

Vigilanza e controllo

sull'attività dei certificatori qualificati e accreditati

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

Bollettino n. 2 – ottobre 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. 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.

Nel 1° numero viene illustrata l'attività di vigilanza svolta fino ad oggi e definite in sintesi le azioni di vigilanza che si stanno portando avanti.

Questo 2° numero sintetizza invece gli aspetti principali del documento "Linee guida per la vigilanza sui certificatori qualificati". Tale documento costituisce il punto di riferimento per effettuare una vigilanza sulla base di schemi e principi ben delineati.

Il presente bollettino fornisce anche indicazioni sul calendario delle ispezioni ai certificatori accreditati da svolgersi entro il 2006.

Il contenuto del bollettino è stato presentato ai certificatori in data 13 ottobre 2006.

Le Linee Guida

IL documento “Linee guida per la vigilanza sui certificatori qualificati” definisce una base comune di valutazione su cui fondare le operazioni di vigilanza al fine di garantire il giusto equilibrio nel valutare il rispetto delle norme da parte dei certificatori.

L’ampia gamma delle attività svolte da questi soggetti può comportare il rispetto della normativa anche con soluzioni tecniche differenti. La doverosa “neutralità” della legislazione, che non specifica tutti i requisiti tecnici nei minimi dettagli, rende necessarie regole trasparenti e condivise atte a garantire il rispetto della normativa e l’equilibrio nelle valutazioni.

Le “Linee guida” indicano - sia ai certificatori qualificati, sia a coloro che espletano tale vigilanza tramite verifiche e ispezioni (tali soggetti sono denominati valutatori) - le modalità con cui le operazioni vengono svolte dai valutatori. Inoltre vengono descritte anche le attività di supporto che i certificatori devono fornire ai medesimi valutatori nel corso di tali operazioni

La struttura del documento

Le “Linee guida” sono strutturate in base allo schema delle specifiche tecniche europee ETSI TS 101 456 e del Technical Report ETSI TR 102 437.

Tale scelta deriva dal fatto che il TS 101 456 - sulla cui attuazione il TR 102 437 fornisce le indicazioni operative - è stato redatto dallo European Telecommunications Standard Institute - ETSI nell’ambito della European Electronic Signature Standardisation Initiative - EESSI, lanciata nel 1999 su impulso della Commissio-

ne Europea con lo scopo di fornire una adeguata base tecnica alla Direttiva 1999/93/CE.

In particolare, ETSI TS 101 456 è lo schema di politiche di sicurezza per la certificazione (Certificate Policy) adottato da numerosi paesi membri dell’UE e quindi costituisce una base comune in tali paesi. La normativa italiana sulle firme elettroniche è conforme a tale specifica.

L’altro documento ETSI TR 102 437 è impostato in base ad un documento redatto dall’organismo dei Paesi Bassi TTP-NL con finalità analoghe a quelle contenute nelle “Linee guida”. Costituisce quindi un fattore di uniformità che si sta affermando a livello comunitario.

Nella stesura delle “Linee guida” si è tenuto conto anche delle indicazioni sulle misure di sicurezza specificate nel documento ISO/IEC 17799 e ai controlli indicati nell’altro documento ISO/IEC 27001. Il tutto è riportato negli ambiti della normativa italiana.

Le “Linee guida” dopo i classici capitoli introduttivi che riportano il quadro giuridico e tecnico di riferimento - fornendo anche le principali modalità di impostazione delle verifiche - entra nel dettaglio degli aspetti tecnico-giuridici dell’attività di certificatore qualificato. Ad ognuno di essi viene dedicato un capitolo, suddiviso in tre paragrafi:

- il primo indica i dispositivi giuridici applicabili;
- il secondo indica le attività operative e di supporto che il certificatore deve svolgere per rendere possibili le operazioni di vigilanza;
- il terzo indica le attività sulle quali si può basare il valutatore nello svolgimento della sua attività.

Fasi della vigilanza

Le attività di vigilanza si articolano nelle seguenti fasi :

1. acquisizione da parte del valutatore dei documenti già in possesso del CNIPA (manuale operativo, piano per la sicurezza, struttura organizzativa, ecc.);
2. acquisizione da parte del valutatore di determinato materiale e documentazione del certificatore (procedure, certificati, marche temporali, verbali, ecc.);
3. analisi dei documenti sopra citati;
4. effettuazione delle verifiche “fisiche” presso le sedi del certificatore e acquisizione di eventuale ulteriore materiale e documentazione;
5. redazione del verbale dell’ispezione;
6. comunicazione del verbale al certificatore e al CNIPA.

Cosa verrà richiesto al certificatore nell’ispezione ?

Il certificatore, a richiesta, deve esibire la documentazione atta a dimostrare il rispetto dei requisiti di legge e di sicurezza, in conformità, ove applicabile, con gli standard prodotti da ETSI e da ISO/IEC.

Il certificatore dovrebbe essere almeno in possesso di:

- verbali di ispezioni effettuate presso le proprie sedi e presso le sedi di eventuali fornitori esterni;
- verbali di prove di ripartenza dei sistemi e del recupero di dati dai siti di backup;
- documentazione relativa alle misure correttive adottate per gestire le situazioni anomale riscontrate durante le ispezioni.

Inoltre il certificatore deve garantire al team di valutazione l’accesso a sistemi e locali utilizzati per la fornitura dei servizi di certificazione, anche se di pertinenza di suoi fornitori.

Ispezioni previste nel 2006

Entro la fine dell’anno verranno effettuate ispezioni presso cinque certificatori. La data esatta della singola ispezione sarà comunicata al certificatore interessato con un breve anticipo, con almeno 48 ore.

Il prossimo numero

Il prossimo numero del bollettino – in programma inizio 2007 - riporterà la sintesi dei risultati delle prime cinque attività di vigilanza e il calendario di massima dell’intero piano di ispezioni del 2007.