ALLEGATO "6"

LA FIRMA DIGITALE

La firma digitale, realizzata in conformità alle leggi vigenti, rende validi e rilevanti a tutti gli effetti di legge, i documenti informatici, la loro archiviazione su supporto informatico e la loro trasmissione per via telematica.
Nelle applicazioni in cui è rilevante conservare nel tempo il valore legale del documento informatico è necessario poter attribuire ad esso una data certa e dimostrare che la firma è stata apposta durante il periodo di validità della chiave pubblica del sottoscrittore.
Ciò si ottiene attraverso la "marca temporale" (servizio usufruibile tramite l'utilizzo di internet), una sorta di certificato informatico firmato a sua volta da un certificatore riconosciuto nell'ordinamento giuridico italiano (albo certificatori AIPA), che associa data e ora a quel particolare documento.
Qualsiasi tipo di documento informatico è firmabile e cifrabile, in modo da garantire il più elevato livello di riservatezza. Un singolo documento, inoltre, può essere firmato da un numero illimitato di sottoscrittori.
Nel caso di documenti con particolare rilevanza legale, l'utilizzo dei formati specificati negli standard internazionali ISO (ad esempio ASCII, TIFF, JPEG) o de facto (come il PDF) può agevolare la possibilità di dimostrarne il contenuto in giudizio.
La tecnologia What You See Is What You Sign – ciò che vedi è ciò che firmi – elabora i documenti visualizzati all'interno di un'area di memoria protetta, controllando le operazioni di calcolo dell'impronta e relativo passaggio alla smartcard, in modo da associare la firma al documento con il maggior livello di sicurezza possibile. Il sottoscrittore, vedendo il documento al momento della firma, può immediatamente verificarne la correttezza.
Le funzioni di verifica di un documento firmato permettono di stabilire l'integrità del documento (non alterazione), l'identità del sottoscrittore e la validità della firma a tutti i livelli quali: certificazione della chiave pubblica da parte di un certificatore accreditato, presenza di tale certificatore nell'Elenco Pubblico di AIPA al momento della verifica, autenticità dell'Elenco Pubblico di AIPA, eventuale presenza del certificato di chiave pubblica del sottoscrittore nelle liste dei certificati sospesi o revocati, validità di tutti i certificati coinvolti nel processo (AIPA, Certificatore, Sottoscrittore).
In particolare il sistema è compatibile con il servizio di posta *LISP* (*Lombardia Integrata Posta Sicura*), uno dei *Servizi di Base* previsto dalla *Rete Regionale Lombarda* (*RRL*) realizzata dalla Giunta Regionale.

Il protocollo supporta interamente tutte le funzionalità necessarie per implementare la gestione della firma digitale sia per gli atti in partenza che in arrivo.
In particolare si può:
- firmare uno o più documenti da inviare successivamente ai destinatari tramite posta elettronica
- verificare l'autenticità dei mittenti ed estrarre i documenti in arrivo, pervenuti via posta elettronica

La funzionalità di firma è implementata su tutte le modalità di lavoro, compresa la protocollazione in sola partenza.

Operativamente per firmare documenti risolviamo tre situazioni:

1. l'unica postazione preposta alla firma dei documenti è la postazione centrale del protocollo; tutti i firmatari dovranno recarsi presso tale postazione per apporre la propria firma sui singoli documenti. Si delineano tre differenti modalità:

1.1. la firma viene apposta durante la normale procedura di protocollazione (sul singolo atto, man mano che si protocolla);

1.2. la firma viene apposta al termine della protocollazione, per un insieme di documenti distinti relativi a numeri di protocolli diversi (per esempio il Segretario firmerà contestualmente i singoli documenti in un unico momento della giornata, a seguito delle normali attività di protocollazione);

1.3. la firma viene apposta sul documento prima che questi sia protocollato.

2. durante la protocollazione (anche per la protocollazione in partenza) i documenti legati al singolo atto vengono firmati; per far ciò ognuna delle postazioni preposte alla gestione della protocollazione (anche per la protocollazione in partenza) deve essere dotata di lettore di chip-card;

3. i documenti già firmati pervengono all'ufficio protocollo che dovrà a sua volta provvedere alla protocollazione. In questo caso l'addetto del protocollo dovrà comunque avere la possibilità di visionare il documento firmato per poterne desumere il contenuto e gli estremi.