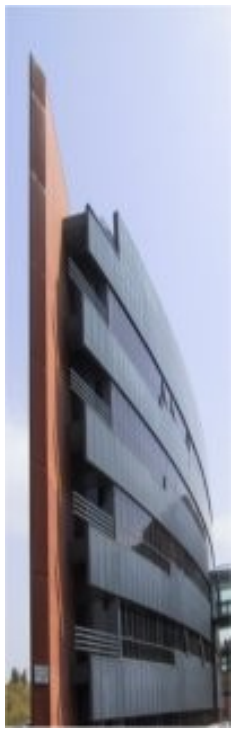
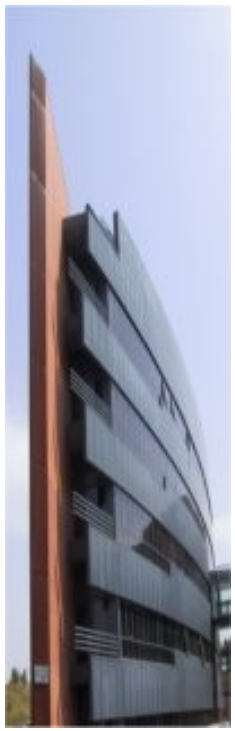
Configuración segura de SecureW2 en una organización Eduroam.

Nicolás Velázquez Campoy
Tecnologías de la Información
Universidad Autónoma de Madrid
XXIII GT – RedIRIS – 26 Jun. 2007



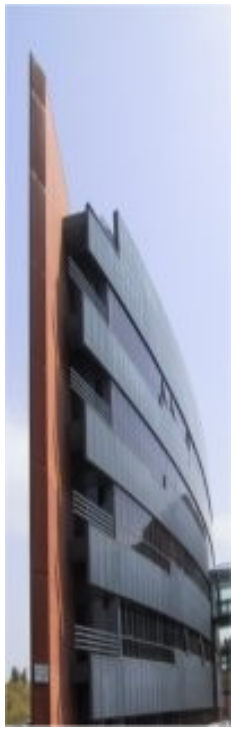
SecureW2 y EAP-TTLS.

- Índice.
  - Que es EAP.
  - Que es 802.1X
  - PEAP / TTLS.
  - SecureW2. Parámetros. Significado.
  - SCS.
  - EAP-TTLS y Man in the Middle.
  - SecureW2. Posibles configuraciones en una organización Eduroam.
  - Packs de instalación.
  - Certificados.
  - SecureW2. Conclusiones.
  - Otros clientes.
  - Referencias.



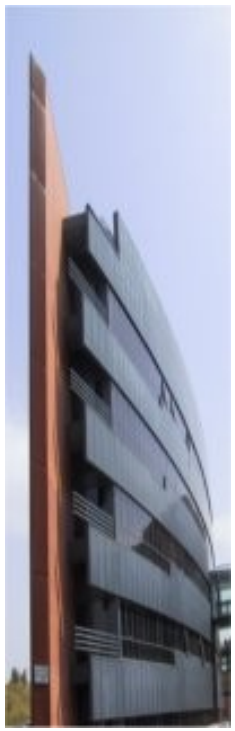
SecureW2 / EAP

- EAP es un “framework” de acceso validado a la red. A cualquier tipo de red. O sea, una arquitectura general sobre la que se definen diferentes tipos: TLS, TTLS, PEAP, GTC, etc.
- De forma general, significa que el usuario debe IDENTIFICARSE correctamente ANTES de ENTRAR.
- El proceso EAP es PREVIO A LA ENCRIPTACIÓN que mas tarde se pueda acordar (WPA, WPA2, etc.).
- De aquí que EAP requiera su propia forma de encriptación y comprobación de seguridad ante la captura de tráfico -> Man in the Middle.



EAP / 802.1X

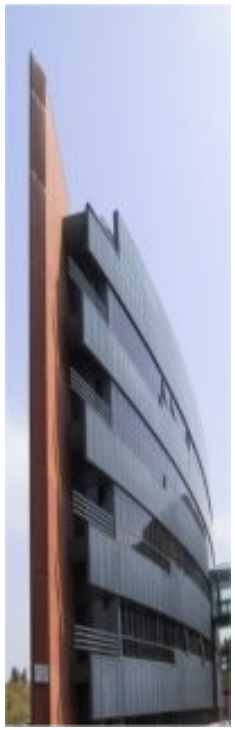
- 802.1X es EAPOL=EAP Over Lan. 802.1X engloba a EAP.
- 802.1X define roles de Suplicante/Cliente (SecureW2), Autenticador (Red Wireless o Wired) y Servidor de Autenticación (Radius).
- El Autenticador, la red inalámbrica en este caso, es un simple proxy. Así, aunque debe soportar 802.1X y EAP genéricos, no se requiere configurar un modo de EAP en la red inalámbrica.
- Redes inalámbricas: aparte de incluir EAP, 802.1X define.
  - Una serie de mensajes para facilitar la conexión.
  - Un procedimiento con el que el AP y el suplicante comparten y renuevan claves de encriptación.
- WEP+802.1X es muchísimo mejor que WPA2/PSK por la rotación de claves.



TTLS / PEAP Parecidos

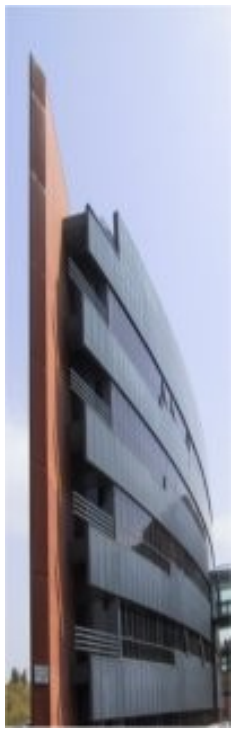
- Los dos son modos EAP:
  - TTLS es el modo 21
  - PEAP es el modo 25
- El modo de funcionamiento es muy, muy parecido.
  - Ambos establecen túnel TLS para ocultar usuario/password de ojos indiscretos.
  - Ambos establecen un método idéntico para que el cliente se asegure de que el usuario y la password se envían al radius adecuado

    -> Comprobación de certificados.



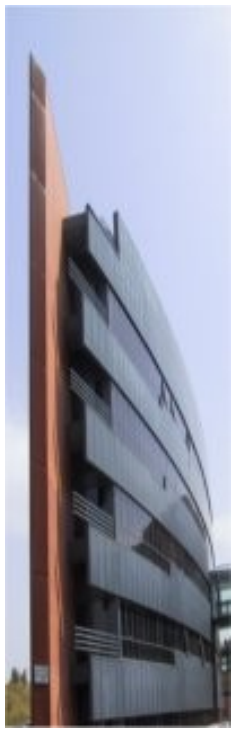
TTLS / PEAP Diferencias

- TTLS.
  - Mas flexible. Soporta mas formas de codificar o enviar usuario/password dentro del túnel: PAP, CHAP, MS-CHAP, MS-CHAP2, AVP, otros EAPs. Importante y muy útil si se tienen diferentes sistemas de validación de usuarios: LDAP, unix password, MS-AD.
    - Esas codificaciones han de ser soportadas por el cliente y por el radius.
  - Hay una implementación, SecureW2, muy interesante.
- PEAP.
  - Los SOs Microsoft incorporan cliente PEAP nativo.
  - Mas adecuado para entornos Microsoft.
  - Menos codificaciones.MS-CHAP2 es la mas extendida.
  - Incompatibilidad versiones Microsoft PEAPv0 y Cisco PEAPv1.
  - Microsoft dirige.



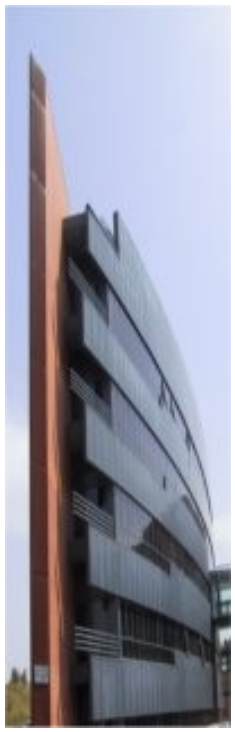
SecureW2 / EAP-TTLS (1/2)

- SecureW2 es una implementación de EAP-TTLS.
- Puede hacer uso de ciertas características de EAP-TTLS e ignorar otras, según se configure.
- Permite hacer packs de instalación preconfigurados por los administradores con:
  - Instalación de claves públicas,
  - Menús de selección (NSI) y
  - Asignación de perfiles: actualizaciones, SSIDs, wireless, wired, encriptación, etc.
- SecureW2 decide, también, sobre cuestiones anejas que no tienen que ver estrictamente con EAP-TTLS.
  - Donde almacenar y de donde leer claves públicas.
  - Que comprobar en las claves y como verificarlas.
  - Como componer las identities.



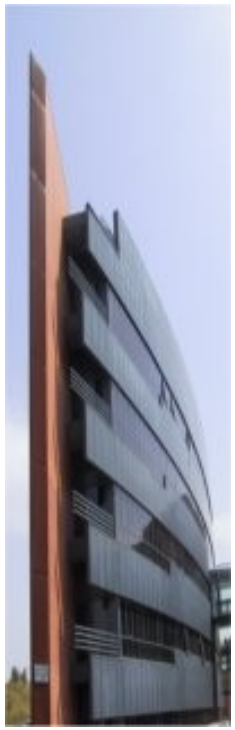
SecureW2 / EAP-TTLS (2/2)

- Parámetros básicos de SecureW2/EAP-TTLS desde la parte del cliente.
  - Outer identity -> Se solicita clave pública del radius con el que se va a establecer el túnel TLS. Se transmite en claro sin encriptar.
  - Certificados y CAs -> Almacenamiento de claves públicas en el cliente para verificar si realmente es nuestro radius el que contesta y con el que vamos a establecer el túnel.
  - Inner identity (código de usuario)/ Password -> Elementos a proteger con el túnel TLS.
- Por cada uno de los parámetros, veamos a continuación cuantas formas de generarlos hay y sus interrelaciones en SecureW2.

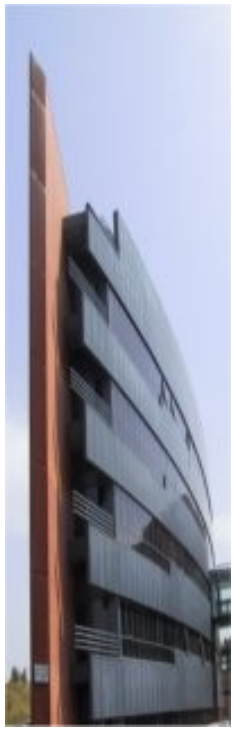


SecureW2 / Passw e Inner Identity

- Password: Es lo que queremos que vaya encriptado con un túnel TLS usando la clave pública del radius de nuestra organización para que solo la vea él.
- Inner Identity: Código de usuario.
  - Irá encriptada.
  - Volverá en claro sin encriptar asociada a un OK o un REJECT.
  - Dos formatos. Es lo que el usuario final escribe:
    1. usuario
    2. usuario@dominio
  - Por cortesía hacia la organización visitada y para una mas correcta generación de la Outer Identity, que se describe mas adelante, es recomendable que sea de la forma usuario@dominio en todos los casos.
  - La parte @dominio de la Inner Identity se puede utilizar para componer la Outer Identity.

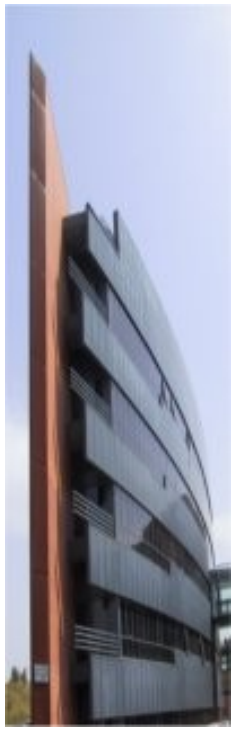


SecureW2 / Pantalla Inner Identity



SecureW2 / Outer Identity

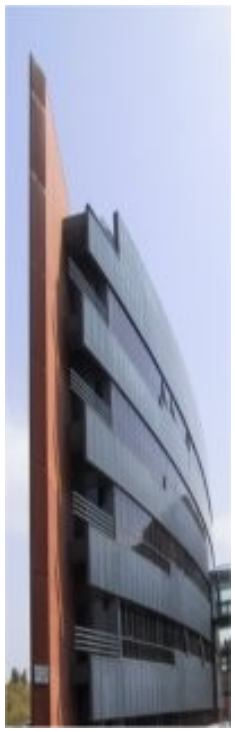
- El cliente pide a la red que le haga llegar la clave pública del radius con el que se va a establecer el túnel TLS.
- Su único campo válido y a ser tenido en cuenta es @dominio.
- No lleva asociada password ni va encriptada en modo alguno.
- Debe ser anónima. No debe ser igual a la Inner. Bastaría con un analizador para obtener códigos de usuario.
- En la 3.2.0 se aplica el RFC 4282.
  - El RFC 4282 indica que el código de usuario, en este caso, debe ser campo vacío.
  - -> aparecen problemas con el stripping de freeradius y en Mobile usando SecureW2 3.2.0 que no aparecían en 3.1.2.



SecureW2/Pant Outer Identity (1/4)

- Varios formatos:
  1. Outer IGUAL Inner -> NO RECOMENDABLE. Además vulnera el RFC 4282.
     - Se consigue desmarcando la opción de *Alternate Outer Identity* en SecureW2.

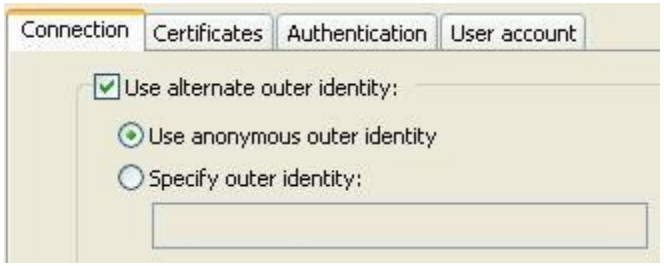
Bastaría con un analizador de red capturando paquetes para obtener códigos de usuario correctos.

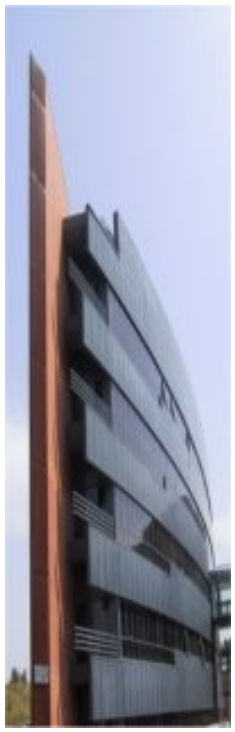


SecureW2/Pant Outer Identity (2/4)

1. Outer compuesta de forma automática por el SecureW2 usando anonymous (3.1.2) o campo vacío (3.2.0) y el @dominio que el usuario final ponga en la Inner. Recomendada.
   - Se consigue marcando *Alternate Outer Identity* y la opción *Use Anonymous Outer Identity*.

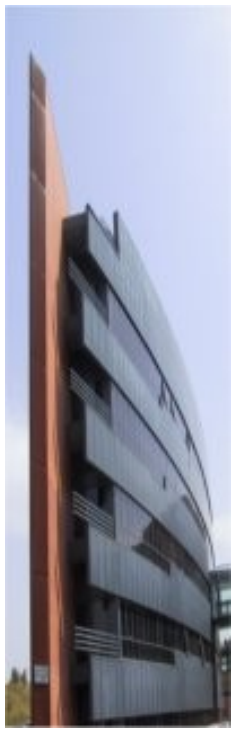
Una captura con un analizador solo obtiene montones de anonymous@dominio.





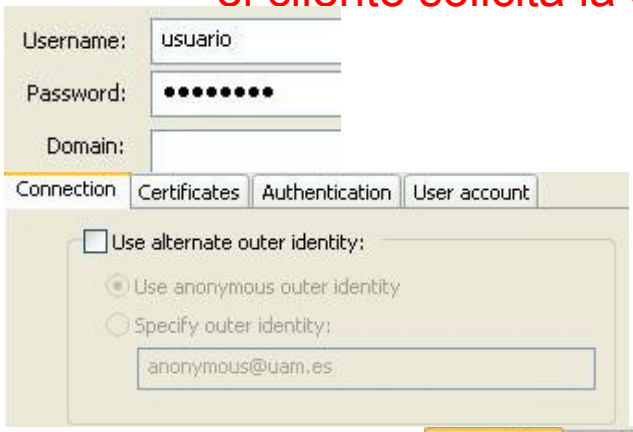
SecureW2/Pant Outer Identity (3/4)

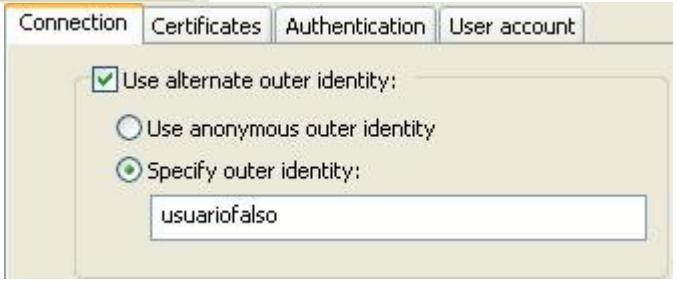
1. Outer fija e independiente de Inner.
   - Se consigue marcando *Alternate Outer Identity* y la opción *Specify Outer Identiy*. Además hay que rellenar el casillero poniendo un valor fijo, pepe@dominio, nadie@dominio, usuariofalso@dominio.
   - A veces inevitable (Mobile y 3.2.0) pero no es la mejor.

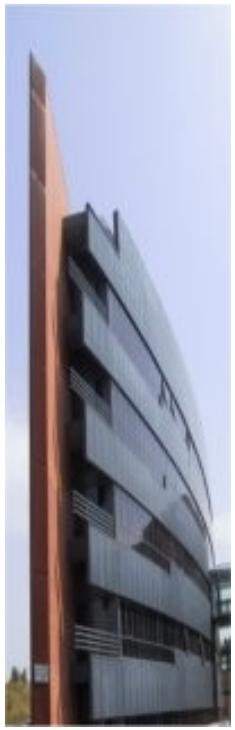


SecureW2/Pant Outer Identity (4/4)

- Outer sin @dominio. El usuario final no le pone @dominio a su código de usuario, o bien tenemos una Outer fija mal escrita; *anonymous* en vez de el mas correcto *anonymous@dominio*. El significado, en este caso, es que el cliente solicita la clave pública del radius mas cercano.

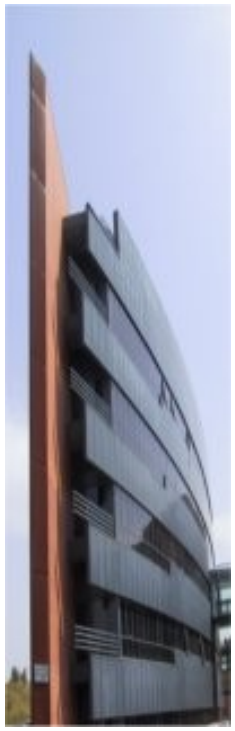






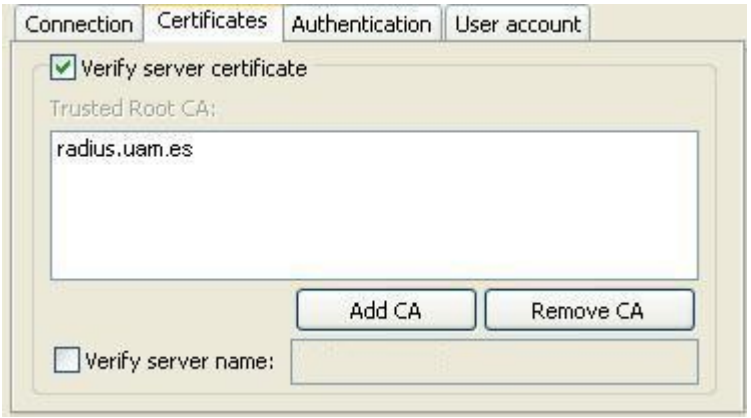
SecureW2 / Certificados

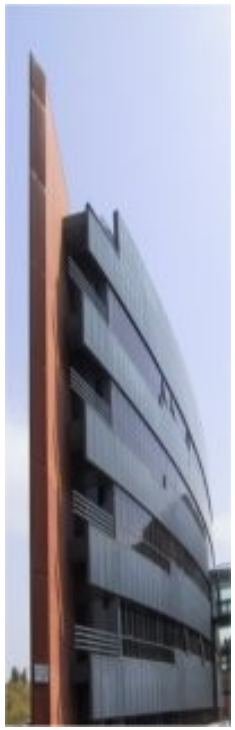
- El cliente SecureW2 / TTLS puede o no, a demanda del usuario o del administrador, verificar que el radius con el que va a tunelar o encriptar la Inner Identity y la Password es VERDADERAMENTE SU RADIUS.
- La verificación se realiza comparando las claves públicas que almacena el cliente con las que le llegan por la red al cliente como resultado de la Outer Identity que emitió.



SecureW2 / Pant Certificados (1/4)

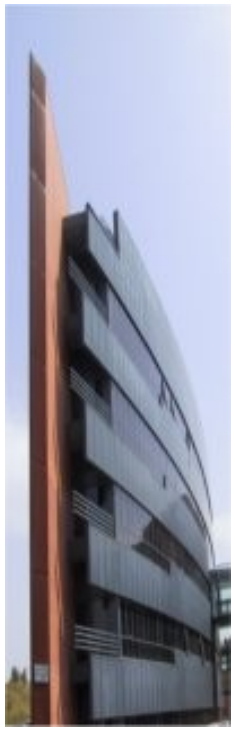
- Esto se puede hacer de varias formas:
  - El cliente lleva consigo la clave pública de *SU* radius para comparar.
    - Problemas si el periodo de validez de la clave pública es corto o hay varias máquinas con sus claves públicas en juego.





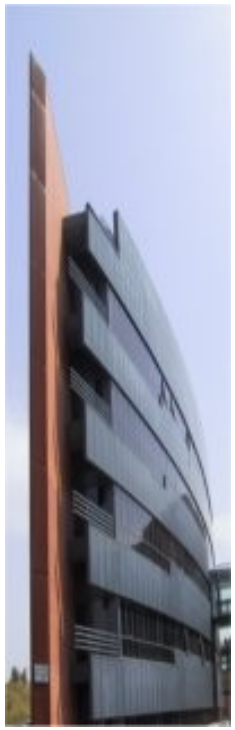
SecureW2 / Certificados (2/4)

1. El cliente lleva consigo las claves públicas de la cadena de CAs para comparar. Mas general.



SecureW2 / Pant Certificados (3/4)

1. El cliente lleva las claves públicas de la Cadena de CAs y comprueba, además, el nombre de máquina, o el dominio. Mejor que el caso 2 y sigue manteniendo la generalidad. RECOMENDADA.

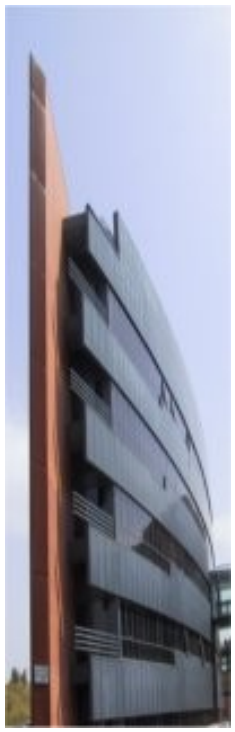


SecureW2 / Pant Certificados (4/4)

1. El cliente lleva las claves públicas de la Cadena de CAs y, además, la clave pública de su radius. Redundante y con los mismos problemas que el caso 1.

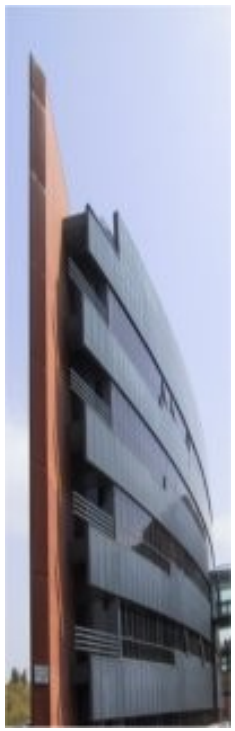
O

+



SecureW2 / SCS (1/2)

- SCS es una iniciativa de TERENA y varios NRENs que proporciona certificados:
  - De una root CA acreditada por WebTrust.
  - Para servidores corporativos.
  - De instituciones académicas y de investigación europeas.
- Con el objeto de:
  - Facilitar el uso de canales seguros.
  - Simplificar el uso de firmas digitales en los clientes. La root CA, GlobalSign, es una de las que Microsoft mantiene actualizada en sus sistemas operativos.

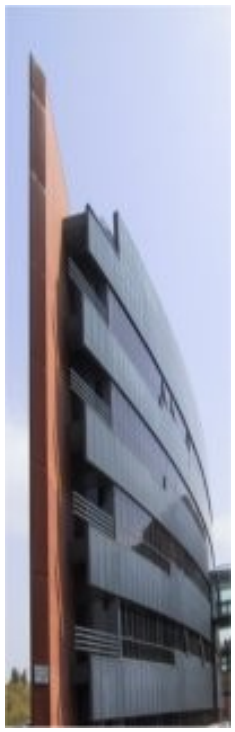


SecureW2 / SCS (2/2)

- Por tanto, ahora mismo, muchas organizaciones Eduroam europeas y en el futuro, muchas mas, tendrán certificados firmados por la misma root CA y CA intermedia.
- Uno de los objetivos es que si el servidor presenta toda la cadena de certificados:

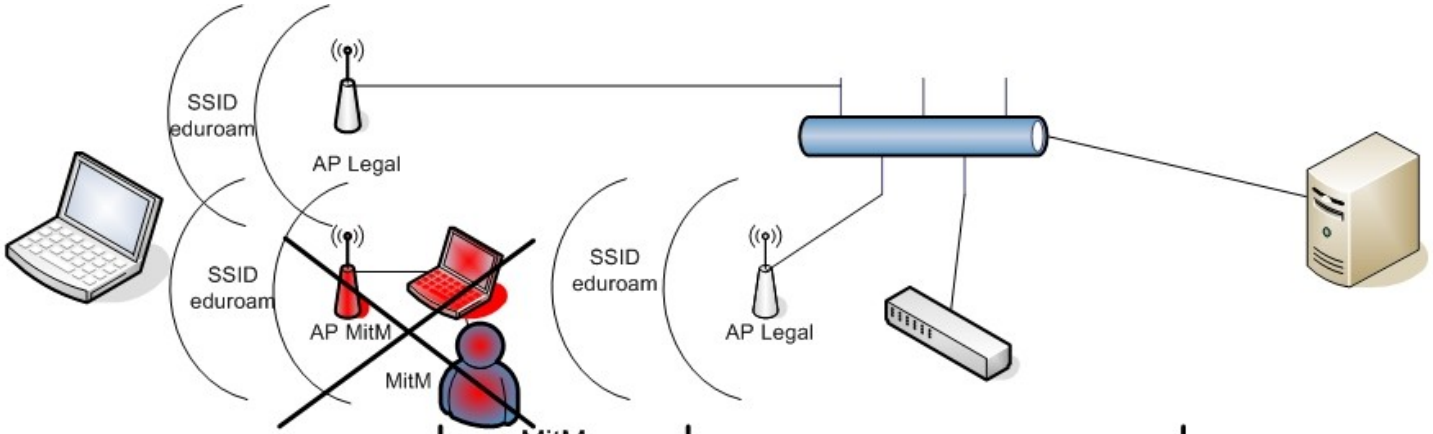
  serv + int CA + int CA + ….. + root CA

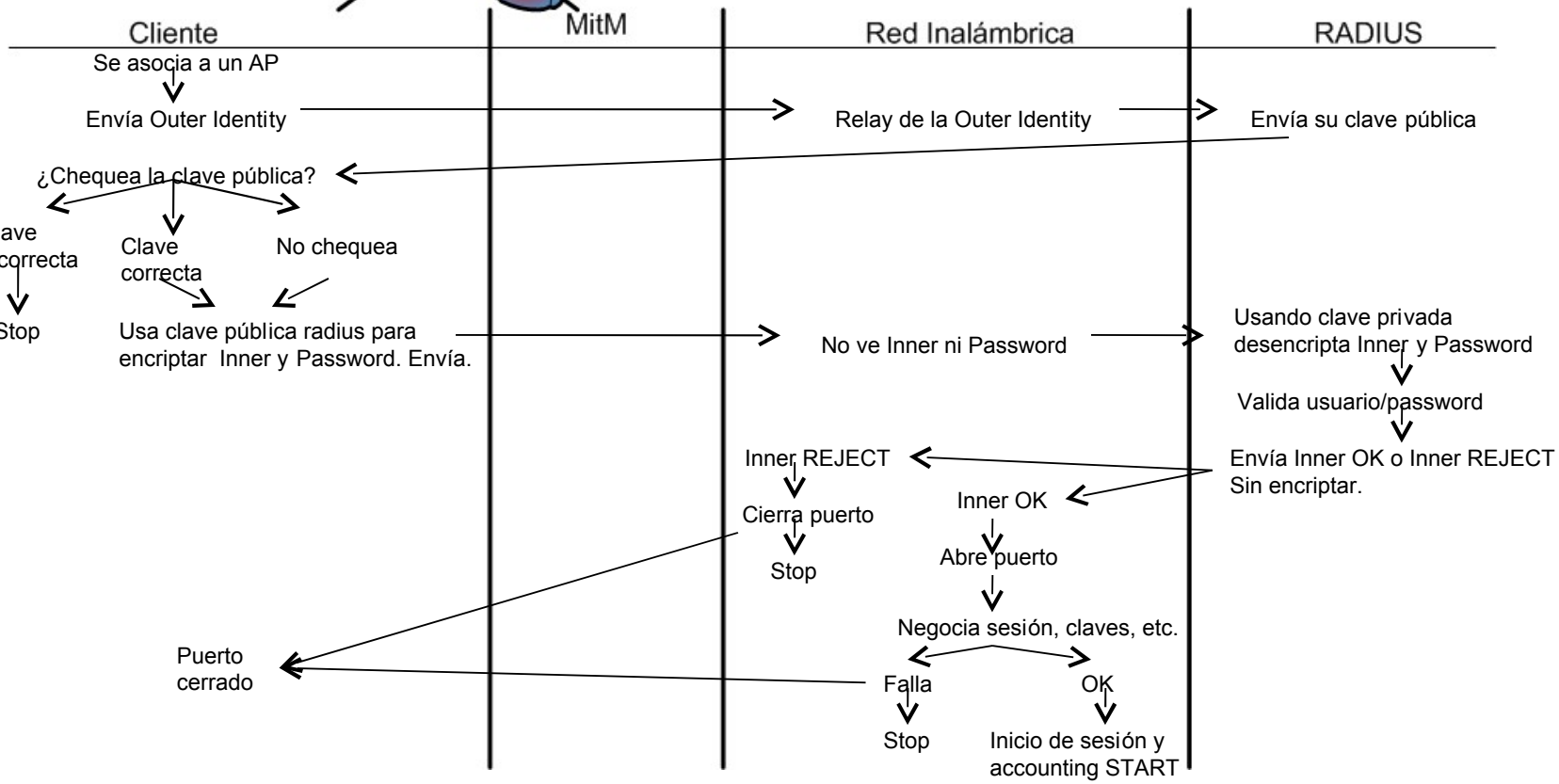
  el cliente puede verificar toda la cadena con solo conocer la clave pública de la root CA. Si esa root CA es una de las que Microsoft incorpora en sus SOs, todo es mucho mas fácil, y no le aparecen al usuario mensajes de petición de aceptación de certificados.

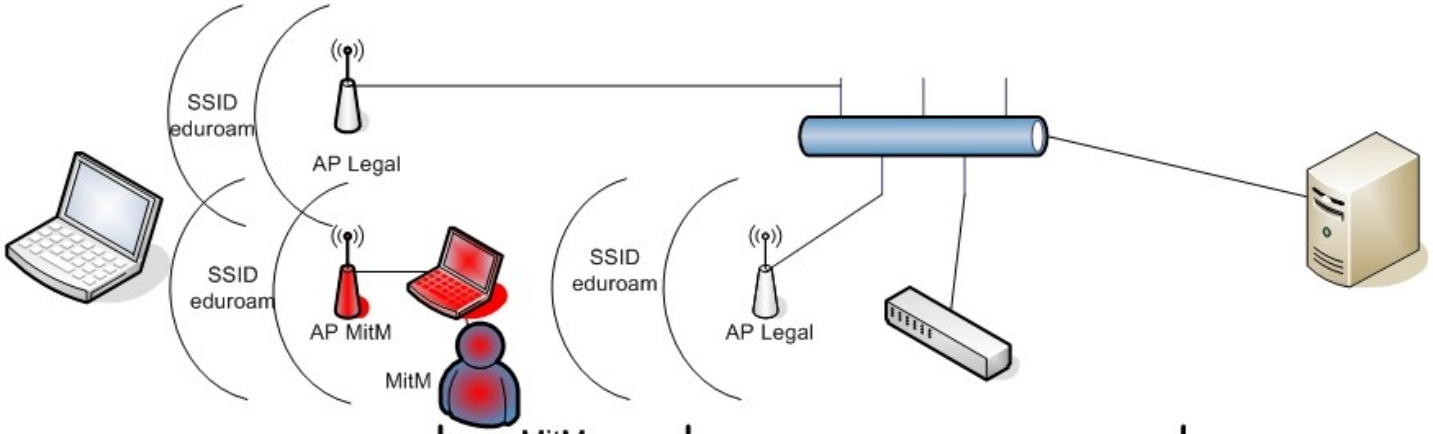


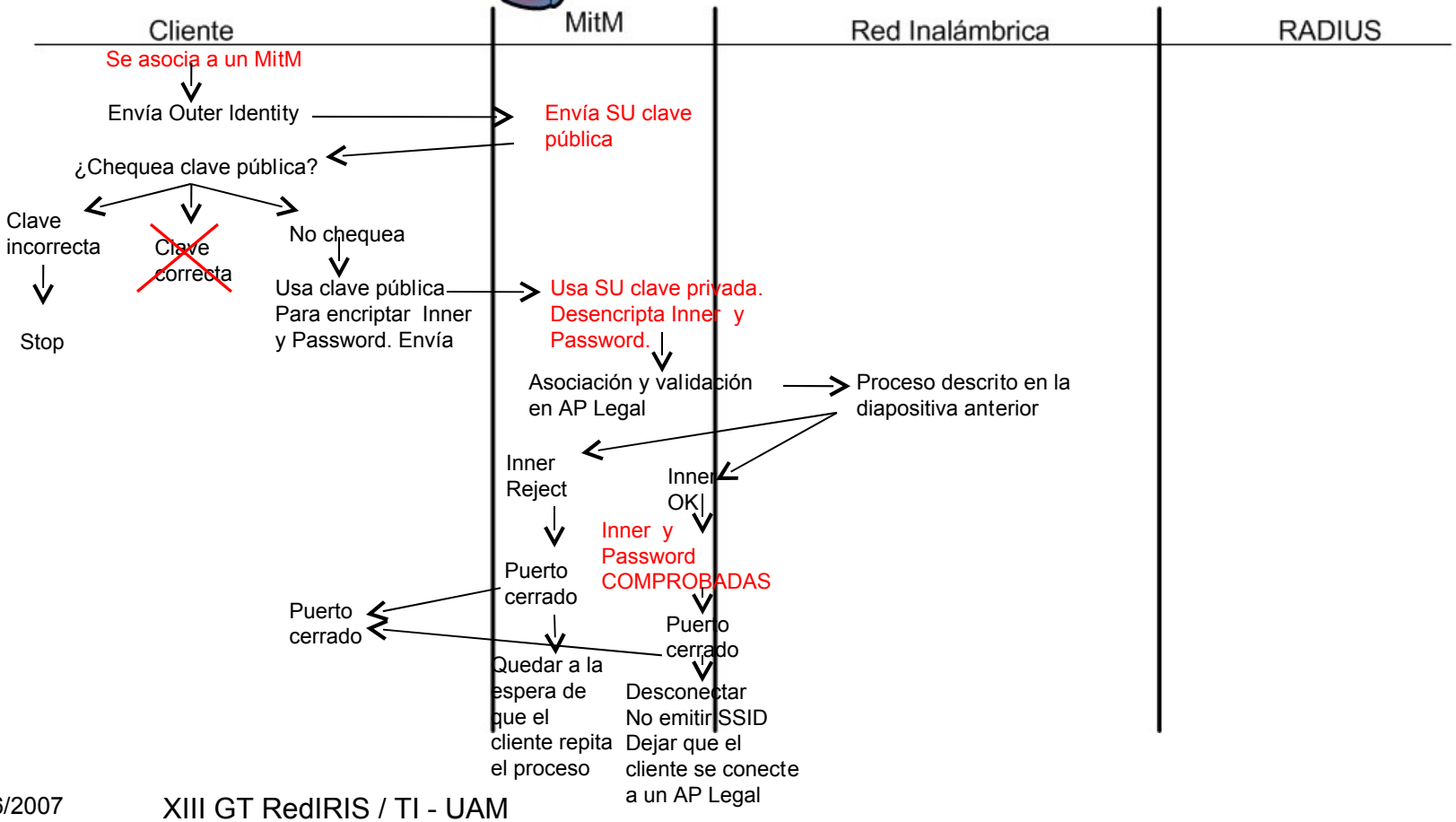
EAP-TTLS / MitM

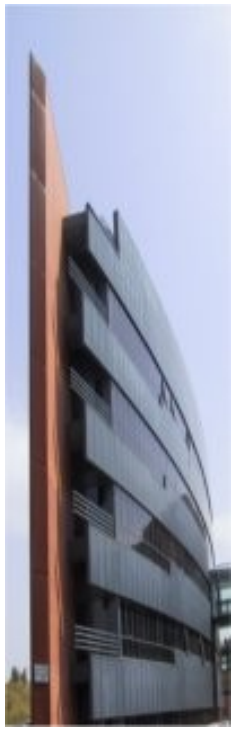
- Veamos como, EAP-TTLS, correctamente usado, protege a los usuarios de un ataque Man in the Middle.
  1. Conexión legal.
  2. Conexión con un MitM.


SSID
eduroam
AP Legal
SSID
eduroam
AP MitM
MitM
SSID
eduroam
AP Legal


Cliente
MitM
Red Inalámbrica
RADIUS
Se asocia a un AP
Envía Outer Identity
Relay de la Outer Identity
Envía su clave pública
¿Chequea la clave pública?
Clave incorrecta
Clave correcta
No chequea
Stop
Usa clave pública radius para encriptar Inner y Password. Envía.
No ve Inner ni Password
Usando clave privada desencripta Inner y Password
Valida usuario/password
Envía Inner OK o Inner REJECT Sin encriptar.
Inner REJECT
Cierra puerto
Stop
Inner OK
Abre puerto
Negocia sesión, claves, etc.
Puerto cerrado
Falla
OK
Stop
Inicio de sesión y accounting START

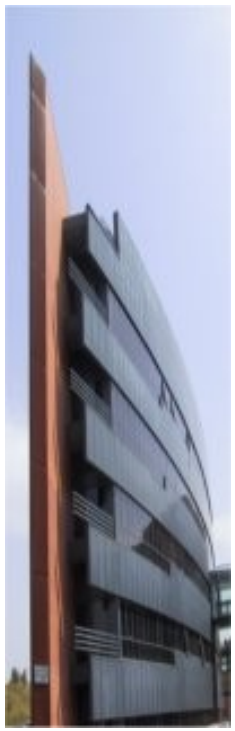

SSID
eduroam
AP Legal
SSID
eduroam
AP MitM
MitM
SSID
eduroam
AP Legal


Cliente
MitM
Red Inalámbrica
RADIUS
Se asocia a un MitM
Envía Outer Identity
Envía SU clave pública
¿Chequea clave pública?
Clave incorrecta
Clave correcta
No chequea
Stop
Usa clave pública Para encriptar Inner y Password. Envía
Usa SU clave privada. Desencripta Inner y Password.
Asociación y validación en AP Legal
Proceso descrito en la diapositiva anterior
Inner Reject
Inner OK
Inner y Password COMPROBADAS
Puerto cerrado
Puerto cerrado
Puerto cerrado
Quedar a la espera de que el cliente repita el proceso
Desconectar
No emitir SSID
Dejar que el cliente se conecte a un AP Legal



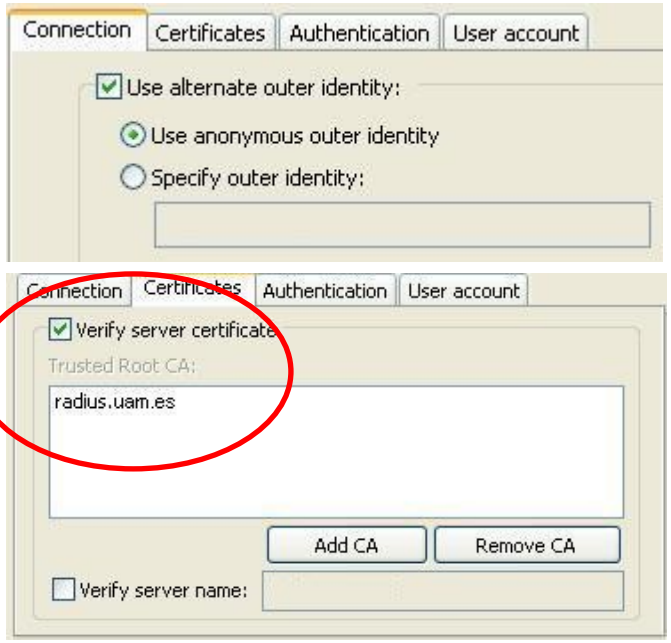
SecureW2 / Eduroam

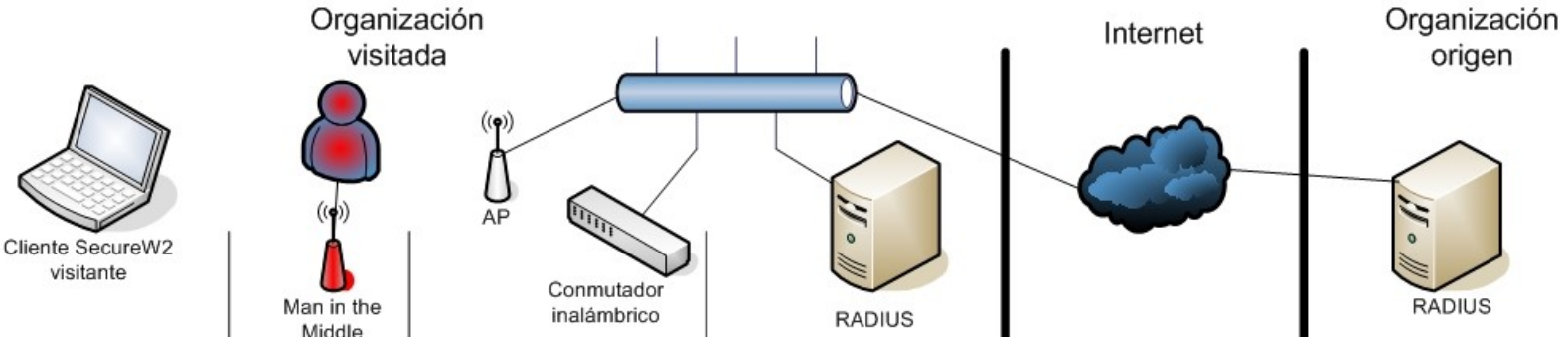
- Veamos ahora los diferentes escenarios que hay en organizaciones Eduroam.
- Supondremos, como caso mas general, que el cliente es un visitante de otra organización Eduroam.
- Indicaremos que elementos del árbol “legal” de Eduroam pueden ver el código de usuario/contraseña.
- Y, para completar, veremos que necesita un MitM, en cada caso, para capturar usuario/password.
- *Identifique cual es el escenario de su organización*.



SecureW2 / Clave de radius

- Outer Identity correcta -> se pide clave pública de nuestro radius.
- Se verifica que la clave pública que se recibe es la de nuestro radius.

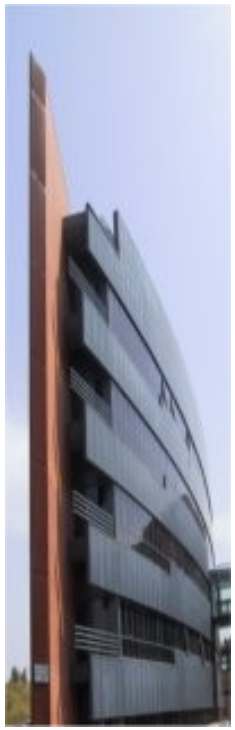




SeureW2 dispone de la clave pública de su radius de origen					
Envía Outer Identity correcta. Sin encriptar.		Proxy de la Outer Identity	Ignora usuario. Procesa @dominio. Si el dominio es propio, procesa.		
			Si el dominio es externo hace proxy de la Outer. Sin encriptar.	Hace proxy de la Outer. Sin encriptar.	radius de la organización @dominio recibe Outer.
					Envía su clave pública.
Recibe clave pública radius. Verifica coincidencia.					
Si no coincide, abortar. Si coincide, emplear para encriptar Inner y Password	*No puede capturar passwords. Cualquier modificación de los intercambios aborta el acceso.*	Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Desencripta Inner y Password.
					Verifica usuario / password.
					Envía Inner OK o Inner REJECT. Sin encriptar. No se envía password.
		Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	
		Si Inner OK, abre puerto, negocia sesión y START al accounting si todo va bien.			

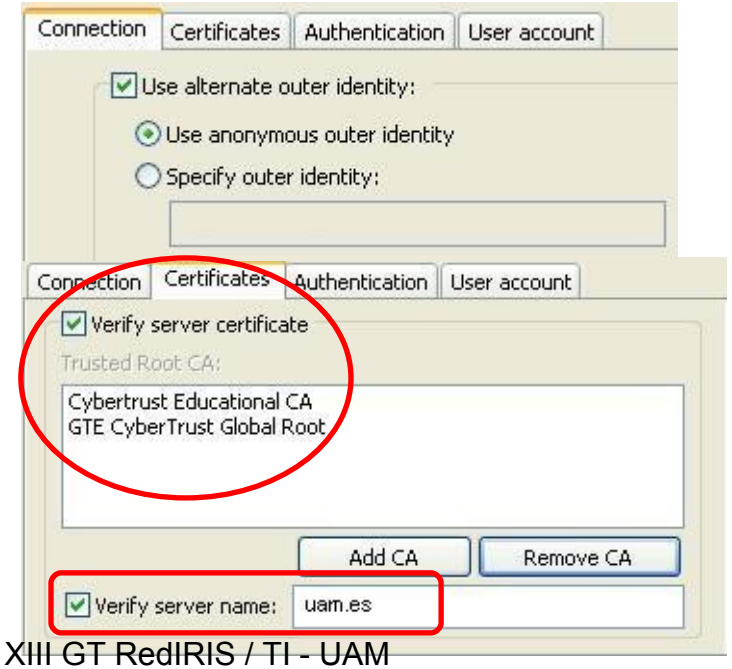
¿Qué máquinas legales Eduroam pueden llegar a ver la password? Solo el cliente y el radius de la organización de origen.

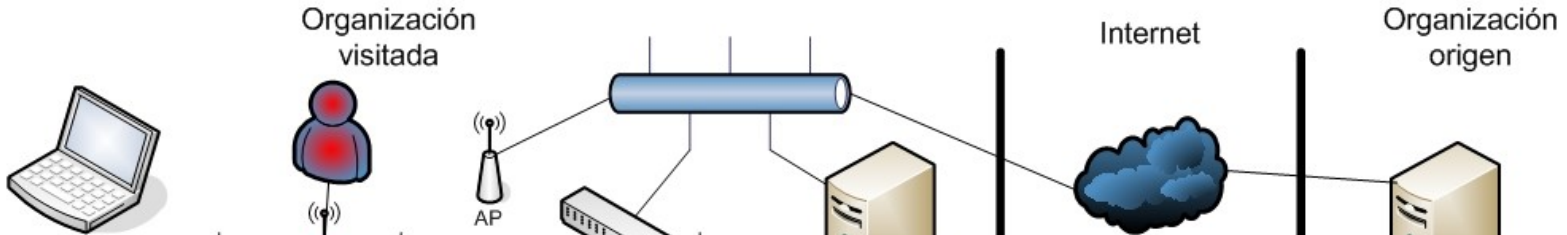
¿Qué necesita un MitM para capturar la password? La clave privada del radius de origen.



SecureW2 / Cadena CAs y Nombre

- Outer Identity correcta -> se pide clave pública de nuestro radius.
- Se verifica clave pública de las CAs que firman la clave pública de nuestro radius.
- Y se comprueba si el cn, common name, es uno concreto, radius.dominio o es mas general, dominio





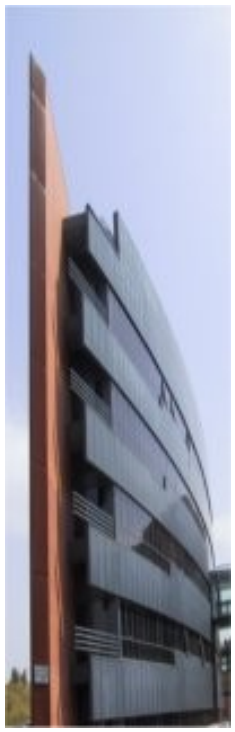
SeureW2 dispone de la cadena de CAs que firman la clave pública de su radius de origen y del nombre* o dominio** del radius					
Envía Outer Identity correcta. Sin encriptar.		Proxy de la Outer Identity	Ignora usuario. Procesa @dominio. Si el dominio es propio, procesa.		
			Si el dominio es externo hace proxy de la Outer. Sin encriptar.	Hace proxy de la Outer. Sin encriptar.	radius de la organización @dominio recibe Outer.
					Envía su clave pública.
Recibe clave pública radius. Verifica CAs firmantes y nombre.					
Si no coincide, abortar. Si coincide, emplear para encriptar Inner y Password	*No puede capturar passwords. Cualquier modificación de los intercambios aborta el acceso.*	Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Desencripta Inner y Password.
					Verifica usuario / password.
					Envía Inner OK o Inner REJECT. Sin encriptar. No se envía password.
		Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	
		Si Inner OK, abre puerto, negocia sesión y START al accounting si todo va bien.			

¿Qué máquinas legales Eduroam pueden llegar a ver la password?

Solo el cliente y el radius de la organización de origen.

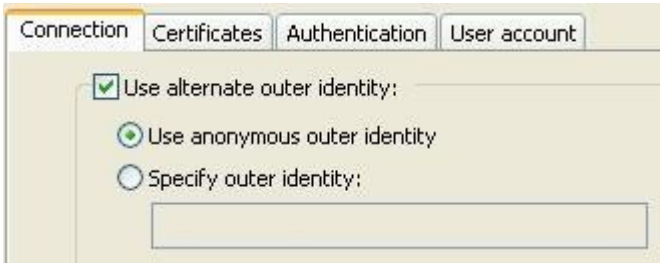
¿Qué necesita un MitM para capturar la password?

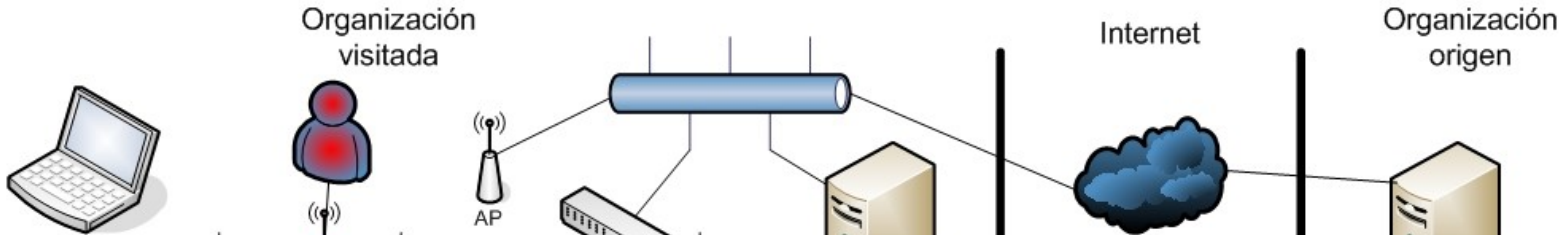
La clave privada del radius* o de alguna máquina del mismo dominio**, cuya clave pública esté firmada por las mismas CAs.



SecureW2 / Cadena de CAs

- Outer Identity correcta -> se pide clave pública de nuestro radius.
- Se verifica clave pública de las CAs que firman la clave pública de nuestro radius.



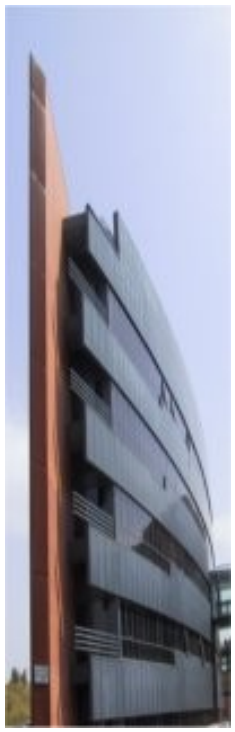


SeureW2 dispone de la cadena de CAs que firman la clave pública de su radius de origen					
Envía Outer Identity correcta. Sin encriptar.		Proxy de la Outer Identity	Ignora usuario. Procesa @dominio. Si el dominio es propio, procesa.		
			Si el dominio es externo hace proxy de la Outer. Sin encriptar.	Hace proxy de la Outer. Sin encriptar.	radius de la organización @dominio recibe Outer.
					Envía su clave pública.
Recibe clave pública radius. Verifica CAs firmantes.					
Si no coincide, abortar. Si coincide, emplear para encriptar Inner y Password		Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Desencripta Inner y Password.
					Verifica usuario / password.
					Envía Inner OK o Inner REJECT. Sin encriptar. No se envía password.
		Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	
		Si Inner OK, abre puerto, negocia sesión y START al accounting si todo va bien.			

Extremadamente difícil. Debe disponer de una clave privada de otra organización con certificados SCS.

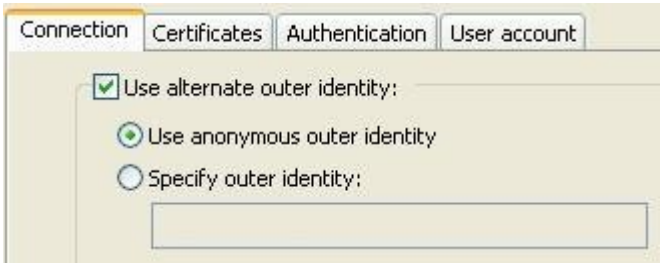
¿Qué máquinas legales Eduroam pueden llegar a ver la password? Solo el cliente y el radius de la organización de origen.

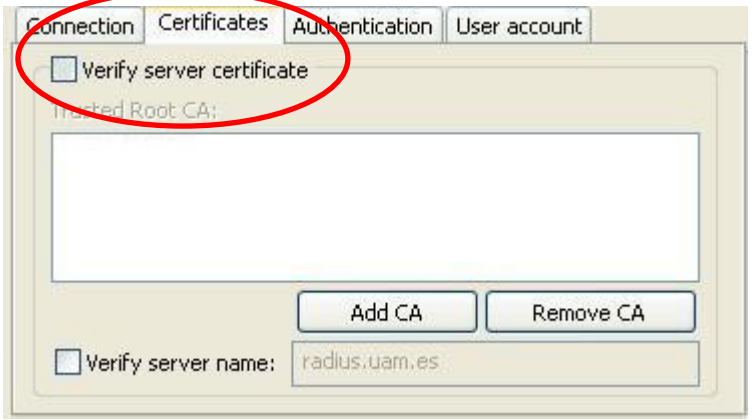
¿Qué necesita un MitM para capturar la password? La clave privada de alguna máquina cuya clave pública esté firmada por las mismas CAs -> Proyecto europeo SCS.

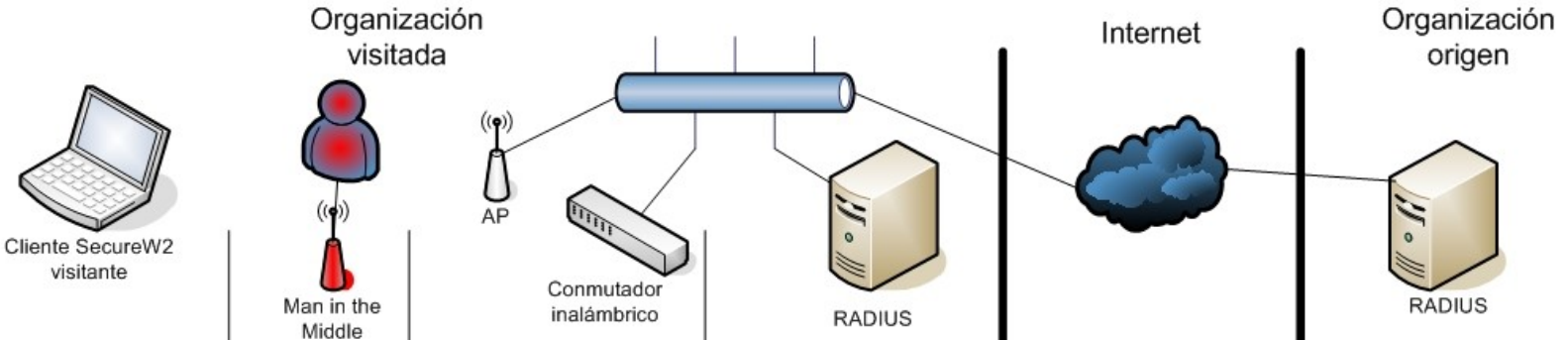


SecureW2 / No verifica

- Outer Identity correcta -> pedimos clave pública de nuestro radius.
- No se verifica nada de la clave pública que nos llega.





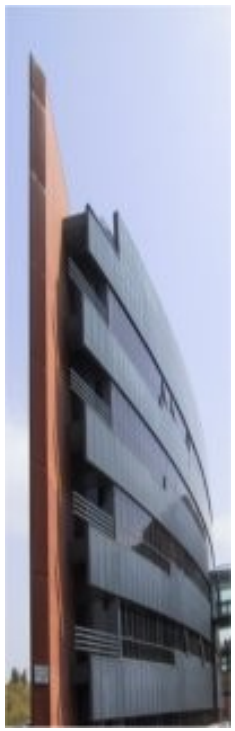


SecureW2 no dispone de ninguna clave pública.					
Envía Outer Identity correcta. Sin encriptar.		Proxy de la Outer Identity	Ignora usuario. Procesa @dominio. Si el dominio es propio, procesa.		
			Si el dominio es externo hace proxy de la Outer. Sin encriptar.	Hace proxy de la Outer. Sin encriptar.	radius de la organización @dominio recibe Outer.
					Envía su clave pública.
Recibe clave pública radius. No verifica nada.					
Emplea clave pública para encriptar Inner y Password		Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Inner y Password en túnel TLS. No se ven	Desencripta Inner y Password.
					Verifica usuario / password.
					Envía Inner OK o Inner REJECT. Sin encriptar. No se envía password.
		Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	
		Si Inner OK, abre puerto, negocia sesión y START al accounting si todo va bien.			

Puede capturar passwords configurando casi de cualquier manera el software.

¿Qué máquinas legales Eduroam pueden llegar a ver la password? El cliente y el radius de la organización de origen.

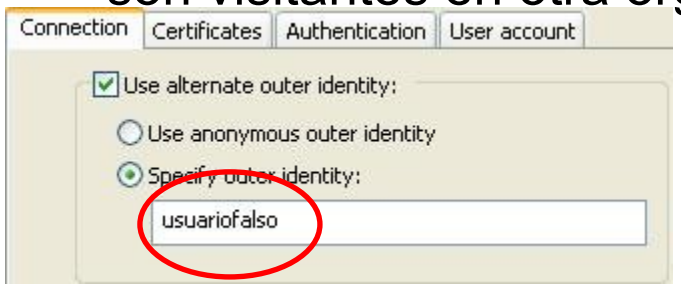
¿Qué necesita un MitM para capturar la password? La clave privada y pública que quiera.

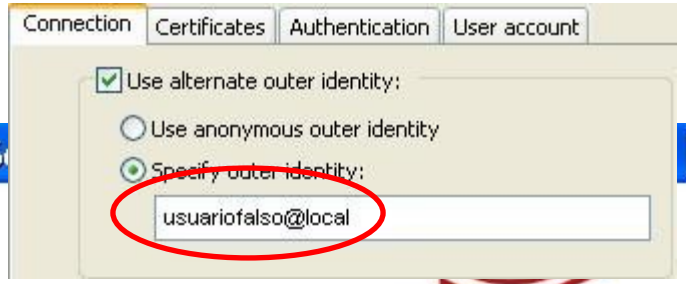


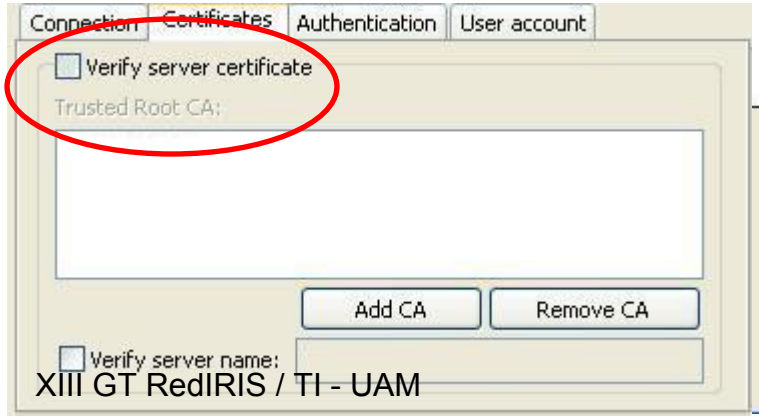
SecureW2 / PI

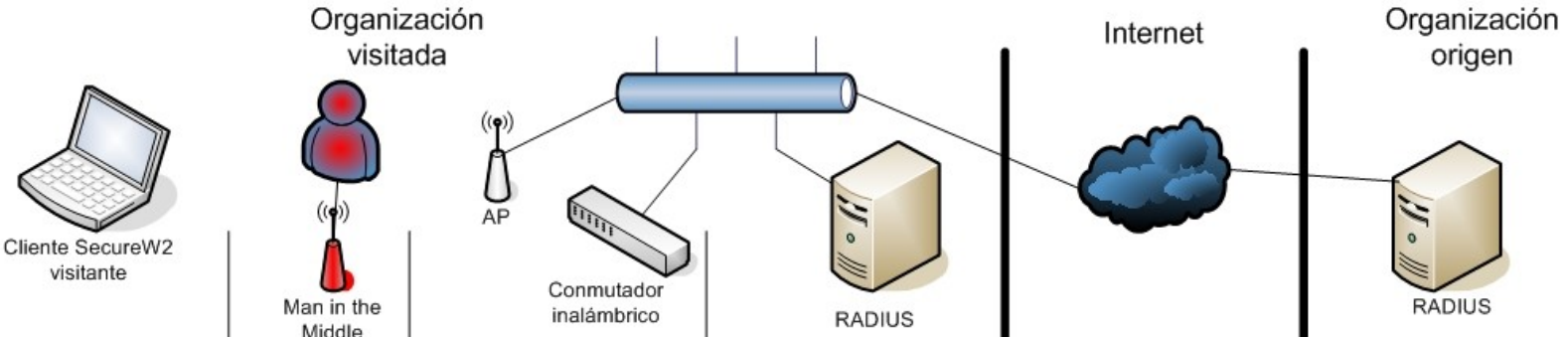
- Outer Identity incorrecta, *usuario* en vez de *usuario@dominio*

  -> pedimos clave pública del radius mas cercano.
- Esta configuración OBLIGA a nuestros usuarios, cuando son visitantes en otra organización, a NO VERIFICAR







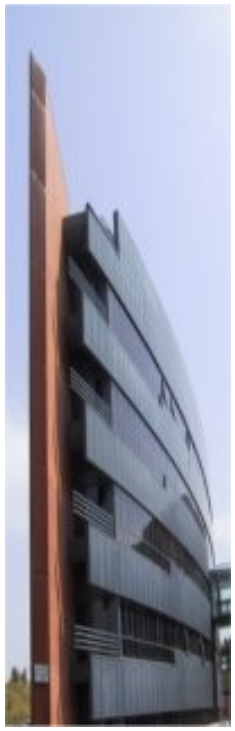


SecureW2 no dispone de ninguna clave pública.					
Envía Outer Identity local o sin dominio. Sin encriptar.		Proxy de la Outer Identity	Ignora usuario. Procesa @dominio. El dominio es propio.		
			Envía su clave pública.		
Recibe clave pública radius. No verifica nada.					
Emplea clave pública para encriptar Inner y Password		Inner y Password en túnel TLS. No se ven	Desencripta Inner y Password. Ve que es externo y reenvía sin encriptar	Inner y Password sin Encriptar. Se ven.	Verifica usuario / password.
					Envía Inner OK o Inner REJECT. Sin encriptar. No se envía password.
		Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	Se ve Inner OK o REJECT.	
		Si Inner OK, abre puerto, negocia sesión y START al accounting si todo va bien.			

Puede capturar passwords configurando casi de cualquier manera el software.

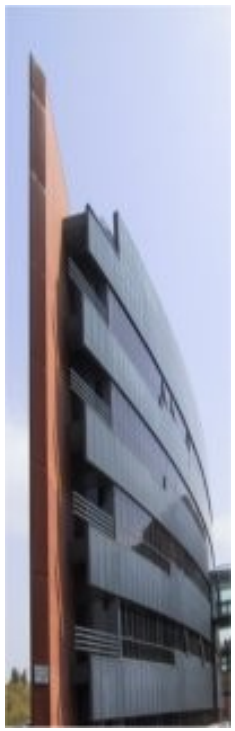
¿Qué máquinas legales Eduroam pueden llegar a ver la password? El cliente y todos los radius hasta la organización de origen.

¿Qué necesita un MitM para capturar la password? La clave privada y pública que quiera.



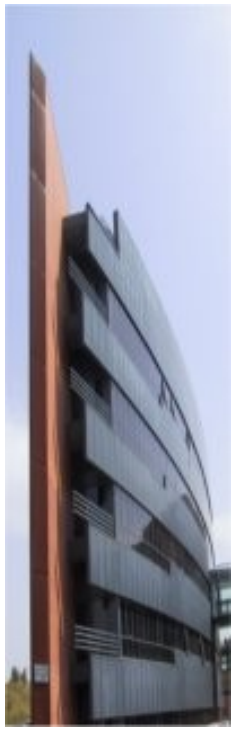
Eduroam / Responsabilidad.

- Los servicios técnicos de las organizaciones son los que proponen las configuraciones óptimas y SEGURAS que deben utilizar los usuarios finales.
- Los usuarios finales podrían pedir responsabilidades si la configuración propuesta no protege de las amenazas o deja lo mas valioso, username y password, al alcance de un ataque.



SecureW2 / Pack instalación (1/2)

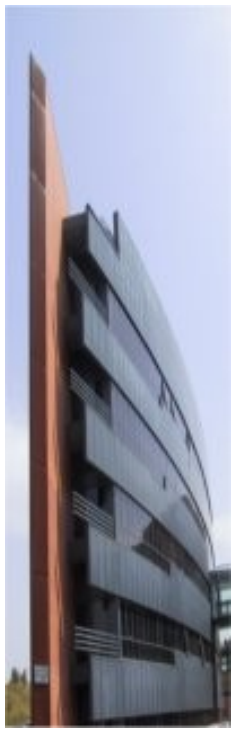
- SecureW2.inf
  - Durante la instalación que realiza el usuario final, según haya preconfigurado el administrador, se realizan de forma desatendida todas estas acciones:
    - Configura encriptación, asigna SSIDs con perfiles diferenciados, instala y configura certificados, configura identities, etc. etc.
  - Descripción de parámetros y valores por defecto en la Adminguide de SecureW2.
    - http://www.securew2.org/wiki/AdminGuide
  - Se simplifica trabajo al usuario y documentación a elaborar.
  - El usuario no sabe donde cambiar la configuración. *Ventaja*.



SecureW2 / Pack instalación (2/2)

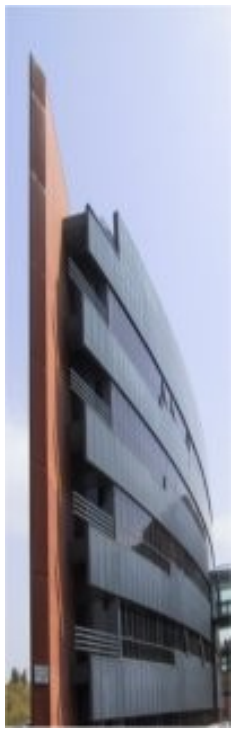
- Uso de perfiles propios y serializados. No recomendable utilizar el perfil DEFAULT ya que no indica nada y obliga a revisión completa en caso de problemas. La serialización permite identificar rápidamente:
  - Actualizaciones, cambios, wired/wireless, resolución de problemas, etc.
- Ya que estamos, aconsejable rellenar correctamente incluso parámetros que, a priori, no utilizaremos.
- El fichero SecureW2.inf SOLO SIRVE Y FUNCIONA EN LA INSTALACIÓN. Después de la instalación el .inf se puede borrar. La equivalencia entre los parámetros de .inf y la configuración manual, marcando y desmarcando en el interfaz gráfico, es trivial.

- NSI.
  - Pack de instalación para varias organizaciones o personalidades.



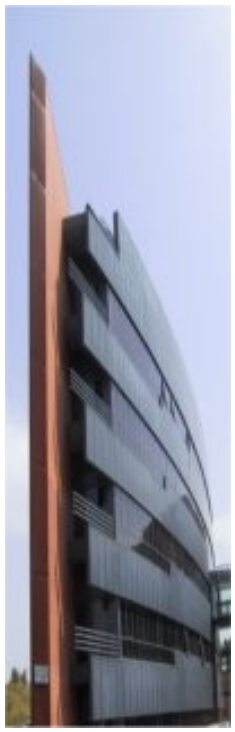
Certificados / Eduroam (1/2)

- Altamente recomendado: VERIFICAR.
  - La gran ventaja de la movilidad Eduroam, supone que nuestros usuarios van a sitios lejanos y van a poner su password en juego.
  - Hay que asegurarles que su password no se ve en ningún caso.
  - Pero es que, incluso cuando están en nuestra organización, deben estar protegidos.
  - Si no verificamos certificados estamos igual de expuestos usando TTLS, PEAP o enviando la password en claro.
  - Tres opciones.
    - Cadena de CAs + verificación de dominio. -> Recomendado.
    - Cadena de CAs. Ligeramente peor que la anterior.
    - Clave pública radius. La mas segura de todas pero poco flexible.



Certificados / Eduroam (2/2)

- Mejor usar certificados de servicio que de máquina. www.dominio, smtp.dominio, etc., normalmente, no suelen usar los certificados de las máquinas reales que dan cpu a esos servicios, sino certificados propios para www, smtp, etc.
- Con el paquete de instalación se simplifica la instalación y comprobación de los certificados en SecureW2.
- Si el usuario está adscrito a dos o mas organizaciones Eduroam, esto supone certificados e identities cambiantes.
  - Varios perfiles.
  - El usuario debe aprender, entonces, a cambiar perfiles.

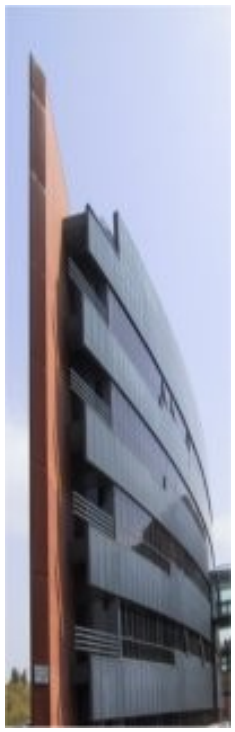


SecureW2 / Problemas (1/3)

- **No sirve cualquier fichero de certificado**. -> Seguir el manual.
  - No todos los ficheros .cer son iguales. Es necesario obtener los ficheros .cer según indica el manual de administración de SecureW2 para que funcione con el pack de instalación SecureW2.inf.
  - También se puede configurar el SecureW2, momentáneamente, PARA QUE NOS MUESTRE y para que incorpore, si así lo queremos, los certificados que el radius nos presenta.
    - Advanced -> Allow users to setup new connections

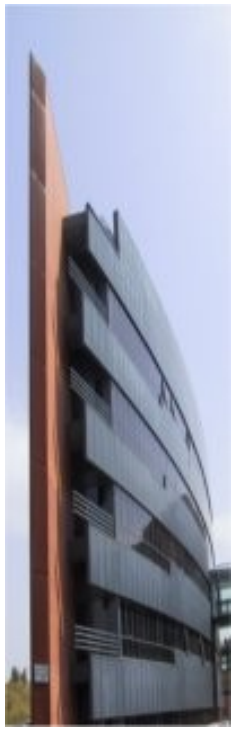
  Es una opción que no debe quedarse permanentemente activada. El usuario podría aceptar cualquier certificado que se le presente -> MitM

  También es una herramienta con la que los administradores pueden ver que certificados presenta la red inalámbrica -> verificación de red legal y detección de MitM.



SecureW2 / Problemas (2/3)

- **Si la verificación de certificados falla**. -> No es evidente.
  - SecureW2, simplemente, no conecta.
  - No da mensaje de error explicito y se queda “Intentando autenticar”.
- **Asignación de interfaz exacto en preinstalación no es posible.**
  - Debido a la identificación de interfaces en Windows.
  - Pero con el SSID es suficiente.
- **Si se pone Outer Identity correcta y FIJA. -> Genera mala costumbre en el usuario.**
  - En Inner Identity, en este caso, se podría poner *usuario* en vez de *usuario@dominio* y funcionaría.
  - Confuso y poco amable para la organización visitada.
  - Utilizar sólo cuando es la única solución -> 3.2.0 en Mobile .
  - Recomendable utilizar la forma dinámica ya descrita de Outer Identity.

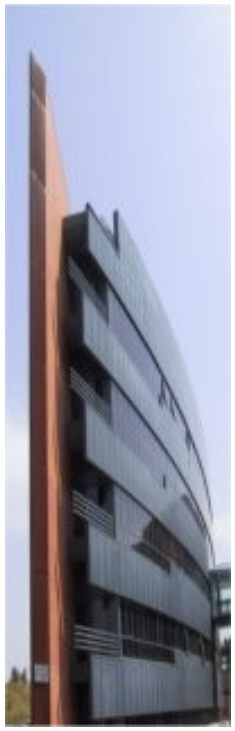


SecureW2 / Problemas (3/3)

- **Outer Identity dinámica y RFC 4282.**
  - Su aplicación a partir de la 3.2.0 hace que la forma dinámica no use anonymous, sino campo vacío.
    - Grave problema en Mobile y de stripping en freeradius.

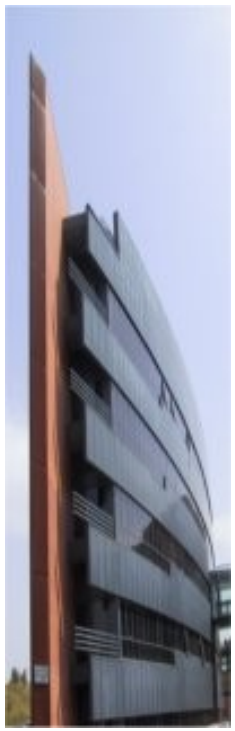
  SecureW2 estudia seriamente dar marcha atrás en futuras versiones.
- **Grabar password -> Vulnerabilidad.**
  - Marcando Save user credentials.
  - No recomendable.
  - Provoca conexiones automáticas no pedidas ni controladas por el usuario.
  - Guarda la contraseña en el pc -> vulnerabilidad al alcance de paquetes como Cain y Abel.
  - El usuario olvida su password.

  Mas que problemas, son malos usos derivados la flexibilidad que proporciona el SecureW2, y limitaciones de Windows y RFCs.



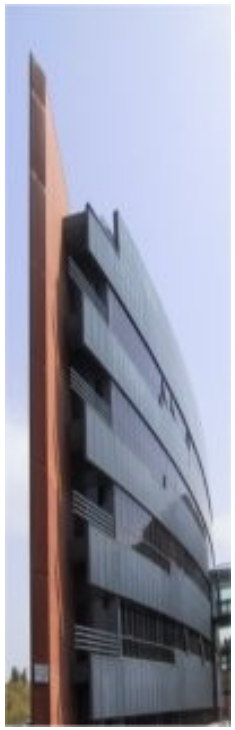
Otros clientes y SO (1/2)

- SecureW2 y Mobile.
  - Problemas en el registro con la actualización de 3.1.2 a 3.2.0.
  - Sin problemas en una instalación limpia de 3.2.0
  - No permite preconfiguración con SecureW2.inf
  - En 3.2.0 (RFC4282), problema con Outer Identity dinámica. El username vacío no es soportado por Mobile.
- Odyssey Funk.
  - El comercial de mas éxito.
- AEGIS Meetinghouse / Cisco.
  - Desaparecido ???. ¿Qué hará Cisco con el cliente que mas SOs abarcaba?
- WPA-Supplicant y Linux.
  - Versión Windows reciente.
  - Permite verificar certificados.



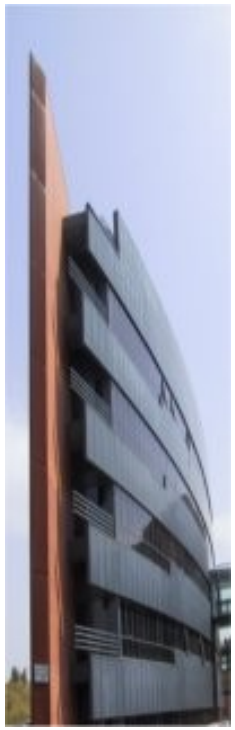
Otros clientes y SO (2/2)

- Mac-OSX.
  - Problema. Cualquier nuevo certificado que presente la red wireless es propuesto al usuario para su aceptación. Es como si tuviese permanentemente activada la opción Allow users to setup new connection.
- Clientes específicos para cada tarjeta hechos por el fabricante. En ellos lo mas corriente es:
  - Outer Identity explícita y fija.
  - No verifican certificados.
  - Perfiles o packs de instalación -> No tienen sentido.
  - A veces, incluso en los del mismo fabricante, no coinciden menús ni opciones.
- Xsupplicant – OpenSea
  - En desarrollo.
  - Nuevo comienzo. Se extenderá a SOs Microsoft.
- Wire1X
  - Poco extendido.



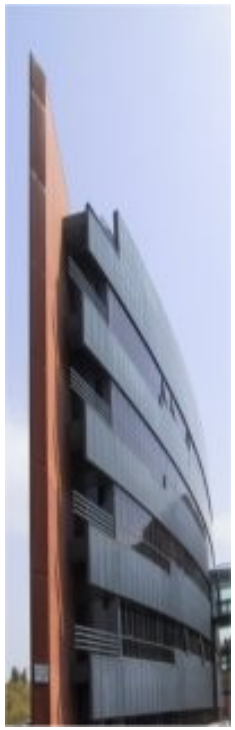
SecureW2 / Conclusiones (1/2)

- Excelente implementación de uno de los EAP mas flexibles.
- Estable en 2K/XP/Vista. Problemas en Mobile debidos al propio Windows.
- Uno de los clientes TTLS mas usados. Preferido en Eduroam.
- Gran flexibilidad. Permite realizar de varios modos la configuración de los parámetros de EAP-TTLS.
- Muchas formas de codificación de la Inner Identity.
- Requiere una configuración cuidadosa pero son pocos los parámetros a considerar.
- SOLO es SEGURO SI se VERIFICA CERTIFICADO.
  - Es la única forma de asegurar a nuestros usuarios que nadie mas ve su passsword.



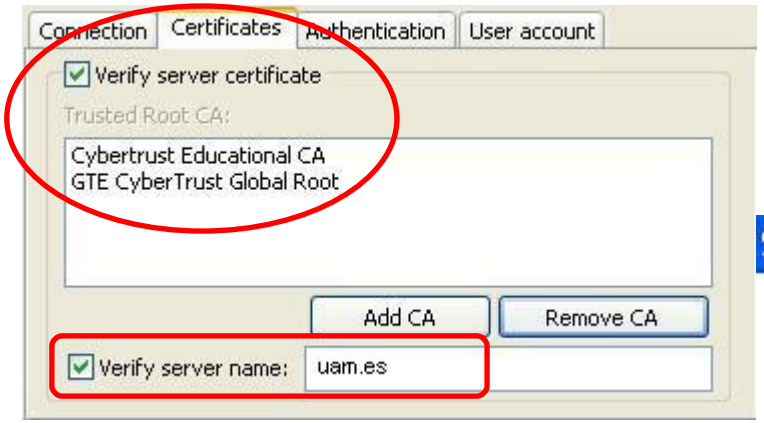
SecureW2 / Conclusiones (2/2)

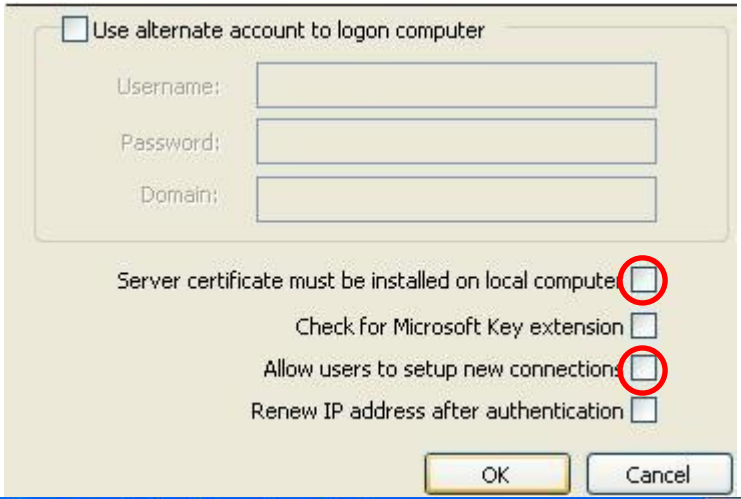
- Por tanto, la OUTER IDENTITY debe ser CORRECTAy distinta de la Inner. El código de usuario de la Outer debe ser NO SIGNIFICATIVO.
- La Inner Identity debe ser la adecuada en Eduroam: user@dominio
  - En nuestra organización también, no solo cuando salimos a otra organización Eduroam. Buena costumbre.
- Recomendable que no guarde la contraseña.
- Permite packs de instalación (2K/XP/Vista).
  - En la propia organización (.inf).
  - De varias organizaciones o varios tipos de usuarios a elegir (NSIS).
- Permite perfiles para diferentes SSIDs, encriptaciones, usos y personalidades.
- Los problemas mas graves son externos: Windows y RFCs.



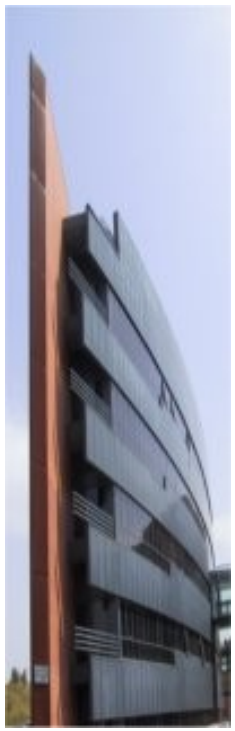
SecureW2 / OK


Connection
Certificates
Authentication
User account
Use alternate outer identity:
Use anonymous outer identity
Specify outer identity:


Connection
Certificates
Authentication
User account
Verify server certificate
Trusted Root CA:
Cybertrust Educational CA
GTE CyberTrust Global Root
Add CA
Remove CA
Verify server name:
uam.es


Use alternate account to logon computer
Username:
Password:
Domain:
Server certificate must be installed on local compute
Check for Microsoft Key extension
Allow users to setup new connections
Renew IP address after authentication
OK
Cancel


SecureW2 Credentials
SecureW2
Username:
usuario@uam.es
Password:
Domain:
Save user credentials
OK
Cancel



SecureW2 / Referencias

- www.securew2.com
- www.eduroam.es
- 802.11 Wireless Networks / Matthew S. Gast / O'Reilly
- www.freeradius.org
- www.opus1.com/nac/index.html#8021X
- www.microsoft.com/technet/community/columns/cableguy/default.mspx
- www.microsoft.com/downloads/details.aspx?familyid=05951071-6b20-4cef-9939-47c397ffd3dd&displaylang=en
- www.cisco.com/univercd/cc/td/doc/product/metro/me2400/12225seg/2400scg/sw8021x.htm
- en.wikipedia.org/wiki/Extensible_Authentication_Protocol