Com configurar un client wireless en WinXP

WPA-EAPTLS supplicant

Afegim el certificat client al sistema

 \cdot Necessitem el fitxer .per i .p12 generats amb el OpenSSL o qualsevol entitat certificadora



· Instal·lem el certificat de l'entitat emisora: root.der, per fer-ho només hem de fer doble click sobre de la icona.



Un cop es prem "Instalar certificado..." ens surt un assistent que ens guia en com instal·lar el certificat, premem "siguiente" i ens surt aquesta pantalla:

Almacén de certificados		
os almacenes de certificados.	s son áreas del sistema donde s	se guardan los certificados.
Windows puede seleccion posible especificar una ub	nar automáticamente un almacé picación para <mark>e</mark> l certificado.	in de certificados, o bien es
O S <u>e</u> leccionar automát	ticamente el almacén de certific	ados en base al tipo de certific
⊙ <u>C</u> olocar todos los ce	ertificados en el siguiente almace	én
Almacén de certific	cados:	
Entidades emisora	as raíz de confianza	E <u>x</u> aminar

Tal com es veu en la captura, cal marcar la segona opció i despré s através de lo botó "Examinar..." cal seleccionar la opció "Entidades emisoras raíz de confianza". Després premem "Sieguiente" i finalment "Finalizar", llavors apareix el següent:

Adverte	ncia de seguridad 🛛 🔀
	Está a punto de instalar un certificado desde una autoridad de certificados (CA) que afirma representar a:
-	Client certificate
	Windows no puede validar que el certificado procede realmente de "Client certificate". Póngase en contacto con "Client certificate" para confirmar su origen. El siguiente número le ayudará en este proceso:
	Huella digital (sha1): E8C6E00B F9D31C88 CA6C2D4C CF7AD4B3 9C91F834
	Advertencia: Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer clic en "Sí", asume este riesgo.
	¿Desea instalar este certificado?
1	<u></u> №

On ens informa de les consequències del que estem fent, obviament cal que diguem que si perquè el certificat de client que instal·lem després sigui vàlid.

Amb això ja tenim instal·lat el certificat de l'entitat certificadora. Ara cal que instal·lem el certificat de client necessari per connectar-se a la xarxa inal·lambrica. Això ho començarem a fer amb un doble click sobre la icona: root.p12 i veurem:

sistente para importación de certificados	X
Archivo para importar	
Especifique el archivo que desea importar.	
Nombre de archivo:	
E:\certs\root.p12	
Intercambio de información personal: PKCS #12 (.PFX,.P12) Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B) Almacén de certificados en serie de Microsoft (.SST)	
< <u>Atrás</u> Siguien <u>te</u> > Car	ncelar

Anem a "Siguiente" i ens demana la paraula de pas (password) necessaria per desxifrar el fitxer que conté el certificat client per connectar-se al servidor, aquesta paraula de pas s'ha definit al generar els certificats:

ontraseña	
Para mantener la seguridad,	la clave privada se protege con una contraseña.
Escriba la contraseña para la	a dave privada.
<u>C</u> ontraseña:	

Habilitar protección se	oura de claves privadas. Si habilita esta opción, se le
Habilitar protección se avisará cada vez que	gura de claves privadas. Si habilita esta opción, se le la clave privada sea usada por una aplicación.
Habilitar protección se avisará cada vez que	egura de claves privadas. Si habilita esta opción, se le la clave privada sea usada por una aplicación. no exportable. Esto le permitirá hacer una copia de
Habilitar protección se avisará cada vez que Marcar esta dave com seguridad de las dave	egura de claves privadas. Si habilita esta opción, se le la clave privada sea usada por una aplicación. no exportable. Esto le permitirá hacer una copia de es o transportarlas en otro momento.
 <u>H</u>abilitar protección se avisará cada vez que <u>M</u>arcar esta dave com seguridad de las dave 	gura de claves privadas. Si habilita esta opción, se le la clave privada sea usada por una aplicación. no exportable. Esto le permitirá hacer una copia de es o transportarlas en otro momento.
Habilitar protección se avisará cada vez que Marcar esta dave com seguridad de las dave	egura de claves privadas. Si habilita esta opción, se le la clave privada sea usada por una aplicación. no exportable. Esto le permitirá hacer una copia de es o transportarlas en otro momento.

Després premem "Siguiente" i en la nova pantalla deixem seleccionada la opció per defecte i tornem a prema "Siguiente":

stente para importación de	e certificados
Los almacenes de certificados son	n áreas del sistema donde se guardan los certificados.
Windows puede seleccionar a posible especificar una ubicaci	utomáticamente un almacén de certificados, o bien es ión para el certificado.
Seleccionar automáticam	iente el almacén de certificados en base al tipo de certificado
O <u>C</u> olocar todos los certific Almacén de certificado	ados en el siguiente almacén s: Examinar
	< <u>A</u> trás Siguien <u>t</u> e > Cancelar

I després apretem "Finalizar".

Ara ja tenim tots els certificats instal·lats. Ara només cal configurar la connexió perquè usi aquest certificats.

Verificar la instal·lació dels certificats

Anem a "Inicio" després "Ejecutar..." i escribim "mmc" premem "Acpetar" i carreguem el "Microsoft Managment Console":

🚡 Consola1		
Ar <u>c</u> hivo <u>A</u> cción <u>V</u> er <u>F</u> avoritos Ve <u>n</u> ta	na Ayuda	
← → 🖪 😼 🔮		
🚡 Raíz de consola		
aiz de consola	Nombre	
	No hay elementos disponibles en esta vista.	
	4	

Ara anem a "Archivo" i seleccionem "Agregar o quitar complemento..." i apareix el següent:

Agregar o qui	tar complemento	? 🛛
Independiente	Extensiones	
Usar esta pági la consola. Co <u>m</u> plementos agregados a:	na para agregar o quitar un complemento inde	ependiente de
- Descripción		
Agregar	Quitar Acerca de	
	Acepta	r Cancelar

Ara premem "Agregar..." i apareix el següent, on seleccionem "Certificados" i premem "Aceptar":



Ara la pantalla del "mmc" queda com segueix i si seleccionem "Raiz de consola" exapandim "Personal" ara seleccionem "Certificados" i ens hauria d'apareixer el certificat "Cliente certificate", el segon certificat que hem instal·lat:

🚡 Consola1					<u>- 🗆 ×</u>
Archivo Acción Ver Eavoritos V ← → <	'e <u>n</u> tana Ay <u>u</u> da s: usuario actual∖	Personal\Certif	ficados		_ [] ×
🔲 Raíz de consola	Enviado a 🕢	Emitido por	Fecha de cad	Propósitos pl	Nombre descriptive
Certificados: usuario actual Personal Certificados Entidades emisoras raíz de co Confianza empresarial Dijeto de usuario de Active Dijeto de usuario de Active Certificados en los que no se Certificados en los que no se Autoridades de certificación Personas de confianza Solicitudes de inscripción de	Client certificate	Client certificate	24/01/2006	<todos></todos>	<ninguno></ninguno>
					•
El almacén Personal contiene un certific	ado.				

Si volem veure el certificat de l'entitat emisora (o sigui, el nostre OpenSSL) podem buscar-lo a: "Entidades emisoras raíz de.." i després "Certificados"

🚡 Consola1					<u> </u>
Archivo Acción ⊻er Eavoritos V Image: state st	entana Ayuda	Entidades emis	oras raíz de co	nfianza∖Certifi	cados
Raíz de consola	Enviado a 🛆	Emitido por	Fecha de cad	Propósitos pl	Nombre descrit
Certificados: usuario actual Personal Certificados Entidades emisoras raíz de co Confianza empresarial Entidades emisoras de cert. Endidades emisoras de cert. Endidades de confianza Certificados en los que no se Autoridades de confianza Personas de confianza Solicitudes de inscripción de	Image: Class 3 Primary Class 3 Public P Class 3 Public P Class 3 Public P Class 3 Primar	Class 3 Primary Class 3 Public Class 3 Public Class 3 Public	07/07/2019 02/08/2028 08/01/2004 07/07/2019	Correo segur Correo segur Correo segur Correo segur	CertPlus Class : VeriSign Class : VeriSign Class : CertPlus Class :
	Class 31'S Prima Client certificate Copyright (c) 1	Client certificate Copyright (c) Deutsche Tel	0//0//2019 24/01/2006 31/12/1999 10/07/2019	<todos> Impresión de</todos>	<pre><ninguno> Microsoft Time Deutsche Tele</ninguno></pre>
	Deutsche Tele DST (ANX Net DST (NRF) Roo	Deutsche Tel DST (ANX Net DST (NRF) Ro	10/07/2019 09/12/2018 08/12/2008	Correo segur Correo segur Correo segur	Deutsche Tele DST (ANX Net DST (National I
	DST (UPS) Roo DST RootCA X1	DST (UPS) Ro DST RootCA X1	07/12/2008 28/11/2008	Correo segur Correo seaur	DST (United P. DST RootCA X
El almacén Entidades emisoras raíz de co	onfianza contiene 108	certificados.			

Anem a veure les xarxes disponibles:



I ara apretem a: "Cambiar el orden de las redes preferidas"

General Redes inalámbricas	Opciones avanzadas
🔽 Usar <u>W</u> indows para estab	ecer mi configuración de red inalámbrica
Redes <u>d</u> isponibles:	
Haga clic en el siguiente bo redes inalámbricas o para o	tón para conectarse o desconectarse de btener más información acerca de ellas.
	Ver redes inalámbricas
Conectar automaticamente (Automático)	a redes disponibles en el orden siguiente: Subir Baiar
Agregar	al)
Obtener más información ac establecer una configuració	erca de cómo n de red inalámbrica. Opciones a <u>v</u> anzadas

Seleccionem la xarxa que en el llistat de xarxes ens indica que té l'WPA activat, normalment l'SSID ja ens sona ja que l'hem configurat nosaltres, no? Un cop seleccionada apretem "Propiedades" i deixem la pantalla de "Propiedades" tal com segueix:

come propiedades	? 🔀
Asociación Autenticación	Conexión
<u>N</u> ombre de red (SSID):	
Clave de red inalámbrica -	
Esta red requiere una clav	re para lo siguiente:
Autenticación de red:	WPA 😽
<u>C</u> ifrado de datos:	ТКІР
Clave de <u>r</u> ed:	0000050
Confirme la clave de red.	
Indice de clave (avanzadi ⊡ La cla <u>v</u> e la proporcioni	o): 1
Ésta es una red de equip puntos de acceso inalár	o a equipo (ad hoc). No se utilizan Ibrico
	Aceptar Cancelar

Canviem de pestanya i la deixem com segueix:

nin prop	viedades	? 2
Asociación	Autenticación	Conexión
Seleccione redes Ethe	e esta opción pa Imet inalámbrica	ra proporcionar acceso autenticado a s:
✓ <u>H</u> abilita	r la autenticació	n IEEE 802.1X en esta red
<u>T</u> ipo de EAP:	Tarjeta intelige	ente u otro certificado 🛛 💉
Autenti	car como equipo ble	Propiedades
Autentio equipo	car como in <u>v</u> itad no estén disponi	io cuando el usuario o la información de ibles
		Aceptar Cancelar

Premem "Propiedades" i deixem les opcions com la captura. És important seleccionar el certificat "Client certificate" que és el certificat que hem instal·lat anteriorment per connectar-nos al a xarxa. Si posteriorment la xarxa no us connectes podria ser que això no estigués ben seleccionat ja que si prems "Aceptar" a totes les opcions que hem obert fins ara no es guarda l'opció seleccionada.

Propiedades de tarjeta inteligente u otros certific 🕐 🔀
A conectar:
O Usar mi <u>t</u> arjeta inteligente
⊙ Usar un <u>c</u> ertificado en este equipo
Utilizar selección simple de certificado (se recomienda)
☑ Validar un certificado de servidor
Conectar a estos servidores:
Entidad emisora ra îz de confianza:
Class 2 Public Primary Certification Authority
Class 3 Primary CA
Class 3 Public Primary Certification Authority
Class 3P Primary CA
Class 515 Filmary CA
Deutsche Telekom Root CA 1
Deutsche Telekom Root CA 2
C
Ver certificado
Usar un nombre de usuario distinto para la conexión
Aceptar

Ara podem tornar a la pantalla incial, on hi havia el llistat de xarxes detectades i preme sobre la xarxa que volem connectar (xarxa amb autenticació WPA). I durant el procés de connexió podrem observar que ens apareix un "globus de text" prop del rellotge que ens informa sobre l'ús del certificat, doncs bé heu de premer sobre aquest "globus" i us apareixerà el següent:

La entidad emi	isora de certificación de raíz para el certificado de servidor
Clier	nt certificate
Haga clic en A	ceptar para conectarse si éste es el certificado correcto y
no volvera a v conexión.	er este mensaje. Haga clic en Cancelar para anular la
	Ver certificado de ceruidor
	Ver certificado de servidor
	Ver certificado de servidor

Com els missatge ens indica després de premer "Aceptar" ja no caldrà tornar a repetir aquest procés. Si tot va bé al cap de pocs segons estarem connectats a la xarxa de forma segura.