителски удостоверения) като информация в полето „Sdi“ на отделен елемент от списъка на услугите на вписан ДУУ. Последствията (предимства и недостатъци) от използването на X.509v3 базови УО или УО от по-високо ниво като стойности в полето „Sdi“ на услуги от ДС трябва да бъдат добре премислени от държавите-членки ([1]). Освен това, когато се прилага такова едно разрешено изключение от основния принцип, държавите-членки ТРЯБВА да осигурят необходимата документация, даваща възможност за конструиране и проверка на удостоверителната верига.

Забележка: ДУУ от рода на издаващите OCSP отговори или CR списъци, които са част от удостоверителни услуги на $ДУУ_{КУ}$ и използват отделни двойки ключове за подписването съответно на OCSP отговори и CR списъци, МОГАТ да бъдат включени също така и в настоящия образец за ССДУ чрез използването на следната комбинация от URI:

— стойност на полето „Service type identifier“ (клауза 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

в комбинация със следната стойност в полетата „Service information extension“ (клауза 5.5.9)/additionalServiceInformation extension (клауза 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

описание: доставчик на информация за състоянието на удостоверения, поддържащ сървър за OCSP като част от услугата на ДУУ, издаващ квалифицирани удостоверения.

— стойност на полето „Service type identifier“ (клауза 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

в комбинация със следната стойност в полетата „Service information extension“ (клауза 5.5.9)/additionalServiceInformation extension (клауза 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

описание: доставчик на информация за състоянието на удостоверения, поддържащ CR списък като част от услугата на ДУУ, издаващ квалифицирани удостоверения.

— стойност на полето „Service type identifier“ (клауза 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Използването на удостоверение от тип X.509v3 на базов УО като стойност на полето „Sdi“ ще накара оператора на схемата да възприеме целия набор от удостоверителни услуги в рамките на такъв базов УО като едно цяло по отношение на „състоянието на надзор/акредитация“. Напр. всяка промяна на състоянието, която се изисква от един УО във вписаната базова йерархия, ще доведе до промяна на състоянието за цялата йерархия.

▼C1

в комбинация със следната стойност в полетата „Service information extension“ (клауза 5.5.9)/additionalServiceInformation extension (клауза 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

описание: базов удостоверителен орган, от който може да бъде проследена удостоверителна йерархия надолу до удостоверителен орган, издаващ квалифицирани удостоверения.

— стойност на полето „Service type identifier“ (клауза 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

в комбинация със следната стойност в „Service information extension“ (клауза 5.5.9)/additionalServiceInformation extension (клауза 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

описание: услуга за издаване на времеви печати като част от услуга на доставчик на удостоверителни услуги, издаващ квалифицирани удостоверения, която генерира времеви маркери, които могат да се използват в процеса на валидиране на квалифициран подпис, с цел да се провери и удължи валидността на даден подпис, ако последният е оттеглен или с изтекъл срок.

Service name (име на услугата) (клауза 5.5.2)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва името, под което указаният в полето „TSP name“ (клауза 5.4.1) ДУУ предлага услугата, указана в полето „Service type identifier“ (клауза 5.5.1). То СЛЕДВА да бъде последователност от многоезични символни низове (реализирани задължително на английски (EN) и евентуално на един или повече национални езици).

Service digital identity (цифрова идентификация на услугата) (клауза 5.5.3)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва поне един уникален за услугата цифров идентификатор, чийто тип е посочен в „Service type identifier“ (клауза 5.5.1) и чрез който услугата може да бъде идентифицирана еднозначно.

В настоящите спецификации цифровият идентификатор, посочен в това поле, СЛЕДВА да бъде съответно удостоверение от тип X.509v3, което е форма на публичните ключове, чрез които ДУУ предлага услугата, чийто тип е указан в „Service type identifier“ (клауза 5.5.1) (т.е. ключът, използван от базов УО/КУ, ключът, с който се подписват удостоверенията [1]) или алтернативно се издават времеви маркери, или се подписват CR списъци или OCSP отговори). Това удостоверение от тип X.509v3 СЛЕДВА да се използва като минимално необходим цифров идентификатор (един вид публични ключове, които ДУУ използва, за да предложи услугата). Допълнителни идентификатори МОГАТ да се използват, както следва, но всички те ТРЯБВА да препращат към същата идентификация (т.е. към съответното удостоверение от тип X.509v3):

[1] Това може да бъде удостоверение от УО, издаващ потребителски удостоверения (напр. CA/PKC(УО/ПКП), CA/QC(УО/КУ), или удостоверение от упълномощен базов УО, от който може да бъде проследена удостоверителна йерархия надолу до квалифицираните потребителски удостоверения. В зависимост от това дали тази информация и информацията, която може да бъде намерена във всяко потребителско удостоверение, издадено въз основа на това базово удостоверение, може да се използва за еднозначното определяне на подходящите характеристики на всяко квалифицирано удостоверение, тези данни („Service digital identity“) може би ще трябва да бъдат допълнени от данните в „Service information extensions“ (вж. клауза 5.5.9).

▼C1

а) отличителното име (DN) на удостоверението, което може да се използва за идентифициране на електронни подписи на услугата на ДУУ, посочена в „Service type identifier“ (клауза 5.5.1);

б) съответният идентификатор на публичен ключ (т.е. SubjectKeyIdentifier X.509v3 или стойност от тип SKI);

в) съответният публичен ключ.

Основен принцип е, че един цифров идентификатор (т.е. съответното удостоверение от тип X.509v3) НЕ СЛЕДВА да фигурира повече от един път в доверителния списък, т.е. СЛЕДВА да съществува само по едно вписване за всяко удостоверение от тип X.509v3 в рамките на една удостоверителна услуга, фигуриращa сред услугите на даден ДУУ, включен в доверителния списък. Обратно, конкретно удостоверение от тип X.509v3 СЛЕДВА да се използва в полето „Sdi“ на една-единствена услуга.

Забележка 1: Единственият случай, в който не е необходимо да се спазва горепосоченият основен принцип, е когато конкретно удостоверение от тип X.509v3 се използва при издаването на различни типове токени на доверителни услуги, за които са в сила различни схеми за надзор/акредитация, например когато удостоверение от тип X.509v3 се използва от ДУУ от една страна при издаване на КУ в рамките на подходяща система за надзор, а от друга страна при издаване на неквалифицирани удостоверения под надзора/акредитацията на друга система. В този случай ще бъдат използвани две вписвания с различни стойности „Sti“ (в горния пример съответно CA/QC и CA/PKC) и еднакви стойности „Sdi“ (съответното удостоверение от тип X.509v3).

Реализациите са обвързани с ASN.1 или XML и СЛЕДВА да са съгласувани със спецификацията ETSI TS 102 231 (вж. приложение A към ETSI TS 102 231 за ASN.1 и приложение B към ETSI TS 102 231 за XML).

Забележка 2: Когато е необходима допълнителна „квалифицираща“ информация за дадено вписване на услуга и ако е уместно, операторът на схемата СЛЕДВА да използва разширението „additionalServiceInformation“ (клауза 5.8.2) на полето „Service information extension“ (клауза 5.5.9) с цел осигуряване на такава допълнителна „квалифицираща“ информация. Допълнително операторът на схемата може да използва по желание клауза 5.5.6 („Scheme service definition URI“).

Service current status (актуално състояние на услугата) (клауза 5.5.4)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва идентификатора на състоянието на услугата с помощта на един от следните URI:

— **Under Supervision (под надзор)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation (услуга в процес на преустановяване на надзора)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased (преустановен надзор)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked (отменен надзор)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

▼M1

— **Акредитирана** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

▼C1

— **Accreditation Ceased (преустановена акредитация)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked (отменена акредитация)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Горепосочените състояния СЛЕДВА да се интерпретират в контекста на настоящите спецификации на доверителния списък, както следва:

— ***Under Supervision (под надзор):*** услугата, посочена в „Service digital identity“ (клауза 5.5.3) и предлагана от доставчика на удостоверителни услуги (ДУУ), указан в „TSP name“ (клауза 5.4.1), е понастоящем под надзор относно съвместимостта ѝ с разпоредбите на Директива 1999/93/ЕО от страна на държавата-членка, посочена в „Scheme territory“ (клауза 5.3.10), в която е установен ДУУ.

▼M1

— ***Supervision of Service in Cessation (услуга в процес на преустановяване на надзора):*** услугата, посочена в „Service digital identity“ (клауза 5.5.3) и предлагана от CSP, указан в „TSP name“ (клауза 5.4.1), е понастоящем на етап преустановяване на надзора, но все още е под надзор до преустановяването или отменянето на надзора. В случай че отговорността за осигуряване на този етап на преустановяване е поета от юридическо лице, различно от посоченото в „TSP name“, идентификацията на това ново или подсигуряващо юридическо лице (подсигуряващ CSP) ТРЯБВА да се предостави в „Scheme service definition URI“ (клауза 5.5.6) и в разширението „TakenOverBy“ (клауза L.3.2) на записа за услугата.

▼C1

— ***Supervision Ceased (преустановен надзор):*** валидността на оценката за целите на надзора е изтекла и услугата, посочена в „Service digital identity“ (клауза 5.5.3), не е оценена повторно. Услугата на е повече под надзор от датата на настоящото състояние, като това означава, че услугата вече не функционира.

— ***Supervision Revoked (отменен надзор):*** услугата или самият ДУУ, които са били под надзор в миналото, не удовлетворяват повече разпоредбите на Директива 1999/93/ЕО, според оценката на държавата-членка, посочена в „Scheme territory“ (клауза 5.3.10), в която е установен ДУУ. Съответно се изисква услугата да прекрати дейността си и се счита, че тя вече не функционира поради горепосочената причина.

Забележка 1: Стойността „Supervision Revoked“ може бъде окончателна, дори ако впоследствие ДУУ прекрати своята дейност; в този случай не е необходимо да се променя състоянието на „Supervision of Service in Cessation“ или на „Supervision Ceased“. Всъщност, единственият начин за промяна на състоянието „Supervision Revoked“ е услугата да възстанови съвместимостта си с разпоредбите на Директива 1999/93/ЕО по преценка на съответната система на надзор, действаща в държавата-членка, притежаваща ДС, и да си възвърне състоянието „Under Supervision“. Състоянията на „Supervision of Service in Cessation“ или на „Supervision Ceased“ се заемат само ако ДУУ непосредствено преустанови своите съответни услуги под надзор, но не и когато надзорът е отменен.

— ***Accredited (акредитирана):*** акредитиращият орган е провел от името на държавата-членка, посочена в „Scheme territory“ (клауза 5.3.10), оценка с цел акредитиране и услугата, посочена в „Service digital identity“ (клауза 5.5.3) и предлагана от ДУУ ([1]), указан в „TSP name“ (клауза 5.4.1), се счита за съвместима с разпоредбите на Директива 1999/93/ЕО.

([1]) Трябва да се отбележи, че този акредитиран ДУУ може да е установен в държава-членка, различна от посочената в „Scheme territory“ на ССДУ реализацията на ДС, или в трета държава (вж. член 7, параграф 1, буква а) от Директива 1999/93/ЕО).

▼C1

Забележка 2: Когато се използват в контекста на ДУУ, издаващ КУ, който е установен на територията, посочена в „Scheme territory“ (клауза 5.3.10), състоянията „Accreditation Revoked“ и „Accreditation Ceased“ ТРЯБВА да бъдат считани за „преходни състояния“ и НЕ ТРЯБВА да бъдат използвани като стойности в полето „Service current status“, тъй като (ако се използват) те ТРЯБВА да бъдат последвани незабавно от състояние „Under supervision“ в полето „Service approval history information“ или в полето „Service current status“, евентуално последвано от друго състояние на надзор измежду посочените по-горе, както е указано на фигура 1. Когато се използват в контекста на ДУУ, който не издава КУ, и съществува само схема за „доброволна акредитация“ без съответна схема за надзор или в контекста на ДУУ, издаващ КУ, който не е установен на територията, посочена в „Scheme territory“ (клауза 5.3.10) (напр. в трета държава), споменатите състояния „Accreditation Revoked“ и „Accreditation Ceased“ МОГАТ да се използват като стойности в полето „Service current status“:

— ***Accreditation Ceased (преустановена акредитация):*** валидността на оценката за целите на акредитирането е изтекла и услугата, посочена в „Service digital identity“ (клауза 5.5.3), не е оценена повторно.

— ***Accreditation Revoked (отменена акредитация):*** услугата, посочена в „Service digital identity“ (клауза 5.5.3) и предлагана от доставчика на удостоверителни услуги (ДУУ), указан в „TSP name“ (клауза 5.4.1), след като първоначално е удовлетворявала критериите на схемата вече не отговаря на изискванията (или това се отнася за нейния доставчик) на разпоредбите на Директива 1999/93/ЕО.

Забележка 3: Използват се едни и същи стойности за ДУУ, издаващи КУ, и за ДУУ, които не издават КУ (напр. доставчици на услуги за времеви печати, издаващи времеви маркери, ДУУ, издаващи неквалифицирани удостоверения и т.н.). Полето „Service type identifier“ (клауза 5.5.1) се използва за указване на различните приложими системи за надзор/акредитация.

Забележка 4: Допълнителна, свързана със състоянието „квалифицираща“ информация, дефинирана на нивото на националните системи за надзор/-акредитация на ДУУ, които не издават КУ, МОЖЕ да бъде предоставена на ниво услуга, когато е уместно и се изисква (например за да се разграничават различни нива на качество/сигурност). Операторите на схемите СЛЕДВА да използват разширението „additionalServiceInformation“ (клауза 5.8.2) на полето „Service information extension“ (клауза 5.5.9) с цел осигуряване на такава допълнителна „квалифицираща“ информация. Допълнително операторът на схемата може да използва по желание клауза 5.5.6 („Scheme service definition URI“).

Current status starting date and time (начална дата и час на актуалното състояние) (клауза 5.5.5)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва датата и часа на преминаване в актуалното състояние (стойностите за дата и час отговарят на спецификациите от ETSI TS 102 231, клауза 5.1.4).

Scheme service definition URI (URI за определенията на услугите на схемата) (клауза 5.5.6)

Това поле е НЕЗАДЪЛЖИТЕЛНО и ако съществува, СЛЕДВА да указва онези URI, чрез които доверяващите се страни могат да получат специфична информация за услугите, предлагани от оператора на схемата, под формата на многоезични указатели (като английската езикова версия се предоставя задължително, а евентуално може да съществуват и други национални езикови версии).

Когато се използва полето, указаните URI ТРЯБВА да предлагат адрес за достъп до информация, описваща услугата, както е определено от схемата. Когато е уместно, то може да съдържа по-конкретно:

a) URI, указващ идентификацията на подсигуряващия ДУУ, когато става въпрос за услуга в процес на преустановяване на надзора, за която съществува подсигуряващ ДУУ (виж „Service current status“ — клауза 5.5.4);

▼C1

б) URI, водещ към документ, предлагащ допълнителна информация, свързана с използването на някои определени на национално ниво специфични квалификации за дадена услуга, предоставяща токени на доверителна услуга и намираща се под надзор/акредитация, в съответствие с употребата на полето „Service information extension“ (клауза 5.5.9) и с разширението „additionalServiceInformation“ съгласно определението в клауза 5.8.2.

Service supply points (точки за доставка на услугата) (клауза 5.5.7)

Това поле е НЕЗАДЪЛЖИТЕЛНО и ако съществува, СЛЕДВА да указва онези URI, чрез които доверяващите се страни могат да получат достъп до услугатаq чрез поредица от символни низове, чийто синтаксис ТРЯБВА да е в съответствие с RFC 3986.

TSP service definition URI (URI за определенията на услугите на ДДУ) (клауза 5.5.8)

Това поле е НЕЗАДЪЛЖИТЕЛНО и ако съществува, СЛЕДВА да указва онези URI, чрез които доверяващите се страни могат да получат специфична информация за услугите, предлагани от ДДУ, под формата на многоезични указатели (като английската езикова версия се предоставя задължително, а евентуално може да съществуват и други национални езикови версии). Използваните URI ТРЯБВА да предлагат адрес за достъп до информация, описваща услугата, както е определена от ДДУ.

Service information extensions (разширена информация за услугата) (клауза 5.5.9)

В контекста на настоящите спецификации това поле е НЕЗАДЪЛЖИТЕЛНО, но СЛЕДВА да се използва, ако предоставената в „Service digital identity“ (клауза 5.5.3) информация не е достатъчна за еднозначното идентифициране на квалифицираните удостоверения, издадени от тази услуга, и/или наличната информация в съответните квалифицирани удостоверения не позволява да бъде установено чрез машинна обработка дали КУ се поддържа от SSCD ([1]).

Когато неговата употреба е ЗАДЪЛЖИТЕЛНА в контекста на настоящите спецификации, напр. за услуги от типа УО/КУ, незадължителното поле „Service digital identity“ („Sie“) СЛЕДВА да се използва и структурира в съответствие с разширението „Qualifications“, определено в приложение L.3.1 към ETSI TS 102 231, като поредица от един или повече кортежи, като всеки кортеж включва:

— (филтри) информация за допълнително идентифициране на указаната в полето „Sdi“ удостоверителна услуга, която определя услуга, за която се изисква/предлага допълнителна информация, с оглед на установяване наличието или липсата на поддръжка за SSCD (и/или предоставяне на юридическо лице); и

— свързана информация („квалификатори“), указваща дали този допълнително уточнен набор от служебни квалифицирани удостоверения се поддържа от SSCD (ако тази свързана информация има стойността „QCSSCDStatusAsInCert“, тя е част от КУ и е в стандартен, подходящ за машинна обработка формат ([2]) съгласно ETSI), и/или информация дали такива КУ се издават и на юридически лица (по подразбиране те се издават само на физически лица).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): означава, че е гарантирано от ДУУ и контролирано (надзорен модел) или проверено (акредитационен модел) от държавата-членка (съответно от нейния надзорен орган или акредитиращ орган), че за всяко КУ, издадено от услугата (КУО), посочена в „Service digital identity“ (клауза 5.5.3), и допълнително идентифицирано чрез (филтри) горепосочената информация за допълнително идентифициране на указаната в „Sdi“ удостоверителна услуга, този конкретен набор от квалифицирани удостоверения, за който е необходима тази допълнителна информация относно наличието или липсата на поддръжка от SSCD, **СЕ поддържа от SSCD** (т.е. че частният ключ, свързан с публичния ключ в удостоверението, се съхранява в механизъм (устройство) за създаване на защитени електронни подписи съгласно приложение III към Директива 1999/93/ЕО);

([1]) Вж. раздел 2.2 от настоящия документ.

([2]) Има се предвид една подходяща комбинация от дефинираната в ETSI декларация QcCompliance, декларации QcSSCD [ETSI TS 101 862] или обектен идентификатор (OID) QCP/QCP+ [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/-SvcInfoExt/QCNoSSCD): означава, че е гарантирано от ДУУ и контролирано (надзорен модел) или проверено (акредитационен модел) от държавата-членка (съответно от нейния надзорен орган или акредитиращ орган), че за всяко КУ, издадено от услугата (RootCA/QC или CA/QC), посочена в „Service digital identity“ (клауза 5.5.3), и допълнително идентифицирано чрез (филтри) горепосочената информация за допълнително идентифициране на указаната в „Sdi“ удостоверителна услуга, този конкретен набор от квалифицирани удостоверения, за който е необходима тази допълнителна информация относно наличието или липсата на поддръжка от SSCD, **НЕ СЕ поддържа от SSCD** (т.е. че частният ключ, свързан с публичния ключ в удостоверението, **не** се съхранява в механизъм (устройство) за създаване на защитени електронни подписи съгласно приложение III към Директива 1999/93/ЕО).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): означава, че е гарантирано от ДУУ и контролирано (надзорен модел) или проверено (акредитационен модел) от държавата-членка (съответно от нейния надзорен орган или акредитиращ орган), че за всяко КУ, издадено от услугата (CA/QC), посочена в „Service digital identity“ (клауза 5.5.3), и допълнително идентифицирано чрез (филтри) горепосочената информация за допълнително идентифициране на указаната в „Sdi“ удостоверителна услуга, този конкретен набор от квалифицирани удостоверения, за който е необходима тази допълнителна информация относно наличието или липсата на поддръжка от SSCD, **СЛЕДВА да съдържа информация, подходяща за машинна обработка, относно наличието или липсата на поддръжка от SSCD за КУ**;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): означава, че е гарантирано от ДУУ и контролирано (надзорен модел) или проверено (акредитационен модел) от държавата-членка (съответно от нейния надзорен орган или акредитиращ орган), че за всяко КУ, издадено от услугата (КУО), посочена в „Service digital identity“ (клауза 5.5.3), и допълнително идентифицирано чрез (филтри) горепосочената информация за допълнително идентифициране на указаната в „Sdi“ удостоверителна услуга, удостоверенията от този конкретен набор от квалифицирани удостоверения, за които е необходима тази допълнителна информация относно издаването на юридически лица, **СА** издадени на юридически лица.

Тези квалификатори се използват в разширение само ако типът на услугата е http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Това поле зависи от реализацията (ASN.1 или XML) и ТРЯБВА да е съгласувано със спецификациите от приложение L.3.1 към ETSI TS 102 231.

▼M1

В контекста на XML реализация специфичното съдържание на тази допълнителна информация трябва да се кодира, като се използват файловете xsd, предоставени в приложение C на ETSI TS 102 231.

▼C1

Service Approval History (история на одобрението на услугата)

Това поле е НЕЗАДЪЛЖИТЕЛНО, но ТРЯБВА да съществува, ако стойността на „Historical information period“ (клауза 5.3.12) не е нула. В контекста на настоящите спецификации схемата ТРЯБВА да съхранява историческа информация. В случай че се предвижда съхраняването на историческа информация, но услугата няма история, предхождаща настоящото състояние (т.е. това е първото ѝ състояние или историческата информация не е съхранена от оператора на схемата), това поле СЛЕДВА да бъде празно. В противен случай за всяка промяна на актуалното състояние на дадена услуга на ДУУ, която се е случила по време на историческия период, посочен в ETSI TS 102 231, клауза 5.3.12, СЛЕДВА да се предоставя информация за предходното състояние на одобрение в низходящ хронологичен ред на промените на състоянието (т.е. датата и часа на влизане в сила на следващото състояние на одобрение).

▼C1

Това СЛЕДВА да бъде последователност от исторически данни, както е описано по-долу.

TSP(1) Service(1) History(1) (ДДУ(1) услуга(1) история(1)

Service type identifier (идентификатор на типа на услугата) (клауза 5.6.1)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва идентификатора на типа на услугата във формата и със значението, използвани в „TSP Service Information — Service type identifier“ (клауза 5.5.1).

Service name (име на услугата) (клауза 5.6.2)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва името, под което ДУУ предлага услугата, указана в полето „TSP Service Information —Service type identifier“ (клауза 5.5.1), във формата и със значението, използвани в „TSP Service Information — Service name“ (клауза 5.5.2). Не се изисква името в тази клауза да бъде същото като в клауза 5.5.2. Промяната на името МОЖЕ да е една от причините за приемането на ново състояние.

▼M1

Service digital identity (цифрова идентификация на услугата) (клауза 5.6.3)

Това поле е ЗАДЪЛЖИТЕЛНО и ТРЯБВА да указва поне една форма на цифровия идентификатор (например удостоверение X.509v3), използван в „TSP Service Information — Service digital identity“ (клауза 5.5.3) във формата и със значението, определени в ETSI TS 102 231, клауза 5.5.3.

Забележка: За стойност на удостоверението X.509v3, използвана в „Sdi“ клауза 5.5.3 на услуга, трябва да съществува само едно вписване на услугата в доверителен списък за стойността „Sti:Sie/additionalServiceInformation“. Информацията в поле „Sdi“ (клауза 5.6.3), използвана в информацията за историята на състоянието на одобряване на услуга във връзка с вписването на услуга, и използваната в това вписване на услуга информация „Sdi“ (клауза 5.5.3) ТРЯБВА да се отнасят за същата стойност на удостоверението X.509v3. Когато за вписана услуга се променя „Sdi“ (т.е. подновяване или нов ключ на удостоверение X.509v3 например за CA/PKC или CA/QC) или се създава нова „Sdi“ за такава услуга дори с идентични стойности за свързаните „Sti“, „Sn“ и [„Sie“], това означава, че операторът на схемата (Scheme Operator) ТРЯБВА да създаде запис за услугата, различаващ се от предишния.

▼C1

Service previous status (предходно състояние на услугата) (клауза 5.6.4)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва идентификатора на предходното състояние на услугата във формата и със значението, използвани в „TSP Service Information — Service current status“ (клауза 5.5.4).

Previous status starting date and time (начална дата и час на предходното състояние) (клауза 5.6.5)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва датата и часа на влизане в действие на съответното предходно състояние във формата и със значението, използвани в „TSP Service Information — Service current status starting date and time“ (клауза 5.5.5).

Service information extensions (разширена информация за услугата) (клауза 5.6.6)

Това поле е НЕЗАДЪЛЖИТЕЛНО и МОЖЕ да се използва от оператори на схеми за предоставяне на специфична, свързана с услугата информация във формата и със значението, използвани в „TSP Service Information — Service information extensions“ (клауза 5.5.9).

▼C1

TSP(1) Service(1) History(2) (ДДУ(1) услуга(1) история(2)

Вписване за ДДУ(1) услуга(1) история(2) (предхождаща история(1)

…

TSP(1) Service(2) (ДДУ(1) услуга(2)

Вписване за ДДУ(1) услуга 2 (ако е уместно)

ДДУ(1) услуга(2) история(1)

…

TSP(2) Information (информация за ДДУ(2)

Вписване за ДДУ 2 (ако е уместно)

Вписване за ДДУ 2 услуга 1

Вписване за ДДУ 2 услуга 1 история 1

…

▼M1

▼C2

Signed TSL

▼M1

Предназначената за четене от човек форма на TSL реализацията на доверителния списък, създадена съгласно настоящите спецификации, и по-специално съгласно глава IV, СЛЕДВА да е подписана от оператора, посочен в „Scheme operator name“ (клауза 5.3.4), за да се гарантира нейната автентичност и цялост ([1]). Форматът на подписа СЛЕДВА да е PAdES part 3 (ETSI TS 102 778-3 ([2])), но МОЖЕ да е PAdES part 2 (ETSI TS 102 778-2 ([3])) в контекста на конкретния модел на доверие, установен чрез публикуването на удостоверенията, използвани за подписване на доверителния списък.

Машинно четимата форма на TSL реализацията на доверителния списък, създадена съгласно настоящите спецификации, ТРЯБВА да е подписана от оператора, посочен в „Scheme operator name“ (клауза 5.3.4), за да се гарантира нейната автентичност и цялост. Машинно четимата форма на TSL реализацията на доверителния списък, създадена съгласно настоящите спецификации, ТРЯБВА да е във формат XML и ТРЯБВА да съответства на спецификациите, посочени в приложения B и C от ETSI TS 102 231.

Подписът ТРЯБВА да е във формат XAdES BES или EPES, както е определено от спецификациите на ETSI TS 101903 за XML реализации. Такава реализация на електронния подпис ТРЯБВА да отговаря на изискванията, посочени в приложение B към ETSI TS 102 231 ([4]). Допълнителни основни изисквания по отношение на въпросния подпис са посочени в следващите раздели.

▼C1

Scheme identification (идентификация на схемата) (клауза 5.7.2)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да съдържа позоваване, включено от оператора на схемата, което идентифицира еднозначно описаната в настоящите спецификации схема и създадения ССДУ, и ТРЯБВА да бъде включено в изчисляването на подписа. Очаква се това да бъде низ от символи или низ от битове.

([1]) В случай че предназначената за четене от човек форма на TSL реализацията на доверителния списък не е подписана, нейната автентичност и цялост ТРЯБВА да бъдат гарантирани чрез подходящ съобщителен канал с еквивалентно ниво на сигурност. Използването на TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2“) се препоръчва за тази цел и контролната сума — „отпечатък“ (fingerprint) на удостоверението на TLS канала ТРЯБВА да бъде предоставена по метода „out of band“ от държавата-членка на TSL потребителите.

([2]) ETSI TS 102 778-3 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

([4]) Подписващото удостоверение на оператора на схемата задължително трябва да бъде защитено чрез подпис по един от начините, определени от ETSI TS 101903, и ds:keyInfo следва да съдържа съответната верига от удостоверения, когато е приложимо.

▼M1

В контекста на настоящите спецификации това позоваване ТРЯБВА да включва „TSL type“ (клауза 5.3.3), „Scheme name“ (клауза 5.3.6) и стойността на разширението SubjectKeyIdentifier на удостоверението, използвано от оператора на схемата, за да подпише TSL по електронен път.

▼C1

Signature algorithm identifier (идентификатор на сигнатурния алгоритъм) (клауза 5.7.3)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да указва идентификатора на криптографския алгоритъм, използван за създаването на подписа. В зависимост от използвания алгоритъм то МОЖЕ да се нуждае от допълнителни параметри. Това поле ТРЯБВА да бъде включено в изчисляването на подписа.

Signature value (сигнатурна стойност) (клауза 5.7.4)

Това поле е ЗАДЪЛЖИТЕЛНО и СЛЕДВА да съдържа действителната стойност на цифровия подпис. Всички полета на ССДУ (с изключение на самата сигнатурна стойност) ТРЯБВА да бъдат включени в изчисляването на подписа.

TSL extensions (разширения на ССДУ) (клауза 5.8)

expiredCertsRevocationInfo Extension (клауза 5.8.1)

Това разширение е НЕЗАДЪЛЖИТЕЛНО. Ако се използва, то ТРЯБВА да е съобразено със спецификациите на ETSI TS 102 231, клауза 5.8.1.

additionalServiceInformation Extension (клауза 5.8.2)

Ако се използва, това НЕЗАДЪЛЖИТЕЛНО разширение ТРЯБВА да се употребява само на ниво на услугата и само в полето, определено в клауза 5.5.9 („Service information extension“). Използва се за предоставяне на допълнителна информация за услугата. Това СЛЕДВА да бъде поредица от един или повече кортежи, като всеки кортеж включва:

а) URI, указващ допълнителна информация, например:

— URI, указващ определена на национално ниво специфична квалификация за услуга под надзор/акредитация, предоставяща токени на доверителна услуга, например:

— специфична степен на детайлност по отношение на сигурността/качеството на национална схема за надзор/акредитация на ДУУ, които не издават КУ (напр. RGS */**/*** във Франция, специфично състояние на „надзор“, установено от националното законодателство за някои ДУУ, издаващи КУ, в Германия), вж. забележка 4 към „Service current status“ — клауза 5.5.4;

— или специфично правно състояние на услуга под надзор/-акредитация, предоставяща токени на доверителна услуга (напр. определени на национално ниво квалифицирани ТДУ (токени на доверителна услуга), какъвто е случаят в Германия и Унгария);

— или значение на специфичен идентификатор на политиката в полето „Sdi“ на удостоверение от тип X.509v3;

— или регистриран URI, както е определен в „Service type identifier“, клауза 5.5.1, за да бъде специфицирана допълнително посочената в „Sti“ услуга като съставен елемент на услуга на доставчик на удостоверителни услуги, издаващ КУ (напр. OCSP-QC, CRL-QC и RootCA-QC);

б) незадължителен символен низ, съдържащ стойността на serviceInformation, с посоченото в схемата значение (напр. *, ** или ***);

в) всяка друга незадължителна допълнителна информация, предоставена в специфичен за схемата формат.

▼M1

Този URI СЛЕДВА да насочва към четима от човек информация (поне на английски и евентуално на един или повече национални езици), считана за подходяща и достатъчна за разбиране от доверяваща се страна на разширението и по-конкретно обясняваща значението на дадените URI, специфициращи възможните стойности на serviceInformation, и значението на всяка от тях.

Qualifications Extension (клауза L.3.1)

Описание: Това поле е НЕЗАДЪЛЖИТЕЛНО, но ТРЯБВА да съществува, ако употребата му е ЗАДЪЛЖИТЕЛНА, напр. за услуги на RootCA/QC (базови УО/КУ) или CA/QC, както и ако:

— информацията, предоставена в „Service digital identity“, не е достатъчна за еднозначното идентифициране на квалифицираните удостоверения, издадени от тази услуга

— наличната в съответните квалифицирани удостоверения информация не позволява да бъде установено чрез машинна обработка дали квалифицираното удостоверение (QC) се поддържа от дадено устройство за създаване на защитени електронни подписи (SSCD).

Когато се използва, това разширение на нивото на услугата ТРЯБВА да се използва само в полето, описано в „Service information extension“ (клауза 5.5.9) и ТРЯБВА да съответства на спецификациите, посочени в приложение L.3.1 на ETSI TS 102 231.

TakenOverBy Extension (клауза L 3.2)

Описание: Това разширение е НЕЗАДЪЛЖИТЕЛНО, но ТРЯБВА да съществува, когато услуга, правната отговорност за която е била носена преди от определен ДУУ (CSP), е поета от друг ДДУ (TSP), и е предназначено за формално обявяване на правната отговорност за услугата, както и за да се даде възможност на софтуера за проверка да покаже на потребителя някои подробности от правно естество. Информацията, предоставена в това разширение, ТРЯБВА да е в съответствие с използването на клауза 5.5.6 и ТРЯБВА да отговаря на спецификациите в приложение L.3.2 към ETSI TS 102 231.

▼**M1**

„ГЛАВА II

При създаването на своите доверителни списъци държавите-членки използват:

кодове с малки букви за езика и кодове с главни букви за страната;

кодове за езика и страната съгласно предоставената по-долу таблица;

когато се използва нелатинска азбука (със свой собствен код за езика), се добавя транслитерация на латиница със съответните езикови кодове, посочени в таблицата по-долу.

Кратко наименование (на местен език)	Кратко наименование (на английски)	Код на страната	Код на езика	Пояснения	Транслитерация на латиница
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Препоръчан от ЕС код на страната	el-Latn
España	Spain	ES	es	Също и каталонски език (ca), баски език (eu), галисийски език (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Кратко наименование (на местен език)	Кратко наименование (на английски)	Код на страната	Код на езика	Пояснения	Транслитерация на латиница
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Препоръчан от ЕС код на страната	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Транслитерация на латиница: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.“

▼C1

ГЛАВА IV

СПЕЦИФИКАЦИИ ЗА ПРЕДНАЗНАЧЕНИЯ ЗА ЧЕТЕНЕ ОТ ЧОВЕКА ФОРМАТ НА ССДУ РЕАЛИЗАЦИЯТА НА ДОВЕРИТЕЛНИЯ СПИСЪК

ТРЯБВА да бъде осигурен публичен достъп с електронни средства до предназначения за четене от човека документ (ПЧД) на ССДУ реализацията на доверителния списък. Той БИ ТРЯБВАЛО да се предлага под формата на документ във формат PDF в съответствие с ISO 32000, който ТРЯБВА да е форматиран съгласно профила PDF/A (ISO 19005).

Съдържанието на ПЧД на ССДУ реализацията на доверителния списък на базата на PDF/A БИ ТРЯБВАЛО да отговаря на следните изисквания:

▼M1

— Заглавието на четимата от човек форма на доверителните списъци се конструира като конкатенация на следните елементи:

  — незадължително изображение на националния флаг на държавата-членка;

  — шпация;

  — кратко наименование на страната на местния език (или езици) (както е посочено в първата колона от таблицата в глава II);

  — шпация;

  — „(“;

  — кратко наименование на страната на английски език (както е посочено във втората колона от таблицата в глава II) в скобите;

  — „)“: като затваряща скоба и разделител;

  — шпация;

  — „Trusted List“;

  — незадължително лого на оператора на схемата на държавата-членка.

▼C1

— Структурата на ПЧД БИ ТРЯБВАЛО да отразява логическия модел, описан в раздел 5.1.2 на ETSI TS 102 231.

— Всяко налично поле БИ ТРЯБВАЛО да е описано и описанието да съдържа:

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

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

  — значение (описание) на стойността на полето, когато е уместно и в частност както е посочено в приложение D към ETSI TS 102 231 или в настоящите спецификации за регистрирани URI (напр. „Удостоверителен орган, издаващ удостоверения с публичен ключ.“);

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

— Най-малко следните полета и съответни стойности на цифровите удостоверения, посочени в полето „Service digital identity“, БИ ТРЯБВАЛО да бъдат представени в ПЧД:

  — Версия

  — Сериен номер

  — Сигнатурен алгоритъм

  — Издател

  — Валидно от

  — Валидно до

  — Предмет

▼C1

— 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

— ПЧД БИ ТРЯБВАЛО да може да се отпечатва лесно

— ПЧД МОЖЕ да бъде подписан електронно. Когато е подписан, подписът ТРЯБВА да е на оператора на схемата и да съответства на същите спецификации за подпис, които се прилагат за ССДУ реализацията на доверителния списък.