REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 23 luglio 2014

in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, dovuta in particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.

(2) Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.

(3) La direttiva 1999/93/CE del Parlamento europeo e del Consiglio ([3]) trattava le firme elettroniche senza fornire un quadro transfrontaliero e transettoriale completo per transazioni elettroniche sicure, affidabili e di facile impiego. Il presente regolamento rafforza ed estende l'acquis di tale direttiva.

(4) La comunicazione della Commissione del 26 agosto 2010, dal titolo «Agenda digitale europea» ha individuato nella frammentazione del mercato digitale, nella mancanza di interoperabilità e nell'aumento della criminalità cibernetica i grandi ostacoli al circolo virtuoso dell'economia digitale. Nella relazione 2010 sulla cittadinanza dell'UE, intitolata «Eliminare gli ostacoli all'esercizio dei diritti dei cittadini dell'Unione», la Commissione ha ulteriormente sottolineato la necessità di risolvere i principali problemi che impediscono ai cittadini dell'Unione di godere dei vantaggi di un mercato unico digitale e di servizi digitali transfrontalieri.

(5) Nelle conclusioni del 4 febbraio 2011 e del 23 ottobre 2011 il Consiglio europeo ha invitato la Commissione a creare un mercato unico digitale entro il 2015, a fare rapidi progressi in settori essenziali dell'economia digitale e a promuovere un mercato unico digitale pienamente integrato favorendo l'impiego transfrontaliero dei servizi online, con particolare riguardo all'agevolazione dell'identificazione e dell'autenticazione elettronica sicura.

(6) Nelle conclusioni del 27 maggio 2011, il Consiglio ha invitato la Commissione a contribuire al mercato unico digitale creando le condizioni adatte per il riconoscimento reciproco

transfrontaliero di funzioni essenziali quali l'identificazione elettronica, i documenti elettronici, le firme elettroniche e i servizi elettronici di recapito, nonché per l'interoperabilità dei servizi di eGovernment in tutta l'Unione europea.

(7) Nella risoluzione del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico ([4]), il Parlamento europeo ha sottolineato l'importanza della sicurezza dei servizi elettronici, in particolare delle firme elettroniche, e della necessità di creare un'infrastruttura pubblica essenziale a livello paneuropeo ed ha invitato la Commissione ad allestire un Portale europeo delle autorità di convalida per garantire l'interoperabilità transfrontaliera delle firme elettroniche e per aumentare la sicurezza delle transazioni effettuate utilizzando Internet.

(8) La direttiva 2006/123/CE del Parlamento europeo e del Consiglio ([5]) dispone che gli Stati membri creino «sportelli unici» per garantire che tutte le procedure e formalità relative all'accesso a un'attività di servizi ed al suo svolgimento possano essere facilmente espletate a distanza ed elettronicamente attraverso lo sportello unico corrispondente e con le autorità competenti. Numerosi servizi online accessibili presso gli sportelli unici richiedono l'identificazione, l'autenticazione e la firma elettroniche.

(9) In molti casi i cittadini non possono valersi della loro identificazione elettronica per autenticarsi in un altro Stato membro perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti in altri Stati membri. Tale barriera elettronica impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno. Disporre di mezzi di identificazione elettronica riconosciuti reciprocamente permetterà di agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di operare su base transfrontaliera evitando molti ostacoli nelle interazioni con le autorità pubbliche.

(10) La direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([6]) istituisce una rete di autorità nazionali responsabili dell'assistenza sanitaria online. Per migliorare la sicurezza e la continuità dell'assistenza sanitaria transfrontaliera, tale rete deve elaborare orientamenti sull'accesso transfrontaliero ai dati e ai servizi elettronici, anche sostenendo «misure comuni di identificazione e autenticazione per agevolare la trasferibilità dei dati nell'assistenza sanitaria transfrontaliera». Il riconoscimento reciproco dell'identificazione e dell'autenticazione elettronica è un fattore essenziale per realizzare l'assistenza sanitaria transfrontaliera per i cittadini europei. Quando i cittadini viaggiano per ottenere assistenza medica, la loro cartella clinica deve essere accessibile nel paese in cui si sottopongono alle cure. Ciò richiede un quadro di identificazione elettronica solido, sicuro e affidabile.

(11) Il presente regolamento dovrebbe essere applicato nel pieno rispetto dei principi relativi alla protezione dei dati personali ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio ([7]). A tale riguardo, per quanto concerne il principio del riconoscimento reciproco stabilito dal presente regolamento, l'autenticazione in un servizio online dovrebbe riguardare esclusivamente il trattamento di dati di identificazione che siano adeguati, pertinenti e non eccedenti per garantire l'accesso a detto servizio online. Inoltre, gli obblighi previsti dalla direttiva 95/46/CE in materia di riservatezza e sicurezza dei trattamenti dovrebbero essere rispettati dai prestatori di servizi fiduciari e dagli organismi di vigilanza.

(12) Un obiettivo del presente regolamento è l'eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici. Il presente regolamento non intende intervenire riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli

Stati membri. Lo scopo del presente regolamento è garantire che per accedere ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

(13) È opportuno che gli Stati membri rimangano liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica, e che possano decidere dell'eventuale partecipazione del settore privato nell'offerta di tali mezzi. È opportuno che gli Stati membri non abbiano l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione. Spetta agli Stati membri decidere se notificare alla Commissione tutti, alcuni o nessuno dei regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici.

(14) Occorre che il presente regolamento fissi talune condizioni in merito all'obbligo di riconoscimento dei mezzi di identificazione elettronica e alle modalità di notifica dei regimi di identificazione elettronica. È opportuno che tali condizioni aiutino gli Stati membri a costruire la necessaria fiducia nei rispettivi regimi di identificazione elettronica e a riconoscere reciprocamente i mezzi di identificazione elettronica che fanno parte dei regimi notificati. È opportuno che il principio del riconoscimento reciproco si applichi ove il regime di identificazione elettronica dello Stato membro notificante soddisfi le condizioni di notifica e la notifica sia stata pubblicata nella *Gazzetta ufficiale dell'Unione europea*. Tuttavia, il principio del riconoscimento reciproco dovrebbe riguardare esclusivamente l'autenticazione nei servizi online. È opportuno che l'accesso a tali servizi online e la loro fornitura finale al richiedente siano strettamente collegati al diritto a usufruire di tali servizi alle condizioni fissate nel diritto nazionale.

(15) L'obbligo di riconoscere i mezzi di identificazione elettronica dovrebbe riferirsi esclusivamente ai mezzi il cui livello di garanzia dell'identità corrisponde a un livello pari o superiore a quello richiesto per il servizio online in questione. Inoltre, tale obbligo dovrebbe applicarsi solo qualora l'organismo del settore pubblico in questione utilizzi il livello di garanzia «significativo» o «elevato» in relazione all'accesso a tale servizio online. È opportuno che gli Stati membri mantengano la libertà, conformemente al diritto comunitario, di riconoscere mezzi di identificazione elettronica aventi livelli di garanzia dell'identità inferiori.

(16) I livelli di garanzia dovrebbero caratterizzare il grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata. Il livello di garanzia dipende dal grado di sicurezza fornito dai mezzi di identificazione elettronica riguardo all'identità pretesa o dichiarata di una persona tenendo conto dei procedimenti (ad esempio, controllo e verifica dell'identità, e autenticazione), delle attività di gestione (ad esempio, l'entità che rilascia i mezzi di identificazione elettronica e la procedura di rilascio di tali mezzi) e dei controlli tecnici messi in atto. Come risultato dei progetti pilota su larga scala finanziati dall'Unione, della normazione e di attività a livello internazionale, esistono varie definizioni e descrizioni tecniche dei livelli di garanzia. In particolare, il progetto pilota su larga scala STORK e la norma ISO 29115 fanno riferimento, tra l'altro, ai livelli 2, 3 e 4, che dovrebbero essere tenuti nella massima considerazione all'atto di stabilire le norme, le procedure e i requisiti tecnici minimi per i livelli di garanzia basso, significativo ed elevato ai sensi del presente regolamento, assicurando al contempo l'applicazione coerente del presente regolamento in particolare per quanto riguarda il livello di garanzia elevato in relazione al controllo dell'identità ai fini del rilascio di certificati qualificati. I requisiti stabiliti dovrebbero essere

neutrali dal punto di vista tecnologico. Dovrebbe essere possibile soddisfare i requisiti di sicurezza necessari attraverso tecnologie differenti.

(17) È opportuno che gli Stati membri incoraggino il settore privato a impiegare volontariamente mezzi di identificazione elettronica nell'ambito di un regime notificato a fini di identificazione ove necessario per servizi online o transazioni elettroniche. La facoltà di ricorrere a tali mezzi di identificazione elettronica consentirebbe al settore privato di avvalersi dell'identificazione e autenticazione elettroniche già ampiamente impiegate in molti Stati membri almeno per i servizi pubblici e di agevolare alle imprese e ai cittadini l'accesso transfrontaliero ai loro servizi online. Per facilitare l'impiego transfrontaliero di tali mezzi di identificazione elettronica da parte del settore privato, è opportuno che la possibilità di autenticazione offerta da uno Stato membro sia disponibile alle parti del settore privato facenti affidamento sulla certificazione stabilite al di fuori del territorio di detto Stato membro alle stesse condizioni applicate alle parti del settore privato facenti affidamento sulla certificazione stabilite nel suddetto Stato membro. Di conseguenza, per quanto riguarda le parti del settore privato facenti affidamento sulla certificazione, lo Stato membro notificante può definire termini di accesso ai mezzi di autenticazione. Detti termini di accesso possono indicare se i mezzi di autenticazione relativi al regime notificato sono attualmente disponibili alle parti del settore privato facenti affidamento sulla certificazione.

(18) Il presente regolamento dovrebbe prevedere la responsabilità dello Stato membro notificante, della parte che rilascia i mezzi di identificazione elettronica e della parte che gestisce la procedura di autenticazione per mancato rispetto degli obblighi pertinenti a norma del presente regolamento. Tuttavia, il presente regolamento dovrebbe essere applicato conformemente alle norme nazionali in materia di responsabilità. Pertanto esso non pregiudica tali norme nazionali in ordine, ad esempio, alla definizione dei danni o alle pertinenti norme procedurali applicabili, incluso l'onere della prova.

(19) La sicurezza dei regimi di identificazione elettronica è fondamentale per un affidabile riconoscimento reciproco transfrontaliero dei mezzi di identificazione elettronica. In tale contesto, gli Stati membri dovrebbero cooperare in materia di sicurezza e interoperabilità dei regimi di identificazione elettronica a livello dell'Unione. Ogniqualvolta i regimi di identificazione elettronica richiedano alle parti che fanno affidamento sulla certificazione di utilizzare hardware o software specifici a livello nazionale, l'interoperabilità transfrontaliera richiede che tali Stati membri non impongano tali requisiti e le spese relative alle parti facenti affidamento sulla certificazione stabilite al di fuori del loro territorio. In tal caso si dovrebbero esaminare ed elaborare soluzioni appropriate nell'ambito del quadro di interoperabilità. Tuttavia, sono inevitabili i requisiti tecnici derivanti dalle specifiche inerenti ai mezzi di identificazione elettronica nazionali e suscettibili di avere ripercussioni per i detentori di tali mezzi elettronici (ad esempio, le smart card).

(20) È opportuno che la cooperazione degli Stati membri agevoli l'interoperabilità tecnica dei regimi di identificazione elettronica notificati, al fine di promuovere un elevato livello di fiducia e sicurezza, in funzione del grado di rischio. È opportuno che lo scambio di informazioni e la condivisione delle migliori prassi fra Stati membri, finalizzati al riconoscimento reciproco dei regimi, facilitino tale cooperazione.

(21) È anche opportuno che il presente regolamento istituisca un quadro giuridico generale per l'impiego dei servizi fiduciari. Tuttavia, non è opportuno che istituisca un obbligo generale di farne uso o che installi un punto di accesso per tutti i servizi fiduciari esistenti. In particolare, non è auspicabile che il regolamento copra la prestazione di servizi fiduciari usati esclusivamente nell'ambito di sistemi chiusi da un insieme definito di partecipanti che

non hanno ripercussioni su terzi. Ad esempio, i sistemi istituiti in imprese o amministrazioni pubbliche per la gestione delle procedure interne che fanno uso di servizi fiduciari non dovrebbero essere soggetti ai requisiti previsti dal presente regolamento. Solo i servizi fiduciari prestati al pubblico aventi ripercussioni su terzi dovrebbero soddisfare i requisiti previsti dal presente regolamento. Non è neanche auspicabile che il presente regolamento copra aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici nei casi in cui la normativa nazionale o unionale stabilisca obblighi quanto alla forma. Inoltre, non dovrebbe avere ripercussioni sugli obblighi di forma nazionali relativi ai registri pubblici, in particolare i registri commerciali e catastali.

(22) Al fine di contribuire al loro impiego transfrontaliero generale, è opportuno che sia possibile utilizzare i servizi fiduciari come prove in procedimenti giudiziali in tutti gli Stati membri. Spetta al diritto nazionale definire gli effetti giuridici dei servizi fiduciari, salvo che il presente regolamento provveda altrimenti.

(23) Nella misura in cui il presente regolamento disponga l'obbligo di riconoscere un servizio fiduciario, tale servizio fiduciario può essere rifiutato solo qualora il destinatario dell'obbligo non sia in grado di leggerlo o verificarlo per motivi tecnici che sfuggono al suo immediato controllo. Tuttavia, tale obbligo non dovrebbe di per se stesso esigere che un organismo pubblico ottenga l'hardware e il software necessari per la leggibilità tecnica di tutti i servizi fiduciari esistenti.

(24) Gli Stati membri possono mantenere o introdurre disposizioni nazionali, conformemente al diritto dell'Unione, in materia di servizi fiduciari, nella misura in cui detti servizi non siano pienamente armonizzati dal presente regolamento. Tuttavia, i servizi fiduciari conformi al presente regolamento dovrebbero godere della libera circolazione nel mercato interno.

(25) È opportuno che gli Stati membri mantengano la libertà di definire altri tipi di servizi fiduciari oltre a quelli inseriti nell'elenco ristretto di servizi fiduciari di cui al presente regolamento, ai fini del loro riconoscimento a livello nazionale quali servizi fiduciari qualificati.

(26) In considerazione del ritmo dei mutamenti tecnologici, occorre che il presente regolamento adotti un approccio aperto all'innovazione.

(27) È opportuno che il presente regolamento sia neutrale sotto il profilo tecnologico. È auspicabile che gli effetti giuridici prodotti dal presente regolamento siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti.

(28) Al fine di migliorare in particolare la fiducia delle piccole e medie imprese (PMI) e dei consumatori nel mercato interno e di promuovere l'impiego dei servizi e prodotti fiduciari, è opportuno introdurre le nozioni di servizi fiduciari qualificati e di prestatori di servizi fiduciari qualificati, per precisare i requisiti e gli obblighi che garantiscano un elevato livello di sicurezza di tutti i servizi e prodotti fiduciari qualificati impiegati o prestati.

(29) In linea con gli obblighi assunti a norma della Convenzione delle Nazioni Unite per i diritti delle persone con disabilità, approvata con decisione 2010/48/CE del Consiglio ([8]), in particolare l'articolo 9 della Convenzione, le persone con disabilità dovrebbero poter utilizzare servizi fiduciari e prodotti destinati al consumatore finale impiegati nella prestazione di tali servizi alle stesse condizioni degli altri consumatori. Ove fattibile, pertanto, i servizi fiduciari prestati e i prodotti destinati all'utilizzatore finale impiegati per la prestazione di detti servizi dovrebbero essere resi accessibili alle persone con disabilità. La valutazione di fattibilità dovrebbe includere considerazioni tecniche ed economiche.

(30)Gli Stati membri dovrebbero designare uno o più organismi di vigilanza per lo svolgimento delle attività di vigilanza previste dal presente regolamento. Gli Stati membri dovrebbero altresì avere facoltà di decidere, di comune accordo con un altro Stato membro, di designare un organismo di vigilanza nel territorio di tale altro Stato membro.

(31)Gli organismi di vigilanza dovrebbero cooperare con le autorità di protezione dei dati, ad esempio informandole in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali. In particolare, è opportuno che la trasmissione di informazioni copra gli incidenti di sicurezza e le violazioni dei dati personali.

(32)È opportuno che tutti i prestatori di servizi fiduciari adottino buone prassi di sicurezza in funzione dei rischi connessi con le loro attività, in modo da migliorare la fiducia degli utilizzatori nel mercato unico.

(33)È opportuno che le disposizioni sull'uso degli pseudonimi nei certificati non impediscano agli Stati membri di chiedere l'identificazione delle persone in base alla normativa unionale o nazionale.

(34)È opportuno che tutti gli Stati membri si adeguino a requisiti essenziali comuni di vigilanza per garantire un livello paragonabile di sicurezza dei servizi fiduciari qualificati. Per facilitare l'applicazione coerente di tali requisiti in tutta l'Unione occorre che gli Stati membri adottino procedure paragonabili e scambino informazioni sulle loro attività di vigilanza e sulle migliori prassi del settore.

(35)Tutti i prestatori di servizi fiduciari dovrebbero essere soggetti ai requisiti del presente regolamento, in particolare a quelli in materia di sicurezza e responsabilità, al fine di garantire la dovuta diligenza, la trasparenza e l'attendibilità delle loro operazioni e servizi. Tuttavia, tenendo conto del tipo di servizi fornito dai prestatori di servizi fiduciari, per quanto riguarda tali requisiti è opportuno distinguere tra servizi fiduciari qualificati e non qualificati.

(36)L'istituzione di un regime di vigilanza per tutti i prestatori di servizi fiduciari dovrebbe assicurare parità di condizioni per la sicurezza e l'attendibilità delle loro operazioni e servizi, contribuendo in tal modo alla tutela degli utenti e al funzionamento del mercato interno. I prestatori di servizi fiduciari non qualificati dovrebbero essere soggetti ad attività di vigilanza ex post semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni. Pertanto l'organismo di sorveglianza non dovrebbe avere un obbligo generale di vigilanza sui prestatori di servizi non qualificati. L'organismo di sorveglianza dovrebbe adottare misure solo quando viene informato (ad esempio, dallo stesso prestatore di servizi fiduciari non qualificati, da un altro organismo di sorveglianza, mediante la notifica di un utente o di un partner commerciale o in base a sue indagine proprie) che un prestatore di servizi fiduciari non qualificato non soddisfa i requisiti del presente regolamento.

(37)Il presente regolamento dovrebbe prevedere la responsabilità di tutti i prestatori di servizi fiduciari. In particolare, stabilisce il regime di responsabilità in base al quale tutti i prestatori di servizi fiduciari dovrebbero essere responsabili dei danni provocati a persone fisiche o giuridiche a causa del mancato rispetto degli obblighi previsti dal presente regolamento. Al fine di agevolare la valutazione del rischio finanziario che i prestatori di servizi fiduciari possano dover sostenere o che debbano coprire con polizze assicurative, il presente regolamento autorizza i prestatori di servizi fiduciari a stabilire limiti, a talune condizioni, all'uso dei servizi da essi prestati e non essere pertanto responsabili dei danni derivanti dall'uso dei servizi oltre i suddetti limiti. I clienti dovrebbero essere debitamente e

anticipatamente informati di tali limiti. Tali limiti dovrebbero essere riconoscibili per i terzi, ad esempio inserendo informazioni sui limiti nei termini e nelle condizioni del servizio prestato o attraverso altri mezzi riconoscibili. Allo scopo di dare effetto a tali principi, il presente regolamento dovrebbe essere applicato conformemente alle norme nazionali sulla responsabilità. Pertanto, il presente regolamento non pregiudica tali norme nazionali in ordine, ad esempio, alla definizione dei danni, del dolo, della negligenza o alle pertinenti norme procedurali applicabili.

(38) La notifica delle violazioni di sicurezza e delle valutazioni di rischio per la sicurezza è essenziale per fornire informazioni adeguate alle parti interessate in caso di violazione di sicurezza o perdita di integrità.

(39) Per consentire alla Commissione e agli Stati membri di valutare l'efficacia del meccanismo di notifica delle violazioni di cui al presente regolamento, è opportuno imporre l'obbligo agli organismi di vigilanza di fornire informazioni riassuntive alla Commissione e all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

(40) Per consentire alla Commissione e agli Stati membri di valutare l'efficacia del meccanismo di vigilanza perfezionato di cui al presente regolamento, è opportuno chiedere agli organismi di vigilanza di riferire sulle loro attività. Ciò servirebbe ad agevolare lo scambio di buone prassi fra organismi di vigilanza e consentirebbe di verificare l'applicazione coerente ed efficiente dei requisiti essenziali di vigilanza in tutti gli Stati membri.

(41) Per garantire che i servizi fiduciari qualificati siano sostenibili e duraturi e migliorare la fiducia degli utilizzatori nella continuità di detti servizi, è opportuno che gli organismi di vigilanza verifichino l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nel caso in cui prestatori di servizi fiduciari qualificati cessino le loro attività.

(42) Per facilitare la vigilanza sui prestatori di servizi fiduciari qualificati, ad esempio allorché un prestatore offre i suoi servizi sul territorio di uno Stato membro in cui non è soggetto a vigilanza o qualora i computer di un prestatore siano situati nel territorio di uno Stato membro diverso da quello in cui il prestatore è stabilito, è opportuno istituire un sistema di assistenza mutua fra gli organismi di vigilanza negli Stati membri.

(43) Al fine di assicurare la conformità dei prestatori di servizi fiduciari qualificati e dei servizi da essi prestati ai requisiti stabiliti dal presente regolamento, un organismo di valutazione della conformità dovrebbe effettuare una valutazione della conformità; i prestatori di servizi fiduciari qualificati dovrebbero trasmettere all'organismo di vigilanza le relazioni di valutazione di conformità risultanti. Ogniqualvolta l'organismo di vigilanza richieda a un prestatore di servizi fiduciari qualificato di presentare una relazione di valutazione di conformità ad hoc, l'organismo di vigilanza dovrebbe rispettare in particolare i principi di buona amministrazione, compreso l'obbligo di fornire le motivazioni delle sue decisioni, nonché il principio di proporzionalità. Pertanto, l'organismo di vigilanza dovrebbe debitamente giustificare la propria decisione di imporre una valutazione di conformità ad hoc.

(44) Il presente regolamento mira a garantire un quadro coerente affinché i servizi fiduciari siano dotati di un livello elevato di sicurezza e certezza giuridica. A tale riguardo, nel trattare la valutazione di conformità di prodotti e servizi, la Commissione dovrebbe, ove opportuno, cercare sinergie con i pertinenti regimi europei e internazionali vigenti, quali il regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([9]) che sancisce gli obblighi in materia di accreditamento degli organismi di valutazione della conformità e vigilanza del mercato di prodotti.

(45)Per consentire un processo di avviamento efficiente, che conduca all'inclusione dei prestatori di servizi fiduciari qualificati e dei servizi fiduciari qualificati da essi offerti negli elenchi di fiducia, è opportuno incoraggiare interazioni preliminari fra gli aspiranti prestatori di servizi fiduciari qualificati e l'organismo di vigilanza competente, in vista di facilitare l'esercizio della dovuta diligenza nell'offerta di servizi fiduciari qualificati.

(46)Gli elenchi di fiducia sono elementi essenziali nel costruire la fiducia fra operatori di mercato perché indicano la condizione qualificata del prestatore di servizi al momento della vigilanza.

(47)La fiducia nei servizi online e la loro agevolezza sono essenziali perché gli utilizzatori possano beneficiare a pieno dei servizi elettronici e avvalersi consapevolmente di essi. A tale scopo si dovrebbe creare un marchio di fiducia UE per individuare i servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati. Tale marchio di fiducia UE per i servizi fiduciari qualificati distinguerebbe chiaramente i servizi fiduciari qualificati da altri servizi fiduciari, contribuendo così alla trasparenza sul mercato. L'utilizzo di un marchio di fiducia UE da parte dei prestatori di servizi fiduciari qualificati dovrebbe essere volontario e non dovrebbe implicare requisiti aggiuntivi diversi da quelli previsti dal presente regolamento.

(48)Sebbene sia necessario un elevato livello di sicurezza per garantire il riconoscimento reciproco delle firme elettroniche, in casi specifici come nel contesto della decisione 2009/767/CE della Commissione ([10]), è opportuno che siano accettate anche firme elettroniche con una garanzia di sicurezza più debole.

(49)Il presente regolamento dovrebbe stabilire il principio secondo il quale alla firma elettronica non dovrebbero essere negati gli effetti giuridici per il motivo della sua forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata. Tuttavia, spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal presente regolamento secondo cui una firma elettronica qualificata dovrebbe avere un effetto giuridico equivalente a quello di una firma autografa.

(50)Poiché attualmente le autorità competenti negli Stati membri utilizzano formati diversi di firme elettroniche avanzate per firmare elettronicamente i loro documenti, occorre garantire che almeno alcuni formati di firma elettronica possano essere supportati tecnicamente dagli Stati membri allorché ricevono documenti firmati elettronicamente. Analogamente, allorché le autorità competenti negli Stati membri fanno uso di sigilli elettronici, occorre garantire che supportino almeno alcuni formati di sigillo elettronico avanzato.

(51)È opportuno che il firmatario possa affidare a terzi i dispositivi per la creazione di una firma elettronica qualificata, purché siano rispettati appropriati meccanismi e procedure per garantire che il firmatario mantenga il controllo esclusivo sull'uso dei suoi dati di creazione di firma elettronica e l'uso del dispositivo soddisfi i requisiti della firma elettronica qualificata.

(52)Visti i suoi molteplici vantaggi economici, sarà ulteriormente sviluppata la creazione di firme elettroniche a distanza, qualora l'ambiente di creazione di firma elettronica sia gestito da un prestatore di servizi fiduciari a nome del firmatario. Tuttavia, per garantire che alle firme elettroniche sia attribuito lo stesso riconoscimento giuridico delle firme elettroniche create con un ambiente interamente gestito dall'utente, i prestatori che offrono servizi di firma elettronica a distanza dovrebbero applicare procedure di sicurezza di gestione e amministrative specifiche e utilizzare sistemi e prodotti affidabili, che in particolare comprendano canali di comunicazione elettronici sicuri per garantire l'affidabilità

dell'ambiente di creazione di firma elettronica e assicurare che sia utilizzato sotto il controllo esclusivo del firmatario. Nel caso di una firma elettronica qualificata creata mediante un dispositivo di creazione di firma elettronica a distanza, dovrebbero applicarsi i requisiti applicabili ai prestatori di servizi fiduciari qualificati, stabiliti dal presente regolamento.

(53) La sospensione dei certificati qualificati è una prassi operativa abituale dei prestatori di servizi fiduciari in una serie di Stati membri, che è diversa dalla revoca e comporta la perdita di validità temporanea di un certificato. La certezza del diritto richiede che la situazione di sospensione di un certificato sia sempre indicata chiaramente. A tale scopo i prestatori di servizi fiduciari dovrebbero avere la responsabilità di indicare chiaramente la situazione del certificato e, in caso di sospensione, il periodo di tempo esatto durante il quale il certificato è sospeso. È opportuno che il presente regolamento non imponga ai prestatori di servizi fiduciari o agli Stati membri l'utilizzo della sospensione, ma preveda norme di trasparenza nei casi in cui tale prassi è disponibile.

(54) L'interoperabilità transfrontaliera e il riconoscimento dei certificati qualificati è una condizione essenziale per il riconoscimento transfrontaliero delle firme elettroniche qualificate. Pertanto, i certificati qualificati non dovrebbero essere soggetti a requisiti obbligatori oltre ai requisiti di cui al presente regolamento. Tuttavia, a livello nazionale, dovrebbe essere consentita l'inclusione di attributi specifici, quali identificatori unici, nei certificati qualificati, purché tali attributi specifici non ostacolino l'interoperabilità transfrontaliera e il riconoscimento dei certificati e delle firme elettroniche qualificati.

(55) La certificazione della sicurezza delle tecnologie d'informazione basata su norme internazionali, come l'ISO 15408 e i metodi di valutazione e le disposizioni di riconoscimento reciproco connessi, è uno strumento importante per verificare la sicurezza dei dispositivi per la creazione di una firma elettronica qualificata e dovrebbe essere promossa. Soluzioni e servizi innovativi, quali la firma in cloud e la firma mobile, tuttavia, si basano su soluzioni tecniche e organizzative per dispositivi per la creazione di una firma elettronica qualificata per i quali possono non essere ancora disponibili norme di sicurezza o per i quali può essere in corso la prima certificazione della sicurezza delle tecnologie d'informazione. Il livello di sicurezza di tali dispositivi per la creazione di una firma elettronica qualificata potrebbe essere valutato utilizzando procedure alternative solo se tali norme di sicurezza non sono disponibili o se la prima certificazione della sicurezza delle tecnologie d'informazione è in corso. Tali processi dovrebbero essere comparabili alle norme per la certificazione della sicurezza delle tecnologie d'informazione sempre che i livelli di sicurezza siano equivalenti. Tali processi potrebbero essere agevolati da una revisione tra pari.

(56) Il presente regolamento dovrebbe stabilire i requisiti relativi a dispositivi per la creazione di una firma elettronica qualificata al fine di assicurare la funzionalità delle firme elettroniche avanzate. Il presente regolamento non dovrebbe contemplare la globalità dell'ambiente del sistema in cui tali dispositivi operano. Pertanto, l'ambito di applicazione della certificazione dei dispositivi per la creazione di una firma qualificata dovrebbe essere limitato all'hardware e al software di sistema utilizzato per gestire e proteggere i dati per la creazione di una firma elettronica creati, memorizzati o trattati nel dispositivo di creazione di una firma. Come specificato nelle norme pertinenti, l'ambito di applicazione dell'obbligo di certificazione dovrebbe escludere le applicazioni relative alla creazione di una firma.

(57) Per garantire la certezza giuridica della validità della firma, è essenziale specificare i componenti di una firma elettronica qualificata, che dovrebbero essere valutati dalla parte

facente affidamento sulla certificazione che effettua la convalida. Inoltre, è opportuno che attraverso la specificazione degli obblighi dei prestatori di servizi fiduciari qualificati che possono offrire un servizio di convalida qualificata a parti facenti affidamento sulla certificazione che non vogliono o non possono effettuare esse stesse la convalida di firme elettroniche qualificate siano stimolati gli investimenti del settore privato e pubblico in tali servizi. È opportuno che entrambi gli elementi rendano la convalida delle firme elettroniche qualificate semplice e agevole per tutte le parti a livello dell'Unione.

(58) Qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.

(59) È opportuno che i sigilli elettronici fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.

(60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di sigilli elettronici dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di sigillo elettronico, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.

(61) È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.

(62) Al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il presente regolamento dovrebbe richiedere l'uso di un sigillo elettronico avanzato o di una firma elettronica avanzata o di altri metodi equivalenti. È prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal sigillo elettronico avanzato o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti nel presente regolamento.

(63) I documenti elettronici sono importanti per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno. Il presente regolamento dovrebbe stabilire il principio secondo cui a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo nella sua forma elettronica al fine di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica.

(64) Nel trattare i formati delle firme e dei sigilli elettronici avanzati, la Commissione dovrebbe basarsi sulle prassi, sulle norme e sulla legislazione esistente, in particolare la decisione 2011/130/UE della Commissione ([11]).

(65) Oltre ad autenticare il documento rilasciato dalla persona giuridica, i sigilli elettronici possono anche servire ad autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server.

(66) È essenziale prevedere un quadro giuridico per agevolare il riconoscimento transfrontaliero tra gli ordinamenti giuridici nazionali esistenti relativi ai servizi elettronici di recapito certificato. Tale quadro potrebbe aprire inoltre per i prestatori di servizi fiduciari dell'Unione

nuove opportunità di mercato per l'offerta di nuovi servizi elettronici di recapito certificati paneuropei.

(67) I servizi di autenticazione dei siti web prevedono un mezzo tramite il quale il visitatore di un sito può accertarsi che dietro a quel sito web vi è un'entità reale e legittima. Tali servizi contribuiscono a diffondere sicurezza e fiducia nelle transazioni commerciali on line, in quanto gli utenti si fideranno di un sito web che è stato autenticato. La fornitura e l'uso di servizi di autenticazione dei siti web sono interamente volontari. Tuttavia, affinché l'autenticazione dei siti web divenga un mezzo per rafforzare la fiducia, fornire un'esperienza migliore all'utente e promuovere la crescita nel mercato interno, è opportuno che il presente regolamento stabilisca obblighi minimi in materia di sicurezza e responsabilità per i prestatori e i loro servizi. A tal fine, si è tenuto conto dei risultati delle iniziative industriali esistenti, ad esempio, il Forum Autorità di certificazione/Browser (CA/B Forum). Inoltre, il presente regolamento non dovrebbe impedire l'uso di altri mezzi o metodi di autenticazione di un sito web non rientranti nel presente regolamento e non dovrebbe vietare ai prestatori di servizi di autenticazione dei siti web di paesi terzi di prestare i propri servizi ai clienti dell'Unione. Tuttavia, i servizi di autenticazione dei siti web di un prestatore di un paese terzo dovrebbero essere riconosciuti come qualificati ai sensi del presente regolamento solo se è stato concluso un accordo internazionale tra l'Unione e il paese di stabilimento di detto prestatore.

(68) La nozione di «persone giuridiche» secondo le disposizioni del trattato sul funzionamento dell'Unione europea (TFUE) in materia di stabilimento lascia agli operatori la libertà di scegliere la forma giuridica che ritengono opportuna per svolgere la loro attività. Di conseguenza, per «persone giuridiche» ai sensi del TFUE si intendono tutte le entità costituite conformemente al diritto di uno Stato membro o da esso disciplinate, a prescindere dalla loro forma giuridica.

(69) Le istituzioni, gli organi, gli uffici e le agenzie dell'Unione sono incoraggiate a riconoscere l'identificazione elettronica e i servizi fiduciari contemplati dal presente regolamento ai fini dell'amministrazione cooperativa facendo tesoro, in particolare, delle buone prassi esistenti e dei risultati dei progetti in corso nei settori contemplati dal presente regolamento.

(70) Al fine di completare determinati aspetti tecnici dettagliati del presente regolamento in modo flessibile e veloce, dovrebbe essere delegato alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE riguardo ai criteri che devono soddisfare gli organismi responsabili della certificazione dei dispositivi per la creazione di una firma elettronica qualificata. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio.

(71) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione, in particolare per specificare i numeri di riferimento delle norme il cui impiego conferisce una presunzione di adempimento di determinati requisiti stabiliti nel presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([12]).

(72) In sede di elaborazione degli atti delegati o di esecuzione, la Commissione dovrebbe tenere debito conto delle norme e delle specifiche tecniche elaborate da organizzazioni e organismi

di normalizzazione europei e internazionali, in particolare il Comitato europeo di normalizzazione (CEN), l'Istituto europeo delle norme di telecomunicazione (ETSI), l'Organizzazione internazionale per la standardizzazione (ISO) e l'Unione internazionale delle telecomunicazioni (UIT), al fine di assicurare un livello elevato di sicurezza e interoperabilità dell'identificazione elettronica e dei servizi fiduciari.

(73) Per motivi di certezza del diritto e di chiarezza è opportuno abrogare la direttiva 1999/93/CE.

(74) Per garantire la certezza giuridica per operatori di mercato che già fanno uso di certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE, è necessario prevedere un idoneo periodo transitorio. Analogamente, dovrebbero essere stabilite misure transitorie per i dispositivi per la creazione di una firma sicura, la cui conformità sia stata determinata ai sensi della direttiva 1999/93/CE, nonché per i prestatori di servizi di certificazione che rilasciano certificati qualificati entro il 1º luglio 2016. Infine, è altresì necessario dotare la Commissione dei mezzi per adottare atti di esecuzione e atti delegati prima di tale data.

(75) Le date di applicazione stabilite nel presente regolamento non pregiudicano gli obblighi esistenti già contratti dagli Stati membri in base al diritto dell'Unione, in particolare della direttiva 2006/123/CE.

(76) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della portata dell'azione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(77) Il garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([13]) e ha espresso un parere il 27 settembre 2012 ([14]),

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, il presente regolamento:

a) fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro,

b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; e

c) istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati diautenticazione di siti web.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.

2. Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.

3. Il presente regolamento non pregiudica il diritto nazionale o unionale legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma.

Articolo 3

Definizioni

Ai fini del presente regolamento si intende per:

1) «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;

2) «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;

3) «dati di identificazione personale», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;

4) «regime di identificazione elettronica», un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche;

5) «autenticazione», un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica;

6) «parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;

7) «organismo del settore pubblico», un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;

8) «organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio ([15]);

9) «firmatario», una persona fisica che crea una firma elettronica;

10) «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

11) «firma elettronica avanzata», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;

12) «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;

13) «dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;

14) «certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;

15) «certificato qualificato di firma elettronica», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;

16) «servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

    a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure

    b) creazione, verifica e convalida di certificati di autenticazione di siti web; o

    c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;

17) «servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;

18) «organismo di valutazione della conformità», un organismo ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati;

19) «prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;

20) «prestatore di servizi fiduciari qualificato», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;

21) «prodotto», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;

22) «dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;

23) «dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;

24) «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;

25) «sigillo elettronico», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;

26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;

27) «sigillo elettronico qualificato», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;

28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

29) «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;

30) «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;

31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

33) «validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;

34) «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

35) «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;

36) «servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;

37) «servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;

38) «certificato di autenticazione di sito web», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;

39) «certificato qualificato di autenticazione di sito web», un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV;

40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;

41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

Articolo 4

Principio del mercato interno

1. Non sono imposte restrizioni alla prestazione di servizi fiduciari nel territorio di uno Stato membro da parte di un prestatore di servizi fiduciari stabilito in un altro Stato membro per motivi che rientrano negli ambiti di applicazione del presente regolamento.

2. I prodotti e i servizi fiduciari conformi al presente regolamento godono della libera circolazione nel mercato interno.

Articolo 5

Trattamento e protezione dei dati

1. Il trattamento dei dati a carattere personale è effettuato a norma della direttiva 95/46/CE.

2. Fatti salvi gli effetti giuridici che il diritto nazionale attribuisce agli pseudonimi, gli Stati membri non vietano l'uso di pseudonimi nelle transazioni elettroniche.

CAPO II
IDENTIFICAZIONE ELETTRONICA

Articolo 6

Riconoscimento reciproco

1. Ove il diritto o la prassi amministrativa nazionale richiedano l'impiego di un'identificazione elettronica mediante mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del settore pubblico online in uno Stato membro, i mezzi di identificazione elettronica rilasciati in un altro Stato membro sono riconosciuti nel primo Stato membro ai fini dell'autenticazione transfrontaliera di tale servizio online, purché soddisfino le seguenti condizioni:

a) i mezzi di identificazione elettronica sono rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9;

b) il livello di garanzia dei mezzi di identificazione elettronica corrisponde a un livello di garanzia pari o superiore al livello di garanzia richiesto dall'organismo del settore pubblico competente per accedere al servizio online in questione nel primo Stato membro, sempre che il livello di garanzia di tali mezzi di identificazione elettronica corrisponda al livello di garanzia significativo o elevato;

c) l'organismo del settore pubblico competente usa il livello di garanzia significativo o elevato in relazione all'accesso a tale servizio online.

Tale riconoscimento ha luogo non oltre 12 mesi dalla data in cui la Commissione pubblica l'elenco i di cui alla lettera a), primo comma.

2. Un mezzo di identificazione elettronica rilasciato nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9 e che corrisponde al livello di garanzia basso può essere riconosciuto dagli organismi del settore pubblico ai fini dell'autenticazione transfrontaliera del servizio prestato online da tali organismi.

Articolo 7

Ammissibilità alla notifica dei regimi di identificazione elettronica

Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell'articolo 9, paragrafo 1, purché soddisfi tutte le seguenti condizioni:

a) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica sono rilasciati:

i) dallo Stato membro notificante;

ii) su incarico dello Stato membro notificante; o

iii) a titolo indipendente dallo Stato membro notificante e sono riconosciuti da tale Stato membro;

b) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica possono essere utilizzati per accedere almeno a un servizio che è fornito da un organismo del settore pubblico e che richiede l'identificazione elettronica nello Stato membro notificante;

c) il regime di identificazione elettronica e i mezzi di identificazione elettronica rilasciati conformemente alle sue disposizioni soddisfano i requisiti di almeno uno dei livelli di garanzia stabiliti nell'atto di esecuzione di cui all'articolo 8, paragrafo 3;

d) lo Stato membro notificante garantisce che i dati di identificazione personale che rappresentano unicamente la persona in questione siano attribuiti, conformemente alle specifiche tecniche, norme e procedure relative al pertinente livello di garanzia definito nell'atto di esecuzione di cui all'articolo 8, paragrafo 3, alla persona fisica o giuridica di cui all'articolo 3, punto 1, al momento in cui è rilasciata l'identificazione elettronica nell'ambito di detto regime;

e) la parte che rilascia i mezzi di identificazione elettronica nell'ambito di detto regime assicura che i mezzi di identificazione elettronica siano attribuiti alla persona di cui alla lettera d) del presente articolo conformemente alle specifiche, norme e procedure tecniche relative al pertinente livello di garanzia definito nnell'atto di esecuzione di cui all'articolo 8, paragrafo 3;

f) lo Stato membro notificante garantisce la disponibilità dell'autenticazione online, per consentire alle parti facenti affidamento sulla certificazione stabilite nel territorio di un altro Stato membro di confermare i dati di identificazione personale che hanno ricevuto in forma elettronica.

Per le parti facenti affidamento sulla certificazione diverse dagli organismi del settore pubblico, lo Stato membro notificante può definire i termini di accesso a tale autenticazione. Quando l'autenticazione transfrontaliera è effettuata in relazione a un servizio online prestato da un organismo del settore pubblico, essa è fornita a titolo gratuito.

Gli Stati membri non impongono alcun requisito tecnico specifico sproporzionato alle parti facenti affidamento sulla certificazione che intendono effettuare tale autenticazione, qualora tali requisiti impediscano o ostacolino notevolmente l'interoperabilità dei regimi di identificazione elettronica notificati;

g) almeno sei mesi prima della notifica di cui all'articolo 9, paragrafo 1, lo Stato membro notificante fornisce agli altri Stati membri, ai fini dell'obbligo previsto dall'articolo 12, paragrafo 5, una descrizione di detto regime conformemente alle modalità procedurali stabilite dagli atti di esecuzione di cui all'articolo 12, paragrafo 7;

h) il regime di identificazione elettronica soddisfa i requisiti definiti nell'atto di esecuzione di cui all'articolo 12, paragrafo 8.

Articolo 8

Livelli di garanzia dei regimi di identificazione elettronica

1. Un regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1, specifica livelli di garanzia basso, significativo e/o elevato per i mezzi di identificazione

elettronica rilasciati nell'ambito di detto regime.

2. I livelli di garanzia basso, significativo e elevato soddisfano rispettivamente i seguenti criteri:

a) il livello di garanzia basso si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza limitato riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre il rischio di uso abusivo o alterazione dell'identità;

b) il livello di garanzia significativo si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza significativo riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre significativamente il rischio di uso abusivo o alterazione dell'identità;

c) il livello di garanzia elevato si riferisce a un mezzo di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce riguardo all'identità pretesa o dichiarata di una persona un grado di sicurezza più elevato dei mezzi di identificazione elettronica aventi un livello di garanzia significativo ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità.

3. Entro il 18 settembre 2015, tenendo conto delle norme internazionali pertinenti e fatto salvo il paragrafo 2, la Commissione, mediante atti di esecuzione, definisce le specifiche, norme e procedure tecniche minime in riferimento alle quali sono specificati i livelli di garanzia basso, significativo e elevato dei mezzi di identificazione elettronica ai fini del paragrafo 1.

Le suddette specifiche, norme e procedure tecniche minime sono fissate facendo riferimento all'affidabilità e alla qualità dei seguenti elementi:

a) della procedura di controllo e verifica dell'identità delle persone fisiche o giuridiche che chiedono il rilascio dei mezzi di identificazione elettronica;

b) della procedura di rilascio dei mezzi di identificazione elettronica richiesti;

c) del meccanismo di autenticazione mediante il quale la persona fisica o giuridica usa i mezzi di identificazione elettronica per confermare la propria identità a una parte facente affidamento sulla certificazione;

d) dell'entità che rilascia i mezzi di identificazione elettronica;

e) di qualsiasi altro organismo implicato nella domanda di rilascio dei mezzi di identificazione elettronica; e

f) delle specifiche tecniche e di sicurezza dei mezzi di identificazione elettronica rilasciati.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 9

Notifica

1. Lo Stato membro notificante rende note alla Commissione le informazioni seguenti e, senza indugio, qualsiasi loro successiva modifica:

a) una descrizione del regime di identificazione elettronica, con indicazione dei suoi livelli di garanzia e della o delle entità che rilasciano i mezzi di identificazione elettronica nell'ambito del regime;

b) il regime di vigilanza e il regime di informazioni sulla responsabilità applicabili per quanto riguarda:

   i) la parte che rilascia i mezzi di identificazione elettronica; e

   ii) la parte che gestisce la procedura di autenticazione;

c) l'autorità o le autorità responsabili del regime di identificazione elettronica;

d) informazioni sull'entità o sulle entità che gestiscono la registrazione dei dati unici di identificazione personale;

e) una descrizione di come sono soddisfatti i requisiti definiti negli atti di esecuzione di cui all'articolo 12, paragrafo 8;

f) una descrizione dell'autenticazione di cui all'articolo 7, lettera f);

g) disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra.

2. Un anno dopo la data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un elenco dei regimi di identificazione elettronica notificati ai sensi del paragrafo 1 del presente articolo e le informazioni fondamentali al riguardo.

3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo 2, pubblica nella *Gazzetta ufficiale dell'Unione europea* le modifiche dell'elenco di cui al paragrafo 2 entro due mesi dalla data di ricezione di tale notifica.

4. Uno Stato membro può presentare alla Commissione una richiesta di eliminazione del regime di identificazione elettronica da esso notificato dall'elenco di cui al paragrafo 2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricezione della richiesta dello Stato membro.

5. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure delle notifiche a norma del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 10

Violazione della sicurezza

1. In caso di violazione o parziale compromissione del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, o dell'autenticazione di cui all'articolo 7, lettera f), con limitazione dell'affidabilità dell'autenticazione transfrontaliera di tale regime, lo Stato membro notificante senza indugio sospende o revoca tale autenticazione transfrontaliera o le sue parti compromesse e ne informa gli altri Stati membri e la Commissione.

2. Una volta posto rimedio alla violazione o alla compromissione di cui al paragrafo 1, lo Stato membro notificante ristabilisce l'autenticazione transfrontaliera e informa senza indugio gli altri Stati membri e la Commissione.

3. Qualora non sia posto rimedio alla violazione o alla compromissione di cui al paragrafo 1 entro tre mesi dalla sospensione o dalla revoca, lo Stato membro notificante notifica agli altri Stati membri e alla Commissione il ritiro del regime di identificazione elettronica.

La Commissione pubblica senza indebito ritardo le corrispondenti modifiche dell'elenco di cui all'articolo 9, paragrafo 2, nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 11

Responsabilità

1. Lo Stato membro notificante è responsabile per i danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dei suoi obblighi di cui all'articolo 7, lettere d) e f), in una transazione transfrontaliera.

2. La parte che rilascia i mezzi di identificazione elettronica è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dell'obbligo di cui all'articolo 7, lettera e), in una transazione transfrontaliera.

3. La parte che gestisce la procedura di autenticazione è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica per non avere garantito la corretta gestione dell'autenticazione di cui all'articolo 7, lettera f), in una transazione transfrontaliera.

4. I paragrafi 1, 2 e 3 si applicano conformemente alle norme nazionali in materia di responsabilità.

5. I paragrafi 1, 2 e 3 lasciano impregiudicata la responsabilità conformemente al diritto nazionale delle parti di una transazione in cui sono utilizzati mezzi di identificazione elettronica che rientrano nel regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1.

Articolo 12

Cooperazione e interoperabilità

1. I regimi nazionali di identificazione elettronica notificati a norma dell'articolo 9, paragrafo 1, sono interoperabili.

2. È istituito un quadro di interoperabilità ai fini del paragrafo 1.

3. Il quadro di interoperabilità risponde ai seguenti criteri:

a) mira a essere neutrale dal punto di vista tecnologico e non comporta discriminazioni tra specifiche soluzioni tecniche nazionali per l'identificazione elettronica all'interno di uno Stato membro;

b) segue, ove possibile, le norme europee e internazionali;

c) facilita l'applicazione del principio della tutela della vita privata fin dalla progettazione (privacy by design); e

d) garantisce che i dati personali siano trattati a norma della direttiva 95/46/CE.

4. Il quadro di interoperabilità è composto da:

a) un riferimento ai requisiti tecnici minimi connessi ai livelli di garanzia di cui all'articolo 8;

b) una mappatura dei livelli di garanzia nazionali dei regimi di identificazione elettronica notificati in base ai livelli di garanzia di cui all'articolo 8;

c) un riferimento ai requisiti tecnici minimi di interoperabilità;

d) un riferimento a un insieme minimo di dati di identificazione personale che rappresentano un'unica persona fisica o giuridica, disponibile nell'ambito dei regimi di identificazione elettronica;

e) norme di procedura;

f) disposizioni per la risoluzione delle controversie; e

g) norme di sicurezza operativa comuni.

5. Gli Stati membri cooperano per quanto riguarda:

a) l'interoperabilità dei regimi di identificazione elettronica notificati ai sensi dell'articolo 9, paragrafo 1, e dei regimi di identificazione elettronica che gli Stati membri intendono notificare; e

b) la sicurezza dei regimi di identificazione elettronica.

6. La cooperazione fra gli Stati membri riguarda:

a) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i regimi di identificazione elettronica e, in particolare, i requisiti tecnici connessi all'interoperabilità e ai livelli di garanzia;

b) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i metodi di lavoro con i livelli di garanzia dei regimi di identificazione elettronica di cui all'articolo 8;

c) la valutazione tra pari dei regimi di identificazione elettronica che rientrano nel presente regolamento; e

d) l'esame degli sviluppi pertinenti nel settore dell'identificazione elettronica.

7. Entro il 18 marzo 2015, la Commissione, mediante atti di esecuzione, fissa le modalità procedurali necessarie per facilitare la collaborazione fra gli Stati membri di cui ai paragrafi 5 e 6, al fine di promuovere un elevato livello di fiducia e di sicurezza, commisurato al grado di rischio esistente.

8. Entro il 18 settembre 2015, al fine di garantire condizioni uniformi di esecuzione del requisito di cui al paragrafo 1, la Commissione, fatti salvi i criteri di cui al paragrafo 3 e tenendo conto dei risultati della cooperazione fra gli Stati membri, adotta atti di esecuzione sul quadro di interoperabilità quale definito al paragrafo 4.

9. Gli atti di esecuzione di cui a paragrafi 7 e 8 sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

CAPO III
SERVIZI FIDUCIARI

SEZIONE 1
Disposizioni generali

Articolo 13

Responsabilità e onere della prova

1. Fatto salvo il paragrafo 2, i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.

L'onere di dimostrare il dolo o la negligenza di un prestatore di servizi fiduciari non qualificato ricade sulla persona fisica o giuridica che denuncia il danno di cui al primo comma.

Si presume il dolo o la negligenza di un prestatore di servizi fiduciari qualificato, salvo se questi dimostra che il danno di cui al primo comma si è verificato senza suo dolo o negligenza.

2. Se i prestatori di servizi fiduciari informano debitamente e preventivamente i loro clienti delle limitazioni d'uso dei servizi da essi forniti e se tali limitazioni sono riconoscibili da parte di terzi, non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati.

3. I paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità.

Articolo 14

Relazioni internazionali

1. I servizi fiduciari prestati da prestatori di servizi fiduciari stabiliti in un paese terzo sono riconosciuti giuridicamente equivalenti ai servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione qualora i servizi fiduciari aventi origine nel paese terzo siano riconosciuti a norma di un accordo concluso fra l'Unione e il paese terzo in questione o un'organizzazione internazionale a norma dell'articolo 218 TFUE.

2. Gli accordi di cui al paragrafo 1 garantiscono, in particolare, che:

a) i requisiti che si applicano ai prestatori di servizi fiduciari qualificati stabiliti nell'Unione e ai servizi fiduciari qualificati che prestano siano soddisfatti dai prestatori di servizi fiduciari nel paese terzo o presso le organizzazioni internazionali con cui è concluso l'accordo, nonché dai servizi fiduciari da essi prestati;

b) i servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione sono riconosciuti come giuridicamente equivalenti ai servizi fiduciari prestati da prestatori di servizi fiduciari nel paese terzo o presso l'organizzazione internazionale con cui è concluso l'accordo.

Articolo 15

Accessibilità per le persone con disabilità

Ove possibile, i servizi fiduciari prestati e i prodotti destinati all'utilizzatore finale impiegati per la prestazione di detti servizi sono resi accessibili alle persone con disabilità.

Articolo 16

Sanzioni

Gli Stati membri stabiliscono norme relative alle sanzioni da applicare in caso di violazioni del presente regolamento. Le sanzioni previste sono effettive, proporzionate e dissuasive.

SEZIONE 2

Vigilanza

Articolo 17

Organismo di vigilanza

1. Gli Stati membri designano un organismo di vigilanza stabilito nel loro territorio o, di comune accordo con un altro Stato membro, un organismo di vigilanza stabilito in tale altro

Stato membro. Tale organismo è responsabile di compiti di vigilanza nello Stato membro designante.

Agli organismi di vigilanza sono conferiti i poteri necessari e le risorse adeguate per l'esercizio dei loro compiti.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dei rispettivi organismi di vigilanza designati.

3. Il ruolo dell'organismo di vigilanza è il seguente:

a) vigilare sui prestatori di servizi fiduciari qualificati stabiliti nel territorio dello Stato membro designante per assicurarsi, mediante attività di vigilanza ex ante e ex post, che essi e i servizi fiduciari qualificati da essi prestati rispondano ai requisiti di cui al presente regolamento;

b) adottare misure, ove necessario, in relazione a prestatori di servizi fiduciari non qualificati stabiliti nel territorio dello Stato membro designante, mediante attività di vigilanza ex post, qualora sia informato che tali prestatori di servizi fiduciari non qualificati o i servizi fiduciari da essi prestati presumibilmente non soddisfano i requisiti stabiliti dal presente regolamento.

4. Ai fini del paragrafo 3 e fatte salve le limitazioni ivi previste, l'organismo di vigilanza ha, in particolare, i compiti seguenti:

a) cooperare con altri organismi di vigilanza e assisterli a norma dell'articolo 18;

b) analizzare le relazioni di valutazione della conformità di cui all'articolo 20, paragrafo 1, e all'articolo 21, paragrafo 1;

c) informare gli altri organismi di vigilanza e il pubblico in merito a violazioni della sicurezza o perdita di integrità a norma dell'articolo 19, paragrafo 2;

d) riferire alla Commissione in merito alle sue principali attività a norma del paragrafo 6 del presente articolo;

e) svolgere verifiche o chiedere a un organismo di valutazione della conformità di effettuare una valutazione di conformità dei prestatori di servizi fiduciari qualificati a norma dell'articolo 20, paragrafo 2;

f) cooperare con le autorità di protezione, in particolare informandole senza indugio dei dati in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali;

g) concedere la qualifica ai prestatori di servizi fiduciari e ai servizi da essi prestati e ritirare tale qualifica a norma degli articoli 20 e 21;

h) informare l'organismo responsabile dell'elenco nazionale di fiducia di cui all'articolo 22, paragrafo 3, in merito alle proprie decisioni di concedere o ritirare la qualifica, salvo se tale organismo è anche l'organismo di vigilanza;

i) verificare l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nei casi in cui il prestatore di servizi fiduciari qualificati cessa le sue attività, inclusi i modi in cui le informazioni sono mantenute accessibili a norma dell'articolo 24, paragrafo 2, lettera h);

j) imporre ai prestatori di servizi fiduciari di rimediare a qualsiasi mancato adempimento dei requisiti di cui al presente regolamento.

5. Gli Stati membri possono imporre che l'organismo di vigilanza istituisca, mantenga e aggiorni un'infrastruttura fiduciaria secondo le condizioni di cui al diritto nazionale.

6. Entro il 31 marzo di ogni anno, ogni organismo di vigilanza presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile insieme a una sintesi delle notifiche di violazione ricevute da prestatori di servizi fiduciari a norma dell'articolo 19, paragrafo 2.

7. La Commissione mette a disposizione degli Stati membri la relazione annuale di cui al paragrafo 6.

8. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui al paragrafo 6. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 18

Assistenza reciproca

1. Gli organismi di vigilanza collaborano fra loro al fine di scambiarsi buone prassi.

Un organismo di vigilanza, previa ricezione di una richiesta giustificata da parte di un altro organismo di vigilanza, fornisce a quest'ultimo assistenza perché possano svolgere le attività di organismi di vigilanza in modo coerente. L'assistenza reciproca può coprire, in particolare, le richieste di informazioni e le misure di vigilanza, quali richieste di svolgere ispezioni in connessione con le relazioni di valutazione della conformità di cui agli articoli 20 e 21.

2. L'organismo di vigilanza cui è presentata una richiesta di assistenza può rifiutare tale richiesta per uno dei seguenti motivi:

a) l'organismo di vigilanza non è competente a fornire l'assistenza richiesta;

b) l'assistenza richiesta non è proporzionata alle attività di vigilanza dell'organismo di vigilanza svolte a norma dell'articolo 17;

c) fornire l'assistenza richiesta sarebbe incompatibile con il presente regolamento.

3. Ove appropriato, gli Stati membri possono autorizzare i rispettivi organismi di vigilanza a svolgere indagini congiunte con la partecipazione di membri del personale di organismi di vigilanza di altri Stati membri. Le disposizioni e le procedure per tali indagini congiunte sono convenute e stabilite dagli Stati membri interessati conformemente al rispettivo diritto nazionale.

Articolo 19

Requisiti di sicurezza relativi ai prestatori di servizi fiduciari

1. I prestatori di servizi fiduciari qualificati e non qualificati adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati. Tenuto conto degli ultimi sviluppi tecnologici, tali misure assicurano un livello di sicurezza commisurato al grado di rischio esistente. In particolare, sono adottate misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti.

2. Senza indugio ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza, i prestatori di servizi fiduciari qualificati e non qualificati notificano all'organismo di vigilanza e, ove applicabile, ad altri organismi interessati, quali l'ente nazionale competente per la sicurezza delle informazioni o l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.

Qualora sia probabile che la violazione della sicurezza o la perdita di integrità abbia effetti negativi su una persona fisica o giuridica a cui è stato prestato il servizio fiduciario, il prestatore di servizi fiduciari notifica senza indugio anche alla persona fisica o giuridica la violazione di sicurezza o la perdita di integrità.

Ove appropriato, in particolare qualora la violazione di sicurezza o la perdita di integrità riguardi due o più Stati membri, l'organismo di vigilanza notificato ne informa gli organismi di vigilanza negli altri Stati membri interessati e l'ENISA.

L'organismo di vigilanza notificato informa il pubblico o impone al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico.

3. L'organismo di vigilanza trasmette all'ENISA, una volta all'anno, una sintesi delle notifiche di violazione di sicurezza e perdita di integrità pervenute dai prestatori di servizi fiduciari.

4. La Commissione può, mediante atti di esecuzione:

a) specificare ulteriormente le misure di cui al paragrafo 1; e

b) definire i formati e le procedure, comprese le scadenze, applicabili ai fini del paragrafo 2.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 3

Servizi fiduciari qualificati

Articolo 20

Vigilanza dei prestatori di servizi fiduciari qualificati

1. I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità. Lo scopo della verifica è di confermare che i prestatori di servizi fiduciari qualificati e i servizi fiduciari qualificati da essi prestati soddisfano i requisiti di cui al presente regolamento. I prestatori di servizi fiduciari qualificati presentano la pertinente relazione di valutazione di conformità all'organismo di vigilanza entro il termine di tre giorni lavorativi dalla sua ricezione.

2. Fatto salvo il paragrafo 1, l'organismo di vigilanza può, in qualsiasi momento, condurre una verifica o chiedere a un organismo di valutazione della conformità di eseguire una valutazione di conformità dei prestatori di servizi fiduciari qualificati, a spese di tali prestatori di servizi fiduciari, per confermare che essi e i servizi fiduciari qualificati da essi prestati rispondono ai requisiti di cui al presente regolamento. Laddove siano state rilevate violazioni delle norme di protezione dei dati personali, l'organismo di vigilanza comunica alle autorità di protezione dei dati i risultati delle verifiche.

3. Ove l'organismo di vigilanza imponga al prestatore di servizi fiduciari qualificato di rimediare agli eventuali mancati adempimenti dei requisiti di cui al presente regolamento e ove il prestatore non agisca di conseguenza e, se applicabile, entro un limite di tempo stabilito dall'organismo di vigilanza, quest'ultimo, tenendo conto in particolare della dimensione, della durata e delle conseguenze di tale mancato adempimento, può ritirare la qualifica di tale prestatore o del servizio interessato da esso prestato e informare l'organismo di cui all'articolo 22, paragrafo 3, al fine di aggiornare gli elenchi di fiducia di cui all'articolo 22, paragrafo 1.

L'organismo di vigilanza comunica al prestatore di servizi fiduciari qualificato la revoca della sua qualifica o della qualifica del servizio interessato.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento per le seguenti norme:

a) accreditamento degli organismi di valutazione della conformità e per la relazione di valutazione di conformità di cui al paragrafo 1;

b) regole in materia di audit in base alle quali gli organismi di valutazione effettueranno le loro valutazioni della conformità dei prestatori di servizi fiduciari qualificati di cui al paragrafo 1.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 21

Avviamento di un servizio fiduciario qualificato

1. Qualora i prestatori di servizi fiduciari, privi di qualifica, intendano avviare la prestazione di servizi fiduciari qualificati, trasmettono all'organismo di vigilanza una notifica della loro intenzione insieme a una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità.

2. L'organismo di vigilanza verifica se il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al presente regolamento e, in particolare, i requisiti per i prestatori di servizi fiduciari qualificati e per i servizi fiduciari qualificati da essi prestati.

Se conclude che il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al primo comma, l'organismo di vigilanza concede la qualifica al prestatore di servizi fiduciari e ai servizi fiduciari da esso prestati e informa l'organismo di cui all'articolo 22, paragrafo 3, affinché aggiorni gli elenchi di fiducia di cui all'articolo 22, paragrafo 1, non oltre tre mesi dopo la notifica a norma del paragrafo 1 del presente articolo.

Se la verifica non si è conclusa entro tre mesi dalla notifica, l'organismo di vigilanza ne informa il prestatore di servizi fiduciari specificando i motivi del ritardo e il periodo necessario per concludere la verifica.

3. I prestatori di servizi fiduciari qualificati possono iniziare a prestare il servizio fiduciario qualificato dopo che la qualifica è stata registrata negli elenchi di fiducia di cui all'articolo 22, paragrafo 1.

4. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 22

Elenchi di fiducia

1. Tutti gli Stati membri istituiscono, mantengono e pubblicano elenchi di fiducia, che includono le informazioni relative ai prestatori di servizi fiduciari qualificati per i quali sono responsabili, unitamente a informazioni relative ai servizi fiduciari qualificati da essi prestati.

2. Gli Stati membri istituiscono, mantengono e pubblicano, in modo sicuro, gli elenchi di fiducia di cui al paragrafo 1, firmati o sigillati elettronicamente in una forma adatta al trattamento automatizzato.

3. Gli Stati membri notificano alla Commissione, senza indugio, informazioni sull'organismo responsabile dell'istituzione, del mantenimento e della pubblicazione degli elenchi nazionali di fiducia, precisando dove gli elenchi sono pubblicati, e sui certificati utilizzati per firmare o sigillare tali elenchi di fiducia e le eventuali modifiche apportate.

4. La Commissione rende pubbliche, attraverso un canale sicuro, le informazioni di cui al paragrafo 3 in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

5. Entro il 18 settembre 2015, la Commissione, mediante atti di esecuzione, specifica le informazioni di cui al paragrafo 1 e definisce le specifiche tecniche e i formati per gli elenchi di fiducia applicabili ai fini dei paragrafi da 1 a 4. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 23

Marchio di fiducia UE per i servizi fiduciari qualificati

1. Dopo la registrazione della qualifica di cui all'articolo 21, paragrafo 2, secondo comma, nell'elenco di fiducia di cui all'articolo 22, paragrafo 1, i prestatori di servizi fiduciari qualificati possono utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.

2. Quando utilizzano il marchio di fiducia UE per i servizi fiduciari qualificati di cui al paragrafo 1, i prestatori di servizi fiduciari qualificati garantiscono che sul loro sito web sia disponibile un link all'elenco di fiducia pertinente.

3. Entro il 1º luglio 2015 la Commissione, mediante atti di esecuzione, fornisce criteri specifici relativi alla forma e, in particolare, alla presentazione, alla composizione, alla dimensione e al disegno del marchio di fiducia UE per i servizi fiduciari qualificati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 24

Requisiti per i prestatori di servizi fiduciari qualificati

1. Allorché rilascia un certificato qualificato per un servizio fiduciario, un prestatore di servizi fiduciari qualificato verifica, mediante mezzi appropriati e conformemente al diritto nazionale, l'identità e, se del caso, eventuali attributi specifici della persona fisica o giuridica a cui il certificato qualificato è rilasciato.

Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato direttamente o ricorrendo a un terzo conformemente al diritto nazionale:

a) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica; o

b) a distanza, mediante mezzi di identificazione elettronica, con cui prima del rilascio del certificato qualificato è stata garantita una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisfano i requisiti fissati all'articolo 8 riguardo ai livelli di garanzia «significativo» o «elevato»; o

c) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato a norma della lettera a) o b); o

d) mediante altri metodi di identificazione riconosciuti a livello nazionale che forniscono una garanzia equivalente sotto il profilo dell'afffidabilità alla presenza fisica. La garanzia equivalente è confermata da un organismo di valutazione della conformità.

2. Un prestatore di servizi fiduciari qualificato che presta servizi fiduciari qualificati:

a) informa l'organismo di vigilanza di eventuali cambiamenti nella prestazione dei propri servizi fiduciari qualificati e dell'intenzione di cessare tali attività;

b) impiega personale e, ove applicabile, subcontraenti dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie e che hanno ricevuto una formazione adeguata in materia di norme di sicurezza e di protezione dei dati personali e applica procedure amministrative e gestionali, che corrispondono a norme europee o internazionali;

c) riguardo alla responsabilità civile per danni a norma dell'articolo 13, mantiene risorse finanziarie adeguate e/o si procura un'assicurazione di responsabilità civile appropriata, conformemente al diritto nazionale;

d) prima di avviare una relazione contrattuale informa, in modo chiaro e completo, chiunque intenda utilizzare un servizio fiduciario qualificato dei termini e delle condizioni esatte per l'utilizzo di tale servizio, comprese eventuali limitazioni del suo utilizzo;

e) utilizza sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità dei processi che assicurano;

f) utilizza sistemi affidabili per memorizzare i dati a esso forniti, in modo verificabile, affinché:

   i) siano accessibili alla consultazione del pubblico soltanto con il consenso della persona a cui i dati fanno riferimento;

   ii) soltanto le persone autorizzate possano effettuare inserimenti e modifiche ai dati memorizzati;

   iii) l'autenticità dei dati sia verificabile;

g) adotta misure adeguate contro le falsificazioni e i furti di dati;

h) registra e mantiene accessibili per un congruo periodo di tempo, anche dopo la cessazione delle attività del prestatore di servizi fiduciari qualificato, tutte le informazioni pertinenti relative a dati rilasciati e ricevuti dal prestatore di servizi fiduciari qualificato, in particolare a fini di produzione di prove nell'ambito di procedimenti giudiziali e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;

i) dispone di un piano di cessazione delle attività aggiornato per garantire la continuità del servizio conformemente alle disposizioni verificate dall'organismo di vigilanza a norma dell'articolo 17, paragrafo 4, lettera i);

j) garantisce il trattamento lecito dei dati personali a norma della direttiva 95/46/CE;

k) se i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati, istituiscono una banca dati dei certificati aggiornata.

3. Se un prestatore di servizi fiduciari qualificato che rilascia certificati qualificati decide di revocare un certificato, registra tale revoca nella propria banca dati dei certificati e pubblica la situazione di revoca del certificato tempestivamente e, in ogni caso, entro 24 ore dal ricevimento della richiesta. La revoca diventa immediatamente effettiva all'atto della pubblicazione.

4. In considerazione del paragrafo 3, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati trasmettono alle parti facenti affidamento sulla certificazione informazioni sulla situazione di validità o revoca dei certificati qualificati da essi rilasciati. Queste informazioni sono rese disponibili almeno per ogni certificato rilasciato in qualsiasi momento e oltre il periodo di validità del certificato, in modo automatizzato, affidabile, gratuito ed efficiente.

5. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sistemi e prodotti affidabili, che soddisfano i requisiti di cui al paragrafo 2, lettere e) ed f), del presente articolo. Si presume che i requisiti di cui al presente articolo siano stati rispettati ove i sistemi e i prodotti affidabili adempiano a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 4

Firme elettroniche

Articolo 25

Effetti giuridici delle firme elettroniche

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.

2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.

3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

Articolo 26

Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Articolo 27

Firme elettroniche nei servizi pubblici

1. Se uno Stato membro richiede una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate, le firme elettroniche avanzate basate su un certificato qualificato di firma elettronica e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

2. Se uno Stato membro richiede una firma elettronica avanzata basata su un certificato qualificato per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate basate su un certificato qualificato e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per un utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, una firma elettronica dotata di un livello di garanzia di

sicurezza più elevato di quello della firma elettronica qualificata.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alle firme elettroniche avanzate. Si presume che i requisiti per le firme elettroniche avanzate di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 26, siano rispettati ove una firma elettronica avanzata soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento delle firme elettroniche avanzate o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 28

Certificati qualificati di firme elettroniche

1. I certificati qualificati di firme elettroniche soddisfano i requisiti di cui all'allegato I.

2. I certificati qualificati di firme elettroniche non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato I.

3. I certificati qualificati di firme elettroniche possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento delle firme elettroniche qualificate.

4. Qualora un certificato qualificato di firme elettroniche sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea di un certificato qualificato di firma elettronica:

a) in caso di temporanea sospensione di un certificato qualificato di firma elettronica, il certificato perde la sua validità per il periodo della sospensione;

b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.

6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di firma elettronica. Si presume che i requisiti di cui all'allegato I siano stati rispettati ove un certificato qualificato di firma elettronica risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 29

Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata

1. I dispositivi per la creazione di una firma elettronica qualificata soddisfano i requisiti di cui all'allegato II.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai dispositivi per la creazione di una firma elettronica qualificata. Si presume che i requisiti di cui all'allegato II siano stati rispettati ove un dispositivo per la creazione di una

firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 30

Certificazione dei dispositivi per la creazione di una firma elettronica qualificata

1. La conformità dei dispositivi per la creazione di una firma elettronica qualificata con i requisiti stabiliti all'allegato II è certificata da appropriati organismi pubblici o privati designati dagli Stati membri.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dell'organismo pubblico o privato di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione degli Stati membri.

3. La certificazione di cui al paragrafo 1 si basa su uno dei seguenti elementi:

a) un processo di valutazione di sicurezza condotto conformemente a una delle norme per la valutazione di sicurezza dei prodotti informatici incluse nell'elenco redatto conformemente al secondo comma; o

b) un processo diverso da quello di cui alla lettera a), a condizione che utilizzi livelli di sicurezza comparabili e che l'organismo pubblico o privato di cui al paragrafo 1 notifichi tale processo alla Commissione. Detto processo può essere utilizzato solo in assenza delle norme di cui alla lettera a) ovvero quando è in corso un processo di valutazione di sicurezza di cui alla lettera a).

La Commissione adotta, mediante atti di esecuzione, un elenco di norme per la valutazione di sicurezza dei prodotti delle tecnologie dell'informazione di cui alla lettera a). Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 48, paragrafo 2.

4. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 47 riguardo alla fissazione di criteri specifici che gli organismi designati di cui al paragrafo 1 del presente articolo devono soddisfare.

Articolo 31

Pubblicazione di un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati

1. Gli Stati membri notificano alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la conclusione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica qualificata certificati dagli organismi di cui all'articolo 30, paragrafo 1. Essi notificano inoltre alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la cancellazione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica che non sono più certificati.

2. Sulla base delle informazioni pervenutele, la Commissione redige, pubblica e mantiene un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati.

3. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure applicabili ai fini del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 32

Requisiti per la convalida delle firme elettroniche qualificate

1. Il processo di convalida di una firma elettronica qualificata conferma la validità di una firma elettronica qualificata purché:

a) il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I;

b) il certificato qualificato sia stato rilasciato da un prestatore di servizi fiduciari qualificato e fosse valido al momento della firma;

c) i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione;

d) l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione;

e) l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era utilizzato al momento della firma;

f) la firma elettronica sia stata creata da un dispositivo per la creazione di una firma elettronica qualificata;

g) l'integrità dei dati firmati non sia stata compromessa;

h) i requisiti di cui all'articolo 26 fossero soddisfatti al momento della firma;

2. Il sistema utilizzato per convalidare la firma elettronica qualificata fornisce alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e le consente di rilevare eventuali questioni attinenti alla sicurezza.

3. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alla convalida delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove la convalida delle firme elettroniche qualificate risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 33

Servizio di convalida qualificato delle firme elettroniche qualificate

1. Un servizio di convalida qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che:

a) fornisce la convalida a norma dell'articolo 32, paragrafo 1; e

b) consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore del servizio di convalida qualificato.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di convalida qualificato di cui al paragrafo 1. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il servizio di convalida di una firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 34

Servizio di conservazione qualificato delle firme elettroniche qualificate

1. Un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le modalità del servizio di conservazione qualificato delle firme elettroniche qualificate rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 5

Sigilli elettronici

Articolo 35

Effetti giuridici dei sigilli elettronici

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.

3. Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

Articolo 36

Requisiti dei sigilli elettronici avanzati

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Articolo 37

Sigilli elettronici nei servizi pubblici

1. Se uno Stato membro richiede un sigillo elettronico avanzato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati, i sigilli elettronici avanzati basati su un certificato qualificato di sigillo elettronico e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

2. Se uno Stato membro richiede un sigillo elettronico avanzato basato su un certificato qualificato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per

suo conto, tale Stato membro riconosce i sigilli elettronici avanzati basati su un certificato qualificato e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per l'utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello del sigillo elettronico qualificato.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sigilli elettronici avanzati. Si presume che i requisiti per i sigilli elettronici avanzati di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 36 siano rispettati ove un sigillo elettronico avanzato soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento dei sigilli elettronici avanzati o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 38

Certificati qualificati di sigilli elettronici

1. I certificati qualificati di sigilli elettronici soddisfano i requisiti di cui all'allegato III.

2. I certificati qualificati di sigilli elettronici non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato III.

3. I certificati qualificati di sigilli elettronici possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento dei sigilli elettronici qualificati.

4. Qualora un certificato qualificato di un sigillo elettronico sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea dei certificati qualificati di sigilli elettronici:

a) in caso di temporanea sospensione di un certificato qualificato di sigillo elettronico, il certificato perde la sua validità per il periodo della sospensione;

b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.

6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 39

Dispositivi per la creazione di un sigillo elettronico qualificato

1. L'articolo 29 si applica mutatis mutandis ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.

2. L'articolo 30 si applica mutatis mutandis alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.

3. L'articolo 31 si applica mutatis mutandis alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

Articolo 40

Convalida e conservazione dei sigilli elettronici qualificati

Gli articoli 32, 33 e 34 si applicano mutatis mutandis alla convalida e alla conservazione dei sigilli elettronici qualificati.

SEZIONE 6

Validazione temporale elettronica

Articolo 41

Effetti giuridici della validazione temporale elettronica

1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.

2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.

3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

Articolo 42

Requisiti per la validazione temporale elettronica qualificata

1. Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti:

a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;

b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e

c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al collegamento della data e dell'ora ai dati e a fonti accurate di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e alla fonte accurata di misurazione del tempo rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 7

Servizi elettronici di recapito certificato

Articolo 43

Effetti giuridici di un servizio elettronico di recapito certificato

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.

2. I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

Articolo 44

Requisiti per i servizi elettronici di recapito certificato qualificati

1. I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:

a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;

b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;

c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;

e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;

f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai processi di invio e ricezione dei dati. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 8

Autenticazione dei siti web

Articolo 45

Requisiti per i certificati qualificati di autenticazione di siti web

1. I certificati qualificati di autenticazione di siti web soddisfano i requisiti di cui all'allegato IV.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di autenticazione di siti web. Si presume che i requisiti di cui all'allegato IV siano stati rispettati ove un certificato qualificato di autenticazione di sito web risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

CAPO IV
DOCUMENTI ELETTRONICI

Articolo 46

Effetti giuridici dei documenti elettronici

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

CAPO V
DELEGA DI POTERE E DISPOSIZIONI DI ESECUZIONE

Articolo 47

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare gli atti delegati di cui all'articolo 30, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal 17 settembre 2014.

3. La delega di potere di cui all'articolo 30, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

5. L'atto delegato adottato ai sensi dell'articolo 30, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 48

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

CAPO VI

DISPOSIZIONI FINALI

Articolo 49

Riesame

La Commissione riesamina l'applicazione del presente regolamento e presenta una relazione in proposito al Parlamento europeo e al Consiglio entro il 1º luglio 2020. La Commissione valuta in particolare se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche, compresi l'articolo 6, l'articolo 7, lettera f), e gli articoli 34, 43, 44 e 45, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso e dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici.

La relazione di cui al primo comma è corredata, se necessario, di proposte legislative.

Ogni quattro anni dopo la relazione di cui al primo paragrafo la Commissione presenta inoltre al Parlamento europeo e al Consiglio una relazione sui progressi compiuti nella realizzazione degli obiettivi del presente regolamento.

Articolo 50

Abrogazione

1. La direttiva 1999/93/CEE è abrogata con effetto dal 1º luglio 2016.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento.

Articolo 51

Disposizioni transitorie

1. I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata a norma dell'articolo 3, paragrafo 4, della direttiva 1999/93/CE sono considerati dispositivi per la creazione di una firma elettronica qualificata a norma del presente regolamento.

2. I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza.

3. Un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE presenta una relazione di valutazione della conformità all'organismo di vigilanza quanto prima e, comunque, non oltre il 1º luglio 2017. Fino alla presentazione della suddetta relazione di valutazione della conformità e fino a che l'organismo di vigilanza non ne abbia completato la valutazione, il prestatore di servizi di certificazione è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento.

4. Se un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE non presenta una relazione di valutazione della conformità all'organismo di vigilanza entro i termini di cui al paragrafo 3, egli non è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento a decorrere dal 2 luglio 2017.

Articolo 52

Entrata in vigore

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Il presente regolamento si applica a decorrere dal 1º luglio 2016, a eccezione delle seguenti disposizioni:

a) articolo 8, paragrafo 3, articolo 9, paragrafo 5, articolo 12, paragrafi da 2 a 9, articolo 17, paragrafo 8, articolo 19, paragrafo 4, articolo 20, paragrafo 4, articolo 21, paragrafo 4, articolo 22, paragrafo 5, articolo 23, paragrafo 3, articolo 24, paragrafo 5, articolo 27, paragrafi 4 e 5, articolo 28, paragrafo 6, articolo 29, paragrafo 2, articolo 30, paragrafi 3 e 4, articolo 31, paragrafo 3, articolo 32, paragrafo 3, articolo 33, paragrafo 2, articolo 34, paragrafo 2, articolo 37, paragrafi 4 e 5, articolo 38, paragrafo 6, articolo 42, paragrafo 2, articolo 44, paragrafo 2, articolo 45, paragrafo 2, articolo 47 e articolo 48, che si applicano dal 17 settembre 2014;

b) l'articolo 7, l'articolo 8, paragrafi 1 e 2, gli articoli 9, 10, 11 e l'articolo 12, paragrafo 1, si applicano a decorrere dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8;

c) l'articolo 6 si applica a decorrere da tre anni dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8.

3. Quando il regime di identificazione elettronica notificato è compreso nell'elenco pubblicato dalla Commissione ai sensi dell'articolo 9 prima della data di cui al paragrafo 2, lettera c), del presente articolo, il riconoscimento dei mezzi di identificazione elettronica in virtù di tale regime ai sensi dell'articolo 6 ha luogo non oltre 12 mesi dopo la pubblicazione di detto regime ma non prima della data di cui al paragrafo 2, lettera c), del presente articolo.

4. Nonostante il paragrafo 2, lettera c), del presente articolo, uno Stato membro può decidere che i mezzi di identificazione elettronica a norma del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, da un altro Stato membro, siano riconosciuti nel primo Stato membro a decorrere dalla data di pubblicazione degli atti di esecuzione di cui agli articoli 8, paragrafo 3, e 12, paragrafo 8. Gli Stati membri interessati ne informano la Commissione. La Commissione rende pubbliche tali informazioni.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 23 luglio 2014

Per il Parlamento europeo

Il presidente

M. SCHULZ

Per il Consiglio

Il presidente

S. GOZI

([1]) GU C 351 del 15.11.2012, pag. 73.

([2]) Posizione del Parlamento europeo del 3 aprile 2014 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 23 luglio 2014.

([3]) Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa a un quadro comunitario per le firme elettroniche (GU L 13 del 19.1.2000, pag. 12).

([4]) GU C 50 E del 21.2.2012, pag. 1.

([5]) Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno (GU L 376 del 27.12.2006, pag. 36).

([6]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

([7]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

([8]) Decisione 2010/48/CE del Consiglio, del 26 novembre 2009, relativa alla conclusione, da parte della Comunità europea, della convenzione delle Nazioni Unite sui diritti delle persone con disabilità (GU L 23 del 27.1.2010, pag. 35).

([9]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

([10]) 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 (GU L 274 del 20.10.2009, pag. 36).

([11]) Decisione 2011/130/UE della Commissione, del 25 febbraio 2011, che istituisce requisiti minimi per il trattamento transfrontaliero dei documenti firmati elettronicamente dalle autorità competenti a norma della direttiva 2006/123/CE del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno (GU L 53 del 26.2.2011, pag. 66).

([12]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

([13]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

([14]) GU C 28 del 30.1.2013, pag. 6.

([15]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

ALLEGATO I

REQUISITI PER I CERTIFICATI QUALIFICATI DI FIRMA ELETTRONICA

I certificati qualificati di firma elettronica contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

   — per una persona giuridica: il nome e, se del caso, il numero di registrazione quali figurano nei documenti ufficiali,

   — per una persona fisica: il nome della persona;

c) è chiaramente indicato almeno il nome del firmatario, o uno pseudonimo, qualora sia usato uno pseudonimo;

d) i dati di convalida della firma elettronica che corrispondono ai dati per la creazione di una firma elettronica;

e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;

i) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;

j) qualora i dati per la creazione di una firma elettronica connessi ai dati di convalida della firma elettronica siano ubicati in un dispositivo per la creazione di una firma elettronica qualificata, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

ALLEGATO II

REQUISITI PER I DISPOSITIVI PER LA CREAZIONE DI UNA FIRMA ELETTRONICA QUALIFICATA

1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno quanto segue:
   a) è ragionevolmente assicurata la riservatezza dei dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica;
   b) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica possono comparire in pratica una sola volta;
   c) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;
   d) i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.
2. I dispositivi per la creazione di una firma elettronica qualificata non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.
3. La generazione o la gestione dei dati per la creazione di una firma elettronica per conto del firmatario può essere effettuata solo da un prestatore di servizi fiduciari qualificato.
4. Fatto salvo il punto 1, lettera d), i prestatori di servizi fiduciari qualificati che gestiscono dati per la creazione di una firma elettronica per conto del firmatario possono duplicare i dati per la creazione di una firma elettronica solo a fini di back-up, purché rispettino i seguenti requisiti:
   a) la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali;
   b) il numero di insiemi di dati duplicati non eccede il minimo necessario per garantire la continuità del servizio.

ALLEGATO III

REQUISITI PER I CERTIFICATI QUALIFICATI DEI SIGILLI ELETTRONICI

I certificati qualificati dei sigilli elettronici contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di sigillo elettronico;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

   — per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,

   — per una persona fisica: il nome della persona;

c) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

d) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;

e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;

i) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;

j) qualora i dati per la creazione di un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

ALLEGATO IV

REQUISITI PER I CERTIFICATI QUALIFICATI DI AUTENTICAZIONE DI SITI WEB

I certificati qualificati di autenticazione di siti web contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di autenticazione di sito web;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

   — per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,

   — per una persona fisica: il nome della persona;

c) per le persone fisiche: almeno il nome della persona a cui è stato rilasciato il certificato, o uno pseudonimo. Qualora sia usato uno pseudonimo, ciò è chiaramente indicato;

per le persone giuridiche: almeno il nome della persona giuridica cui è stato rilasciato il certificato e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

d) elementi dell'indirizzo, fra cui almeno la città e lo Stato, della persona fisica o giuridica cui è rilasciato il certificato e, se del caso, quali appaiono nei documenti ufficiali;

e) il nome del dominio o dei domini gestiti dalla persona fisica o giuridica cui è rilasciato il certificato;

f) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

g) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

h) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

i) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera h) è disponibile gratuitamente;

j) l'ubicazione dei servizi competenti per lo status di validità del certificato a cui ci si può rivolgere per informarsi sulla validità dei certificato qualificato.