

TIMBRO DIGITALE

IL CERTIFICATO HA VALIDITA' 6 MESI. OLTRE I 6 MESI E' SUFFICIENTE COMPILARE LA SEGUENTE DICHIARAZIONE (ART. 41 D.P.R. 445/2000):
IL/LA SOTTOSCRITTO/A DICHIARA CHE LE INFORMAZIONI CONTENUTE NEL PRESENTE CERTIFICATO NON SONO VARIATE DALLA DATA DI
RILASCIO.

COSA FA...

TIMBRO DIGITALE



estensione del Digital Trust al cartaceo

Può accadere che si renda necessario stampare su supporto cartaceo un documento informatico firmato digitalmente con garanzia però di mantenerne inalterato il valore legale.

Cos'è il timbro Digitale

Il Timbro Digitale è un codice a barre bidimensionale (glifo) che contiene non solo l'immagine originale del documento ma anche le verifiche di congruità, originalità dei contenuti e della firma. Il glifo viene elaborato e apposto sul documento informatico da un server dedicato a tale procedimento.

la Verifica con il Viewer

Il sistema di Timbro Digitale prevede anche un processo di verifica, proprio come la firma digitale, attraverso l'uso del modulo software Viewer in grado di decodificare il glifo e quindi estrarne sia la versione originale che le informazioni necessarie a verificare l'attendibilità del documento e della firma digitale nonché eventuali difformità rispetto alla versione stampata sulla quale si trova il glifo.



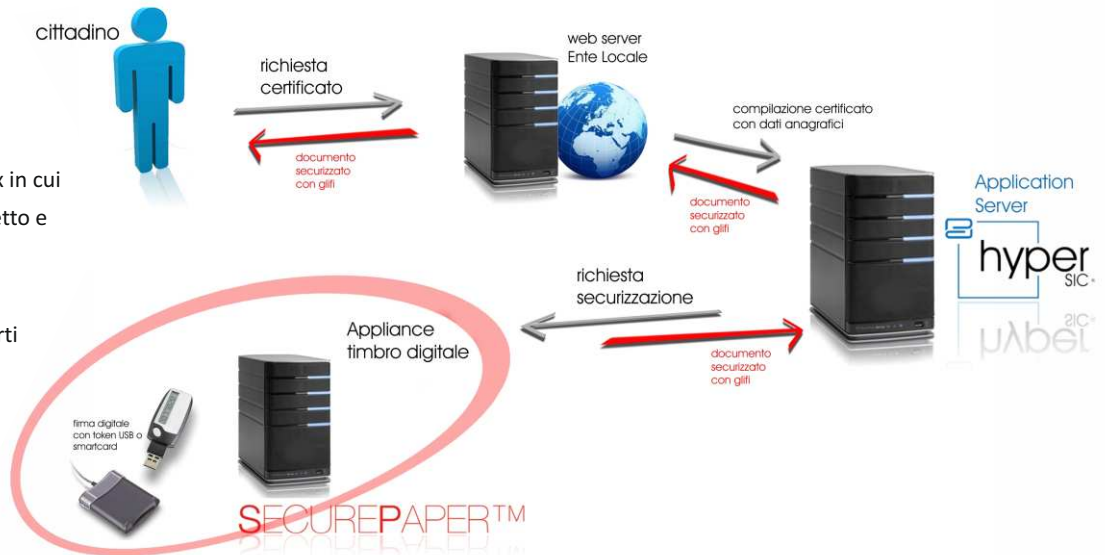
Il cittadino, effettuata la propria autenticazione sul portale dell'Ente o presso uno sportello autorizzato presidiato o automatico (es. totem), accede ai servizi offerti dalla piattaforma di emissione delle certificazioni on line di hyperSIC® alla quale sottopone la richiesta di un certificato.

Questa richiesta viene elaborata dal server hyperSIC® dell'Ente che genera il certificato e lo inoltra all'Appliance di SecurePaper™, collocato fisicamente presso il Comune o altra sede sicura (es. server farm accreditata).

L'appliance esegue nell'ordine le seguenti operazioni:

- Riceve la richiesta tramite web service
- Codifica il contenuto del documento trasformandolo in XML se necessario
- Firma digitalmente la codifica XML tramite PKCS#7 aggiungendo all'interno della busta, se necessario, dati di servizio (numero di pagine, numerazione univoca, uffici di riferimento, ecc.) utilizzando le firme digitali dell'Ente, di tipo smartcard o token USB, che sono ad esso collegato tramite apposito box in cui ciascuna è blindata con lucchetto e sigillo numerato
- Crea il PDF per il richiedente, utilizzando come sfondo le parti fisse pre-configurate come il logo dell'Ente la firma grafica ed alcuni altri dati fissi, ed appone i glifi (serie di Codici a Barre BiDimensionali) creando il timbro digitale

- Restituisce al server hyperSIC® dell'Ente il PDF securizzato e cioè il certificato con timbro digitale.



In nessun caso dati sensibili non firmati digitalmente lasciano il perimetro dei sistemi dell'Ente.



Timbratura «di massa»

L'interfaccia esposta dal sistema di securizzazione può essere affiancata o sostituita da una modalità di scambio dati batch, in cui in luogo delle chiamate al servizio esposto via web service si hanno delle cartelle condivise, più indicate per volumi importanti di transazioni.

TECNOLOGIA

SINCRONISMO ED INTEGRAZIONE PERFETTA TRA SISTEMI ALL'AVANGUARDIA...



SECUREPAPER™ è l'applicazione per l'apposizione del timbro digitale brevettata da LAND Srl, **partner di A.P.Systems**.

SECUREPAPER™ è in grado di proteggere i documenti in tutte le fasi del loro ciclo di vita, indipendentemente dal supporto utilizzato, sia esso cartaceo che elettronico.

SECUREPAPER™ gestisce il documento elettronico firmato digitalmente e lo trasforma in un codice grafico bidimensionale capace di contenere l'intero documento e la relativa firma digitale.

Tutti i documenti timbrati digitalmente si dicono securizzati: essi sono composti da due fondamentali elementi che sono il documento di supporto e l'originale contenuto nei glifi (codici a barre bidimensionali). I documenti vengono prodotti da un apposito server, detto appliance, che effettua tutte le operazioni di preparazione del documento, compressione, firma, ed applicazione dei glifi alla pagina. I documenti così securizzati possono essere inviati via email, pubblicati su un portale, salvati su una chiavetta USB o, banalmente, stampati su carta.

SECUREPAPER™ consente di generare documentazione ibrida sicura (anticontraffazione e valida ai fini legali) e conforme all'originale in modalità completamente automatica.

SECUREPAPER™

hyperSIC® è il sistema informatico gestionale web-native che consente alla Pubblica Amministrazione Locale di raggiungere obiettivi organizzativi in linea con le esigenze di efficacia, efficienza e risparmio e passare quindi alla generazione 2.0, perché:



- realizzato in conformità alle moderne caratteristiche di applicazioni web ad architettura multi-tier ed operante su protocolli di comunicazione standard;
- conforme alle linee guida per l'ICT emanate dal CNIPA (ndr - oggi DigitPA);
- consente la piena e corretta INTEGRAZIONE tra gli ambienti verticali dell'organizzazione PAL: demografici, contabili, risorse umane, tributari, segretariali, tecnico ecc... grazie alla TOTALE COMPLETEZZA di funzionalità disponibili per tutte le aree e i servizi dell'organizzazione dell'Ente;
- permette la drastica **riduzione** dei costi di gestione e consulenza del CED con risparmi che superano il **50%** della spesa per questi servizi;
- semplifica le opportunità di utilizzo e/o collegamento del sistema "fuori le mura" sia in termini di interazione con altre strutture informatiche (cooperazione applicativa) che di sedi remote.
- integrato senza alcuna difficoltà con gli strumenti digitali oggi sempre più necessari per interagire con la PA ossia la firma digitale, la PEC, timbro digitale, ...