Cómo implantar un Certificado Raíz de una Entidad Certificadora en Firefox

Firefox por defecto no trae algunos certificados de entidades certificadoras que solemos utilizar, un ejemplo de esto es la FNMT.

Si accedemos con este navegador a una página que está certificada por esta entidad nos aparece la siguiente pantalla.

	Esta conexion no esta vernicada
~2	Ha pedido a Firefox que se conecte de forma segura a de la constante de la conecte de la conecte de la cone 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.
	ISácame de aquí!
	Detalles técnicos
	Entiendo los riesgos

Para evitar esta pantalla debemos seguir los siguientes pasos:

- 1. Obtener el certificado de la entidad emisora
- 2. Implantarlo en nuestro navegador

El primer paso depende de la entidad emisora, vamos a suponer que tenemos en nuestro equipo un archivo .cer donde está el certificado que vamos a implantar.



Para el segundo paso abriremos el navegador Firefox, en el menú Herramientas pulsaremos en Opciones.

Opciones							×
		<u>م</u>		60		*	-
General	Pestanas	Contenido	Aplicaciones	Privacidad	Seguridad	Avanzado	

En la parte superior de la ventana haremos clic en Avanzado.

Aquí pulsaremos en la pestaña Cifrado.

Opciones						
		重页		90		÷
General	Pestañas	Contenido	Aplicaciones	Privacidad	Seguridad	Avanzado
General	Red Actualiz	ar Cifrado				
Protocol	los ———					
🔽 Usa	ar SSL <u>3</u> .0		V	Usar TLS <u>1</u> .0		
Certifica	ados					
Cuando	Cuando un servidor requiera mi certificado personal:					
O Seje	O Seleccionar uno automáticamente 💿 Preguntar siempre					
Ver cer	rtificado <u>s</u>	Listas de <u>r</u> evo	cación <u>V</u> alio	dación Dis	p <u>o</u> sitivos de s	eguridad

Y después en el botón Ver certificados.

Ahora nos encontramos dentro del Administrador de Certificados.

Administrador de certificados		_ 🗆
Sus certificados Personas Servidores Autoridades Otro	os	
Tiene certificados archivados que identifican a estas autorida	ades certificadoras:	
Nombre del certificado	Dispositivo de seguridad	E.
AddTrust Class 1 CA Root	Builtin Object Token	-
AddTrust External CA Root	Builtin Object Token	
AddTrust Public CA Root	Builtin Object Token	
AddTrust Qualified CA Root	Builtin Object Token	
🖃 America Online Inc.		
America Online Root Certification Authority 1	Builtin Object Token	
America Online Root Certification Authority 2	Builtin Object Token	
AOL Member CA	Disp. software de seguridad	
🖃 AOL Time Warner Inc.		
AOL Time Warner Root Certification Authority 1	Builtin Object Token	-
Ver Editar Importar Exportar	Elimina <u>r</u>	
		Aceptar

Para introducir un certificado de servidor nuevo, tendremos que hacer clic en la pestaña **Autoridades** y después pulsar el botón **importar.**

Se nos abrirá una ventana para elegir el fichero donde esta nuestro certificado, una vez seleccionado pulsaremos el botón **Abrir**.

Buscar en:	🚞 CEA FN	NMT	•	00	• 🖭 😢	
Documentos	E FNMTCla	ase2CA.cer				
Escritorio						
Dis Nis						
documentos Mi PC						
ي ا	81	1				Abria
Ais sitios de red	Nompre:	1				ADRI

A continuación nos aparecerá la siguiente pantalla:

Descargando certificado	×
Se le ha pedido que confíe en una nueva Autoridad Certificadora (CA).	
2Quiere conriar en "Autoridad certificadora (sin nombre)" para los siguientes propositos?	
Confiar en esta CA para identificar sitios web.	1
🔲 Confiar en esta CA para identificar usuarios de correo.	
🔲 Confiar en esta CA para identificar desarrolladores de software.	
Antes de confiar en esta CA para cualquier propósito, debe examinar el certificado, política y	
procedimientos de la CA (si estan disponibles).	
Ver Examinar certificado de CA	
Aceptar Cancelar	1

Como lo que nos interesa es identificar sitios web **marcaremos** el primer cuadro que tiene el texto: "**Confiar en esta CA para identificar sitios web**", y después pulsaremos el botón aceptar.

¿Quiere confiar en "Autoridad certificadora (sin nombre)" para los siguientes propósitos?
Confiar en esta CA para identificar sitios web.

Después volveremos a la pantalla anterior donde si nos movemos con la barra de desplazamiento deberemos ver el certificado que acabamos de implantar.

Nombre del certificado	Dispositivo de seguridad	₽		
MD5 Collisions Inc. (http://www.phreedom.org/md5)	Builtin Object Token			
Equifax Secure Global eBusiness CA-1	Builtin Object Token			
Equifax Secure eBusiness CA-1	Builtin Object Token			
E FNMT				
FNMT Clase 2 CA - FNMT	Disp. software de seguridad	-		
🖃 GeoTrust Inc.				
GeoTrust Global CA	Builtin Object Token			
GeoTrust Global CA 2	Builtin Object Token			
GeoTrust Universal CA	Builtin Object Token			
GeoTrust Universal CA 2	Builtin Object Token	-		
Ver Editar Importar Exportar	. Elimina <u>r</u>			

Para terminar pulsaremos el botón **aceptar** en el administrador de certificados, y una vez en la pantalla de opciones volveremos a pulsar el botón **aceptar**.

Si recargamos la primera página ya no nos debería salir el aviso inicial y podríamos entrar sin ningún problema.