DECISIONE DI ESECUZIONE DELLA COMMISSIONE

del 14 ottobre 2013

che modifica la decisione 2009/767/CE per quanto riguarda l'elaborazione, l'aggiornamento e la pubblicazione degli elenchi di fiducia dei prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte degli Stati membri

[notificata con il numero C(2013) 6543]

(Testo rilevante ai fini del SEE)

(2013/662/UE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione 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) La decisione 2009/767/CE 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 ([2]), obbliga gli Stati membri a mettere a disposizione le informazioni necessarie per la convalida delle firme elettroniche avanzate basate su un certificato qualificato. Le informazioni devono essere presentate in maniera uniforme utilizzando i cosiddetti «elenchi di fiducia» contenenti le informazioni relative ai prestatori di servizi di certificazione che rilasciano al pubblico certificati qualificati in conformità alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche ([3]), soggetti a supervisione/accreditamento da parte degli Stati membri.

(2) L'esperienza pratica maturata con l'attuazione della decisione 2009/767/CE da parte degli Stati membri ha dimostrato che sono necessari alcuni miglioramenti per massimizzare i benefici degli elenchi di fiducia. Inoltre, l'Istituto europeo per le norme di telecomunicazione (*European Telecommunications Standards Institute* — ETSI) ha pubblicato nuove specifiche tecniche per gli elenchi di fiducia (TS 119 612) che, pur essendo basate sulle specifiche attualmente contenute nell'allegato della decisione, apportano un certo numero di miglioramenti alle specifiche vigenti.

(3) Occorre pertanto modificare la decisione 2009/767/CE in modo da fare riferimento alle specifiche tecniche 119 612 dell'ETSI e da incorporare le modifiche considerate necessarie per migliorare e facilitare l'attuazione e l'uso degli elenchi di fiducia.

(4) Affinché gli Stati membri possano apportare ai loro attuali elenchi di fiducia le modifiche tecniche necessarie, è opportuno che la presente decisione si applichi a decorrere dal 1º febbraio 2014.

(5) Le misure di cui alla presente decisione sono conformi al parere del comitato della direttiva servizi,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Modifiche della decisione 2009/767/CE

La decisione 2009/767/CE è così modificata:

1) l'articolo 2 è così modificato:

a) i paragrafi 1, 2 e 2 *bis* sono sostituiti dai seguenti:

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

2. Gli Stati membri elaborano e pubblicano l'elenco di fiducia in formato leggibile a macchina, conformemente alle specifiche di cui all'allegato. Se lo Stato membro sceglie di pubblicare l'elenco di fiducia in formato leggibile all'uomo, il formato soddisfa le specifiche di cui all'allegato.

2 *bis*. Gli Stati membri firmano elettronicamente il formato leggibile a macchina dell'elenco di fiducia per garantirne l'autenticità e l'integrità. Lo Stato membro che pubblica l'elenco di fiducia in formato leggibile all'uomo assicura che il formato contenga gli stessi dati del formato leggibile a macchina e lo firma elettronicamente con lo stesso certificato utilizzato per il formato leggibile a macchina.»;

([1]) GU L 376 del 27.12.2006, pag. 36.
([2]) GU L 274 del 20.10.2009, pag. 36.
([3]) GU L 13 del 19.1.2000, pag. 12.

b) è inserito il seguente paragrafo 2 *ter*:

«2 *ter*. Gli Stati membri assicurano che il formato leggibile a macchina dell'elenco di fiducia sia accessibile nel sito di pubblicazione in qualsiasi momento, senza interruzione, salvo a fini di manutenzione.»;

c) il paragrafo 3 è sostituito dal seguente:

«3. Gli Stati membri comunicano alla Commissione le seguenti informazioni:

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

b) il sito di pubblicazione del formato leggibile a macchina dell'elenco di fiducia;

c) due o più certificati a chiave pubblica del gestore del sistema, con periodi di validità sfasati di almeno tre mesi, corrispondenti alle chiavi private che possono essere usate per firmare elettronicamente il formato leggibile a macchina dell'elenco di fiducia;

d) qualsiasi modifica apportata alle informazioni di cui alle lettere a), b) e c).»;

d) è inserito il seguente paragrafo 3 *bis*:

«3 *bis*. Se lo Stato membro pubblica l'elenco di fiducia in formato leggibile all'uomo, le informazioni di cui al paragrafo 3 sono comunicate anche per tale formato.»;

2) l'allegato è sostituito dall'allegato della presente decisione.

Articolo 2

Applicazione

La presente decisione si applica a decorrere dal 1º febbraio 2014.

Articolo 3

Destinatari

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 14 ottobre 2013

Per la Commissione

Michel BARNIER

Membro della Commissione

ALLEGATO

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

REQUISITI GENERALI

1. **Introduzione**

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 secondo le quali gli Stati membri trasmettono le informazioni relative allo status 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 alle pertinenti disposizioni della direttiva 1999/93/CE. Devono essere fornite anche le serie storiche di informazioni relative allo status di supervisione/accreditamento dei servizi di certificazione soggetti a supervisione/accreditamento.

L'informazione è finalizzata in primo luogo a facilitare il processo di convalida delle firme elettroniche qualificate (QES) e delle firme elettroniche avanzate (AdES) ([2]) basate su un certificato qualificato ([3]) ([4]).

Tra le informazioni obbligatorie da inserire nell'elenco di fiducia (TL) devono figurare, come minimo, le informazioni sui CSP soggetti a supervisione/accreditamento che rilasciano certificati qualificati (QC) ([5]) conformemente alle disposizioni della direttiva 1999/93/CE [articolo 3, paragrafi 2 e 3, e articolo 7, paragrafo 1, lettera a)], comprese, se non incluse nei certificati qualificati, le informazioni sui certificati qualificati sui quali si basa una firma elettronica, nonché l'indicazione se la firma è generata o no da un dispositivo per la creazione di una firma sicura (*Secure Signature Creation Device* — SSCD) ([6]).

Informazioni supplementari relative ad altri prestatori di servizi di certificazione che non rilasciano certificati qualificati ma che forniscono servizi connessi con le firme elettroniche (ad esempio prestatori di servizi di certificazione che forniscono servizi di marcatura temporale e che rilasciano *token* di marca temporale, CPS che rilasciano certificati non qualificati ecc.) possono essere inserite nell'elenco di fiducia a livello nazionale su base facoltativa, purché tali CSP siano o soggetti a supervisione/accreditamento in maniera analoga ai prestatori di servizi di certificazione che rilasciano certificati qualificati o siano approvati nel quadro di un diverso regime nazionale di approvazione. Il regime nazionale di approvazione di alcuni Stati membri può differire dai regimi di supervisione o di accreditamento facoltativo applicabili ai prestatori di servizi di certificazione che rilasciano certificati qualificati per quanto riguarda i requisiti applicabili e/o l'organizzazione responsabile. Nelle presenti specifiche le espressioni «soggetto ad accreditamento» e/o «soggetto a supervisione» coprono anche i regimi nazionali di approvazione, ma gli Stati membri sono tenuti a fornire informazioni supplementari sulla natura del regime nazionale nel rispettivo elenco di fiducia, compresi chiarimenti sulle possibili differenze rispetto ai regimi di supervisione/accreditamento applicati ai prestatori di servizi di certificazione che rilasciano certificati qualificati.

Il modello comune si basa sulle specifiche tecniche 119 612 V1.1.1 dell'ETSI ([7]) (di seguito «ETSI TS 119 612») riguardanti l'elaborazione, la pubblicazione, la localizzazione, l'accesso, l'autenticazione e l'integrità degli elenchi.

2. **Struttura del modello comune per l'elenco di fiducia**

Il modello comune per l'elenco di fiducia degli Stati membri è strutturato, conformemente alle ETSI TS 119 612, nelle seguenti categorie di informazioni:

1) il tag dell'elenco di fiducia, che ne facilita l'individuazione nelle ricerche elettroniche;

2) informazioni sull'elenco di fiducia e sul relativo regime di rilascio;

3) una sequenza di campi contenenti informazioni di identificazione inequivocabili su tutti i CSP oggetto di supervisione/accreditamento nell'ambito del regime (la sequenza è facoltativa, vale a dire che se non è usata la si suppone vuota, in altri termini si considera che nessun CSP è soggetto a supervisione o accreditamento nello Stato membro associato ai fini dell'elenco di fiducia);

4) per ogni CSP elencato i dati relativi ai servizi di fiducia specifici che presta, il cui status attuale è registrato nell'elenco di fiducia, sono forniti come sequenza di campi che identificano in modo inequivocabile i servizi di certificazione soggetti a supervisione/accreditamento prestati dal CPS e il loro status attuale (la sequenza deve avere come minimo una voce);

([1]) Quali definiti all'articolo 2, punto 11, della direttiva 1999/93/CE.
([2]) Quali definite all'articolo 2, punto 2, della direttiva 1999/93/CE.
([3]) In tutto il presente documento per indicare la firma elettronica avanzata (AdES) basata su un certificato qualificato (QC) viene utilizzato l'acronimo «$AdES_{QC}$».
([4]) Si noti che esiste un certo numero di servizi elettronici basati su AdES semplici, il cui uso transfrontaliero sarebbe altresì facilitato, purché i servizi di certificazione che ne sono alla base (ad esempio il rilascio di certificati non qualificati) siano inseriti tra i servizi soggetti a supervisione/accreditamento da parte dello Stato membro nella parte informativa facoltativa dell'elenco di fiducia.
([5]) Quali definiti all'articolo 2, punto 10, della direttiva 1999/93/CE.
([6]) Quale definito all'articolo 2, punto 6, della direttiva 1999/93/CE.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) — Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5) per ogni servizio di certificazione soggetto a supervisione/accreditamento elencato, le informazioni sulla storia dello status, se applicabile;

6) la firma applicata sull'elenco di fiducia.

Nel caso dei CSP che rilasciano QC, la struttura dell'elenco di fiducia, in particolare la componente dell'informazione sul servizio (ai sensi del precedente punto 4), consente che le informazioni supplementari inserite nelle estensioni delle informazioni sui servizi compensino le situazioni in cui il certificato qualificato contenga informazioni (leggibili a macchina) insufficienti sul suo status «qualificato», sul fatto che possa essere o no basato su un SSCD e, soprattutto informazioni che tengano conto del fatto che la maggior parte dei CSP (commerciali) utilizzano un'unica autorità di certificazione (CA) per il rilascio di diversi tipi di certificati entità finale, sia qualificati che non qualificati.

Nel contesto dei servizi di generazione dei certificati (CA), il numero di voci sui servizi presenti nell'elenco per un CSP può essere ridotto quando esistono uno o più servizi di CA di livello superiore nella PKI (*Public Key Infrastructure*) del CSP (ad esempio nell'ambito di una gerarchia di CA che va dalla CA radice fino alle CA che rilasciano i certificati) includendo detti servizi di CA di livello superiore invece dei servizi di CA che rilasciano certificati entità finale (ad esempio, inserendo unicamente la CA radice del CSP). Tuttavia in tali casi, le informazioni sullo status si applicano all'intera gerarchia di servizi di CA sotto il servizio elencato, e deve essere rispettato e garantito il principio che prevede che sia assicurato il collegamento inequivocabile tra un servizio di certificazione di un CSP_{QC} e l'insieme dei certificati destinati a essere identificati come QC.

2.1. *Descrizione delle informazioni di ciascuna categoria*

1. Tag dell'elenco di fiducia

2. Informazioni sull'elenco di fiducia e sul relativo regime di rilascio

In questa categoria rientrano le seguenti informazioni:

— l'**identificativo della versione del formato** dell'elenco di fiducia,

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

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

— le **informazioni sul gestore (proprietario) del regime** relativo all'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),

— le **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 sito in cui sono reperibili informazioni sul o sui regimi (modello di regime, norme, criteri, comunità di applicazione, tipo ecc.),

  — periodo di conservazione delle informazioni (serie storiche),

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

— **data e ora di pubblicazione** dell'elenco di fiducia,

— **prossimo aggiornamento previsto** dell'elenco di fiducia.

3. Informazioni di identificazione inequivocabili su ogni CSP soggetto a supervisione/accreditamento nel quadro del regime

Questa serie deve comprendere quantomeno le seguenti informazioni:

— la denominazione del CSP quale figura nei registri ufficiali (compreso l'identificativo utente (UID) dell'organizzazione CPS secondo le prassi seguite negli Stati membri),

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

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

4. Per ogni CSP elencato una sequenza di campi contenenti informazioni di identificazione inequivocabili sul servizio di certificazione prestato dal CPS e soggetto a supervisione/accreditamento nel quadro della direttiva 1999/93/CE

Questa serie include quantomeno le seguenti informazioni per ciascun servizio di certificazione del CSP elencato:

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

— la denominazione (commerciale) del servizio: denominazione (commerciale) del servizio di certificazione,

— l'identità digitale del servizio: identificativo univoco del servizio di certificazione,

— lo status attuale del servizio: identificativo dello status attuale del servizio;

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

— se del caso, l'estensione delle informazioni sul servizio: informazioni supplementari sul servizio (inserite direttamente o mediante riferimento ad un sito da cui le informazioni possono essere scaricate), ossia informazioni sulla definizione del servizio fornite dal gestore del regime, informazioni di accesso relative al servizio, informazioni sulla definizione del servizio fornite dal CPS ed estensioni delle informazioni sul servizio. Ad esempio, per i servizi CA/QC, una sequenza facoltativa di tuple di informazione, ciascuna delle quali fornisce:

  — i criteri da utilizzare per identificare più precisamente (filtrare), all'interno del servizio di fiducia identificato, la serie precisa di risultati relativi ai servizi [ad esempio una serie di certificati (qualificati)] per cui sono richieste/fornite informazioni supplementari relative allo status, informazioni indicanti se il certificato è basato o no su un SSCD e/o è rilasciato ad una persona giuridica, e

  — i «qualificatori» associati, indicanti se la serie di risultati relativi ai servizi identifica certificati da considerare qualificati e/o se i certificati qualificati identificati del servizio 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).

5. Per ogni servizio di certificazione elencato le informazioni storiche sul relativo status

6. La firma elaborata elettronicamente a fini di autenticazione su tutti i campi dell'elenco di fiducia tranne il valore della firma stesso.

3. **Orientamenti per la creazione e la modifica delle voci dell'elenco di fiducia**

3.1. *Informazioni sullo status dei servizi soggetti a supervisione/accreditamento e dei relativi prestatori in un unico elenco*

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 dello Stato membro in questione ai fini del controllo della conformità alle pertinenti disposizioni della direttiva 1999/93/CE».

L'elenco di fiducia è l'unico strumento di cui si serve lo Stato membro in questione per fornire informazioni sullo status di supervisione/accreditamento dei servizi di certificazione e dei relativi prestatori:

— **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** ai fini del controllo della conformità alle 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 di accreditamento facoltativo ad essi relativi, è opportuno distinguere due tipologie di CSP, ovvero i prestatori di servizi di certificazione (CPS) che rilasciano certificati qualificati (QC) al pubblico (CSP_{QC}) e quelli che non rilasciano tali certificati al pubblico ma che forniscono altri servizi (accessori) 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 ai fini del controllo della conformità alle 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 regime di supervisione vigente nello Stato membro, salvo il caso in cui non siano stabiliti nello stesso,

— il regime di «supervisione» (o il regime di «accreditamento facoltativo») applicabile è definito dalla direttiva 1999/93/CE, di cui deve rispettare le pertinenti disposizioni, in particolare le disposizioni dell'articolo 3, paragrafo 3, dell'articolo 8, paragrafo 1, dell'articolo 11 e del considerando 13, [o, rispettivamente, articolo 2, punto 13, articolo 3, paragrafo 2, articolo 7, paragrafo 1, lettera a), articolo 8, paragrafo 1, articolo 11 e considerando 4 e da 11 a 13];

— **CSP che non rilasciano QC**:

— possono rientrare nel regime di «accreditamento facoltativo» (quale definito dalla direttiva 1999/93/CE e in conformità alla stessa) e/o in un «regime di approvazione riconosciuto» definito e attuato su base nazionale ai fini del controllo della conformità alle disposizioni della direttiva ed eventualmente alle disposizioni della normativa nazionale in materia di prestazione di servizi di certificazione (secondo la definizione dell'articolo 2, punto 11, della direttiva 1999/93/CE);

— alcuni degli oggetti fisici o binari (logici) generati o emessi a seguito della prestazione di un servizio di certificazione possono ricevere una «qualificazione» specifica sulla base della loro conformità alle disposizioni e ai requisiti fissati a livello nazionale, ma è probabile che la portata di tale qualificazione sia limitata esclusivamente al livello nazionale.

Ogni Stato membro deve elaborare e gestire un unico elenco di fiducia indicante lo status di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte dello Stato membro. L'elenco di fiducia comprende almeno i CSP che rilasciano QC. L'elenco di fiducia può altresì indicare lo status di altri servizi di certificazione soggetti a supervisione o accreditamento nell'ambito di un regime di approvazione definito a livello nazionale.

3.2. *Una serie unica di valori di status di supervisione/accreditamento*

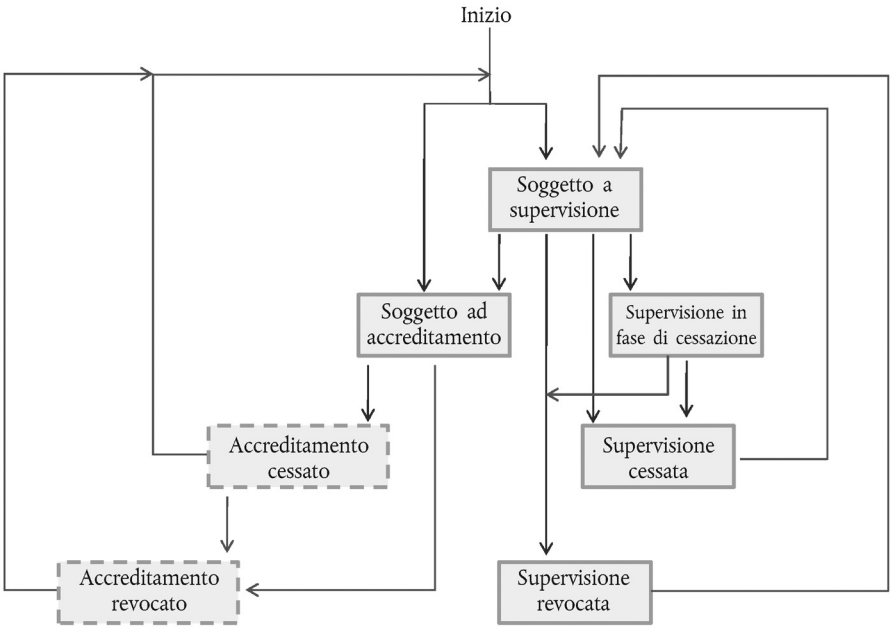
Nell'elenco di fiducia il fatto che il servizio sia attualmente «soggetto a supervisione» o «soggetto ad accreditamento» è indicato dal valore del suo status attuale. Inoltre, lo status di supervisione o di accreditamento può essere positivo («soggetto a supervisione», «accreditato», «supervisione in fase di cessazione»), cessato («supervisione cessata», «accreditamento cessato») o revocato («supervisione revocata», «accreditamento revocato») ed è indicato con i corrispondenti valori. Durante la sua durata lo stesso servizio di certificazione può passare da uno status di supervisione ad uno di accreditamento e viceversa ([1]).

La successiva figura 1 descrive il flusso previsto di un 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 passarlo da uno status di accreditamento a uno status di supervisione, ad esempio per motivi commerciali e/o economici.

Figura 1

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



Legenda:

Status transitorio quando esiste un modello di supervisione associato (ad es. per i CSP che rilasciano QC soggetti ad accreditamento e supervisione nello Stato membro in cui sono stabiliti)
Possibile status attuale quando non esiste un modello di supervisione associato (ad es. per i CSP soggetti ad accreditamento in uno Stato membro in cui non sono stabiliti)

Possibile status attuale

Il servizio di certificazione che rilascia QC stabilito in uno Stato membro deve essere soggetto a supervisione (da parte dello Stato membro in cui è stabilito) e può chiedere volontariamente l'accreditamento. Il valore di status di tale servizio, se incluso nell'elenco di fiducia, deve essere uno dei valori riportati nella figura come «valore di status attuale» conformemente al suo status effettivo e deve cambiare, se del caso, in base al flusso di status descritto sopra. Tuttavia, «accreditamento cessato» e «accreditamento revocato» devono entrambi essere valori di «status transitorio» se il corrispondente servizio del CSP_{QC} è inserito nell'elenco di fiducia dello Stato membro di stabilimento, in quanto il servizio deve essere di norma soggetto a supervisione (anche quando non è o non è più soggetto ad accreditamento). Quando il servizio corrispondente è elencato (accreditato) in uno Stato membro diverso da quello di stabilimento, questi valori possono essere valori finali.

Gli Stati membri che hanno istituito o sono in procinto di istituire «regimi di approvazione riconosciuti», definiti e attuati 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 (secondo la definizione dell'articolo 2, punto 11, della direttiva 1999/93/CE), devono inserire tali regimi in una delle due categorie seguenti:

— «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 da 11 a 13),

— «supervisione», come previsto dalla direttiva 1999/93/CE e attuato da disposizioni e requisiti nazionali in conformità del relativo ordinamento.

Pertanto un servizio di certificazione che non rilascia QC può essere soggetto a supervisione o ad accreditamento facoltativo. Il valore di status di tale servizio, se incluso nell'elenco di fiducia, deve essere uno dei valori riportati nella figura come «valore di status attuale» (cfr. la figura 1) conformemente al suo status effettivo e deve cambiare, se del caso, in base al flusso di status descritto sopra.

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

— informazioni sul regime 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 regime 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 le parti che fanno affidamento sui 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 nell'elenco di fiducia l'informazione sullo status di supervisione/accreditamento si riferisce ai servizi dei CSP che non rilasciano QC, le summenzionate serie di informazioni sono fornite nei campi «*Scheme information URI*» (clausola 5.3.7, informazioni fornite dagli Stati membri), «*Scheme type/community/rules*» (clausola 5.3.9, testo comune a tutti gli Stati membri e informazioni specifiche fornite dallo Stato membro su base facoltativa) e «*TSL policy/legal notice*» (clausola 5.3.11, testo comune a tutti gli Stati membri con riferimento alla direttiva 1999/93/CE, con la possibilità per ogni Stato membro di aggiungere testi/riferimenti ad esso specifici).

Informazioni supplementari di «qualificazione» definite al livello dei 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 dell'estensione «*additionalServiceInformation*» (clausola 5.5.9.4) del campo «*Service information extension*» (clausola 5.5.9). Ulteriori informazioni sulle corrispondenti specifiche tecniche sono fornite nelle specifiche dettagliate di cui al capitolo I.

Sebbene in uno Stato membro organismi distinti possano essere responsabili della supervisione e dell'accreditamento dei servizi di certificazione, è previsto che per ogni servizio di certificazione sia utilizzata una sola voce e che il relativo status di supervisione/accreditamento sia aggiornato conformemente.

3.3. *Voci dell'elenco di fiducia volte a facilitare la convalida di QES e $AdES_{QC}$*

L'aspetto più importante della creazione dell'elenco di fiducia è l'elaborazione della parte obbligatoria dello stesso, ossia l'«elenco dei servizi» dei CSP che rilasciano QC, in modo che essa rifletta l'esatto status di ciascun servizio di certificazione che rilascia QC e che sia garantito 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).

Le informazioni richieste possono includere informazioni diverse da quelle riportate alla voce «*Service digital identity*» di una CA (radice), in particolare informazioni che consentono di identificare lo status di QC dei certificati rilasciati dal servizio CA e di accertare se le firme supportate sono create o no da un SSCD. Pertanto, l'organismo designato nello Stato membro incaricato di elaborare, modificare e gestire l'elenco di fiducia deve tenere conto del profilo attuale e del contenuto di ogni QC rilasciato, per ogni servizio CSP_{QC} che figura nell'elenco di fiducia.

Idealmente ogni QC rilasciato dovrebbe contenere la dichiarazione di conformità dei QC definita dall'ETSI (*QcCompliance*) ([1]) 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 la generazione di firme elettroniche e/o che ciascun QC rilasciato include uno degli identificativi dell'oggetto (*Object Identifier* — OID) per la politica dei certificati QCP/QCP+, quali definiti nella EN 319 411-2 dell'ETSI ([2]). L'uso di norme di riferimento differenti da parte dei CSP che rilasciano QC, il fatto che l'interpretazione di tali norme vari considerevolmente, nonché la non conoscenza dell'esistenza e della preesistenza di alcune norme o specifiche tecniche normative hanno determinato differenze nel contenuto effettivo dei QC attualmente rilasciati (ad esempio per quanto riguarda l'uso delle dichiarazioni QC definite dall'ETSI), impedendo di conseguenza alle parti riceventi di fare affidamento unicamente sul certificato del firmatario (e sul percorso/sulla catena ad esso associati) per verificare, quantomeno in modo leggibile a macchina, se il certificato su cui si basa una firma elettronica sia dichiarato o no come QC e se esso sia associato o no ad un SSCD mediante il quale è stata generata la firma elettronica.

([1]) Cfr. ETSI EN 319 412-5 (*Electronic Signatures and Infrastructures (ESI): Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile*) per la definizione della dichiarazione.

([2]) ETSI EN 319 411-2 (*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.*

Completando i campi «*Service type identifier*» («Sti»), «*Service name*» («Sn») e «*Service digital identity*» («Sdi») della voce relativa al servizio nell'elenco di fiducia con le informazioni fornite nel campo «*Service information extensions*» («Sie») è possibile determinare pienamente il tipo specifico di certificato qualificato rilasciato dal servizio di certificazione di un CSP che rilascia QC elencato e fornire informazioni sul fatto che sia basato o no su un SSCD (quando tali informazioni mancano nel QC rilasciato). A questa voce è associata l'informazione specifica «*Service current status*» («Scs»), come illustrato nella successiva figura 2.

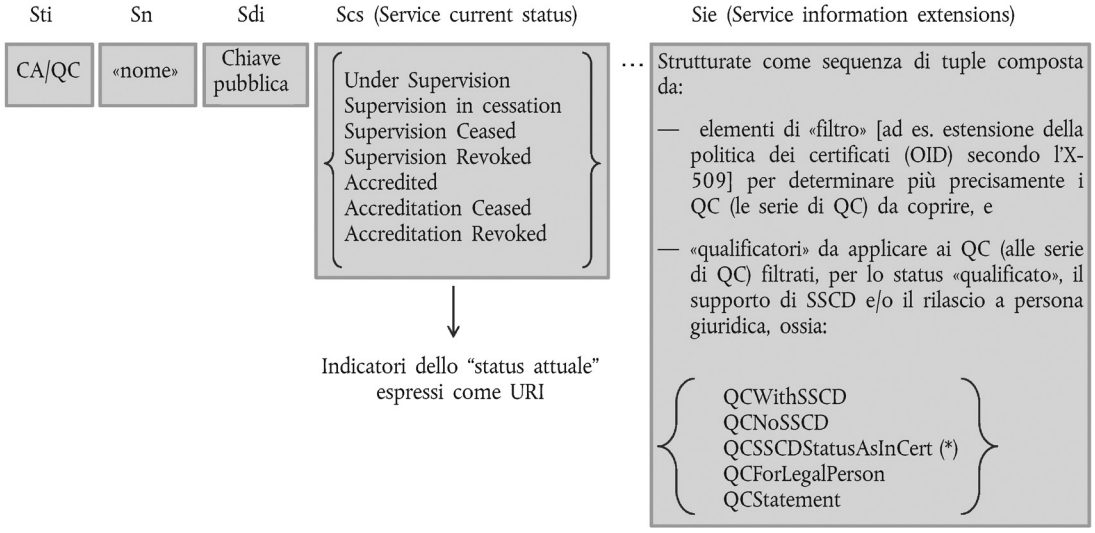
Inserire nell'elenco il servizio con la semplice indicazione dell'«Sdi» di una CA (radice) significherebbe che è garantito (dal CSP che rilascia QC ma anche dall'organismo di supervisione/accreditamento responsabile del CSP) che qualsiasi certificato entità finale rilasciato tramite tale (gerarchia di) CA (radice) contiene informazioni definite dalle norme ETSI leggibili a macchina sufficienti 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 fosse vera (ad esempio, nel QC non vi è alcuna indicazione, basata sulle norme ETSI e leggibile a macchina, che esso è basato su un SSCD), se viene elencato semplicemente l'«Sdi» della CA (radice) si può solo ipotizzare che i QC rilasciati tramite tale gerarchia di CA (radice) non siano basati su alcun SSCD. Per indicare che i QC in questione devono essere considerati basati su un SSCD, occorre utilizzare il campo «Sie» (ciò indica anche che l'informazione è garantita dal CSP che rilascia i QC e soggetta a supervisione/accreditamento da parte rispettivamente dell'organismo di supervisione o di accreditamento).

Figura 2

Voce dell'elenco di fiducia relativa al servizio del CSP che rilascia QC inserito nell'elenco di fiducia

Principi generali — regole di creazione e modifica — voci dei CSP_{QC} (servizi elencati)

Voce relativa al servizio di un CSP_{QC} elencato:



(*) significa che è garantito che tale informazione è contenuta in un QC di una CA/QC definita nei campi Sdi-[Sie] (se il QC non contiene nulla, allora il significato è NoSSCD)

Le presenti specifiche tecniche relative al modello comune per l'elenco di fiducia consentono di utilizzare una combinazione di cinque tipi principali di informazioni nella voce relativa al servizio:

— «*Service type identifier*» («Sti»), che identifica, ad esempio, la CA che rilascia QC («CA/QC»),

— «*Service name*» («Sn»),

— le informazioni del campo «*Service digital identity*» («Sdi») che identificano il servizio elencato: ad esempio, (come minimo) la chiave pubblica della CA che rilascia QC,

— per i servizi CA/QC, l'informazione facoltativa del campo «*Service information extension*» («Sie»), che consente l'inserimento di un certo numero di informazioni specifiche inerenti al servizio per quanto riguarda lo status di revoca dei certificati scaduti, caratteristiche supplementari dei QC, l'acquisizione di un CSP da parte di un altro CSP ed altre informazioni supplementari sul servizio. Ad esempio, le caratteristiche supplementari dei QC sono rappresentate da 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 nel campo «Sdi», la serie precisa di certificati qualificati per cui sono richieste/fornite informazioni supplementari relative allo status «qualificato» e informazioni indicanti se il certificato è basato o no su un SSCD e/o rilasciato ad una persona giuridica, e

  — le informazioni associate («qualificatori») indicanti se i certificati qualificati della serie sono da considerare «qualificati», si basano o no su un SSCD o se le informazioni associate sono parte del 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),

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

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

  — lo status di supervisione/accreditamento.

3.4. *Orientamenti per la creazione, 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/di accreditamento) che, per un servizio inserito nell'elenco identificato da un «Sdi», tutti i QC basati su un SSCD contengono la dichiarazione di conformità dei QC (*QcCompliance*) definita dall'ETSI e la dichiarazione QcSSCD e/o l'identificativo di oggetto (OID) QCP+, è sufficiente l'uso di un «Sdi» appropriato e la «Sie» può essere utilizzata in via facoltativa e non è necessario che contenga le informazioni relative al supporto SSCD;

2) se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/accreditamento) che per un servizio inserito nell'elenco identificato da un «Sdi», tutti i QC non basati su un SSCD contengono la dichiarazione di conformità dei QC (*QcCompliance*) e/o l'identificativo di oggetto (OID) QCP, e non contengono la dichiarazione QcSSCD o l'identificativo di oggetto (OID) QCP+, è sufficiente l'uso di un «Sdi» appropriato e la «Sie» può essere utilizzata in via facoltativa e non è necessario che contenga le informazioni relative al supporto SSCD (il che significa: non basato su un SSCD);

3) se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/di accreditamento) che per un servizio compreso nell'elenco identificato da un «Sdi» tutti i QC contengono la dichiarazione di conformità dei QC (*QcCompliance*) e che 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 l'CSP o mediante altre informazioni specifiche sui CSP contenute nel QC, direttamente o indirettamente, e leggibili o no a macchina), ma i certificati basati su SSCD non contengono NÉ la dichiarazione QcSSCD NÉ l'identificativo di oggetto (OID) QCP + dell'ETSI, l'uso di un «Sdi» appropriato può non essere sufficiente E la «Sie» deve essere utilizzata per indicare in modo esplicito che il servizio è basato su SSCD, oltre ad un'eventuale estensione dell'informazione per identificare la serie di certificati coperti. È probabile che debbano essere utilizzati differenti «valori di informazione sul supporto SSCD» per lo stesso «Sdi» quando viene utilizzata la «Sie»;

4) se esiste la garanzia (fornita dal CSP_{QC} e soggetta a supervisione/accreditamento da parte dell'organismo di supervisione/di accreditamento) che per un servizio compreso nell'elenco identificato da un «Sdi», uno qualsiasi dei QC non contiene la dichiarazione di conformità dei QC (*QcCompliance*), 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 all'«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 i 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 «Sdi» appropriato non è sufficiente E la «Sie» deve essere utilizzata per includere informazioni esplicite sulla qualificazione. È probabile che debbano essere utilizzati differenti «valori di informazione sul supporto SSCD» per lo stesso «Sdi» quando viene utilizzata la «Sie».

Il principio generalmente applicato è che per un CSP inserito nell'elenco di fiducia vi deve essere una voce relativa al servizio per singola chiave pubblica per un servizio di certificazione del tipo CA/QC, ovvero per autorità di certificazione che rilascia (direttamente) QC. In talune circostanze eccezionali e in condizioni attentamente gestite, l'organismo di supervisione/di accreditamento dello Stato membro può decidere di utilizzare, come «Sdi» dell'unica voce dell'elenco di servizi prestati da detto CSP elencato, la chiave pubblica di una CA radice o di una CA di livello superiore nell'ambito della PKI del CSP (ad esempio nell'ambito di una gerarchia di CA del CSP che va dalla CA radice fino a varie CA di rilascio) anziché elencare tutti i servizi delle CA di rilascio subordinate (ossia specificare nell'elenco 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). Gli Stati membri devono valutare attentamente le conseguenze (vantaggi e svantaggi) dell'uso della chiave pubblica della CA radice o della CA di livello superiore come valore «Sdi» nella voce relativa al servizio iscritto nell'elenco di fiducia. Inoltre, se viene utilizzata questa eccezione autorizzata al principio generale, gli Stati membri devono fornire la documentazione necessaria per facilitare l'elaborazione e la verifica del percorso di certificazione. Ad esempio: nel caso di un CSP_{QC} che utilizza una CA radice che ingloba diverse CA che rilasciano certificati qualificati (QC) e certificati non qualificati (non QC), i cui QC contengono unicamente la dichiarazione di conformità dei QC (*QcCompliance*) ma non indicano se il servizio si basa o no su un SSCD, elencare soltanto l'«Sdi» della CA radice significherebbe, secondo le norme sopraindicate, che nessuno dei QC rilasciati sotto tale CA radice è basato su un SSCD. Per i QC che sono basati effettivamente su un SSCD ma che non includono una dichiarazione leggibile a macchina indicante detto supporto, 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), l'elenco di fiducia dovrebbe utilizzare la «Sie» e il campo associato «*Qualifications Extension*», ad esempio per fornire informazioni di filtro per identificare la serie/le serie di certificati mediante l'uso di OID specifici dei CSP_{QC} che possano essere utilizzati dai CSP_{QC} per distinguere tra differenti tipi di QC (alcuni basati su un SSCD e altri no) e per associare esplicite «informazioni sul supporto SSCD» alla serie/alle serie di certificati (filtrati) identificati mediante l'uso dei «qualificatori».

Gli **orientamenti generali per l'utilizzazione** di applicazioni, servizi o prodotti relativi alla firma elettronica basati su un elenco di fiducia conforme alle presenti specifiche tecniche sono i seguenti:

La voce «Sti» «CA/QC» (e analogamente la voce CA/QC ulteriormente qualificata come «*Root CA/QC*» mediante l'uso dell'estensione della «Sie» «*additional Service Information Extension*»):

— indica che tutti i certificati entità finale rilasciati dalla CA identificata mediante l'«Sdi» (e analogamente all'interno della gerarchia CA, partendo dalla CA radice identificata dall'«Sdi») del CSP corrispondente (cfr. campi associati delle informazioni sul TSP) sono QC, **purché** ciò sia indicato nel certificato mediante l'uso dell'opportuna dichiarazione QC leggibile a macchina (ossia *QcCompliance*) 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 presente alcuna informazione nel campo «*Qualification Extension*» della «Sie» o se un certificato entità finale presentato come QC non è ulteriormente identificato da un'informazione correlata nel campo «*Qualification Extension*» della «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 il non uso) delle opportune dichiarazioni QC (ovvero *QcCompliance*, QcSSCD) e/o OID QCP(+) definiti dall'ETSI è garantito come conforme a quanto indicato dal CSP_{QC},

— **e SE** è presente un'informazione nel campo «*Qualification Extension*» della «Sie», in aggiunta alle regole interpretative di cui sopra relative all'uso standard, i certificati identificati mediante l'uso di questa informazione del campo «*Qualification Extension*» della «Sie», costruita sul principio di una sequenza di filtri che identificano ulteriormente una serie di certificati, devono essere considerati sulla base dei «qualificatori» associati che forniscono informazioni supplementari sullo status qualificato, sul «supporto SSCD» e/o sulla «persona giuridica come soggetto» (ad esempio i certificati che contengono un OID specifico nell'estensione della politica dei certificati e/o che hanno uno specifico modello di «utilizzazione della chiave» e/o che sono filtrati mediante l'uso di un valore specifico che compare in un campo o in un'estensione specifici del certificato ecc.). I predetti «qualificatori» rientrano nella seguente serie di «*Qualifiers*» utilizzati per compensare la mancanza di informazioni nel corrispondente contenuto dei QC e, rispettivamente:

  — per indicare lo status qualificato: «QCStatement», indicante che il/i certificato/i identificato/i è/sono qualificato/i,

    E/O

  — per indicare la natura del supporto SSCD:

    — «QCWithSSCD», avente il significato di «QC basato su un SSCD», oppure

    — «QCNoSSCD», avente il significato di «QC non basato su un SSCD», oppure

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

    E/O

— per indicare il rilascio ad una persona giuridica:

— «QCForLegalPerson», avente il significato di «certificato rilasciato ad una persona giuridica».

3.5. *Servizi su cui sono basati i servizi «CA/QC» ma che non rientrano nell'«Sdi»del «CA/QC»*

I servizi di status di validità dei certificati relativi ai QC, per i quali le informazioni sullo status di validità dei certificati (ad esempio risposte CRL e OCSP) sono firmate da un'entità la cui chiave privata non è certificata da un percorso di certificazione che porta ad una CA elencata che rilascia QC («CA/QC»), sono inclusi nell'elenco di fiducia inserendoli come tali (ossia rispettivamente con un tipo di servizio «OCSP/QC» o «CRL/QC»), perché questi servizi possono essere considerati parte dei servizi «qualificati» soggetti a supervisione/accreditamento connessi alla prestazione 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 elencati devono essere considerati «validi» e conformi al valore di status del servizio CA/QC elencato.

Disposizione analoga può applicarsi ai servizi di certificazione che rilasciano certificati non qualificati (servizio del tipo «CA/PKC»).

L'elenco di fiducia include i servizi di status di validità dei certificati quando le informazioni sulla localizzazione relative a tali servizi non sono presenti nei certificati entità finale a cui si applicano i servizi di status di validità.

4. **Definizioni e acronimi**

Ai fini del presente documento sono utilizzati 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	1) prestatore di servizi di certificazione che crea e assegna certificati a chiave pubblica; o 2) servizio tecnico di generazione dei certificati utilizzato dal prestatore di servizi di certificazione che crea e assegna certificati a chiave pubblica. *NOTA*: cfr. la clausola 4 della EN 319 411-2 [1] per ulteriori spiegazioni del concetto di autorità di certificazione.
Autorità di certificazione che rilascia certificati qualificati	CA/QC	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	La supervisione prevista all'articolo 3, paragrafo 3, della direttiva 1999/93/CE. La direttiva 1999/93/CE impone agli Stati membri di istituire un regime appropriato di supervisione dei CPS stabiliti nel loro territorio che rilasciano al pubblico certificati qualificati, il quale assicuri il rispetto delle 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 prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte dello Stato membro interessato ai fini del controllo della conformità con le disposizioni della direttiva 1999/93/CE.

Termine	Acronimo	Definizione
Elenco di status dei servizi di fiducia	TSL	Forma di elenco firmato utilizzato come base per la presentazione di informazioni sullo status dei servizi di fiducia conformemente alle ETSI TS 119 612.
Servizio di fiducia		Servizio che permette di accrescere la fiducia nelle operazioni elettroniche (in generale, ma non necessariamente, mediante l'uso di tecniche crittografiche o di materiale riservato) (ETSI TS 119 612). *NOTA*: il termine è utilizzato in un'accezione più ampia di servizio di certificazione che rilascia certificati o che fornisce altri servizi connessi alle firme elettroniche.
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 di CSP).
Token del servizio di fiducia	TrST	Oggetto fisico o binario (logico) generato o rilasciato a seguito dell'uso di un servizio di fiducia. Esempi di TrST binari sono i certificati, gli elenchi di revoca dei certificati (*Certificate Revocation List* — CRL), i *token* di marca temporale (*Time Stamp Token* — TST) e le risposte del protocollo sullo status dei certificati *online* (*Online Certificate Status Protocol* — OCSP).
Firma elettronica qualificata	QES	AdES basata su un QC e creata da un dispositivo per la creazione di una firma sicura (*Secure Signature Creation Device* — SSCD), quale definito 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	$AdES_{QC}$	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.

([1]) EN 319 411-2: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.*

Nei successivi capitoli le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «OBBLIGATORIO», «DOVREBBE», «DOVREBBERO», «NON DOVREBBE», «NON DOVREBBERO», «SI RACCOMANDA», «PUÒ», «POSSONO» e «FACOLTATIVO» devono essere interpretate nel significato di cui al documento RFC 2119. ([1])

CAPITOLO I

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

Le presenti specifiche si basano sulle specifiche e sui requisiti di cui alle specifiche tecniche 119 612 v1.1.1 dell'ETSI (di seguito ETSI TS 119 612).

Qualora nelle presenti specifiche non siano indicati requisiti specifici si DEVONO applicare integralmente i requisiti delle clausole 5 e 6 delle ETSI TS 119 612. Se invece nelle presenti specifiche sono indicati requisiti specifici, questi PREVALGONO sui corrispondenti requisiti delle ETSI TS 119 612. In caso di discrepanza tra le presenti specifiche e le specifiche delle ETSI TS 119 612, DEVONO essere applicate le presenti specifiche.

Scheme operator name (clausola 5.3.4)

Questo campo DEVE essere presente e DEVE essere conforme alle specifiche della clausola 5.3.4 delle TS 119 612.

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

Un paese PUÒ avere organismi distinti di supervisione/accreditamento e anche altri organismi incaricati delle attività operative correlate. Spetta a ciascuno Stato membro designare il gestore del regime relativo al suo elenco di fiducia. L'organismo di supervisione, l'organismo di accreditamento e il gestore del regime (qualora si tratti di organismi distinti) devono avere ciascuno i propri compiti e responsabilità.

Le situazioni in cui la responsabilità della supervisione, dell'accreditamento e degli aspetti operativi è attribuita a organismi diversi DEVONO essere sempre indicate come tali nelle informazioni sul regime inserite nell'elenco di fiducia, comprese le informazioni specifiche sul regime riportate nel campo «*Scheme information URI*» (clausola 5.3.7).

Scheme name (clausola 5.3.6)

Questo campo DEVE essere presente e DEVE essere conforme alle specifiche della clausola 5.3.6 delle TS 119 612 e per il regime DEVE essere usata la seguente denominazione:

«EN_name_value» = «Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures».

[IT: «Elenco dello status di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte del gestore del regime dello Stato membro di cui in riferimento ai fini del controllo della conformità alle pertinenti disposizioni della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche»].

Scheme information URI (clausola 5.3.7)

Questo campo DEVE essere presente e DEVE essere conforme alle specifiche della clausola 5.3.7 delle TS 119 612; le «informazioni appropriate sul regime» DEVONO includere come minimo:

— informazioni introduttive generali, comuni a tutti gli Stati membri, relative all'ambito di applicazione e al contesto dell'elenco di fiducia e al/ai regime/i soggiacente/i di supervisione/accreditamento. Il testo comune da utilizzare è il testo seguente, in cui la stringa di caratteri «[*nome del pertinente Stato membro*]» DEVE essere sostituita dal nome dello Stato membro interessato:

«Il presente elenco è «L'elenco di fiducia dei prestatori di servizi di certificazione soggetti a supervisione/accreditamento» contenente informazioni sullo status di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione (CSP) soggetti a supervisione/accreditamento da parte di [*nome del pertinente Stato membro*] ai fini del controllo della conformità alle pertinenti disposizioni della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

L'elenco di fiducia ha l'obiettivo di:

— elencare e fornire informazioni affidabili sullo status di supervisione/accreditamento dei servizi di certificazione forniti dai prestatori di servizi di certificazione soggetti a supervisione/accreditamento da parte di [*nome del pertinente Stato membro*] ai fini del controllo della conformità alle pertinenti disposizioni della direttiva 1999/93/CE,

— consentire la convalida sicura delle firme elettroniche basate sui servizi di certificazione elencati soggetti a supervisione/accreditamento forniti dai CSP che figurano nell'elenco.

L'elenco di fiducia di uno Stato membro fornisce, come minimo, informazioni sui CSP soggetti a supervisione/accreditamento che rilasciano certificati qualificati conformemente alle disposizioni della direttiva 1999/93/CE [articolo 3, paragrafi 2 e 3, e articolo 7, paragrafo 1, lettera a)], comprese, qualora non siano incluse nei certificati qualificati, informazioni sui certificati qualificati su cui si basa la firma elettronica, precisando se la firma è generata o no da un dispositivo per la creazione di una firma sicura.

I CSP che rilasciano certificati qualificati (QC) inseriti nel presente elenco sono soggetti alla supervisione di [*nome del pertinente Stato membro*] e possono anche essere accreditati ai fini del controllo della conformità alle 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). Il regime di «supervisione» (o il regime di «accreditamento facoltativo») applicabile è definito dalla direttiva 1999/93/CE, di cui deve rispettare le pertinenti disposizioni, in particolare le disposizioni dell'articolo 3, paragrafo 3, dell'articolo 8, paragrafo 1, e dell'articolo 11 (o, rispettivamente, articolo 2, punto 13, articolo 3, paragrafo 2, articolo 7, paragrafo 1, lettera a), articolo 8, paragrafo 1, articolo 11).

Informazioni supplementari relative ad altri CSP soggetti a supervisione/accreditamento che non rilasciano QC ma che forniscono servizi connessi con le firme elettroniche (ad esempio CSP che forniscono servizi di marcatura temporale e che rilasciano *token* di marca temporale, CPS che rilasciano certificati non qualificati ecc.) sono inserite nell'elenco di fiducia a livello nazionale su base facoltativa.»;

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

  — informazioni sul regime 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 regime 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 ognuno 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 per sottoporsi a supervisione/accreditamento,

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

— se pertinente, informazioni dettagliate sulle «qualificazioni» specifiche che alcuni degli oggetti fisici o binari (logici) generati o emessi a seguito della fornitura di un servizio di certificazione possono ricevere, sulla base della loro conformità alle disposizioni e ai requisiti fissati a livello nazionale, indicando il significato delle «qualificazioni» e le disposizioni e i requisiti nazionali a esse associati.

Ulteriori informazioni specifiche, a livello degli Stati membri, relative al regime POSSONO essere fornite su base facoltativa, tra cui:

— informazioni sui criteri e sulle norme per la selezione dei supervisori/revisori e sulle modalità con cui i CSP vengono da loro supervisionati (controllati) o accreditati (sottoposti ad audit),

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

Scheme type/community/rules (clausola 5.3.9)

Questo campo DEVE essere presente e DEVE essere conforme alle specifiche della clausola 5.3.9 delle TS 119 612 e DEVE includere almeno due URI:

— un URI comune a tutti gli elenchi di fiducia degli Stati membri che punta verso un testo esplicativo che DEVE essere applicabile a tutti gli elenchi di fiducia:

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

  Testo esplicativo:

  Partecipazione ad un regime

  Ogni Stato membro deve creare un «elenco di fiducia dei prestatori di servizi di certificazione soggetti a supervisione/accreditamento» contenente informazioni sullo status di supervisione/accreditamento dei servizi di certificazione dei prestatori di servizi di certificazione (CSP) soggetti a supervisione/accreditamento da parte dello Stato membro ai fini del controllo della conformità alle pertinenti disposizioni della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

  La presente attuazione degli elenchi di fiducia deve essere referenziata anche nell'elenco di link (puntatori) verso l'elenco di fiducia di ogni Stato membro, redatto dalla Commissione europea.

  Politiche/regole per la valutazione dei servizi inseriti nell'elenco

  L'elenco di fiducia di uno Stato membro deve fornire, come minimo, informazioni sui CSP soggetti a supervisione/accreditamento che rilasciano certificati qualificati conformemente alle disposizioni della direttiva 1999/93/CE [articolo 3, paragrafi 2 e 3, e articolo 7, paragrafo 1, lettera a)], comprese informazioni sui certificati qualificati (QC) su cui si basa la firma elettronica, precisando se la firma è generata o no da un dispositivo per la creazione di una firma sicura.

([1]) Le ultime due serie di informazioni rivestono importanza cruciale per le parti che fanno affidamento sui certificati, in quanto consentono loro di valutare il livello di qualità e di sicurezza dei sistemi di supervisione/accreditamento applicabili ai CSP che non rilasciano QC. 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, testo comune a tutti gli Stati membri) e «*TSL policy/legal notice*» (clausola 5.3.11, testo comune a tutti gli Stati membri che fa riferimento alla direttiva 1999/93/CE, con la possibilità per ciascuno Stato membro di aggiungere testi/riferimenti ad esso specifici). 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).

I CSP che rilasciano certificati qualificati (QC) devono essere soggetti alla supervisione dello Stato membro in cui sono stabiliti (se sono stabiliti in uno Stato membro) e possono anche essere accreditati ai fini del controllo della conformità alle 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 accreditati in uno Stato membro devono comunque essere soggetti al pertinente regime di supervisione vigente in tale Stato membro, salvo il caso in cui non siano stabiliti nello stesso. Il regime di «supervisione» (o il regime di «accreditamento facoltativo») applicabile è definito dalla direttiva 1999/93/CE, di cui deve rispettare le pertinenti disposizioni, in particolare le disposizioni dell'articolo 3, paragrafo 3, dell'articolo 8, paragrafo 1, e dell'articolo 11 (o, rispettivamente, articolo 2, punto 13), articolo 3, paragrafo 2, articolo 7, paragrafo 1, lettera a), articolo 8, paragrafo 1, e articolo 11).

Informazioni supplementari relative ad 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 CSP che forniscono servizi di marcatura temporale e che rilasciano *token* di marca temporale, CPS che rilasciano certificati non qualificati ecc.) possono essere inserite nell'elenco di fiducia a livello nazionale su base facoltativa.

I CPS che non rilasciano QC ma che forniscono servizi accessori possono rientrare nel regime di «accreditamento facoltativo» (quale definito dalla direttiva 1999/93/CE e in conformità alla stessa) e/o in un «regime di approvazione riconosciuto» definito e attuato su base nazionale ai fini del controllo della conformità alle disposizioni della direttiva 1999/93/CE ed eventualmente alle disposizioni della normativa nazionale in materia di prestazione di servizi di certificazione (secondo la definizione di cui all'articolo 2, punto 11), della direttiva 1999/93/CE). Alcuni degli oggetti fisici o binari (logici) generati o emessi a seguito della prestazione di un servizio di certificazione possono ricevere una «qualificazione» specifica sulla base della loro conformità alle disposizioni e ai requisiti fissati a livello nazionale, ma è probabile che la portata di tale qualificazione sia limitata esclusivamente al livello nazionale.

Interpretazione dell'elenco di fiducia

Gli **orientamenti generali per l'utilizzazione** di applicazioni, servizi o prodotti relativi alla firma elettronica basati su un elenco di fiducia conforme all'allegato della decisione della Commissione [riferimento alla presente decisione] sono i seguenti:

la voce «*Service type identifier*» («Sti») «CA/QC» (e analogamente la voce «CA/QC» ulteriormente qualificata come «*RootCA/QC*» mediante l'uso dell'estensione «*additional Service Information*» della «*Service Information Extension*» («Sie»)]

— indica che tutti i certificati entità finale rilasciati dalla CA identificata mediante il «*Service digital identifier*» («Sdi») (e analogamente all'interno della gerarchia CA, partendo dalla CA radice identificata dall'«Sdi») del CSP corrispondente (cfr. campi associati delle informazioni sul TSP) sono certificati qualificati (QC), **purché** ciò sia indicato nel certificato mediante l'uso di opportune dichiarazioni QC definite dalla EN 319 412-5 (ossia *QcCompliance*, QcSSCD ecc.) e/o OID QCP(+) definiti dalla EN 319 411-2 (e che ciò sia garantito dal CSP emittente e assicurato dall'organismo di supervisione/accreditamento dello Stato membro).

Nota: se non è presente alcuna informazione nel campo «*Qualification Extension*» della «Sie» o se un certificato entità finale presentato come QC non è ulteriormente identificato da un'informazione correlata nel campo «*Qualification Extension*» della «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 il non uso) delle opportune dichiarazioni QC definite dall'ETSI (ovvero *QcCompliance*, QcSSCD ecc.) e/o OID QCP(+) definiti dall'ETSI è garantito come conforme a quanto indicato dal CSP che rilascia QC,

— **e SE** è presente un'informazione nel campo «*Qualification Extension*» della «Sie», in aggiunta alle regole interpretative di cui sopra relative all'uso standard, i certificati identificati mediante l'uso di questa informazione del campo «*Qualification Extension*» della «Sie», costruita sul principio di una sequenza di filtri che identificano ulteriormente una serie di certificati, devono essere considerati sulla base dei «qualificatori» associati che forniscono informazioni supplementari sullo status qualificato, sul «supporto SSCD» e/o sulla «persona giuridica come soggetto» (ad esempio i certificati che contengono un OID specifico nell'estensione della politica dei certificati e/o che hanno uno specifico modello di «utilizzazione della chiave» e/o che sono filtrati mediante l'uso di un valore specifico che compare in un campo o in un'estensione specifici del certificato ecc.). I predetti «qualificatori» rientrano nella seguente serie di «*Qualifiers*» utilizzati per compensare la mancanza di informazioni nel corrispondente contenuto dei QC e, rispettivamente:

— per indicare lo status qualificato: «QCStatement», indicante che il/i certificato/i individuato/i è/sono qualificato/i,

E/O

— per indicare la natura del supporto SSCD:

— «QCWithSSCD», avente il significato di «QC basato su un SSCD», oppure

— «QCNoSSCD», avente il significato «QC non basato su un SSCD», oppure

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

E/O

— per indicare il rilascio ad una persona giuridica:

— «QCForLegalPerson», avente il significato di «certificato rilasciato ad una persona giuridica».

La regola interpretativa generale per ogni altra voce di tipo «Sti» prescrive che il servizio elencato denominato secondo il valore del campo «Sn» e identificato in modo univoco dal valore del campo «Sdi» abbia uno status attuale di supervisione/accreditamento conforme al valore del campo «Scs» a decorrere dalla data indicata nel campo «*Current status starting date and time*». Le regole di interpretazione specifiche per tutte le informazioni supplementari sul servizio elencato (ad esempio il campo «*Service information extensions*») sono disponibili, se del caso, all'URI specifico dello Stato membro come parte del presente campo «*Scheme type/community/rules*».

Per ulteriori dettagli sui campi, per la descrizione e per il significato degli elenchi di fiducia degli Stati membri si rinvia alle specifiche tecniche del modello comune per l'«elenco di fiducia dei prestatori di servizi di certificazione soggetti a supervisione/accreditamento» di cui all'allegato della decisione 2009/767/CE della Commissione,

— un URI specifico per l'elenco di fiducia di ogni Stato membro che punti verso un testo descrittivo che DEVE essere applicabile all'elenco di fiducia dello Stato membro:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC dove «CC» = codice paese ISO 3166-1 ([1]) alpha-2 utilizzato nel campo «*Scheme territory*» (clausola 5.3.10)

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

— che fornisce agli utilizzatori una descrizione specifica del modo in cui usare e interpretare il contenuto dell'elenco di fiducia per quanto riguarda i servizi di certificazione non connessi con il rilascio di QC. Questo testo può essere utilizzato per indicare che i regimi nazionali di supervisione/accreditamento possono applicare un diverso trattamento ai CSP che non rilasciano QC e per specificare il modo in cui i campi «*Scheme service definition URI*» (clausola 5.5.6) e «*Service information extension*» (clausola 5.5.9) possono essere usati a tal fine.

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

TSL policy/legal notice (clausola 5.3.11)

Questo campo DEVE essere presente e DEVE essere conforme alle specifiche della clausola 5.3.11 delle TS 119 612: l'avviso legale/sulla politica concernente lo status giuridico del regime o i requisiti giuridici soddisfatti dal regime nell'ordinamento in cui è stabilito e/o eventuali limitazioni e condizioni ai sensi delle quali l'elenco di fiducia è tenuto e pubblicato DEVE essere una stringa di caratteri multilingue (solo testo) divisa in due parti:

1. una prima parte obbligatoria comune a tutti gli elenchi di fiducia degli Stati membri (con l'inglese britannico come lingua obbligatoria ed eventualmente una o più lingue nazionali), indicante che il quadro normativo applicabile è la direttiva 1999/93/CE e i corrispondenti atti di attuazione nell'ordinamento dello Stato membro indicato 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 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

([1]) ISO 3166-1:2006: «*Codes for the representation of names of countries and their subdivisions Part 1: Country codes*».

Testo nella o nelle lingue ufficiali degli Stati membri: (traduzione ufficiale del testo in lingua inglese riportato sopra: «Il quadro normativo di riferimento per la presente applicazione TSL dell'elenco di fiducia dei prestatori di servizi di certificazione soggetti a supervisione/accreditamento per [nome del pertinente Stato membro] è la direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche e i corrispondenti provvedimenti di attuazione nell'ordinamento di [nome del pertinente Stato membro].)»;

2. una seconda parte facoltativa, specifica per ogni elenco di fiducia (con l'inglese britannico come lingua obbligatoria ed 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).

CAPITOLO II

CONTINUITÀ DEGLI ELENCHI DI FIDUCIA

I certificati che devono essere notificati alla Commissione a norma dell'articolo 3, lettera c), della presente decisione DEVONO essere rilasciati in modo tale da:

— presentare date di validità sfasate almeno di tre mesi,

— essere creati su nuove coppie di chiavi, perché non possono essere ricertificate coppie di chiavi utilizzate in precedenza.

In caso di compromissione o disattivazione di UNA delle chiavi private corrispondenti alla chiave pubblica che potrebbe essere usata per convalidare la firma dell'elenco di fiducia e che è stata notificata alla Commissione e pubblicata negli elenchi centrali di puntatori della Commissione, gli Stati membri:

— ripubblicano, senza indugio, un nuovo elenco di fiducia firmato con una chiave privata non compromessa, nel caso in cui l'elenco di fiducia pubblicato sia stato firmato con una chiave privata compromessa o disattivata,

— notificano tempestivamente alla Commissione il nuovo elenco di certificati a chiave pubblica corrispondenti alle chiavi private che potrebbero essere utilizzate per firmare gli elenchi di fiducia.

In caso di compromissione o disattivazione di TUTTE le chiavi private corrispondenti alle chiavi pubbliche che potrebbero essere usate per convalidare la firma dell'elenco di fiducia e che sono state notificate alla Commissione e pubblicate negli elenchi centrali di puntatori della Commissione, gli Stati membri:

— generano nuove coppie di chiavi che potrebbero essere utilizzate per firmare gli elenchi di fiducia e i corrispondenti certificati a chiave pubblica,

— ripubblicano, senza indugio, un nuovo elenco di fiducia firmato con una delle nuove chiavi private e il cui corrispondente certificato a chiave pubblica deve essere notificato,

— notificano tempestivamente alla Commissione il nuovo elenco di certificati a chiave pubblica corrispondenti alle chiavi private che potrebbero essere usate per firmare gli elenchi di fiducia.

CAPITOLO III

SPECIFICHE PER IL FORMATO LEGGIBILE ALL'UOMO DELL'ELENCO DI FIDUCIA

Il formato leggibile all'uomo (HR) dell'elenco di fiducia elaborato e pubblicato DOVREBBE essere fornito sotto forma di documento PDF (*Portable Document Format*) conforme a ISO 32000 ([1]) che DEVE essere formattato conformemente al profilo PDF/A (ISO 19005 ([2])).

Il contenuto del formato HR basato su PDF/A dell'elenco di fiducia DOVREBBE soddisfare i seguenti requisiti:

— la struttura del formato HR DOVREBBE riflettere il modello logico descritto nelle TS 119 612;

— 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, (ad esempio «autorità di certificazione che rilascia certificati a chiave pubblica»),

  — se del caso, versioni in più lingue naturali secondo quanto previsto nell'elenco di fiducia,

([1]) ISO 32000-1:2008: *Document management — Portable document format — Part 1: PDF 1.7*.
([2]) ISO 19005-2:2011: *Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2)*.

— i seguenti campi e i corrispondenti valori dei certificati digitali presenti nel campo «Service digital identity» DOVREBBERO essere come minimo presenti nel formato HR:

  — versione (*Version*)

  — numero di serie (*Serial number*)

  — algoritmo di firma (*Signature algorithm*)

  — emittente (*Issuer*)

  — valido da (*Valid from*)

  — valido fino a (*Valid to*)

  — soggetto (*Subject*)

  — chiave pubblica (*Public key*)

  — politiche dei certificati (*Certificate Policies*)

  — identificativo della chiave del soggetto (*Subject Key Identifier*)

  — punti di distribuzione CRL (*CRL Distribution Points*)

  — identificativo della chiave dell'autorità (*Authority Key Identifier*)

  — utilizzazione della chiave (*Key Usage*)

  — limitazioni di base (*Basic constraints*)

  — algoritmo dell'impronta digitale (*Thumbprint algorithm*)

  — impronta digitale (*Thumbprint*),

— il formato HR DOVREBBE essere facile da stampare,

— il formato HR DEVE essere firmato dal gestore del regime secondo il *PAdES Signatures baseline profile* ([1]).

([1]) ETSI TS 103 172 (marzo 2012) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile