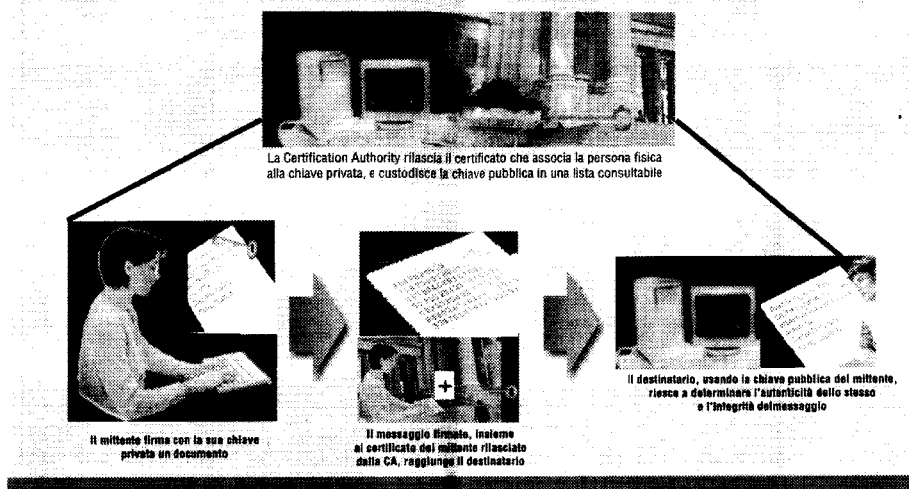


Risolto a metà aprile un problema operativo legato ai differenti criteri di verifica d'autenticità

# Firma digitale all'ultimo atto

Definita dagli enti certificatori coinvolti la standardizzazione delle caratteristiche del documento

## I PUNTI CHIAVE



**Fase due:  
la lettura  
omogenea  
dei dati  
in tutt'Europa**

**L**a firma digitale, già operativa dai primi mesi dell'anno, a metà aprile ha sciolto l'ultimo nodo, quello della interoperabilità tra diversi enti certificatori, che impediva di utilizzare tutta la potenzialità innovativa di questo strumento. L'impianto normativo avviato da Franco Bassanini con la legge 59 del 15 marzo 1997 prevede infatti alcuni principi di base. Per fare in modo che un atto firmato in rete abbia lo stesso valore legale di un documento cartaceo, è infatti indispensabile identificare con assoluta certezza chi appone la firma (identità); che il documento non possa essere modificato mentre passa da un computer all'altro (integrità); che, una volta firmato, qualunque degli attori non possa rinnegare la propria firma (non ripudiabilità).

Non dimentichiamo che l'impianto normativo della

legge 59, come il regolamento predisposto dall'Aipa contenuto nel Dpr n.513 del 10 novembre '97 e gli aspetti tecnici e organizzativi previsti nel Dpcm dell'8 febbraio 1999, ha il compito non solo di garantire i privati che sottoscrivono un contratto (compito già impegnativo), ma anche gli atti che coinvolgono la Pubblica amministrazione. Con la firma digitale Bassanini ha infatti voluto non solo facilitare i rapporti di business a distanza, ma anche accelerare l'iter dei provvedimenti amministrativi, senza rinunciare alle garanzie indispensabili, e far dialogare in rete cittadini e Pa.

Ma per garantire l'identità dei soggetti (pubblici o privati) che utilizzano la firma è necessario un ente certificatore che vigili sull'identità, integrità e non ripudiabilità della firma stessa. Ma chi firma deve anche essere tutelato nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione. Il Dpr 513/97 richiede quindi che il certificatore sia in possesso di determinati requisiti e sia incluso in un elenco pubblico, consultabile online, predi-

sposto e tenuto aggiornato dall'Autorità per l'informatica nella Pubblica amministrazione (Aipa). Quando però i primi enti certificatori abilitati hanno iniziato a svolgere i loro compiti, nonostante rispondessero a direttive imposte da standard internazionali si è visto che, di fatto, esistevano alcune differenze di natura tecnica che impedivano il dialogo tra certificati emessi dai diversi enti certificatori. Dal marzo scorso dunque gli enti certificatori (candidati o già ammessi dall'Aipa) si

sono seduti intorno a un tavolo e hanno definito i requisiti minimi di interoperabilità.

«Gli standard purtroppo — afferma Mario Gentili, funzionario dell'Aipa — danno libertà a interpretazioni di natura sintattica o semantica che vanno a discapito della omogeneità operativa e della corretta interazione tra gli utenti che utilizzano la firma digitale. Se per esempio il certificato di firma rilasciato da un

ente certificatore "A" utilizza come carattere di separazione delle informazioni il trattino e il certificato di firma rilasciato da un ente certificatore "B" usa lo slash, alla fine nessuno è più in grado di leggere la firma certificata dall'altro, sebbene tutte contengano l'informazione principale. Si trattava di raggiungere un accordo sul trattamento di alcune informazioni, previste da standard internazionali, ma la cui interpretazione locale era lasciata alla libertà di chi sviluppava il software».

I certificatori quindi hanno ridiscusso e trovato un accordo sul formato del certificato della firma (per esempio dove mettere il codice fiscale), sulle estensioni del certificato (obbligatorietà e contenuto di alcune informazioni), sulla modalità in cui si imbastiva un messaggio firmato. L'accordo è stato raggiunto anche sulle Crl, le liste di revoca che contengono l'informazione sulla validità temporale del certificato.

«L'interoperabilità raggiunta — continua Gentili — costituisce infatti un primo passo significativo verso la standardizzazione *de facto*. È stata concepita in Italia con queste caratteristiche, ma sarà anche proposta in sede europea per garantire sicurezza e omogeneità sia per le transazioni più importanti sia per i semplici acquisti online. Attualmente l'Europa sta affrontando le tematiche sulla firma che l'Italia ha già definito».

**MARIA ROSARIA ZINCONE**

