



#CyberCamp18

La autenticación con certificados en las Sedes Electrónicas

El sector público en peligro





Índice

- 1. Las Sedes Electrónicas del Sector Público y la Identificación del Ciudadano en ellas.**
- 2. Autenticación por certificado en aplicaciones web.**
- 3. Despropósitos con certificado en aplicaciones web.**
- 4. ¿Qué estoy haciendo mal?**
- 5. *Phishing* para obtener firmas electrónicas.**





Presentación

■ Tomás García-Merás Capote

- Consultor de Sector Público especializado en Administración Electrónica.
 - Autor de sistemas de firma electrónica: Cliente @firma, AutoFirma, FRe, etc.
 - Consultor para numerosas administraciones públicas:
 - Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, Ministerio del Interior, Senado de España, Fábrica Nacional de Moneda y Timbre, CIEMAT, Metro de Madrid, etc.
- Gerente de Sector Público en la empresa atSistemas.
- Miembro de los grupos de trabajo de Blockchain NWC10Lab (<https://www.nwc10lab.com/>) y BAES Blockchain Labs (Universidad de Alicante, <https://baes.iei.ua.es/>).





Presentación

■ Tomás García-Merás Capote

- ¡Ávido colaborador de MAME! (preservación y emulación de máquinas antiguas: <https://github.com/mamedev/mame>).
- Si dispones o tienes acceso a placas arcade, hardware antiguo (de cualquier tipo...), cartuchos extraños de videojuegos, máquinas olvidadas... ¡Llámame!





#CyberCamp18

Las Sedes Electrónicas del Sector Público y la Identificación del Ciudadano en ellas





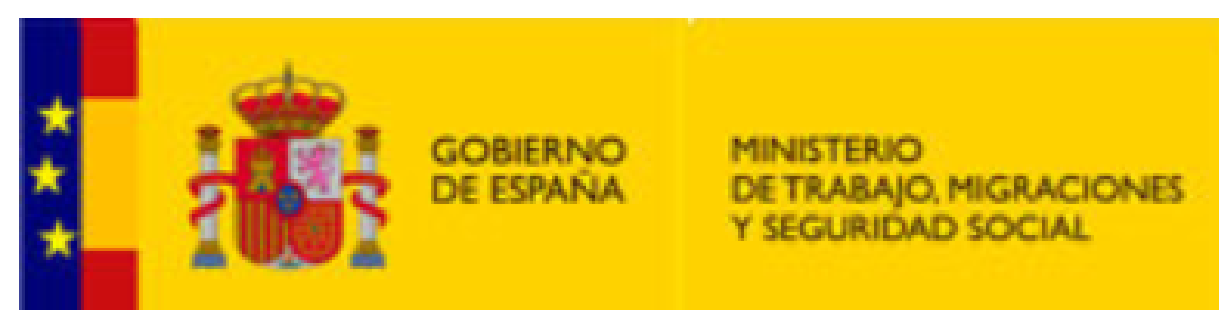
¿Qué es una sede electrónica?

- La sede electrónica no es una web normal, es el equivalente electrónico a la vieja “ventanilla” en la que los ciudadanos se relacionan con las administraciones públicas.
- Están fuertemente reguladas por Ley (Leyes 39 y 40 de 2015, de procedimiento administrativo y régimen jurídico de las administraciones).
- Deben permitir a los ciudadanos identificarse mediante certificados electrónicos.





Ejemplo de Sede Electrónica: Seguridad Social



Seguridad Social
SedeElectrónica

[Sugerencias y quejas](#)

[Preguntas frecuentes](#)

▼ **Castellano**



[Ciudadanos](#)

[Empresas](#)

[Administraciones y Mutuas](#)



Informes y Certificados

Variación de Datos

Pensiones

Incapacidad

Familia

[Inicio](#) / [Ciudadanos](#)

Informes y Certificados

Asistencia sanitaria: Consulta del derecho y emisión del documento acreditativo del derecho



Certificado Provisional Sustitutorio (CPS)





#CyberCamp18

Autenticación por certificado en aplicaciones web





¿Cómo se implementa (correctamente) la autenticación con certificado en una aplicación web?

- **Prácticamente, solo hay dos maneras de implementar bien la autenticación con certificado (que son la misma):**
 - Implementar autenticación con SSL cliente (bajo HTTPS).
 - Delegar la autenticación en un proveedor de identidad... Que implemente autenticación por SSL cliente (bajo HTTPS).
 - En el sector público se utiliza el proveedor de identidad CI@ve (<https://administracionelectronica.gob.es/ctt/clave>).





Ejemplo de autenticación en la sede de la Seguridad Social

Informe de bases y cuotas ingresadas

Para acceder a este servicio compruebe los **requisitos técnicos** necesarios.

Acceso directo a trámites:

-  Certificado digital
-  Usuario + Contraseña
-  Cl@ve
-  Sin certificado
-  Vía SMS

A través de este servicio puede obtener, imprimir y/o consultar on-line un informe en el que se recogen las bases de cotización y las cuotas de Seguridad Social ingresadas desde 1999 en los Regímenes y/o Sistemas Especiales. Si accede sin certificado digital el informe le será remitido por correo postal.

Más información 





Ejemplo de autenticación en la sede de la Seguridad Social

GOBIERNO DE ESPAÑA

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

¿Qué es Cl@ve?

Ayuda

Elija el método de identificación

Si no transcurren más de 60 minutos entre autenticaciones y llamadas a Cl@ve, se le autenticará automáticamente de forma transparente.

- DNle / Certificado electrónico**
Acceder >
- Cl@ve PIN**
Acceder >
Para usarlo es necesario [registrarse](#)
- Cl@ve permanente**
Acceder >
Para usarlo es necesario [registrarse](#)
- Ciudadanos UE**





Implementación de la autenticación SSL cliente (I)

- **Únicamente es necesario configurar en el servidor web:**
 - La obligatoriedad de que el usuario se identifique con su certificado.
 - Qué certificados aceptamos (de qué emisores).
 - Los medios de validación del certificado (OCSP, CRL...).
- **La aplicación recibe entonces el certificado con el que el usuario se ha identificado.**
 - El servidor web ha comprobado que el usuario dispone de la clave privada, que el certificado ha sido emitido por una autoridad soportada y que es válido (está dentro de su fecha de validez y no ha sido revocado).





Implementación de la autenticación SSL cliente (II)

- Una vez configurado el servidor web, nuestra aplicación puede entonces usar los datos del certificado para identificar al usuario (por nombre, DNI, clave pública...).

```
@Override
protected void service(final HttpServletRequest request, final HttpServletResponse response) {
    final X509Certificate[] certs =
        (X509Certificate[]) request.getAttribute("javax.servlet.request.X509Certificate");
    try (
        final PrintWriter out = response.getWriter();
    ) {
        if (null != certs && certs.length > 0) {
            out.write("<h1>Autenticado con certificado: '" + certs[0] + "'</h1>");
        }
        else {
            out.write("<h1>Autenticado sin certificado</h1>"); //$NON-NLS-1$
        }
    }
}
```





Despropósitos con certificado en aplicaciones web gracias a la aplicación AutoFirma





La aplicación AutoFirma (I)

AutoFirma v1.6.4

Archivo Herramientas Ayuda

Bienvenido a AutoFirma

En esta pantalla puede firmar electrónicamente ficheros que se encuentren en su disco duro. Cuando firma electrónicamente un fichero pueden incorporarse a este ciertos datos personales, entre los que pueden encontrarse su número de DNI, su nombre y apellidos o incluso información sobre su situación laboral si utiliza un certificado profesional. Consulte las políticas de seguridad y protección de datos de los receptores de los ficheros firmados antes de enviarlos o distribuirlos. A partir de este punto, no inserte o extraiga ninguna tarjeta inteligente o dispositivo criptográfico USB.

Importante: No inserte ni retire tarjetas de ninguno de los lectores de tarjetas inteligentes hasta finalizar la ejecución de este programa.

[Seleccionar ficheros a firmar](#)



C:\Users\tgarciameras\Desktop\2018-039788_PPT.pdf [Ver Fichero](#)

Tipo de firma: Firma PDF

Tipo de fichero: Documento Adobe PDF

Fecha última modificación: 14 de noviembre de 2018 12:06

Tamaño: 240 KB

[Hacer la firma visible dentro del PDF](#)

[Firmar](#)





La aplicación AutoFirma (II)

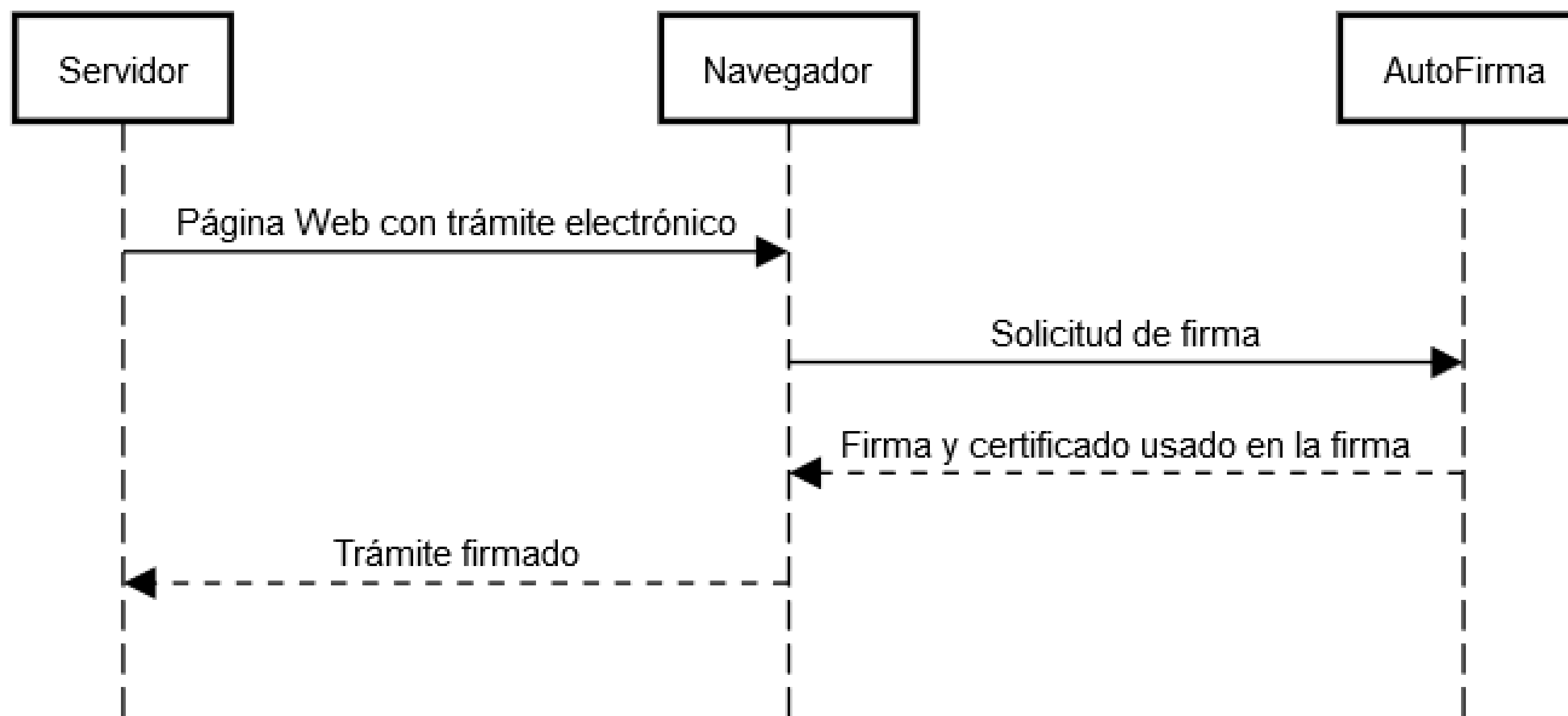
- La aplicación AutoFirma permite hacer firmas electrónicas en trámites puramente Web.
- Consiste en una aplicación local (que debe instalar el ciudadano en su equipo, disponible para Linux, macOS y Windows) y una biblioteca de integración JavaScript (que debe usar el integrador en su aplicación Web para solicitar una firma electrónica).
- Es una aplicación pensada para la firma electrónica de documentos, **pero no para la autenticación de usuarios.**





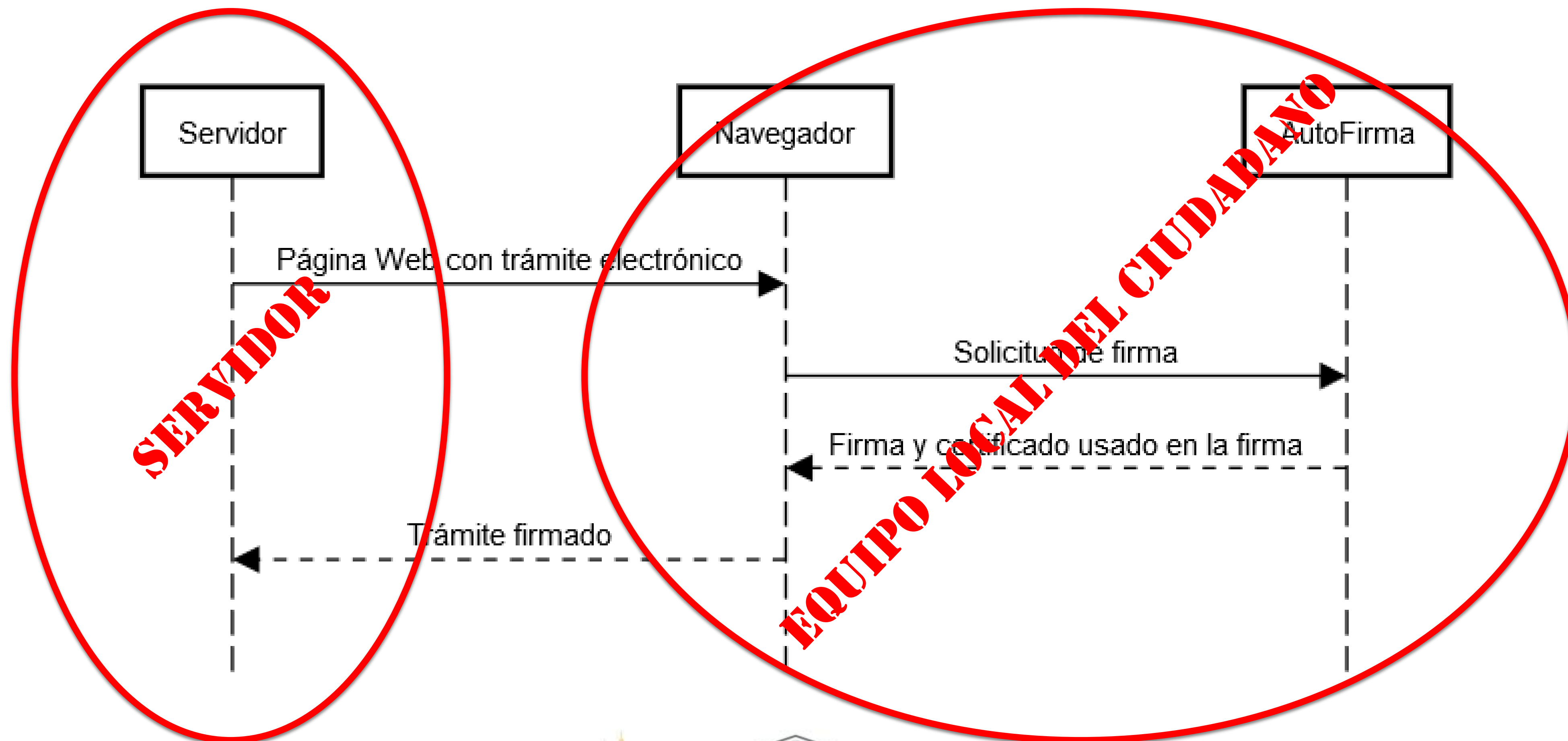
La aplicación AutoFirma (III) - ¿Cómo funciona?

Secuencia de operaciones típica de AutoFirma





La aplicación AutoFirma (IV) - ¿Cómo funciona?





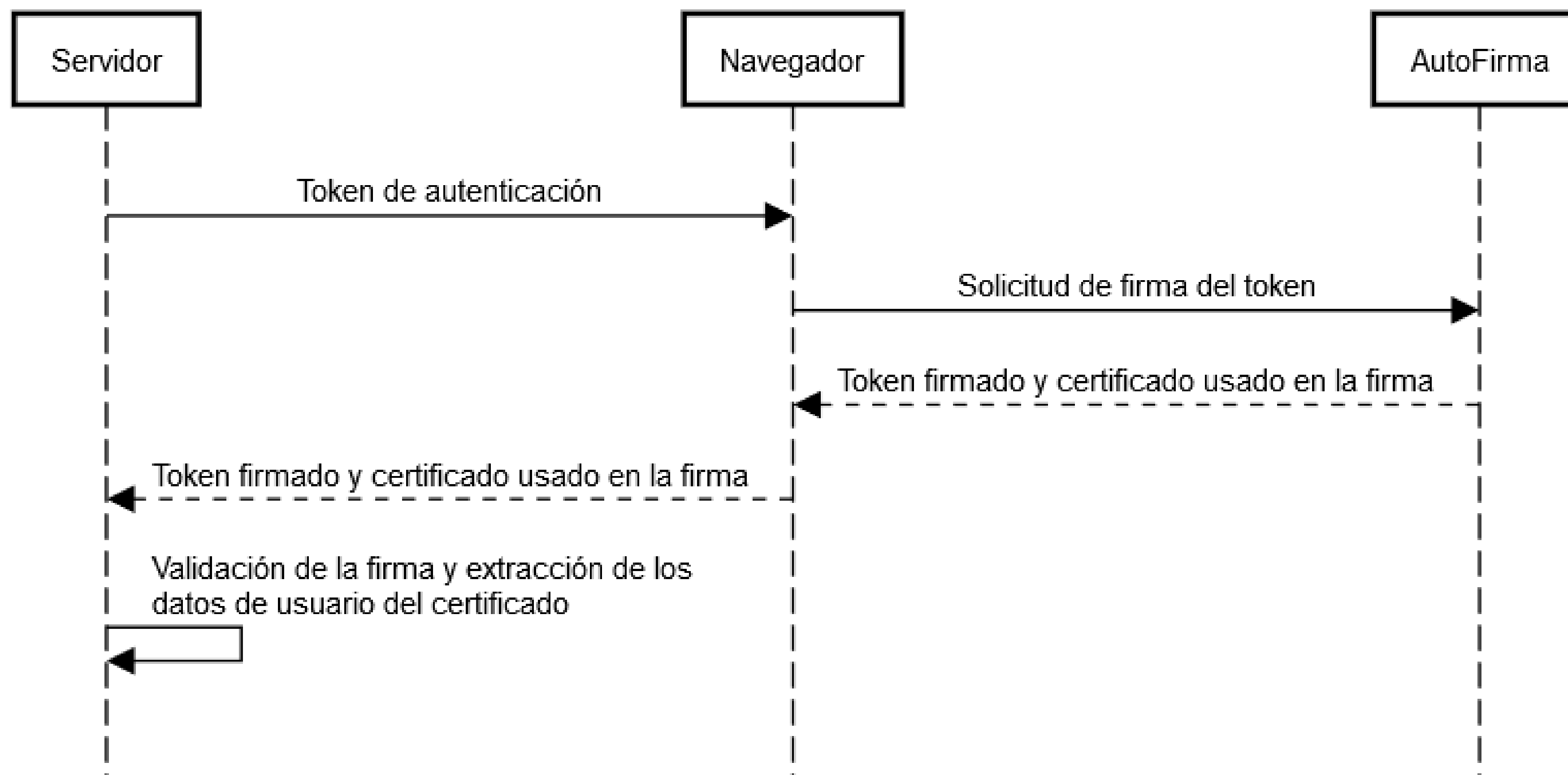
La aplicación AutoFirma (V) - Autenticación

- Para evitar el “problema” de configurar SSL cliente, muchos organismos optan por pervertir la finalidad de AutoFirma y usarlo para autenticar a los usuarios
- La idea es simple, desde la aplicación solicitamos al usuario que firma electrónicamente (con su certificado) un *token* de autenticación usando AutoFirma.





La aplicación AutoFirma (y VI) - Autenticación





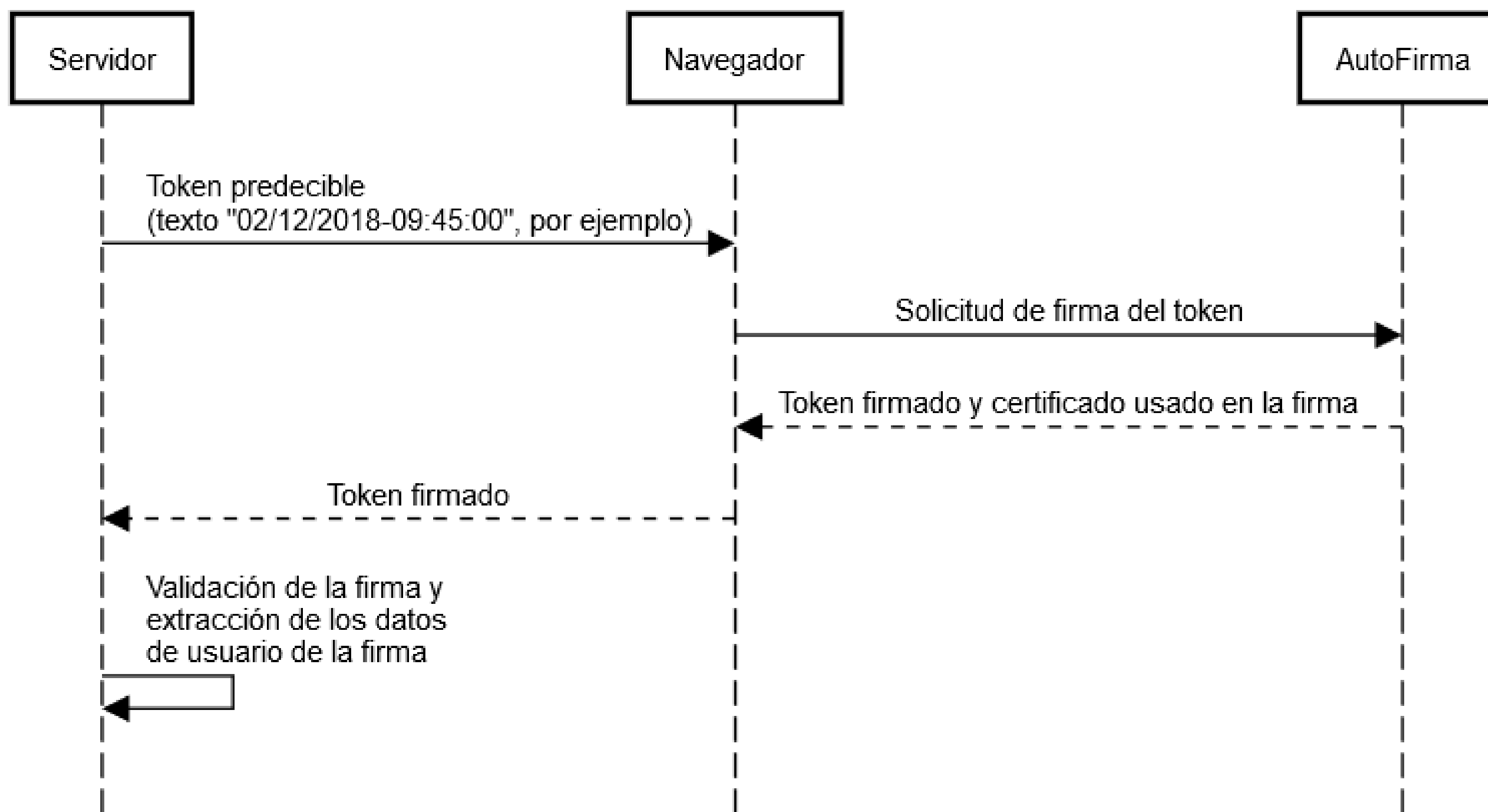
#CyberCamp18

Empieza la fiesta: ¿Qué estoy haciendo mal?





Uso de un *token* predecible para autenticación (I)





Uso de un *token* predecible para autenticación (II)

- **Se hace firmar al usuario un texto predecible**
 - Un mismo *token* firmado no puede reutilizarse (es predecible, pero único), pero si consigo engañar al usuario (*phishing*) para que firme un token que preveo será válido, tendremos acceso a una sesión con su identidad en la sede.
 - Un ejemplo es hacerle firmar la fecha y hora de inicio del trámite, y rechazar valores que se desplacen más allá de una ventana de tiempo (unos minutos).
 - En el *phishing* puedo hacer que firme varios posibles valores del *token*, para tener varios intentos.





Uso de un *token* predecible para autenticación (y III)

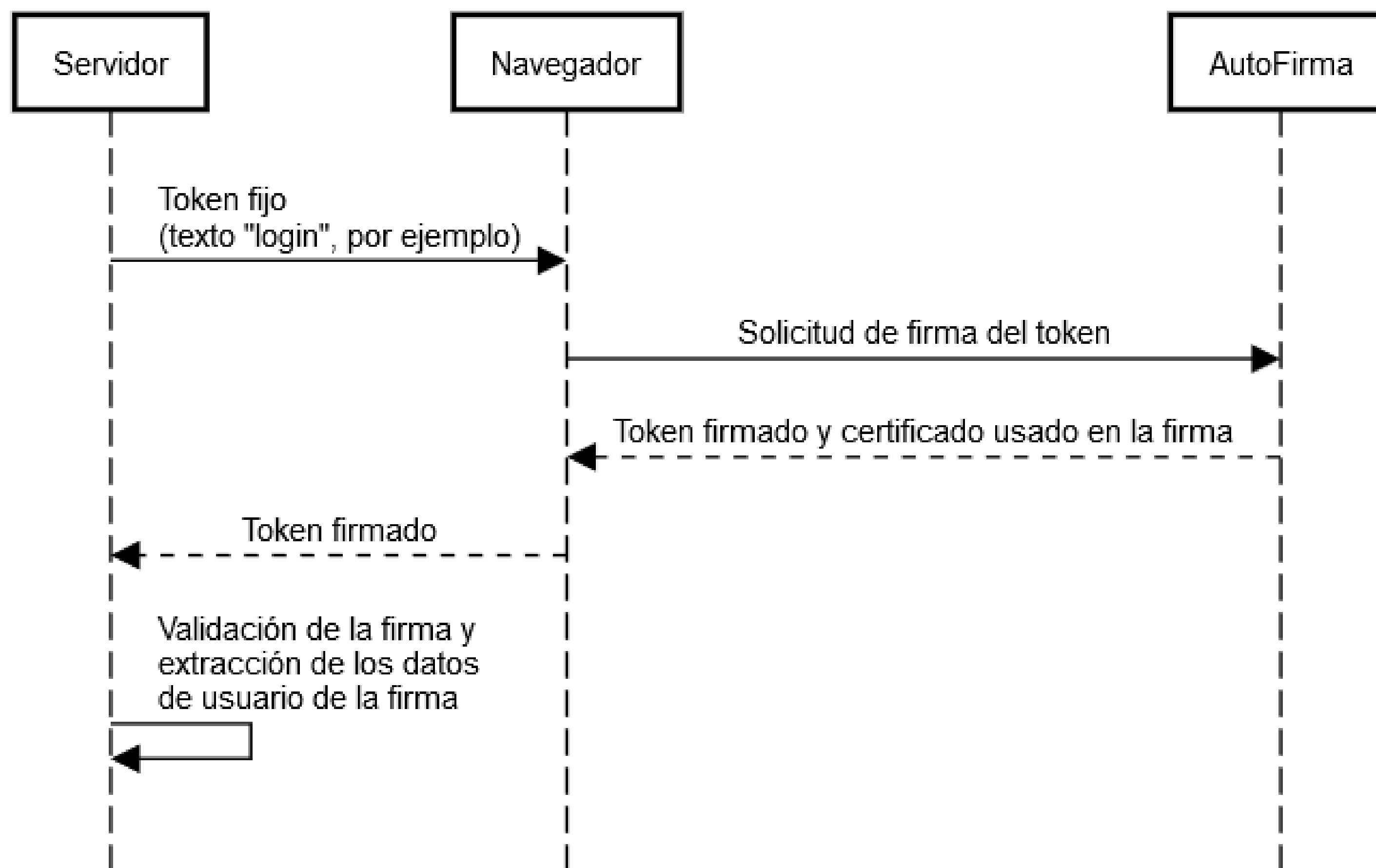
- **Clasificación:**

ABERRACIÓN





Uso de un *token* fijo para autenticación (I)





Uso de un *token* fijo para autenticación (II)

- **Se hace firmar al usuario un texto... Pero este texto es siempre el mismo**
 - Un mismo *token* firmado podría reutilizarse todas las veces que queramos, ya que nunca varía.
 - Si conseguimos interceptar un *token* firmado o engañar al usuario para que lo firme (*phishing*) tendremos acceso total a su identidad en la sede electrónica.





Uso de un *token* fijo para autenticación (y III)

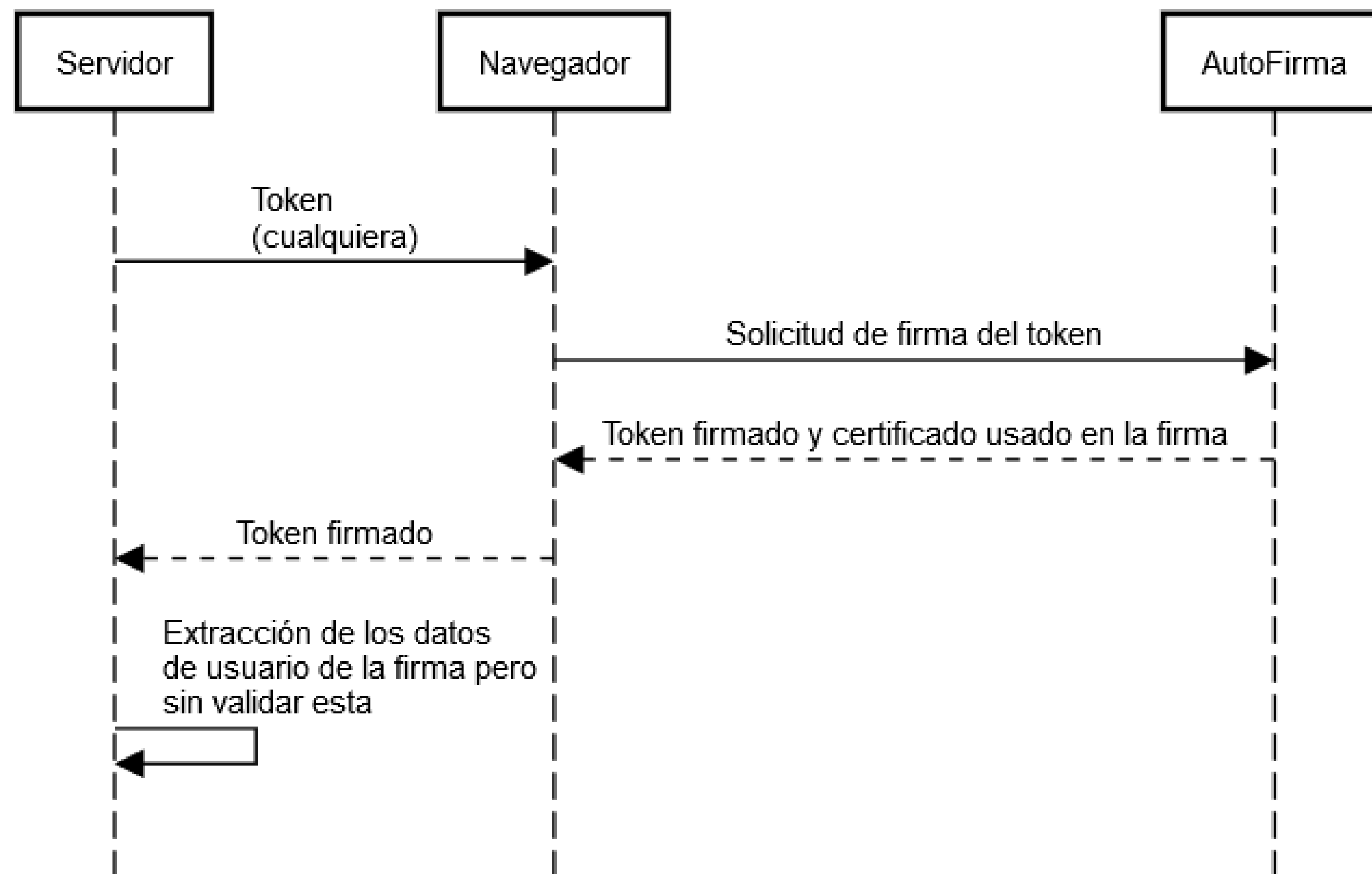
- **Clasificación:**

ABOMINACIÓN





Uso de un *token*, pero no comprobarlo (I)





Uso de un *token*, pero no comprobarlo (II)

- Se hace firmar al usuario un *token*, pero luego no se comprueba qué es lo que ha firmado realmente, solo quién lo ha firmado
- Con enviarle una firma válida (que podemos extraer de un PDF firmado o de cualquier lado) va a darlo por bueno.
 - A veces hay organismos que ni tan siquiera comprueban que la firma sea válida...





Uso de un *token*, pero no comprobarlo (y III)

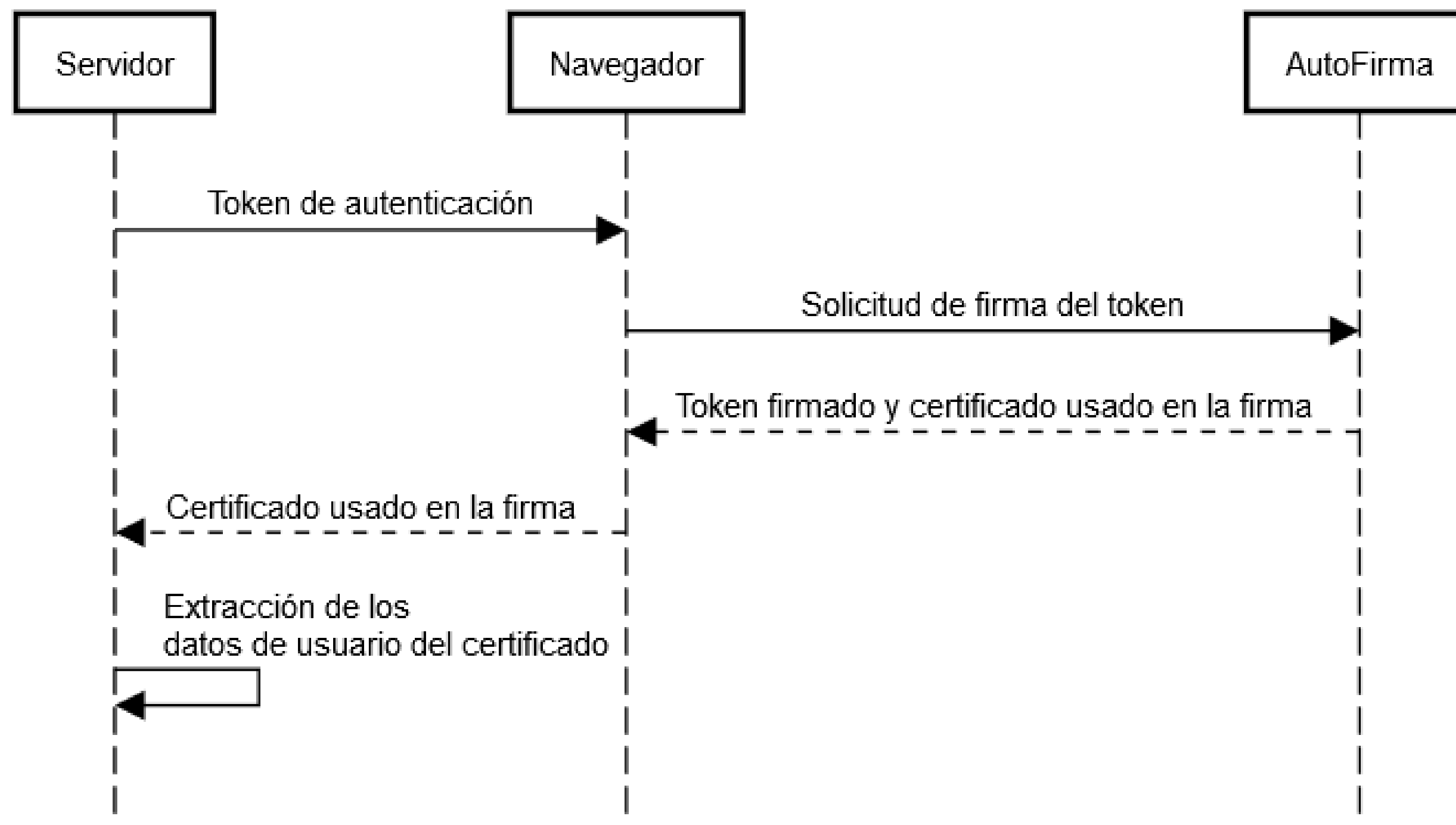
- **Clasificación:**

ABOMINACIÓN





Uso de la clave pública para autenticación (I)





Uso de la clave pública para autenticación (II)

- **En vez de enviar la firma al servidor se envía el certificado usado para generar la firma.**
- Pero... ¡Los certificados son públicos! Pueden ser extraídos sin dificultad de cualquier documento firmado, desde un PDF hasta un correo electrónico firmado.
 - Se ha usado realmente la clave pública para autenticar al usuario.
- Increíble, pero este procedimiento se ha usado intensivamente en el pasado en sedes electrónicas... Y se sigue usando en algunas.





Uso de la clave pública para autenticación (y III)

- **Clasificación:**

NO HAY PALABRA ÉLFICA, NI EN LENGUA ENT, NI DE MORDOR NI HUMANA QUE PUEDA DESCRIBIR ESTE HORROR





¿*Phishing* para obtener firmas electrónicas? Más fácil de lo que parece





Firmas sin autorización con AutoFirma

- **¡Sorpresa! AutoFirma permite desencadenar firmas electrónicas sin la autorización explícita del firmante... ¡Incluso desencadenar un lote de múltiples firmas!**
 - Solo necesitamos que entre en una página Web y pulse un botón o un enlace (en ciertos navegadores web ni eso, con que entre en la página vale).
 - El usuario verá la imagen de arranque de AutoFirma (*splash*), pero no puede cancelar el proceso.
 - Incluso si cierra el navegador web probablemente será demasiado tarde.





Tomás García-Merás Capote:

- tgarciameras@atSistemas.com
- clawgrip@hotmail.com
- <https://www.linkedin.com/in/tomas-gmeras/>

GRACIAS

