CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Vigilanza e controllo

sull'attività dei certificatori qualificati e accreditati

(articolo 31 D.lgs. 7 marzo 2005, n. 82)

Bollettino n. 1 – luglio 2006

Finalità

Il presente bollettino, a cura dell'Ufficio Standard e metodologie d'identificazione, ha l'obiettivo di informare sull'attività di vigilanza sui certificatori qualificati, effettuata dal CNIPA a cura del medesimo Ufficio.

L'attività viene svolta al fine di ottemperare agli obblighi legislativi in capo a questo Centro come previsto dall'articolo 31 del Codice dell'amministrazione digitale.

Questo primo numero descrive l'attività di vigilanza svolta fino ad oggi e sintetizza le azioni che si stanno intraprendendo affinché la vigilanza sia effettuata sulla base di schemi e principi ben delineati descritti in appositi documenti al fine, da un lato, di formalizzare le attività di vigilanza, dall'altro di garantire adeguato rispetto dei principi di trasparenza ed imparzialità cui la vigilanza dovrà continuare ad ispirarsi come è stato fino a oggi.

La vigilanza

La Direttiva europea 1999/93/CE prescrive, all'articolo 3 comma 3, che "***Ciascuno Stato membro provvede affinché venga istituito un sistema appropriato che consenta la supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio e rilascia al pubblico certificati qualificati***".

Tale organismo è stato identificato, da ultimo, dall'articolo 31 del Codice della amministrazione digitale nel Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

Il CNIPA deve quindi ottemperare a diverse previsioni normative derivanti dal conferimento delle funzioni di vigilanza e controllo sull'attività dei certificatori qualificati, oltre che a quelli derivanti dall'attività di accreditamento volontario.

Per chiarezza di informazione si ricorda che i "certificatori qualificati" sono i soggetti che intendono emettere certificati qualificati secondo la Direttiva europea 1999/93/CE, soggetti che si distinguono in certificatori "accreditati" e "notificati".

La differenza sostanziale fra le due tipologie è che i primi si sottopongono ad apposita istruttoria preventiva volta a verificare il possesso in capo agli stessi dei requisiti richiesti dalle norme in materia.

Altra sostanziale differenza è che lo scambio con le pubbliche amministrazioni di documenti sottoscritti con firma digitale deve far uso di certificati qualificati rilasciati da certificatori accreditati.

Queste ragioni fanno si che, alla data, tutti i certificatori qualificati hanno intrapreso le azioni necessarie per essere accreditati. Ciò premesso, recependo la Direttiva europea citata precedentemente, il CNIPA è stato designato, anche a livello comunitario, a operare come l'organismo nazionale di accreditamento e di vigilanza sulle attività svolte dai certificatori accreditati([1]).

Inoltre, è opportuno ricordare che tali soggetti non svolgono solo l'attività di certificazione inerente la firma digitale ma anche, ai sensi del regolamento (DPR 117/2004) relativo alla Carta Nazionale dei Servizi (CNS), l'attività di rilascio dei certificati di autenticazione necessari all'emissione di tale smart card.

A parte il rispetto degli obblighi normativi, la vigilanza su tali soggetti è ovviamente fondamentale per l'intero impianto della firma digitale nel nostro Paese.

Difatti, la robustezza degli algoritmi utilizzati, la sicurezza dei dispositivi sicuri per la generazione della firma (smart card), i meccanismi crittografici utilizzati, non servirebbero a garantire nulla se il soggetto che certifica la corrispondenza fra una chiave pubblica ed i dati anagrafici del titolare della stessa, ad esempio, non agisse con serietà e competenza, garantendo quindi i richiesti livelli di affidabilità, qualità e sicurezza.

L'attività di vigilanza effettuata

Quanto detto fino ad ora non deve trarre in inganno e far pensare che i certificatori non siano mai stati, ad oggi, oggetto di alcuna verifica.

[1] http://europa.eu.int/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#Italy

Il CNIPA tramite l'Ufficio designato (oggi denominato Standard e tecnologie d'identificazione) ha sempre effettuato verifiche, sia attraverso la rete, sia, nel limite delle risorse economiche assegnate, con delle visite presso alcune sedi operative dei certificatori.

Durante tale attività vari certificatori sono stati sollecitati a intraprendere le necessarie azioni per mantenere il rispetto della normativa vigente in materia.

Gli interventi maggiormente significativi si sono verificati nelle seguenti situazioni:

- autorità di registrazione che dichiarava in modo improprio di essere certificatore accreditato. Si trattava invece solamente della organizzazione che svolgeva l'attività di registrazione per nome e per conto di un certificatore accreditato.

- Erronea versione di software per il rinnovo dei certificati nella smart card. Tale software compilato in modalità "*debug*" è stato erroneamente distribuito. Questo ha causato la registrazione del PIN su un file di LOG all'insaputa del titolare con conseguente problema di sicurezza. L'altissimo numero di utenti coinvolti ha indotto il certificatore, oltre che all'ovvia correzione del software, anche a modificare alcuni processi organizzativi interni.

- Nel rilascio della smart card di firma veniva inserito nel campo deputato a contenere l'organizzazione di appartenenza del titolare della firma, la denominazione del certificatore. Anche in questo caso l'intervento del certificatore è stato tempestivo e efficace.

- I canali informativi ufficialmente resi disponibili dal certificatore ai titolari fornivano informazioni inesatte o comunque ambigue o, in altri casi, gli operatori non erano a conoscenza delle modalità di fruizione di servizi che il certificatore accreditato è obbligato a fornire, quale ad esempio il servizio di marcatura temporale.

Ma seppur nella routine della vigilanza è opportuno ricordare anche le decine di interventi relativi a:

- verifica della conformità dei documenti sottoscritti alle norme sulla interoperabilità relative al riconoscimento e alla verifica del documento informatico (Deliberazione CNIPA 4/2005). In tal senso è estremamente significativa l'attività di collaborazione, nei casi dubbi, con il Garante per la protezione dei dati personali per la verifica delle notifiche sottoscritte digitalmente;

- modifiche dell'assetto societario o dell'organizzazione del certificatore non comunicate tempestivamente dal certificatore stesso al CNIPA;

- puntuale controllo dei formati delle informazioni inserite nell'elenco pubblico tenuto dal CNIPA;

- puntuale controllo delle informazioni diffuse dai certificatori per verificarne la conformità alla normativa.

Anche nei casi sinteticamente appena citati la risposta correttiva dei certificatori è stata sempre sufficientemente rapida, precisa e risolutiva.

Le sanzioni

Da notare che legislazione in materia non prevede alcuna forma di sanzione nel caso di inadempienza da parte dei certificatori. Le norme vigenti in altri Stati membri dell'UE, consentono di intervenire con gradualità commisurata alla gravità dell'inadempienza rilevata.

Ad esempio vi sono sanzioni pecuniarie che vanno da poche centinaia di euro, fino a interventi limite che vedono il divieto di proseguire l'attività.

In Italia, non essendo prevista alcuna gradualità di intervento, si può solo vietare al soggetto inadempiente di proseguire l'attività di certificazione.

Tale sanzione, i cui effetti difficilmente reversibili sono di una gravità estrema, non è mai stata applicata in quanto non commisurata alle inadempienze fino ad oggi rilevate che, fra l'altro, sono state rapidamente colmate ad opera dei certificatori accreditati.

I piani per il futuro

Da quanto descritto fino ad ora emerge evidente l'esigenza di eseguire una sempre maggiore attività di vigilanza che necessita tuttavia di essere efficacemente strutturata e giustamente formalizzata.

Per far fronte a questa necessità questo Centro nazionale, attraverso l'Ufficio standard e tecnologie d'identificazione, sta formalizzando le modalità operative della vigilanza attraverso la redazione di apposite linee guida.

Le attività previste vedranno la seguente evoluzione:

- entro il mese di settembre 2006 si prevede di predisporre una prima bozza del documento "Linee guida per la vigilanza sui certificatori qualificati";
- entro la seconda decade del mese di ottobre si incontreranno Assocertificatori e i certificatori accreditati al fine di rendere manifesti i principi ispiratori ed ottenere il riconoscimento da parte dei soggetti controllati dei principi di neutralità e trasparenza delle "Linee guida";
- entro la prima decade di novembre verrà rilasciata la prima versione delle "Linee guida";
- nella seconda decade di novembre avranno inizio gli interventi di vigilanza presso le sedi operative dei certificatori;
- entro la seconda decade di dicembre 2006 termineranno gli interventi programmati per l'anno 2006 e che saranno effettuati presso 5 certificatori.

L'attività di vigilanza proseguirà, quindi, nel 2007 in modo da verificare tutti i certificatori accreditati che, alla data odierna, ammontano a diciotto soggetti. Aver eseguito la vigilanza presso un certificatore non esclude che possa essere ripetuta presso il medesimo soggetto anche dopo poco tempo. La vigilanza viene effettuata infatti periodicamente ma anche d'ufficio o a seguito di segnalazioni da parte di terzi di situazioni che richiedono una verifica da parte del CNIPA. Comunque, a parte casi particolari, la vigilanza sistematica con visita presso le sedi certificatore avverrà almeno una volta all'anno.

Il prossimo bollettino è programmato per l'autunno 2006 e conterrà tra l'altro la sintesi delle "Linee guida".