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 firma elettronica qualificata e ai dispositivi per la creazione di un sigillo elettronico qualificato.

(2) L'incarico di elaborare le specifiche tecniche necessarie alla produzione e alla commercializzazione dei prodotti, tenendo conto dello stato attuale della tecnologia, è affidato alle organizzazioni competenti in materia di normalizzazione.

(3) L'ISO/IEC (International Organisation for Standardization/International Electrotechnical Commission) stabilisce i concetti e i principi generali in materia di sicurezza delle tecnologie dell'informazione e specifica il modello generale di valutazione da seguire come base per valutare le proprietà di sicurezza dei prodotti di questo settore.

(4) Il comitato europeo di normazione (CEN) ha elaborato, nell'ambito del mandato M/460 conferitogli dalla Commissione, 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. Tali norme sono ritenute idonee per valutare la conformità di tali dispositivi ai pertinenti requisiti di cui all'allegato II del regolamento (UE) n. 910/2014.

(5) L'allegato II di detto regolamento stabilisce che solo un prestatore di servizi fiduciari qualificati possa gestire i dati per la creazione di una firma elettronica per conto del firmatario. I requisiti in materia di sicurezza e le pertinenti specifiche in materia di certificazione differiscono nel caso in cui il firmatario sia in possesso materiale di un prodotto e se un prestatore di servizi fiduciari qualificati agisce per conto del firmatario. Per trattare entrambe le situazioni nonché promuovere lo sviluppo nel tempo di prodotti e di criteri di valutazione idonei a esigenze particolari, l'allegato della presente decisione dovrebbe elencare norme che disciplinino entrambe le situazioni.

(6) Al momento dell'adozione della presente decisione, diversi prestatori di servizi fiduciari offrono già 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 specificatamente secondo i requisiti relativi ai dispositivi per la creazione di firme e sigilli qualificati. Tuttavia le norme pubblicate, quali la norma EN 419211 (applicabile alle firme elettroniche create in un ambiente gestito integralmente, ma non necessariamente in via esclusiva, dall'utilizzatore) non esistono ancora per una parte di mercato altrettanto importante di prodotti remoti certificati. Poiché le norme eventualmente idonee a tali fini si trovano attualmente in fase di sviluppo, nel momento in cui saranno disponibili e ritenute conformi ai requisiti di cui all'allegato II del regolamento (UE) n. 910/2014 la Commissione integrerà la presente decisione. Fino al momento in cui sarà stabilito l'elenco di tali norme è possibile avvalersi di un processo alternativo per valutare la conformità di tali prodotti, alle condizioni di cui all'articolo 30, paragrafo 3, lettera b), del regolamento (UE) n. 910/2014.

(7) L'allegato della presente decisione fa riferimento alla norma EN 419211, che consta di più parti (da 1 a 6) intese a disciplinare situazioni diverse. Le parti 5 e 6 della suddetta norma presentano estensioni connesse all'ambiente

([1]) GU L 257 del 28.8.2014, pag. 73.

del dispositivo per la creazione di una firma qualificata, quale la comunicazione con le applicazioni attendibili per la creazione della firma. I fabbricanti del prodotto hanno la facoltà di applicare liberamente tali estensioni. Secondo il considerando 56 del regolamento (UE) n. 910/2014, l'ambito di applicazione ai sensi degli articoli 30 e 39 di detto regolamento è limitato alla protezione dei dati per la creazione di una firma, mentre ne sono escluse le applicazioni per la creazione della firma.

(8) Per garantire che le firme o i 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, sono prerequisiti per la sicurezza del prodotto certificato idonei algoritmi crittografici, lunghezze di chiave e funzioni hash. Poiché la materia non è stata armonizzata a livello europeo, gli Stati membri dovrebbero collaborare per concordare gli algoritmi crittografici, le lunghezze di chiave e le funzioni hash da usare nell'ambito delle firme e dei sigilli elettronici.

(9) L'adozione della presente decisione rende obsoleta la decisione 2003/511/CE della Commissione ([1]). È pertanto necessario abrogarla.

(10) Le misure di cui alla presente decisione sono conformi al parere del comitato di cui all'articolo 48 del regolamento (UE) n. 910/2014,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. Le norme per valutare la sicurezza dei prodotti delle tecnologie dell'informazione applicabili alla certificazione dei dispositivi per la creazione di una firma elettronica qualificata o per la creazione di un sigillo elettronico qualificato a norma dell'articolo 30, paragrafo 3, lettera a), o dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014, ove i dati per la creazione della firma elettronica o alla creazione del sigillo elettronico siano detenuti integralmente, ma non necessariamente in via esclusiva, in un ambiente gestito dall'utilizzatore, sono elencate nell'allegato della presente decisione.

2. Fino all'istituzione da parte della Commissione di un elenco di norme per valutare la sicurezza dei prodotti delle tecnologie dell'informazione applicabili alla certificazione dei dispositivi per la creazione di una firma elettronica qualificata o per la creazione di un sigillo elettronico qualificato, nel caso in cui un prestatore di servizi fiduciari qualificato gestisca i dati per la creazione di una firma elettronica o i dati per la creazione di un sigillo elettronico per conto di un firmatario o del creatore di un sigillo, la certificazione di tali prodotti è basata su un processo che, a norma dell'articolo 30, paragrafo 3, lettera b), rispetta livelli di sicurezza pari a quelli di cui all'articolo 30, paragrafo 3, lettera a), e sia notificata alla Commissione dall'organismo pubblico o privato di cui all'articolo 30, paragrafo 1, del regolamento (UE) n. 910/2014.

Articolo 2

La decisione 2003/511/CE è abrogata.

Articolo 3

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

Fatto a Bruxelles, il 25 aprile 2016

Per la Commissione
Il presidente
Jean-Claude JUNCKER

([1]) Decisione 2003/511/CE della Commissione, del 14 luglio 2003, relativa alla pubblicazione dei numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica conformemente alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio (GU L 175 del 15.7.2003, pag. 45).

ALLEGATO

ELENCO DELLE NORME DI CUI ALL'ARTICOLO 1, PARAGRAFO 1

— ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, parti da 1 a 3, come elencato in appresso:

  — ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009.

  — ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 2. ISO, 2008.

  — ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3. ISO, 2008

  e

— ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation,

  e

— EN 419211 — Profili di protezione per dispositivi di creazione di firma sicura, parti da 1 a 6, come opportuno, come elencato in appresso:

  — EN 419211-1:2014 — Profili di protezione per dispositivi di creazione di firma sicura — Parte 1: Visione d'insieme

  — EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

  — EN 419211-3:2013 — Profili di protezione per dispositivi di creazione di firma sicura — Parte 3: Dispositivi con importazione di chiave

  — EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

  — EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application

  — EN 419211-6:2014 — Profili di protezione per dispositivi di creazione di firma sicura — Parte 6: Estensione per il dispositivo con importazione di chiave e canale attendibile per applicazione di creazione di firma