COMMISSIONE EUROPEA

Bruxelles, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

(Testo rilevante ai fini del SEE)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

La presente relazione illustra una proposta di quadro normativo destinata a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno.

Instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico. La mancanza di fiducia scoraggia i consumatori, le imprese e le amministrazioni dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.

L'*Agenda digitale europea*[1] individua barriere che si frappongono allo sviluppo digitale dell'Europa e propone l'adozione di norme sulle firme elettroniche (azione fondamentale 3) e sul riconoscimento reciproco dell'identificazione e dell'autenticazione elettronica (azione fondamentale 16), in modo da istituire un quadro normativo chiaro che elimini la frammentazione, promuova l'interoperabilità, sviluppi la cittadinanza digitale e prevenga la criminalità cibernetica. L'adozione di norme per garantire il riconoscimento reciproco dell'identificazione e dell'autenticazione elettronica in tutta l'UE e il riesame della direttiva sulle firme elettroniche sono un'azione fondamentale anche dell'*Atto per il mercato unico*[2], per la realizzazione del mercato unico. La *Tabella di marcia per la stabilità e la crescita*[3] sottolinea il ruolo fondamentale, per lo sviluppo dell'economia digitale, del futuro quadro normativo comune per il riconoscimento e l'accettazione reciproci dell'identificazione e dell'autenticazione elettronica attraverso le frontiere.

Il quadro normativo proposto, che consiste in un "*regolamento del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*", mira a consentire transazioni elettroniche sicure e omogenee fra imprese, cittadini 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.

La normativa unionale esistente, vale a dire la direttiva 1999/93/CE relativa a un "*quadro comunitario per le firme elettroniche*"[4], si limita essenzialmente alle sole firme elettroniche. Non esiste un quadro unionale transfrontaliero e transettoriale completo per garantire transazioni elettroniche sicure, affidabili e di facile impiego, che comprenda l'identificazione, l'autenticazione e le firma elettronica.

L'obiettivo è quello di potenziare la normativa esistente e ampliarla per coprire il riconoscimento e l'accettazione reciproci a livello dell'UE dei regimi di identificazione elettronica notificata e di altri servizi fiduciari elettronici essenziali connessi.

2. CONSULTAZIONE DELLE PARTI INTERESSATE E VALUTAZIONI D'IMPATTO

La presente iniziativa è il risultato di ampie consultazioni sul riesame dell'attuale quadro normativo sulle firme elettroniche, durante le quali la Commissione ha raccolto i contributi

[1] COM(2010) 245 del 19.5.2010.
[2] COM (2011) 206 definitivo del 13.4.2011.
[3] COM(2011) 669 del 12.10.2011.
[4] GU L 13 del 19.1.2000, pag. 12.

degli Stati membri, del Parlamento europeo e di altre parti interessate[5]. Una consultazione pubblica online è stata integrata da un "gruppo pilota di PMI" incaricato di individuare i punti di vista e le esigenze specifiche delle PMI e da altre consultazioni mirate delle parti interessate[6,7]. La Commissione ha anche avviato una serie di studi sull'identificazione elettronica, sull'autenticazione elettronica, sulle firme elettroniche e sui servizi fiduciari connessi (eIAS).

Le consultazioni hanno evidenziato che un'ampia maggioranza di parti interessate si trova d'accordo sulla necessità di riesaminare il quadro attuale per colmare le lacune della direttiva sulle firme elettroniche. Tale approccio è infatti ritenuto migliore per rispondere alle sfide poste dal rapido sviluppo delle nuove tecnologie (in particolare per quanto riguarda l'accesso mobile e online) e dalla crescente globalizzazione, pur mantenendo la neutralità tecnologica del quadro giuridico.

In linea con l'approccio "Legiferare meglio", la Commissione ha svolto una valutazione dell'impatto di misure alternative. Sono stati valutati tre gruppi di opzioni strategiche, che riguardavano in particolare: 1) il campo di applicazione del nuovo quadro, 2) lo strumento giuridico e 3) il livello di vigilanza necessario[8]. L'opzione prescelta consiste nel migliorare la certezza giuridica, stimolare il coordinamento della vigilanza nazionale, garantire il riconoscimento e l'accettazione reciproci dei regimi di identificazione elettronica e incorporare servizi fiduciari essenziali connessi. La valutazione d'impatto ha concluso che in tal modo si otterrebbero miglioramenti significativi della certezza giuridica, della sicurezza e della fiducia per quanto riguarda le transazioni elettroniche transfrontaliere, riducendo la frammentazione del mercato.

---

5 Per dettagli sulle consultazioni, cfr. http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

6 Un seminario delle parti interessate si è tenuto il 10.3.2011 con rappresentanti dei settori pubblico e privato e del mondo accademico per discutere su quali provvedimenti normativi siano necessari per affrontare le sfide di domani. Si è trattato di un forum interattivo che ha permesso uno scambio di opinioni e la mappatura delle diverse posizioni sulle questioni sollevate nel corso della consultazione pubblica. Numerose organizzazioni hanno inviato spontaneamente dei documenti per illustrare le loro vedute.

7 In particolare, la presidenza polacca dell'UE ha organizzato una riunione con gli Stati membri sul tema delle firme elettroniche, tenutasi a Varsavia il 9.11.2011, e un'altra sull'identificazione elettronica, tenutasi a Poznan il 17.11.2011. Il 25.1.2012 la Commissione ha indetto un seminario con gli Stati membri per discutere le questioni in sospeso sull'identificazione, l'autenticazione e le firme elettroniche.

8 Nel primo gruppo, si sono esaminate quattro opzioni: abrogazione della direttiva sulle firme elettroniche; status quo; migliorare la certezza giuridica, stimolare il coordinamento della vigilanza nazionale e garantire il riconoscimento e l'accettazione reciproci delle eID; espansione per incorporare determinati servizi fiduciari connessi. Il secondo gruppo consisteva nella valutazione dei meriti relativi della possibilità di regolamentazione mediante uno o due strumenti e dell'opportunità di ricorrere a una direttiva piuttosto che a un regolamento. Il terzo gruppo ha raffrontato le implicazioni dell'attuazione di regimi nazionali di vigilanza basati su requisiti essenziali comuni di vigilanza, rispetto a un sistema di vigilanza unionale. Tutte le opzioni strategiche sono state valutate, con l'aiuto di un gruppo che comprendeva tutte le direzioni generali della Commissione interessate, sotto il profilo della loro efficacia per il raggiungimento degli obiettivi strategici, dell'impatto economico sulle parti interessate (compreso il bilancio delle istituzioni dell'UE), dell'impatto sociale e ambientale e degli effetti sugli oneri amministrativi.

3. ELEMENTI GIURIDICI DELLA PROPOSTA

3.1 Base giuridica

La proposta si basa sull'articolo 114 del TFUE, riguardante l'adozione di disposizioni per eliminare barriere esistenti al funzionamento del mercato interno. I cittadini, le imprese e le amministrazioni trarranno vantaggi dal riconoscimento e dall'accettazione reciproci dell'identificazione elettronica, dell'autenticazione elettronica, delle firme elettroniche e di altri servizi fiduciari attraverso le frontiere ove ciò si riveli necessario per avviare e completare procedimenti o transazioni elettroniche.

Si ritiene che un regolamento sia lo strumento giuridico più appropriato. Essendo direttamente applicabile a norma dell'articolo 288 del TFUE, un regolamento ridurrà la frammentazione normativa e fornirà una maggiore certezza giuridica introducendo un insieme armonizzato di regole fondamentali che contribuiranno al funzionamento del mercato interno.

3.2 Sussidiarietà e proporzionalità

Affinché l'azione a livello dell'Unione sia giustificata, deve essere rispettato il principio di sussidiarietà.

a) Natura transnazionale del problema (verifica di necessità)

Il carattere transnazionale degli eIAS richiede un'azione dell'UE. Da solo, un intervento interno (vale a dire nazionale) non basterebbe per raggiungere gli obiettivi e realizzare le mete indicate nella *strategia Europa 2020*[9]. D'altro canto, l'esperienza ha dimostrato che le misure nazionali hanno di fatto creato barriere all'interoperabilità delle firme elettroniche nell'Unione e hanno attualmente lo stesso effetto sull'identificazione elettronica, sull'autenticazione elettronica e sui servizi fiduciari connessi. È quindi necessario che l'UE crei un quadro che permetta di affrontare l'interoperabilità transfrontaliera e migliorare il coordinamento dei regimi nazionali di vigilanza. Tuttavia, l'identificazione elettronica non può essere disciplinata dal regolamento proposto secondo le stesse modalità generiche applicabili agli altri servizi fiduciari elettronici perché l'emissione di mezzi di identificazione è una prerogativa nazionale. La proposta s'incentra perciò esclusivamente sugli aspetti transfrontalieri dell'identificazione elettronica.

Il regolamento proposto crea condizioni eque di concorrenza per le imprese che prestano servizi fiduciari le quali attualmente operano in un contesto in cui le differenze fra le normative nazionali sono spesso fonte di incertezze giuridiche e oneri supplementari. La certezza del diritto risulta significativamente rafforzata da chiari obblighi di accettazione, da parte degli Stati membri, dei servizi fiduciari qualificati, che creano ulteriori incentivi per spingere le imprese ad estendere le loro attività oltre le frontiere del loro paese. Ad esempio, un'impresa potrà partecipare elettronicamente ad un appalto pubblico indetto dall'amministrazione di un altro Stato membro senza rischiare il blocco della sua firma elettronica a causa di requisiti nazionali specifici e di problemi di interoperabilità. Analogamente, un'impresa potrà firmare contratti elettronicamente con una controparte situata in un altro Stato membro senza doversi preoccupare di eventuali requisiti legali diversi per servizi fiduciari quali i sigilli elettronici, i documenti elettronici o la validazione temporale. Inoltre, le lettere di messa in mora potranno essere trasmesse da uno Stato membro all'altro con la certezza che saranno legalmente valide in entrambi. Da ultimo, il commercio

[9] Comunicazione della Commissione: Europa 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 del 3.3.2010.

online diventerà più affidabile quando i potenziali acquirenti avranno la possibilità di verificare che stanno effettivamente accedendo al sito del venditore prescelto e non a un sito contraffatto.

L'ampia accettazione dei mezzi di identificazione elettronica riconosciuti reciprocamente e delle firme elettroniche agevolerà la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di espandersi al di là delle frontiere senza andare incontro ad ostacoli nelle interazioni con le autorità pubbliche. In pratica, ne deriveranno significativi guadagni di efficienza sia per le imprese che per i cittadini nell'adempimento delle formalità amministrative. Ad esempio, gli studenti potranno iscriversi elettronicamente ad un'università estera, i cittadini potranno trasmettere la dichiarazione dei redditi online a un altro Stato membro e i pazienti avranno accesso online alla loro cartella clinica. In assenza di mezzi di identificazione elettronica che godano di riconoscimento reciproco, i medici non potranno accedere alle informazioni mediche di cui hanno bisogno per prestare le cure al paziente e occorrerà ripetere esami di laboratorio già effettuati.

b) Valore aggiunto (verifica di efficacia)

Attualmente il coordinamento volontario fra Stati membri non è in grado di realizzare gli obiettivi sopra delineati e non è probabile che ciò avvenga in futuro. Ne derivano la duplicazione degli sforzi, l'istituzione di standard diversi, caratteristiche transnazionali delle ricadute generate dalle TIC e la complessità amministrativa inerente ad un coordinamento istituito mediante accordi bilaterali e multilaterali.

Inoltre, l'esigenza di superare problemi, quali a) l'assenza di certezza giuridica in presenza di disposizioni nazionali eterogenee derivanti da interpretazioni divergenti della direttiva sulle firme elettroniche e b) una mancanza di interoperabilità fra i sistemi di firma elettronica istituiti a livello nazionale in seguito all'applicazione non uniforme delle norme tecniche, richiede un tipo di coordinamento fra Stati membri che può realizzarsi in modo più efficace a livello dell'UE.

3.3 Illustrazione dettagliata della proposta

3.3.1 CAPO I – DISPOSIZIONI GENERALI

L'articolo 1 definisce l'oggetto del regolamento.

L'articolo 2 definisce il campo d'applicazione materiale del regolamento.

L'articolo 3 contiene le definizioni della terminologia utilizzata nel regolamento. Alcune definizioni sono state riprese dalla direttiva 1999/93/CE, altre sono state rese più chiare, integrate da elementi aggiuntivi o introdotte ex novo.

L'articolo 4 determina i principi del mercato interno in funzione dell'applicazione territoriale del regolamento. Si fa menzione esplicita dell'inesistenza di restrizioni alla libertà di prestazione di servizi e di circolazione dei prodotti.

3.3.2 CAPO II – IDENTIFICAZIONE ELETTRONICA

L'articolo 5 dispone il riconoscimento e l'accettazione reciproci dei mezzi di identificazione elettronica che rientrano in un regime da notificare alla Commissione alle condizioni fissate dal regolamento. La maggior parte degli Stati membri ha introdotto una qualche forma di sistema di identificazione elettronica. Tuttavia, tali sistemi differiscono fra loro per molti

aspetti. La mancanza di una base giuridica comune che obblighi ogni Stato membro a riconoscere e accettare i mezzi di identificazione elettronica rilasciati in altri Stati membri per accedere a servizi online, insieme con l'inadeguatezza dell'interoperabilità transfrontaliera delle identificazioni elettroniche nazionali, crea barriere che impediscono ai cittadini e alle imprese di trarre pieno vantaggio dal mercato unico digitale. Il riconoscimento e l'accettazione reciproci di tutti i mezzi di identificazione elettronica che rientrano in un regime notificato ai sensi del presente regolamento elimina tali ostacoli giuridici.

Il regolamento non obbliga gli Stati membri a introdurre o notificare regimi di identificazione elettronica, ma a riconoscere ed accettare le identificazioni elettroniche notificate per quei servizi online il cui accesso richiede un'identificazione elettronica a livello nazionale. L'incremento potenziale delle economie di scala ottenute mediante l'impiego transfrontaliero di mezzi di identificazione elettronica e sistemi di autenticazione elettronica notificati potranno stimolare gli Stati membri a notificare i loro regimi di identificazione elettronica. L'articolo 6 fissa le cinque condizioni per la notifica dei regimi di identificazione elettronica:

gli Stati membri possono notificare i regimi di identificazione elettronica che essi accettano sotto la loro giurisdizione nei casi in cui l'identificazione elettronica è obbligatoria per servizi pubblici. Un ulteriore obbligo impone che i rispettivi mezzi di identificazione elettronica siano rilasciati direttamente dallo Stato membro che notifica un regime o a suo nome o almeno sotto la sua responsabilità.

Gli Stati membri devono garantire un legame univoco fra i dati di identificazione elettronica e la persona a cui questi si riferiscono. Tale obbligo non significa che una stessa persona non possa avere più mezzi di identificazione elettronica, ma questi ultimi devono essere tutti collegati alla stessa persona.

L'affidabilità di un'identificazione elettronica dipende dalla disponibilità di mezzi di autenticazione (ossia la possibilità di controllare la validità dei dati dell'identificazione elettronica). Il regolamento obbliga gli Stati membri notificanti a fornire l'autenticazione online gratuita ai terzi. La possibilità di autenticazione deve essere disponibile in modo ininterrotto. Non si possono imporre requisiti tecnici specifici, quali hardware o software, alle parti che ricorrono a tale autenticazione. Questa disposizione non si applica ad eventuali requisiti imposti agli utilizzatori (titolari) dei mezzi di identificazione elettronica che siano tecnicamente necessari per utilizzarli, quali lettori di carte.

Gli Stati membri devono accettare la responsabilità dell'univocità del legame (cioè del fatto che i dati di identificazione attribuiti ad una persona non siano collegati a nessun'altra persona) e della possibilità di autenticazione (ossia la possibilità di controllare la validità dei dati di identificazione elettronica). La responsabilità degli Stati membri non comprende altri aspetti del processo di identificazione né qualsiasi transazione che richiede l'identificazione.

L'articolo 7 contiene regole sulla notifica alla Commissione dei regimi di identificazione elettronica.

L'articolo 8 mira a garantire l'interoperabilità tecnica dei regimi di identificazione notificati, mediante un approccio coordinato che comprende atti delegati.

3.3.3 CAPO III – SERVIZI FIDUCIARI

3.3.3.1 Sezione 1 – Disposizioni generali

L’articolo 9 definisce i principi connessi alla responsabilità dei prestatori di servizi fiduciari qualificati e non qualificati. Esso si basa sull’articolo 6 della direttiva 1999/93/CE ed estende il diritto al risarcimento dei danni causati da un prestatore negligente di servizi fiduciari in seguito all’inosservanza di buone pratiche di sicurezza che diano luogo a una violazione della sicurezza con un impatto significativo sul servizio.

L’articolo 10 descrive il meccanismo di riconoscimento e accettazione dei servizi fiduciari qualificati prestati da un prestatore stabilito in un paese terzo. Esso si basa sull’articolo 7 della direttiva 1999/93/CE mantenendone solo l’unica opzione praticabile che consiste nel consentire tale riconoscimento in base a un accordo internazionale fra l’Unione europea e paesi terzi o organizzazioni internazionali.

L’articolo 11 definisce i principi della protezione e della limitazione dei dati. Si basa sull’articolo 8 della direttiva 1999/93/CE.

L’articolo 12 dispone che i servizi fiduciari siano accessibili alle persone disabili.

3.3.3.2 Sezione 2 – Vigilanza

L’articolo 13 obbliga gli Stati membri ad istituire organismi di vigilanza, sulla base dell’articolo 3, paragrafo 3, della direttiva 1999/93/CE, chiarendone ed ampliandone il mandato per quanto riguarda sia i prestatori di servizi fiduciari che i prestatori di servizi fiduciari qualificati.

L’articolo 14 introduce un meccanismo esplicito di mutua assistenza fra organismi di vigilanza negli Stati membri per facilitare la vigilanza transfrontaliera dei prestatori di servizi fiduciari. Introduce regole sulle operazioni congiunte e sul diritto delle autorità di vigilanza di parteciparvi.

L’articolo 15 introduce l’obbligo per i prestatori di servizi fiduciari qualificati e non qualificati di attuare provvedimenti tecnici e organizzativi appropriati per garantire la sicurezza delle loro attività. Inoltre, gli organismi competenti di vigilanza e le altre autorità pertinenti devono essere informati di tutte le violazioni della sicurezza. Se del caso, ne informano a loro volta gli organismi di vigilanza di altri Stati membri e – direttamente o attraverso il prestatore di servizi fiduciari interessato – il pubblico.

L’articolo 16 fissa le condizioni per la vigilanza dei prestatori di servizi fiduciari qualificati e dei servizi fiduciari qualificati da essi prestati. Obbliga i prestatori di servizi fiduciari qualificati a sottoporsi a una verifica annuale da parte di un organismo indipendente riconosciuto, per confermare all’organismo di vigilanza che adempiono gli obblighi sanciti dal regolamento. Inoltre, l’articolo 16, paragrafo 2, dà all’organismo di vigilanza il diritto di svolgere verifiche sul posto dei prestatori di servizi fiduciari qualificati, in qualsiasi momento. L’organismo di vigilanza ha anche la facoltà di emettere istruzioni vincolanti ai prestatori di servizi fiduciari qualificati per porre rimedio, in modo appropriato, ad eventuali inadempienze rilevate da una verifica di sicurezza.

L’articolo 17 riguarda le attività svolte dall’organismo di vigilanza su richiesta di un prestatore di servizi fiduciari che desideri avviare un servizio fiduciario qualificato.

L'articolo 18 dispone la preparazione di elenchi di fiducia[10] che contengono informazioni sui prestatori di servizi fiduciari soggetti a vigilanza e sui servizi qualificati da essi offerti. Tali informazioni devono essere rese pubbliche utilizzando un modello comune, per facilitarne l'impiego automatizzato e garantire un grado di dettaglio appropriato.

L'articolo 19 fissa i requisiti che i prestatori di servizi fiduciari qualificati devono soddisfare per essere riconosciuti come tali. Si basa sull'allegato II della direttiva 1999/93/CE.

3.3.3.3 Sezione 3 – Firma elettronica

L'articolo 20 sancisce le regole relative all'effetto giuridico delle firme elettroniche delle persone fisiche. Chiarisce ed estende l'articolo 5 della direttiva 1999/93/CE, introducendo l'obbligo esplicito di conferire alle firme elettroniche qualificate lo stesso effetto giuridico delle firme autografe. Inoltre, gli Stati membri devono garantire l'accettazione transfrontaliera delle firme elettroniche qualificate, nel contesto della fornitura di servizi pubblici, e non devono introdurre obblighi aggiuntivi che potrebbero trasformarsi in barriere all'impiego di tali firme.

L'articolo 21 fissa i requisiti per i certificati di firma qualificata. Chiarisce l'allegato I della direttiva 1999/93/CE ed elimina disposizioni che non hanno funzionato nella pratica (p. es. limiti al valore delle transazioni).

L'articolo 22 fissa i requisiti per i dispositivi per la creazione di firme elettroniche qualificate. Chiarisce i requisiti per i dispositivi per la creazione di una firma di cui all'articolo 3, paragrafo 5, della direttiva 1999/93/CE, che ora dovranno essere considerati dispositivi per la creazione di una firma qualificata ai sensi del regolamento proposto. Chiarisce anche che la portata di un dispositivo per la creazione di una firma qualificata può andare ben oltre un semplice contenitore di dati per la creazione di firme. La Commissione potrà anche stabilire un elenco di numeri di riferimento di norme applicabili ai requisiti di sicurezza sui dispositivi.

L'articolo 23, basato sull'articolo 3, paragrafo 4, della direttiva 1999/93/CE, introduce il concetto di certificazione dei dispositivi per la creazione di una firma elettronica qualificata per determinarne la conformità ai requisiti di sicurezza di cui all'allegato II. Tali dispositivi devono essere riconosciuti da tutti gli Stati membri quali conformi ai requisiti allorché un procedimento di certificazione è svolto da un organismo di certificazione designato da uno Stato membro. La Commissione pubblicherà un elenco positivo di tali dispositivi certificati ai sensi dell'articolo 24. La Commissione potrà anche elaborare un elenco di numeri di riferimento di norme applicabili alla valutazione di sicurezza dei prodotti delle tecnologie dell'informazione di cui all'articolo 23, paragrafo 1.

L'articolo 24 riguarda la pubblicazione di un elenco di dispositivi per la creazione di una firma elettronica qualificata, da parte della Commissione, previa notifica di conformità inviata dagli Stati membri.

L'articolo 25 si basa sulle raccomandazioni dell'allegato IV della direttiva 1999/93/CE per stabilire disposizioni vincolanti per la convalida di firme elettroniche qualificate, per migliorare la certezza giuridica di tali convalide.

[10] Gli elenchi di fiducia di cui alla decisione 2009/767/CE della Commissione, modificata dalla decisione 2010/425/CE della Commissione, saranno la base di una nuova decisione della Commissione sugli elenchi di fiducia derivata dal presente regolamento.

L’articolo 26 fissa le condizioni per i servizi di convalida qualificati.

L’articolo 27 fissa le condizioni per la conservazione a lungo termine delle firme elettroniche qualificate. Tale conservazione è resa possibile dall’impiego di procedure e tecnologie in grado di estendere l’affidabilità dei dati di convalida delle firme elettroniche qualificate oltre il termine della loro validità tecnologica, quando la falsificazione potrebbe diventare più facile per i criminali cibernetici.

3.3.3.4 Sezione 4 – Sigilli elettronici

L’articolo 28 riguarda gli effetti giuridici dei sigilli elettronici delle persone giuridiche. Il sigillo elettronico qualificato dà luogo a una presunzione legale di garanzia dell’origine e dell’integrità dei documenti elettronici a cui è associato.

L’articolo 29 fissa i requisiti per i certificati qualificati di sigillo elettronico.

L’articolo 30 fissa i requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato, per la loro certificazione e per la pubblicazione del relativo elenco.

L’articolo 31 stabilisce le condizioni di convalida e conservazione dei sigilli elettronici qualificati.

3.3.3.5 Sezione 5 – Validazione temporale elettronica

L’articolo 32 riguarda gli effetti giuridici della validazione temporale elettronica. La validazione temporale elettronica dà luogo a una presunzione legale relativa alla certezza della data e dell’ora.

L’articolo 33 fissa i requisiti per la validazione temporale elettronica qualificata.

3.3.3.6 Sezione 6 – Documenti elettronici

L’articolo 34 riguarda gli effetti giuridici e le condizioni di accettazione dei documenti elettronici. Esiste una presunzione legale specifica quanto all’autenticità e all’integrità dei documenti elettronici firmati con una firma elettronica qualificata o recanti un sigillo elettronico qualificato. Per quanto riguarda l’accettazione dei documenti elettronici, ove per la prestazione di un servizio pubblico si richieda un documento originale o una copia autenticata, sono accettati negli altri Stati membri senza requisiti aggiuntivi almeno i documenti elettronici rilasciati dalle persone competenti per rilasciare i documenti richiesti e considerati alla stregua di originali o di copie autenticate dalla normativa nazionale dello Stato membro di origine.

3.3.3.7 Sezione 7 – Servizi elettronici di recapito

L’articolo 35 verte sugli effetti giuridici dei dati inviati o ricevuti mediante un servizio elettronico di recapito. Per i servizi elettronici di recapito esiste la presunzione legale specifica quanto all’integrità dei dati inviati o ricevuti e all’accuratezza della data e dell’ora in cui tali dati sono inviati o ricevuti. È anche garantita l’accettazione reciproca dei servizi elettronici di recapito qualificati a livello dell’UE.

L’articolo 36 fissa i requisiti per i servizi elettronici di recapito qualificati.

3.3.3.8 Sezione 8 – Autenticazione dei siti web

Questa sezione mira ad assicurare la garanzia di autenticità di un sito web in relazione al suo proprietario.

L'articolo 37 stabilisce i requisiti per i certificati qualificati di autenticazione di sito web, che possono essere utilizzati per garantire l'autenticità di un sito web. Un certificato qualificato di autenticazione di sito web fornirà un insieme minimo di informazioni affidabili sul sito stesso e sull'esistenza legale del suo proprietario.

3.3.4 CAPO IV – ATTI DELEGATI

L'articolo 38 contiene le disposizioni standard per l'esercizio delle deleghe a norma dell'articolo 290 del TFUE (atti delegati), che dà la facoltà al legislatore di delegare alla Commissione il potere di adottare atti non legislativi di portata generale che integrano o modificano determinati elementi non essenziali di un atto legislativo.

3.3.5 CAPO V – ATTI DI ESECUZIONE

L'articolo 39 dispone la procedura di comitato necessaria per il conferimento delle competenze di esecuzione alla Commissione nei casi in cui, conformemente all'articolo 291 del TFUE, sono necessarie condizioni uniformi di esecuzione degli atti giuridicamente vincolanti dell'Unione. Si applica la procedura d'esame.

3.3.6 CAPO VI – DISPOSIZIONI FINALI

L'articolo 40 impone alla Commissione di valutare l'applicazione del regolamento e presentare relazioni al riguardo.

L'articolo 41 abroga la direttiva 1999/93/CE e contiene disposizioni per agevolare la transizione dall'infrastruttura esistente per le firme elettroniche ai nuovi requisiti del regolamento.

L'articolo 42 reca la data di entrata in vigore del regolamento.

4. INCIDENZA SUL BILANCIO

Le specifiche implicazioni di bilancio della proposta riguardano i compiti assegnati alla Commissione europea, come indicato nella scheda finanziaria legislativa allegata alla presente proposta.

La proposta non ha ripercussioni sulle spese operative.

La scheda finanziaria legislativa che accompagna la presente proposta di regolamento ricomprende le incidenze di bilancio del regolamento stesso.

2012/0146 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

(Testo rilevante ai fini del SEE)

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[11],

sentito il garante europeo della protezione dei dati[12],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico. La mancanza di fiducia scoraggia i consumatori, le imprese e le amministrazioni 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, consentendo interazioni elettroniche sicure e omogenee fra imprese, cittadini 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, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche[13], riguarda essenzialmente le firme elettroniche e non fornisce 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.

---

11 GU C [...] del [...], pag.
12 GU C [...] del [...], pag.
13 GU L 13 del 19.1.2000, pag. 12.

(4) L'Agenda digitale europea[14] della Commissione 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 sua Relazione 2010 sulla cittadinanza dell'Unione, la Commissione ha ulteriormente sottolineato la necessità di risolvere i principali problemi che impediscono ai cittadini europei di godere dei vantaggi di un mercato unico digitale e di servizi digitali transfrontalieri[15].

(5) Il Consiglio europeo ha invitato la Commissione a creare un mercato unico digitale entro il 2015[16], a fare rapidi progressi in settori essenziali dell'economia digitale ed a promuovere un mercato unico digitale pienamente integrato[17] favorendo l'impiego transfrontaliero dei servizi online, con particolare riguardo all'agevolazione dell'identificazione e dell'autenticazione elettronica sicura.

(6) 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 eGovermnent in tutta l'Unione europea[18].

(7) 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[19].

(8) La direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno[20] 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 prestatori di servizi stabiliti in un altro Stato membro non possono valersi della loro identificazione elettronica per accedere a tali servizi perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti e accettati in altri Stati membri. Si tratta di una barriera elettronica che impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno. Disporre di mezzi di identificazione elettronica riconosciuti e accettati reciprocamente permetterà di

---

14 COM(2010) 245 definitivo/2.

15 Relazione 2010 sulla cittadinanza dell'Unione – Eliminare gli ostacoli all'esercizio dei diritti dei cittadini dell'Unione, COM(2010) 603 definitivo, punto 2.2.2, pag. 13.

16 4/2/2011: EUCO 2/1/11.

17 23/10/2011: EUCO 52/1/11.

18 Conclusioni del Consiglio sul piano d'azione europeo per l'eGovernment 2011-2015, 3093ª sessione del Consiglio Trasporti, Telecomunicazioni e Energia, Bruxelles, 27 maggio 2011.

19 Risoluzione del Parlamento europeo del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico, 21.9.2010, P7_TA(2010)0320, e risoluzione del Parlamento europeo del 15 giugno 2010 sulla governance di internet: le prossime tappe, P7_TA(2010)0208.

20 GU L 376 del 27.12.2006, pag. 36.

agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di espandersi al di là delle frontiere evitando molti ostacoli nelle interazioni con le autorità pubbliche.

(10) La 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[21], 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 e l'accettazione reciproci dell'identificazione e dell'autenticazione elettronica sono fattori essenziali 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) 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'accesso ai servizi pubblici. Il presente regolamento non intende intervenire sui sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli Stati membri. Lo scopo del presente regolamento è garantire che per l'accesso ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

(12) Occorre che gli Stati membri rimangano liberi di utilizzare o introdurre mezzi propri di accesso ai servizi online, a fini di identificazione, 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. Spetta agli Stati membri decidere se notificare 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.

(13) Occorre che il presente regolamento fissi talune condizioni in merito all'obbligo di accettazione dei mezzi di identificazione elettronica e alle modalità di notifica dei regimi. È opportuno che tali condizioni aiutino gli Stati membri a costruire la necessaria fiducia nei rispettivi regimi di identificazione elettronica e a riconoscere ed accettare reciprocamente i mezzi di identificazione elettronica che fanno parte dei regimi notificati. È opportuno che il principio del riconoscimento e dell'accettazione reciproci si applichi ove lo Stato membro notificante soddisfi le condizioni di notifica e la notifica sia stata pubblicata nella Gazzetta ufficiale dell'Unione europea. Tuttavia, occorre che l'accesso a tali servizi online e la loro fornitura finale al richiedente siano strettamente collegati al diritto ad usufruire di tali servizi alle condizioni stipulate dalla normativa nazionale.

(14) Occorre che gli Stati membri possano decidere di coinvolgere il settore privato nell'emissione dei mezzi di identificazione elettronica e di consentire al settore privato l'impiego di mezzi di identificazione elettronica nell'ambito di un regime notificato a

[21] GU L 88 del 4.4.2011, pag. 45.

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, occorre che la possibilità di autenticazione offerta dagli Stati membri sia disponibile alle parti facenti affidamento sulla certificazione senza discriminare fra il settore pubblico e il settore privato.

(15) L'impiego transfrontaliero di mezzi di identificazione elettronica nell'ambito di un regime notificato richiede che gli Stati membri collaborino nella fornitura dell'interoperabilità tecnica. Ciò esclude qualsiasi norma tecnica nazionale che imponga a soggetti di altri paesi, per esempio, di procurarsi specifici hardware o software per verificare e convalidare l'identificazione elettronica notificata. D'altro canto, è inevitabile l'imposizione di requisiti tecnici agli utilizzatori, derivanti dalle specifiche proprie del token utilizzato (p. es. smart card).

(16) È opportuno che la cooperazione fra gli Stati membri sia funzionale all'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. Occorre che lo scambio di informazioni e la condivisione delle migliori pratiche fra Stati membri, finalizzati al riconoscimento reciproco dei regimi, facilitino tale cooperazione.

(17) È anche opportuno che il presente regolamento istituisca un quadro giuridico generale per l'impiego dei servizi fiduciari elettronici. Tuttavia, non è opportuno che istituisca un obbligo generale di farne uso. In particolare, non è auspicabile che il regolamento copra la prestazione di servizi sulla base di accordi volontari di diritto privato, né aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici nei casi in cui la normativa nazionale o unionale preveda obblighi quanto alla forma.

(18) Al fine di contribuire all'impiego transfrontaliero generale di servizi fiduciari elettronici, è opportuno che sia possibile presentarli come prove in procedimenti giudiziali in tutti gli Stati membri.

(19) 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.

(20) In considerazione del ritmo dei mutamenti tecnologici, occorre che il presente regolamento adotti un approccio aperto alle innovazioni.

(21) Occorre 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.

(22) Al fine di migliorare la fiducia dei cittadini 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 volti a garantire un elevato livello di sicurezza di tutti i servizi e prodotti fiduciari qualificati impiegati o prestati.

(23) In linea con gli obblighi assunti a norma della Convenzione ONU per i diritti delle persone con disabilità, entrata in vigore nell'Unione, occorre garantire che le persone con disabilità possano utilizzare servizi fiduciari e prodotti destinati al consumatore finale impiegati nella prestazione di tali servizi alle stesse condizioni degli altri consumatori.

(24) Un prestatore di servizi fiduciari è responsabile del trattamento di dati personali e come tale deve adempiere agli obblighi di cui alla 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[22]. In particolare, è necessario ridurre al minimo possibile la raccolta di dati, tenendo conto dello scopo del servizio prestato.

(25) È opportuno che gli organismi di vigilanza collaborino e scambino informazioni con le autorità di protezione dei dati per garantire l'applicazione corretta della normativa sulla protezione dei dati da parte dei prestatori di servizi. In particolare, è auspicabile che lo scambio di informazioni copra gli incidenti di sicurezza e le violazioni dei dati personali.

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

(27) 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.

(28) È necessario 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 dei requisiti in tutta l'Unione è opportuno che gli Stati membri adottino procedure paragonabili e scambino informazioni sulle loro attività di vigilanza e sulle migliori pratiche del settore.

(29) 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.

(30) 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 fare obbligo agli organismi di vigilanza di fornire informazioni riassuntive alla Commissione e all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

(31) Per consentire alla Commissione e agli Stati membri di valutare l'impatto del presente regolamento, è opportuno che gli organismi di vigilanza abbiano l'obbligo di fornire statistiche sui servizi fiduciari qualificati e sulla loro utilizzazione.

---

22 GU L 281 del 23.11.1995, pag. 31.

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

(33) 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 garantiscano la conservazione dei dati dei prestatori di servizi fiduciari qualificati e li mantengano accessibili per un periodo di tempo appropriato, anche in caso di cessazione delle attività di un prestatore di servizi fiduciari qualificato.

(34) 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.

(35) Spetta ai prestatori di servizi fiduciari adempiere agli obblighi disposti dal presente regolamento per l'offerta di servizi fiduciari, in particolare per i servizi fiduciari qualificati. Gli organismi di vigilanza hanno la responsabilità di sorvegliare le modalità con cui i prestatori di servizi fiduciari adempiono a tali obblighi.

(36) 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.

(37) Gli elenchi di fiducia sono elementi essenziali per costruire la fiducia fra operatori di mercato perché indicano la condizione qualificata del prestatore di servizi al momento della vigilanza, ma non sono un requisito indispensabile per acquisire lo status di prestatore qualificato e offrire servizi fiduciari qualificati che derivano dall'osservanza delle disposizioni del presente regolamento.

(38) Dopo essere stato oggetto di notifica, un servizio fiduciario qualificato non può essere rifiutato per l'espletamento di un procedimento o di una formalità amministrativa da parte dell'ente pubblico interessato per il fatto di non figurare in uno degli elenchi di fiducia elaborati dagli Stati membri. A tal fine, per ente pubblico si intende qualsiasi autorità pubblica o altra entità incaricata della fornitura di servizi di eGovernment quali dichiarazione fiscale online, richiesta di certificati di nascita, partecipazione ad appalti pubblici online, ecc.

(39) 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, 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 del mercato interno[23], è opportuno che siano accettate anche firme elettroniche con una garanzia di sicurezza più debole.

(40) È auspicabile 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.

(41) Per garantire la certezza giuridica della validità della firma, è essenziale dettagliare quali componenti di una firma elettronica qualificata debbano essere valutati dalla parte facente affidamento sulla certificazione che effettua la convalida. Inoltre, è opportuno che attraverso la definizione 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 o pubblico in tali servizi. È auspicabile che entrambi gli elementi rendano la convalida delle firme elettroniche qualificate semplice e agevole per tutte le parti a livello dell'Unione.

(42) 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.

(43) 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.

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

(45) Per migliorare l'impiego transfrontaliero dei documenti elettronici, è opportuno che il presente regolamento disponga che i documenti elettronici generino effetti giuridici e siano considerati di pari valore ai documenti cartacei, in funzione della valutazione del rischio e purché ne siano garantite l'autenticità e l'integrità. È anche importante, per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno, che i documenti elettronici originali, o copie autenticate degli stessi, rilasciati da organi competenti in uno Stato membro in osservanza della normativa nazionale vigente siano accettati come tali anche negli altri Stati membri. È opportuno che il presente regolamento lasci impregiudicato il diritto degli Stati membri di determinare ciò che costituisce un originale o una copia a livello nazionale ma garantisca che essi possano essere utilizzati come tali anche in altri Stati membri.

(46) 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.

---

[23] GU L 274 del 20.10.2009, pag. 36.

Analogamente, allorché le autorità competenti negli Stati membri fanno uso di sigilli elettronici, occorre garantire che supportino almeno alcuni formati di sigillo elettronico avanzato.

(47) 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.

(48) Rendendo possibile l'autenticazione dei siti web e dei loro proprietari diventerebbe più difficile falsificarli e si ridurrebbero le frodi.

(49) Per completare determinati aspetti tecnici dettagliati del presente regolamento in modo flessibile e veloce, occorre delegare alla Commissione il potere di adottare atti, ai sensi dell'articolo 290 del trattato sul funzionamento dell'Unione europea, riguardo all'interoperabilità dell'identificazione elettronica, alle misure di sicurezza obbligatorie per i prestatori di servizi fiduciari, agli organismi indipendenti riconosciuti responsabili della verifica dei prestatori di servizi, agli elenchi di fiducia, ai requisiti relativi ai livelli di sicurezza delle firme elettroniche, ai requisiti relativi ai certificati qualificati per le firme elettroniche e alla loro convalida e conservazione, agli organismi responsabili della certificazione dei dispositivi per la creazione di una firma elettronica qualificata, ai requisiti relativi ai livelli di sicurezza dei sigilli elettronici e ai certificati qualificati per i sigilli elettronici, all'interoperabilità fra servizi di recapito. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche presso esperti.

(50) Nel contesto della preparazione e della stesura degli atti delegati, è necessario che la Commissione garantisca la trasmissione corretta, tempestiva e simultanea dei documenti pertinenti al Parlamento europeo e al Consiglio.

(51) Per garantire condizioni uniformi di attuazione del presente regolamento, occorre attribuire 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 di cui al presente regolamento o definiti negli atti delegati. Occorre che tali competenze siano esercitate conformemente alle disposizioni del 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[24].

(52) Per motivi di certezza del diritto e di chiarezza occorre abrogare la direttiva 1999/93/CE.

(53) Per assicurare la certezza giuridica agli operatori di mercato che già fanno uso di certificati qualificati rilasciati a norma della direttiva 1999/93/CE, è necessario prevedere un idoneo periodo transitorio. È altresì necessario dotare la Commissione dei mezzi per adottare atti di esecuzione e atti delegati prima di tale data.

(54) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri e possono dunque, a motivo della portata dell'azione, essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al

[24] GU L 55 del 28.2.2011, pag. 13.

principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo, segnatamente per quanto attiene al ruolo della Commissione di coordinatrice delle attività nazionali,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

1. Il presente regolamento stabilisce le norme per l'identificazione elettronica e i servizi fiduciari elettronici per le transazioni elettroniche, allo scopo di garantire il buon funzionamento del mercato interno.

2. Il presente regolamento fissa le condizioni a cui gli Stati membri riconoscono e accettano i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro.

3. Il presente regolamento istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, la validazione temporale elettronica, i documenti elettronici, i servizi elettronici di recapito e l'autenticazione dei siti web.

4. Il presente regolamento garantisce che i servizi e prodotti fiduciari ad esso conformi sono autorizzati a circolare liberamente nel mercato interno.

Articolo 2

Campo di applicazione

1. Il presente regolamento si applica all'identificazione elettronica fornita dagli Stati membri o a loro nome o sotto la loro responsabilità, nonché ai prestatori di servizi fiduciari stabiliti nell'Unione.

2. Il presente regolamento non si applica alla prestazione di servizi fiduciari elettronici sulla base di accordi volontari di diritto privato.

3. Il presente regolamento non si applica agli aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici per i quali la normativa nazionale o unionale prevedano obblighi formali.

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 per rappresentare in modo univoco una persona fisica o giuridica;

2) “mezzi di identificazione elettronica”, un’unità materiale o immateriale contenente dati di cui al punto 1 del presente articolo, utilizzata per accedere ai servizi online di cui all’articolo 5;

3) “regime di identificazione elettronica”, un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica a persone di cui al punto 1 del presente articolo;

4) “autenticazione”, un processo elettronico che consente di convalidare l’identificazione elettronica di una persona fisica o giuridica; oppure l’origine e l’integrità di dati elettronici;

5) “firmatario”, una persona fisica che crea una firma elettronica;

6) "firma elettronica", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata dal firmatario per firmare;

7) "firma elettronica avanzata", una firma elettronica che soddisfi i seguenti requisiti:

(a) è connessa esclusivamente al firmatario;

(b) è idonea ad 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 cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati;

8) “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;

9) “dati per la creazione di una firma elettronica”, i dati unici utilizzati dal firmatario per creare una firma elettronica;

10) “certificato”, un attestato elettronico che collega al certificato i dati di convalida di una firma elettronica o di un sigillo elettronico di una persona fisica o giuridica, rispettivamente, e conferma i dati di detta persona;

11) “certificato qualificato di firma elettronica”, un attestato utilizzato a sostegno delle firme elettroniche, rilasciato da un prestatore di servizi fiduciari qualificato e conforme ai requisiti di cui all'allegato I;

12) “servizio fiduciario”, qualsiasi servizio elettronico che consiste nella creazione, verifica, convalida, nel trattamento e nella conservazione di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito, autenticazione di siti web e certificati elettronici, compresi i certificati di firma elettronica e di sigillo elettronico;

13) “servizio fiduciario qualificato”, un servizio fiduciario che soddisfa i requisiti pertinenti di cui al presente regolamento;

14) “prestatore di servizi fiduciari”, una persona fisica o giuridica che presta uno o più servizi fiduciari;

15) “prestatore di servizi fiduciari qualificato”, un prestatore di servizi fiduciari che soddisfa i requisiti di cui al presente regolamento;

16) “prodotto”, un hardware o software o i suoi componenti, destinati ad essere utilizzati per la prestazione di servizi fiduciari;

17) “dispositivo per la creazione di una firma elettronica”, un software o hardware configurato utilizzato per creare una firma elettronica;

18) "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;

19) “creatore di un sigillo”, una persona giuridica che crea un sigillo elettronico;

20) "sigillo elettronico", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici per garantire l’origine e l’integrità dei dati associati;

21) "sigillo elettronico avanzato", un sigillo elettronico che soddisfi i seguenti requisiti:

(a) è connesso in maniera unica 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, utilizzare 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;

22) “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;

23) “dati per la creazione di un sigillo elettronico”, i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

24) “certificato qualificato di sigillo elettronico”, un attestato utilizzato a sostegno di un sigillo elettronico, rilasciato da un prestatore di servizi fiduciari qualificato e conforme ai requisiti di cui all'allegato III;

25) “validazione temporale elettronica”, dati in forma elettronica che collegano altri dati elettronici ad una particolare ora e data, così da provare che tali dati esistevano in quel momento;

26) “validazione temporale elettronica qualificata”, una validazione temporale elettronica che soddisfa i requisiti di cui all’articolo 33;

27) “documento elettronico”, un documento in formato elettronico;

28) “servizio elettronico di recapito”, un servizio che consente la trasmissione di dati 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;

29) “servizio elettronico di recapito qualificato”, un servizio elettronico di recapito che soddisfa i requisiti di cui all’articolo 36;

30) “certificato qualificato di autenticazione di sito web”, un attestato che consente di autenticare un sito web e collega il sito alla persona a cui il certificato è rilasciato; il certificato è rilasciato da un prestatore di servizi fiduciari qualificato e soddisfa i requisiti di cui all’allegato IV;

31) “dati di convalida”, dati utilizzati per convalidare una firma elettronica o 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 conformi al presente regolamento godono della libera circolazione nel mercato interno.

CAPO II

IDENTIFICAZIONE ELETTRONICA

Articolo 5

Riconoscimento e accettazione reciproci

Ove la normativa nazionale o la prassi amministrativa richiedano l’impiego di un’identificazione elettronica mediante mezzi di identificazione e autenticazione elettronica per accedere ad un servizio online, ogni mezzo di identificazione elettronica rilasciato in un altro Stato membro e che rientri in un regime compreso nell’elenco pubblicato dalla Commissione conformemente alla procedura di cui all’articolo 7 è riconosciuto e accettato ai fini dell’accesso a detto servizio.

Articolo 6

Condizioni di notifica dei regimi di identificazione elettronica

1. Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell’articolo 7 se soddisfa tutte le seguenti condizioni:

(a) i mezzi di identificazione elettronica sono rilasciati dallo Stato membro notificante oppure a suo nome o sotto la sua responsabilità;

(b) i mezzi di identificazione elettronica possono essere utilizzati per accedere almeno ai servizi pubblici che richiedono l’identificazione elettronica nello Stato membro notificante;

(c) lo Stato membro notificante garantisce che i dati di identificazione personale siano attribuiti univocamente alla persona fisica o giuridica di cui all’articolo 3, punto 1;

(d) lo Stato membro notificante garantisce la disponibilità di una possibilità di autenticazione online, in qualsiasi momento e a titolo gratuito, per consentire agli utilizzatori di convalidare i dati di identificazione personale che hanno ricevuto in forma elettronica. Gli Stati membri non impongono alcun requisito tecnico specifico alle parti facenti affidamento sulla certificazione stabilite fuori del loro territorio che intendono effettuare tale autenticazione. In caso di violazione o parziale compromissione del regime di identificazione notificato o della possibilità di autenticazione, gli Stati membri sospendono o revocano senza indugio il regime di identificazione notificato o la possibilità di autenticazione o le loro parti compromesse e ne informano gli altri Stati membri e la Commissione ai sensi dell'articolo 7;

(e) lo Stato membro notificante è giuridicamente responsabile:

- i) dell'attribuzione univoca dei dati di identificazione personale di cui alla lettera c) e

- ii) della possibilità di autenticazione di cui alla lettera d).

2. La lettera e) del paragrafo 1 lascia impregiudicata la responsabilità delle parti di una transazione in cui sono utilizzati mezzi di identificazione elettronica che rientrano nel regime notificato.

Articolo 7

Notifica

1. Gli Stati membri che notificano un regime di identificazione elettronica inoltrano alla Commissione le informazioni seguenti e, senza indugio, qualsiasi successiva modifica:

(a) una descrizione del regime di identificazione elettronica notificato;

(b) le autorità responsabili del regime di identificazione elettronica notificato;

(c) informazioni su chi gestisce la registrazione degli identificatori personali univoci;

(d) una descrizione della possibilità di autenticazione;

(e) disposizioni per la sospensione o la revoca del regime di identificazione notificato o della possibilità di autenticazione o di parti compromesse dell'uno o dell'altra.

2. Sei mesi dopo l'entrata in vigore del regolamento, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* l'elenco dei regimi di identificazione elettronica notificati ai sensi del paragrafo 1 e le relative informazioni principali.

3. Se la Commissione riceve una notifica dopo la fine del periodo di cui al paragrafo 2, aggiorna l'elenco entro tre mesi.

4. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure della notifica di cui ai paragrafi 1 e 3. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 8

Coordinamento

1. Gli Stati membri collaborano fra loro per garantire l'interoperabilità dei mezzi di identificazione elettronica che rientrano in un regime notificato e per promuoverne la sicurezza.

2. La Commissione, mediante atti di esecuzione, fissa le modalità necessarie per facilitare la collaborazione fra gli Stati membri di cui al paragrafo 1, al fine di promuovere un elevato livello di fiducia e di sicurezza, commisurato al grado di rischio esistente. Detti atti di esecuzione riguardano, in particolare, lo scambio di informazioni, di esperienze e di buone pratiche in materia di regimi di identificazione elettronica, la valutazione tra pari dei regimi di identificazione elettronica notificati e l'esame di sviluppi pertinenti verificatisi nel settore dell'identificazione elettronica da parte delle autorità competenti degli Stati membri. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

3. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 riguardo all'agevolazione dell'interoperabilità transfrontaliera dei mezzi di identificazione elettronica, fissando requisiti tecnici minimi.

CAPO III

SERVIZI FIDUCIARI

Sezione 1

Disposizioni generali

Articolo 9

Responsabilità

1. I prestatori di servizi fiduciari sono responsabili di qualsiasi danno diretto causato a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi di cui all'articolo 15, paragrafo 1, salvo se possono dimostrare di non aver agito con negligenza.

2. I prestatori di servizi fiduciari qualificati sono responsabili di qualsiasi danno diretto causato a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi di cui al presente regolamento, in particolare all'articolo 19, salvo se possono dimostrare di non aver agito con negligenza.

Articolo 10

Prestatori di servizi fiduciari di paesi terzi

1. I servizi fiduciari qualificati e i certificati qualificati forniti da prestatori di servizi fiduciari qualificati stabiliti in un paese terzo sono accettati quali servizi fiduciari qualificati e certificati qualificati forniti da prestatori di servizi fiduciari qualificati stabiliti nel territorio dell'Unione purché i servizi fiduciari qualificati o i certificati qualificati aventi origine nel paese terzo siano riconosciuti a norma di un accordo fra l'Unione e paesi terzi od organizzazioni internazionali in conformità all'articolo 218 del TFUE.

2. In relazione al paragrafo 1, tali accordi garantiscono che i requisiti che si applicano ai servizi fiduciari qualificati e ai certificati qualificati forniti da prestatori di servizi fiduciari qualificati stabiliti nel territorio dell'Unione siano soddisfatti dai prestatori di servizi fiduciari nei paesi terzi o presso le organizzazioni internazionali, in particolare per quanto riguarda la protezione dei dati personali, la sicurezza e la vigilanza.

Articolo 11

Trattamento e protezione dei dati

1. I prestatori di servizi fiduciari e gli organismi di vigilanza garantiscono un trattamento dei dati personali leale e lecito ai sensi della direttiva 95/46/CE.

2. I prestatori di servizi fiduciari trattano i dati personali in conformità alla direttiva 95/46/CE. Il trattamento si limita rigorosamente ai dati minimi necessari per rilasciare e conservare un certificato o per prestare un servizio fiduciario.

3. I prestatori di servizi fiduciari garantiscono la riservatezza e l'integrità dei dati riferiti alla persona a cui il servizio fiduciario viene prestato.

4. Fatti salvi gli effetti giuridici che la legislazione nazionale attribuisce agli pseudonimi, gli Stati membri non vietano al prestatore di servizi fiduciari di riportare sui certificati di firma elettronica uno pseudonimo in luogo del nome del firmatario.

Articolo 12

Accessibilità per le persone con disabilità

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 in tutti i casi in cui ciò è possibile.

Sezione 2

Vigilanza

Articolo 13

Organismo di vigilanza

1. Gli Stati membri designano un organismo appropriato stabilito nel loro territorio o, di comune accordo, in un altro Stato membro sotto la responsabilità dello Stato membro designante. Agli organismi di vigilanza sono conferiti tutti i poteri di vigilanza e di indagine necessari per l'esercizio dei loro compiti.

2. L'organismo di vigilanza è responsabile dell'esecuzione dei seguenti compiti:

(a) monitorare i prestatori di servizi fiduciari stabiliti nel territorio dello Stato membro designante per assicurarsi che soddisfino i requisiti di cui all'articolo 15;

(b) svolgere la vigilanza dei prestatori di servizi fiduciari qualificati stabiliti nel territorio dello Stato membro designante e dei servizi fiduciari qualificati da essi prestati per assicurarsi che essi e i servizi fiduciari qualificati da essi prestati soddisfino i requisiti pertinenti stabiliti dal presente regolamento:

(c) assicurare che le informazioni e dati pertinenti di cui all'articolo 19, paragrafo 2, lettera g), registrati da prestatori di servizi fiduciari qualificati, siano conservati e mantenuti accessibili dopo la cessazione delle attività di un prestatore di servizi fiduciari qualificato, per un periodo di tempo appropriato onde garantire la continuità del servizio.

3. Ciascun organismo di vigilanza presenta alla Commissione e agli Stati membri una relazione annuale sulle attività di vigilanza svolte nell'ultimo anno civile, entro la fine del primo trimestre dell'anno successivo. La relazione comprende almeno:

(a) informazioni sulle attività di vigilanza;

(b) una sintesi delle notifiche di violazione ricevute da prestatori di servizi fiduciari a norma dell'articolo 15, paragrafo 2;

(c) statistiche sul mercato e sull'uso dei servizi fiduciari qualificati, comprese informazioni sui prestatori di servizi fiduciari qualificati, sui servizi fiduciari qualificati che essi prestano, sui prodotti che utilizzano e la descrizione generale dei loro clienti.

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

5. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 con riguardo alla definizione delle procedure applicabili ai compiti di cui al paragrafo 2.

6. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure della relazione di cui al paragrafo 3. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 14

Assistenza reciproca

1. Gli organismi di vigilanza collaborano fra loro al fine di scambiarsi buone pratiche e trasmettersi vicendevolmente, con la massima celerità, informazioni pertinenti e assistenza reciproca per poter svolgere le attività in modo coerente. L'assistenza reciproca copre, in particolare, le richieste di informazioni e le misure di vigilanza, quali richieste di svolgere ispezioni in connessione con verifiche di sicurezza di cui agli articoli 15, 16 e 17.

2. L'organismo di vigilanza cui è presentata una richiesta di assistenza non può rifiutare di darvi seguito, salvo che:

(a) non sia competente per trattarla, oppure

(b) l'intervento richiesto sia incompatibile con il presente regolamento.

3. Ove appropriato, gli organismi di vigilanza possono svolgere indagini congiunte con la partecipazione di membri del personale di organismi di vigilanza di altri Stati membri.

L'organismo di vigilanza dello Stato membro in cui si svolgerà l'indagine può, conformemente al proprio ordinamento nazionale, delegare compiti investigativi al personale dell'organismo di vigilanza assistito. Tali poteri possono essere esercitati solamente sotto la guida e in presenza del personale dell'organismo di vigilanza ospitante. Il personale dell'organismo di vigilanza assistito è soggetto alla legislazione nazionale dell'organismo di vigilanza ospitante. L'organismo di vigilanza ospitante assume la responsabilità delle azioni del personale dell'organismo di vigilanza assistito.

4. La Commissione può, mediante atti di esecuzione, specificare le modalità e le procedure dell'assistenza reciproca di cui al presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 15

Requisiti di sicurezza relativi ai prestatori di servizi fiduciari

1. I prestatori di servizi fiduciari stabiliti nel territorio dell'Unione adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati. Tenuto conto delle attuali conoscenze in materia, dette 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 le parti interessate sono informate degli effetti negativi di eventuali incidenti.

Fatto salvo l'articolo 16, paragrafo 1, il prestatore di servizi fiduciari può presentare all'organismo di vigilanza la relazione di una verifica di sicurezza svolta da un organismo indipendente riconosciuto, per confermare l'avvenuta adozione di misure di sicurezza appropriate.

2. I prestatori di servizi fiduciari notificano all'organismo di vigilanza competente, all'organismo nazionale competente per la sicurezza dell'informazione e ad altre parti interessate quali le autorità di protezione dei dati, senza indugio e ove possibile entro 24 ore dall'esserne venuti a conoscenza, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati e sui dati personali ivi custoditi.

Ove appropriato, in particolare qualora la violazione di sicurezza o la perdita di integrità riguardi due o più Stati membri, l'organismo di vigilanza interessato ne informa gli organismi di vigilanza negli altri Stati membri e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

L'organismo di vigilanza interessato può anche informare il pubblico o imporre al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione sia nell'interesse pubblico.

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

4. Al fine dell'attuazione dei paragrafi 1 e 2, l'organismo di vigilanza competente ha la facoltà di diramare istruzioni vincolanti ai prestatori di servizi fiduciari.

5. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 con riguardo all'ulteriore specificazione delle misure di cui al paragrafo 1.

6. La Commissione può, mediante atti di esecuzione, definire le circostanze, le modalità e le procedure, comprese le scadenze, applicabili ai fini dei paragrafi da 1 a 3. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 16

Vigilanza dei prestatori di servizi fiduciari qualificati

1. I prestatori di servizi fiduciari qualificati sono sottoposti una volta all'anno ad una verifica da parte di un organismo indipendente riconosciuto, per confermare che essi e i servizi fiduciari qualificati da essi prestati soddisfano i requisiti di cui al presente regolamento, e presentano la relazione di verifica di sicurezza all'organismo di vigilanza.

2. Fatto salvo il paragrafo 1, l'organismo di vigilanza può in qualsiasi momento, su iniziativa propria o in risposta ad una richiesta della Commissione, condurre una verifica dei prestatori di servizi fiduciari qualificati per confermare che essi e i servizi fiduciari qualificati da essi prestati continuano a soddisfare le condizioni di cui al presente regolamento. L'organismo di vigilanza comunica alle autorità di protezione dei dati i risultati delle verifiche effettuate nei casi in cui siano state rilevate violazioni delle norme di protezione dei dati personali.

3. L'organismo di vigilanza ha la facoltà di diramare istruzioni vincolanti ai prestatori di servizi fiduciari qualificati per ingiungere che rimedino a qualsiasi mancato adempimento rilevato nella relazione di verifica di sicurezza.

4. Con riferimento al paragrafo 3, se il prestatore di servizi fiduciari qualificato non rimedia a un siffatto mancato adempimento entro un limite di tempo stabilito dall'organismo di vigilanza, esso perde la propria qualifica e l'organismo di vigilanza gli comunica che la sua situazione sarà modificata di conseguenza negli elenchi di fiducia di cui all'articolo 18.

5. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 con riguardo alla specificazione delle condizioni per il riconoscimento dell'organismo indipendente che conduce la verifica di cui al paragrafo 1 del presente articolo, all'articolo 15, paragrafo 1, e all'articolo 17, paragrafo 1.

6. La Commissione può, mediante atti di esecuzione, definire le circostanze, le procedure e le modalità applicabili ai fini dei paragrafi 1, 2 e 4. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 17

Avviamento di un servizio fiduciario qualificato

1. I prestatori di servizi fiduciari qualificati notificano all'organismo di vigilanza la loro intenzione di iniziare a prestare un servizio fiduciario qualificato e presentano all'organismo di vigilanza una relazione di verifica di sicurezza effettuata da un organismo indipendente riconosciuto, a norma dell'articolo 16, paragrafo 1. I prestatori di servizi fiduciari possono

iniziare a prestare il servizio fiduciario qualificato dopo aver presentato la notifica e la relazione di verifica di sicurezza all'organismo di vigilanza.

2. Una volta presentati i documenti richiesti all'organismo di vigilanza a norma del paragrafo 1, i prestatori di servizi qualificati sono inseriti negli elenchi di fiducia di cui all'articolo 18 per indicare l'avvenuta presentazione della notifica.

3. L'organismo di vigilanza verifica che il prestatore di servizi fiduciari qualificato e i servizi fiduciari qualificati da esso prestati soddisfino i requisiti del presente regolamento.

L'organismo di vigilanza registra la qualifica dei prestatori di servizi fiduciari qualificati e dei servizi fiduciari qualificati da essi prestati negli elenchi di fiducia in seguito all'esito positivo della verifica e non oltre un mese dopo l'avvenuta notifica a norma del paragrafo 1.

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

4. Un servizio fiduciario qualificato che abbia provveduto alla notifica di cui al paragrafo 1 non può essere rifiutato per l'espletamento di una procedura o formalità amministrativa da parte dell'ente pubblico interessato per il fatto di non essere incluso negli elenchi di cui al paragrafo 3.

5. La Commissione può, mediante atti di esecuzione, definire le circostanze, le modalità e le procedure applicabili ai fini dei paragrafi da 1 a 3. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 18

Elenchi di fiducia

1. Tutti gli Stati membri istituiscono, mantengono e pubblicano elenchi di fiducia con informazioni relative ai prestatori di servizi fiduciari qualificati per i quali sono competenti, unitamente ad informazioni relative ai servizi fiduciari qualificati da essi prestati.

2. Gli Stati membri istituiscono, mantengono e pubblicano, in modo sicuro, 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 il certificato utilizzato per firmare o sigillare detti 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. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 con riguardo alla definizione delle informazioni di cui al paragrafo 1.

6. La Commissione può, mediante atti di esecuzione, definire 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 39, paragrafo 2.

Articolo 19

Requisiti per i prestatori di servizi fiduciari qualificati

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

Tali informazioni sono verificate dal prestatore di servizi qualificato o da un terzo autorizzato che agisce sotto la responsabilità del prestatore di servizi qualificato:

(a) mediante la comparizione fisica della persona fisica o di un rappresentante autorizzato della persona giuridica o

(b) a distanza, mediante mezzi di identificazione elettronica nell'ambito di un regime notificato rilasciati conformemente alla lettera a).

2. I prestatori di servizi fiduciari qualificati che prestano servizi fiduciari qualificati:

(a) impiegano personale dotato delle competenze, dell'esperienza e delle qualifiche necessarie, che applica procedure amministrative e gestionali che corrispondono a standard europei o internazionali ed ha ricevuto formazioni appropriate in materia di sicurezza e di norme di protezione dei dati personali;

(b) si assumono la responsabilità civile per danni mantenendo risorse finanziarie adeguate o attraverso un regime assicurativo di responsabilità civile appropriato;

(c) prima di avviare una relazione contrattuale informano chiunque intenda utilizzare un servizio fiduciario qualificato dei termini e delle condizioni esatte per l'utilizzazione di tale servizio;

(d) utilizzano sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità del processo che assicurano;

(e) utilizzano sistemi affidabili per memorizzare i dati ad essi forniti, in modo verificabile affinché:

- siano accessibili alla consultazione del pubblico soltanto con il consenso della persona a cui i dati sono stati rilasciati,
- soltanto le persone autorizzate possano effettuare inserimenti e modifiche;
- l'autenticità delle informazioni sia verificabile;

(f) adottano misure contro le falsificazioni e i furti di dati;

(g) registrano per un congruo periodo di tempo 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. Tali registrazioni possono essere elettroniche;

(h) dispongono di un piano di cessazione delle attività aggiornato per garantire la continuità del servizio conformemente alle disposizioni diramate dall'organismo di vigilanza a norma dell'articolo 13, paragrafo 2, lettera c);

(i) garantiscono il trattamento lecito dei dati personali a norma dell'articolo 11.

3. I prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati registrano nella loro banca dati dei certificati la revoca del certificato entro dieci minuti a decorrere dall'entrata in vigore della revoca.

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 in qualsiasi momento almeno per ogni certificato rilasciato, 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. Si presume che i requisiti di cui all'articolo 19 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 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

Sezione 3

Firma elettronica

Articolo 20

Effetti giuridici e accettazione delle firme elettroniche

1. Alla 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.

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

3. Le firme elettroniche qualificate sono riconosciute e accettate in tutti gli Stati membri.

4. Ove si richieda una firma elettronica con un livello di garanzia di sicurezza inferiore a quello della firma elettronica qualificata, in particolare per l'accesso a un servizio online offerto da un ente pubblico sulla base di una valutazione appropriata dei rischi che detto servizio comporta, tutte le firme elettroniche che raggiungono almeno lo stesso livello di garanzia di sicurezza sono riconosciute e accettate.

5. Gli Stati membri non richiedono, per l'accesso transfrontaliero a un servizio online offerto da un ente pubblico, una firma elettronica dotata di un livello di garanzia di sicurezza più elevato di quello di una firma elettronica qualificata.

6. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 per definire i diversi livelli di sicurezza della firma elettronica di cui al paragrafo 4.

7. La Commissione può, mediante atti di esecuzione, stabilire numeri di riferimento delle norme applicabili ai livelli di sicurezza della firma elettronica. Si presume che il livello di sicurezza definito in un atto delegato adottato ai sensi del paragrafo 6 sia stato rispettato ove una firma elettronica soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea.*

Articolo 21

Certificati qualificati di firma elettronica

1. I certificati qualificati di firma elettronica soddisfano i requisiti di cui all'allegato I.

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

3. Qualora un certificato qualificato di firma elettronica sia stato revocato dopo l'iniziale attivazione, esso decade completamente della propria validità e la sua situazione non viene ripristinata in nessuna circostanza mediante un rinnovo della validità.

4. La Commissione ha il potere di adottare atti delegati conformemente all'articolo 38 con riguardo all'ulteriore specificazione dei requisiti di cui all'allegato I.

5. 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 adempia a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 22

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 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 23

Certificazione dei dispositivi per la creazione di una firma elettronica qualificata

1. I dispositivi per la creazione di una firma elettronica qualificata possono essere certificati da appropriati organismi pubblici o privati designati dagli Stati membri purché siano stati sottoposti a un processo di valutazione di sicurezza condotto conformemente a una delle norme per la valutazione di sicurezza dei prodotti informatici incluse in un elenco da stabilire a cura della Commissione mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

2. Gli Stati membri notificano alla Commissione e agli altri Stati membri i nomi e gli indirizzi dell'organismo pubblico o privato da essi designato ai sensi del paragrafo 1.

3. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 con riguardo alla fissazione di criteri specifici che gli organismi designati ai sensi del paragrafo 1 devono soddisfare.

Articolo 24

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

1. Gli Stati membri notificano alla Commissione, senza indugio, informazioni sui dispositivi per la creazione di una firma elettronica qualificata certificati dagli organismi di cui all'articolo 23. Essi notificano inoltre alla Commissione, senza indugio, 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 le circostanze, 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 39, paragrafo 2.

Articolo 25

Requisiti per la convalida delle firme elettroniche qualificate

1. Una firma elettronica qualificata è considerata valida purché sia possibile stabilire con un elevato grado di sicurezza che all'atto della firma:

(a) il certificato associato alla firma è un certificato di firma elettronica qualificata conforme alle disposizioni di cui all'allegato I;

(b) il certificato qualificato richiesto è autentico e valido;

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

(d) l'insieme di dati che rappresenta il firmatario in modo univoco è correttamente trasmesso alla parte facente affidamento sulla certificazione;

(e) l’impiego di un eventuale pseudonimo è chiaramente indicato alla parte facente affidamento sulla certificazione, se del caso;

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

(g) l’integrità dei dati firmati non è stata compromessa;

(h) sono soddisfatti i requisiti di cui all’articolo 3, punto 7;

(i) il sistema utilizzato per convalidare la firma fornisce alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e consente all’utilizzatore di rilevare eventuali questioni attinenti alla sicurezza.

2. La Commissione ha il potere di adottare atti delegati conformemente all'articolo 38 con riguardo all’ulteriore specificazione dei requisiti di cui al paragrafo 1.

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 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell’Unione europea*.

Articolo 26

Servizio di convalida qualificato per le firme elettroniche qualificate

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

(a) fornisce la convalida a norma dell’articolo 25, paragrafo 1, e

(b) consente agli utilizzatori 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, lettera b), siano stati rispettati ove il servizio di convalida della firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell’Unione europea*.

Articolo 27

Conservazione delle firme elettroniche qualificate

1. Un servizio di conservazione delle firme elettroniche qualificate è prestato da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere

l’affidabilità dei dati di convalida della firma elettronica qualificata oltre il periodo di validità tecnologica.

2. La Commissione ha il potere di adottare atti delegati conformemente all'articolo 38 con riguardo all’ulteriore specificazione dei requisiti di cui al paragrafo 1.

3. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alla conservazione delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le misure di conservazione delle firme elettroniche qualificate rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell’Unione europea*.

Sezione 4

Sigilli elettronici

Articolo 28

Effetti giuridici del sigillo elettronico

1. Al 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.

2. Un sigillo elettronico qualificato gode della presunzione legale di garanzia dell’origine e dell’integrità dei dati a cui è associato.

3. I sigilli elettronici qualificati sono riconosciuti e accettati in tutti gli Stati membri.

4. Ove si richieda un sigillo elettronico con un livello di garanzia di sicurezza inferiore a quello del sigillo elettronico qualificato, in particolare per l’accesso a un servizio online offerto da un ente pubblico sulla base di una valutazione appropriata dei rischi che detto servizio comporta, tutti i sigilli elettronici che raggiungono almeno lo stesso livello di garanzia di sicurezza sono accettati.

5. Gli Stati membri non richiedono, per l’accesso a un servizio online offerto da un ente pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello dei sigilli elettronici qualificati.

6. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 per definire i diversi livelli di garanzia di sicurezza dei sigilli elettronici di cui al paragrafo 4.

7. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai livelli di garanzia di sicurezza dei sigilli elettronici. Si presume che il livello di garanzia di sicurezza definito in un atto delegato adottato ai sensi del paragrafo 6 sia stato rispettato se un sigillo elettronico soddisfa dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell’Unione europea*.

Articolo 29

Requisiti per i certificati qualificati di sigillo elettronico

1. I certificati qualificati di sigillo elettronico soddisfano i requisiti di cui all'allegato III.

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

3. Qualora un certificato qualificato di sigillo elettronico sia stato revocato dopo l'iniziale attivazione, esso perde la propria validità e il suo status non viene ripristinato in nessun caso mediante un rinnovo della validità.

4. La Commissione ha il potere di adottare atti delegati conformemente all'articolo 38 con riguardo all'ulteriore specificazione dei requisiti di cui all'allegato III.

5. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di sigillo elettronico. 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 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 30

Dispositivi per la creazione di un sigillo elettronico qualificato

1. L'articolo 22 si applica *mutatis mutandis* ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.

2. L'articolo 23 si applica *mutatis mutandis* alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.

3. L'articolo 24 si applica *mutatis mutandis* alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

Articolo 31

Convalida e conservazione dei sigilli elettronici qualificati

Gli articoli 25, 26 e 27 si applicano *mutatis mutandis* alla convalida e alla conservazione dei sigilli elettronici qualificati.

Sezione 5

Validazione temporale elettronica

Articolo 32

Effetto giuridico della validazione temporale elettronica

1. Alla validazione temporale elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

2. La validazione temporale elettronica gode della presunzione legale di garanzia dell'ora e della data che indica e dell'integrità dei dati a cui tale ora e data sono associate.

3. La validazione temporale elettronica qualificata è riconosciuta e accettata in tutti gli Stati membri.

Articolo 33

Requisiti per la validazione temporale elettronica qualificata

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

(a) è accuratamente collegata al tempo universale coordinato (UTC) in modo tale da escludere qualsiasi possibilità di modifica non rilevabile della data;

(b) si basa su una fonte accurata di misurazione del tempo;

(c) è rilasciata da un prestatore di servizi fiduciari qualificato;

(d) è apposta mediante una firma elettronica avanzata o 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 preciso dell'ora e della data ai dati e a una fonte accurata di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove un collegamento preciso della data e dell'ora ai dati e una fonte accurata di misurazione del tempo soddisfino dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

Sezione 6

Documenti elettronici

Articolo 34

Effetti giuridici e accettazione dei documenti elettronici

1. Un documento elettronico è considerato equivalente a un documento cartaceo ed è ammissibile come prova nei procedimenti giudiziali, tenuto conto del suo livello di garanzia di autenticità e di integrità.

2. Un documento recante una firma elettronica qualificata o un sigillo elettronico qualificato della persona competente per rilasciarlo gode della presunzione legale di autenticità e di integrità, purché non contenga elementi dinamici in grado di modificarlo automaticamente.

3. Ove per la prestazione di un servizio online offerto da un ente pubblico si richieda un documento originale o una copia autenticata, negli altri Stati membri sono accettati senza requisiti aggiuntivi almeno documenti elettronici rilasciati dalle persone competenti per

rilasciare i documenti richiesti e considerati alla stregua di originali o di copie autenticate dalla normativa nazionale dello Stato membro di origine.

4. La Commissione può, mediante atti di esecuzione, definire i formati delle firme elettroniche e dei sigilli elettronici che sono accettati ogniqualvolta uno Stato membro richieda un documento munito di firma o di sigillo per la fornitura di un servizio online offerto da un ente pubblico di cui al paragrafo 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Sezione 7

Servizio elettronico di recapito qualificato

Articolo 35

Effetto legale di un servizio elettronico di recapito

1. I dati inviati o ricevuti mediante un servizio elettronico di recapito sono ammissibili come prova in procedimenti giudiziali per quanto riguarda l'integrità dei dati e la certezza dell'ora e della data in cui i dati sono stati inviati o ricevuti da uno specifico destinatario.

2. I dati inviati o ricevuti mediante un servizio elettronico di recapito qualificato godono della presunzione legale quanto all'integrità dei dati e all'accuratezza dell'ora e della data della spedizione o della ricezione dei dati indicate dal sistema elettronico di recapito qualificato.

3. La Commissione ha il potere di adottare atti delegati a norma dell'articolo 38 con riguardo alla specificazione di meccanismi per l'invio o la ricezione di dati mediante servizi elettronici di recapito da utilizzare per promuovere l'interoperabilità dei servizi elettronici di recapito.

Articolo 36

Requisiti per i servizi elettronici di recapito qualificati

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

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

(b) consentono l'identificazione univoca del mittente e, se del caso, del destinatario;

(c) il processo di invio e ricezione dei dati è garantito 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;

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

(e) la data di invio e di ricezione e qualsiasi modifica dei dati devono essere indicate da una validazione temporale elettronica qualificata;

(f) qualora dei dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a e) 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 sia conforme a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

Sezione 8

Autenticazione dei siti web

Articolo 37

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. I certificati qualificati di autenticazione di siti web sono riconosciuti e accettati in tutti gli Stati membri.

3. La Commissione ha il potere di adottare atti delegati conformemente all'articolo 38 con riguardo all'ulteriore specificazione dei requisiti di cui all'allegato IV.

4. 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 dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione provvede a pubblicarli nella *Gazzetta ufficiale dell'Unione europea*.

CAPO IV

ATTI DELEGATI

Articolo 38

Esercizio della delega

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

2. Il potere di adottare atti delegati di cui all'articolo 8, paragrafo 3, all'articolo 13, paragrafo 5, all'articolo 15, paragrafo 5, all'articolo 16, paragrafo 5, all'articolo 18, paragrafo 5, all'articolo 20, paragrafo 6, all'articolo 21, paragrafo 4, all'articolo 23, paragrafo 3, all'articolo 25, paragrafo 2, all'articolo 27, paragrafo 2, all'articolo 28, paragrafo 6, all'articolo 29, paragrafo 4, all'articolo 30, paragrafo 2, all'articolo 31, all'articolo 35, paragrafo 3, e all'articolo 37, paragrafo 3, è conferito alla Commissione per un periodo indeterminato a decorrere dall'entrata in vigore del presente regolamento.

3. La delega di cui all'articolo 8, paragrafo 3, all'articolo 13, paragrafo 5, all'articolo 15, paragrafo 5, all'articolo 16, paragrafo 5, all'articolo 18, paragrafo 5, all'articolo 20, paragrafo 6, all'articolo 21, paragrafo 4, all'articolo 23, paragrafo 3, all'articolo 25, paragrafo 2, all'articolo 27, paragrafo 2, all'articolo 28, paragrafo 6, all'articolo 29, paragrafo 4, all'articolo 30, paragrafo 2, all'articolo 31, all'articolo 35, paragrafo 3, e all'articolo 37, paragrafo 3, può essere revocata in ogni momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega dei poteri precisati nella decisione medesima. 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 a norma dell'articolo 8, paragrafo 3, dell'articolo 13, paragrafo 5, dell'articolo 15, paragrafo 5, dell'articolo 16, paragrafo 5, dell'articolo 18, paragrafo 5, dell'articolo 20, paragrafo 6, dell'articolo 21, paragrafo 4, dell'articolo 23, paragrafo 3, dell'articolo 25, paragrafo 2, dell'articolo 27, paragrafo 2, dell'articolo 28, paragrafo 6, dell'articolo 29, paragrafo 4, dell'articolo 30, paragrafo 2, dell'articolo 31, dell'articolo 35, paragrafo 3, e dell'articolo 37, paragrafo 3, 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.

CAPO V

ATTI DI ESECUZIONE

Articolo 39

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 40

Relazione

La Commissione riferisce al Parlamento europeo e al Consiglio in merito all'applicazione del presente regolamento. La prima relazione è trasmessa entro quattro anni dall'entrata in vigore del presente regolamento. Le relazioni successive sono trasmesse ogni quattro anni.

Articolo 41

Abrogazione

1. La direttiva 1999/93/CE è abrogata.

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

3. 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 qualificata ai sensi del presente regolamento.

4. I certificati qualificati rilasciati a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza, ma per non più di cinque anni dall'entrata in vigore del presente regolamento.

Articolo 42

Entrata in vigore

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

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

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*La presidente*

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 il numero di registrazione quali appaiono nei documenti ufficiali,
- per una persona fisica: il nome;

(c) un insieme di dati che rappresentano in modo univoco il firmatario a cui è rilasciato il certificato e comprendono almeno il nome del firmatario o uno pseudonimo identificato come tale;

(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 competenti per lo status di validità dei certificato 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 relativi ai dispositivi per la creazione di una firma qualificata

1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno che:

(a) è assicurata la segretezza dei dati per la creazione di una firma elettronica utilizzati per generare una firma elettronica;

(b) i dati per la creazione di una firma elettronica utilizzati per generare una firma elettronica possono comparire una sola volta;

(c) i dati per la creazione di una firma elettronica utilizzati per generare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;

(d) i dati per la creazione di una firma elettronica utilizzati nella generazione della stessa possono essere sufficientemente 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 sono effettuate da un prestatore di servizi fiduciari qualificato.

4. 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 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 di sigillo elettronico

I certificati qualificati di sigillo elettronico 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 il numero di registrazione quali appaiono nei documenti ufficiali,
- per una persona fisica: il nome;

(c) un insieme di dati che rappresenta in modo univoco la persona giuridica a cui è rilasciato il certificato e include almeno il nome e 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 competenti per lo status di validità dei certificato 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 il numero di registrazione quali appaiono nei documenti ufficiali,
- per una persona fisica: il nome;

(c) un insieme di dati che rappresenta in modo univoco la persona giuridica a cui è rilasciato il certificato e include almeno il nome e il numero di registrazione quali appaiono nei documenti ufficiali;

(d) elementi dell'indirizzo, fra cui almeno la città e lo Stato membro, della persona giuridica a cui è rilasciato il certificato quali appaiono nei documenti ufficiali;

(e) il nome del dominio o dei domini gestiti dalla persona giuridica a 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 che avalla la firma elettronica avanzata o il sigillo elettronico avanzato di cui alla lettera g) 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.

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

La presente scheda finanziaria illustra le esigenze, in termini di spese amministrative, dell'attuazione del proposto regolamento *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*.

In seguito alla procedura legislativa e alla discussione per l'adozione del regolamento proposto da parte del Parlamento europeo e del Consiglio, la Commissione necessiterà di dodici ETP per elaborare gli atti delegati e di esecuzione connessi, garantire la disponibilità delle norme organizzative e tecniche, trattare le informazioni notificate dagli Stati membri – in particolare per mantenere le informazioni connesse agli elenchi di fiducia –, garantire la sensibilizzazione delle parti interessate – in particolare cittadini e PMI – sui vantaggi dell'utilizzazione dell'identificazione elettronica, dell'autenticazione elettronica, delle firme elettroniche e dei servizi fiduciari connessi (eIAS) e intavolare discussioni con paesi terzi in vista di raggiungere l'interoperabilità eIAS a livello mondiale.

1.1. Denominazione della proposta/iniziativa

Proposta della Commissione di regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

1.2. Settori interessati nella struttura ABM/ABB[25]

09 SOCIETÀ DELL'INFORMAZIONE

1.3. Natura della proposta/iniziativa

☐ La proposta/iniziativa riguarda **una nuova azione**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[26]

☐ La proposta/iniziativa riguarda **la proroga di un'azione esistente**

☑ La proposta/iniziativa riguarda **un'azione riorientata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivo/obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

Gli obiettivi generali della proposta sono quelli delle strategie generali dell'UE in cui essa si inserisce, quali la strategia Europa 2020, che mira a "trasformare l'UE in un'economia intelligente, sostenibile e inclusiva caratterizzata da alti livelli di occupazione, produttività e coesione sociale".

25 ABM: Activity Based Management – ABB: Activity Based Budgeting (bilancio per attività).

26 A norma dell'articolo 49, paragrafo 6, lettera a) o b), del regolamento finanziario.

1.4.2. Obiettivo/obiettivi specifici e attività ABM/ABB interessate

Migliorare la fiducia nelle transazioni elettroniche paneuropee e garantire il riconoscimento legale transfrontaliero dell'identificazione elettronica, dell'autenticazione elettronica, delle firme elettroniche e dei servizi fiduciari connessi, nonché un livello elevato di protezione dei dati e di responsabilizzazione degli utilizzatori nel mercato unico (cfr. l'Agenda digitale europea, azioni fondamentali 3 e 16).

Attività ABM/ABB interessate

09 02 – Quadro normativo dell'Agenda digitale europea

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Creare un contesto regolamentare chiaro per i servizi eIAS in grado di migliorare la convenienza, la fiducia e la sicurezza degli utenti nel mondo digitale.

1.4.4. Indicatori di risultato e di incidenza

Precisare gli indicatori che permettono di seguire la realizzazione della proposta/iniziativa.

1. L'esistenza di fornitori di eIAS che hanno attività in più Stati membri dell'UE;

2. il grado in cui i dispositivi diventano interoperabili (come i lettori di smart card) fra settori e paesi;

3. l'uso degli eIAS da parte di tutte le categorie di popolazione;

4. il grado in cui gli eIAS sono utilizzati dagli utilizzatori finali per le transazioni nazionali e internazionali (transfrontaliere);

5. il grado di armonizzazione fra Stati membri della normativa in materia di eIAS;

6. i regimi di identificazione elettronica notificati alla Commissione;

7. i servizi accessibili mediante mezzi di identificazione elettronica notificati nel settore pubblico (p. es. eGovernment, assistenza sanitaria online, eJustice, appalti pubblici elettronici);

8. i servizi accessibili mediante mezzi di identificazione elettronica notificati nel settore privato (p. es. servizi bancari online, commercio elettronico, giochi d'azzardo online, connessione a siti web, servizi internet più sicuri).

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità da coprire nel breve e lungo termine

Le differenze verificatesi fra Stati membri nel recepimento della direttiva sulle firme elettroniche, dovute a divergenze di interpretazione a livello nazionale, hanno portato a problemi transfrontalieri di interoperabilità e quindi a un panorama segmentato a livello di UE, con distorsioni nel mercato interno. A ciò si aggiunge la mancanza di fiducia nei sistemi elettronici, che impedisce ai cittadini europei di trarre vantaggio dagli stessi tipi di servizi del mondo digitale a cui hanno accesso nel mondo reale.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea

L'azione a livello dell'Unione europea produrrebbe vantaggi evidenti rispetto all'azione a livello degli Stati membri. L'esperienza ha dimostrato che le misure nazionali non solo sono insufficienti a rendere le transazioni elettroniche possibili attraverso le frontiere, ma hanno addirittura creato barriere all'interoperabilità delle firme elettroniche in tutta l'Unione e stanno sortendo attualmente lo stesso effetto per quanto riguarda l'identificazione elettronica, l'autenticazione elettronica e i servizi fiduciari connessi.

1.5.3. Insegnamenti tratti da esperienze analoghe

La proposta si basa sull'esperienza acquisita con la direttiva sulle firme elettroniche e sui problemi causati da un recepimento e da un'applicazione frammentari di tale direttiva, che hanno impedito di raggiungerne gli obiettivi.

1.5.4. Coerenza ed eventuale sinergia con altri strumenti pertinenti

La direttiva sulle firme elettroniche è interessata da numerose altre iniziative dell'UE istituite per eliminare i problemi di interoperabilità e di riconoscimento e accettazione transfrontaliera in connessione con alcuni tipi di transazioni elettroniche, quali la direttiva sui servizi, la direttiva sugli appalti pubblici, la direttiva IVA riveduta (fatture elettroniche) e il regolamento sull'iniziativa dei cittadini europei.

Inoltre, il regolamento proposto istituirà un quadro normativo propizio all'ampia diffusione dei progetti pilota su larga scala avviati a livello dell'UE per sostenere lo sviluppo di mezzi interoperabili e affidabili di comunicazione elettronica (fra cui SPOCS, a sostegno dell'attuazione della direttiva sui servizi; STORK, a sostegno dello sviluppo e dell'impiego di eID interoperabili; PEPPOL, a sostegno dello sviluppo e dell'impiego di soluzioni interoperabili per gli appalti elettronici; epSOS, a sostegno dello sviluppo e dell'impiego di soluzioni interoperabili per l'assistenza sanitaria online; eCodex, a sostegno dello sviluppo e dell'impiego di soluzioni interoperabili per l'eJustice).

1.6. Durata e incidenza finanziaria

☐ Proposta/iniziativa di **durata limitata**

– ☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ Incidenza finanziaria dal AAAA al AAAA

☑ Proposta/iniziativa di **durata illimitata**

1.7. Modalità di gestione previste[27]

☑ **Gestione centralizzata diretta** da parte della Commissione

[27] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

☐ **Gestione centralizzata indiretta** con delega delle funzioni di esecuzione a:

– ☐ agenzie esecutive

– ☐ organismi creati dalle Comunità[28]

– ☐ organismi pubblici nazionali/organismi investiti di attribuzioni di servizio pubblico

– ☐ persone incaricate di attuare azioni specifiche di cui al titolo V del trattato sull'Unione europea, che devono essere indicate nel pertinente atto di base ai sensi dell'articolo 49 del regolamento finanziario

☐ **Gestione concorrente** con gli Stati membri

☐ **Gestione decentrata** con paesi terzi

☐ **Gestione congiunta** con organizzazioni internazionali ***(specificare)***

Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".

Osservazioni

[//]

[28] A norma dell'articolo 185 del regolamento finanziario.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

La prima valutazione avrà luogo 4 anni dopo l'entrata in vigore del regolamento. Il regolamento comprende una disposizione esplicita sulla relazione che la Commissione trasmetterà al Parlamento europeo e al Consiglio sull'applicazione del regolamento stesso. Le relazioni successive saranno trasmesse ogni quattro anni. Sarà applicata la metodologia della Commissione in materia di valutazione. Tali valutazioni saranno realizzate con l'aiuto di studi mirati relativi all'attuazione degli strumenti giuridici, questionari inviati alle autorità nazionali, discussioni con esperti, seminari, sondaggi Eurobarometro, ecc.

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

È stata effettuata una valutazione d'impatto che accompagna la proposta di regolamento. Il nuovo strumento giuridico disporrà il riconoscimento e l'accettazione reciproci dell'identificazione elettronica attraverso le frontiere, migliorerà l'attuale quadro sulle firme elettroniche, rafforzerà la vigilanza nazionale sui prestatori di servizi fiduciari e conferirà efficacia giuridica e riconoscimento legale ai servizi fiduciari connessi. Inoltre, esso introduce l'impiego di atti delegati e di esecuzione quale meccanismo per garantire la flessibilità nei confronti degli sviluppi tecnologici.

2.2.2. Modalità di controllo previste

Gli stanziamenti supplementari saranno controllati secondo le modalità di controllo esistenti applicate dalla Commissione.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e di tutela in vigore o previste.

Gli stanziamenti supplementari saranno soggetti alle esistenti misure di prevenzione delle frodi applicate dalla Commissione.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio di spesa esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero [Denominazione…..……..….]	Diss./Non diss. (29)	di paesi EFTA[30]	di paesi candidati[31]	di paesi terzi	ai sensi dell'articolo 18, paragrafo 1, lettera a bis), del regolamento finanziario
5	09. 01 01 01 Spese relative al personale in attività di servizio nella DG Società dell'informazione e media	Non diss.	NO	NO	NO	NO
5	09. 01 02 01 Personale esterno	Non diss.	NO	NO	NO	NO

29 Diss. = Stanziamenti dissociati / Non diss. = Stanziamenti non dissociati.

30 EFTA: Associazione europea di libero scambio.

31 Paesi candidati e, se del caso, paesi potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Rubrica del quadro finanziario pluriennale:	Numero	[Rubrica 1. **Crescita intelligente e inclusiva** ……..……]

DG: INFSO			Anno **2014**	Anno **2015**	Anno **2016**	Anno **2017**	Anno 2018	**Anno 2019**	**Anno 2020**	**TOTALE**
• Stanziamenti operativi										
Numero della linea di bilancio – N.A.	Impegni	(1)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
	Pagamenti	(2)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Numero della linea di bilancio – N.A.	Impegni	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Pagamenti	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici[32]			0.000	0.000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Numero della linea di bilancio		(3)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
TOTALE degli stanziamenti per la DG INFSO	Impegni	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Pagamenti	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**

Rubrica del quadro finanziario pluriennale:	**5**	"Spese amministrative"

Mio EUR (al terzo decimale)

[32] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

		Anno **2014**	Anno **2015**	Anno **2016**	Anno **2017**	Anno **2018**	Anno **2019**	Anno **2020**	**TOTALE**
		DG: INFSO							
• Risorse umane		1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**
• Altre spese amministrative									
TOTALE DG INFSO	Stanziamenti	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

Mio EUR (al terzo decimale)

		Anno **2014**	Anno **2015**	Anno **2016**	Anno **2017**	Anno **2018**	Anno **2019**	Anno **2020**	**TOTALE**
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**
	Pagamenti	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

3.2.2. Incidenza prevista sugli stanziamenti operativi

– ☑ La proposta/iniziativa non comporta l'utilizzazione di stanziamenti operativi

– ☐ La proposta/iniziativa comporta l'utilizzazione di stanziamenti operativi, come spiegato di seguito:

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.3.1. Sintesi

– ☐ La proposta/iniziativa non comporta l'utilizzazione di stanziamenti amministrativi

– ☑ La proposta/iniziativa comporta l'utilizzazione di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **N 2014**	Anno **2015**	Anno **2016**	Anno **2017**	Anno **2018**	Anno **2019**	Anno **2020**	**TOTALE**
RUBRICA 5 del quadro finanziario pluriennale								
Risorse umane	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**
Altre spese amministrative								
Totale parziale RUBRICA 5 del quadro finanziario pluriennale	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

Esclusa la RUBRICA 5[33] del quadro finanziario pluriennale								
Risorse umane								
Altre spese di natura amministrativa								
Totale parziale esclusa la RUBRICA 5 del quadro finanziario pluriennale								

TOTALE	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

[33] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.2. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzazione di risorse umane
– ☑ La proposta/iniziativa comporta l'utilizzazione di risorse umane, come spiegato di seguito:

Stima da esprimere in numeri interi (o, al massimo, con un decimale)

		Anno **2014**	Anno **2015**	Anno **2016**	Anno **2017**	Anno **2018**	Anno **2019**	Anno **2020**
• Posti della tabella dell'organico (posti di funzionari e di agenti temporanei)								
09 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)		9	9	9	9	9	9	9
XX 01 01 02 (nelle delegazioni)								
XX 01 05 01 (ricerca indiretta)								
10 01 05 01 (ricerca diretta)								
• Personale esterno (in equivalenti a tempo pieno: ETP)[34]								
09 01 02 01 (AC, INT, END della dotazione globale)		3	3	3	3	3	3	3
XX 01 02 02 (AC, INT, JED, AL e END nelle delegazioni)								
XX 01 04 ***yy***[35]	- in sede[36]							
	- nelle delegazioni							
XX 01 05 02 (AC, INT, END – ricerca indiretta)								
10 01 05 02 (AC, INT, END – ricerca diretta)								
Altre linee di bilancio (specificare)								
TOTALE		**12**	**12**	**12**	**12**	**12**	**12**	**12**

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	Gestire le procedure legislative per l'adozione, da parte del Parlamento europeo e del Consiglio, del regolamento previsto e dei relativi atti delegati / di esecuzione. Settori prioritari: 1. Istituire un nuovo quadro normativo sui servizi fiduciari elettronici 2. Promuovere l'adozione dei servizi fiduciari elettronici sensibilizzando maggiormente le PMI e i cittadini quanto al potenziale di tali servizi 3. Dare proseguimento alla direttiva 1999/93/CE, compresi gli aspetti internazionali 4. Sviluppare il potenziale dei progetti pilota su larga scala per accelerare la realizzazione concreta dell'obiettivo del nuovo quadro normativo
Personale esterno	Come sopra

[34] AC= agente contrattuale; INT = personale interinale (*intérimaire*); JED = giovane esperto in delegazione (*jeune expert en délégation*) ; AL= agente locale; END= esperto nazionale distaccato.

[35] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

[36] Principalmente per i fondi strutturali, il Fondo europeo agricolo per lo sviluppo rurale (FEASR) e il Fondo europeo per la pesca (FEP).

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

– ☑ La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

– ☐ La proposta/iniziativa implica una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

Spiegare la riprogrammazione richiesta, precisando le linee di bilancio interessate e gli importi corrispondenti.

– ☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale[37].

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

– ☑ La proposta/iniziativa non prevede il cofinanziamento da parte di terzi

– ☐ La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

3.3. Incidenza prevista sulle entrate

– ☑ La proposta/iniziativa non ha alcuna incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

- ☐ sulle risorse proprie
- ☐ sulle entrate varie

[37] Cfr. punti 19 e 24 dell'Accordo interistituzionale.