Sono state pubblicate nella Gazzetta Ufficiale UE le norme per valutare la sicurezza dei prodotti delle tecnologie delle informazioni applicabili alla certificazione dei dispositivi per la creazione di una firma elettronica qualificata o per la creazione di un sigillo elettronico qualificato.

di Daniele Tumietto

FIRMA ELETTRONICA QUALIFICATA E SIGILLO ELETTRONICO QUALIFICATO: PUBBLICATE LE NORME PER VALUTARE LA SICUREZZA DEI PRODOTTI DELLE TECNOLOGIE DELLE INFORMAZIONI

Daniele TUMIETTO, *commercialista, partner di Menocarta.net, componente Forum Italiano della Fattura Elettronica presso l'Agenzia delle Entrate, componente Expert Group del CEN per la "Core Invoice" CEN/TC 434, componente Advisory Group CEF per il "Match-making Website" CEN/TC 440, collaboratore Osservatori della School of Management del Politecnico di Milano in materia di e-invoicing ed e-procurement, componente ISOC – Internet Society.*

Il Regolamento Europeo n. 910 del 23 luglio 2014 "eIDAS" dal 1° luglio 2016 ha progressivamente iniziato a sostituire la Direttiva 1999/93/CE riguardante le firme elettroniche, modificando il contesto normativo interno con importanti novità e nuovi servizi che riguarderanno prima le Pubbliche Amministrazioni e poi imprese che professionisti.

Nel grafico sottostante è indicata la tempificazione dell'avvio di eIDAS:

17.09.2014 – Entrata in vigore del Regolamento eIDAS (Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio).

29.09.2015 – Riconoscimento volontario di eID (Electronic IDentification) notificati (strumenti per garantire un accesso sicuro ai servizi online e di effettuare transazioni elettroniche in modo più sicuro).

01.07.2016 – Applicazione regolamento eIDAS e abrogazione Direttiva 1999/93/CEE.

1.07.2017 – Termine per la presentazione da parte di un prestatore di servizi di certificazione (che rilascia certificati qualificati a norma della direttiva 1999/93/CE) di una relazione di valutazione della conformità all'organismo di vigilanza per essere un prestatore di servizi fiduciari qualificato.

29.09.2018 – Riconoscimento obbligatorio transfrontaliero dei sistemi di identificazione elettronica notificati dagli Stati membri. Operatività del nodo eIDAS che costituisce il punto di connessione facente parte di un'architettura di interoperabilità dell'identificazione elettronica, realizzato in conformità con il Regolamento di esecuzione (UE) 2015/1501 della Commissione.

***Figura 1**- Le tappe del Regolamento eIDAS (Fonte: Agenzia per l'Itaia Digitale)*

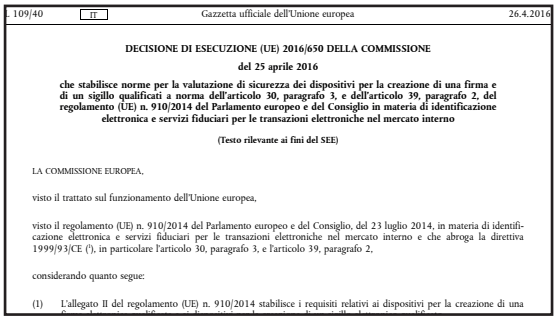
Con l'utilizzo dello strumento giuridico del Regolamento, l'Unione Europea ha scelto la strada di emanare nuove norme che diventino immediatamente leggi di tutti gli Stati membri una volta che sia avvenuta la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea, senza la necessità di dover emanare norme interne di recepimento e demandando agli atti di esecutivi della Commissione Europea le regole tecniche di attuazione, che devono richiamare gli standard emanati dagli enti di normazione CEN/ETSI.

Pertanto questo è lo schema di funzionamento giuridico del Regolamento:

***Figura 2** - Schema di funzionamento giuridico del Regoamento eIDAS*

Si rammenta che attraverso l'emanazionedel Regolamento:

- l'adozione in tutti gli stati membri del nuovo contesto giuridico di riferimento è molto più rapida e semplice,
- vi è un unico contesto giuridico di riferimento che non può essere modificato da leggi nazionali, salvo rare eccezioni.



L 109/40 IT Gazzetta ufficiale dell'Unione europea 26.4.2016

DECISIONE DI ESECUZIONE (UE) 2016/650 DELLA COMMISSIONE

del 25 aprile 2016

che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 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)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto 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 (1), in particolare l'articolo 30, paragrafo 3, e l'articolo 39, paragrafo 2,

considerando quanto segue:

(1) L'allegato II del regolamento (UE) n. 910/2014 stabilisce i requisiti relativi ai dispositivi per la creazione di una

Con la recente **DECISIONE DI ESECUZIONE (UE) 2016/650 della Commissione del 25 aprile 2016** che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, sono state pubblicate nella Gazzetta Ufficiale UE le norme per valutare la sicurezza dei prodotti delle tecnologie delle informazioni applicabili alla certificazione dei dispositivi per la creazione di una FEQ o per la creazione di un SEQ.

La predetta disposizione ha in premessa alcuni "Considerando" che sono molto importanti per comprendere la *ratio* della norma, e di 3 articoli. Nei Considerando è indicato che:

1. in tale considerando sono ricordati i requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata e ai dispositivi per la creazione di un sigillo elettronico qualifico, ai sensi dell'allegato II del Regolamento (UE) n. 910/2014;
2. gli enti di normalizzazione hannol'incarico di elaborare le specifiche tecniche necessarie alla produzione e alla commercializzazione dei prodotti;
3. l'ISO/IEC (*International Organisation for Standardization/International Electrotechnical Commission*) statuisce i concetti e i principi generali in materia di sicurezza delle tecnologie dell'informazione. Inoltreindica quale è il modello generale di valutazione da seguire come base per valutare le proprietà di sicurezza dei prodotti di questo settore;
4. il CEN (Comitato Europeo di Normazione) ha realizzato le norme relative ai dispositivi per la creazione di una firma elettronica e di un sigillo qualificati, dove i dati per la creazione della firma elettronica o alla creazione del sigillo elettronico sono detenuti in un ambiente gestito integralmente, ma non necessariamente in via esclusiva, dall'utilizzatore;
5. solo il prestatore di servizi fiduciari qualificati può gestire i dati per la creazione di una firma elettronica per conto del firmatario (allegato II del regolamento). I requisiti in materia di sicurezza e le pertinenti specifiche in materia di certificazione sono diverse a seconda che il firmatario sia in possesso materiale di un prodotto e se un prestatore di servizi fiduciari qualificati agisce per conto del firmatario;
6. in considerazione del fatto che diversi prestatori di servizi fiduciari propongono attualmente soluzioni per gestire i dati per la creazione di una firma elettronica per conto dei loro clienti, le certificazioni dei prodotti sono attualmente limitate ai moduli di sicurezza hardware certificati secondo diverse norme, ma non sono ancora certificati secondo i requisiti relativi ai dispositivi per la creazione di firme e sigilli qualificati. Poiché alcune norme in questione sono in fase di sviluppo, nel momento in cui saranno disponibili (e conformi ai requisiti di cui all'allegato II del Regolamento) la Commissione integrerà la presente decisione;
7. l'allegato della presente decisione fa riferimento alla norma EN 419211, che consta di più parti (da 1 a 6) intese a disciplinare differenticontesti. I fabbricanti del prodotto hanno la facoltà di applicare liberamente tali estensioni e, ai sensi dei considerando 56 del Regolamento, l'ambito di applicazione degli articoli 30 e 39 è limitato alla protezione dei dati per la creazione di una firma, con esclusionidelle applicazioni per la creazione della firma;
8. sono previsti, per la sicurezza del prodotto certificato, idonei algoritmi crittografici, lunghezze di chiave e funzioni hash attraverso cui assicurare che le firme/sigilli elettronici generati da un dispositivo per la creazione di una firma o di un sigillo qualificati siano affidabilmente protetti da contraffazioni conformemente all'allegato II del regolamento (UE) n. 910/2014.

Un particolare molto importante di questa normativa è che questa decisione di esecuzione si applica limitatamente ai dispositivi sotto il diretto controllo dell'utilizzatore degli stessi (come *smart card*, *Token USB*, ecc.), mentre non si applica ai dispositivi di firma remota (come HSM). ©