Cristina Vicarelli
Avvocato

# eIDAS, cos'è e perché ci riguarda

È conosciuto come Regolamento eIDAS (o anche semplicemente come eIDAS) il **Regolamento (UE) N. 910/2014** del Parlamento Europeo e del Consiglio del 23 luglio 2014 **in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE,** la quale trattava le firme elettroniche, senza tuttavia fornire un quadro transfrontaliero e transettoriale completo per transazioni elettroniche sicure, affidabili e di facile impiego in tutti i diversi Stati dell'UE.

Trattandosi di una direttiva, la normativa era stata tradotta nelle diverse normative nazionali; in Itallia ciò era avvenuto soprattutto attraverso il Codice dell'Amministrazione Digitale (CAD).

Il Regolamento eiDAS, invece, non necessita di essere accolto nelle norme nazionali: essendo un Regolamento esso è direttamente ed immediatamente applicabile in tutti gli Stati membri. Sarà la normativa nazionale, eventualmente in conflitto, a dover essere adeguata alle prescrizioni regolamentari ed è quanto sta accadendo in Italia con il Codice dell'Amministrazione Digitale. Il Regolamento eIDAS, pertanto, ha rafforzato ed esteso l'*acquis* della precedente direttiva, proponendosi di rafforzare la fiducia nelle transazioni elettroniche nel mercato interno, fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.

Secondo il legislatore europeo, infatti, instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, dovuta in

particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.

Non solo firme elettroniche, quindi: l'acronimo che contraddistingue il Regolamento deriva dall'insieme dei servizi che vengono disciplinati in via elettronica (electronic IDentification Authentication and Signature): identificazione, autenticazione e firme (ma anche sigilli), e non solo: il Regolamento si preoccupa anche di normare i servizi connessi, come i servizi di recapito (sempre elettronico) transfrontaliero. Sino ad ora i cittadini dei diversi stati (ma anche le imprese) non riuscivano ad avvalersi della loro identificazione elettronica per autenticarsi in un altro Stato membro perché i regimi nazionali di identificazione elettronica del loro paese non erano riconosciuti in altri Stati membri. Tale barriera elettronica impediva ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno. Disporre di mezzi di identificazione elettronica riconosciuti reciprocamente permetterà di agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di operare su base transfrontaliera evitando molti ostacoli nelle interazioni con le autorità pubbliche.

E' evidente che questa normativa non spiegherà i suoi effetti solo nei rapporti tra cittadini, imprese e pubbliche amministrazioni: la disciplina delle firme, dei sigilli, dei servizi di recapito, è idonea  a influire anche negli scambi commerciali tra privati, si pensi alle forme di accettazione in uso nelle contrattualistica che assiste l'e-commerce, ad esempio.

## Quando?

Il Regolamento eidas è stato approvato e pubblicato nel 2014, e, sebbene alcune disposizioni siano entrate in vigore già nel 2014, la gran parte delle norme è entrata in vigore il 10 luglio 2016.

## I PUNTI FONDAMENTALI

Il Regolamento si snoda lungo due direttrici principali, da una parte è teso a normare l'i**dentificazione elettronica**, ossia *"il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica*" dall'altra i "**servizi fiduciari"** ossia servizi elettronici forniti normalmente dietro remunerazione e consistenti nei seguenti elementi:

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

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

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

## 1. IDENTIFICAZIONE ELETTRONICA

La prima parte del Regolamento eIDAS è dedicata all'identificazione elettronica e riguarda gli Stati membri e solo indirettamente i privati. Questa parte del Regolamento tratteggia un quadro normativo volto a eliminare le barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici. Non interviene direttamente sui sistemi di gestione dell'identità elettronica e le relative infrastrutture istituiti negli Stati membri: lo scopo è garantire che per accedere ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura. Gli Stati membri, pertanto, rimarranno liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica, potranno decidere circa eventuale partecipazione del settore privato nell'offerta di tali mezzi; essi non avranno l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione, ma potranno decidere, in ordine ai regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici, se notificarne alcuni, tutti o

nessuno. Il Regolamento, invece si preoccupa di fissare talune condizioni in merito all'obbligo di **riconoscimento reciproco** dei mezzi di identificazione elettronica e alle modalità di notifica dei regimi di identificazione elettronica. L'obbligo di mutuo riconoscimento viene parametrato ai **livelli di garanzia** dell'identità: essi caratterizzano il **grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona**, fornendo così la garanzia che la persona che pretende di avere una determinata identità sia effettivamente la persona cui tale identità è stata assegnata. Come è ben spiegato nel considerando 16, "Il livello di garanzia dipende dal grado di sicurezza fornito dai mezzi di identificazione elettronica riguardo all'identità pretesa o dichiarata di una persona tenendo conto dei procedimenti (ad esempio, controllo e verifica dell'identità, e autenticazione), delle attività di gestione (ad esempio, l'entità che rilascia i mezzi di identificazione elettronica e la procedura di rilascio di tali mezzi) e dei controlli tecnici messi in atto. Come risultato dei progetti pilota su larga scala finanziati dall'Unione, della normazione e di attività a livello internazionale, esistono varie definizioni e descrizioni tecniche dei livelli di garanzia. In particolare, il progetto pilota su larga scala **STORK** e la norma **ISO 29115** fanno riferimento, tra l'altro, ai livelli 2, 3 e 4, che dovrebbero essere tenuti nella massima considerazione all'atto di stabilire le norme, le procedure e i requisiti tecnici minimi per i livelli di garanzia **basso, significativo ed elevato** ai sensi del presente regolamento, assicurando al contempo l'applicazione coerente del presente regolamento in particolare per quanto riguarda il livello di garanzia elevato in relazione al controllo dell'identità ai fini del rilascio di certificati qualificati. I requisiti stabiliti dovrebbero essere neutrali dal punto di vista tecnologico. Dovrebbe essere possibile soddisfare i requisiti di sicurezza necessari attraverso tecnologie differenti".

Sebbene, come abbiamo visto, questa parte del Regolamento non sia direttamente rivolta al settore privato "si ritiene opportuno che gli Stati membri incoraggino il settore privato a **impiegare volontariamente mezzi di identificazione elettronica** nell'ambito di un **regime notificato** a fini di identificazione ove necessario per servizi online o transazioni elettroniche".

## 2. SERVIZI FIDUCIARI

La seconda parte del Regolamento, invece, riguarda i servizi fiduciari ed è questa la parte che maggiormente interessa il settore privato.

Secondo il Regolamento il "servizio fiduciario" è un servizio elettronico fornito **normalmente dietro remunerazione** e consistente nei seguenti elementi:

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

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

**C)** conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Anche in ordine ai servizi fiduciari il Regolamento eIDAS rappresenta il quadro giuridico generale di riferimento. Il Regolamento non istituisce un obbligo generale di fare uso dei servizi fiduciari o di installare un punto di accesso per tutti i servizi fiduciari esistenti. Secondo il legislatore europeo, infatti non è auspicabile che il Regolamento copra la prestazione di servizi fiduciari usati esclusivamente nell'ambito di sistemi chiusi da un insieme definito di partecipanti che non hanno ripercussioni su terzi. Ad esempio, i sistemi istituiti in imprese o amministrazioni pubbliche per la gestione delle procedure interne che fanno uso di servizi fiduciari non dovrebbero essere soggetti ai requisiti previsti dal Regolamento eIDAS. Solo i servizi fiduciari prestati al pubblico che hanno ripercussioni su terzi dovrebbero soddisfare tali requisiti. Il Regolamento, inoltre, **non riguarda gli aspetti legati alla conclusione e alla validità di contratti o di altri negozi giuridici nei casi in cui la normativa nazionale o unionale stabilisca obblighi di forma.** Piuttosto, al fine di contribuire al loro impiego transfrontaliero generale, sarà possibile utilizzare i servizi fiduciari **come prove** in procedimenti giudiziali in tutti gli Stati membri.

Le persone fisiche o giuridiche che prestano uno o più servizi fiduciari sono definite "prestatori di servizi fiduciari". Un prestatore di servizi fiduciari qualificato è colui che

presta uno o più servizi fiduciari qualificati e cui l'**organismo di vigilanza** assegna la qualifica di prestatore di servizi fiduciari qualificato. I prestatori di servizi fiduciari qualificati sono sottoposti a vigilanza da parte dei relativi organismi, possono essere iscritti in "**Elenchi di fiducia**" tenuta dai singoli Stati membri e successivamente possono utilizzare il "**marchio di fiducia UE**" per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.

Gli Stati membri hanno l'obbligo di designare gli **organismi di vigilanza.** Gli organismi di vigilanza devono **cooperare con le autorità di protezione dei dati**, ad esempio informandole in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni **delle norme** di protezione dei dati personali. È opportuno, però, che la trasmissione di informazioni copra gli **incidenti di sicurezza** e le **violazioni dei dati personal**i. Il regolamento prevede che prestatori di servizi fiduciari rispettino stringenti obblighi di sicurezza e si assumano le **responsabilità connesse ai rischi** che gravano l'attività.

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

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

ne ricorrano i presupposti, la notifica della violazione può anche essere divulgata al pubblico dalle autorità.

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

Per comprendere meglio la portata di questi aspetti sarà bene richiamare il considerando 36: La notifica delle violazioni di sicurezza (**security breach**) e delle valutazioni di rischio per la sicurezza (**security risk assessment**) è essenziale per fornire informazioni adeguate alle parti interessate in caso di violazione di sicurezza o perdita di integrità. Gli aspetti tecnici saranno comunque chiariti dall'ENISA che sta emanando linee guida ad hoc.

## A1. FIRME ELETTRONICHE (eSignature)

Il Regolamento eIDAS stabilisce il principio secondo cui alla firma elettronica non possono essere negati effetti giuridici per il motivo della sua forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata. Tuttavia, spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal Regolamento stesso secondo cui alla firma elettronica qualificata è riconosciuto un effetto giuridico equivalente a quello di una firma autografa.

In ordine alle firme elettroniche, il Regolamento eIDAS definisce tre tipologie di firma:

- firma elettronica
- firma elettronica avanzata
- firma elettronica qualificata.

### La firma elettronica

Il regolamento definisce la firma elettronica come "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e **utilizzati dal firmatario per firmare**".

Rispetto alla normativa previgente vi è un mutamento evidente nella esplicitazione della finalità: l'abrogata direttiva, infatti, definiva la firma elettronica come "dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione". Cade quindi il riferimento all'autenticazione che viene sostituito dalla utilizzazione dei dati (associati logicamente ad altri dati) allo scopo di firmare.

La firma elettronica appartiene, diversamente dalla direttiva, **solo alla persona fisica**. Firmatario, pertanto, può essere soltanto una persona fisica. Le persone giuridiche, come vedremo, potranno avvalersi dei "sigilli elettronici".

La normativa definisce anche il «dispositivo per la creazione di una firma elettronica» che è un software o hardware configurato utilizzato per creare una firma elettronica, e il «certificato di firma elettronica», che altro non è se non un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona.

Se ne deduce che ove correttamente configurata, anche una **casella da flaggare**, accompagnata da una breve dichiarazione, può rappresentare una firma elettronica. In un documento diffuso dal Department for Business, Energy and Industrial strategy del Regno Unito viene inclusa nella firma elettronica anche la **firma digitalizzata** (o scannerizzata).

## La firma elettronica avanzata

La "firma elettronica avanzata", è una firma elettronica che soddisfa determinati requisiti. Questi requisiti sono indicati dall'articolo 26 del Regolamento:

a) è connessa **unicamente** al firmatario;

b) è idonea a **identificare** il firmatario;

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

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

Occorre che siano soddisfatti **tutti i** requisiti sopra indicati.

## La firma elettronica qualificata

La "firma elettronica qualificata", è 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;

Il dispositivo per la creazione di una firma elettronica qualificata è un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento eIDAS, mentre il "certificato qualificato di firma elettronica" è un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS;

Quindi la firma elettronica qualificata è una firma che:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

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

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

e) è creata con un "**dispositivo** per la creazione di una firma elettronica qualificata";

f) è basata su un "**certificato** qualificato per firme elettroniche".

Il Regolamento eIDAS attribuisce direttamente alla firma elettronica qualificata lo stesso valore della **firma autografa**, come abbiamo visto sopra.

Viene promossa la **certificazione della sicurezza** delle tecnologie d'informazione basata su norme internazionali, come l'ISO 15408 e i metodi di valutazione e le disposizioni di riconoscimento reciproco connessi, perché è considerata uno strumento importante per verificare la sicurezza dei dispositivi per la creazione di una firma elettronica qualificata.

### E la firma digitale?

La firma digitale, invenzione tutta italiana, è una firma elettronica qualificata ai sensi del Regolamento eIDAS, ed equivale, pertanto, alla firma autografa.

### A2. SIGILLI ELETTRONICI (eSeal)

I sigilli elettronici comprovano l'emissione di un documento elettronico **da parte di una determinata persona giuridica**, dando la certezza dell'origine e dell'integrità del documento stesso. Tuttavia qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia prevista anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.

Un "sigillo elettronico" consiste in dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica **per garantire l'origine e l'integrità** di questi ultimi, e viene creato tramite un "dispositivo per la creazione di un sigillo elettronico" che è un software o hardware configurato e utilizzato per creare un sigillo elettronico.

Anche i sigilli elettronici come le firme possono essere anche avanzati o qualificati.

Un sigillo elettronico **avanzato** è un sigillo che presenta tutti i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

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

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

**Un sigillo elettronico qualificato** è 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.

Il "dispositivo per la creazione di un sigillo elettronico qualificato" è un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II del Regolamento; mentre il "certificato qualificato di sigillo elettronico" è un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III del Regolamento eIDAS. Il sigillo elettronico qualificato gode della **presunzione di integrità** dei dati **e di correttezza** dell'origine di quei dati a cui è associato.

## A3. VALIDAZIONE TEMPORALE

La "validazione temporale elettronica", consiste in dati in forma elettronica che collegano altri dati in forma elettronica **a una particolare ora e data**, così da provare che questi ultimi esistevano in quel momento.

La "validazione temporale elettronica qualificata" è una validazione temporale elettronica che soddisfa tutti i seguenti requisiti:

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

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

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

Solo la validazione temporale elettronica qualificata gode della **presunzione di accuratezza** della data e dell'ora che indica **e di integrità** dei dati ai quali tali data e ora sono associate.

## A4. RECAPITO CERTIFICATO

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

I "servizi elettronici di recapito qualificato certificato" sono servizi elettronici di recapito certificato che soddisfano tutti i seguenti requisiti:

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

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

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

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

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

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

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

### eIDAS, servizi accessori: la convalida

Si tratta di un servizio accessorio che consiste in un processo di **verifica e conferma** della validità di una **firma o di un sigillo elettronico**.

In buona sostanza tale processo comporta la verifica che i requisiti del Regolamento sono soddisfatti da una firma elettronica (qualificata) o da un sigillo elettronico (qualificato), allo scopo di confermarne la validità. Il Regolamento prevede anche la verifica e validazione dei certificati di autenticazione dei siti web (cfr. art 3 punto 16 Reg. eIDAS "creazione, **verifica e convalida** di certificati di autenticazione di siti web").

## B. AUTENTICAZIONE DEI SITI WEB

Il "certificato di autenticazione di sito web" è un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato; per "certificato **qualificato** di autenticazione di sito web" si intende, invece, un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV del regolamento eIDAS.

I servizi di autenticazione dei siti web, pertanto, prevedono un mezzo tramite il quale il visitatore di un sito può accertarsi che dietro a quel sito web vi è un'entità reale e legittima. Tali servizi nell'ottica del legislatore europeo, contribuiscono a diffondere sicurezza e fiducia nelle transazioni commerciali on line, in quanto gli utenti si fideranno di un sito web che è stato autenticato. La fornitura e l'uso di servizi di autenticazione dei siti web sono interamente volontari. Tuttavia, affinché l'autenticazione dei siti web divenga un mezzo per rafforzare la fiducia, fornire un'esperienza migliore all'utente e promuovere la crescita nel mercato interno, il Regolamento eIDAS -spiega il legislatore nei considerando - dovrebbe stabilire obblighi minimi in materia di sicurezza e responsabilità per i prestatori e i loro servizi. A tal fine, dice il legislatore, si è tenuto conto dei risultati delle iniziative

industriali esistenti, ad esempio, il Forum Autorità di certificazione/Browser (CA/B Forum). Inoltre, il Regolamento non impedisce l'uso di altri mezzi o metodi di autenticazione di un sito web non rientranti nel Regolamento stesso e non vieta ai prestatori di servizi di autenticazione dei siti web di paesi terzi di prestare i propri servizi ai clienti dell'Unione. Tuttavia, i servizi di autenticazione dei siti web di un prestatore di un paese terzo, secondo le intenzioni del legislatore, dovrebbero essere riconosciuti come qualificati ai sensi del Regolamento solo se sia stato concluso un **accordo internazionale** tra l'Unione e il paese di stabilimento di detto prestatore.

## C) CONSERVAZIONE DI FIRME, SIGILLI O CERTIFICATI ELETTRONICI RELATIVI A TALI SERVIZI

Il legislatore europeo mostra di ritenere opportuno che il Regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.

A tal fine dedica alcune disposizioni alla conservazione effettuata dai fornitori di servizi fiduciari.

Innanzi tutto, all'articolo 34 si occupa del **servizio di conservazione qualificato delle firme elettroniche qualificate**, disponendo che un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato *che utilizza procedure e tecnologie* ***in grado di estendere l'affidabilità della*** **firma** ***elettronica qualificata oltre il periodo di validità tecnologica***.

All'articolo 40, invece, dispone che alla **conservazione dei sigilli elettronici qualificati** si applichino, mutatis mutandis, le previsioni relative alla conservazione delle firme (art. 34 del Regolamento eIDAS).

Il termine conservazione non deve trarre in inganno: ciò che il legislatore vuole garantire, infatti, è la possibilità di convalidare il documento a distanza di tempo. La "convalida" è il

processo di verifica e conferma della validità di una firma o di un sigillo elettronico. Come è stato spiegato, il Regolamento eIDAS pone le regole per "preservare" nel tempo le firme elettroniche e i sigilli elettronici e ciò è diverso dall'archiviazione elettronica -da noi nota anche come conservazione digitale o sostitutiva- (che non è un servizio fiduciario previsto da eIDAS). Le due attività si distinguono nettamente per finalità e obiettivi: la conservazione prevista da eIDAS mira a garantire l'affidabilità dei una firma elettronica qualificata o di un sigillo elettronico qualificato attraverso il tempo; la tecnologia alla base di questo tipo di servizi, quindi, è diretta solo verso le firme o i sigilli.

L'archiviazione elettronica, invece, mira ad assicurare che un documento sia memorizzato in modo da garantire la sua integrità (e gli altri attributi di legge). La tecnologia alla base dell'archiviazione elettronica è diretta verso il documento. L'archiviazione elettronica resta di competenza degli Stati membri.

Detto in altre parole, l'archiviazione elettronica dei documenti e la conservazione eIDAS di firme elettroniche e sigilli elettronici sono diverse per natura, sono basate su diverse soluzioni tecniche (legate al documento oppure alla firma elettronica / sigillo elettronico) e hanno scopi diversi (conservazione dei documenti contro conservazione della firma elettronica o del sigillo elettronico che ne estenda nel tempo l'attuale affidabilità).

## Documento informatico o documento elettronico?

Infine, quello a noi era noto come documento informatico viene ora definito "documento elettronico". La terminologia utilizzata dal legislatore è in linea con quella impiegata nella precedente direttiva, lo scarto linguistico è attribuibile alla trasposizione operata al tempo dal legislatore nazionale nel Codice dell'Amministrazione Digitale.

Il legislatore muove dalla considerazione che i documenti elettronici sono importanti per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno. Il Regolamento, pertanto, stabilisce il principio secondo cui a un documento elettronico non possono essere negati gli effetti giuridici a causa della sua forma elettronica e ciò al fine

di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica. In particolare è definito "documento elettronico" qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Quanto agli effetti giuridici dei documenti elettronici, all'articolo 46 il Regolamento dispone che

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