Il decalogo delle firme elettroniche

1) La firma elettronica non vale nulla
È falso. Definendo come firma elettronica in base al regolamento UE 910/2014 (eIDAS) i dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare, tale firma ha il valore stabilito nel CAD nell'articolo 20, comma 1-bis. L' idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. In altre parole non c'è nulla di predefinito ma decide il giudice caso per caso.

2) La firma grafometrica è Firma elettronica avanzata (FEA)
È falso. Questa equivalenza è soddisfatta solo se la firma grafometrica è proposta al sottoscrittore nell'ambito di quanto stabilito nel Titolo V delle regole tecniche sulla firma (DPCM 22 febbraio 2013). In particolare il sottoscrittore aderisce al servizio in modo esplicito sottoscrivendo una dichiarazione di accettazione. Quest'ultimo è anche informato sugli esatti termini e condizioni relative all'uso del servizio, compresa ogni limitazione d'uso. In altre parole firmo in modalità grafometrica solo quello che ho approvato.

3) L'unica firma valida è quella con il file avente l'estensione .p7m
È falso. La normativa comunitaria prevede tre formati per i documenti sottoscritti. Si chiamano CAdES, PAdES e XAdES. In questa sede è sufficiente sottolineare che l'estensione .p7m è quella definita nelle regole nazionali per il CAdES. Solo a norma di legge comunitaria anche il formato PAdES che rappresenta firme di file PDF e lo XAdES che è totalmente in formato XML.

Nella pratica crea qualche dubbio il fatto che un file PDF firmato o no ha la stessa estensione. Sarebbe utile introdurre una nomenclatura specifica per il nome file. Per esempio pippo.pdf potrebbe diventare pippo_signed (o semplicemente _sig.pdf).

4) La firma remota è solo una specifica modalità di sottoscrizione
È vero. La firma remota è definita nel DPCM 22 febbraio 2013 (articolo 1, comma 1, lettera q) come "particolare procedura di firma elettronica qualificata o firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse".

Questa tipologia di firma è una FEQ (firma elettronica qualificata) a tutti gli effetti e una volta apposta non è distinguibile da una qualunque altra FEQ apposta in altro modo. Questo fatto richiede meccanismi di controllo esclusivo per il titolare della sottoscrizione. L'apposizione di una FEQ in modalità remota che utilizzi solo un PIN (e non anche una password monouso) è consentita esclusivamente a fronte di esplicita autorizzazione scritta di AgID a fronte di una richiesta del prestatore di servizi fiduciari qualificato che intende utilizzare la procedura di sicurezza semplificata.

5) La firma remota e la firma automatica sono equivalenti
La firma automatica è definita nell'articolo 1, comma 1, lettera r del DPCM 22 febbraio 2013. Questa definizione sviluppa i principi stabiliti nei commi 2 e 3 dell'articolo 35 del CAD.

La firma apposta con procedura automatica diventa nel gergo comune firma automatica ed è definita come "particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo".

Nella realtà la firma automatica non sempre è utilizzata con piena rispondenza ai suoi requisiti di legge ovvero al principio della consapevolezza della sottoscrizione da parte del titolare.

La firma automatica è nata per la sottoscrizione di documenti informatici che per loro natura non richiedono di essere presentati al titolare della firma, prima dell'apposizione della stessa chiaramente e senza ambiguità. Questo consente di firmare flussi documentali omogenei e in grande quantità. La procedura è utilizzata dal titolare previo consenso e viene avviata sotto il suo controllo esclusivo anche senza presidio puntuale e continuo.

Il titolare che non vede quello che sottoscrive e ne ha dato consenso è tutelato da quanto stabilito nel più volte citato DPCM nell'articolo 5, comma 2. Il certificato qualificato utilizzato per la procedura automatica contiene chiavi specializzate per tale procedura e estensione esplicita per referenziare tale utilizzo. Ogni dispositivo utilizzato per la procedura automatica richiede una specifica e diversa referenza.

In alcuni scenari tale procedura viene utilizzata per sottoscrivere flussi non omogenei di documenti ovvero il sottoscrittore non ha la percezione granulare di quello che sta sottoscrivendo.

In altre parole firma alla cieca con i conseguenti rischi professionali.

L'operazione non è di per sé illegale ma in alcuni casi lo diventa se la firma con procedura automatica snatura la funzione dichiarativa della sottoscrizione consistente nell'assunzione della paternità del documento o, per traslato, dell'espressione del consenso relativo al documento sottoscritto.

Il rischio è basso per fatture o atti di routine; elevato per referti clinici, contratti specifici o comunque documenti non identificabili a priori in un flusso omogeneo.

La firma automatica è comunque una FEQ ma distinguibile da una firma remota. Nel gergo è anche chiamata firma massiva perché viene utilizzata per sottoscrivere flussi copiosi di documenti ma la sua vera origine giuridica è nel fatto che non vedo quello che sottoscrivo.

6) Per certificare il tempo di un documento è obbligatorio utilizzare una marca temporale qualificata
È falso. Il DPCM 22 febbraio 2013 stabilisce nell'articolo 41 i riferimenti temporali opponibili ai terzi. A livello nazionale è possibile e valido utilizzare una marca temporale non qualificata. Se il riferimento temporale deve avere un valore nel mercato interno comunitario allora è indispensabile un marca temporale emessa da un prestatore di servizi fiduciari qualificato ai sensi del regolamento eIDAS.

7) Il sigillo elettronico è la sottoscrizione di una persona giuridica
È falso. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo qualificato è associato.

Utilizzando una classificazione "classica" dottrinale utilizzata dai giuristi possiamo dire che le tre principali funzioni di una sottoscrizione autografa sono: la funzione indicativa, la funzione probatoria e la funzione dichiarativa.

Il sigillo svolge certamente la funzione indicativa in quanto individua e distingue il creatore del sigillo da altri soggetti giuridici. La persona giuridica può essere identificata da un sigillo elettronico.

Il sigillo elettronico è anche idoneo a svolgere la funzione probatoria cioè, nel caso del sigillo qualificato, forma prova sulla correttezza dell'origine dei dati ai quali il sigillo è associato.

La funzione che il regolamento eIDAS non richiama in modo diretto è quella dichiarativa consistente nell'assunzione della paternità del documento.

La funzione dichiarativa non è da escludere per il sigillo elettronico. Ma non essendoci una posizione esplicita nel regolamento eIDAS si deve applicare il diritto nazionale.

8) La mia firma è scaduta
È falso. La sottoscrizione come atto avente valore probatorio non può scadere. Per motivi tecnologici scade (o è revocato/sospeso) il certificato digitale del sottoscrittore. Per evitare problemi è opportuno associare ad uno o più documenti informatici sottoscritti un riferimento temporale opponibile ai terzi. Nella pubblica amministrazione lo strumento più diffuso è fornito dal riferimento temporale contenuto nella segnatura del protocollo informatico.

9) Quando firmo una clausola in un contratto non firmo l'intero documento (PDF)
È vero. Ma è un fatto di visualizzazione. In verità ogni firma PAdES viene generata sull'intero documento. L'azione operativa che mi fa sottoscrivere (e digitare il PIN) con una firma rappresentata graficamente nella "zona" di una clausola fa ritenere che ho firmato solo la clausola. Praticamente è opportuno che ogni clausola sia esplicitamente approvata dal sottoscrittore.

10) Ho ricevuto un documento e ho il messaggio "firma non valida" durante la verifica
Il messaggio "firma non valida" da parte del verificatore di FEQ è spesso utilizzato in modo scorretto. Molto spesso si tratta di un paio di bit fuori posto nel file verificato. Non esiste una soluzione "chiavi in mano" al problema. Sarebbe utile che i verificatori fornissero un maggior numero di informazioni sul fallimento della verifica. In ogni caso si applica l'articolo 63, comma 3 del DPCM 22 febbraio 2013. Le difformità che non mettono a rischio la sicurezza della sottoscrizione (tipo l'evidenza della non integrità del documento) non ne inficiano la validità.

Fonte: https://www.agendadigitale.eu/documenti/firme-elettroniche-un-decalogo-la-risposta-a-dieci-dubbi-ricorrenti/

Firme elettroniche, un decalogo: la risposta a dieci dubbi ricorrenti - G. Manca, 11 maggio 2018