Registros Públicos Digitales:

El Tiempo y su Veracidad

J.Dávila, J.L. Morant, J.Sancho

Facultad de Informática - UPM

Intercambio de Información

Administración - Administrado

Administración

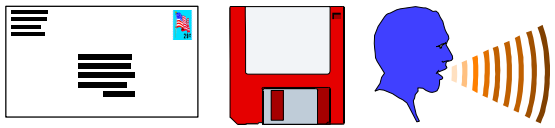
Composición de Expedientes

Datos de Identidad y Actividad

Certificaciones

Servicios de Información

Ciudadano



Datos Multimedia

Registros Públicos

Administración

Libros de Registro

Escrito o Instancia

Recibo

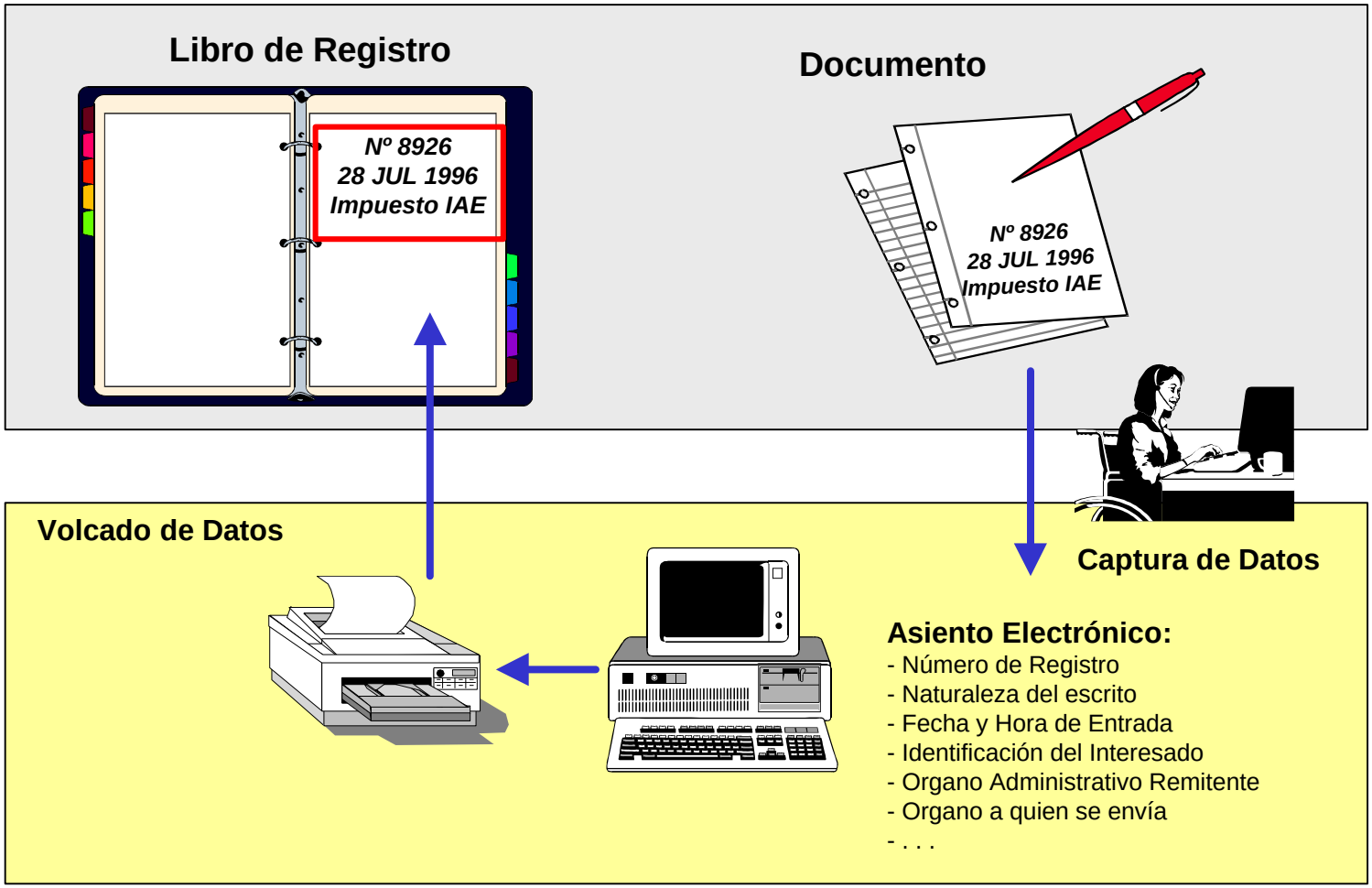
Ciudadano

28 Julio 1998

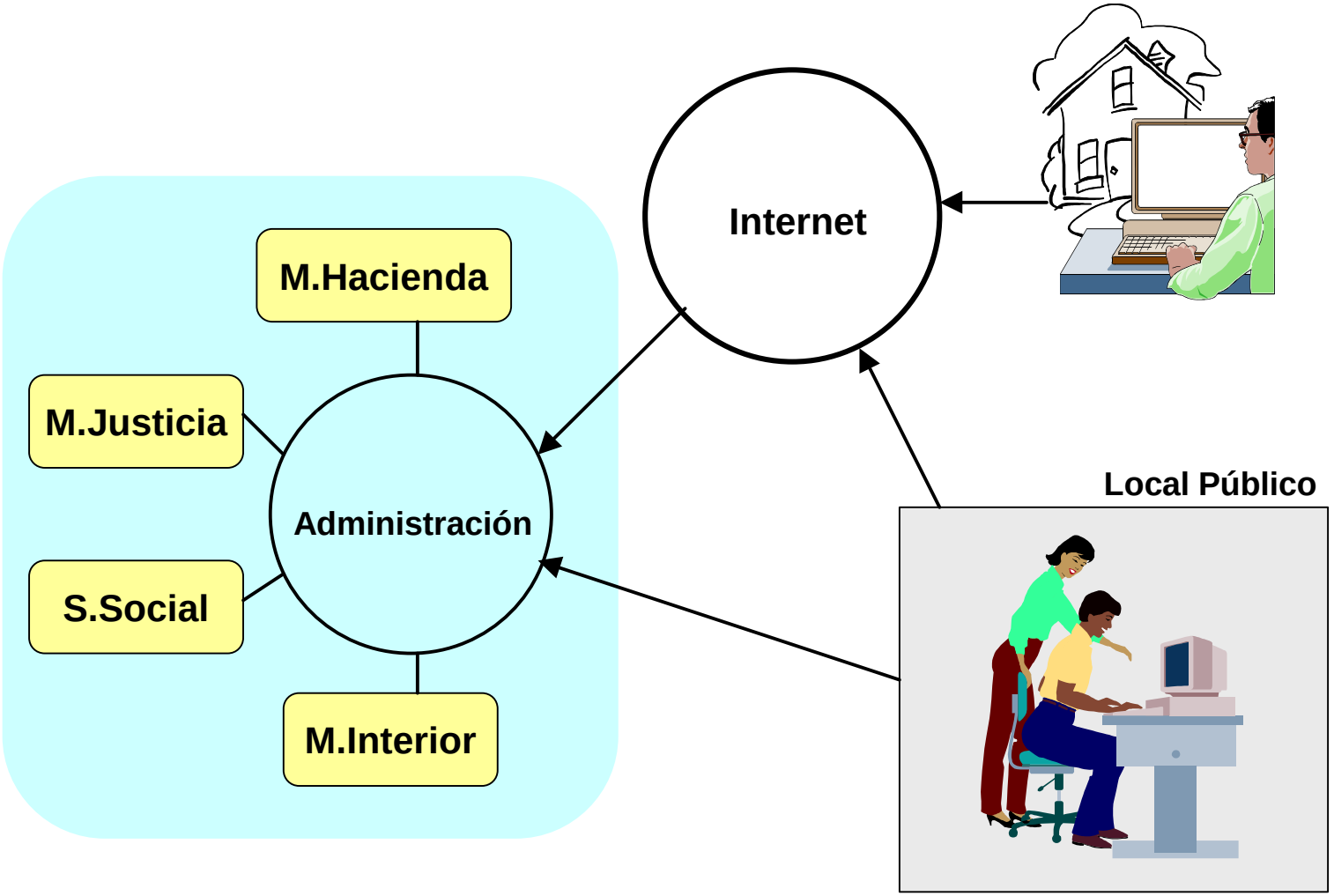
ENTRADA

nº 8926

Registros Informátizados Actuales

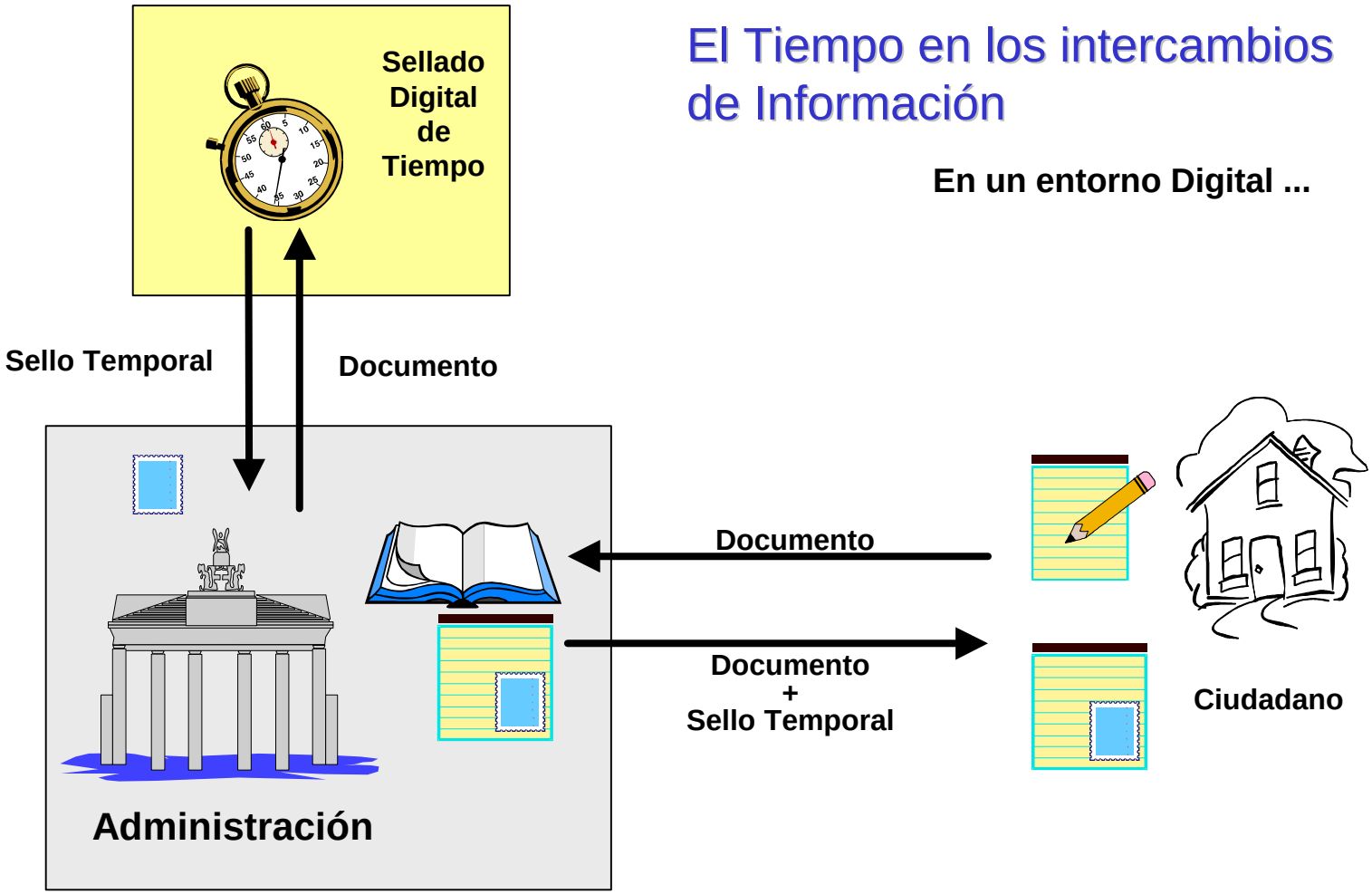


La Ventanilla Unica



El Tiempo en los intercambios de Información

En un entorno Digital ...

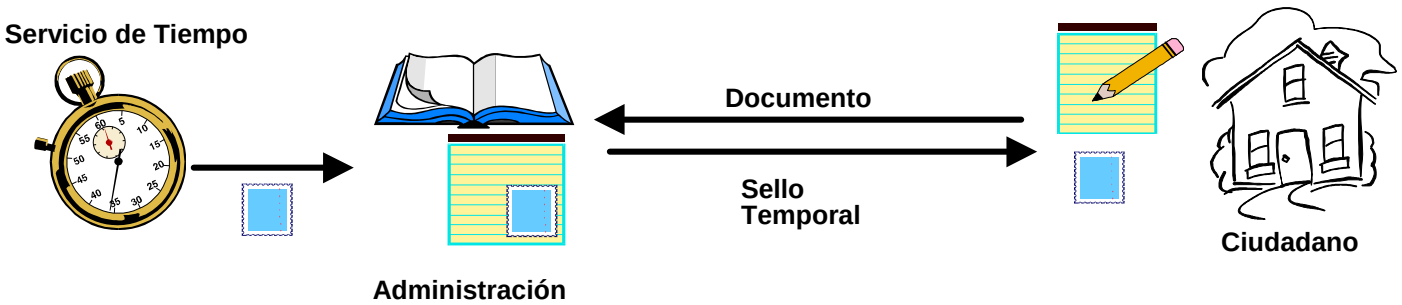


Necesidad del Sellado de Tiempo

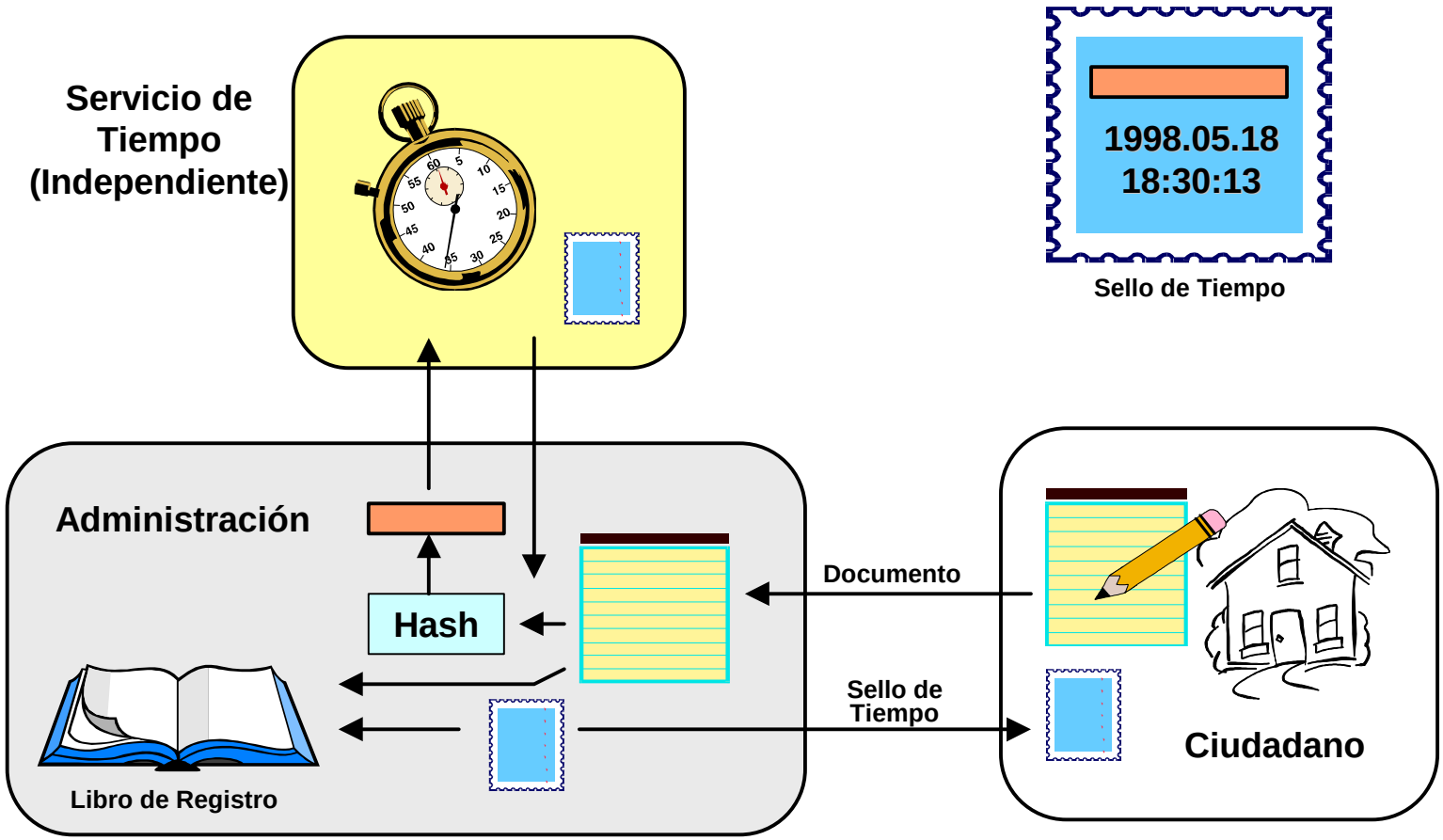
En los escenarios de Ventanilla Unica, en los que los Registros son Digitales, los documentos presentados deben matasellarse para:

- Probar la existencia del documento pretesentado en un tiempo cierto

- Impedir la manipulación, por cualquiera de las partes, del documento registrado



Sellado Digital - Función Resumen



Propiedades del Sellado Digital

- Se sellan los datos en sí y no el soporte de los mismos, de forma que no se puede cambiar ni un bit del documento sin que sea detectado por cualquiera.

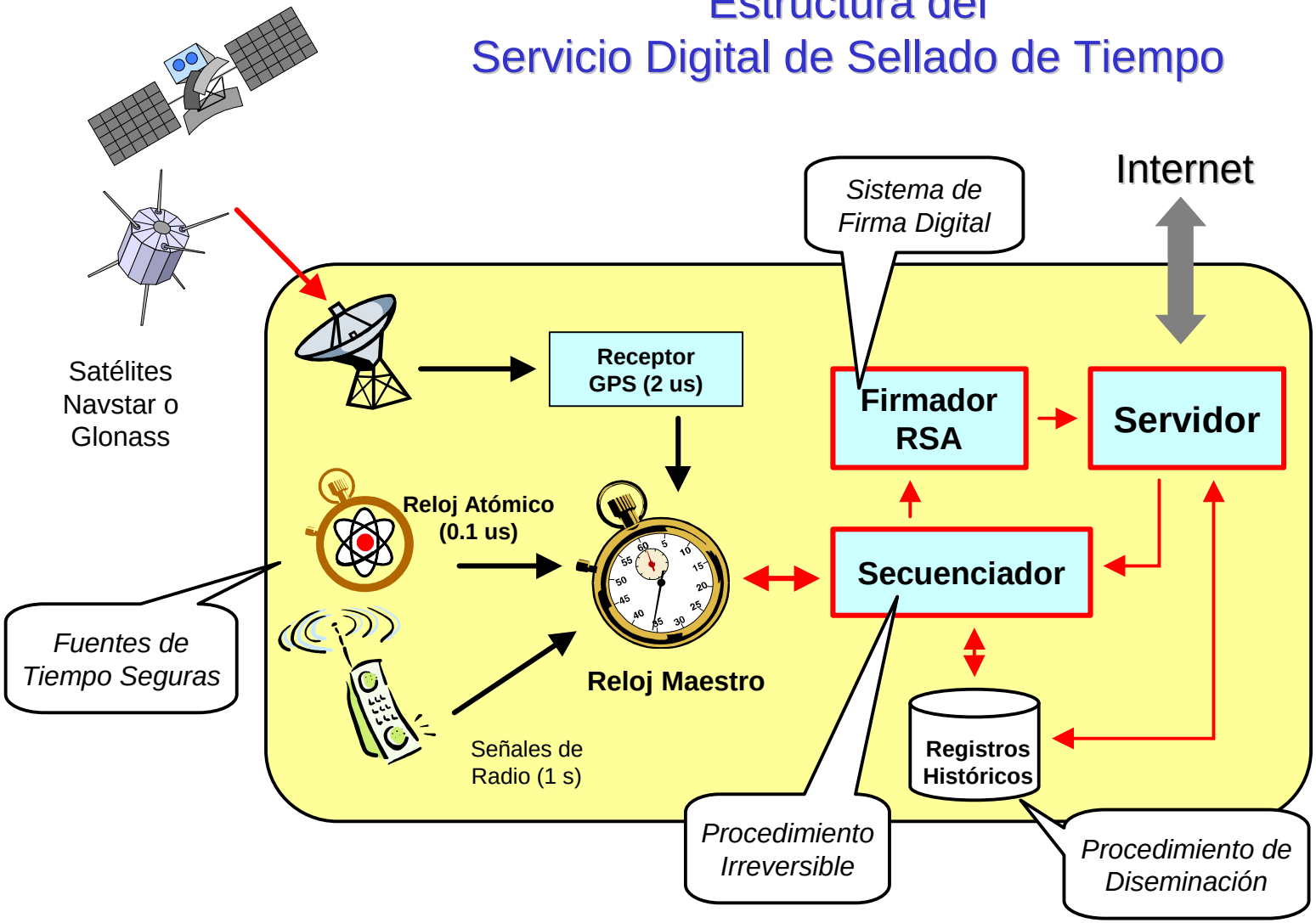
- La fecha y hora en que el Servicio de Sellado Digital de Tiempo recibe los datos relativos al documento es la actual y se obtiene de relojes seguros.

- Utilizando funciones resumen (hash) el contenido del documento no es conocido por nadie que no sea la Administración o el ciudadano, por lo que el servidor queda independiente de ambos.

- El Servicio de Tiempos es independiente de cualesquiera agentes y constituye un servicio inherentemente público.

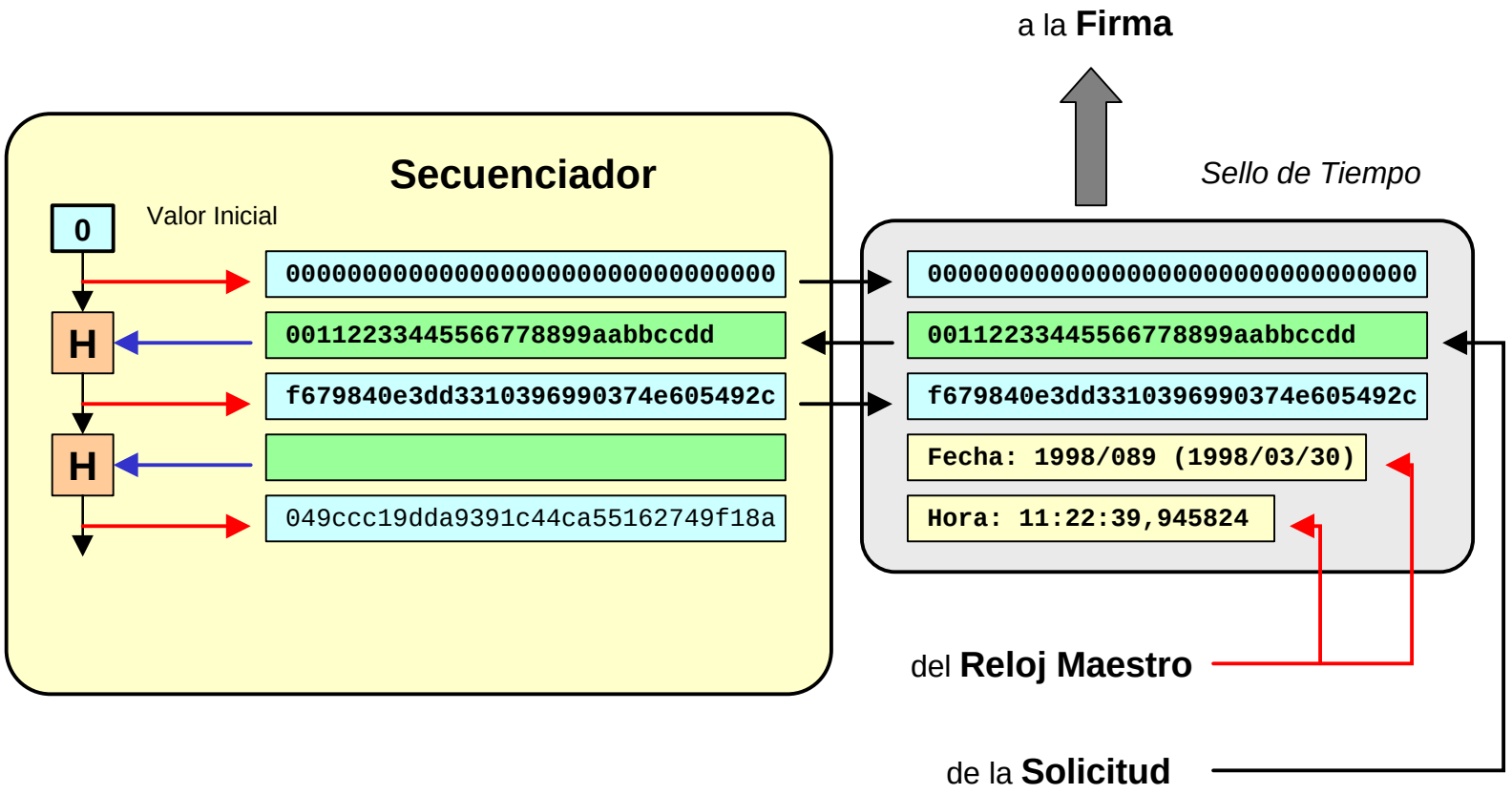
- Los Sellos de Tiempo vinculan un documento con un instante, y no són reutilizables

Estructura del
Servicio Digital de Sellado de Tiempo



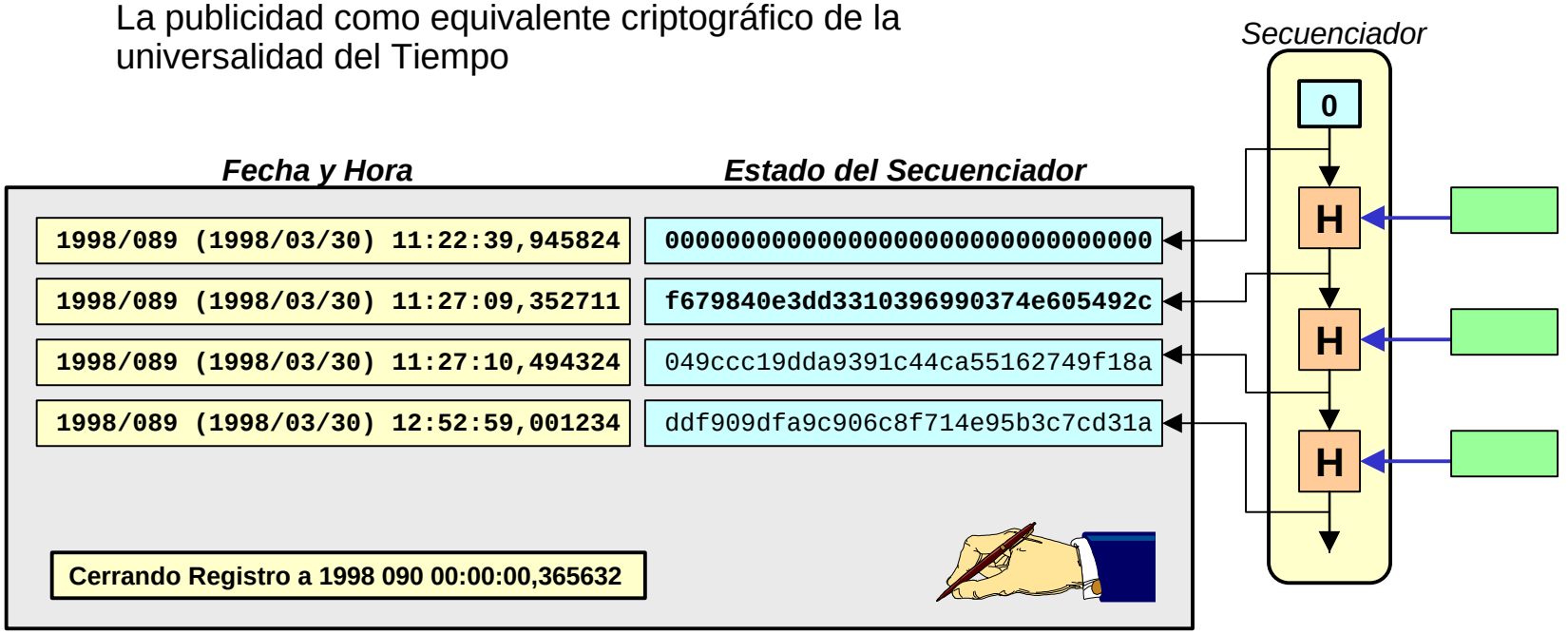
Proceso Irreversible:

Equivalente criptográfico de la irreversibilidad del Tiempo



Procedimiento de Diseminación:

La publicidad como equivalente criptográfico de la universalidad del Tiempo



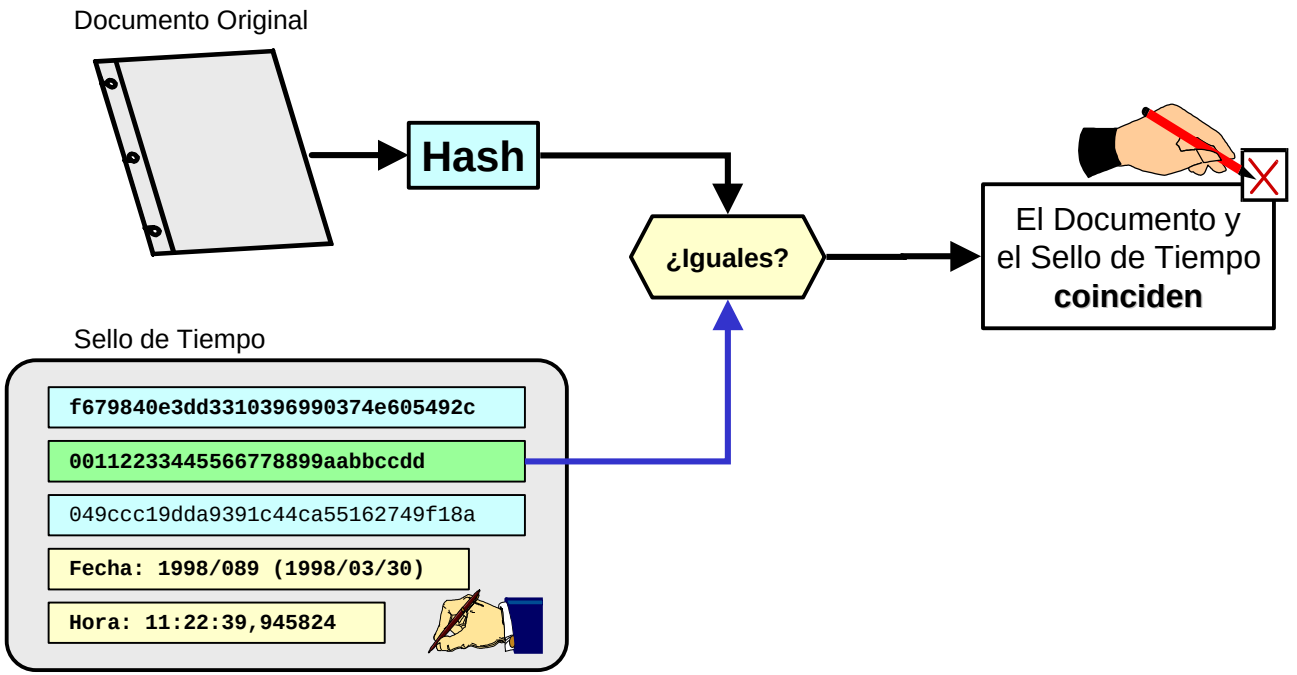
Internet

Los ficheros históricos se difundirán a través de la red manteniéndose numerosas **Copias Auténticas y Accesibles** que dan fé del correcto funcionamiento del Sevidor de Sellos Digitales de Tiempo

Verificar un Sello de Tiempo

1ª Fase

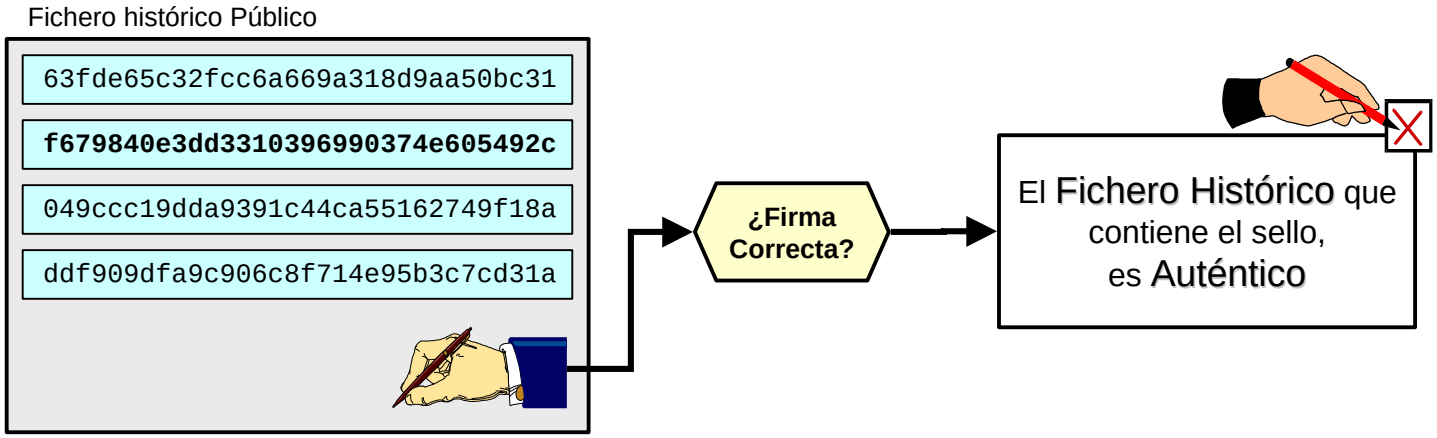
Comprobar fehacientemente que un determinado sello de tiempo está relacionado con el documento



Verificar un Sello de Tiempo ...

2ª Fase

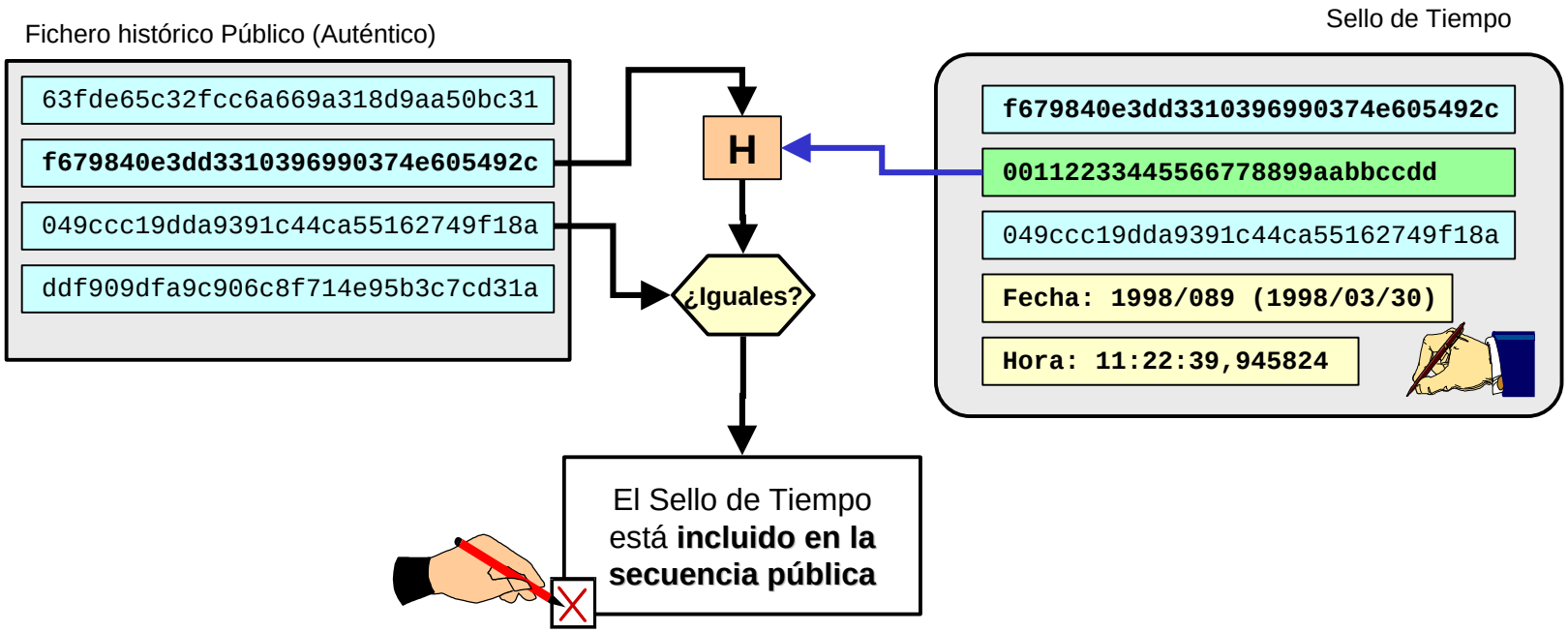
Comprobar fehacientemente que el Fichero Histórico que contiene el sello de tiempo es Auténtico



Verificar un Sello de Tiempo...

3ª Fase

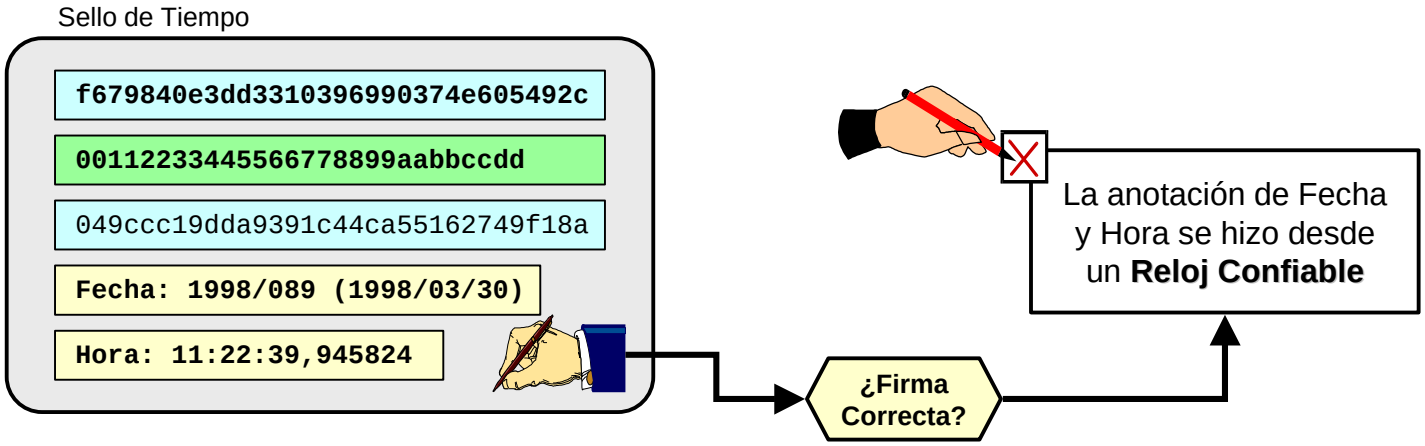
Comprobar fehacientemente que el Sello está incluido en la secuencia (auténtica) publicada por Servicio Digital de Tiempos emisor.



Verificar un Sello de Tiempo ...

3ª Fase

Comprobar la Autenticidad del Sello Digital de Tiempo asociado con el documento, pudiendo así estar seguros de que la Fecha y Hora que aparecen en él eran las que marcaban relojes seguros.



Conclusiones

- Para probar en un entorno puramente digital la existencia, en un determinado instante del tiempo, de un documento o cualquier otro tipo de objeto digital, es imprescindible disponer de Servicios Digitales de Tiempo confiables.

- Los métodos criptográfícos actuales ofrecen soluciones seguras para la prestación de servicios de Sellado Digital de Tiempo dando lugar a un nuevo tipo de Autoridad de Certificación.

- Las Pruebas Digitales de la existencia de cualquier documento en un determinado instante de tiempo sufre, en tanto que firma digital, de un vacío legal que frena cualquier iniciativa de automatización real de los procesos administrativos