



Camerfirma

Implantación de Certificados Digitales en Servidores Web.

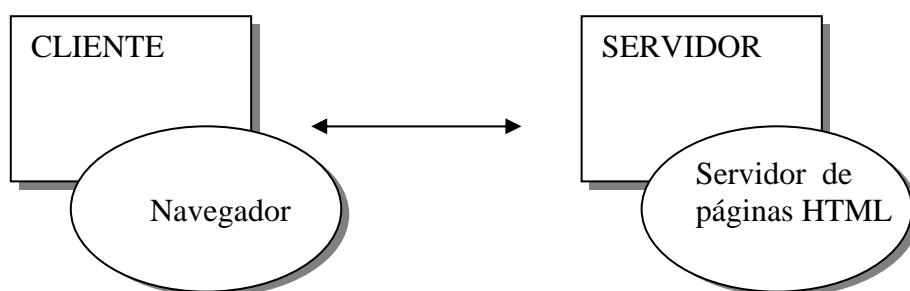
AC CAMERFIRMA SA

CIF A 82743287 Teléfono. 902 361 207 Fax. 91 561 07 69
comercial@camerfirma.com <http://www.camerfirma.com>
Documento Público

1. Objetivos.

El objetivo de este documento es ofrecer al desarrollador una guía para incorporar los certificados digitales en aplicaciones Web.

El esquema de interconexión que nos encontramos es el siguiente:



El certificado digital puede incorporar de forma casi inmediata y sin apenas esfuerzos de desarrollo las siguientes funcionalidades:

- Identificación de la identidad del servidor.
- Cifrado de la comunicación entre las partes.

Adicionalmente:

- Identificación de la identidad del cliente.
- Gestión de permisos (ad-hoc o vía ACL).

Con algún esfuerzo de desarrollo y la utilización de algún componente adicional que presentaremos en este documento posteriormente, podremos incorporar:

- Firma de formularios y ficheros en servidor.

- Envío de correos firmados como recibos o comprobantes electrónicos

2. LA COMUNICACIÓN. EL SSL

La opción mas inmediata para incorporar los certificados digitales es la configuración del protocolo SSL (Secure Socket Layer).

El SSL es un protocolo diseñado por Netscape y pensado para proporcionar sesiones de comunicación cifradas autenticación entre navegadores y servidores de páginas. El protocolo SSL en su versión 3 proporciona también autenticación de cliente. Podemos encontrarnos las siglas TSL (Transport Security Layer) para designar el mismo protocolo. TSL es una revisión de SSL y ofrece mejoras en los mecanismos de seguridad del protocolo.

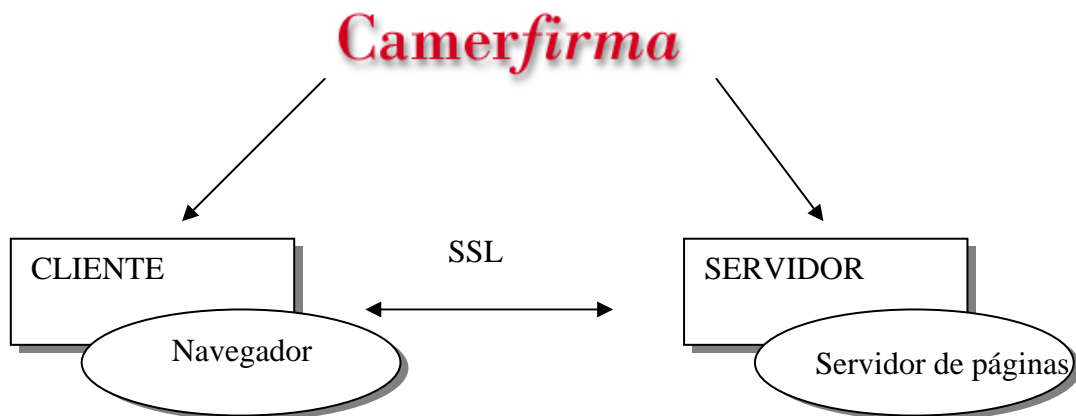
El protocolo de conexión se inicia cuando un usuario invoca el protocolo seguro mediante una llamada del tipo `https://www.servidor.com` la “s” adicional al protocolo llamado `http` significa que necesitamos establecer una conexión segura.

El servidor de páginas debe estar preparado para recibir una conexión de este tipo que normalmente escucha por un puerto distinto (443) a las conexiones no seguras (80).

Cuando una petición segura “https” es recibida, el servidor envía al cliente un certificado digital emitido por una autoridad de certificación, que le identifica como titular de la dirección en Internet.



Los certificados Camerfirma Corporate Express Server cumplen dicha función.



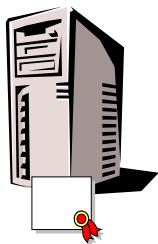
En esta situación estamos en condiciones de asegurar la identidad del servidor y la confidencialidad de la transmisión. Para conocer como se configura el protocolo SSL en un servidor de paginas concreto consultar los siguientes links:

- Para un servidor IIS 5.0 en Windows 2000 :
http://www.camerfirma.com/mod_web/usuarios/pdf/EXTEC2003002.pdf
- Para Apache:
http://www.camerfirma.com/mod_web/usuarios/pdf/EXTEC200004.pdf
- Para Iplanet:
http://www.camerfirma.com/mod_web/usuarios/pdf/EXTEC2001004.pdf
- Para Tomcat:
http://www.camerfirma.com/mod_web/usuarios/pdf/EXTEC2003012.pdf

Para consultar la documentación de instalación en mas servidores consultar la página Web de Camerfirma
<http://www.camerfirma.com/express>.

AC CAMERFIRMA SA

CIF A 82743287 Teléfono. 902 361 207 Fax. 91 561 07 69
comercial@camerfirma.com <http://www.camerfirma.com>
Documento Público



Se instala el certificado en el servidor. El servidor ya está preparado para realizar conexiones SSL.



Camerfirma

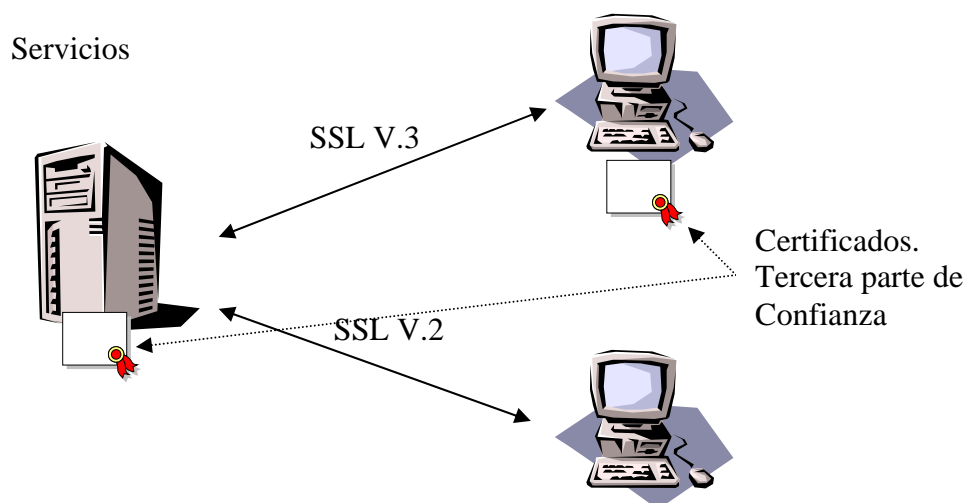
Hasta aquí se puede decir que el procedimiento más comúnmente usado para conectar a sitios seguros queda cerrado, pero el protocolo tiene una fase adicional cuando el servidor también requiere la identificación del usuario que accede al servicio. Los servidores de páginas se pueden configurar para que exijan la autenticación de cliente. En el caso de que éste no pueda proporcionar un certificado válido al servidor, la conexión se cierra enviando una página de aviso al usuario y transmitiéndole la necesidad de tener un certificado para acceder al recurso solicitado. En caso de que el usuario tenga más de un certificado válido la aplicación le dará la posibilidad de elegir uno.

Una vez entregado al servidor realizará las comprobaciones de validez (consulta de la lista de certificados revocados.) y se completará el protocolo. Estaremos entonces en la siguiente situación:

- Servidor autenticado mediante certificado (emitido por una autoridad de certificación).
- Usuario autenticado mediante certificado (emitido por el mismo o por otro prestador).
- Canal seguro mediante cifrado.

En algunos casos la comprobación de la CRL se hace de manera automática en la parte del servidor (cuidado con IIS que suele tener

comportamientos no previsible en la gestión de la lista de revocados). Muchas veces es mejor desactivar la comprobación de CRL en la configuración del servidor y realizar esta operación directamente en la aplicación.



SSL cubre muchas de las necesidades de seguridad para incorporar servicios electrónicos de forma rápida sin prácticamente necesidad de desarrollos. Un proceso que queda fuera del protocolo es el establecimiento de los permisos. La acreditación de la identidad obviamente no implica el derecho a usar un recurso. Una forma de realizarlo es: o bien realizarlo en la aplicación, o configurar el servidor de páginas para que la identidad del usuario sea comprobada sobre las listas de control de accesos (ACL) o sobre el directorio activo de Windows, gestionado por el administrador del servidor de páginas.

En la siguiente figura vemos la información sobre las variables de entorno asociadas recogidas de los certificados de cliente que IIS deja para su uso por las aplicaciones.



CERT_COOKIE	a5569ddcea8ca6646054ef37df3c78cd
CERT_FLAGS	1
CERT_ISSUER	C=ES, E=ac_camerfirma_cc@camerfirma.com, L=Madrid (see current address at www.camerfirma.com/address), OID.2.5.4.5=A82743287, O=AC Camerfirma SA, CN=AC Camerfirma Certificados Camerales
CERT_SERIALNUMBER	3e
CERT_SUBJECT	C=ES, CN=Ramiro Muñoz Muñoz, E=ramirom@camerfirma.com, OID.2.5.4.5=00381184M, SN=Munoz Muñoz, G=Ramiro, OID.1.3.6.1.4.1.17326.30.2=CIF IVA (VAT number as by article 28h of Directive 77/388/EEC), OID.1.3.6.1.4.1.17326.30.3=ESA82743287, O=AC Camerfirma SA, OU=Técnico, T=Director Técnico, Description=Chambers of Commerce Qualified Certificate: Natural Person CAM-PF-SW-PSC



Podemos usar esta información para gestionar los permisos de acceso a las diferentes zonas o transacciones ofrecidas por la aplicación.

El servidor Apache es algo mas generoso en este tipo de informacion como vemos en la tabla que mostramos a continuacion:

Variable Name:	Value Type:	Description:
HTTPS	flag	HTTPS is being used.
SSL_PROTOCOL	string	The SSL protocol version (SSLv2, SSLv3, TLSv1)
SSL_SESSION_ID	string	The hex-encoded SSL session id
SSL_CIPHER	string	The cipher specification name
SSL_CIPHER_EXPORT	string	true if cipher is an export cipher
SSL_CIPHER_USEKEYSIZE	number	Number of cipher bits (actually used)



AC CAMERFIRMA SA

CIF A 82743287 Teléfono. 902 361 207 Fax. 91 561 07 69
comercial@camerfirma.com <http://www.camerfirma.com>
Documento Público



SSL_CIPHER_ALGKEYSIZE	number	Number of cipher bits (possible)
SSL_VERSION_INTERFACE	string	The mod_ssl program version
SSL_VERSION_LIBRARY	string	The OpenSSL program version
SSL_CLIENT_M_VERSION	string	The version of the client certificate
SSL_CLIENT_M_SERIAL	string	The serial of the client certificate
SSL_CLIENT_S_DN	string	Subject DN in client's certificate
SSL_CLIENT_S_DN_x509	string	Component of client's Subject DN
SSL_CLIENT_I_DN	string	Issuer DN of client's certificate
SSL_CLIENT_I_DN_x509	string	Component of client's Issuer DN
SSL_CLIENT_V_START	string	Validity of client's certificate (start time)
SSL_CLIENT_V_END	string	Validity of client's certificate (end time)
SSL_CLIENT_A_SIG	string	Algorithm used for the signature of client's certificate
SSL_CLIENT_A_KEY	string	Algorithm used for the public key of client's certificate
SSL_CLIENT_CERT	string	PEM-encoded client certificate
SSL_CLIENT_CERT_CHAIN <i>n</i>	string	PEM-encoded certificates in client



		certificate chain
SSL_CLIENT_VERIFY	string	NONE, SUCCESS, GENEROUS or FAILED : <i>reason</i>
SSL_SERVER_M_VERSION	string	The version of the server certificate
SSL_SERVER_M_SERIAL	string	The serial of the server certificate
SSL_SERVER_S_DN	string	Subject DN in server's certificate
SSL_SERVER_S_DN_x509	string	Component of server's Subject DN
SSL_SERVER_I_DN	string	Issuer DN of server's certificate
SSL_SERVER_I_DN_x509	string	Component of server's Issuer DN
SSL_SERVER_V_START	string	Validity of server's certificate (start time)
SSL_SERVER_V_END	string	Validity of server's certificate (end time)
SSL_SERVER_A_SIG	string	Algorithm used for the signature of server's certificate
SSL_SERVER_A_KEY	string	Algorithm used for the public key of server's certificate
SSL_SERVER_CERT	string	PEM-encoded server certificate

[where x509 is a component of a X.509 DN:
,ST,L,O,OU,CN,T,I,G,S,D,UID,Email]

3. FIRMA DE FORMULARIOS.

Se puede complementar el protocolo **SSL** con la firma de formularios. En algún momento de la aplicación podemos requerir una evidencia electrónica para demostrar que el usuario ha realizado una transacción concreta. Los navegadores comerciales dependiendo de su fabricante tienen procedimientos distintos para realizar esto:

Netscape ofrecía una utilidad llamada formsign para firmar los datos de un formulario con los certificados gestionados en su almacén, dejando la firma electrónica en una variable que podría ser recogida por el servidor y almacenarla como una evidencia ante posibles problemas de repudio. Explorer necesita un componente **Active X** para la realización de estas operaciones.

Mientras que la herramienta ofrecida por Netscape era de libre uso, el Active X de Microsoft tiene más problemas de uso y hay que acceder a productos distribuidos por empresas comerciales bajo la compra de una licencia. Como alternativa Microsoft nos ofrece unas librerías a disposición de los desarrolladores llamadas **CAPICOM** que nos sirven para realizar estas operaciones sin tener que pasar por la compra de licencias comerciales. Como contrapartida nos encontraremos con un proceso muy poco elegante con textos en inglés.

AC Camerfirma ofrece también applets JAVA para la firma de formularios que tienen la propiedad de ser multiplataforma es decir que sirven tanto en entornos Microsoft como en Netscape.

Para cerrar el proceso de una hipotética aplicación podemos recoger el contenido del formulario y enviarlo por correo electrónico firmado. Esto nos



permitirá utilizar nuestro cliente de correo para validar la firma realizada y almacenar una evidencia de la transacción. Podemos ver un ejemplo completo de acceso **SSL** con identificación de usuario en la página <https://www.camerfirma.com/demo/certificados>.

(www.camerfirma.com/express).

En la página Web de Camerfirma (www.camerfirma.com/express) se puede encontrar información adecuada para realizar tanto la solicitud como la instalación del certificado de servidor. Estos procedimientos varían en función del tipo de servidor para el que se solicita el certificado.



Camerfirma

4. Consulta de Revocados.

Dentro de los procedimientos de control de acceso con el certificado, es importante comprobar la validez de un certificado, es decir si ha sido revocado o no. Para ello podemos utilizar la CRL (Certificate Revocation List) o Lista de Certificados Revocados, que podemos encontrar vía Web. Camerfirma, publica sus CRL's en la URL <http://www.camerfirma.com/camerfirma.crl> .

Una CRL es una lista negra con los certificados que por alguna causa han perdido su valor y que contiene la siguiente estructura:

- número de serie del certificado revocado
- fecha de la revocación
- causa de la revocación (clave comprometida, suspensión temporal...)

Este fichero está firmado por la CA o por una autoridad de revocación en la cual haya delegado la CA.

Existe una opción adicional una CGI donde se puede consultar el estado del certificado pasando como parámetro el numero de serie que se puede obtener de la variable de entorno CERT_SERIALNUMBER. Un ejemplo puede ser <http://crl.camerfirma.com/emprep.cgi?8AFD56G7H8J> de la ejecución de la dirección anterior un "0" si el certificado no es encontrado en las listas de revocación y un "1" si ha sido encontrado el número de serie indicado en la lista de revocación. Este servicio no puede darnos una evidencia electrónica firmada como puede hacer la CRL, pero es una



Camerfirma

AC CAMERFIRMA SA

CIF A 82743287 Teléfono. 902 361 207 Fax. 91 561 07 69
comercial@camerfirma.com <http://www.camerfirma.com>

Documento Público

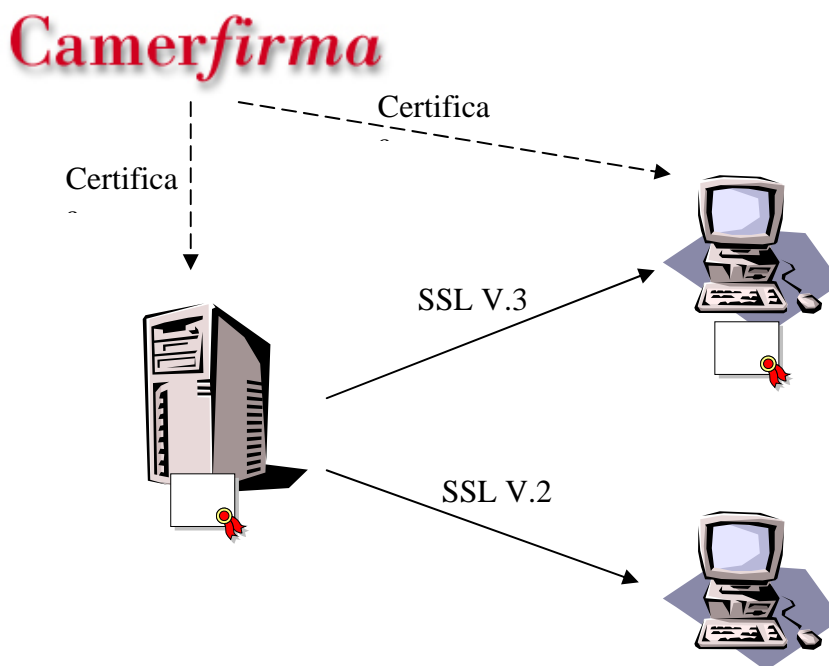
herramienta muy útil para eliminar de forma rápida en tiempo real el riesgo de usar un certificado revocado.

5. Camerfirma como tercera parte de Confianza.

Camerfirma juega el papel de tercera parte de la confianza. Asegura que los dos elementos implicados en un protocolo SSL(cliente y servidor) son quien realmente dicen ser.



Camerfirma



Cualquier consulta o comentario respecto al contenido de este documento notificarla a sopORTE@camerfirma.com.



Camerfirma

Certificado Digital



Camerfirma

AC CAMERFIRMA SA

CIF A 82743287 Teléfono. 902 361 207 Fax. 91 561 07 69
comercial@camerfirma.com <http://www.camerfirma.com>

Documento Público