



COMMISSIONE EUROPEA

Bruxelles, 4.6.2012
SWD(2012) 136 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

**Proposta di
REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

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

{COM(2012) 238 final}
{SWD(2012) 135 final}

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

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

1. CONTESTO POLITICO, QUESTIONI PROCEDURALI E CONSULTAZIONE DELLE PARTI INTERESSATE

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'iniziativa proposta mira a creare un quadro normativo per garantire transazioni elettroniche sicure e omogenee fra imprese, cittadini e amministrazioni, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico.

Le barriere ai servizi elettronici transfrontalieri esistono e vanno eliminate. Per essere strumenti produttivi e non ostacoli, **l'identificazione, l'autenticazione, le firme e i servizi fiduciari complementari (ancillary trust services, eIAS) elettronici** devono essere reciprocamente riconosciuti e accettati in tutta l'UE.

Non esiste un quadro unionale transfrontaliero e multisetoriale completo per i servizi eIAS. A livello dell'UE, esiste un quadro giuridico solamente per le firme elettroniche, ma non per l'identificazione e l'autenticazione elettroniche, né per i servizi fiduciari complementari. Nell'ambito dell'Agenda digitale europea, la Commissione ha annunciato che proporrà misure giuridiche per garantire il riconoscimento reciproco dell'identificazione elettronica (eID) e dell'autenticazione elettronica, in modo da eliminare la frammentazione, promuovere l'interoperabilità, sviluppare la cittadinanza digitale e prevenire la criminalità cibernetica.

Per svolgere la presente valutazione d'impatto, la Commissione ha raccolto i contributi degli Stati membri, del Parlamento europeo e delle parti interessate, in occasione di discussioni, seminari e conferenze. Diversi studi riguardo agli eIAS sono stati avviati e si è provveduto a una rassegna di pubblicazioni in merito. Nel 2011 è stata varata una consultazione pubblica per raccogliere elementi su come la eID e l'autenticazione e le firme elettroniche possono contribuire al mercato unico. Tale consultazione è stata integrata da un'indagine mirata volta a registrare gli specifici pareri e i bisogni delle PMI.

2. DEFINIZIONE DEL PROBLEMA

Gli utilizzatori possono incontrare difficoltà nell'uso transfrontaliero di servizi eIAS. I principali ostacoli che si frappongono all'impiego sicuro e omogeneo di eIAS transfrontalieri sono:

1 — Frammentazione del mercato: ai fornitori di servizi si applicano regole diverse a seconda dello Stato membro servito.

Per quanto riguarda le firme elettroniche, l'armonizzazione introdotta dalla direttiva 1999/93/CE sulle firme elettroniche è insufficiente. Sono stati identificati quattro problemi: un recepimento disomogeneo a livello nazionale in seguito ad interpretazioni divergenti della direttiva da parte degli Stati membri, l'invocazione *de facto* di una deroga per le applicazioni del settore pubblico, standard antiquati e obblighi poco chiari di vigilanza, che portano a problemi transfrontalieri di interoperabilità, a un panorama UE segmentato e a distorsioni nel mercato interno.

Riguardo alla eID, soluzioni tecnologiche diverse per l'identificazione personale nei singoli Stati membri, la mancanza di certezza giuridica per l'uso transfrontaliero di identità elettroniche e la mancanza di una chiara ripartizione delle responsabilità in materia di correttezza dei dati identificativi sono tutti fattori che portano a problemi di interoperabilità.

Quanto ai servizi fiduciari complementari, la mancanza di un quadro giuridico unionale comporta l'adozione di norme nazionali per alcuni di questi servizi in determinati Stati membri, con costi elevati per i prestatori che desiderano offrire i loro servizi in più Stati. Entrambe queste situazioni creano barriere al mercato interno e una situazione di frammentazione.

2 — Mancanza di fiducia: la mancanza di fiducia nei sistemi elettronici, negli strumenti disponibili e nel quadro giuridico può creare l'impressione che esistano meno salvaguardie giuridiche rispetto alle situazioni di interazione fisica.

Per le firme elettroniche, gli obblighi nazionali di vigilanza sono qualitativamente diversi da uno Stato membro all'altro, impedendo alle parti di affidarsi a una firma elettronica per valutare in che modo un fornitore di servizi sia sorvegliato.

Per la eID e i servizi fiduciari complementari, norme nazionali eterogenee non aiutano gli utilizzatori a sentirsi sicuri quando interagiscono online in situazioni transfrontaliere.

I quattro principali fattori chiave dei problemi elencati sono:

A: Campo di applicazione troppo ristretto dell'attuale quadro giuridico

I servizi eIAS sono indispensabili per un'ampia gamma di interazioni elettroniche come i servizi telebancari (eBanking), l'amministrazione in linea (eGovernment) e i servizi sanitari online (eHealth). A livello dell'UE esiste un quadro regolamentare limitato e imperfetto, incentrato essenzialmente sulle firme elettroniche. Non esiste alcun quadro specifico per il riconoscimento e la validazione temporale della eID o per i servizi fiduciari complementari, quali la validazione temporale e i sigilli elettronici.

B: Mancanza di coordinamento fra lo sviluppo delle firme elettroniche e dell'eID

Le infrastrutture nazionali di eIAS si sono sviluppate isolatamente, senza un coordinamento a livello dell'UE. Ne è derivata l'assenza di interoperabilità transfrontaliera delle soluzioni tecniche, che crea barriere alle transazioni elettroniche. La mancanza di riconoscimento e accettazione reciproci è uno dei motivi per cui sia gli utilizzatori che i prestatori di servizi elettronici sono scettici rispetto all'introduzione di servizi eIAS.

C: Mancanza di trasparenza delle garanzie di sicurezza

Una sicurezza forte e armonizzata è essenziale per la creazione di soluzioni affidabili. Ciò riveste particolare importanza per l'accesso a servizi che comportano dati personali sensibili come quelli sanitari. La direttiva 1999/93/CE ha riconosciuto che la certezza giuridica si può conferire esclusivamente alle firme elettroniche che garantiscono la sicurezza e sono pertanto

sufficientemente protette dalle contraffazioni e dalle frodi (firme elettroniche avanzate e qualificate).

Gli utilizzatori percepiscono la mancanza di sistemi sicuri di eID come una grossa barriera. La mancanza di un quadro giuridico armonizzato per la eID significa che la sicurezza e l'affidabilità delle eID ufficiali non può essere determinata in modo oggettivo nelle situazioni transfrontaliere. Ne derivano barriere transfrontaliere, una conseguente mancanza di fiducia e un mercato frammentato.

Un'altro motivo di preoccupazione è il furto di identità: eID sicure possono contribuire a ridurre questo rischio, mentre eID poco sicure rendono più facile per i criminali procurarsi eID false o compromesse.

D: Scarsa informazione e adesione da parte degli utilizzatori

La complessità delle tecnologie impiegate per le transazioni elettroniche e il ruolo essenziale di terzi fiduciari crea un ambiente in cui risulta difficile valutare la fiducia. In particolare, gli utilizzatori finali, che generalmente non dispongono di conoscenze sufficienti, devono potersi affidare a regole che stabiliscano chiari diritti e responsabilità per tutte le parti interessate (prestatori di servizi fiduciari, utilizzatori finali e organismi di governance).

3. SCENARIO DI BASE

Lo scenario di base dell'iniziativa è il mantenimento dello status quo. Si prevede che in questo scenario i problemi attuali si evolverebbero come segue:

I problemi di frammentazione e interoperabilità non verrebbero risolti: è probabile che gli Stati membri continuerebbero a recepire e applicare la direttiva 1999/93/CE.

La certezza giuridica non sarebbe garantita: i problemi creati dalla mancanza di riconoscimento reciproco delle firme elettroniche e dalla mancanza di un quadro giuridico per disciplinare il riconoscimento e l'accettazione reciproci della eID e dei servizi fiduciari complementari impedirebbe il riconoscimento giuridico di una serie di interazioni transfrontaliere.

Le necessità degli utilizzatori non sarebbero pienamente soddisfatte: nel quadro attuale, non è possibile avvalersi pienamente delle opportunità offerte dagli sviluppi tecnologici.

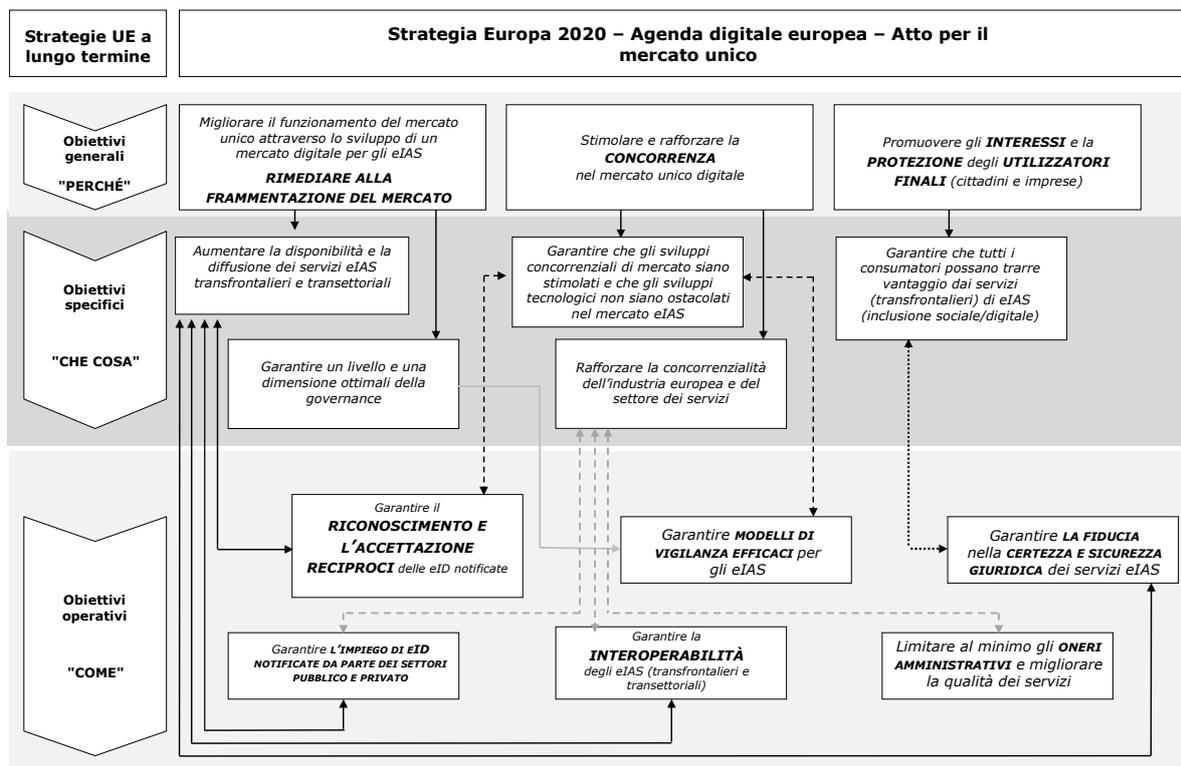
Grandi iniziative europee non svilupperebbero tutto il loro potenziale: iniziative europee quali le direttive sui servizi, sugli appalti pubblici e sull'IVA (fatture elettroniche) o i progetti pilota su larga scala ICT-PSP¹, che mirano ad eliminare i problemi di interoperabilità e di riconoscimento transfrontaliero legati a determinati tipi di interazioni elettroniche, potrebbero operare solo a livello di progetti pilota per la mancanza di un quadro normativo transettoriale.

4. OBIETTIVI STRATEGICI

Sono stati identificati quattro **obiettivi generali**: garantire lo sviluppo di un mercato unico digitale; promuovere lo sviluppo di servizi pubblici transfrontalieri fondamentali; incentivare e rafforzare la concorrenza nel mercato unico; migliorare la facilità d'impiego (per cittadini e imprese). Tali obiettivi sono in linea con strategie dell'UE quali la *Strategia Europa 2020*, l'*Agenda digitale europea*, l'*Atto per il mercato unico* e la *Tabella di marcia per la stabilità e la crescita*.

¹ http://ec.europa.eu/information_society/activities/ict_psp/about.

Gli **obiettivi specifici** esprimono i risultati sperati per il mercato eIAS (“che cosa”) dall’adozione dell’*obiettivo operativo* (“come”). Per ciascun obiettivo specifico sono stati individuati diversi **obiettivi operativi**.



5. OPZIONI STRATEGICHE

Per risolvere i problemi e raggiungere gli obiettivi, sono stati valutati tre gruppi di opzioni: 1) campo di applicazione del quadro previsto, 2) strumento giuridico e 3) livello di vigilanza:

- Nel primo gruppo, “*campo di applicazione del quadro normativo*”, si esaminano quattro opzioni:

Opzione 0: Abrogazione della direttiva 1999/93/CE e assenza di attività normative in materia di eID o servizi fiduciari complementari.

Questa opzione consiste nella cessazione di tutte le attività dell’UE nel campo delle firme elettroniche. La direttiva 1999/93/CE verrebbe abrogata e non si proporrebbe nessuna misura legislativa per il riconoscimento reciproco della eID.

- *Opzione 1:* Status quo (scenario di base)

La Direttiva 1999/93/CE sarebbe mantenuta senza modifiche. Non si proporrebbe nessuna norma sulla eID.

- *Opzione 2:* Migliorare la certezza giuridica, stimolare il coordinamento della supervisione nazionale e garantire il riconoscimento e l'accettazione reciproci delle eID

Si amplierebbe il campo d'applicazione della direttiva 1999/93/CE integrandovi disposizioni sul riconoscimento e sull'accettazione transfrontalieri dei regimi di "eID notificata"². Le disposizioni della direttiva sulle firme elettroniche sarebbero riviste per remediare alle attuali debolezze e così armonizzare meglio i modelli nazionali di vigilanza.

- *Opzione 3: Espansione per incorporare taluni servizi fiduciari complementari*

Questa opzione espande l'opzione 2 incorporando i servizi fiduciari complementari e le credenziali nel campo d'applicazione della proposta.

Gli elementi complementari essenziali da incorporare nella normativa sarebbero: validazione temporale, sigilli elettronici, conservazione delle informazioni a lungo termine, recapito certificato dei documenti elettronici, ammissibilità dei documenti elettronici e autenticazione dei siti web.

- Nel secondo gruppo, che comprende uno "strumento giuridico", si prendono in considerazione quattro opzioni:

O uno strumento legislativo complessivo (opzione A) o due strumenti distinti (opzione B)

La legislazione consisterebbe in un'unica misura complessiva che coprirebbe l'identificazione elettronica, l'autenticazione e la firma, oppure in due strumenti, vale a dire una decisione della Commissione sulla eID e una revisione della direttiva sulle firme elettroniche.

Una direttiva (opzione C) o un regolamento (opzione D):

L'atto potrebbe essere una direttiva o un regolamento.

- Al terzo livello, "vigilanza", si prendono in considerazione due opzioni:

Opzione i): Mantenimento dei regimi nazionali di vigilanza

Gli attuali regimi di vigilanza nazionali sarebbero mantenuti e maggiormente armonizzati mediante requisiti comuni essenziali.

Opzione ii): Istituzione di un sistema di vigilanza unionale

Si istituirebbe un sistema di vigilanza unionale per ridurre o eliminare le differenze fra i sistemi nazionali di supervisione. Ciò potrebbe avvenire in due modi:

Sub-opzione a: sostituzione dei regimi nazionali di vigilanza esistenti con un unico regime e organismo unionale.

² "eID notificata": un regime di eID notificato alla Commissione da uno Stato membro al fine del suo riconoscimento e della sua accettazione transfrontalieri.

Il concetto di eID notificata non si limita a eID rilasciate dal settore pubblico: gli Stati membri possono notificare anche eID rilasciate da soggetti privati riconosciute per l'impiego nei loro servizi del settore pubblico. Questo approccio è necessario perché non tutte le autorità degli Stati membri rilasciano eID. L'approccio transettoriale della normativa consentirebbe al settore privato di integrare l'impiego di eID notificate nei servizi elettronici ove ci fosse bisogno di un'identificazione elettronica sicura.

Sub-opzione b: istituzione di un regime e organismo di vigilanza unionale mantenendo in parallelo i regimi di vigilanza nazionali (ciascuno Stato membro potrebbe scegliere fra il proprio regime e quello unionale).

6. RAFFRONTO DELLE OPZIONI E IMPATTI

Le opzioni strategiche sono state valutate e raffrontate allo scenario di base (opzione 1) in termini di efficacia, efficienza e coerenza.

6.1. Campo di applicazione del quadro

L'**opzione 0** non contribuirebbe al raggiungimento degli obiettivi individuati nella relazione di valutazione di impatto, non aumenterebbe la disponibilità e la diffusione di servizi eIAS transfrontalieri e transettoriali, non garantirebbe un livello di governance ottimale, non stimolerebbe gli sviluppi di mercato, non contribuirebbe al rafforzamento della competitività dell'industria europea e dei settori dei servizi e non garantirebbe agli utilizzatori finali di poter trarre vantaggio dai servizi eIAS. Al contrario, tale opzione ostacolerebbe gli sviluppi tecnologici nel mercato eIAS, perturberebbe il processo attualmente in corso per rendere possibili servizi elettronici transfrontalieri e manterrebbe la frammentazione del mercato dell'UE e un panorama disomogeneo dei servizi fiduciari.

L'**opzione 1** non raggiungerebbe gli obiettivi. Manterrebbe le ambiguità esistenti e la situazione dei servizi fiduciari rimarrebbe disomogenea per quanto riguarda la vigilanza. L'incertezza regolamentare permanerebbe e la segmentazione continuerebbe a svilupparsi nell'Unione europea, portando a distorsioni della concorrenza nel mercato interno e aumentando la probabilità dell'adozione di approcci divergenti a livello nazionale.

L'**opzione 2** migliorerebbe la certezza del diritto, rafforzerebbe la vigilanza e garantirebbe il riconoscimento e l'accettazione reciproci delle eID, oltre a dare un contributo significativo al raggiungimento di tutti gli obiettivi individuati nella relazione sulla valutazione di impatto e a produrre risultati economici, sociali e ambientali positivi.

I servizi eIAS diventerebbero più attraenti e aumenterebbe la redditività degli investimenti in infrastrutture e servizi eIAS. Inoltre, gli eIAS diventerebbero disponibili per tutti i settori e tutti i tipi di imprese e si eliminerebbero le barriere transfrontaliere. Si aprirebbero nuovi mercati e nuovi investimenti, stimolando così l'innovazione.

Si ridurrebbe l'attuale frammentazione del mercato, grazie al miglioramento dell'interoperabilità transfrontaliera ottenuto attraverso la possibilità di riferimenti a norme tecniche.

Il riconoscimento e l'accettazione reciproci della eID contribuirebbe ulteriormente allo smantellamento delle barriere esistenti nel mercato interno. Da ultimo, è probabile che l'omogeneità della vigilanza risultante dai requisiti essenziali comuni incrementerebbe la fiducia, faciliterebbe l'individuazione delle frodi e contribuirebbe a prevenire il furto dell'identità.

L'**opzione 3** renderebbe i servizi eIAS ancor più attraenti e ne incrementerebbe così l'impatto positivo estendendo il quadro per incorporarvi determinati servizi fiduciari complementari essenziali.

Si ritiene che l'opzione 3 sia più adatta delle opzioni 0, 1 o 2 a conseguire un impatto significativo sulle transazioni elettroniche sicure e di facile impiego.

6.2. Strumento giuridico

Ricorrendo ad un **unico strumento** per istituire un quadro complessivo si garantirebbe la coerenza della normativa che disciplina i diversi aspetti degli eIAS. **Due strumenti distinti** rischierebbero di introdurre divergenze fra le disposizioni normative adottate per le firme elettroniche e per l'identificazione elettronica, oltre che – in particolare – fra gli approcci adottati.

L'adozione di una **direttiva** non aiuterebbe a risolvere gli attuali problemi di interoperabilità delle firme elettroniche che derivano dalle divergenze nel recepimento della direttiva 1999/93/CE negli Stati membri. Un **regolamento** è di applicazione immediata senza previa interpretazione e permette così di ottenere una migliore armonizzazione. Per questi motivi è più adatto al raggiungimento degli obiettivi della normativa proposta.

L'adozione di un unico regolamento appare la modalità più efficace per raggiungere gli obiettivi.

6.3. Livello di vigilanza

Con l'**opzione "i"** la nuova normativa conserverebbe gli attuali regimi nazionali di vigilanza ed imporrebbe requisiti essenziali comuni ai prestatori di servizi. Un approccio armonizzato unionale per le firme elettroniche e per i servizi fiduciari complementari migliorerebbe l'efficacia della vigilanza, aumenterebbe la certezza del diritto e promuoverebbe la fiducia e la sicurezza delle transazioni elettroniche.

L'**opzione "ii"** assicurerebbe una vigilanza omogenea, efficiente e di alta qualità in tutta l'UE. La **sub-opzione "b"** presenta il vantaggio di una maggiore flessibilità rispetto all'organismo unionale unico di vigilanza previsto nella **sub-opzione "a"**: gli Stati membri che contano pochi o nessun prestatore di servizi fiduciari stabiliti sul loro territorio potrebbero trovare vantaggioso trasferire i compiti di vigilanza ad un organismo di vigilanza unionale. Altri Stati membri avrebbero la facoltà di mantenere il loro regime di vigilanza, se lo desiderassero. Tuttavia, un modello di vigilanza unionale centralizzato solleva problemi di sussidiarietà.

In ossequio al principio di sussidiarietà la (opzione i) appare essere la più appropriata.

7. MOTIVI DI UN INTERVENTO A LIVELLO DELL'UE, VALORE AGGIUNTO UNIONALE E SUSSIDIARIETÀ

Come per la direttiva 1999/93/CE, la base giuridica della proposta legislativa è l'articolo 114 del TFUE sul mercato interno, perché si tratta di eliminare barriere esistenti al funzionamento del mercato interno promuovendo il riconoscimento e l'accettazione reciproci della eID, dell'autenticazione, delle firme e dei servizi fiduciari complementari a livello transfrontaliero, ove necessari per l'espletamento di transazioni elettroniche.

In considerazione della natura per sé non territoriale dei servizi eIAS, un intervento a livello dell'Unione europea è adeguato e proporzionato per l'attuazione del mercato unico digitale. Misure regolamentari adottate a livello degli Stati membri non sono ritenute in grado di raggiungere lo stesso risultato. Pertanto, l'intervento dell'UE è necessario, appropriato e giustificato.

8. MONITORAGGIO E VALUTAZIONE

La Commissione monitorerà l'applicazione della normativa mediante un dialogo permanente con le parti interessate e la raccolta di dati statistici e riferirà al Parlamento europeo e al Consiglio sull'impatto della nuova normativa quattro anni dopo la sua entrata in vigore.