Trattandosi di un semplice strumento di documentazione, esso non impegna la responsabilità delle istituzioni

►B ►C1 **DECISIONE DELLA COMMISSIONE**

del 16 ottobre 2009

che stabilisce misure per facilitare l'uso di procedure per via elettronica mediante gli «sportelli unici» di cui alla direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno

[notificata con il numero C(2009) 7806]

(Testo rilevante ai fini del SEE)

(2009/767/CE) ◄

(GU L 274 del 20.10.2009, pag. 36)

Modificato da:

		Gazzetta ufficiale		
		n.	pag.	data
►M1	Decisione 2010/425/UE della Commissione del 28 luglio 2010	L 199	30	31.7.2010

Rettificata da:

►C1 Rettifica, GU L 299 del 14.11.2009, pag. 18 (2009/767/CE)
►C2 Rettifica, GU L 4 del 7.1.2011, pag. 6 (2009/767/CE)

▼B
▼C1

DECISIONE DELLA COMMISSIONE

del 16 ottobre 2009

che stabilisce misure per facilitare l'uso di procedure per via elettronica mediante gli «sportelli unici» di cui alla direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno

[notificata con il numero C(2009) 7806]

(Testo rilevante ai fini del SEE)

(2009/767/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno [1], in particolare l'articolo 8, paragrafo 3,

considerando quanto segue:

(1) Gli obblighi di semplificazione amministrativa imposti agli Stati membri dal capo II della direttiva 2006/123/CE, in particolare dagli articoli 5 e 8, comprendono l'obbligo di semplificare le procedure e le formalità relative all'accesso e all'esercizio di un'attività di servizio e l'obbligo di garantire che dette procedure e formalità possano essere espletate con facilità dai prestatori di servizi, a distanza e per via elettronica, mediante lo «sportello unico».

(2) L'espletamento di procedure e di formalità mediante lo «sportello unico» deve essere possibile a livello transfrontaliero tra gli Stati membri, come stabilito dall'articolo 8 della direttiva 2006/123/CE.

(3) Al fine di conformarsi all'obbligo di semplificare le procedure e le formalità e di facilitare l'uso transfrontaliero degli «sportelli unici», le procedure per via elettronica dovrebbero basarsi su soluzioni semplici, anche per quanto riguarda l'uso delle firme elettroniche. Qualora, dopo un'adeguata valutazione dei rischi delle procedure e delle formalità concrete, siano ritenuti necessari un elevato livello di sicurezza o l'equivalenza con una firma manoscritta, per determinate procedure e formalità potrebbero essere richieste ai prestatori di servizi firme elettroniche avanzate basate su un certificato qualificato con o senza dispositivo per la creazione di una firma sicura.

[1] GU L 376 del 27.12.2006, pag. 36.

▼C1

(4) Il quadro comunitario per le firme elettroniche è stato istituito dalla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa a un quadro comunitario per le firme elettroniche ([1]). Al fine di facilitare un uso transfrontaliero efficace delle firme elettroniche avanzate basate su un certificato qualificato, è opportuno migliorare il livello di fiducia nelle firme elettroniche a prescindere dallo Stato membro in cui ha sede il firmatario o il prestatore di servizi di certificazione che rilascia il certificato qualificato. Per conseguire questo obiettivo una soluzione potrebbe essere, ad esempio, quella di rendere più accessibili in forma affidabile le informazioni necessarie per la convalida delle firme elettroniche, in particolare le informazioni relative ai prestatori di servizi di certificazione soggetti a supervisione/accreditamento in uno Stato membro e ai servizi da loro offerti.

(5) È necessario garantire che gli Stati membri rendano accessibili al pubblico tali informazioni mediante un modello comune al fine di facilitarne l'uso e di garantire un adeguato livello di dettaglio, che consenta alla parte ricevente di convalidare la firma elettronica,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Uso e accettazione delle firme elettroniche

1. Se giustificato sulla base di un'adeguata valutazione dei possibili rischi, e conformemente all'articolo 5, paragrafi 1 e 3, della direttiva 2006/123/CE, gli Stati membri, ai fini dell'espletamento delle procedure e formalità mediante lo sportello unico di cui all'articolo 8 della direttiva 2006/123/CE, possono esigere dal prestatore di servizi l'uso di firme elettroniche avanzate basate su un certificato qualificato, con o senza dispositivo per la creazione di una firma sicura, secondo quanto definito e disciplinato dalla direttiva 1999/93/CE.

2. Per l'espletamento delle procedure e formalità di cui al paragrafo 1, gli Stati membri accettano tutte le firme elettroniche avanzate basate su un certificato qualificato, con o senza dispositivo per la creazione di una firma sicura, fatta salva la loro possibilità di limitare tale accettazione alle firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura, se ciò è giustificato dalla valutazione del rischio di cui al paragrafo 1.

3. Gli Stati membri non subordinano l'accettazione delle firme elettroniche avanzate basate su un certificato qualificato, con o senza dispositivo per la creazione di una firma sicura, a requisiti tali da ostacolare l'uso, da parte dei prestatori di servizi, di procedure per via elettronica mediante gli sportelli unici.

([1]) GU L 13 del 19.1.2000, pag. 12.

▼C1

4. Le disposizioni del paragrafo 2 non impediscono agli Stati membri di accettare firme elettroniche diverse dalle firme elettroniche avanzate basate su un certificato qualificato, con o senza dispositivo per la creazione di una firma sicura.

Articolo 2

Elaborazione, aggiornamento e pubblicazione degli elenchi di fiducia

1. Gli Stati membri elaborano, aggiornano e pubblicano, conformemente alle specifiche tecniche dell'allegato, un «elenco di fiducia» contenente informazioni minime relative ai prestatori di servizi di certificazione che rilasciano al pubblico certificati qualificati e che sono soggetti alla loro supervisione/accreditamento.

▼M1

2. Gli Stati membri elaborano e pubblicano l'elenco di fiducia sia in un formato leggibile all'uomo che in un formato leggibile a macchina, conformemente alle specifiche riportate nell'allegato.

2 *bis*. Gli Stati membri firmano elettronicamente il loro elenco di fiducia in formato leggibile a macchina e, come minimo, pubblicano il formato leggibile all'uomo di tale elenco facendo ricorso ad un canale sicuro, al fine di garantirne l'autenticità e l'integrità.

3. Gli Stati membri notificano alla Commissione le seguenti informazioni:

a) il nome dell'organismo o degli organismi responsabili dell'elaborazione, aggiornamento e pubblicazione dell'elenco di fiducia, sia in formato leggibile all'uomo che in formato leggibile a macchina;

b) i luoghi in cui sono pubblicati i formati leggibili all'uomo e i formati leggibili a macchina dell'elenco di fiducia;

c) il certificato a chiave pubblica usato per avviare il canale sicuro attraverso il quale è pubblicato l'elenco di fiducia in formato leggibile all'uomo oppure, se questo è firmato elettronicamente, il certificato a chiave pubblica usato per firmarlo;

d) il certificato a chiave pubblica usato per firmare elettronicamente l'elenco di fiducia in formato leggibile a macchina;

e) qualsiasi modifica apportata alle informazioni di cui alle lettere da a) a d).

4. La Commissione mette a disposizione degli Stati membri, attraverso un canale sicuro su un server web autenticato, le informazioni di cui al paragrafo 3 notificate dagli Stati membri, sia in un formato leggibile all'uomo che in un formato leggibile a macchina e firmato.

▼C1

Articolo 3

Applicazione

La presente decisione si applica a decorrere dal 28 dicembre 2009.

Articolo 4

Destinatari

Gli Stati membri sono destinatari della presente decisione.

▼C1

ALLEGATO

SPECIFICHE TECNICHE DI UN MODELLO COMUNE PER L'«ELENCO DI FIDUCIA DEI PRESTATORI DI SERVIZI DI CERTIFICAZIONE SOGGETTI A SUPERVISIONE/ACCREDITAMENTO»

PREFAZIONE

1. **Considerazioni generali**

Il modello comune per l'«elenco di fiducia dei prestatori di servizi di certificazione soggetti a supervisione/accreditamento» degli Stati membri ha l'obiettivo di definire le modalità comuni con cui gli Stati membri trasmettono le informazioni relative alla situazione in materia di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione (CSP) ([1]) soggetti a supervisione/accreditamento da parte degli Stati membri per quanto riguarda la conformità con le pertinenti disposizioni della direttiva 1999/93/CE. Ciò comprende la fornitura delle serie storiche di informazioni relative alla situazione di supervisione/accreditamento dei servizi di certificazione soggetti a supervisione/accreditamento.

Tra le informazioni obbligatorie da inserire nell'elenco di fiducia (TL) devono figurare informazioni minime sui CSP soggetti a supervisione/accreditamento che rilasciano certificati qualificati (QC) ([2]) conformemente alle disposizioni della direttiva 1999/93/CE [articolo 3, paragrafi 3 e 2, e articolo 7, paragrafo 1, lettera a)], comprese le informazioni sui certificati qualificati basati sulla firma elettronica, creata o no da un dispositivo per la creazione di una firma sicura (SSCD) ([3]).

Informazioni complementari relative a altri prestatori di servizi di certificazione soggetti a supervisione/accreditamento che non rilasciano certificati qualificati ma forniscono servizi connessi con le firme elettroniche (ad esempio prestatori di servizi di certificazione che forniscono servizi di orodatazione e che rilasciano gettoni di orodatazione, CPS che rilasciano certificati non qualificati, ecc.) possono essere inseriti in un elenco di fiducia a livello nazionale e su base facoltativa.

Questa informazione è finalizzata in primo luogo a facilitare il processo di convalida delle firme elettroniche qualificate (QES) e delle firme elettroniche avanzate (AdES) ([4]) basate su un certificato qualificato ([5]) ([6]).

Il modello unico proposto è compatibile con un'applicazione basata sulle specifiche della norma ETSI TS 102 231 ([7]) utilizzate per l'elaborazione, la pubblicazione, la collocazione, l'accesso, l'autenticazione e l'accettazione di siffatti elenchi.

([1]) Quali definiti all'articolo 2, punto 11, della direttiva 1999/93/CE.
([2]) Quali definiti all'articolo 2, punto 10, della direttiva 1999/93/CE.
([3]) Quale definito all'articolo 2, punto 6, della direttiva 1999/93/CE.
([4]) Quali definite all'articolo 2, punto 2, della direttiva 1999/93/CE.
([5]) Nel presente documento viene utilizzato l'acronimo «$AdES_{QC}$» per una firma elettronica avanzata (AdES) basata su un certificato qualificato (QC).
([6]) Si noti che esiste un certo numero di servizi elettronici basati su AdES semplici, il cui uso transfrontaliero sarebbe facilitato se i servizi di certificazione di supporto (ad esempio quelli che rilasciano certificati non qualificati) facessero parte dei servizi soggetti a supervisione/controllo da parte degli Stati membri nella parte informativa facoltativa dell'elenco di fiducia.
([7]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Orientamenti per la gestione delle voci nell'elenco di fiducia (TL)**

2.1. *Un TL centrato su servizi di certificazione soggetti a supervisione/accreditamento*

Servizi di certificazione e prestatori di servizi di certificazione in un elenco unico

L'elenco di fiducia di uno Stato membro è definito come «l'elenco dello status di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte degli Stati membri per quanto riguarda la conformità con le pertinenti disposizioni della direttiva 1999/93/CE».

Nell'elenco di fiducia devono essere inseriti:

— **tutti i prestatori di servizi di certificazione**, quali definiti all'articolo 2, punto 11, della direttiva 1999/93/CE, ovvero «un'entità o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche»,

— **che sono soggetti a supervisione/accreditamento** per quanto riguarda la conformità con le pertinenti disposizioni della direttiva 1999/93/CE.

Nel considerare le definizioni e le disposizioni della direttiva 1999/93/CE, in particolare per quanto riguarda i CSP e i sistemi di supervisione e accreditamento facoltativo ad essi relativi, è opportuno distinguere tra due tipologie di CSP, ovvero i prestatori di servizi di certificazione che rilasciano certificati qualificati (QC) al pubblico (CSP_{QC}) e quelli che non rilasciano tali certificati al pubblico ma che forniscono «altri servizi (ausiliari) connessi alle firme elettroniche»:

— **CSP che rilasciano QC:**

  — devono essere sotto la supervisione dello Stato membro in cui sono stabiliti (se sono stabiliti in uno Stato membro) e possono anche essere accreditati per la conformità con le disposizioni della direttiva 1999/93/CE, compresi i requisiti dell'allegato I (requisiti per i QC) e dell'allegato II (requisiti per i CSP che rilasciano QC). I CSP che rilasciano QC e che sono accreditati in uno Stato membro devono essere soggetti al pertinente sistema di supervisione vigente in tale Stato membro, salvo il caso in cui non siano stabiliti nello stesso,

  — il sistema di «supervisione» applicabile (e il sistema di «accreditamento facoltativo») sono definiti nella direttiva 1999/93/CE e devono rispettarne le pertinenti disposizioni, in particolare quelle dell'articolo 3, paragrafo 3, dell'articolo 8, paragrafo 1, dell'articolo 11 e del considerando 13), [e rispettivamente quelle dell'articolo 2, punto 13, dell'articolo 3, paragrafo 2, dell'articolo 7, paragrafo 1, lettera a), dell'articolo 8, paragrafo 1, dell'articolo 11 e dei considerando 4 e da 11 a 13].

— **CSP che non rilasciano QC:**

  — possono rientrare nel sistema di «accreditamento facoltativo» (quale definito nella direttiva 1999/93/CE e conforme alla stessa) e/o in un «regime di approvazione riconosciuto» definito e attuato su base nazionale ai fini del controllo della conformità con le disposizioni della direttiva ed eventualmente con le disposizioni della normativa nazionale in materia di fornitura di servizi di certificazione (nell'accezione dell'articolo 2, punto 11, della direttiva),

  — alcuni degli oggetti fisici o binari (logici) generati o rilasciati a seguito della fornitura di un servizio di certificazione potrebbero beneficiare di una «qualifica» specifica sulla base della loro conformità con le disposizioni e i requisiti nazionali, ma è probabile che la portata di tale qualifica sarebbe limitata al livello nazionale.

▼C1

L'elenco di fiducia di uno Stato membro deve fornire informazioni minime sui CSP soggetti a supervisione/accreditamento che rilasciano certificati qualificati al pubblico conformemente alle disposizioni della direttiva 1999/93/CE [articolo 3, paragrafi 3 e 2, e articolo 7, paragrafo 1, lettera a)], informazioni sui certificati qualificati basati sulla firma elettronica, precisando se la firma è creata o no da un dispositivo per la creazione di una firma sicura.

Informazioni complementari relative a altri CSP soggetti a supervisione/accreditamento che non rilasciano QC al pubblico (ad esempio, CSP che forniscono servizi di orodatazione e che rilasciano gettoni di orodatazione, CPS che rilasciano certificati non qualificati, ecc.) possono essere inseriti in un elenco di fiducia a livello nazionale e su base facoltativa.

L'elenco di fiducia ha l'obiettivo di:

— elencare e fornire informazioni affidabili sulla situazione di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte dello Stato membro responsabile dell'elaborazione e della gestione dell'elenco ai fini della conformità con le pertinenti disposizioni della direttiva 1999/93/CE,

— facilitare la convalida delle firme elettroniche basate sui servizi di certificazione soggetti a supervisione/accreditamento dei CSP che figurano nell'elenco.

Una serie unica di valori di supervisione/accreditamento

Ogni Stato membro deve elaborare e gestire un unico TL per indicare la situazione di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte dello Stato membro.

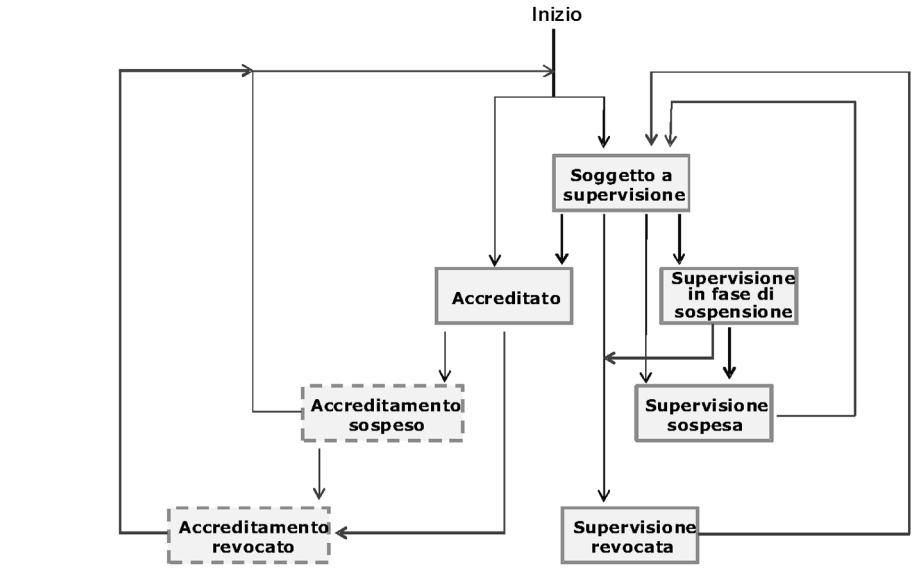
Il fatto che il servizio sia attualmente soggetto a supervisione/accreditamento parte del suo status attuale. Oltre a questo lo status di supervisione o accreditamento può essere «in corso», «in fase di sospensione», «sospeso» o persino «revocato». Durante la sua durata lo stesso servizio di certificazione può passare da uno status di supervisione a uno di accreditamento e viceversa ([1]).

La figura 1 riportata di seguito descrive il percorso atteso, per un singolo servizio di certificazione, tra i possibili status di supervisione/accreditamento:

([1]) Ad esempio un prestatore di servizi di certificazione stabilito in uno Stato membro che fornisce un servizio di certificazione inizialmente soggetto alla supervisione dello Stato membro (organismo di supervisione) può, dopo un certo periodo, passare all'accreditamento facoltativo per il servizio di certificazione soggetto a supervisione. Analogamente un prestatore di servizi di certificazione stabilito in un altro Stato membro può decidere di non interrompere un servizio di certificazione accreditato ma di passare da uno status di accreditamento a uno status di supervisione, ad esempio per motivi commerciali e/o economici.

▼C1

Flusso previsto dello status di supervisione/accreditamento di un servizio CSP



Legenda:

Status transitorio quando esiste un modello di supervisione corrispondente (come ad esempio per i CSP che rilasciano QC quando sono stabiliti in uno Stato membro).

Status attuale possibile quando non esiste un modello di supervisione corrispondente (come ad esempio per i CSP che non rilasciano QC).

Status attuale possibile.

Figura 1

Un servizio di certificazione che rilascia QC deve essere soggetto a supervisione (se è stabilito in uno Stato membro) e può ottenere l'accreditamento facoltativo. Lo status di un tale servizio se riportato nell'elenco di fiducia può corrispondere a uno qualsiasi dei valori riportati nella figura come «valore di status attuale». Va notato tuttavia che «accreditamento sospeso» e «accreditamento revocato» devono essere esclusivamente valori di status di «temporaneo» nel caso di servizi CSP_{QC} stabiliti in uno Stato membro, in quanto tali servizi devono comunque essere soggetti a supervisione (anche quando non siano o non siano più accreditati).

Gli Stati membri che hanno istituito, o siano in procinto di istituire, un «regime di approvazione riconosciuto», definito e attuato su base nazionale ai fini del controllo della conformità dei servizi dei CSP che non rilasciano QC con le disposizioni della direttiva 1999/93/CE e con eventuali disposizioni della normativa nazionale in materia di fornitura di servizi di certificazione (nell'accezione dell'articolo 2, punto 11, della direttiva), sono tenuti a inserire tali regimi in una delle due seguenti categorie:

— «accreditamento facoltativo», quale definito e disciplinato nella direttiva 1999/93/CE [articolo 2, punto 13, articolo 3, paragrafo 2, articolo 7, paragrafo 1, lettera a), articolo 8, paragrafo 1, articolo 11, considerando 4 e 11-13],

— «supervisione», come previsto dalla direttiva 1999/93/CE e attuato dalle disposizioni e requisiti nazionali in conformità delle relative legislazioni.

▼C1

Di conseguenza un servizio di certificazione che non rilascia QC può essere oggetto di supervisione o ottenere l'accreditamento facoltativo. Lo status di un tale servizio, se riportato nell'elenco di fiducia, può avere uno qualsiasi dei valori riportati nella figura come «valore di status attuale» (cfr. figura 1).

L'elenco di fiducia deve contenere informazioni relative ai regimi di supervisione/accreditamento soggiacenti, e in particolare:

— informazioni sul sistema di supervisione applicabile a tutti i CSP_{QC},

— se pertinente, informazioni sul regime nazionale di «accreditamento facoltativo» applicabile a tutti i CSP_{QC},

— se pertinente, informazioni sul sistema di supervisione applicabile a tutti i CSP che non rilasciano QC,

— se pertinente, informazioni sul regime nazionale di «accreditamento facoltativo» applicabile a tutti i CSP che non rilasciano QC.

Le ultime due serie di informazioni rivestono importanza cruciale per gli utilizzatori dei certificati, in quanto consentono loro di valutare il livello di qualità e di sicurezza dei sistemi di supervisione/accreditamento applicati a livello nazionale ai CSP che non rilasciano QC. Quando l'informazione sullo status di supervisione/accreditamento è fornita nel TL in relazione ai servizi dei CSP che non rilasciano QC, le informazioni sopramenzionate devono essere fornite a livello del TL mediante l'uso dei campi «Scheme information URI» (clausola 5.3.7 — informazioni fornite dagli Stati membri),«Scheme type/community/rules» (clausola 5.3.9 — mediante l'uso di un testo comune a tutti gli Stati membri e di informazioni specifiche, facoltative, fornite da uno Stato membro) e «TSL policy/legal notice» (clausola 5.3.11 — un testo comune a tutti gli Stati membri con riferimento alla direttiva 1999/93/CE, con la possibilità per ciascuno Stato membro di aggiungere testi/riferimenti specifici per tale Stato membro). Informazioni supplementari di «qualificazione» definite al livello dei sistemi nazionali di supervisione/accreditamento per CSP che non rilasciano QC possono essere fornite a livello del servizio se pertinente e richiesto (ad esempio per distinguere tra livelli diversi di qualità/sicurezza) mediante l'uso dell'estensione «additionalServiceInformation» (clausola 5.8.2) come parte della «Service information extension» (clausola 5.5.9). Ulteriori informazioni sulle specifiche tecniche corrispondenti sono fornite nelle specifiche dettagliate del capitolo I.

Nonostante il fatto che in uno Stato membro organismi distinti possano essere responsabili della supervisione e dell'accreditamento dei servizi di certificazione, è previsto che sia utilizzata una sola voce per un singolo servizio di certificazione [identificata dal campo «Service digital identity» come previsto dalla norma ETSI TS 102 231 ([1])] e che lo status di supervisione/accreditamento sia aggiornato di conseguenza. Il significato degli status di cui sopra è descritto nella pertinente clausola 5.5.4 delle specifiche tecniche dettagliate di cui al capitolo I.

2.2. *Voci del TL destinate a facilitare la convalida di QES e $AdES_{QC}$*

L'aspetto più importante della creazione di un TL è la definizione della parte obbligatoria dello stesso, ovvero l'«elenco dei servizi» per i CSP che rilasciano QC, al fine di stabilire l'esatto status di ciascun servizio di certificazione che rilascia QC e di garantire che le informazioni fornite in ciascuna voce siano sufficienti per facilitare la convalida di QES e $AdES_{QC}$ (quando combinate con il contenuto del QC entità finale rilasciato dal CSP nell'ambito del servizio di certificazione menzionato nella voce di cui trattasi).

([1]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

Poiché non esiste un profilo autenticamente interoperabile e transfrontaliero per i QC, tra le informazioni richieste potrebbero figurarne altre oltre a quelle del campo «Service digital identity» di un'unica CA (radice), in particolare le informazioni che identificano lo status QC del certificato rilasciato e che chiariscono se le firme siano state create o no mediante un SSCD. L'organismo designato in uno Stato membro per elaborare, modificare e gestire il TL (il «gestore di sistema» secondo la norma ETSI TS 102 231) deve pertanto tenere conto del profilo attuale e del contenuto del certificato per ogni QC rilasciato da ciascun CSP_{QC} che figura nell'elenco.

Idealmente ciascun QC rilasciato dovrebbe contenere la dichiarazione di conformità ([1]) dei QC stabilita dall'ETSI (QcCompliance) quando tale certificato è dichiarato come QC, nonché la dichiarazione QcSSCD definita dall'ETSI quando si dichiara che il certificato è basato su un SSCD per generare firme elettroniche e/o che ciascun QC rilasciato include uno degli identificativi dell'oggetto (OID) per la politica dei certificati QCP/QCP+, quali definiti nella norma ETSI TS 101 456 ([2]). L'uso di differenti norme di riferimento da parte dei CSP che rilasciano QC, il fatto che l'interpretazione di tali norme varia considerevolmente come pure la scarsa consapevolezza dell'esistenza e della preesistenza di alcune norme o specifiche tecniche normative ha determinato differenze nel contenuto effettivo dei QC attualmente rilasciati (ad esempio per quanto riguarda l'uso delle dichiarazioni QC definite dall'ETSI) e, di conseguenza, impedisce agli utilizzatori di fare affidamento solo sul certificato del firmatario (e sul percorso ad esso associato) per verificare, quantomeno in modo leggibile a macchina, se il certificato su cui si basa una firma elettronica sia dichiarato o no un QC e se esso sia associato o no a un SSCD mediante il quale è stata generata la firma elettronica.

Compilando i campi «Service type identifier» («Sti»), «Service name» («Sn»), e «Service digital identity» («Sdi») ([3]) con le informazioni fornite nel campo «Service information extensions» («Sie») si permette al modello unico di TL proposto di determinare appieno il tipo specifico di certificato qualificato rilasciato da un servizio di certificazione di un CSP compreso nell'elenco che rilascia QC e di comunicare se esso è basato o no su un SSCD (qualora tale informazione non sia riportata nel QC). A questa voce è associata ovviamente un'informazione specifica «Service current status» («Scs»), come illustrato nella figura 2 riportata di seguito.

Elencare un servizio fornendo semplicemente il campo «Sdi» di una CA (radice) significherebbe che esso è garantito (da un CSP che rilascia QC ma anche dall'organismo di supervisione/accreditamento responsabile di tale CSP), che qualsiasi certificato entità finale rilasciato tramite tale gerarchia di CA (radice) contiene sufficienti informazioni definite dalle norme ETSI e leggibili a macchina per verificare se si tratti o no di un QC e se esso sia basato o no su un SSCD. Nel caso in cui, ad esempio, l'ultima asserzione non sia vera (ad esempio, nel QC non vi è alcuna indicazione basata sulle norme ETSI e leggibile a macchina che esso sia basato su un SSCD), se viene elencato semplicemente il campo «Sdi» della CA (radice) si può solo concludere che i QC rilasciati tramite tale gerarchia di CA (radice) non siano basati su alcun SSCD. Per poter considerare i QC in questione basati su un SSCD è necessario che tale indicazione sia fornita utilizzando il campo «Sie» (indicante inoltre che tale informazione è garantita dal CSP che rilascia i QC ed è soggetto a supervisione/accreditamento da parte rispettivamente di un organismo di supervisione o di accreditamento).

([1]) Refer to ETSI TS 101 862 — Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

([2]) ETSI TS 101 456 — Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

([3]) Ovvero, come minimo, un certificato X.509 v3 della QCA emittente o di una CA superiore nel percorso di certificazione.

▼C1

Principi generali – Norme di modifica – Voci CSP_{QC} (servizi compresi nell' elenco)

Voce relative ad un servizio per un CSP_{QC} compreso nell'elenco:

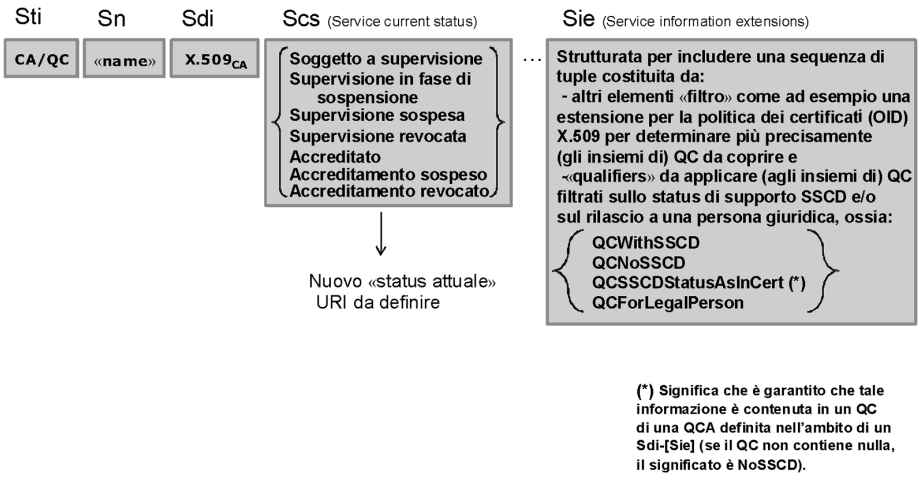


Figura 2

Voce relativa a un servizio di un CSP compreso nell'elenco che rilascia QC nel TL attuato nel formato TSL

Le presenti specifiche tecniche relative al modello comune per il TL consentono di utilizzare una combinazione di cinque tipi principali di informazioni nella voce relativa a un servizio:

— il «Service type identifier» («Sti»), ovvero l'identificazione di una CA che rilascia QC («CA/QC»),

— il «Service name» («Sn»),

— le informazioni del campo «Service digital identity» («Sdi») che identifica un servizio elencato, ad esempio, (come minimo) il certificato X.509v3 di una CA che rilascia QC,

— per i servizi CA/QC informazioni facoltative relative al campo «Service information extensions» («Sie») che permettono di includere una sequenza di una o più tuple, ciascuna delle quali fornisce:

  — i criteri da utilizzare per identificare più precisamente (filtrare), all'interno del servizio di certificazione identificato dal campo «Sdi», il servizio (ovvero un insieme di certificati qualificati) per cui sono richieste/fornite informazioni supplementari indicanti che il certificato è basato o no sull'SSCD (e/o è rilasciato a una persona giuridica), e

  — le informazioni associate («qualifiers») indicanti se questa serie di servizi di certificati qualificati identificati più precisamente si basano o no su un SSCD o se le informazioni associate sono parte di un QC in formato standard leggibile a macchina e/o informazioni relative al fatto che tali QC sono rilasciati a persone giuridiche (di norma si considera che essi siano rilasciati soltanto a persone fisiche),

▼C1

— informazioni sullo «status attuale» della voce relativa a tale servizio che specificano:

— se si tratta di un servizio oggetto di supervisione o accreditato, e

— lo status di supervisione/accreditamento.

2.3. *Orientamenti per la modifica e l'utilizzo delle voci relative ai servizi CSP_{QC}*

Gli **orientamenti generali per la creazione e la modifica delle voci** sono i seguenti:

1) Se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/organismo di accreditamento) che per un servizio compreso nell'elenco e identificato da un campo «Sdi», tutti i QC basati su un SSCD contengono la dichiarazione di conformità dei QC stabilita dall'ETSI e la dichiarazione QcSSCD e/o l'identificativo di oggetto (OID) QCP +, l'uso di un appropriato «Sdi» è sufficiente e il campo «Sie» può essere utilizzato in via facoltativa e non è necessario che contenga le informazioni relative al SSCD.

2) Se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/organismo di accreditamento) che per un servizio compreso nell'elenco e identificato da un campo «Sdi», tutti i QC non basati su un SSCD contengono la dichiarazione di conformità dei QC e/o l'identificativo di oggetto (OID) QCP, ma sono tali da non dover contenere la dichiarazione QcSSCD e/o l'identificativo di oggetto (OID) QCP+, l'uso di un appropriato campo «Sdi» è sufficiente e il campo «Sie» può essere utilizzato in via facoltativa e non è necessario che contenga le informazioni relative al SSCD (il che significa in altri termini che non è basato su un SSCD).

3) Se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/organismo di accreditamento) che per un servizio compreso nell'elenco e identificato da un campo «Sdi», tutti i QC contengono la dichiarazione di conformità dei QC stabilita dall'ETSI, e alcuni di questi QC sono basati su un SSCD mentre altri non lo sono (ad esempio la differenza può essere stabilita mediante differenti OID per la politica dei certificati specifici per CSP o mediante altre informazioni specifiche sui CSP contenute nel QC, direttamente o indirettamente e leggibili o no a macchina) ma non contengono NÉ la dichiarazione QcSSCD NÉ l'identificativo di oggetto (OID) QCP + dell'ETSI, l'uso di un appropriato campo «Sdi» può non essere sufficiente E il campo «Sie» deve essere utilizzato per indicare in modo esplicito che il servizio è basato sul SSCD oltre a una eventuale estensione dell'informazione per identificare l'insieme dei certificati coperti. È probabile che differenti «SSCD support information values» debbano essere utilizzati per lo stesso campo «Sdi» quando viene utilizzato il campo «Sie».

4) Se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/organismo di accreditamento) che per un servizio compreso nell'elenco e identificato da un campo «Sdi», uno qualsiasi dei QC non contiene la dichiarazione di conformità dei QC, l'identificativo di oggetto (OID) QCP, la dichiarazione QcSSCD o l'identificativo di oggetto (OID) QCP+, ma è garantito che alcuni di questi certificati entità finale rilasciati in base a tale «Sdi» sono da considerarsi QC e/o sono basati su SSCD mentre altri non lo sono (ad esempio la differenza può essere stabilita mediante differenti OID per la politica dei certificati specifici per CSP_{QC} o mediante altre informazioni specifiche sui CSP_{QC} contenute nel QC, direttamente o indirettamente e leggibili o no a macchina) l'uso di un appropriato campo «Sdi» non è sufficiente E il campo «Sie» deve essere utilizzato per indicare in modo esplicito che il servizio è basato sul SSCD. È probabile che differenti «SSCD support information values» debbano essere utilizzati per lo stesso campo «Sdi» quando viene utilizzato il campo «Sie».

▼C1

Il principio generalmente applicato è che per un CSP inserito nell'elenco di fiducia vi deve essere una voce di servizio per singolo certificato X.509v3 per un servizio di certificazione CA/QC, ovvero un'autorità di certificazione che rilascia (direttamente) QC. In alcune circostanze accuratamente definite e gestite, l'organismo di supervisione/accreditamento di uno Stato membro può decidere di utilizzare il certificato X.509v3 di una CA radice o di livello superiore (ovvero un'autorità di certificazione che non rilascia direttamente QC per entità finali ma che certifica una gerarchia di CA fino a quelle che rilasciano QC a entità finali) come campo «Sdi» di una singola voce nell'elenco di servizi forniti da un CSP iscritto nell'elenco. Gli Stati membri devono valutare accuratamente le conseguenze (positive o negative) dell'uso di un certificato X.509v3 di una CA radice o di livello superiore per i valori di «Sdi» delle voci dei servizi iscritti nel TL e assumersene le conseguenze. Inoltre, se viene utilizzata questa eccezione autorizzata al principio generale, gli Stati membri sono tenuti a fornire la necessaria documentazione per facilitare l'elaborazione e la verifica del percorso di certificazione.

Per illustrare gli orientamenti generali per la creazione e la modifica delle voci può essere dato il seguente esempio: nel caso di un CSP_{QC} che utilizza una CA radice che ingloba diverse CA che rilasciano QC e non QC, ma per il quale i QC contengono unicamente la dichiarazione QcCompliance ma non l'indicazione se il servizio si basi o meno su un SSCD, secondo le norme sopraindicate il fatto di elencare soltanto il campo «Sdi» della CA radice significa che tutti i QC rilasciati nell'ambito della gerarchia di tale CA radice NON sono basati su un SSCD. Ma se tali QC sono effettivamente basati su un SSCD, si raccomanda vivamente di utilizzare la dichiarazione QcSSCD per i QC rilasciati in futuro. Nel frattempo (ovvero fino a quando non sia arrivato a scadenza l'ultimo QC non contenente tale informazione), il TSL dovrebbe utilizzare il campo «Sie» e l'estensione associata «Qualifications», ad esempio filtrando i certificati mediante OID specifici dei CSP_{QC} che possano essere utilizzati dai CSP_{QC} per stabilire una distinzione tra differenti tipi di QC (alcuni basati su un SSCD e altri no), inserendo informazioni esplicite del tipo «SSCD support information» in relazione ai certificati filtrati mediante l'uso di «Qualifiers».

Gli **orientamenti generali** per l'utilizzo di applicazioni, servizi o prodotti relativi alla firma elettronica e basati su una applicazione TSL di un elenco di fiducia sono, conformemente alle presenti specifiche tecniche, i seguenti:

Una voce «Sti» CA/QC (e analogamente una voce CA/QC ulteriormente qualificata come «RootCA/QC» mediante l'uso dell'estensione «Sie»«additionalServiceInformation»)

— indica che tutti i certificati entità finale rilasciati da una CA identificata mediante «Sdi» (e analogamente all'interno della gerarchia CA, partendo dalla CA radice identificata dal campo «Sdi») sono QC a condizione che ciò sia indicato nel certificato mediante l'uso di opportune dichiarazioni QC (ovvero QcC, QcSSCD) e/o OID QCP + definiti dall'ETSI (e che ciò sia garantito dall'organismo di supervisione/accreditamento, cfr. supra gli «orientamenti generali per la creazione e la modifica delle voci»).

Nota: se non è fornita un'informazione «Sie»«Qualification» o se un certificato entità finale presentato come QC non è «ulteriormente identificato» da una voce correlata «Sie», le informazioni «leggibili a macchina» riportate nel QC devono essere soggette a supervisione/accreditamento per dimostrarne l'accuratezza. Ciò significa che l'uso (o no) delle opportune dichiarazioni QC (ovvero QcC, QcSSCD) e/o OID QCP + definiti dall'ETSI è garantito come conforme a quanto indicato dal CSP_{QC},

▼C1

— **e SE** è fornita un'informazione «Sie»«Qualification», in aggiunta alle regole interpretative di cui sopra relative all'uso standard, i certificati identificati mediante l'uso della voce «Sie»«Qualification», che è costruita sul principio di una sequenza di filtri che identificano ulteriormente una serie di certificati e forniscono informazioni supplementari in materia di SSCD e/o «persona giuridica come soggetto» (ad esempio i certificati che contengono un OID nell'estensione sulla politica del certificato e/o che hanno uno specifico «Key usage» e/o che sono filtrati mediante l'uso di un valore specifico che compare in un campo specifico del certificato o estensione, ecc.) devono essere considerati sulla base della seguente serie di «qualifiers», per compensare la mancanza di informazioni nel corrispondente QC, ovvero:

— per indicare il supporto di un SSCD:

  — il valore «QCWithSSCD» indicante che un «QC è basato su un SSCD», oppure

  — il valore «QCNoSSCD» indicante che un «QC non è basato su un SSCD», oppure

  — il valore «QCSSCDStatusAsInCert» indicante che è garantito che tutti i QC contengono, nei campi «Sdi»-«Sie» della voce CA/QC, informazioni relative al supporto SSCD,

  E/O

— per indicare il rilascio a una persona giuridica:

  — il valore «QCForLegalPerson» indicante che il certificato è rilasciato a una persona giuridica.

2.4. *Servizi su cui sono basati i servizi «CA/QC» ma che non sono parte del campo «Sdi»«CA/QC»*

È opportuno considerare anche i casi in cui le risposte CRL e OCSP sono firmate mediante chiavi diverse da quelle di una CA che rilascia QC («CA/QC»). Ciò può avvenire elencando i servizi in questione come tali nell'applicazione TSL del TL (ovvero, con un «Service type identifier» ulteriormente qualificato da un'estensione «additionalServiceInformation», indicante che un servizio OCSP o CRL è parte della fornitura dei QC, ad esempio con un tipo di servizio di «OCSP/QC» o rispettivamente «CRL/QC»), dal momento che questi servizi possono essere considerati parte dei servizi «qualificati» oggetto di supervisione/accreditamento in relazione alla fornitura di servizi di certificazione QC. Ovviamente i risponditori OCSP e gli emittenti di CRL i cui certificati sono firmati dalle CA che si trovano in una gerarchia di servizi CA/QC compresi nell'elenco devono essere considerati «validi» conformemente al valore del servizio CA/QC compreso nell'elenco.

Una disposizione analoga può applicarsi ai servizi di certificazione che rilasciano certificati non qualificati (del tipo di servizio «CA/PKC»), utilizzando i tipi di servizi standard ETSI TS 102 231 OCSP e CRL.

Si noti che l'applicazione TSL del TL DEVE comprendere servizi di revoca quando le relative informazioni non sono incluse nel campo AIA dei certificati finali o quando non sono firmate da una CA compresa tra quelle che figurano nell'elenco.

2.5. *Verso un profilo QC interoperabile*

Di norma si deve cercare di semplificare (ridurre) al massimo il numero delle voci relative ai servizi (differenti campi «Sdi»). A ciò deve tuttavia affiancarsi la corretta identificazione dei servizi connessi con il rilascio dei QC e la fornitura di informazioni di fiducia indicanti se i QC sono basati o no su un SSCD, qualora tale informazione non sia contenuta nei QC rilasciati.

▼C1

Idealmente l'uso del campo «Sie» e dell'estensione «Qualification» dovrebbe essere (rigorosamente) limitato ai casi specifici che devono essere risolti in tale modo, in quanto i QC dovrebbero contenere sufficienti informazioni su quanto dichiarato, ovvero lo stato «qualificato» e sulla presenza o no di un SSCD.

Nella misura del possibile gli Stati membri dovrebbero fare in modo che siano adottati e utilizzati profili QC interoperabili.

3. **Struttura del modello unico per l'elenco di fiducia**

Il modello comune proposto per l'elenco di fiducia degli Stati membri deve essere strutturato nelle seguenti categorie di informazioni:

1) informazione sull'elenco di fiducia e il regime di rilascio dei certificati;

2) una sequenza di campi contenenti informazioni di identificazione non ambigue su tutti i CSP oggetto di supervisione/accreditamento nell'ambito del regime (questa sequenza è facoltativa, ovvero se non viene usata si suppone che sia vuota, in altri termini che nessun CSP è soggetto a supervisione o accreditamento nello Stato membro associato e nell'ambito dell'elenco di fiducia);

3) per ogni CSP inserito nell'elenco una sequenza di campi contenenti informazioni di identificazione non ambigue sul servizio di certificazione oggetto di supervisione/accreditamento fornito dal CSP (questa sequenza deve avere come minimo una voce);

4) per ogni servizio di certificazione oggetto di supervisione/accreditamento, l'identificazione dello status attuale del servizio e la relativa storia.

Nel caso di un CSP che rilascia QC l'identificazione non ambigua del servizio di certificazione da inserire nell'elenco deve tenere conto delle situazioni in cui nel certificato qualificato non sono disponibili informazioni sufficienti sul suo essere «qualificato», del fatto che possa essere basato su un SSCD, soprattutto considerando che la maggior parte dei CSP (commerciali) utilizzano un'unica CA qualificata per il rilascio di diversi tipi di certificati entità finale, sia qualificati che non qualificati.

Il numero delle voci dell'elenco per CSP riconosciuto può essere ridotto qualora esistano uno o più servizi di CA di livello superiore, ad esempio nell'ambito di una gerarchia commerciale di CA che va dalla CA radice fino alle CA che rilasciano i certificati. Tuttavia, anche in questi casi deve essere mantenuto e garantito il principio che impone di garantire un collegamento senza ambiguità tra un servizio di certificazione CSP_{QC} e l'insieme dei certificati da identificare.

1. *Informazione sull'elenco di fiducia e il regime di rilascio dei certificati*

In questa categoria rientrano le seguenti informazioni:

— un'**etichetta (tag)** dell'elenco di fiducia per facilitare l'identificazione di quest'ultimo nel corso di ricerche elettroniche e che ne confermi gli obiettivi quando è in formato leggibile all'uomo,

— un **formato** di elenco di fiducia e un **identificativo della versione di formato**,

— un **numero d'ordine (o di pubblicazione)** dell'elenco di fiducia,

— **informazioni sul tipo** di elenco di fiducia (ad esempio per indicare che l'elenco di fiducia in questione contiene informazioni sullo status di supervisione/accreditamento dei servizi di certificazione forniti da CSP oggetto di supervisione/accreditamento da parte dello Stato membro considerato ai fini del rispetto delle disposizioni della direttiva 1999/93/CE),

▼C1

— **informazioni sul proprietario** dell'elenco di fiducia (ad esempio, nome, indirizzo, coordinate di contatto, ecc. dell'organismo dello Stato membro incaricato di elaborare, pubblicare in modo sicuro e aggiornare l'elenco di fiducia),

— **informazioni sul o sui regimi soggiacenti di supervisione/accreditamento** ai quali è associato l'elenco di fiducia e in particolare, ma non unicamente, le seguenti:

  — il paese in cui si applica,

  — informazioni su o riferimento al luogo in cui sono reperibili informazioni sul o sui regimi (modello di regime, norme, criteri, comunità di applicazione, tipo, ecc.),

  — periodo di mantenimento delle informazioni (serie storiche),

— **politica e/o avviso legale, impegni, responsabilità** dell'elenco di fiducia,

— **data e ora di pubblicazione e prossimo aggiornamento previsto** dell'elenco di fiducia.

2. *Informazioni di identificazione non ambigue su tutti i CSP riconosciuti dal regime*

Questa serie deve comprendere quantomeno le seguenti informazioni:

— la denominazione del CSP quale figura nei registri ufficiali (compreso eventualmente il nome utente (UID) dell'organizzazione CPS secondo le prassi utilizzate negli Stati membri),

— l'indirizzo del CPS e le coordinate di contatto,

— informazioni aggiuntive sul CPS inserite direttamente o mediante riferimento a un sito da cui possono essere scaricate.

3. *Per ogni CSP inserito nell'elenco una sequenza di campi contenenti informazioni di identificazione non ambigue sul servizio di certificazione fornito dal CPS e soggetto a supervisione/accreditamento nel quadro della direttiva 1999/93/CE*

Questa serie deve comprendere quantomeno le seguenti informazioni per ciascun servizio di certificazione di un CSP incluso nell'elenco:

— un identificativo del tipo di servizio di certificazione (ad esempio, un identificativo indicante che il servizio di certificazione soggetto a controllo/accreditamento fornito dal CSP è un'autorità di certificazione che rilascia QC),

— denominazione (commerciale) del servizio di certificazione,

— un identificativo unico e non ambiguo del servizio di certificazione,

— informazioni aggiuntive sul servizio di certificazione (ad esempio inserite direttamente o mediante riferimento a un sito da cui possono essere scaricate, informazioni di accesso relative al servizio),

— per i servizi CA/QC, una sequenza facoltativa di tuple di informazione, in cui ciascuna tupla indica:

  i) i criteri da utilizzare per identificare più precisamente (filtrare), all'interno del servizio di certificazione identificato «Sdi», il servizio preciso (ovvero un insieme di certificati qualificati) per cui sono richieste/fornite informazioni supplementari per quanto concerne il fatto che il certificato è basato o no sull'SSCD (e/o è rilasciato a una persona giuridica); e

  ii) le informazioni associate («qualifiers») indicanti se questa serie di servizi di certificati qualificati rilasciati da un servizio identificato più precisamente si basano o no su un SSCD e/o informazioni relative al fatto che tali QC sono rilasciati a persone giuridiche (di norma si considera che essi siano rilasciati a persone fisiche).

▼C1

4. *Per ogni servizio di certificazione, l'identificazione dello status attuale del servizio e la relativa storia*

Questa serie deve comprendere quantomeno le seguenti informazioni:

— un identificativo dello status attuale,

— la data e l'ora di inizio dello status attuale,

— informazioni storiche su tale status.

4. **Definizioni e acronimi**

Ai fini del presente documento sono utilizzate le seguenti definizioni e i seguenti acronimi:

Termine	Acronimo	Definizione
Prestatore di servizi di certificazione	CSP	Quale definito all'articolo 2, punto 11, della direttiva 1999/93/CE.
Autorità di certificazione	CA	Una CA è un CSP e può utilizzare diverse chiavi di firme private di diverse CA tecniche, ciascuna con un certificato associato, per rilasciare certificati entità finale. Una CA è un'autorità cui fanno affidamento uno o più utilizzatori per la creazione e il rilascio di certificati. Facoltativamente l'autorità di certificazione può creare le chiavi dell'utente [ETSI TS 102 042]. L'identificazione della CA avviene di norma mediante le informazioni di identificazione presenti nel campo «emittente» del certificato della CA che serve a certificare la chiave pubblica associata alla chiave di firma privata della CA e che viene di fatto usata dalla CA per rilasciare i certificati. Una CA può avere diverse chiavi di firma. Ogni chiave di una CA è identificata da un identificativo unico che figura nel campo Authority Key Identifier del certificato della CA.
Autorità di certificazione che rilascia certificati qualificati	CA/QC	Una CA conforme ai requisiti di cui all'allegato II della direttiva 1999/93/CE che rilascia certificati qualificati conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE.
Certificato	Certificato	Quale definito all'articolo 2, punto 9, della direttiva 1999/93/CE.
Certificato qualificato	QC	Quale definito all'articolo 2, punto 10, della direttiva 1999/93/CE.
Firmatario	Firmatario	Quale definito all'articolo 2, punto 3, della direttiva 1999/93/CE.
Supervisione	Supervisione	Il termine «supervisione» è utilizzato nell'accezione della direttiva 1999/93/CE (articolo 3, paragrafo 3). La direttiva stabilisce che gli Stati membri devono provvedere affinché venga istituito un sistema appropriato di supervisione dei CPS stabiliti nel loro territorio e che rilasciano al pubblico certificati qualificati, accertandosi così che siano rispettate le disposizioni della direttiva.
Accreditamento facoltativo	Accreditamento	Quale definito all'articolo 2, punto 13, della direttiva 1999/93/CE.
Elenco di fiducia	TL	Designa l'elenco indicante lo status di supervisione/accreditamento dei servizi di certificazione dei CPS che sono soggetti a supervisione/accreditamento dello Stato membro interessato per verificarne la conformità con le disposizioni della direttiva 1999/93/CE.

▼C1

Termine	Acronimo	Definizione
Elenco di status dei servizi di fiducia	TSL	Elenco firmato utilizzato come base per la presentazione di informazioni sullo status dei servizi di fiducia conformemente alle specifiche della norma ETSI TS 102 231.
Servizio di fiducia		Servizio che permette di aumentare la fiducia nelle transazioni elettroniche (in generale, ma non necessariamente, mediante l'uso di tecniche crittografiche o di materiale riservato) (ETSI TS 102 231).
Prestatore di servizi di fiducia	TSP	Organismo che gestisce uno o più servizi (elettronici) di fiducia (questo termine è utilizzato in un'accezione più ampia rispetto a CSP).
Gettoni di servizio di fiducia	TrST	Un oggetto fisico o binario (logico) generato o rilasciato a seguito dell'uso di un servizio di fiducia. Esempi di TrST binari sono i certificati, i CRL, i gettoni di orodatazione e le risposte OCSP.
Firma elettronica qualificata	QES	Un'AdES basata su un QC e creata da un SSCD, quale definita all'articolo 2 della direttiva 1999/93/CE.
Firma elettronica avanzata	AdES	Quale definita all'articolo 2, punto 2, della direttiva 1999/93/CE.
Firma elettronica avanzata basata su un certificato qualificato	$AdES_{QC}$	Una firma elettronica conforme ai requisiti applicabili alle AdES e basata su un QC, quale definito all'articolo 2 della direttiva 1999/93/CE.
Dispositivo per la creazione di una firma sicura	SSCD	Quale definito all'articolo 2, punto 6, della direttiva 1999/93/CE.

CAPITOLO I

SPECIFICHE TECNICHE DETTAGLIATE DI UN MODELLO COMUNE PER L'«ELENCO DI FIDUCIA DI FORNITORI DI SERVIZI DI CERTIFICAZIONE QUALIFICATI SOGGETTI A SUPERVISIONE/ACCREDITAMENTO»

Nella parte seguente del documento le parole chiave «DEVE», «NON DEVE», «OBBLIGATORIO», «DOVREBBE», «NON DOVREBBE», «SI RACCOMANDA», «SI CONSIGLIA», «PUÒ», «POSSONO», «NON PUÒ», «NON POSSONO» e «FACOLTATIVO» devono essere interpretate nell'accezione di cui al documento RFC 2119 ([1]).

►M1 Le presenti specifiche si basano sulle specifiche e sui requisiti della norma ETSI TS 102 231 v.3.1.2. Qualora nelle presenti specifiche non siano indicati requisiti specifici si DEVONO applicare integralmente i requisiti della norma ETSI TS 102 231 v.3.1.2. ◄ Se invece nelle presenti specifiche sono indicati requisiti specifici, questi ultimi DEVONO essere applicati al posto dei requisiti di ETSI TS 102 231, integrandoli tuttavia, per quanto riguarda il formato, con i requisiti di ETSI TS 102 231. In caso di discrepanze tra le presenti specifiche e quelle della norma ETSI TS 102 231, DEVONO essere applicate le presenti specifiche.

([1]) IETF RFC 2119: «Key words for use in RFCs to indicate Requirements Levels».

▼C1

A livello linguistico DEVE essere attuato e fornito un supporto almeno in lingua inglese (EN) e, eventualmente e in aggiunta all'inglese, in una o più lingue nazionali.

L'indicazione della data e dell'ora DEVE essere conforme alla clausola 5.1.4 di ETSI TS 102 231.

L'uso degli URI DEVE essere conforme alla clausola 5.1.5 di ETSI TS 102 231.

Informazioni sul regime di rilascio dell'elenco di fiducia

Tag

TSL tag (clausola 5.2.1)

Questo campo è OBBLIGATORIO e DEVE essere conforme alla clausola 5.2.1 di ETSI TS 102 231.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (clausola 5.3.1)

Questo campo è OBBLIGATORIO e DEVE essere impostato sul valore «3» (intero).

TSL sequence number (clausola 5.3.2)

▼M1

Il presente campo è OBBLIGATORIO e DEVE specificare il numero di sequenza della TSL. Questo valore, che comincia per il valore intero «1» al momento della prima pubblicazione dell'elenco di fiducia, DEVE essere aumentato ad ogni pubblicazione successiva dell'elenco. Esso NON DEVE essere resettato a «1» in caso di incremento del «TSL version identifier» di cui sopra.

▼C1

TSL type (clausola 5.3.3)

▼M1

Questo campo è OBBLIGATORIO e indica il tipo di TSL. DEVE essere impostato su http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (generico).

▼C1

Nota: per essere conforme alla clausola 5.3.3 della norma ETSI TS 102 231, e per indicare il tipo di TSL, facendo riferimento all'esistenza delle presenti specifiche che disciplinano l'applicazione TSL degli elenchi di fiducia degli Stati membri ([1]) e consentendo a un analizzatore sintattico (parser) di determinare quale formato dei campi seguenti ([2]) è impiegato quando tali campi hanno significati specifici (o alternativi) a seconda del tipo di TSL rappresentato (in questo caso l'elenco di fiducia di uno Stato membro), l'URI specifico di cui sopra DEVE essere registrato e descritto come segue:

([1]) Ovvero «l'elenco indicante lo status di supervisione/accreditamento dei servizi di certificazione dei CPS che sono soggetti alla supervisione/controllo dello Stato membro interessato per verificarne la conformità con le disposizioni della direttiva 1999/93/CE» (in breve l'«elenco di fiducia»).

([2]) Ovvero i campi specificati da ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Fornitura di informazioni armonizzate sullo stato dei servizi di fiducia «affinate» dalle presenti specifiche in modo da indicare la creazione dell'elenco di fiducia degli Stati membri.

▼M1

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

▼C1

Descrizione: un'applicazione TSL di un elenco indicante lo status di supervisione/accreditamento dei servizi di certificazione forniti da prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte dello Stato membro che possiede l'applicazione TSL per quanto concerne la conformità con le disposizioni pertinenti della direttiva 1999/93/CE mediante un processo diretto di supervisione (facoltativo o normativo).

Scheme operator name (clausola 5.3.4)

Questo campo è OBBLIGATORIO e DEVE specificare il nome dell'organismo dello Stato membro incaricato di elaborare, pubblicare e aggiornare l'elenco di fiducia nazionale. Esso DEVE indicare la denominazione ufficiale con la quale opera l'entità giuridica o incaricata (ad esempio nel caso di enti amministrativi governativi) associata a tale organismo. La denominazione in parola DEVE essere quella utilizzata negli atti ufficiali (legali) di registrazione o autorizzazione e alla quale dovrebbe essere indirizzata ogni comunicazione ufficiale. Si DEVE trattare di una sequenza di stringhe di caratteri multilingui e DEVE essere attuata con l'inglese (EN) come lingua obbligatoria e eventualmente con una o più lingue nazionali.

Nota: un paese PUÒ avere organismi distinti di supervisione/accreditamento e anche altri organismi incaricati delle attività operative correlate. ►M1 Spetta a ciascuno Stato membro designare il gestore del sistema per l'applicazione TSL dell'elenco di fiducia dello Stato membro. ◄ L'ente di supervisione, l'ente di accreditamento e il gestore del sistema (quando siano enti distinti) devono avere ciascuno i propri compiti e responsabilità.

Qualsiasi situazione in cui diversi organismi sono responsabili della supervisione, dell'accreditamento e degli aspetti operativi DEVE essere coerentemente indicata come tale nelle informazioni sul sistema comprese nel TL, comprese le informazioni specifiche del sistema indicate dallo «Scheme information URI» (clausola 5.3.7).

▼M1

L'entità che firma la TSL è il citato gestore del sistema (clausola 5.3.4).

▼C1

Scheme operator address (clausola 5.3.5)

Questo campo è OBBLIGATORIO e DEVE contenere l'indirizzo dell'entità giuridica o dell'organizzazione designata identificata nel campo «Scheme operator name» (clausola 5.3.4) per le comunicazioni postali ed elettroniche. DEVE contenere sia «PostalAddress» (ossia nome e numero civico, località [Stato o provincia], [codice postale] e il codice paese ISO 3166-1 alpha-2) conformemente alla clausola 5.3.5.1 che «ElectronicAddress» (ossia email e/o sito web URI) conformemente alla clausola 5.3.5.2.

Scheme name (clausola 5.3.6)

Questo campo è OBBLIGATORIO e indica il nome del sistema. Si DEVE trattare di una sequenza di stringhe di caratteri multilingui (con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali), definite come segue:

▼C1

— la versione EN DEVE essere costituita da una stringa di caratteri strutturata come segue:

CC:EN_name_value

dove:

— «CC» = il codice paese ISO 3166-1 alpha-2 utilizzato nel campo «Scheme territory» (clausola 5.3.10),

— «:» = è utilizzato come separatore,

▼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

— La versione nella lingua nazionale di qualsiasi Stato membro DEVE essere costituita da una stringa di caratteri strutturata come segue:

CC:name_value

dove:

— «CC» = il codice di paese ISO 3166-1 alpha-2 utilizzato nel campo «Scheme territory» (clausola 5.3.10),

— «:» = è utilizzato come separatore,

— «name_value» = traduzione ufficiale nella lingua nazionale della stringa «EN_name_value». Per la lingua italiana: «l'elenco indicante lo status di supervisione/accreditamento dei servizi di certificazione dei CPS che sono soggetti alla supervisione/accreditamento dello Stato membro interessato, gestore del sistema, per verificarne la conformità con le pertinenti disposizioni della direttiva 1999/93/CE».

Il nome del sistema è obbligatorio per identificare univocamente il sistema riportato in «Scheme information URI» e anche per garantire che, qualora un gestore di sistema ne gestisca più di uno, ciascuno di essi abbia una denominazione distinta.

Gli Stati membri e i gestori del sistema DEVONO assicurarsi che, quando uno Stato membro o un gestore del sistema gestiscono più di un sistema, ciascun sistema abbia una denominazione distinta.

Scheme information URI (clausola 5.3.7)

Questo campo è OBBLIGATORIO e DEVE specificare il o gli URI in cui gli utilizzatori del certificato possono ottenere informazioni specifiche sul sistema (con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali). Si DEVE trattare di una sequenza di puntatori multilingui, con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali. Gli URI di riferimento DEVONO fornire un percorso verso le informazioni che forniscono «opportune informazioni sul sistema».

Le «opportune informazioni sul sistema» DEVONO includere come minimo:

— informazioni introduttive generali, comuni a tutti gli Stati membri, in relazione al campo di applicazione e al contesto dell'elenco di fiducia e al regime soggiacente di supervisione/accreditamento. Il testo comune da utilizzare è il seguente:

▼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, ecc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.»;

— informazioni specifiche sul regime soggiacente di supervisione/accreditamento, in particolare ([1]):

— informazioni sul sistema di supervisione applicabile a tutti i CSP_{QC},

([1]) Le ultime due serie di informazioni rivestono importanza cruciale per gli utilizzatori dei certificati, in quanto consentono loro di valutare la qualità e il livello di sicurezza dei sistemi di supervisione/accreditamento. Tali serie di informazioni sono fornite nell'elenco di fiducia utilizzando i seguenti campi: «Scheme information URI» (clausola 5.3.7 — informazioni fornite dagli Stati membri), «Scheme type/community/rules» (clausola 5.3.9 — mediante l'uso di un testo comune a tutti gli Stati membri) e «TSL policy/legal notice» (clausola 5.3.11 — un testo comune a tutti gli Stati membri con riferimento alla direttiva 1999/93/CE, con la possibilità per ciascuno Stato membro di aggiungere testi/riferimenti specifici per tale Stato membro). Informazioni supplementari sui sistemi nazionali di supervisione/accreditamento per i CSP che non rilasciano QC possono essere fornite a livello del servizio, se pertinente e richiesto (ad esempio per distinguere tra livelli diversi di qualità/sicurezza) mediante l'uso del campo «Scheme service definition URI» (clausola 5.5.6).

▼C1

— se pertinente, informazioni sul regime nazionale di accreditamento facoltativo applicabile a tutti i CSP_{QC},

— se pertinente, informazioni sul sistema di supervisione applicabile a tutti i CSP che non rilasciano QC,

— se pertinente, informazioni sul regime nazionale di accreditamento facoltativo applicabile a tutti i CSP che non rilasciano QC,

— per ciascuno dei regimi soggiacenti sopraelencati tali informazioni specifiche DEVONO includere quantomeno:

— una descrizione generale,

— informazioni sulla procedura seguita dall'organismo di supervisione/accreditamento per sottoporre a supervisione/accreditamento i CSP e da questi ultimi per sottoporsi a supervisione/accreditamento,

— informazioni sui criteri utilizzati per la supervisione/accreditamento dei CSP,

— se pertinente, informazioni dettagliate sulle «qualifiche» specifiche di cui alcuni degli oggetti fisici o binari (logici) generati o rilasciati a seguito della fornitura di un servizio di certificazione potrebbero beneficiare sulla base della loro conformità con le disposizioni e i requisiti nazionali, indicando il significato di tale «qualifica» e le disposizioni e i requisiti nazionali ad esse associati.

Ulteriori informazioni specifiche, a livello degli Stati membri, relative al sistema POSSONO essere fornite su base volontaria. Esse DEVONO comprendere:

— informazioni sui criteri e le norme per selezionare supervisori/revisori e sulle modalità con cui i CSP vengono da loro supervisionati (controllati) o accreditati (sottoposti a audit);

— altre informazioni generali e le coordinate di contatto connesse con la gestione del sistema.

Status determination approach (clausola 5.3.8)

Questo campo è OBBLIGATORIO e DEVE specificare l'identificativo della metodologia di determinazione dello status. A tal fine DEVE essere utilizzato il seguente URI specifico, registrato e descritto come segue:

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

Descrizione: per un dato Stato membro lo status dei servizi compresi nell'elenco è determinato da o per conto del gestore del sistema mediante un metodo adeguato che consenta la «supervisione» (e, se pertinente, l'«accreditamento facoltativo») dei prestatori di servizi di certificazione che sono stabiliti sul suo territorio (o in un paese terzo nel caso dell'«accreditamento facoltativo») e rilasciano certificati qualificati al pubblico conformemente all'articolo 3, paragrafo 3 [e rispettivamente articolo 3, paragrafo 2 o articolo 7, paragrafo 1, lettera a)] della direttiva 1999/93/CE e, se pertinente, che consenta la «supervisione»/«accreditamento facoltativo» dei prestatori di servizi di certificazione che non rilasciano certificati qualificati sulla base di un «regime di approvazione riconosciuto» definito e attuato su base nazionale ai fini del controllo della conformità dei servizi dei prestatori di servizi di certificazione con la direttiva 1999/93/CE ed eventualmente ampliato da disposizioni della normativa nazionale in relazione alla fornitura di tali servizi di certificazione.

▼C1

Scheme type/community/rules (clausola 5.3.9)

Questo campo è OBBLIGATORIO e DEVE contenere quantomeno i seguenti URI registrati:

— un URI comune a tutti gli elenchi di fiducia degli Stati membri per definire un testo esplicativo che DEVE essere applicabile a tutti i TL:

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

— che informa della partecipazione del sistema dello Stato membro [identificato mediante «TSL type» (clausola 5.3.3) e «Scheme name» (clausola 5.3.6)] a un sistema dei sistemi (ovvero un TSL indirizzato a tutti gli Stati membri che pubblicano e gestiscono un TL in forma di TSL),

— che informa gli utilizzatori delle politiche/norme in base alle quali i servizi inclusi nell'elenco DEVONO essere valutati e da cui può essere determinato il tipo di TSL (cfr. clausola 5.3.3),

— che fornisce agli utilizzatori una descrizione di come usare e interpretare il contenuto dell'applicazione TSL dell'elenco di fiducia. Tali norme d'uso DEVONO essere comuni a tutti gli elenchi di fiducia degli Stati membri, qualunque sia il tipo di servizio compreso nell'elenco e il regime o i regimi di supervisione/accreditamento.

Testo esplicativo:

«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 dicembre 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

— un URI comune a tutti gli elenchi di fiducia degli Stati membri per definire un testo descrittivo che DEVE essere applicabile a tutti i TL degli Stati membri interessati:

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

dove «CC» = il codice di paese ISO 3166-1 alpha-2 utilizzato nel campo «Scheme territory» (clausola 5.3.10),

— dove gli utilizzatori possono reperire informazioni sulle politiche/norme specifiche dello Stato membro in base alle quali i servizi inclusi nell'elenco DEVONO essere valutati conformemente al pertinente sistema di supervisione e regime di accreditamento volontario in vigore nello Stato membro,

— che fornisce agli utilizzatori una descrizione specifica di come usare e interpretare il contenuto dell'applicazione TSL dell'elenco di fiducia di uno Stato membro per quanto riguarda i servizi di certificazione non connessi con il rilascio di QC. Questo testo può essere utilizzato per indicare che in sistemi nazionali di supervisione/accreditamento possono applicare un diverso trattamento dei CSP che non rilasciano QC e il modo in cui i campi «Scheme service definition URI» (clausola 5.5.6) e «Service information extension» possono essere usati a tal fine.

Gli Stati membri POSSONO definire URI supplementari rispetto all'URI specifico per Stato membro di cui sopra (ovvero URI definiti a partire da tale URI gerarchico specifico).

Scheme territory (clausola 5.3.10)

Nell'ambito delle presenti specifiche questo campo è OBBLIGATORIO e DEVE indicare il paese in cui è in vigore il sistema (codice di paese ISO 3166-1 alpha-2).

TSL policy/legal notice (clausola 5.3.11)

Nell'ambito delle presenti specifiche questo campo è OBBLIGATORIO e DEVE indicare la politica del sistema o contenere un avviso relativo allo statuto giuridico del sistema o dei requisiti legali cui il sistema è conforme nella giurisdizione di pertinenza e/o eventuali vincoli e condizioni cui sono soggette la pubblicazione e la gestione del TL.

Si DEVE trattare di una stringa di caratteri multilingui (solo in formato testo) divisa in due parti:

— una prima parte obbligatoria comune a tutti i TL degli Stati membri (con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali), indicante che il quadro normativo applicabile è la direttiva 1999/93/CE e i corrispondenti atti di recepimento nelle legislazioni degli Stati membri indicati nel campo «Scheme Territory».

Versione inglese del testo comune:

«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.»,

Testo nella o nelle lingue ufficiali degli Stati membri: [traduzione ufficiale del testo in lingua inglese riportato sopra].

▼C1

«Il quadro normativo di riferimento per l'applicazione TSL dell'elenco di fiducia dei prestatori di servizi di certificazione per [nome dello Stato membro interessato] è la direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio relativa ad un quadro comunitario per le firme elettroniche e i corrispondenti atti di recepimento nella legislazione di [nome dello Stato membro interessato].»,

— una seconda parte facoltativa, specifica per ogni TL (con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali), indicante i riferimenti a specifici quadri normativi nazionali applicabili (in particolare, ad esempio, quando si riferiscono a regimi nazionali di supervisione/accreditamento di CSP che non rilasciano QC).

Historical information period (clausola 5.3.12)

Questo campo è OBBLIGATORIO e DEVE specificare il periodo di tempo (sotto forma di un numero intero) per il quale sono fornite le serie storiche di dati del TSL. Questo numero intero esprime un numero di giorni e nel contesto delle presenti specifiche DEVE essere superiore o pari a 3 653 (ossia l'applicazione TSL dei TL degli Stati membri contiene serie storiche di dati relative a un minimo di dieci anni). Valori più elevati devono tenere nel debito conto i requisiti giuridici in materia di conservazione dei dati nello Stato membro indicati nel «Scheme Territory» (clausola 5.3.10).

Pointers to other TSLs (clausola 5.3.13)

Nel contesto delle presenti specifiche questo campo è OBBLIGATORIO e DEVE comprendere, quando è disponibile, il puntatore verso un elenco, compilato dalla CE e conforme alla norma ETSI TS 102 231, di tutti i link (puntatori) relativi a tutte le applicazioni TSL degli elenchi di fiducia degli Stati membri. Le specifiche di ETSI TS 102 231, clausola 5.3.13, si applicano se viene reso obbligatorio l'utilizzo dell'identità digitale facoltativa, che rappresenta l'emittente del TSL indicato, nel formato specificato nella clausola 5.5.3.

Nota: in attesa dell'elenco, compilato dalla CE e conforme alla norma ETSI TS 102 231, dei link verso le applicazioni TSL dei TL degli Stati membri, questo campo NON DEVE essere utilizzato.

List issue date and time (clausola 5.3.14)

Questo campo è OBBLIGATORIO e DEVE indicare la data e l'ora (UTC espressa come ora Zulu) in cui il TSL è stato pubblicato utilizzando i valori della data e dell'ora come specificato in ETSI TS 102 231, clausola 5.1.4.

Next update (clausola 5.3.15)

Questo campo è OBBLIGATORIO e DEVE indicare la data e l'ora (UTC espressa come ora Zulu) di pubblicazione del prossimo TSL o essere nullo per indicare un TSL chiuso (utilizzando i valori della data e dell'ora come specificato in ETSI TS 102 231, clausola 5.1.4).

Qualora non si verifichi nessun cambiamento intermedio di status di un TSP o di un servizio coperto dal sistema, il TSL DEVE essere nuovamente pubblicato prima della data di scadenza dell'ultimo TSL.

Nel contesto delle presenti specifiche la differenza fra la data e l'ora del «Next update» e «List issue date and time» NON PUÒ essere superiore a **sei (6)** mesi.

▼C1

Distribution points (clausola 5.3.16)

Questo campo è FACOLTATIVO e, se utilizzato, DEVE specificare i luoghi in cui è pubblicata l'applicazione TSL attuale del TL e dove si possono reperire gli aggiornamenti del TSL attuale. Se sono indicati più punti di distribuzione, tutti DEVONO fornire copie identiche del TSL in corso o della sua versione aggiornata. Quando è utilizzato, questo campo è formattato come una sequenza non vuota di stringhe, ciascuna delle quali è conforme a RFC 3986 ([1]).

Scheme extensions (clausola 5.3.17)

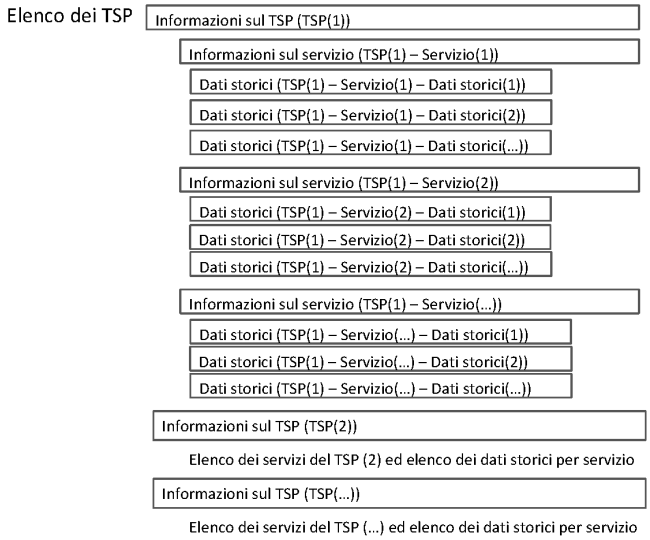
Questo campo è FACOLTATIVO e non è utilizzato nell'ambito della presente specifica.

List of Trust Service Providers

Questo campo è FACOLTATIVO.

Se nessuno dei CSP è o è stato soggetto a supervisione/accreditamento nel quadro del sistema in uno Stato membro, questo campo DEVE essere assente. È tuttavia convenuto che, anche quando in uno Stato membro non esiste un CSP soggetto a supervisione o accreditamento da parte del sistema, lo Stato membro DEVE applicare un TSL con questo campo assente. L'assenza di CSP nell'elenco DEVE significare che non esistono CSP soggetti a supervisione/accreditamento nel paese specificato nel «Scheme Territory».

Qualora uno o più servizi di CSP siano o siano stati soggetti a supervisione/accreditamento nell'ambito del sistema, il campo DEVE contenere una sequenza che identifichi ciascun CSP indicando uno o più di tali servizi soggetti a supervisione/accreditamento, con informazioni particolareggiate sullo status di soggetto a supervisione/accreditamento e sui dati storici dello status di ciascuno dei servizi del CSP (TSP = CSP nella figura seguente).



([1]) IETF RFC 3986: «Uniform Resource Identifiers (URI): Generic syntax».

▼C1

L'elenco dei TSP è organizzato come indicato nella figura che precede. A ciascun TSP corrisponde una sequenza di campi che contengono informazioni sul TSP («**TSP Information**»), seguita da un elenco dei servizi. Per ciascuno dei servizi l'elenco comporta una sequenza di campi contenenti informazioni sul servizio («Service Information») e una sequenza di campi contenenti informazioni sui dati storici dello status di approvazione del servizio («**Service approval history**»).

TSP Information

TSP(1)

T S P n a m e (clausola 5.4.1)

Questo campo è OBBLIGATORIO e DEVE specificare la denominazione dell'**entità giuridica** responsabile dei servizi del CSP che sono o sono stati soggetti a supervisione o accreditamento nell'ambito del sistema. Si tratta di una sequenza di stringhe di caratteri multilingui, con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali. La denominazione DEVE essere quella utilizzata negli atti ufficiali di registrazione e a cui sono inviate tutte le comunicazioni ufficiali.

T S P t r a d e n a m e (clausola 5.4.2)

Questo campo è FACOLTATIVO e, se presente, DEVE indicare una denominazione alternativa utilizzata dal CSP per identificarsi nel contesto specifico della prestazione di quei servizi che figurano nel presente TSL alla voce «TSP name» (clausola 5.4.1).

Nota: nel caso in cui un CSP costituito da un'unica entità giuridica presti servizi utilizzando denominazioni commerciali differenti o in contesti specifici diversi, vi potranno essere altrettante voci CSP quanti sono tali contesti specifici (ad esempio una voce per ogni nome/denominazione commerciale). In alternativa è possibile elencare ogni CSP (entità giuridica) solo una volta e fornire informazioni sul contesto specifico del servizio. Spetta al gestore del sistema dello Stato membro discutere e convenire con il CSP l'approccio più idoneo.

T S P a d d r e s s (clausola 5.4.3)

Questo campo è OBBLIGATORIO e DEVE contenere l'indirizzo dell'entità giuridica o dell'organizzazione designata identificata nel campo «TSP name» (clausola 5.4.1) per le comunicazioni postali e elettroniche. DEVE contenere sia «PostalAddress» (ossia nome e numero civico, località [stato o provincia], [codice postale] e il codice paese ISO 3166-1 alpha-2) conformemente alla clausola 5.3.5.1 che «ElectronicAddress» (ossia e-mail e/o sito web URI) conformemente alla clausola 5.3.5.2.

T S P i n f o r m a t i o n U R I (clausola 5.4.4)

Questo campo è OBBLIGATORIO e DEVE indicare l'URI quando gli utilizzatori (gli utilizzatori del certificato) possono ottenere informazioni specifiche sul CSP. Si DEVE trattare di una sequenza di puntatori multilingui, con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali. L'URI indicato DEVE fornire un percorso verso le informazioni che descrivono le condizioni generali dei servizi del CSP, le pratiche, gli aspetti giuridici, la politica in materia di assistenza ai clienti e le altre informazioni generali che si applicano a tutti i servizi elencati alla voce del CSP nel TSL.

Nota: se un CSP costituito da un'unica entità giuridica presta servizi con diverse denominazioni commerciali o in diversi contesti specifici e questi sono rappresentati da altrettante voci del TSP quanti sono tali contesti, il campo DEVE indicare informazioni relative all'insieme specifico di servizi menzionato in una determinata voce TSP/TradeName.

▼C1

TSP information extensions (clausola 5.4.5)

Questo campo è FACOLTATIVO e, se presente, PUÒ essere utilizzato dal gestore del sistema in conformità alle specifiche ETSI TS 102 231 (clausola 5.4.5) per fornire informazioni specifiche da interpretare secondo le norme del sistema specifico.

List of Services

Questo campo è OBBLIGATORIO e DEVE contenere una sequenza che identifica ciascuno dei servizi riconosciuti del CSP e lo status di approvazione di ciascuno di essi (inclusi i relativi dati storici). Deve figurare nel campo almeno un servizio (anche se le informazioni contenute sono puramente dati storici).

Dato che la conservazione dei dati storici relativi ai servizi elencati è OBBLIGATORIA nell'ambito delle presenti specifiche, detti dati storici DEVONO essere conservati anche se lo status attuale del servizio non richiederebbe di norma la sua inclusione nell'elenco (ad esempio il servizio non è più disponibile). Un CSP DEVE pertanto essere incluso, anche se il suo unico servizio figurante nell'elenco non è più attuale, al fine di conservare i dati storici.

Service Information

TSP(1) Service(1)

Service type identifier (clausola 5.5.1)

▼M1

Questo campo è OBBLIGATORIO e DEVE specificare l'identificativo del tipo di servizio conformemente alle presenti specifiche TSL (ossia «/eSigDir-1999-93-EC-TrustedList/TSLType/generic»).

▼C1

Quando il servizio elencato riguarda il rilascio di certificati qualificati, l'URI indicato DEVE essere http://uri.etsi.org/TrstSvc/Svctype/CA/QC (un'autorità di certificazione che rilascia certificati qualificati).

Quando il servizio elencato concerne il rilascio di gettoni di servizio di fiducia che non sono certificati qualificati (QC) e non riguarda il rilascio di QC, l'URI indicato DEVE essere uno degli URI inerente a tale campo definiti in ETSI 102 231 ed elencati nella clausola D.2. Questa norma DEVE essere applicata anche per i gettoni di servizio di fiducia che sono oggetto di supervisione/accreditamento con riguardo al rispetto di alcune qualifiche specifiche in conformità alle leggi nazionali degli Stati membri (ad esempio nel caso dei gettoni di orodatazione qualificati in Germania e in Ungheria), l'URI indicato DEVE essere uno degli URI inerente a tale campo definiti in ETSI 102 231 ed elencati nella relativa clausola D.2 (ad esempio TSA per gettoni di orodatazione qualificati definiti a livello nazionale). Se del caso, tale qualifica nazionale specifica dei gettoni di servizio di fiducia PUÒ essere indicata nella voce relativa al servizio e l'estensione additionalServiceInformation (clausola 5.8.2) nella clausola 5.5.9 («Service information extension») DEVE essere utilizzata a tale scopo.

▼C1

Come principio generalmente applicato, DEVE esistere una voce per ogni certificato X.509v3 (ad esempio per un servizio di certificazione di tipo CA/QC) dei servizi di certificazione figuranti nell'elenco di un CSP compreso nell'elenco di fiducia [ad esempio un'autorità di certificazione che rilascia (direttamente) QC]. In alcune circostanze accuratamente definite e gestite l'organismo di supervisione o di accreditamento di uno Stato membro PUÒ decidere di utilizzare il certificato X.509v3 di una CA radice o di livello superiore (ad esempio un'autorità di certificazione che non rilascia direttamente QC alle entità finali, ma che certifica una gerarchia di CA fino alle CA che rilasciano QC alle entità finali) come «Sdi» di una voce unica nell'elenco di servizi di un CSP che figura nell'elenco. Gli Stati membri devono valutare attentamente le conseguenze (vantaggi e svantaggi) dell'utilizzo di un tale certificato X.509v3 di una CA radice o di livello superiore come valore «Sdi» di servizi TL e farsene carico ([1]). Inoltre, quando ricorrono a una tale eccezione autorizzata al principio generale, gli Stati membri DEVONO fornire la documentazione necessaria a facilitare la costituzione e la verifica del percorso di certificazione.

Nota: i TSP quali i risponditori OCSP e gli emittenti di CRL che fanno parte dei servizi di certificazione CSP_{QC} e sono soggetti all'uso di coppie di chiavi separate per firmare, rispettivamente, risposte OCSP e CRL POSSONO figurare anche nel presente modello di TSL utilizzando la seguente combinazione di URI:

— valore «Service type identifier» (clausola 5.5.1):

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

combinato con il valore di estensione «Service information extension» (clausola 5.5.9) additionalServiceInformation extension (clausola 5.8.2) seguente:

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

Descrizione: un fornitore di status di certificazione che gestisce un server OCSP nell'ambito di un servizio di un CSP che rilascia certificati qualificati,

— valore «Service type identifier» (clausola 5.5.1):

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

combinato con il valore di estensione «Service information extension» (clausola 5.5.9) additionalServiceInformation extension (clausola 5.8.2) seguente:

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

Descrizione: un fornitore di status di certificazione che gestisce un CRL nell'ambito di un servizio di un CSP che rilascia certificati qualificati,

— valore «Service type identifier» (clausola 5.5.1):

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

([1]) L'utilizzo di un certificato X.509v3 di una CA radice come valore «Sdi» per un servizio elencato obbligherà il gestore del sistema a considerare l'insieme dei servizi di certificazione nell'ambito di tale CA radice come un tutto unico per quanto riguarda lo «status di supervisione/accreditamento». Ad esempio un cambiamento di status di un'unica CA figurante nell'elenco, nella gerarchia radice, comporterà lo stesso cambiamento di status per l'intera gerarchia.

▼C1

combinato con il valore di estensione «Service information extension» (clausola 5.5.9) additionalServiceInformation extension (clausola 5.8.2) seguente:

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

Descrizione: un'autorità di certificazione radice a partire dalla quale si può stabilire un percorso di certificazione fino a un'autorità di certificazione che rilascia certificati qualificati,

— valore «Service type identifier» (clausola 5.5.1):

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

combinato con il valore di estensione «Service information extension» (clausola 5.5.9) additionalServiceInformation extension (clausola 5.8.2) seguente:

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

Descrizione: un servizio di orodatazione facente parte di un servizio di un prestatario di un servizio di certificazione autorizzato a rilasciare certificati qualificati che rilascia TST, i quali possono essere utilizzati nel processo di verifica della firma qualificata per accertare e prorogare la validità della firma quando il QC è revocato o scaduto.

Service name (clausola 5.5.2)

Questo campo è OBBLIGATORIO e DEVE indicare la denominazione con la quale il CSP identificato in «TSP name» (clausola 5.4.1) presta il servizio specificato in «Service type identifier» (clausola 5.5.1). Si DEVE trattare di una sequenza di stringhe di caratteri multilingui, con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali.

Service digital identity (clausola 5.5.3)

Questo campo è OBBLIGATORIO e DEVE indicare almeno una rappresentazione di un identificativo digitale proprio del servizio il cui tipo è specificato in «Service type identifier» (clausola 5.5.1) grazie al quale il servizio può essere identificato senza ambiguità.

Nelle presenti specifiche l'identificativo digitale utilizzato in questo campo DEVE essere il certificato X.509v3 pertinente, poiché si tratta di una rappresentazione della/e chiave/i pubblica/che che il CSP utilizza per prestare il servizio il cui tipo è specificato dal «Service type identifier» (clausola 5.5.1) (ossia la chiave utilizzata da una RootCA/QC, la chiave utilizzata per firmare i certificati ([1]), o alternativamente per rilasciare i gettoni di orodatazione, firmare i CRL o firmare risposte OCSP). Questo certificato X.509v3 correlato DEVE essere utilizzato come identificativo digitale minimo richiesto (essendo la rappresentazione della/e chiave/i pubblica/che che il CSP utilizza per prestare il servizio elencato). Identificativi supplementari POSSONO essere utilizzati nel modo seguente, ma DEVONO tutti riferirsi alla stessa identità (ossia al certificato X.509v3 correlato):

([1]) Si può trattare del certificato di una CA che rilascia certificati di entità finale (ad esempio CA/PKC, CA/QC) o del certificato di una CA radice di fiducia a partire dalla quale si può tracciare un percorso fino ai certificati qualificati di entità finale. A seconda che tali informazioni e le informazioni reperibili nei certificati di entità finale rilasciati dalla radice di fiducia possano essere utilizzate per determinare senza ambiguità le caratteristiche appropriate di un determinato certificato qualificato, esse dovranno essere integrate da dati «Service information extensions» (cfr. clausola 5.5.9).

▼C1

a) la denominazione distinta (DN) del certificato che può essere utilizzata per verificare le firme elettroniche del servizio CSP specificato in «Service type identifier» (clausola 5.5.1);

b) l'identificativo di chiave pubblica correlato (ossia (i.e. X.509v3 SubjectKeyIdentifier o il valore SKI);

c) la chiave pubblica correlata.

Come principio generalmente applicato, l'identificativo digitale (il certificato X.509v3 correlato) NON PUÒ ricorrere più di una volta nell'elenco di fiducia, ossia DEVE esistere una singola voce per ogni certificato X.509v3 per un servizio di certificazione compreso nei servizi figuranti nell'elenco di un CSP compreso nell'elenco di fiducia. Al contrario, un unico certificato X.509v3 DEVE essere utilizzato in una voce di servizio unica come valore «Sdi».

Nota 1: l'unico caso in cui il principio generale di cui sopra può non essere applicato è quello in cui un unico certificato X.509v3 è utilizzato per il rilascio di diversi tipi di gettoni di servizio di fiducia per i quali si applicano diversi regimi di supervisione/accreditamento, ad esempio un unico certificato X.509v3 è utilizzato da un CSP, da un lato, per il rilascio di QC nell'ambito di un sistema di supervisione adeguato e, dall'altro, per il rilascio di certificati non qualificati nell'ambito di uno status diverso di supervisione/accreditamento. In questo caso e nell'esempio citato si utilizzerebbero due voci con valori «Sti» diversi (ossia rispettivamente CA/QC e CA/PKC nell'esempio citato) e con lo stesso valore «Sdi».

Le applicazioni sono dipendenti da ASN.1 o XML e DEVONO essere conformi alle specifiche ETSI TS 102 231 (per ASN.1 si veda l'allegato A di ETSI TS 102 231 e per XML si veda l'allegato B di ETSI TS 102 231).

Nota 2: se è necessario fornire informazioni di «qualificazione» complementari per quanto riguarda la voce del servizio specificato, il gestore del sistema DEVE, ove opportuno, considerare l'utilizzazione dell'estensione «additionalServiceInformation» (clausola 5.8.2) del campo «Service information extension» (clausola 5.5.9) in funzione dello scopo perseguito nel fornire tali informazioni di «qualificazione» complementari. Inoltre il gestore del sistema può, in via facoltativa, utilizzare la clausola 5.5.6 («Scheme service definition URI»).

Service current status (clausola 5.5.4)

Questo campo è OBBLIGATORIO e DEVE specificare l'identificativo dello status del servizio tramite uno dei seguenti URI:

▼C2

— **Under Supervision (Soggetto a supervisione)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision),

— **Supervision of Service in Cessation (Supervisione del servizio in fase di sospensione)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation),

— **Supervision Ceased (Supervisione sospesa)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased),

— **Supervision Revoked (Supervisione revocata)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked),

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

— **Accreditation Ceased (Accreditamento sospeso)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased),

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

▼C1

Gli status di cui sopra DEVONO essere interpretati come segue nel contesto delle presenti specifiche dell'elenco di fiducia:

— ***Soggetto a supervisione:*** il servizio specificato in «Service digital identity» (clausola 5.5.3) fornito dal prestatore di servizi di certificazione (CSP) identificato in «TSP name» (clausola 5.4.1) è attualmente soggetto alla supervisione dello Stato membro indicato in «Scheme territory» (clausola 5.3.10) in cui il CSP è stabilito per verificare il rispetto delle disposizioni della direttiva 1999/93/CE.

▼M1

— ***Supervisione del servizio in fase di sospensione:*** il servizio specificato in «Service digital identity» (clausola 5.5.3) prestato dal prestatore di servizi di certificazione identificato in «TSP name» (clausola 5.4.1) è attualmente in fase di sospensione, ma è ancora oggetto di supervisione fino alla cessazione o alla revoca della stessa. Qualora una persona giuridica diversa da quella indicata in «TSP name» si sia assunta la responsabilità di garantire la fase di sospensione, l'identificazione di tale persona giuridica nuova o di riserva (prestatore di servizi di certificazione di riserva) deve essere fornita nello «Scheme service definition URI» (clausola 5.5.6) e nell'estensione «TakenOverBy» (clausola L.3.2) della voce del servizio.

▼C1

— ***Supervisione sospesa:*** la validità della valutazione di supervisione è scaduta senza che il servizio specificato in «Service digital identity» (clausola 5.5.3) sia stato rivalutato. Attualmente il servizio non è più soggetto a supervisione (a partire dalla data dello status attuale) in quanto si considera che abbia cessato di essere operativo.

— ***Supervisione revocata:*** dopo essere stato soggetto a supervisione, il servizio del CSP e potenzialmente il CSP stesso non hanno più rispettato le disposizioni della direttiva 1999/93/CE, determinate dallo Stato membro specificato nel «Scheme territory» (clausola 5.3.10) in cui il CSP è stabilito. Il servizio è stato pertanto invitato a cessare le sue attività e deve essere considerato sospeso per il motivo sopramenzionato.

Nota 1: Lo status «Supervisione revocata» può avere valore definitivo, anche se il CSP ha completamente cessato la sua attività; in tal caso non è necessario passare allo status «Supervisione del servizio in fase di cessazione» o «Supervisione sospesa». In effetti l'unico modo per cambiare lo status «Supervisione revocata» è ripristinare il rispetto delle disposizioni stabilite nella direttiva 1999/93/CE conformemente al sistema di supervisione adeguato in vigore nello Stato membro che possiede il TL e recuperare lo status «Soggetto a supervisione». Gli status «Supervisione del servizio in fase di sospensione» o «Supervisione sospesa» sono attribuiti solo quando un CSP cessa esso stesso di fornire i servizi soggetti a supervisione, e non quando la supervisione è stata revocata.

— ***Accreditato:*** una valutazione di accreditamento è stata effettuata dall'organismo di accreditamento per conto dello Stato membro specificato nello «Scheme territory» (clausola 5.3.10) e il servizio identificato in «Service digital identity» (clausola 5.5.3) prestato dal CSP ([1]) identificato in «TSP name» (clausola 5.4.1) risulta rispettare le disposizioni della direttiva 1999/93/CE.

([1]) Va osservato che questo CSP accreditato può essere stabilito in uno Stato membro diverso da quello identificato nello «Scheme territory» dell'applicazione TSL della TL o in un paese terzo [cfr. articolo 7, paragrafo 1, lettera a), della direttiva 1999/93/CE].

▼C1

Nota 2: quando sono utilizzati nel contesto di un CSP che rilascia QC stabilito nel «Scheme territory» (clausola 5.3.10), i due status «Accreditamento revocato» e «Accreditamento sospeso» DEVONO essere considerati «status temporanei» e non DEVONO essere utilizzati come valori per «Service current status» dal momento che, se sono utilizzati, DEVONO essere immediatamente seguiti nel «Service approval history» o nel «Service current status» da uno status «Soggetto a supervisione», potenzialmente seguito da uno qualsiasi degli altri status di supervisione sopra definiti, come illustrato nella figura 1. Quando sono utilizzati nel contesto di un CSP che non rilascia QC, quando esiste un solo sistema di «accreditamento facoltativo» associato senza alcun sistema di supervisione associato, o nel contesto di un CSP che rilascia QC, ma non è stabilito nello «Scheme territory» (clausola 5.3.10) (ad esempio in un paese terzo), gli status di «Accreditamento revocato» e «Accreditamento sospeso» POSSONO essere utilizzati come valore per «Service current status»:

— ***Accreditamento sospeso:*** la validità della valutazione di accreditamento è scaduta senza che il servizio specificato in «Service digital identity» (clausola 5.5.3) sia stato rivalutato.

— ***Accreditamento revocato:*** dopo essere stato riconosciuto conforme ai criteri del sistema, il servizio specificato in «Service digital identity» (clausola 5.5.3), fornito dal prestatore di servizi di certificazione (CSP) indicato in «TSP name» (clausola 5.4.1), e potenzialmente lo stesso CSP hanno cessato di rispettare le disposizioni della direttiva 1999/93/CE.

Nota 3: Occorre utilizzare esattamente gli stessi valori di status per i CSP che rilasciano QC e per quelli che non rilasciano QC (ad esempio prestatori di servizi di orodatazione che rilasciano TST, CSP che rilasciano certificati non qualificati, ecc.). Il «Service Type identifier» (clausola 5.5.1) deve essere utilizzato per distinguere fra sistemi di supervisione/accreditamento applicabili.

Nota 4: Informazioni complementari «di qualificazione» correlate allo status e definite a livello dei sistemi nazionali di supervisione/accreditamento per i CSP che non rilasciano QC POSSONO essere fornite a livello del servizio quando ciò sia pertinente e richiesto (ad esempio per distinguere fra diversi livelli di qualità o sicurezza). I gestori del sistema DEVONO utilizzare l'estensione «additionalServiceInformation» (clausola 5.8.2) del campo «Service information extension» (clausola 5.5.9) in funzione dell'obiettivo perseguito nel fornire tali informazioni complementari «qualificate». Inoltre il gestore del sistema può, in via facoltativa, utilizzare la clausola 5.5.6 («Scheme service definition URI»).

Current status starting date and time (clausola 5.5.5)

Questo campo è OBBLIGATORIO e DEVE indicare la data e l'ora in cui lo status di approvazione in corso è entrato in vigore (data e ora come specificate in ETSI TS 102 231, clausola 5.1.4).

Scheme service definition URI (clausola 5.5.6)

Questo campo è FACOLTATIVO e, se presente, DEVE specificare gli URI quando gli utilizzatori del certificato possono ottenere informazioni specifiche sul servizio fornite dal gestore del sistema sotto forma di sequenza di puntatori multilingui, con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali.

Quando sono utilizzati, gli URI di riferimento DEVONO fornire un percorso verso le informazioni che descrivono il servizio come specificato dal sistema. Si PUÒ in particolare trattare degli elementi seguenti, se pertinenti:

a) un URI che indica l'identità del CSP di riserva nel caso della supervisione di un servizio in fase di sospensione in cui è coinvolto un CSP di riserva (si veda «Service current status» — clausola 5.5.4);

▼C1

b) un URI che conduce a documenti che forniscono informazioni complementari sull'utilizzo di una qualifica specifica definita a livello nazionale per un servizio soggetto a supervisione/accreditamento che fornisce gettoni di servizio di fiducia coerente con l'utilizzo del campo «Service information extension» (clausola 5.5.9) con un'estensione «additionalServiceInformation» definita nella clausola 5.8.2.

Service supply points (clausola 5.5.7)

Questo campo è FACOLTATIVO e, se presente, DEVE specificare gli URI quando gli utilizzatori del certificato possono aver accesso al servizio mediante una sequenza di stringhe di caratteri la cui sintassi DEVE essere conforme a RFC 3986.

TSP service definition URI (clausola 5.5.8)

Questo campo è FACOLTATIVO e, se presente, DEVE specificare gli URI quando gli utilizzatori del certificato possono ottenere informazioni specifiche sul servizio fornite dal TSP sotto forma di sequenza di puntatori multilingui, con l'inglese (EN) come lingua obbligatoria e eventualmente una o più lingue nazionali. Gli URI di riferimento DEVONO fornire un percorso verso le informazioni che descrivono il servizio come specificato dal TSP.

Service information extensions (clausola 5.5.9)

Nel contesto delle presenti specifiche questo campo è FACOLTATIVO, ma DEVE essere presente quando le informazioni fornite nel «Service digital identity» (clausola 5.5.3) non sono sufficienti per identificare senza ambiguità i certificati qualificati rilasciati da questo servizio e/o le informazioni presenti nei certificati qualificati corrispondenti non consentono di determinare mediante macchina se il QC è basato su un SSCD ([1]).

Nel contesto delle presenti specifiche, quando il suo uso è NECESSARIO, ad esempio per servizi CA/QC, un campo di informazione facoltativo «Service information extensions» («Sie») DEVE essere utilizzato e strutturato, conformemente all'estensione «Qualifiche» definita in ETSI TS 102 231, allegato L.3.1, sotto forma di una sequenza di una o più tuple, ciascuna delle quali fornisce:

— le informazioni da utilizzare per identificare più precisamente (filtri), nell'ambito del servizio di certificazione identificato «Sdi», il servizio specifico (ossia l'insieme di certificati qualificati) per il quale informazioni supplementari sono richieste/fornite con riguardo alla presenza o all'assenza di un supporto SSCD (e/o al rilascio a una persona giuridica), e

— le informazioni associate («qualifiers») indicanti se questo insieme di certificati qualificati identificato più precisamente è basato su un SSCD o no [quando queste informazioni sono «QCSSCDStatusAsInCert» significa che le informazioni associate fanno parte del QC in una forma standardizzata leggibile a macchina ([2])] e/o informazioni riguardanti il rilascio di tali QC a persone giuridiche (si considera di norma che siano rilasciati unicamente a persone fisiche),

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) significa che il CSP garantisce e lo Stato membro supervisiona (modello di supervisione) o verifica mediante audit (modello di accreditamento), rispettivamente mediante l'organismo di supervisione o di accreditamento, che un QC rilasciato nell'ambito del servizio (QCA) identificato in «Service digital identity» (clausola 5.5.3) e identificato più precisamente dalle informazioni sopramenzionate (filtri) utilizzate per indicare, nell'ambito del servizio di certificazione identificato «Sdi», l'insieme preciso di certificati qualificati per i quali tali informazioni supplementari sono richieste con riguardo alla presenza o all'assenza di un supporto SSCD **SIA** basato su un SSCD (ossia che la chiave privata associata alla chiave pubblica nel certificato è conservata in un dispositivo per la creazione di una firma sicura conforme all'allegato III della direttiva 1999/93/CE),

([1]) Cfr. la sezione 2.2 del presente documento.

([2]) Questo si riferisce a una combinazione appropriata di dichiarazione di conformità Qc definita dall'ETSI, dichiarazioni QcSSCD [ETSI TS 101 862] o di un QCP/QCP + OID definito dall'ETSI [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) significa che il CSP garantisce e lo Stato membro supervisiona (modello di supervisione) o verifica mediante audit (modello di accreditamento), rispettivamente mediante l'organismo di supervisione o di accreditamento, che un QC rilasciato nell'ambito del servizio (RootCA/QC o CA/QC) identificato in «Service digital identity» (clausola 5.5.3) e identificato più precisamente dalle informazioni sopramenzionate (filtri) utilizzate per indicare, nell'ambito del servizio di certificazione identificato «Sdi», l'insieme preciso di certificati qualificati per i quali tali informazioni supplementari sono richieste con riguardo alla presenza o all'assenza di un supporto SSCD **NON SIA** basato su un SSCD (ossia che la chiave privata associata alla chiave pubblica nel certificato non è conservata in un dispositivo per la creazione di una firma sicura conforme all'allegato III della direttiva 1999/93/CE),

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) significa che il CSP garantisce e lo Stato membro supervisiona (modello di supervisione) o verifica mediante audit (modello di accreditamento), rispettivamente mediante l'organismo di supervisione o di accreditamento, che un QC rilasciato nell'ambito del servizio (CA/QC) identificato in «Service digital identity» (clausola 5.5.3) e identificato più precisamente dalle informazioni sopramenzionate (filtri) utilizzate per indicare, nell'ambito del servizio di certificazione identificato «Sdi», l'insieme preciso di certificati qualificati per i quali tali informazioni supplementari sono richieste con riguardo alla presenza o all'assenza di un supporto SSCD DEBBA contenere le informazioni leggibili a macchina che precisano se il QC è basato su un SSCD o no,

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) significa che il CSP garantisce e lo Stato membro supervisiona (modello di supervisione) o verifica mediante audit (modello di accreditamento), rispettivamente mediante l'organismo di supervisione o di accreditamento, che un QC rilasciato nell'ambito del servizio (QCA) identificato in «Service digital identity» (clausola 5.5.3) e identificato più precisamente dalle informazioni sopramenzionate (filtri) utilizzate per indicare, nell'ambito del servizio di certificazione identificato «Sdi», l'insieme preciso di certificati qualificati per i quali tali informazioni supplementari sono richieste con riguardo al rilascio a persone giuridiche **SIA** rilasciato a persone giuridiche.

Questi «qualifiers» devono essere utilizzati solo come estensione se il tipo di servizio è http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Questo campo è specifico all'applicazione (ASN.1 o XML) e DEVE essere conforme alle specifiche previste in ETSI TS 102 231, allegato L.3.1.

▼M1

Nel contesto di un'applicazione XML, il contenuto specifico di tali informazioni supplementari deve essere codificato utilizzando i file xsd forniti nell'allegato C di ETSI TS 102 231.

▼C1

Service Approval History

Questo campo è FACOLTATIVO, ma DEVE essere presente se «Historical information period» (clausola 5.3.12) è diverso da zero. Pertanto, nel contesto delle presenti specifiche, il sistema DEVE conservare i dati storici. Nel caso in cui si intenda conservare i dati storici, ma il servizio non disponga di dati storici anteriori al suo status attuale (ossia si tratta del primo status registrato oppure il gestore del sistema non ha conservato i dati storici), questo campo DEVE essere vuoto. Diversamente, per ciascun cambiamento nello status attuale del servizio TSP intervenuto nel corso del periodo coperto dai dati storici specificato in ETSI TS 102 231, clausola 5.3.12, le informazioni sullo status di approvazione precedente DEVONO essere fornite in ordine cronologico decrescente di data e ora del cambiamento di status (ossia la data e l'ora in cui lo status di approvazione successivo è entrato in vigore).

▼C1

Si DEVE trattare di una sequenza di dati storici quale definita di seguito.

TSP(1) Service(1) History(1)

Service type identifier (clausola 5.6.1)

Questo campo è OBBLIGATORIO e DEVE specificare l'identificativo del tipo di servizio, con il formato e il significato utilizzati in «TSP Service Information — Service type identifier» (clausola 5.5.1).

Service name (clausola 5.6.2)

Questo campo è OBBLIGATORIO e DEVE indicare la denominazione con la quale il CSP ha prestato il servizio identificato in «TSP Service Information — Service type identifier» (clausola 5.5.1), con il formato e il significato utilizzati in «TSP Service Information — Service name» (clausola 5.5.2). Questa clausola non richiede che la denominazione sia la stessa di quella specificata nella clausola 5.5.2. Un cambiamento di denominazione PUÒ essere una delle circostanze che richiede un cambiamento di status.

▼M1

Service digital identity(clausola 5.6.3)

Questo campo è OBBLIGATORIO e DEVE specificare almeno una rappresentazione dell'identificativo digitale (ovvero il certificato X.509v3) usato in «TSP Service Information — Service digital identity» (clausola 5.5.3) con lo stesso formato e significato definito in ETSI TS 102 231, clausola 5.5.3.

Nota: per il valore di un certificato X.509v3 usato nella clausola 5.5.3 «Sdi» di un servizio, in un elenco di fiducia deve figurare un'unica voce di servizio per un valore «Sti:Sie/additionalServiceInformation». Le informazioni «Sdi» (clausola 5.6.3) usate nelle informazioni relative ai dati storici di approvazione del servizio associate alla voce del servizio e le informazioni «Sdi» (clausola 5.5.3) usate alla voce del servizio DEVONO far riferimento allo stesso valore del certificato X.509v3. Qualora un servizio elencato modifichi il suo «Sdi» (ossia rinnovi o ricodifichi un certificato X.509v3, ad esempio per un CA/PKC o un CA/QC) o crei un nuovo «Sdi» per tale servizio, anche con valori identici per i relativi «Sti», «Sn» e [«Sie»], il gestore del sistema DOVRÀ creare una voce di servizio diversa dalla precedente.

▼C1

Service previous status (clausola 5.6.4)

Questo campo è OBBLIGATORIO e DEVE specificare l'identificativo dello status precedente del servizio, con il formato e il significato utilizzati in «TSP Service Information — Service current status» (clausola 5.5.4).

Previous status starting date and time (clausola 5.6.5)

Questo campo è OBBLIGATORIO e DEVE specificare la data e l'ora in cui lo status precedente in questione è entrato in vigore, con il formato e il significato utilizzati in «TSP Service Information — Service current status starting date and time» (clausola 5.5.5).

Service information extensions (clausola 5.6.6)

Questo campo è FACOLTATIVO e PUÒ essere utilizzato dai gestori del sistema per fornire informazioni specifiche inerenti al servizio, con il formato e il significato utilizzati in «TSP Service Information — Service information extensions» (clausola 5.5.9).

▼C1

TSP(1) Service(1) History(2)

Idem per TSP(1) Service(1) History(2) (precedente a History 1)

…

TSP(1) Service(2)

Idem per TSP(1) Service 2 (se del caso)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Idem per TSP 2 (se del caso)

Idem per TSP 2 Service 1

Idem per TSP 2 Service 1 History 1

…

▼M1

Signed TSL

L'attuazione TSL leggibile all'uomo dell'elenco di fiducia, stabilita nell'ambito delle presenti specifiche e, in particolare, del capitolo IV, DOVREBBE essere firmata, perché ne sia garantita l'autenticità e l'integrità ([1]), dallo «Scheme operator name» (clausola 5.3.4). La firma DOVREBBE essere in formato PAdES parte 3 [ETSI TS 102 778-3 ([2])], ma PUÒ essere in formato PAdES parte 2 [ETSI TS 102 778-2 ([3])] nel quadro del modello di fiducia specifico stabilito attraverso la pubblicazione dei certificati usati per firmare gli elenchi di fiducia.

L'attuazione TSL leggibile a macchina dell'elenco di fiducia, stabilita nell'ambito delle presenti specifiche, DEVE essere firmata, perché ne sia garantita l'autenticità e l'integrità, dallo «Scheme operator name» (clausola 5.3.4). L'attuazione TSL leggibile a macchina dell'elenco di fiducia, stabilita nell'ambito delle presenti specifiche, DEVE essere in formato XML e DEVE esser conforme alle specifiche stabilite negli allegati B e C di ETSI TS 102 231.

La firma DEVE essere in formato XAdES BES o EPES, quale definito nelle specifiche ETSI TS 101 903 per le applicazioni XML. Tali applicazioni della firma elettronica DEVONO soddisfare i requisiti indicati nell'allegato B di ETSI TS 102 231 ([4]). I requisiti generali supplementari relativi a tale firma sono indicati nelle sezioni seguenti.

▼C1

Scheme identification (clausola 5.7.2)

Questo campo è OBBLIGATORIO e DEVE specificare un riferimento assegnato dal gestore del sistema che identifichi in modo univoco il sistema descritto nelle presenti specifiche e il TSL stabilito e DEVE essere incluso nel calcolo della firma. Si dovrebbe trattare di una stringa di caratteri o di una stringa di bits.

([1]) In caso l'attuazione TSL leggibile all'uomo dell'elenco di fiducia non fosse firmata, la sua autenticità ed integrità DEVONO essere garantite da un canale di comunicazione adeguato dotato di un livello di sicurezza equivalente. Si raccomanda a tal fine l'uso del TLS (IETF RFC 5246: «The Transport Layer Security (TLS) Protocol, versione 1.2»). Lo Stato membro deve dare agli utenti TLS un accesso fuori banda all'impronta del certificato del canale TLS.

([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]) È obbligatorio proteggere il gestore del sistema che firma il certificato utilizzando uno dei modi specificati in ETSI TS 101 903 e, se pertinente, il ds:keyInfo dovrebbe contenere il percorso del certificato corrispondente.

▼M1

Nel contesto delle presenti specifiche il riferimento assegnato DEVE includere il «TSL type» (clausola 5.3.3), lo «Scheme name» (clausola 5.3.6) e il valore dell'estensione SubjectKeyIdentifier del certificato utilizzato dal gestore del sistema per firmare elettronicamente la TSL.

▼C1

Signature algorithm identifier (clausola 5.7.3)

Questo campo è OBBLIGATORIO e DEVE specificare l'algoritmo crittografico che è stato impiegato per creare la firma. In funzione dell'algoritmo utilizzato, questo campo PUÒ richiedere parametri aggiuntivi. Questo campo DEVE essere incluso nel calcolo della firma.

Signature value (clausola 5.7.4)

Questo campo è OBBLIGATORIO e DEVE contenere il valore reale della firma digitale. Tutti i campi del TSL (tranne il valore stesso della firma) DEVONO essere inclusi nel calcolo della firma.

TSL extensions (clausola 5.8)

Estensione **expiredCertsRevocationInfo** (clausola 5.8.1)

Questa estensione è FACOLTATIVA e, se utilizzata, DEVE rispettare le specifiche di ETSI TS 102 231, clausola 5.8.1.

Estensione **additionalServiceInformation** (clausola 5.8.2)

Questa estensione FACOLTATIVA, se impiegata, DEVE essere utilizzata solo a livello del servizio e solo nel campo definito nella clausola 5.5.9 («Service information extension»). È utilizzata per fornire informazioni supplementari su un servizio. DEVE essere una sequenza di una o più tuple, ciascuna delle quali fornisce:

a) un URI che identifica le informazioni supplementari, ad esempio:

   — un URI che indica una qualifica specifica definita a livello nazionale per un servizio soggetto a supervisione/accreditamento che fornisce gettoni di servizio di fiducia, ad esempio:

      — un livello di articolazione sicurezza/qualità specifico con riguardo al sistema nazionale di supervisione/accreditamento per i CSP che non rilasciano QC (ad esempio RGS */**/*** in Francia, uno status di supervisione particolare stabilito dalla normativa nazionale per CSP specifici che rilasciano QC in Germania), cfr. la nota 4 di «Service current status» — clausola 5.5.4,

      — o uno status giuridico specifico per un servizio soggetto a supervisione/accreditamento che fornisce gettoni di servizio di fiducia (ad esempio «TST qualificati» definiti a livello nazionale come in Germania o Ungheria),

      — o il significato di un identificativo strategico specifico presente in un certificato X.509v3 fornito nel campo «Sdi»,

   — o un URI registrato come specificato nel «Service type identifier», clausola 5.5.1, per precisare la partecipazione del servizio identificato «Sti» in quanto servizio componente di un prestatore di servizio di certificazione che rilascia QC (ad esempio OCSP-QC, CRL-QC e RootCA-QC);

b) una stringa facoltativa contenente il valore serviceInformation, il cui significato è specificato nel sistema (ad esempio *, ** o ***);

c) eventuali informazioni supplementari facoltative fornite in un formato specifico al sistema.

▼**M1**

La dereferenziazione dell'URI DOVREBBE portare ad informazioni leggibili all'uomo (come minimo in inglese ed eventualmente in una o più lingue nazionali) ritenute necessarie e sufficienti per consentire agli utilizzatori del certificato di comprendere l'estensione e, in particolare, che spieghino il significato degli URI indicati, specificando i valori possibili per serviceInformation e il significato di ciascun valore.

Qualifications Extension (clausola L.3.1)

Descrizione: questo campo è FACOLTATIVO, ma DEVE essere presente quando il suo utilizzo è OBBLIGATORIO, ad esempio per i servizi RootCA/QC o CA/QC e quando:

— le informazioni fornite nel «Service digital identity» non sono sufficienti per identificare senza ambiguità i certificati qualificati rilasciati da tale servizio,

— le informazioni presenti nei certificati qualificati corrispondenti non consentono di determinare mediante macchina se il QC è basato o meno su un SSCD.

Quando è impiegata, questa estensione a livello del servizio DEVE essere utilizzata solo nel campo definito in «Service information extension» (clausola 5.5.9) e DEVE essere conforme alle specifiche di cui all'allegato L.3.1 di ETSI TS 102 231.

TakenOverBy Extension (clausola L.3.2)

Descrizione: detta estensione è FACOLTATIVA ma DEVE essere presente quando un servizio, precedentemente soggetto alla responsabilità giuridica di un CSP, è ripreso da un altro TSP ed è inteso ad indicare formalmente la responsabilità giuridica di un servizio e a permettere al software di verifica di svelare all'utente alcune informazioni di carattere giuridico. Le informazioni fornite con tale estensione DEVONO essere compatibili con il relativo uso della clausola 5.5.6 e DEVONO essere conformi alle specifiche dell'allegato L.3.2 di ETSI TS 102 231.

▼**M1**

CAPITOLO II

Nell'elaborare i loro elenchi di fiducia, gli Stati membri useranno:

i codici per le lingue in minuscolo e quelli per i paesi in maiuscolo;

i codici per le lingue e per i paesi in conformità con la tabella fornita di seguito.

Qualora sia presente una grafia in caratteri latini (e il suo relativo codice per la lingua) sarà aggiunta una traslitterazione in caratteri latini accompagnata dal relativo codice per la lingua, come specificato nella tabella sottostante.

Denominazione abbreviata (nella lingua originale)	Denominazione abbreviata (in inglese)	Codice paese	Codice lingua	Note	Traslitterazione in carratteri latini
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	Codice paese raccomandato dall'UE	el-Latn
España	Spain	ES	es	anche catalano (ca), basco (eu), galiziano (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**

Denominazione abbreviata (nella lingua originale)	Denominazione abbreviata (in inglese)	Codice paese	Codice lingua	Note	Traslitterazione in carratteri latini
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Codice paese raccomandato dall'UE	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Traslitterazione in alfabeto latino: България = Bulgaria; Ελλάδα = Elláda (Grecia); Κύπρος = Kýpros (Cipro).

———————

▼C1

CAPITOLO IV

SPECIFICHE PER LA FORMA LEGGIBILE ALL'UOMO DELL'APPLICAZIONE TSL DELL'ELENCO DI FIDUCIA

Una forma leggibile all'uomo (HR — Human Readable) dell'applicazione TSL dell'elenco di fiducia DEVE essere messa a disposizione del pubblico ed essere accessibile per via elettronica. DOVREBBE essere fornita sotto forma di un documento PDF (Portable Document Format) conforme a ISO 32000 che DEVE essere formattato conformemente al profilo PDF/A (ISO 19005).

Il contenuto della forma HR basata sul PDF/A dell'applicazione TSL dell'elenco di fiducia DOVREBBE soddisfare i seguenti requisiti:

▼M1

— il titolo degli elenchi di fiducia in formato leggibile all'uomo sarà costituito dalla concatenazione dei seguenti elementi:

  — immagine facoltativa della bandiera nazionale dello Stato membro,

  — spazio vuoto,

  — denominazione abbreviata del paese nella lingua/nelle lingue d'origine (in conformità a quanto disposto nella prima colonna della tabella al capitolo II),

  — spazio vuoto,

  — «(»,

  — denominazione abbreviata del paese in inglese (in conformità a quanto disposto nella prima colonna della tabella al capitolo II) posto tra parentesi,

  — «):» usato per chiudere la parentesi e come separatore,

  — spazio vuoto,

  — «elenco di fiducia»,

  — logo facoltativo del gestore del sistema dello Stato membro,

▼C1

— la struttura della forma HR DOVREBBE riflettere il modello logico descritto nella sezione 5.1.2 di ETSI TS 102 231,

— ogni campo presente DOVREBBE essere visibile e indicare:

  — il titolo del campo (ad esempio «Service type identifier»),

  — il valore del campo (ad esempio «CA/QC»),

  — il significato (la descrizione) del valore del campo, se del caso, e in particolare come previsto nell'allegato D di ETSI TS 102 231 o nelle presenti specifiche per gli URI registrati (ad esempio «un'autorità di certificazione che rilascia certificati a chiave pubblica»),

  — se del caso, più versioni in lingue naturali come previsto nell'applicazione TSL dell'elenco di fiducia,

— i campi seguenti e i corrispondenti valori dei certificati digitali presenti nel campo «Service digital identity» DOVREBBERO essere quantomeno presenti nella forma HR:

  — versione,

  — numero di serie,

  — algoritmo di firma,

  — emittente,

  — valido da,

  — valido fino a,

  — soggetto,

▼C1

— chiave pubblica,

— politiche di certificazione,

— identificativo della chiave del soggetto,

— punti di distribuzione CRL,

— identificativo della chiave dell'autorità,

— utilizzazione della chiave,

— restrizioni di base,

— algoritmo dell'impronta digitale,

— impronta digitale,

— la forma HR DOVREBBE essere facile da stampare,

— la forma HR PUÒ essere firmata elettronicamente. In tal caso DEVE essere firmata dal gestore del sistema secondo le stesse specifiche relative alla firma valide per l'applicazione TSL dell'elenco di fiducia.