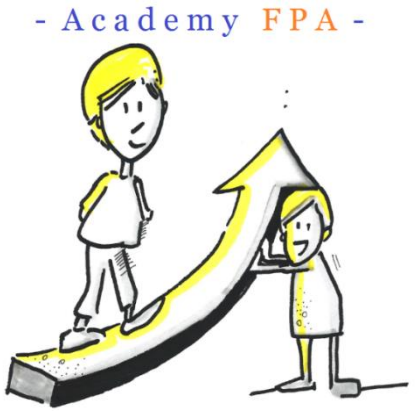

- Academy FPA -

#forumpa2016

Cosa cambia col Regolamento eIDAS: impatti sul CAD, opportunità e obblighi

Andrea Caccia

Servizi Fiduciari

- Il Regolamento eIDAS entra in vigore il 1/7/'16 abrogando ed estendendo la Direttiva 1999/93/CE
- Garanzia delle transazioni elettroniche
  - eIDAS = electronic Identification, Authentication & Signature/Seal
- Definizione di un elenco ristretto di servizi fiduciari (trust services)
  - Emissione di certificati per firme e sigilli elettronici / autenticazione di siti web
  - Validazione e conservazione di firme e sigilli elettronici
  - Validazione temporale
  - Recapito certificato
- Sono consentiti "servizi fiduciari nazionali" in base al Considerando 25: "È opportuno che gli Stati membri mantengano la libertà di definire altri tipi di servizi fiduciari oltre a quelli inseriti nell'elenco ristretto di servizi fiduciari di cui al presente regolamento, ai fini del loro riconoscimento a livello nazionale quali servizi fiduciari qualificati."

Servizi Fiduciari qualificati

- Godono di forme di presunzione legale
- Il certificato qualificato di firma, se associato ad un dispositivo qualificato per la creazione di firme, consente di creare firme elettroniche qualificate
  - Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa ed è riconosciuta come tale in tutti gli Stati membri
- Il certificato qualificato di sigillo, se associato ad un dispositivo qualificato per la creazione di sigilli, consente di creare sigilli elettronici qualificati
  - Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato ed è riconosciuto come tale in tutti gli Stati membri
- Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate ed è riconosciuto come tale in tutti gli Stati membri
- I dati inviati e ricevuti mediante servizio di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio di recapito certificato qualificato.

La qualificazione *(era l'accreditamento di AgID)*

- Ogni Stato membro:
  - designa un organismo di vigilanza per il proprio territorio (per l'Italia sarà designata l'AgID)
  - istituisce, mantiene e pubblica un elenco di fiducia, con le informazioni relative ai prestatori di servizi fiduciari qualificati (e ai servizi fiduciari qualificati prestati) di cui è responsabile
- Per ottenere (o mantenere) la qualifica il prestatore di servizi fiduciari deve:
  - Ottenere ogni 24 mesi una relazione di valutazione della conformità ai requisiti del Regolamento da parte di un Organismo di Certificazione (CAB - Conformity Assessment Body) accreditato secondo il Regolamento (CE) 765/2006

    -> in Italia opera ACCREDIA, Circolare 17/2016 - Schema eIDAS)
  - Chiedere la qualificazione all'Organismo di vigilanza competente sul proprio territorio, allegando la relazione di cui sopra
- Se il richiedente è valutato idoneo l'organismo di vigilanza assegna (o mantiene) la qualifica di prestatore di servizi fiduciari qualificato e garantisce l'aggiornamento dell'elenco di fiducia
- Con la qualificazione può utilizzare sul proprio sito e nelle proprie comunicazioni l'apposito logo

CAB e accreditamento - Contestualizzazione

- L'accreditamento è un'attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate - Tratto dal Regolamento (CE) n. 765/2008
- il sistema di accreditamento, sia esso volontario o cogente, è riconosciuto come strumento di regolazione e protezione dell'interesse pubblico nella libera circolazione dei beni e dei servizi all'interno della UE
- Si inserisce in un contesto mondiale gestito dallo IAF (International Accreditation Forum e da accordi multilaterali (MLA) che opera in genere con organizzazioni regionali
- Gli enti di accreditamento di tutta la regione europea (più ampia della UE) fanno riferimento ad EA
- Il Regolamento eIDAS rimanda al Regolamento (CE) n. 765/2008 quanto alle regole per la valutazione di conformità sei servizi fiduciari
- EA ed ETSI hanno collaborato per definire la norma ETSI EN 319 403 basata sulla norma armonizzata ISO/IEC 17065 per l'accreditamento dei CAB eIDAS - Comunicato: http://goo.gl/2JHlRK
- Lo schema italiano è in linea con quanto richiesto da EA ed è la circolare n. 17/2016 del 19 maggio disponibile sul sito Accredia http://goo.gl/8lrvke
- L'ETSI ha pubblicato un framework di norme a supporto del Regolamento che viene richiamato dalla circolare Accredia
- Il rispetto delle norme costituisce presunzione di conformità ai requisiti del Regolamento

Norme di riferimento per i CAB

Estratto dalla Circolare ACCREDIA n. 17/2016

1) Regole di certificazione

Norma di accreditamento	UNI CEI EN ISO/IEC 17065
Norme di certificazione (riferimenti principali)	ETSI EN 319 401 (nella versione più recente) ETSI EN 319 411-2, supportata dalla ETSI EN 319 411-1 ETSI EN 319 421 e 422 [servizio di emissione di marche temporali] ETSI EN 319 412 (1, 2, 3, 4 e 5) [Limitatamente alle CA]

- Tutte le norme ETSI sono ricercabili e scaricabili gratuitamente dal relativo sito: http://www.etsi.org/standards-search

Da "Certificatori" a Servizi Fiduciari qualidicati

- I certificatori che risultano accreditati alla data in cui entra in vigore eIDAS sono considerati Prestatori di servizi fiduciari qualificati per l'emissione di certificati qualificati ai sensi del Regolamento eIDAS
- Entro un anno (1/7/2017) devono comunque presentare ad AgID una relazione di valutazione della conformità rilasciata da un CAB accreditato
- Si applicano comunque a tutti le nuove regole dal 1/7/2016 pertanto in caso di necessità l'AgID ha la possibilità di richiedere anche prima del 1/7/2017 una relazione di valutazione della conformità rilasciata da un CAB accreditato
- Non vale per l'emissione di marche temporali, la cui validità resterà limitata all'ambito nazionale fino all'eventuale qualificazione secondo le nuove regole
- E' dubbio se è applicabile all'emissione di altri certificati qualificati (sigilli elettronici e web): i certificatori si dovranno attenere alle indicazioni fornite da AgID in quanto responsabile della vigilanza

Servizi Fiduciari "nazionali"

- Non possono essere tipologie di servizo presenti nell'elenco ristretto specificato in eIDAS
- Si applicano le leggi nazionali ed hanno effetto legale solo a livello nazionale, fatto salvo il principio di non discriminazione di firme, sigilli, documenti elettronici
- Possono comunque appoggiarsi, in tutto o in parte, ai meccanismi individuati nel Regolamento, in particolare ad esempio richiedere una relazione di valutazione della conformità ai requisiti nazionali da parte di un Organismo di Certificazione accreditato secondo lo "schema eIDAS" ed essere soggetti a vigilanza
- Esempi di servizi fiduciari nazionali che sono definibili servizi fiduciari nazionali in Italia:
  - Posta elettronica certificata
  - conservatori accreditati
- L'estensione dello "schema eIDAS" a PEC e conservatori dipende dalla versione finale del CAD, è in linea con lo schema di decreto che è stato approvato dal CdM
- È auspicabile comunque che per entrambi questi servizi si valuti un'evoluzione che tenga conto di norme tecniche europee, quando disponibili

Formati di firma/sigillo obbligatori per la PA

- Se uno Stato membro richiede una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico

  -> tale Stato membro riconosce le firme elettroniche avanzate [basate su certificato qualificato o meno] e le firme elettroniche qualificate almeno nei formati o che utilizzino i metodi definiti negli appositi atti di esecuzione

- Se uno Stato membro richiede una firma elettronica avanzata basata su certificato qualificato per utilizzare i servizi online offerti da un organismo del settore pubblico

  -> tale Stato membro riconosce le firme elettroniche avanzate basate su certificato qualificato e qualificate almeno nei formati o che utilizzino i metodi definiti negli appositi atti di esecuzione

- Idem - mutatis mutandis - per i sigilli elettronici avanzati
- Già pubblicata la Decisione di Esecuzione (UE) 2015/1506 della Commissione che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere
- Non vi sono obblighi per il settore privato fermo restando che il rispetto delle norme tecniche referenziate dagli atti delegati dà la presunzione di conformità
- Il Regolamento ha un approccio fondamentalmente neutrale rispetto alla tecnologia e non vincola pertanto rispetto a possibili innovazioni tecnologiche, che potranno essere oggetto di normazione in un secondo momento se adottate dal mercato

Formati di firma/sigillo obbligatori per la PA

Estratto della Decisione di Esecuzione (UE) 2015/1506 sulle firme elettroniche

ALLEGATO

Elenco delle specifiche tecniche per le firme elettroniche avanzate XML, CMS o PDF e per il contenitore con firma associata

Le firme elettroniche avanzate di cui all'articolo 1 della decisione devono rispettare una delle seguenti specifiche tecniche ETSI, ad eccezione della clausola 9:

Profilo di base XAdES	ETSI TS 103171 v.2.1.1. ([1])
Profilo di base CAdES	ETSI TS 103173 v.2.2.1. ([2])
Profilo di base PAdES	ETSI TS 103172 v.2.2.2. ([3])

Il contenitore con firma associata di cui all'articolo 1 della decisione deve rispettare le seguenti specifiche tecniche ETSI:

Profilo di base del contenitore con firma associata	ETSI TS 103174 v.2.2.1. ([4])

Formati di firma/sigillo obbligatori per la PA

Estratto della Decisione di Esecuzione (UE) 2015/1506 sui sigilli elettronici

Elenco delle specifiche tecniche per i sigilli elettronici avanzati XML, CMS o PDF e per il contenitore con sigillo associato

I sigilli elettronici avanzati di cui all'articolo 3 della decisione devono rispettare una delle seguenti specifiche tecniche ETSI, ad eccezione della clausola 9:

Profilo di base XAdES	ETSI TS 103171 v.2.1.1.
Profilo di base CAdES	ETSI TS 103173 v.2.2.1.
Profilo di base PAdES	ETSI TS 103172 v.2.2.2.

Il contenitore con sigillo associato di cui all'articolo 3 della decisione deve rispettare le seguenti specifiche tecniche ETSI:

Profilo di base del contenitore con sigillo associato	ETSI TS 103174 v.2.2.1.

N.B.: L'ETSI ha recentemente pubblicato un nuovo set di norme (ETSI EN 319 122 (CAdES), ETSI EN 319 132 (XAdES), ETSI EN 319 142 (PAdES) e ETSI EN 319 162 (ASiC) ma queste diventeranno obbligatorie solo a seguito della pubblicazione di un eventuale aggiornamento della Decisione 1506

Norme transitorie (Articolo 51 eIDAS)

- I certificatori già accreditati al 1/7/2016 diventano prestatori di un servizio qualificato di emissione di certificati qualificati per la firma elettronica

  -> entro il 1/7/2017 si applicano comunque integralmente le nuove regole che richiedono in particolare la valutazione di conformità da parte di un CAB accreditato secondo lo schema eIDAS (o equivalente)
- Per l'emissione di certificati qualificati per sigillo o per siti web si applicano le norme nuove

  -> è necessaria la qualificazione a partire dal 1/7/2016 salvo diverse comunicazioni dell'AgID
- Per l'emissione di validazioni temporali (marche temporali) si applicano le norme nuove

  -> è necessaria la qualificazione a partire dal 1/7/2016)
- I certificati emessi prima dell'entrata in vigore di eIDAS restano validi fino a scadenza o revoca
- Le firme create prima dell'entrata in vigore di eIDAS restano valide
- La certificazione dei dispositivi di firma (compresi quelli di firma remota) resta valida anche dopo il 1/7/2016

Grazie per l'attenzione