

Camer*firma*

MANUAL:

COMO HACER UN SELLADO DE TIEMPO

Contenido

INTRODUCCION.....	3
SERVIDOR SELLADO DE TIEMPO: XOLIDOSIGN	6
SERVIDOR SELLADO DE TIEMPO: ADOBE READER XI Y ADOBE READER DC	11
ADOBE READER	16
SELLADO DE TIEMPO: ELEMENTOS DEL SERVICIO DE SELLADO DIGITAL.....	18
SELLADO DE TIEMPO: METODOS AUTENTIFICACION DE SELLADO	19
CONCLUSION	20

INTRODUCCION

El sellado de tiempo (time stamping) es un método para probar que un 'dato electrónico' existió en un momento determinado y además que no ha sido modificado desde entonces. Permite por ejemplo probar la existencia de un documento electrónico, su transmisión o recepción por un sistema externo, etc. Mediante la emisión de un sello de tiempo sobre un documento, se generará una evidencia, que determinará la existencia de ese documento en un instante determinado.

En el presente manual se explica cómo se realiza un sellado de tiempo de un documento. Así mismo, podremos ver gráficamente el paso a paso de la utilización de servidores que el usuario final debe usar para que su documento posea la garantía de la no alteración de los datos asociados con la firma electrónica como la fecha, hora y lugar de realización.

SELLADO DE TIEMPO: PASOS

- **Un usuario quiere obtener un sello de tiempo para un documento electrónico que él posee: Ejemplo: contratos, información de investigación, registros médicos, contenidos web, etc.**

Un sello de Tiempo se puede generar para cualquier documento electrónico, ya que, como paso previo del envío de la petición al servidor, se aplica algoritmo de hash

que toma como entrada un conjunto de bytes de cualquier tamaño, sin importar a que tipo de archivo corresponden dichos bytes.

Por tanto, se pueden generar sellos sobre documentos ofimáticos, archivos de audio, imágenes, software, trabajos creativos, etc.

Para sellar varios archivos, lo más simple es crear un fichero de texto con todos los hashes de los archivos deseados para posteriormente ejecutar sobre él un sellado de tiempo. Lógicamente se debe utilizar en la creación de ese fichero de texto un algoritmo de hash seguro, por ejemplo SHA-512.

- **Un resumen digital (técnicamente un hash) se genera para el documento en el ordenador del usuario, mediante uno de los algoritmos permitidos en la plataforma. Con el hash, el identificador de política y el identificador de la aplicación se enviará una petición a la plataforma. La estructura de petición será distinta dependiendo del protocolo que se utilice: Web-Service, TCP o HTTPS.**

Una función hash es una operación matemática que se aplica a un conjunto de datos de tamaño arbitrario, de tal manera que como resultado se obtiene una llamada de bits de tamaño fijo llamada “resumen” hash idéntico.

Es prácticamente imposible generar un documento que sea idéntico a un hash dado.

Por lo tanto, no existe limitación en el tamaño de los datos ya que estos se van a transformar en un hash de tamaño fijo antes de ser enviados al servidor. La única limitación existente puede venir del tiempo necesario aplicando la función resumen así como de límite superior que imponga el algoritmo de hash en cuanto al tamaño de la entrada de datos.

- **Este resumen forma la solicitud que se envía a la autoridad de sellado de tiempo (TSA) que generará el sello de tiempo con el hash, la fecha y hora, obtenida gracias a un cliente NTP sincronizado con una fuente de tiempo fiable, y la firma electrónica.**

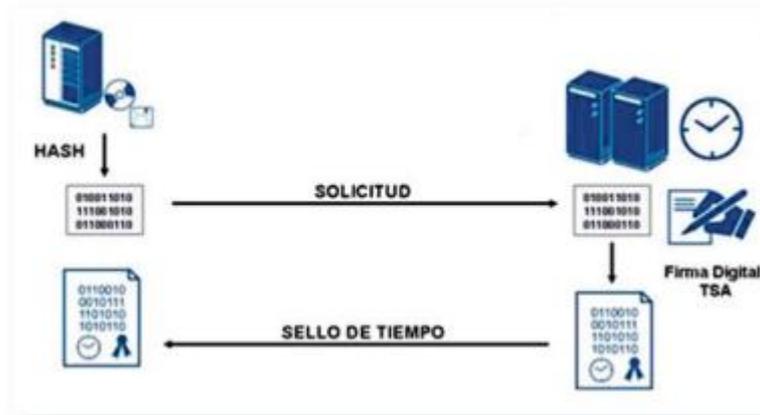
La autoridad de Sellado (Time Stamp Authority) es quien ofrece el servicio de sellado. Su finalidad es comprobar el correcto formato de las peticiones y generar un sello de tiempo bien formado.

Una TSA debe:

- Utilizar una fuente fiable.
- Incluir un valor de tiempo fiable en cada sello.
- Incluir un entero único en cada sello.
- Incluir en cada sello un identificador que indique la política de seguridad con la que el sello ha sido creado.
- Firmar cada sello con una clave generada exclusivamente para este propósito.

En el proceso de generación de los sellos intervienen diversos certificados digitales y claves de firma, ya sea para generar el sello o securizar el canal de comunicación entre las distintas entidades. La validez de estos certificados y la caducidad de los mismos se comprueba a través de una plataforma de firma electrónica.

- **El sello de tiempo se envía de vuelta al usuario, al igual que la petición se podrá enviar mediante protocolos diferentes, TCP, Web Service o HTTPS.**

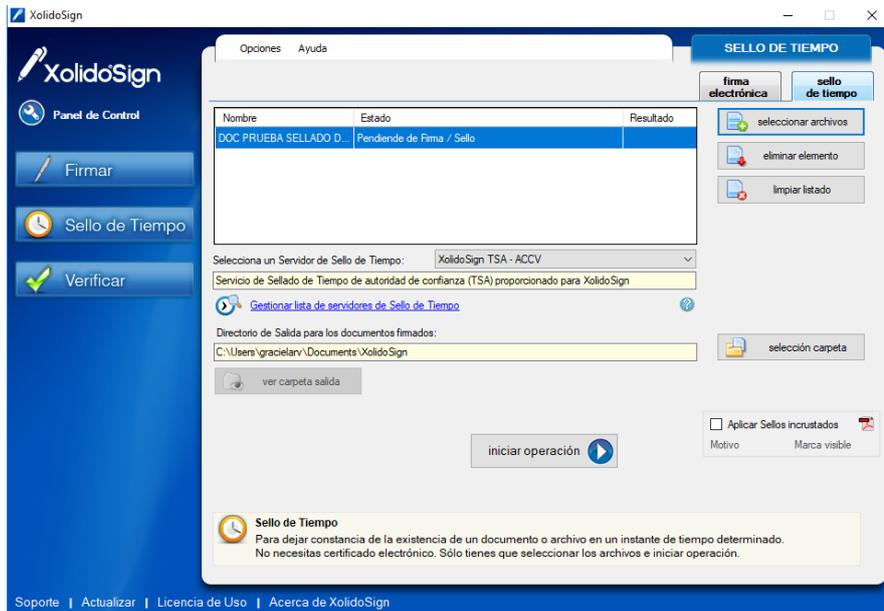


- La TSA mantiene un registro de los sellos emitidos para su futura verificación.

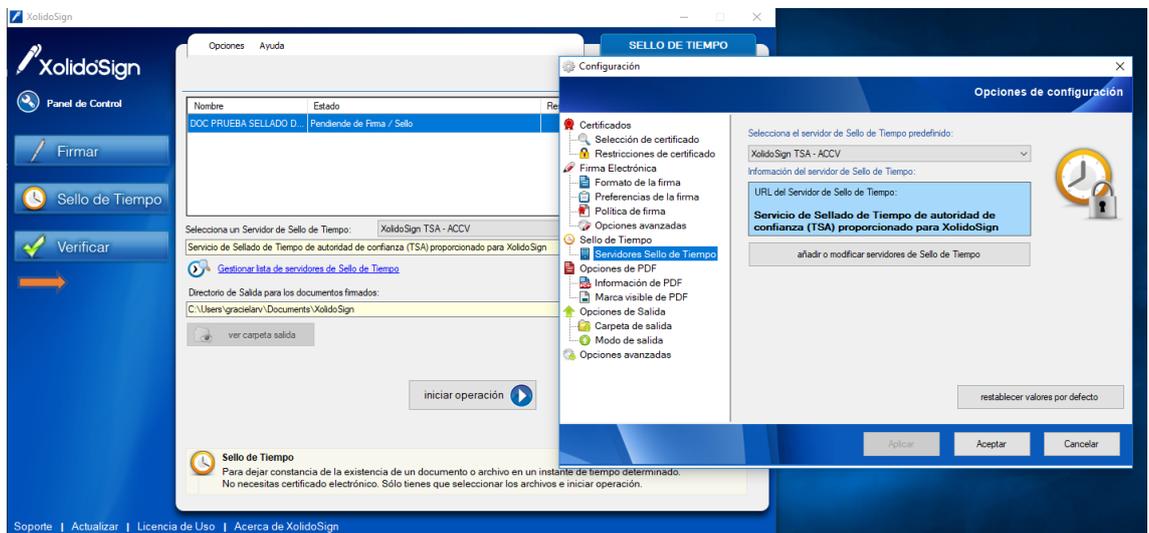
SELLADO DE TIEMPO: SERVIDORES HABITUALES

SERVIDOR SELLADO DE TIEMPO: XOLIDOSIGN

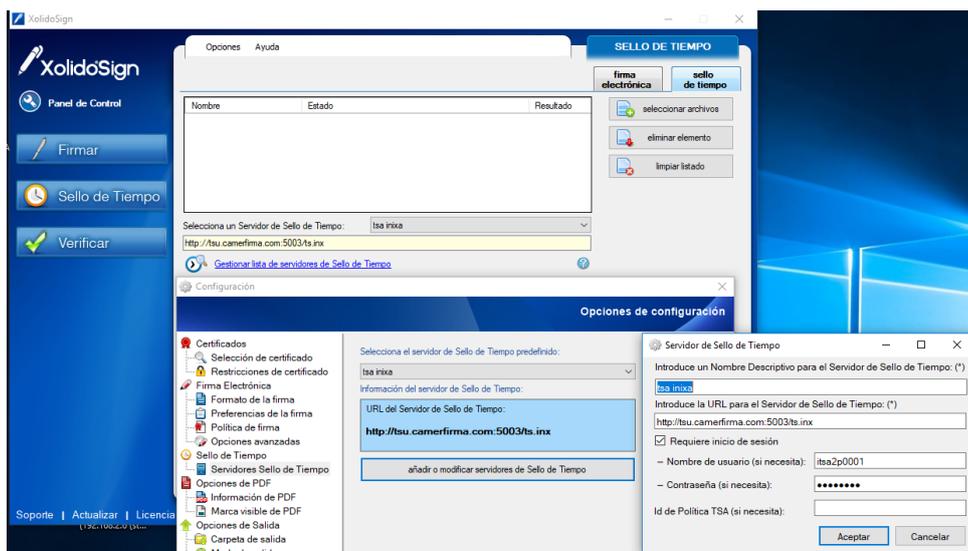
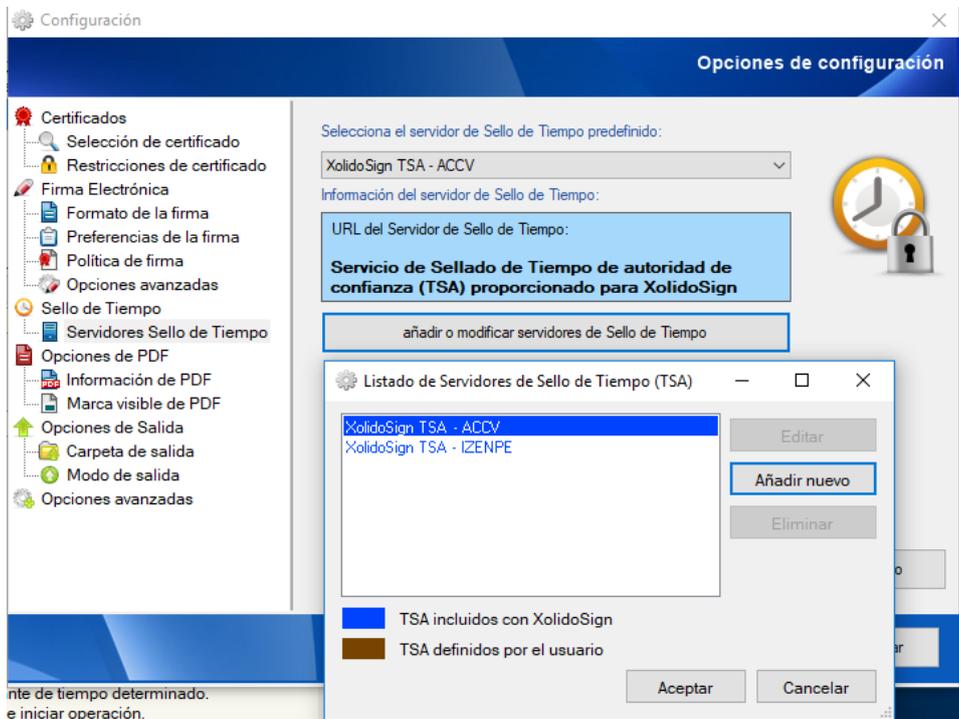
Dentro de esta aplicación, escoger el archivo.



Hacer click en [Gestionar Lista de Servidores de Sello de Tiempo](#)

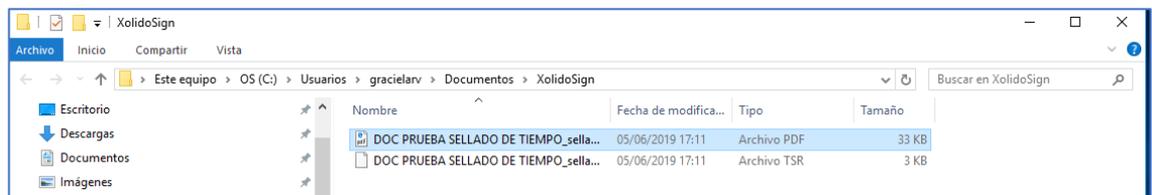
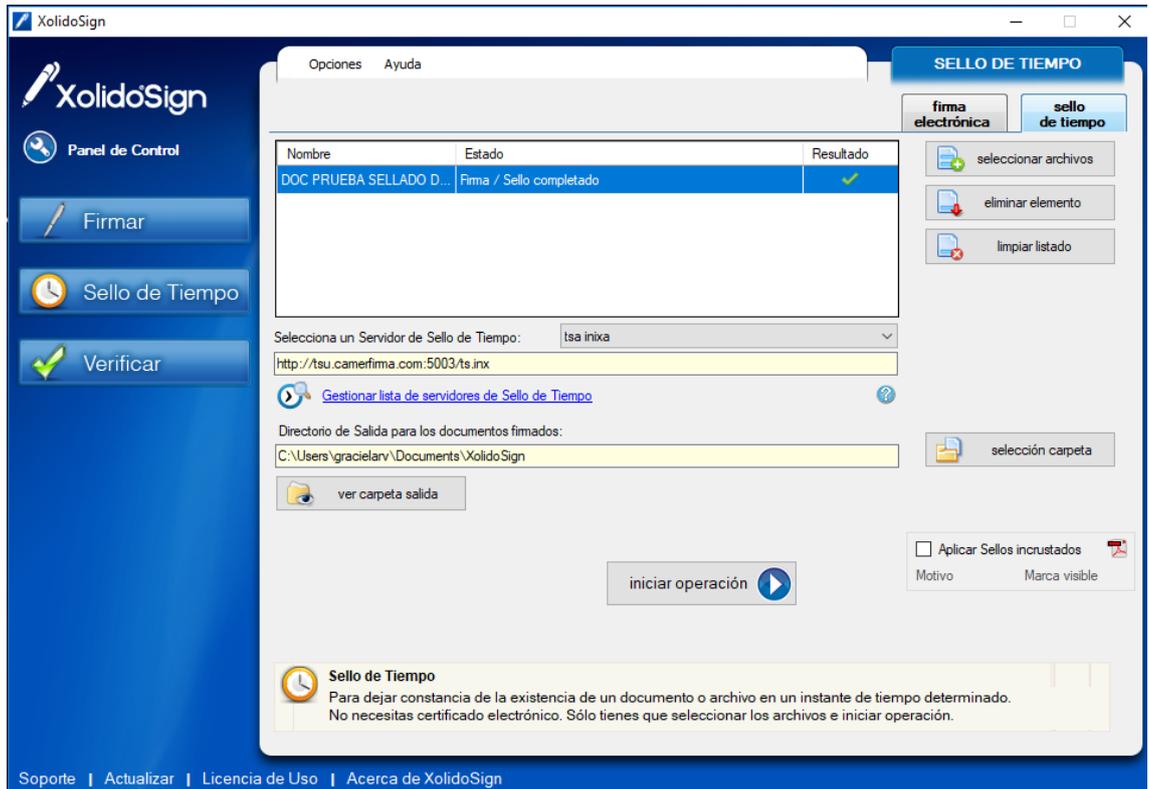


Hacer click en añadir nuevo/ ingresar los datos que nos piden: URL, usuario y contraseña, también nos permite personalizar dándole un nombre: en este caso “camerfirma”

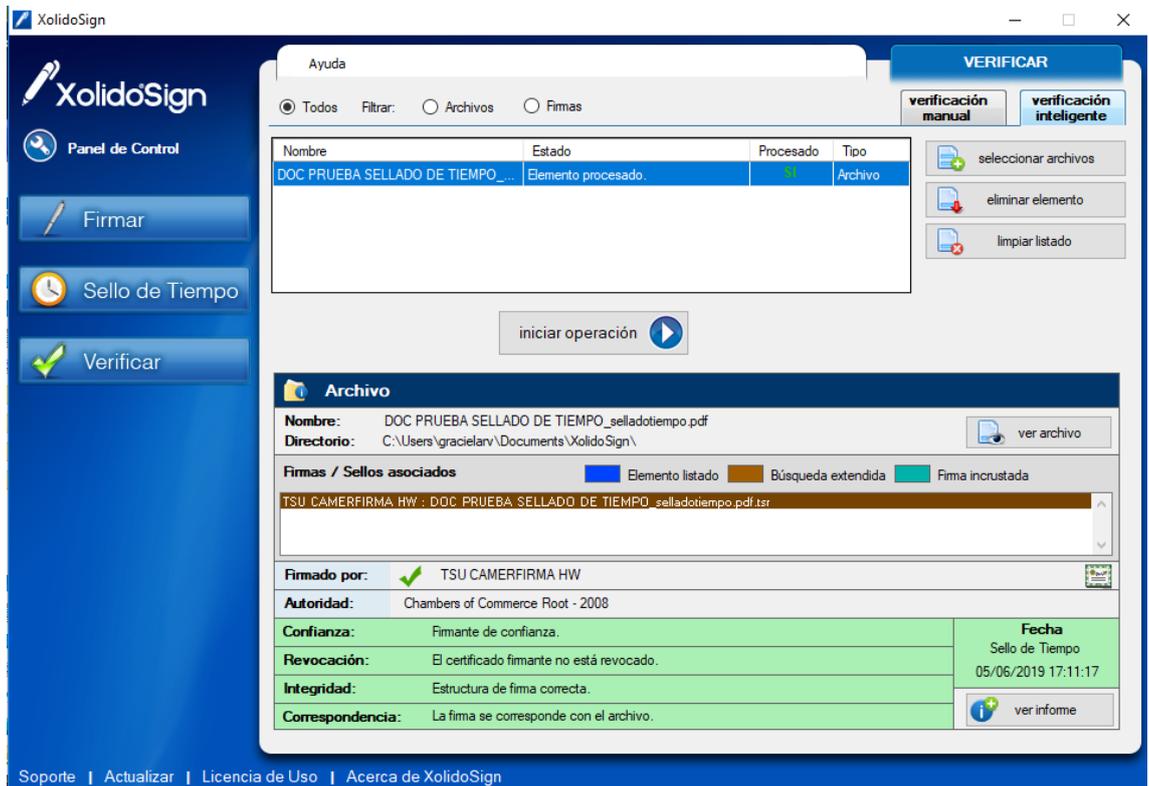
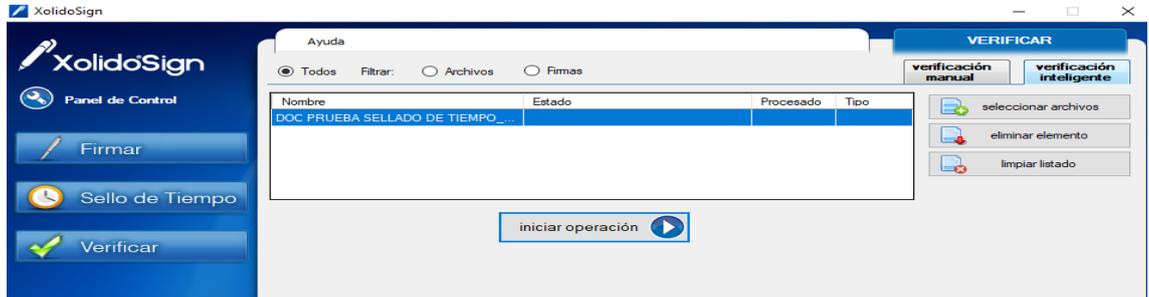


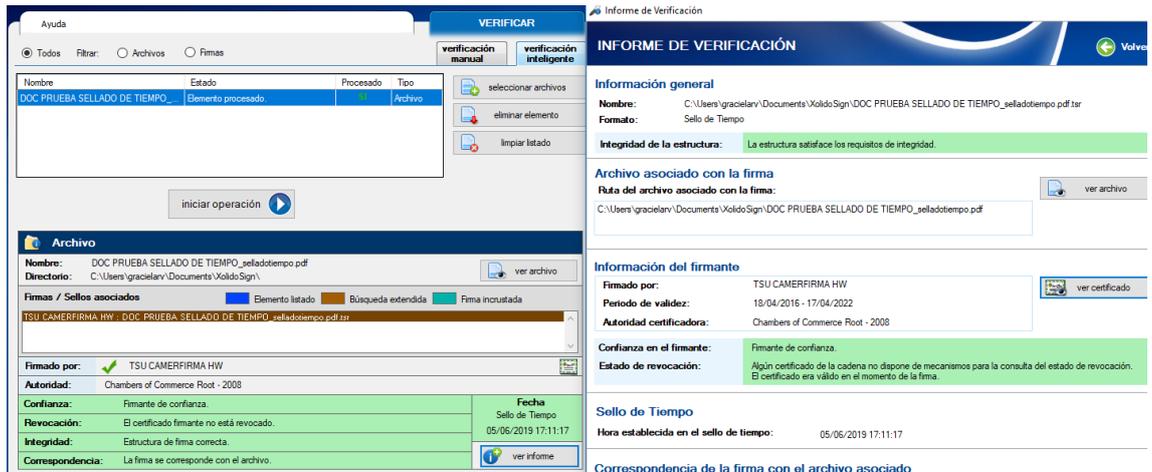
Ahora ya podemos “iniciar operación”. En la casilla “**Resultado**” se mostrará un check verde al lateral del archivo.

Podremos ver el archivo en “ver carpeta salida”



Podemos verificar si se ha realizado correctamente en la pantalla de inicio de la aplicación, hacer click en la tercera opción: **Verificar/ seleccionar archivo/ iniciar operación/ Ver archivo**





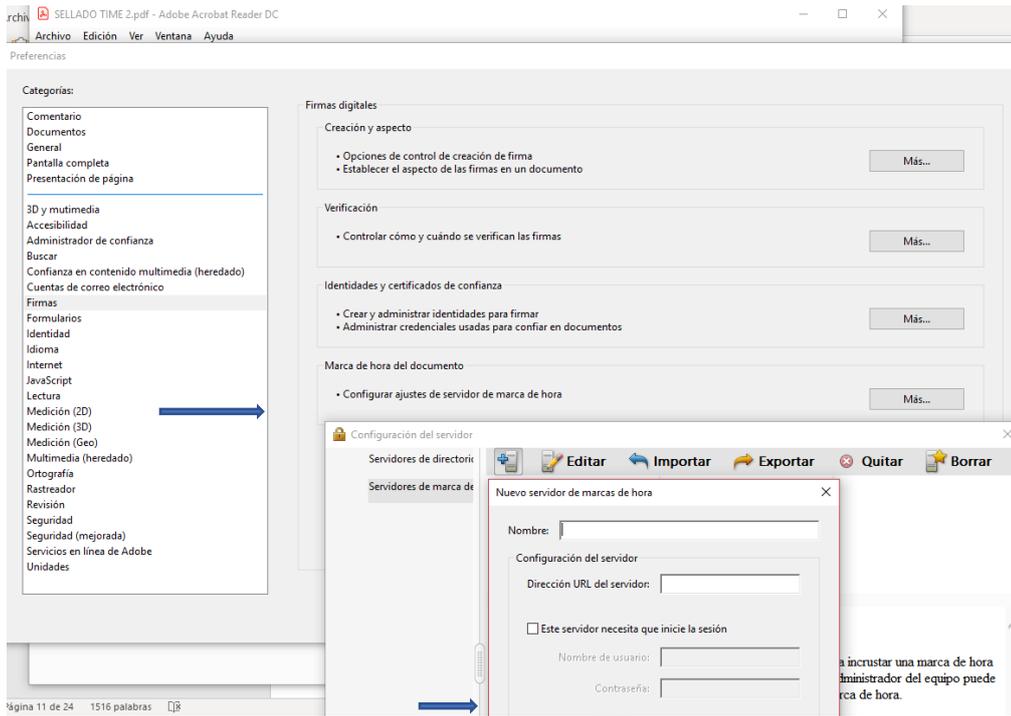
The screenshot displays the 'Informe de Verificación' (Verification Report) for a document titled 'DOC PRUEBA SELLADO DE TIEMPO'. The interface is divided into several sections:

- VERIFICAR:** Includes options for 'verificación manual' and 'verificación inteligente', and buttons for 'seleccionar archivos', 'eliminar elemento', and 'limpiar listado'.
- Archivo:** Shows the document name 'DOC PRUEBA SELLADO DE TIEMPO_selladotempo.pdf' and its directory path. It also lists associated certificates and the signing authority 'TSU CAMERFIRMA HW'.
- Informe de Verificación:**
 - Información general:** Name: C:\Users\graciela\Documents\ValidoSign\DOC PRUEBA SELLADO DE TIEMPO_selladotempo.pdf; Formato: Sello de Tiempo.
 - Integridad de la estructura:** La estructura satisface los requisitos de integridad.
 - Archivo asociado con la firma:** Ruta del archivo asociado con la firma: C:\Users\graciela\Documents\ValidoSign\DOC PRUEBA SELLADO DE TIEMPO_selladotempo.pdf.
 - Información del firmante:** Firmado por: TSU CAMERFIRMA HW; Período de validez: 18/04/2016 - 17/04/2022; Autoridad certificadora: Chambers of Commerce Root - 2008.
 - Confianza en el firmante:** Firmante de confianza.
 - Estado de revocación:** Algunos certificados de la cadena no dispone de mecanismos para la consulta del estado de revocación. El certificado era válido en el momento de la firma.
 - Sello de Tiempo:** Hora establecida en el sello de tiempo: 05/06/2019 17:11:17.
 - Correspondencia de la firma con el archivo asociado:** (Section header visible)
- Summary Table:**

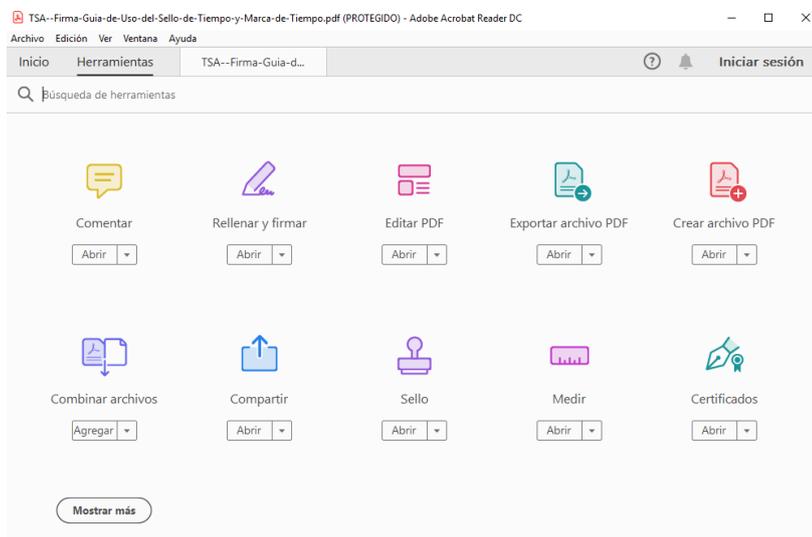
Firmado por:	TSU CAMERFIRMA HW
Autoridad:	Chambers of Commerce Root - 2008
Confianza:	Firmante de confianza.
Revocación:	El certificado firmante no está revocado.
Integridad:	Estructura de firma correcta.
Correspondencia:	La firma se corresponde con el archivo.

SERVIDOR SELLADO DE TIEMPO: ADOBE READER XI Y ADOBE READER DC

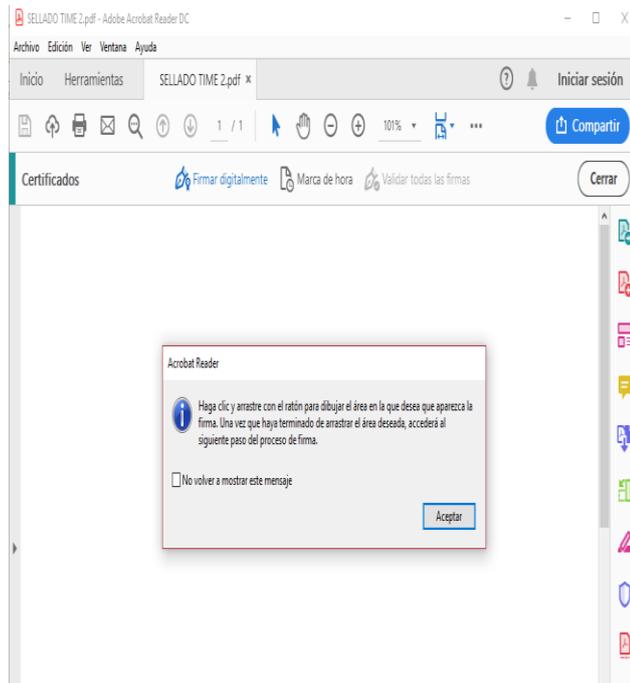
Ingresamos al documento: Edición/Preferencias/ Firmas/ Marca de hora del documento: ingresamos los datos de nombre/URL y marcamos la casilla que habilita introducir el usuario y contraseña



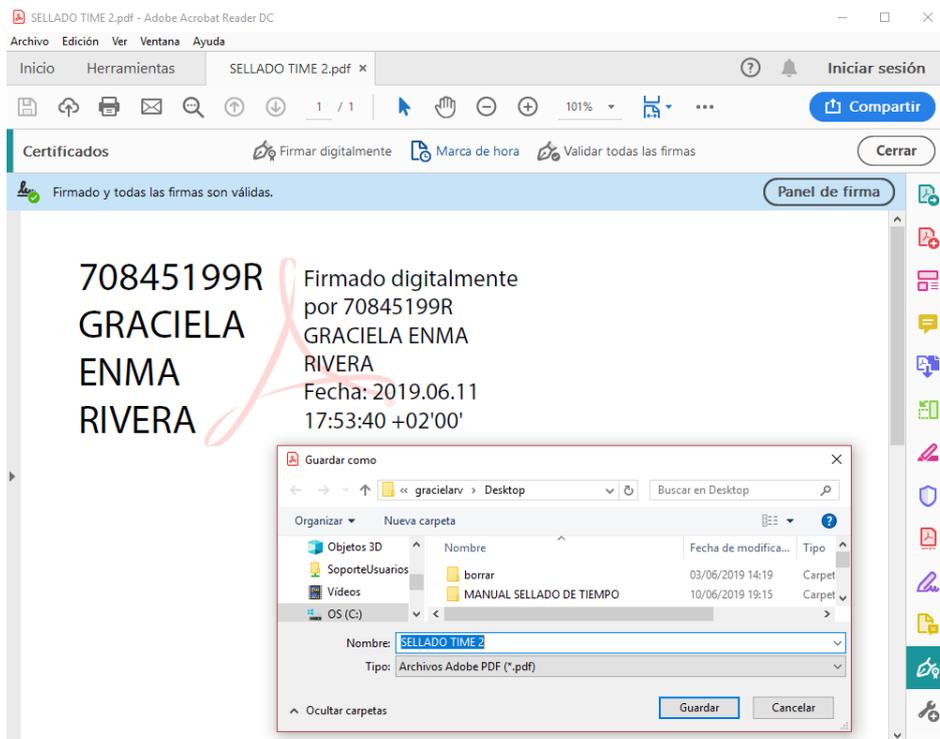
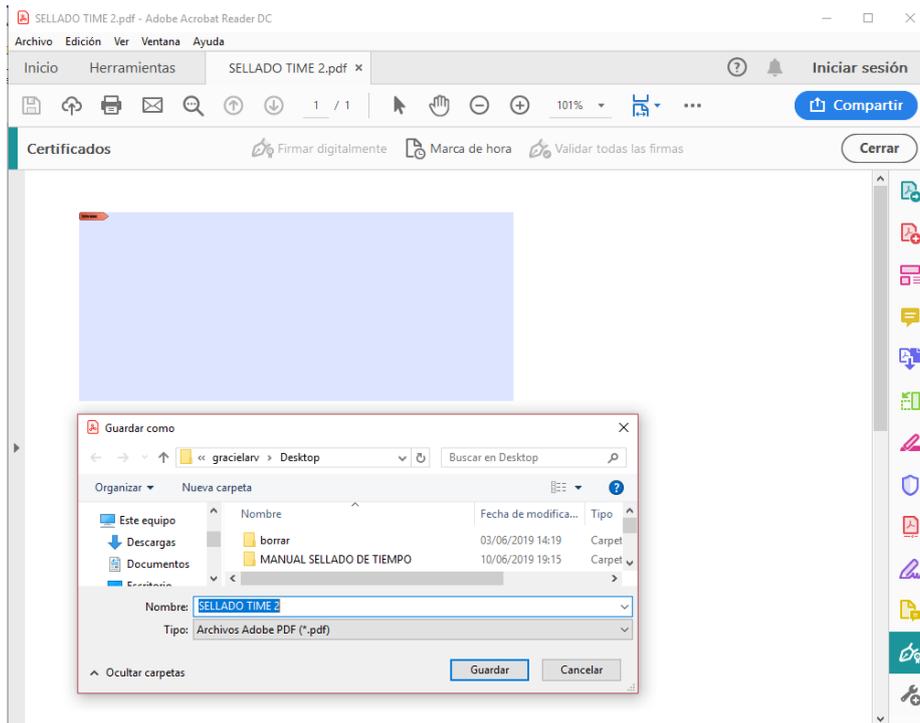
En el documento: Herramientas/ Certificados/



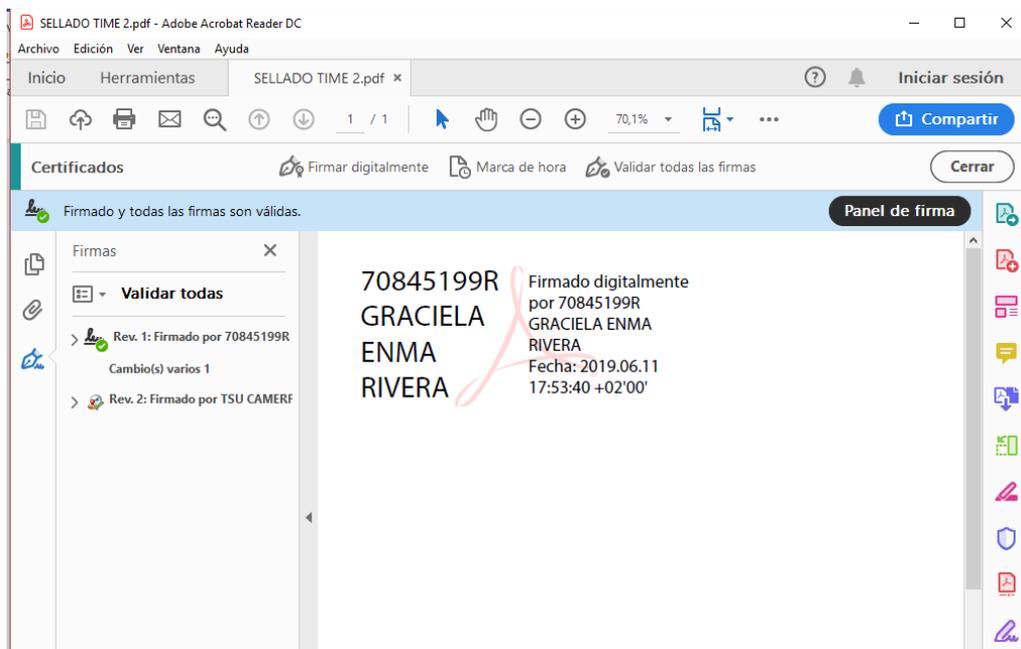
Arrastrar el cursor y señalar donde firmar

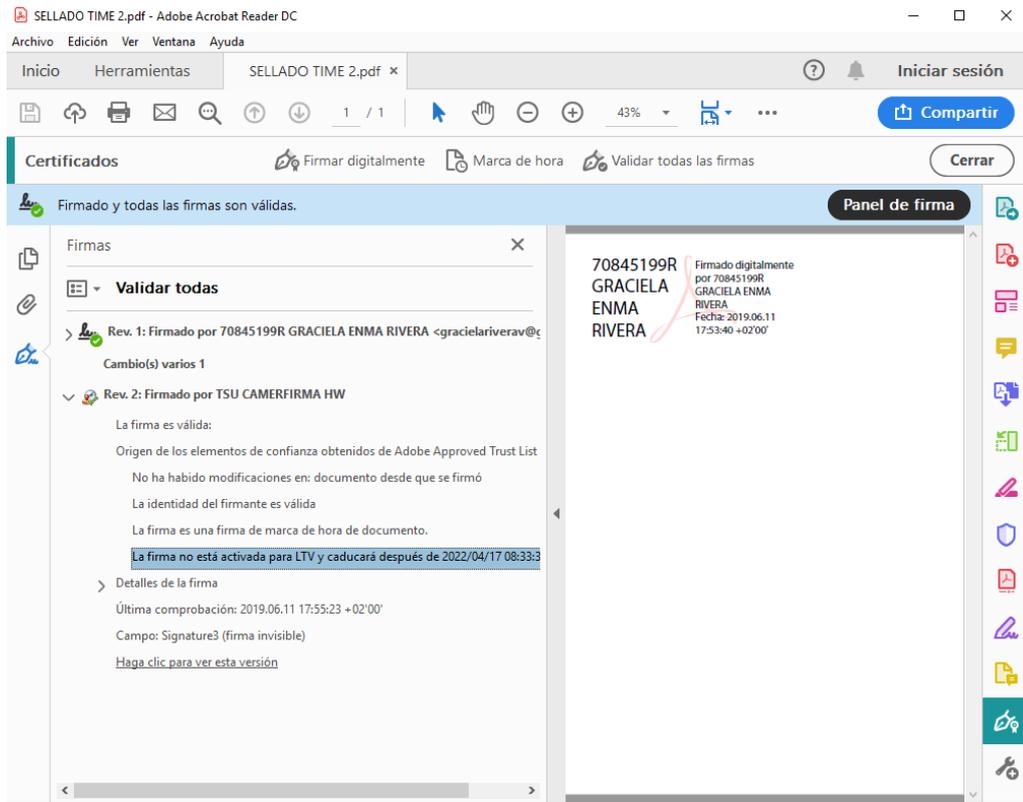


Se guarda el documento (puede reemplazar el anterior)

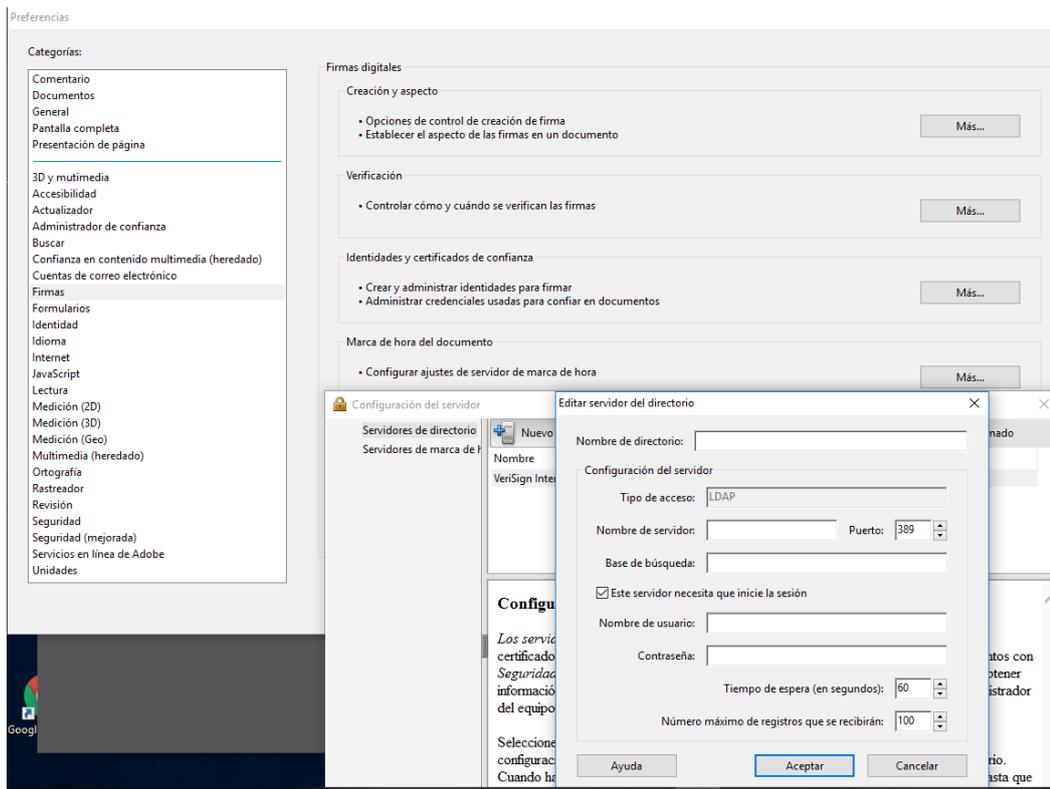
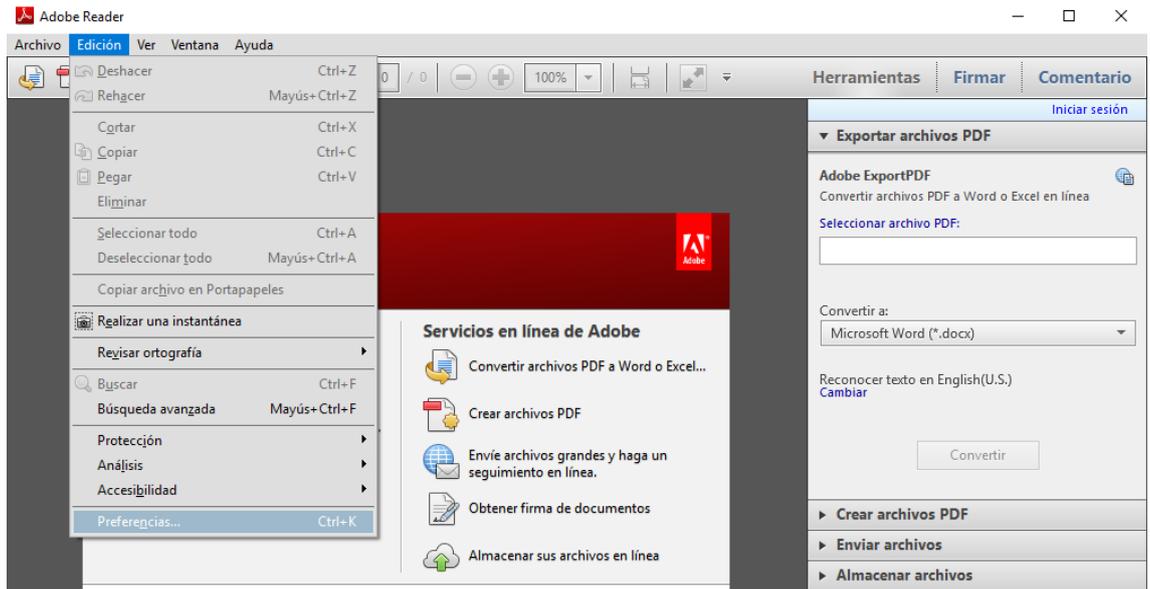


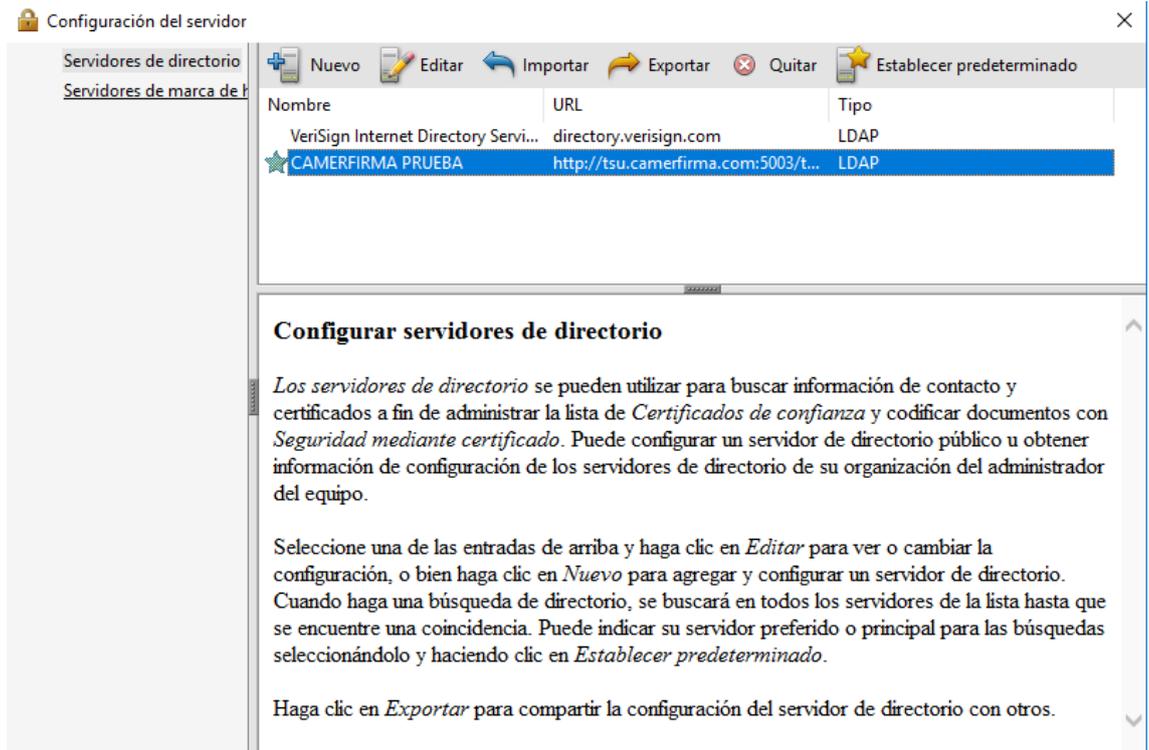
Panel de Firma





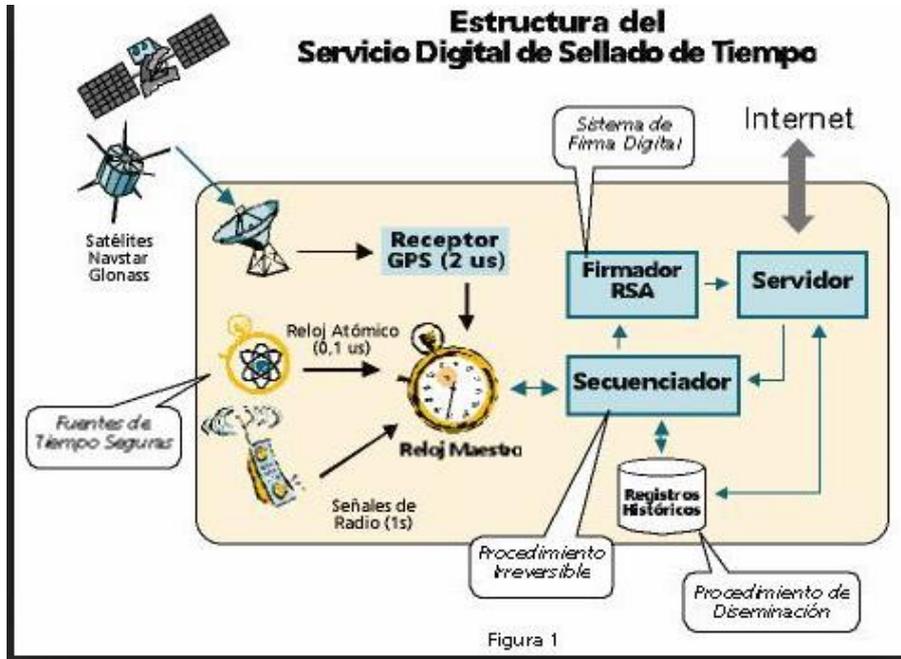
ADOBE READER





SELLADO DE TIEMPO: ELEMENTOS DEL SERVICIO DE SELLADO DIGITAL





SELLADO DE TIEMPO: METODOS AUTENTICACION DE SELLADO

Detalle de TSU de Inixa. - cumplen con los estándares:

- RFC 3161
- RFC 3628

Actualmente Camertifirma dispone el servicio de Usuario/Contraseña, existen diferentes métodos de autenticación, tales como:

Autenticación con Certificado. -

NOMBRE DE PERFIL	DE	URL	CERTIFICADO	OBSERVACIONES
Camertifirma		https://tsu.camertifirma.com:5001	CN: TSU CAMERFIRMA	En producción Cas reconocidas:

		HW O= AC CAMERFIRMA S.A C= ES Sha1	Camerfirma Corporate Server- 2009
--	--	--	---

Autenticación con Certificado. –

NOMBRE DE PERFIL	URL	CERTIFICADO	OBSERVACIONES
Filtrado por IP (Antigua Endesa)	https://tsu.camerfirma.com:15001	CN: TSU CAMERFIRMA HW - 15001 O= AC CAMERFIRMA S.A C= ES Sha256	En producción

CONCLUSION

El sellado de tiempo amplía las ventajas de la firma electrónica sobre las firmas realizadas en papel, puesto que les confiere **seguridad jurídica**.

En el caso de las firmas en papel es imposible deducir la hora o el lugar en el que se realizó la firma. En cambio, las firmas electrónicas proporcionan esta evidencia, con todas las garantías de inalterabilidad que les da el sellado de tiempo.

Con lo cual, en caso de disputa acerca del momento en el que un contrato entró en vigor, por poner un ejemplo, quienes dispongan de un acuerdo firmado electrónicamente con nuestra firma electrónica avanzada tendrán en su poder la capacidad de demostrar de forma fehaciente quién, cuándo y dónde se firmó ese contrato.

Este último factor supone una de las grandes ventajas de la firma electrónica: no sólo sustituye a la firma manuscrita, sino que además ofrece **validez jurídica** a todas las partes que participan en la firma de un contrato.

Es por eso que el sello de tiempo no puede ser proporcionado por una de las partes involucradas en el proceso de firma, ya que entonces las garantías de integridad de la firma y de los datos asociados no serían fiables.

Un sellado de tiempo debe de ser aportado un tercero de confianza, que se conoce como Autoridad de Sellado de Tiempo.