Proyecto conjunto: Servicios de Red e Internet Implantación de Aplicaciones Web

Servidores Web, Certificados seguros para HTTPS, capa SSL y Sistemas Gestores de Contenido

> Antonio José Miñarro Miñarro 2º ASIR – SRI y IAW

SRI y IAW

Actividades con los navegadores (clientes)

1. Visita una Web que utilice HTTPS y comprueba los siguientes datos: Para quién se emitió el certificado, CA, algoritmo, fecha de caducidad y clave pública. Entregar datos obtenidos y pantallas de capturas

La web visitada es la de Caja Murcia con el navegador cliente Google Chrome (<u>https://www.cajamurcia.es</u>). Como vemos a la izquierda de la URI, en la barra de direcciones podemos acceder a la información sobre el certificado que está usando este sitio. Comprobamos que usa certificado por el uso del protocolo HTTP sobre SSL (https://) y por el icono verde de un candado. Accedemos como se muestra en la primera captura y comprobamos los datos necesarios (Capturas 2, 3 y 4)



or de certificados:"www.caja	murcia.es"	23	
eneral Detalles			
Fata anatificada ha aida a			
Este certificado na sido v	erificado para los siguientes usos:	-	
Certificado del servidor S	SL		
Emitido para			
Nombre común (CN)	www.cajamurcia.es		
Organización (O)	BANCO MARE NOSTRUM SA		
Unidad organizativa (OU)	Financial Entity		
Número de serie 31:14:6D:16:E0:6D:FA:AA:C4:27:13:7D:A8:15:C7:97			
Emitido por			
Nombre común (CN)	VeriSign Class 3 Extended Validation SSL SGC CA		
Organización (O)	VeriSign, Inc.		
Unidad organizativa (OU)	VeriSign Trust Network		
Validez			
Emitido el	12/09/2013		
Caduca el	13/10/2014		
Huellas digitales			
Huella digital SHA1	CF:62:97:EC:29:CF:0E:F6:44:4D:F2:05:0F:30:0E:E4:03:11:9	F:F4	
Huella digital MD5	45:D7:14:19:CB:F6:FE:E3:81:52:CE:F4:25:3A:9F:C5		

Gener	al Detalles	
Je	rarquía de certificados	
4	VeriSign Class 3 Public Primary Certification Authority - G5	
	VeriSign Class 3 Extended Validation SSL SGC CA	
	www.cajamurcia.es	
Ca	impos del certificado	
4	www.cajamurcia.es	
	#Certificado	(
	-Versión	
	Número de serie	
Г	Algoritmo de firma del certificado	
_	Emisor	
	⊿ Validez	
	No antes	
	-No antes -No después	
	No antes No después Asunto	

		Cla	ive p	oúbli	ica o	lel s	ujet	0							
	Æ	xten	sion	es											
		No	mbi	re al	tern	ativ	o de	l asu	into	del	cert	ifica	do		
		Res	stric	cion	es b	ásic	as d	e ce	rtific	cado)				
		Uti	lizac	ión	de l	a cla	ive o	le ce	ertifi	cad	D				
		Po	lítica	is de	e cer	tific	ado								
		Pu	ntos	de	distr	ibu	ción	de (CRL						
		Us	o ext	end	ido	de l	a cla	ve							
		Ide	ntifi	cad	or d	e la	clav	e de	la A	uto	rida	d Ce	rtifi	cado	ora (
		Ac	ceso	a la	inf	orm	ació	n de	la a	auto	rida	d			
/alo	or de	el ca	mp	0			acio			10100	- Tara				
Móc	in le	- 13	2048	h h	ital										
a4	cf	32	1e	4b	fd	b9	00	27	b6	da	61	d2	ad	c1	e3
07	4b	ab	0c	a4	9f	2b	d 0	ee	fa	14	42	39	79	64	7d
6c	15	1b	26	4b	6b	97	79	3b	3f	5c	00	50	ef	e5	62
10	5b	d6	d7	c1	61	2c	2c	da	fe	8c	72	85	c5	10	b8
10															
21	ab	16	d4	80	79	4c	19	eb	03	c3	95	76	44	f4	cc
10 21 4d	ab 7a	16 8f	d4 14	80 db	79 e7	4c 42	19 97	eb a7	03 ca	c3 c2	95 41	76 d0	44 11	f4 e4	cc 9c
10 21 4d f8	ab 7a 58	16 8f 24	d4 14 d2	80 db 36	79 e7 8f	4c 42 4b	19 97 7f	eb a7 56	03 ca 2a	c3 c2 8b	95 41 1a	76 d0 b8	44 11 3d	f4 e4 c4	сс 9с 85

Navegadores Web SRI y IAW Antonio José Miñarro

2. Instala el certificado de una Web segura, visita la Web y comprueba que no vuelve a pedirte autorización, borra el certificado y visítala de nuevo. (Windows y Linux). Entregar paso a paso y pantallas de capturas.

En esta ocasión vamos a acceder desde el navegador cliente Mozilla Firefox, porque al parecer Google Chrome instala de manera predeterminada este certificado sin pedirnos confirmación. Para ellos hemos visitado la web de la Agencia Tributaria (www.agenciatributaria.es). Como se ve en esta primera captura, el sitio web nos muestra un mensaje requiriendo la instalación del certificado electrónico Raíz, reconocido por la FNMT, lo que confirma la veracidad del sitio que estamos visitando. La práctica es idéntica en un cliente Mozilla Firefox de Windows que en otro de Linux, por lo que se omiten las capturas y explicación

Firefox 🔨 🔊 Agencia Tributaria - Inicio	× 🔿 Agencia Tributaria - Ayuda	× Conectando	× +
(www.agenciatributaria.es/esede/eSede.h	tml		🏫 ⊽ 🗙 🔀 ▾ Google
🗌 ASIR 📓 IES San Juan Bosco 🚳 Juan Antonio	López Q		
	El acceso seguro a la Sede Electrónica de la Ag Fábrica Nacional de Moneda y Timbre. No es posible comprobar en su navegador si ti Si lo tiene instalado, pinche Aceptar para acced Si no es así, pinche en cancelar para acceder a	encia Tributaria requiere que su navegador i ene instalado el certificado raíz. er a la Sede Electrónica. la ayuda de instalación de los certificados.	reconozca un certificado electrónico Raíz de la
			Aceptar Cancelar

Si clicamos aceptar intentaremos acceder a la web sin instalar el certificado, por lo que tendremos el siguiente mensaje de advertencia:

	Esta conexión no está verificada
YZ	Ha pedido a Firefox que se conecte de forma segura a www.agenciatributaria.gob.es , pero no se puede confirmar que la conexión sea segura.
	Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.
	¿Qué debería hacer?
	Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.
	¡Sácame de aquí!
•	Detalles técnicos
	www.agenciatributaria.gob.es usa un certificado de seguridad no válido.
	No se confía en el certificado porque el certificado emisor es desconocido.
	(Código de error: sec_error_unknown_issuer)
•	Entiendo los riesgos
	Si sabe lo que está haciendo, puede obligar a Firefox a confiar en la identificación de este sitio. Incluso aunque confíe en este sitio, este error puede significar que alguien esté interfiriendo en su conexión.
	No añada una excepción a menos que sepa que hay una razón seria por la que este sitio no use identificación confiable.
	Añadir excepción

Navegadores Web SRI y IAW Antonio José Miñarro

Si intentásemos añadir una excepción para que Firefox accediera aun no teniendo el certificado, no sería posible, al menos para este sitio, ya que como indica el mensaje:

	Está a punto de alterar cómo identifica Firefox este sitio. Los bancos, tiendas y otros sitios públicos legítimos no le pedirán hacer esto. Servidor Dirección: https://www.agenciatributaria.gob.es/AEAT.sede/. Obtener certificado
8	Estado del certificado
	Certificado válido Este sitio proporciona identificación válida y verificada. No hay necesidad de añadir una excepción.
:	Guardar esta excegción de manera permanente
	<u>C</u> onfirmar excepción de seguridad Cancelar

Si clicásemos en Cancelar obtendríamos una página con las instrucciones para descargar e instalar los certificados necesarios. Seguimos las sencillas instrucciones:

See www.agenciatributaria.es/esede/eSede_nsf.shtml	😭 ⊽ 🕑 🚺 ₹ Google	
🗍 ASIR 🌠 IES San Juan Bosco 🛞 Juan Antonio López Q		
Acardia Tributasia	В	ienvenido Ben
Agencia Iributaria	Portal m	ivil 🔝 RSS
Ministerio de Hacienda y Administraciones Públicas Fiscalidad Autonómica y Local Fiscalidad No Residentes Enlaces de Interés		
Agencia Tributaria Ciudadanos Empresas y profesionales	Colaboradores	Búsqueda ava
		Sede
Ayuda		Ele
Inicio » Ayuda en Linea » Información y Requisitos de la nueva Sede Electrónica		

Para acceder correctamente a la Sede Electrónica de la Agencia Tributaria es necesario que descargue e instale los siguientes certificados (certificado raíz y certificado de sede electrónica) emitid Debe descargar los archivos .CER que se corresponden con cada uno de los dos certificados electrónicos necesarios, "AC RAIZ FNMT-RCM" y "AC APE" e instalarlos en el orden que le indicamo (Si lo desea, puede consultar más información al respecto en la página web de la FNMT).

Paso 1: Descarga e instalación del certificado raíz de la FNMT (AC RAIZ FNMT-RCM)

Pulse sobre el botón "Descargar certificado". Aparecerá una ventana solicitando que confíe en una nueva Autoridad Certificadora. Marque las 3 casillas "Confiar en..." y haga clic en "Aceptar" Por último, acepte las siguientes ventanas del navegador.

Descargar certificado

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).





Navegadores Web SRI y IAW Antonio José Miñarro

Ministerio de Hacienda y Administraciones Publicas	Jmica y Local D Fiscalidad No Residentes D Enlaces de Interes				
Agencia Tributaria Ayuda	Cividadassa Cividadassa <thcividadassa< th=""> Cividadassa</thcividadassa<>) 			
Inicio » Ayuda en Linea » Información y Requisit	☑ Confiar en esta CA para identificar sitios web.				
Para acceder correctamente a la Sede Electrónica de la Agencia T	Confiar en esta CA para identificar usuarios de correo.	ado			
Debe descargar los archivos .CER que se corresponden con cada	Confiar en esta CA para identificar desarrolladores de software.				
(Si lo desea, puede consultar más información al respecto en la pá	Anter de confine en este CA con environmentative debe considere el confitte de la station.				
Paso 1: Descarga e instalación del certificado raíz de la	Antes de contrar en esta CA para cualquier proposito, debe examinar el certificado, política y procedimientos de la CA (si están disponibles).				
Pulse sobre el botón "Descargar certificado". Aparecerá una ven	V	"			
Por último, acepte las siguientes ventanas del navegador.					
Descargar certificado	Aceptar Cancelar				
A continuación dispone de una serie de capturas de pantalla que p		Jer I			
Texa da Carlos Construintes de la Carlos Con					

Pulse el botón "Continuar" de esta página para seguir con la instalación del certificado de sede electrónica.

Continuar

Pulse el botón "Continuar" de esta página para seguir con la instalación del certificado de sede electrónica.

Continuar

Paso 2: Descarga e instalación del certificado de la subsede (AC APE)

El procedimiento de descarga e importación es similar al del certificado raíz.

Pulse sobre el botón "Descargar certificado". Aparecerá una ventana solicitando que confie en una nueva Autoridad Certificadora. Marque las 3 casillas "Confiar en..." y haga clic en "Aceptar".

Descargar certificado

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).

Paso 3: Instalación finalizada.

Si ha seguido las indicaciones paso a paso, ya tiene correctamente configurado su navegador para acceder a la nueva Sede Electrónica de la Agencia Tributaria. Pinche aquí para acceder a la sede electrónica.

Puede comprobar que los certificados están correctamente instalados si accede al menú de Firefox, "Herramientas", "Opciones", "Avanzado", y selecciona la pestaña "Cifrado". Haga clic en "Ver certificados" y seleccione "Autoridades"

Localice la autoridad "FNMT-RCM" en el listado, marque AC RAIZ FNMT-RCM y haga clic en el botón "Editar". Verifique que las 3 casillas de la ventana "Editar configuración de confianza de la CA" están marcadas. Pulse "Aceptar".

A continuación seleccione AC-APE FNMT-RCM y realice la misma comprobación. Haga clic en el botón "Editar". Verifique que las 3 casillas de la ventana "Editar configuración de confianza de la CA" están marcadas. Pulse "Aceptar".

Si los certificados están instalados en la pestaña "Autoridades" y las casillas indicadas están activadas su configuración es correcta.

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).



Tras la instalación podemos comprobar en el Administrador de certificados de Firefox como todo está correctamente instalado:

Tiene certificados en archivo que identifican e	stas autoridades certificadoras:	
Nombre del certificado	Dispositivo de seguridad	E.
Equifax Secure eBusiness CA-1	Builtin Object Token	-
▲FNMT-RCM		
AC APE - FNMT-RCM	Disp. software de seguridad	
AC RAIZ FNMT-RCM - FNMT-RCM	Disp. software de seguridad	
Generalitat Valenciana Root CA Generalitat Valenciana	Builtin Object Token	
▲GeoTrust Inc. GeoTrust Global CA	Builtin Object Token	-
Ver Editar confianza Impor	tar E <u>x</u> portar Elimi <u>n</u> ar o dejar de confiar	

Navegadores Web SRI y IAW

Y ya podemos acceder a la web de la Agencia Tributaria de manera segura mediante https, sin el mensaje que nos aparecía antes para instalar certificados:

📕 Firefox 🔪 🔊 Agencia Tributaria - Inicio 🛛 🛛 🗙 🔊	Sede Electrónica - Agencia Tributaria × +
+ https://www.agenciatributaria.gob.es	
🗌 ASIR 🌌 IES San Juan Bosco 🐠 Juan Antonio López Q	
🔒 👬 BEEBANG 📐 Agencia Tribut	aria Sede Electrónica Todos los trámites on líne
Bienvenido a la Sede electrónica de la Agencia Tri	butaria
Desde esta plataforma usted podrá acceder a los servicios horas de los 365 días del año.	electrónicos que la Agencia Tributaria pone a su disposición y podrá realizar sus trámites dura
Procedimientos, Servicios y Trámites (Información y Registro)	Trámites destacados 😨
Impuestos y Tasas	Kenta 2012 Sociedades 2012

Ahora desde el Administrador de certificados forzamos la eliminación de los certificados que hemos instalado:



Y cuando volvemos a visitar el sitio de nuevo, vuelve a aparecer el mensaje anterior:

El acceso seguro a la Sede Electrónica de la Agencia Tributaria requiere que su navegador reconozca un certificado electrónico Raíz de la Fábrica Nacional de Moneda y Timbre.

No es posible comprobar en su navegador si tiene instalado el certificado raíz

Si lo tiene instalado, pinche Aceptar para acceder a la Sede Electrónica.

Si no es así, pinche en cancelar para acceder a la ayuda de instalación de los certificados.

Aceptar	Cancelar
---------	----------

3. Configura el navegador para que acepte todas las cookies, navega unos minutos por tus Web favoritas y consulta las cookies que se han guardado en tu equipo. Una vez comprobadas bórralas para no dejar rastros de tu uso de internet y configura el navegador a su estado anterior. Entrega listado de cookies y pasos realizados.

En las preferencias de Mozilla Firefox encontramos la pestaña Privacidad. Allí podemos ver, en la opción que aparece abajo (eliminar cookies de forma individual), el listado de las cookies almacenadas por el navegador.

😣 🗐 🗐 Prefer	encias de Firef	x					
년 General Pesta	ñas Contenid	o Aplicaciones	Privacidad	Seguridad	CO Sync	کیک Avanzado	
Rastreo O I <u>n</u> dicar a lo: O Indicar a lo: N <u>o</u> indicar a Saber más	s sitios que no c s si <u>t</u> ios que quie a los sitios nada	uiero ser rastread ro ser rastreado sobre mis prefer	do encias de rast	reo			
Historial							
Firefox <u>p</u> odrá	Recordar his	torial		:	÷		
Firefox rec cookies de También p	ordará su histo los sitios Web odría <mark>limpiar su</mark>	rial de navegación que visite. <mark>historial reciente</mark>	n, descargas, f	formularios y Pookies de form	búsqued na individ	as, y guardará tambi <mark>dual</mark> .	én
Barra de direcc	ones						
Cuando se use	la <u>b</u> arra de dire	ecciones, sugerir:	Historial y n	narcadores	÷		
Ay <u>u</u> da						Ce	errar

Si queremos configurar el navegador para que se guarden todas las Cookies tenemos que cambiar a la siguiente opción (Firefox podrá: Usar una configuración personalizada para el historial) y (Aceptar Cookies) y (Siempre) :

8 a Preferencias de Firefox							
General Pestañas Contenido Aplicaciones Privacidad Seguridad	C) Sync	کې Avanzado					
Rastreo Indicar a los sitios que no quiero ser rastreado Indicar a los sitios que quiero ser rastreado No indicar a los sitios nada sobre mis preferencias de rastreo Saber más 							
Historial Firefox <u>p</u> odrá: Usar una configuración personalizada para el historial 🗘							
 Modo permanente de navegación privada Recordar mi historial de descargas y navegación Recordar el historial de formularios y búsquedas 							
✓ Aceptar cookies Aceptar las cookies de terceras partes: Siempre \$		Excepciones					
Mantener hasta que: caduquen ♀		Mo <u>s</u> trar cookies Configuración					



SRI y IAW

Después de navegar un poco observamos la lista de cookies:

🛪 Implantación de Aplicacion 🗶 🕼 Microsoft Word - Actividad 👋 📄 informaticabosco.com 🛛 🗶 📴 Outlook - antonio_jose91@ 🛠 💠								
🖌 🛋 Microsoft Corporation (US) https://dub125.mail.live.com/default.aspx?id=648558.mkt=es 🖄 🗸 😍 🔀 🛪 Hotmail							🗇 👻 🕙 🚼 🔻 Hotmail	
🕅 Más visitados 👻 🚳 Juao Antonio Lóngz								
M HIGS VISICOUGS -	Jo SourrAncon	io copez					://	dub125.mail.live.com/default.aspx?id=64855&mkt=es
General Pestañ	es Contenido	Aplicaciones	Privacidad	Seguridad	C Sync	کیک Avanzado		Bu <u>s</u> car: Las cookies siguientes están guardadas en su equipo:
Rastreo								Sitio
O Indicar a los s	itios que no qui	ero ser rastread	lo					▶ atdmt.com
Indicar a los s	itios que quiero	ser rastreado						▶ bluekai.com
	r <u>e</u> ros que quiero							▶ 🚞 chango.com
O N <u>o</u> Indicar a l	os sitios nada so	obre mis prerer	encias de rasc	reo				▶ 🚞 demdex.net
Saber mas								dub125.mail.live.com
Historial							1	▶ 🚞 google.com
Firefox podrá:	Perordar histo	rial						▶ 🚞 google.es
riferox <u>p</u> oura.	Recordar hisco	1101			•			▶ 🚞 h.atdmt.com
								▶ 🚞 h.live.com
								informaticabosco.com
								▶ 🚞 live.com
Firefox reco	rdará su historia	al de navegaciór	n, descargas, f	ormularios y	búsqueda	as, y guardará tambié	n	▶ 🚞 login.live.com
cookies de le	os sitios Web qu	e visite.		▶ 🚞 mail.live.com				
			1	▶ 🚞 microsoft.com				
También poo	lría limpiar su hi	storial reciente		▶ 🚞 mozilla.org				
				msft.demdex.net				
								people.directory.live.com
								s395148192.mialojamiento.es
								voutube com

Para eliminar las Cookies accedemos al apartado en el que antes hemos consultado las Cookies y podemos eliminarlas de manera individual, con el primer botón (Eliminar Cookies) o todas por completo con el segundo (Eliminar todas las Cookies).

Bu <u>s</u> car:			
Las cookies siguientes están guardadas e	n su equipo:		
Sitio		▼ Nombre de la cookie	
▶ 📄 atdmt.com			
▶ 📄 bluekai.com			
▶ 🚞 chango.com			
▶ 🚞 demdex.net			
dub125.mail.live.com			
▶ agoogle.com			
▶			
▶ <mark> h.atdmt.com</mark>			
h.live.com			
Informaticadosco.com			
Ive.com			
▶ anil live.com			
Nombre: < ninguna cookie seleccionar	las		
Contenido: <ninguna cookie="" seleccionac<="" td=""><td>la></td><td></td><td></td></ninguna>	la>		
Servidor: <ninguna cookie="" seleccionac<="" td=""><td>la></td><td></td><td></td></ninguna>	la>		
Ruta: <ninguna cookie="" seleccionac<="" td=""><td>la></td><td></td><td></td></ninguna>	la>		
Enviar para: <ninguna cookie="" seleccionac<="" td=""><td>la></td><td></td><td></td></ninguna>	la>		
Expira: <ninguna cookie="" seleccionac<="" td=""><td>la></td><td></td><td></td></ninguna>	la>		
Elimina <u>r</u> cookies Elimin <u>a</u> r todas las coo	kies		<u>C</u> errar



Y si queremos que no se guarden Cookies de los sitios que visitimas tendrémos que desmarcar la siguiente opción, desde las preferencias de Firefox, pestaña privacidad:

Firefox <u>p</u> odrá:	i: Usar una configuración personalizada para el historial 🛟					
🗆 Modo per	ma <u>n</u> ente de nave	gación privada				
Recor	dar mi historial c	le descargas y nave	egación			
🐱 Recordar el historial de <u>f</u> ormularios y búsquedas						
	Aceptar cookies					
Acept	ar cookies				Excepciones	
Acept Acep	<mark>ar cookies</mark> tar las cookies d	e terceras partes:	Nunca 🗘		Excepciones	
□ <mark>Acept</mark> Acep <u>M</u> ant	<mark>ar cookies</mark> tar las cookies d ener hasta que:	e terceras partes:	Nunca 🗘		Excepciones	

Una vez borrado el historial de Cookies y desactivada la opción de aceptar Cookies volvemos a navegar y observamos de nuevo el listado:

Bu <u>s</u> car:	٩				
Las cookies siguientes están guardadas en su equipo:					
Sitio 🔻	Nombre de la cookie				
Nombre: <ninguna cookie="" seleccionada=""></ninguna>					
Servidor: <ninguna cookie="" seleccionada=""></ninguna>					
Ruta: <ninguna cookie="" seleccionada=""></ninguna>					
Enviar para: <ninguna cookie="" seleccionada=""></ninguna>					
Expira: <ninguna cookie="" seleccionada=""></ninguna>					
Elimina <u>r</u> cookies Elimin <u>a</u> r todas las cookies	<u>C</u> errar				

Eso si, algunas webs requieren el uso de Cookies, como Hotmail:

	🕿 AS.com X 🕅 MARCA.com X 🖶 Cuenta Microsoft 🗱 📄 informaticabosco.com X	🗩 Web Personal: Juan A 🛛 😡 Habilitar y deshabilita 🗙 💠					
Q	Kirosoft Corporation (US) https://login.live.com/cookiesDisabled.srf?mkt=ES-US&lc=21514	🗇 👻 関 🔹 > aceptar Cookies Mozilla Firefox 🔍 🖖 🏫					
	📓 Más visitados 🔻 🛭 🚳 Juan Antonio López						
	Cuenta Microsoft						
	Es necesario admitir el uso de cookies Actualmente, el explorador está configurado para bloquear cookies. Para poder usar la cuenta Microsoft, el explorador debe permitirías. Las cookies son archivos de texto pequeños que se almacenan en el equipo y comunican a los sítios y servicios de Microsoft cuándo inicias sesión. Para obtener información sobre cómo permitirías, consulta la ayuda en pantalla del explorador web.						