LegalCert
La Firma Digitale
Family

Marcatura Temporale

Servizio di Time Stamping Authority

Data 1 gennaio 2012

InfoCert LegalCert FAMILY

Sommario

1. Introduzione

La marcatura temporale di un documento informatico consiste nella generazione, da parte di una terza parte fidata, di una firma digitale del documento (anche aggiuntiva rispetto a quella del sottoscrittore), alla quale è associata l'informazione relativa ad una data e ad un'ora certa. Un file marcato temporalmente, secondo normativa, ha estensione .TSD (Time Stamping Data): al suo interno contiene il documento del quale si è chiesta la validazione temporale e la marca emessa da InfoCert, in qualità di Ente Certificatore. Il server che genera le marche temporali ricava il tempo, con riferimento al Tempo Universale Coordinato (UTC), da un ricevitore radio sintonizzato (preventivamente tarato e certificato) con il segnale emesso dall'**I**stituto **N**azionale di **RI**cerca **M**etrologica di Torino (INRIM).
Nell'apposita sezione del Manuale Operativo dei Certificati di Sottoscrizione, disponibile sul sito www.firma.infocert.it, è possibile trovare le condizioni di erogazione del servizio ed i vincoli ai quali i richiedenti sono tenuti ad aderire.

2. Riferimenti Normativi

Il servizio si basa sulle regole tecniche emanate dalle competenti autorità italiane: in particolare vengono recepite ed attuate le norme sancite nel Codice dell'amministrazione digitale, nel D.P.C.M. 30/3/2009 e nella delibera CNIPA 45/2009, e recepisce le indicazioni suggerite nel Draft "Time Stamp Protocol (TSP)" del PKIX Working Group di IETF – Maggio 2001 e nel Draft "Policy requirements for time-stamping authorities" di ETSI – Novembre 2001.

3. Caratteristiche del Servizio

La marca temporale è emessa automaticamente da un sistema elettronico sicuro (server della Time Stamping Authority o TSA) dell'Ente Certificatore InfoCert.
La marcatura temporale di un documento informatico prevede che il richiedente invii l'impronta del documento (o il documento cui quest'ultima si riferisce) all'Ente Certificatore.
Il sistema di marcatura riceve l'impronta (o il documento) e vi aggiunge la data e l'ora, ottenendo un'impronta datata. L'Ente Certificatore firma l'impronta datata, cifrandola con la sua chiave di marcatura temporale, ottenendo la marca temporale. Da questa è possibile, attraverso la chiave pubblica dell'Ente Certificatore, recuperare sia l'impronta del documento sia la data e l'ora della sua generazione.
Le marche temporali emesse da InfoCert hanno una validità di 20 anni.
La marcatura temporale di un documento informatico può essere effettuata utilizzando DiKe, il software di firma/verifica fornito gratuitamente da InfoCert, che consente di eseguirne anche un immediato controllo.
La verifica può essere effettuata anche con la funzione disponibile sul sito dell'Ente di Certificazione, all'indirizzo www.firma.infocert.it, o attraverso l'utilizzo di altro software certificato ITSEC E2 che ne condivida gli stessi algoritmi di hashing e crittografia.

Il servizio di marcatura temporale è a **pagamento**, secondo il listino InfoCert.

4. Obiettivi

I principali obiettivi, della marcatura temporale di un documento, sono:

- rendere **opponibile** a terzi un documento informatico **certificando la data certa**, ovvero la data e l'ora in cui sicuramente quel documento esisteva proprio con quel contenuto;

- **estendere** la **validità di un documento informatico** firmato digitalmente **oltre la scadenza del certificato di sottoscrizione**, mantenendola anche nel caso di compromissione del certificato stesso. In questa ipotesi la marca temporale deve essere apposta prima dell'evento che ha compromesso il certificato di sottoscrizione.