Radius con DNIe.

FreeRadius es un paquete de software de código abierto y libre distribución que permite implementar un servidor de RADIUS. El servidor de FreeRadius es modular, para facilitar su extensión, y es muy escalable. Además el almacenamiento de la información de autentificación (usuarios/contraseña) se puede realizar directamente (sobre ficheros de textos de configuración propios) o bien preguntando a bases de datos externas, como MySQL o bien ficheros del sistema/etc/passwd

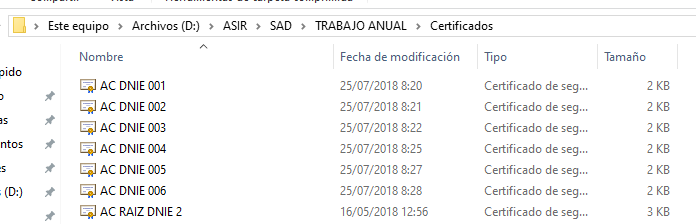
1. PKI del DNIe

Las Autoridades de Certificación que la componen son:

* Una Autoridad de Certificación raíz que sólo emite certificados para sí misma y sus Autoridades de Certificación subordinadas.
* Tres Autoridades de Certificación subordinadas que emiten certificados para los titulares de DNIe, a cada ciudadano le corresponde uno de ellos, como a priori no sabemos cuál será el que firme el certificado de un ciudadano concreto, lo que haremos es concatenar los tres certificados en un fichero junto a la Autoridad raíz de manera que FreeRADIUS pedirá a OpenSSL que recorra el fichero buscando el certificado necesario para un cliente dado siempre que dejemos el certificado de la Autoridad raíz en último lugar.

Primero hay que descargar los cuatro certificados de la web del DNIe:

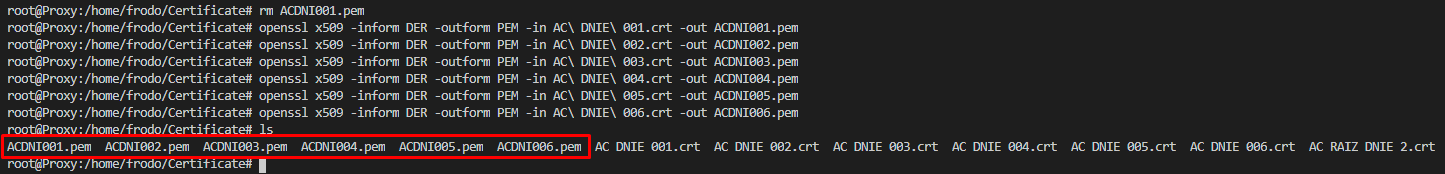
<https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_076&id_menu=68>



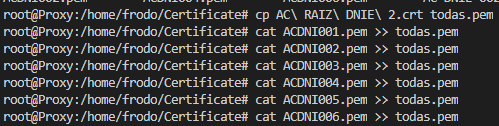
Los descomprimimos y pasamos los cuatro ficheros por SFTP al servidor.



Los ficheros vienen en formato DER (.crt), un formato propio de Windows, lo pasamos a PEM que es un formato más propio de Linux para que no haya ningún problema, lo haremos con OpenSSL situándonos en el directorio donde hemos copiado los ficheros ejecutamos lo siguiente.



Ahora toca concatenar los certificados en único archivo que llamaremos “todas.pem”.



Instalación de FreeRADIUS

Descargaremos FreeRadius 3.0.20 y lo instalaremos.





Será necesario instalas los siguientes paquetes porque contienen librerías de desarrollo necesarias para la instalación de FreeRADIUS.







Ejecutamos él. /configure.





Instalamos radius.



Configuración de FreeRADIUS

Por defecto la instalación se realiza en /usr/local/etc/raddb/.

Empezaremos con el fichero radius.conf, en el apartado PROXY CONFIGURATION deshabilitaremos el servidor proxy y comentaremos el include, no es estrictamente necesario pero ahorrará recursos.



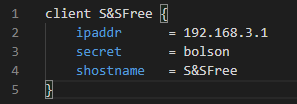


En el apartados *security* modificamos el parámetro *allow\_vulnerable\_openssl* para permitir que FreeRADIUS se inicie con una versión vulnerabe de OpenSSL.



Continuaremos con el fichero clients.conf, aquí añadimos el o los clientes RADIUS esto es el punto de acceso inalámbrico o en mi caso el router inalámbrico que configuraremos con los datos aquí introducidos, añadimos el cliente al final del fichero con la IP y prefijo que tendrá el punto de acceso inalámbrico, la secret es una clave cualquiera que permitirá comunicarse el punto de acceso con el servidor, y un nombre para el cliente que estamos introduciendo (shortname).



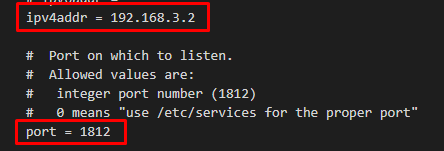


Continuamos con el archivo *default* dentro de *sites-enabled*, en este fichero se configuran los distintos host virtuales al igual que haríamos con Apache. En las secciones *listen* no es estrictamente necesario modificar nada, el servidor funcionará igualmente con la configuración que viene por defecto, las podemos configurar de la siguiente manera para hacer el servidor más seguro evitando que escuche peticiones provenientes de una IP o puertos distintos a los que tenemos planeado.

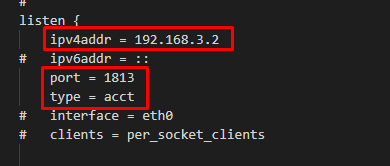
La primera sección *listen* (paquetes de autenticación) la configuramos de la siguiente manera, siendo *ipv4addr* la IP del adaptador que está conectado al mikrotik.







La segunda sección *listen* (paquetes de contabilización) la configuramos de la siguiente manera. La opción ipaddr se deberá cambiar por ipv4addr.



En la sección *authorize* tenemos que deshabilitar el filtro de nombre de usuario, éste comprueba si el nombre de usuario contiene espacios o caracteres inválidos rechazando el acceso es su caso. El CommonName del certificado de cliente contenido en el DNIe se compone de apellidos, nombre, espacios en blanco, una coma y el literal “(AUTENTICACIÓN)”, el filtro rechazaría el acceso no permitiendo que continué la petición del cliente.



Como nuestra intención es que los usuarios únicamente puedan tener acceso a la red WiFi mediante el DNIe, deshabilitaremos los módulos de autenticación que no vamos a utilizar, dejaremos *eap* habilitado ya que es la manera en que se autenticaran los clientes.











Una vez que el usuario está autorizado la sección *authenticate* se encargara de instanciar el módulo de autenticación, esta sección la podemos dejar tal cual ya que hemos descartado los módulos que no vamos a utilizar en la sección anterior.

Por ultimo debemos en el módulo *eap* tenemos que indicar dónde está el certificado de autoridad que controlará las credenciales de los clientes y firmará sus certificados contenidos en el DNIe.





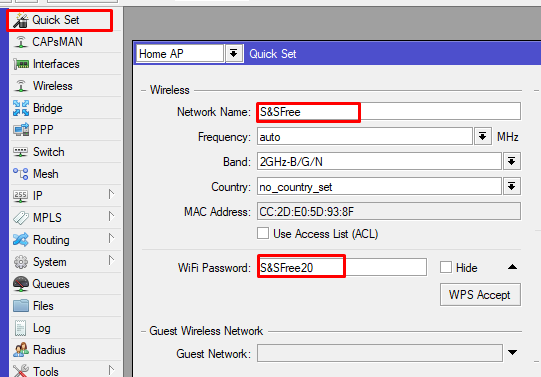
Por ultimo copiamos el fichero con los certificados al directorio de certificados de FreeRADIUS.



Punto de acceso

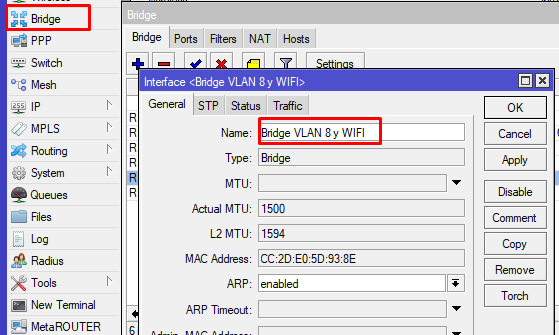
Como cliente RADIUS hace falta configurar un punto de acceso inalámbrico, en este caso se hará con un mikrotik. Lo configuramos con los siguientes pasos.

Pondremos un nombre a la WiFi, en la sección *Quick Set*.

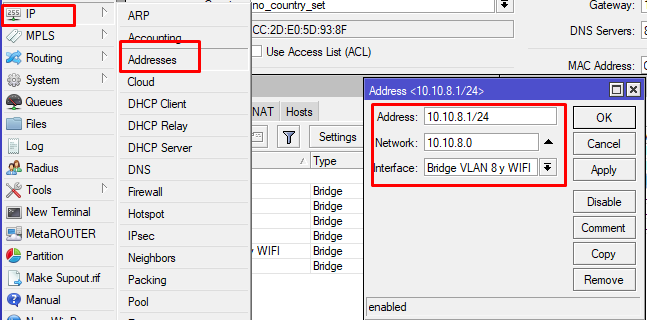


Crearemos un Bridge para la WLAN y definiremos una Ip para dicho Bridge.

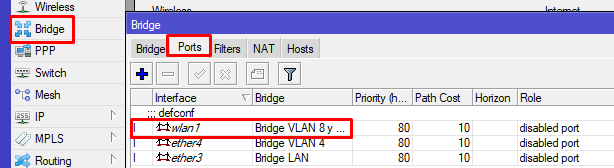
Bridge:

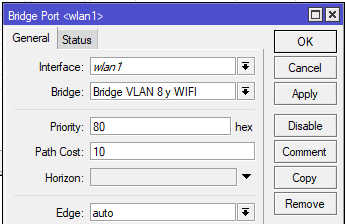


Definir una ip para ese bridge.



Lo siguiente que haremos será asociar el bridge que hemos creado a la interfaz de wlan.

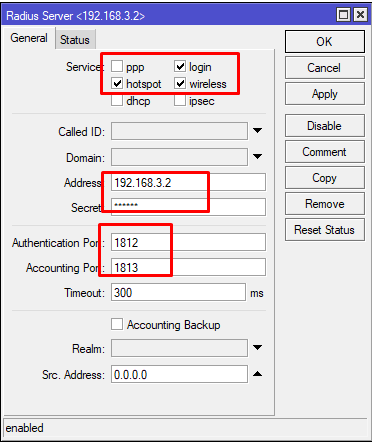




En este caso también se ha creado un servidor DHCP para que reparta IP por la Wifi, pero eso es irrelevante para hacer esta práctica.

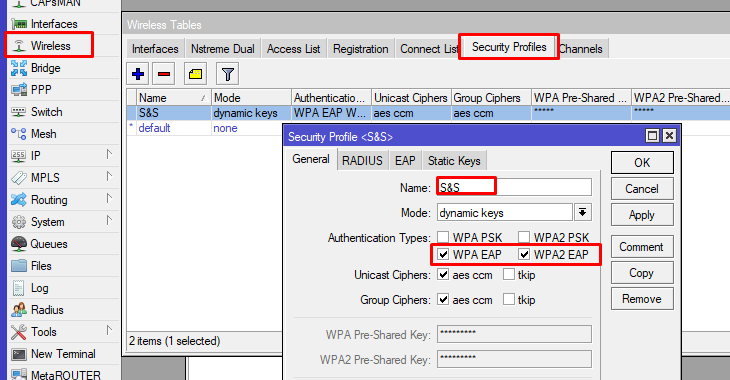
Una vez configurado esto nos iremos a la sección de Radius para hacer la comunicación con el servidor.

En esta sección lo que haremos será marcar las opciones de hostspot y Wireless, pondremos la IP del servidor Radius, la contraseña que hemos definido en el archivo client.conf y los puertos del servidor Radius.

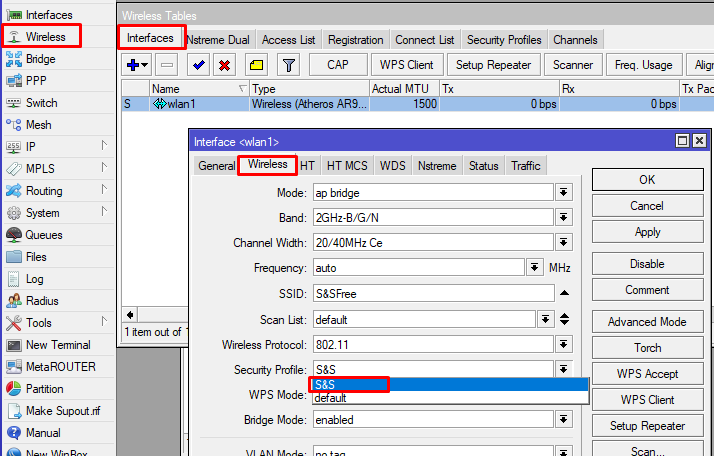


Después de establecer conexión con el servidor lo que haremos será ir a la sección de *Wireless* aquí nos iremos a la Pestaña de *Security Profiles.*

Aquí definiremos el Perfil de seguridad, le pondremos un nombre y marcaremos las opciones de WPA EAP y WPA2EAP, estas dos opciones nos dejaran autenticarnos con los DNIe.



Por ultimo deberemos de ir a la pestaña de Interfaces y seleccionar el perfil de seguridad que acabamos de crear.

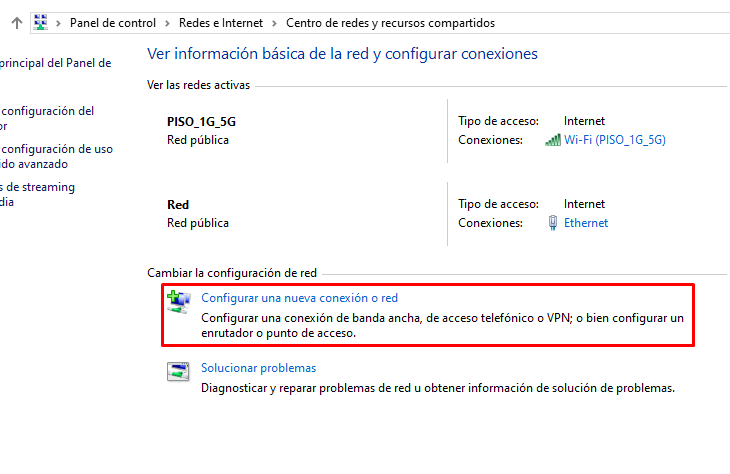


Clientes

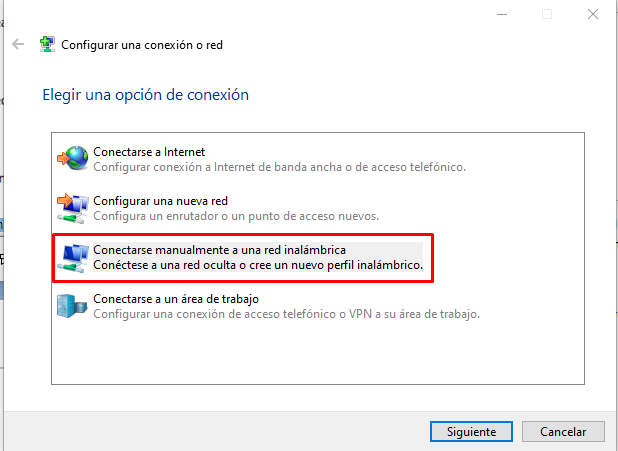
Para que un cliente pueda conectarse a la red WiFi será necesario un PC o portátil con tarjeta de red inalámbrica, sistema operativo Windows, un lector de tarjetas inteligentes, su DNI electrónico, y según qué casos hará falta el software que proporciona el Cuerpo Nacional de Policía llamado “Módulo criptográfico para el DNIe”.

En Windows 7,8 y 10 no es necesaria su instalación ya que al introducir el DNIe en el lector automáticamente se descargarán los drivers necesarios desde Windows Update, permitiendo trabajar al DNIe como dispositivo plug&play.

Vamos a crear una nueva conexión de red inalámbrica, nos vamos a *“Panel de control\Redes e Internet\Centro de redes y recursos compartidos”*, pinchamos sobre *“Configurar una nueva conexión o red”.*



Seleccionamos la opción de *“Conectarse manualmente a una red inalámbrica”* y pulsamos *“Siguiente”*.

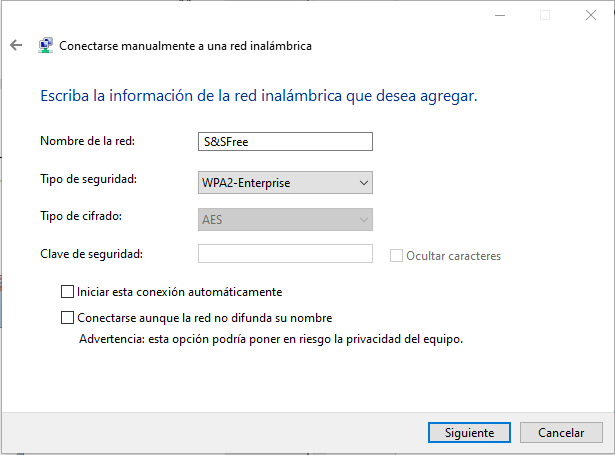


Introducimos los datos que habíamos configurado en el punto de acceso WiFi:

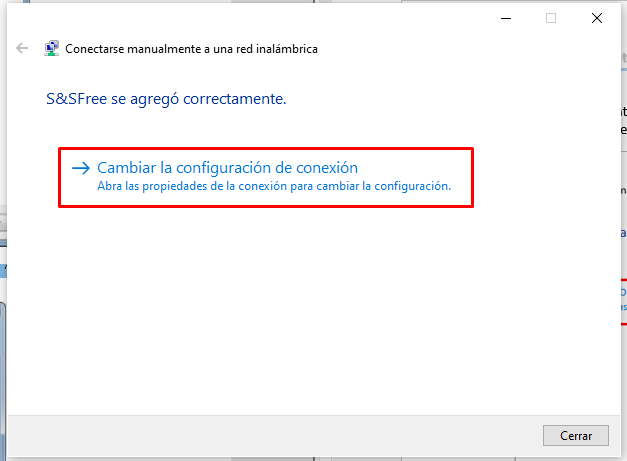
- Nombre de la red: S&SFree

- Tipo de seguridad: WPA2-Enterprise

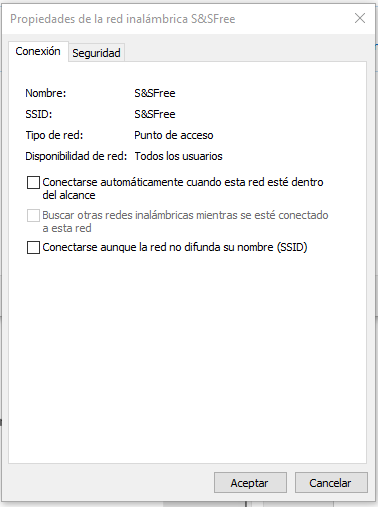
- Tipo de cifrado: AES



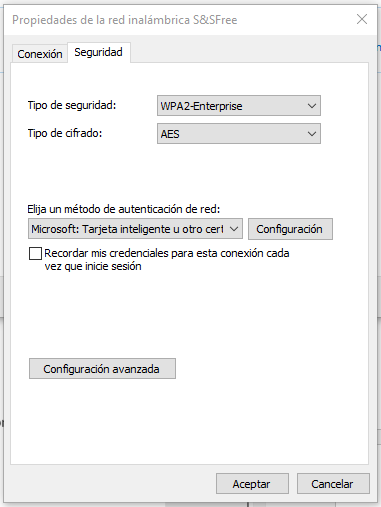
Pulsamos “Siguiente” lo que nos lleva a la siguiente ventana donde pincharemos sobre “Cambiar la configuración de conexión” para realizar algunos ajustes sobre la nueva conexión.



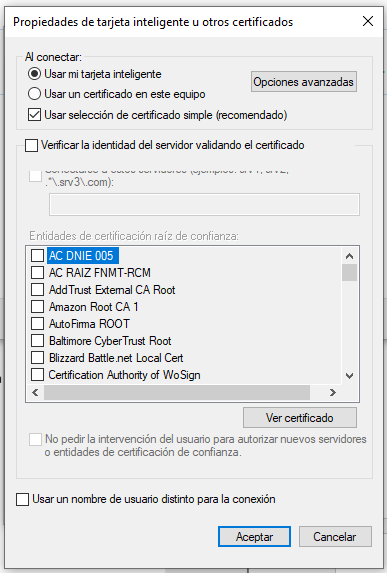
Nos aparece una nueva ventana con las propiedades de la conexión, de la pestaña *“Conexión”* no tocaremos nada.



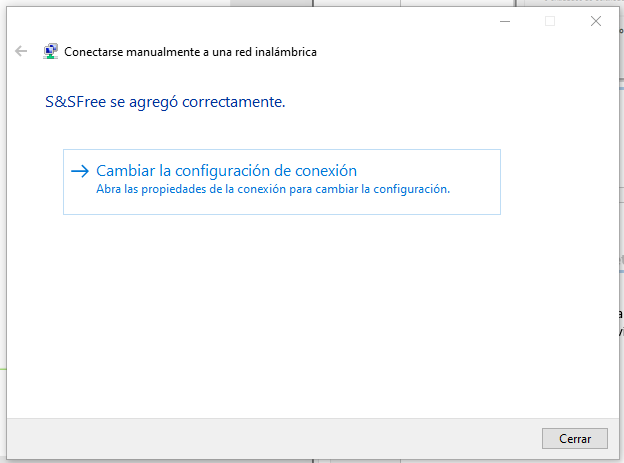
Pasamos a la pestaña *“Seguridad*”, en el menú *“Elija un método de autenticación de red:”* seleccionamos *“Microsoft: Tarjeta inteligente u otro certificado*”, luego pinchamos sobre el botón *“Configuración”*.



En “Al conectar:” seleccionamos “Usar mi tarjeta inteligente”, desmarcamos la casilla “Validar un certificado de servidor”.



Finalmente pinchamos sobre “Cerrar” en la ventana anterior con lo que tendremos configurada la conexión al servidor RADIUS mediante DNIe.

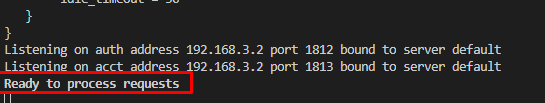


Pruebas

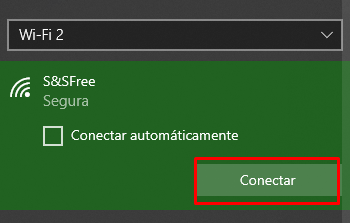
Iniciamos FreeRADIUS con alguno de los siguientes comandos, el “-X” es para iniciarlo en modo debug.



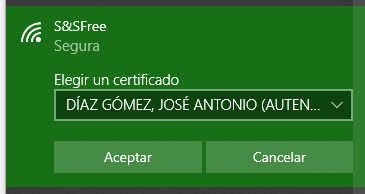
Se iniciará el servidor. Si todo ha ido bien al final del log nos aparecerá el mensaje *“Ready to process requests”.*



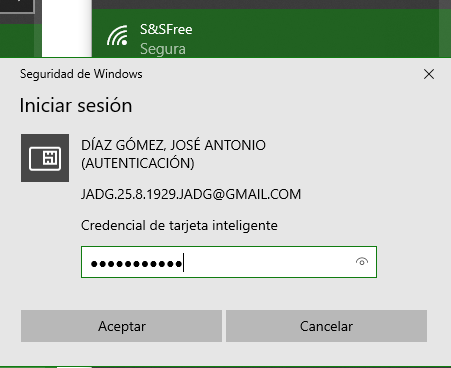
Con el lector de tarjetas inteligentes instalado, conectado, y el DNIe insertado, buscamos la red WiFi que hemos configurado en el cliente FreeRADIUS y le damos a conectar.

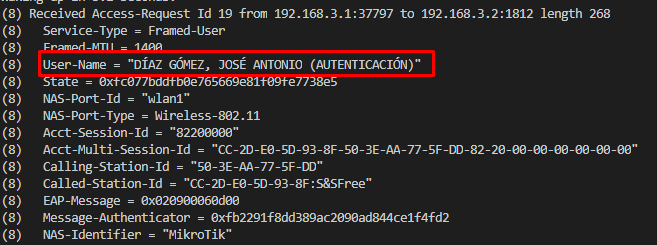


Nos debería de seleccionar el método de autenticación de los certificados del DNIe.



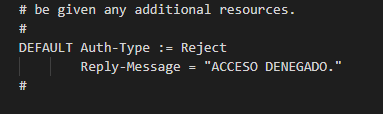
Seguidamente deberemos de poner el PIN del Dnie electrónico y si todo ha ido bien debería de conectar a la red.



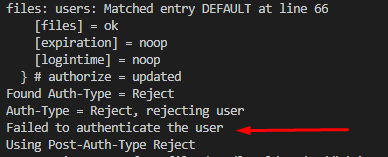


Para poder definir que solo los usuarios que estén en el sistema se puedan loguear se tendrá que definir en el fichero **users** las siguientes opciones.

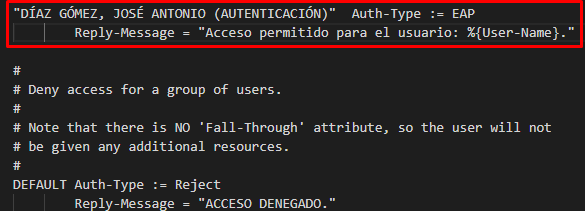




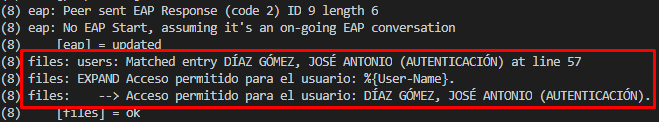
Ahora comprobaremos que no nos deja loguearnos y nos saldrá el siguiente mensaje de error.



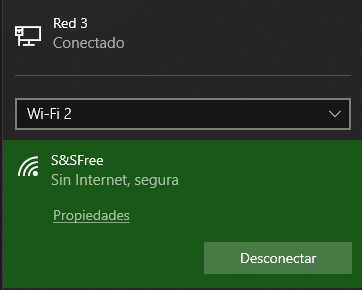
Para poder loguearnos con un usuario especifico solo tendremos que poner las siguientes líneas en el fichero **users**. En este fichero pondré el nombre del usuario y el tipo de protocolo que será **EAP.** La opción definida anteriormente se dejara sin comentar para que solo los usuarios que estén definidos en dicho archivo puedan acceder a la Wi-Fi.



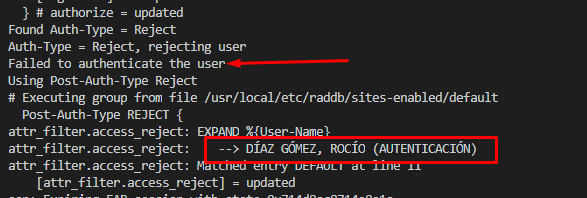
Ahora comprobaremos que el usuario se loguea en la red Wi-Fi y sale el mensaje que hemos definido en el fichero.

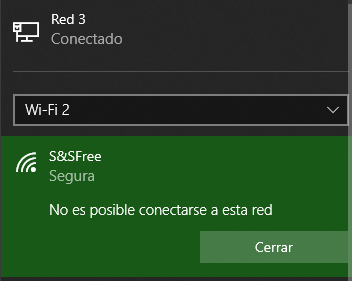


Vemos como se ha conectado a nuestra red.



Comprobamos que utilizando un DNIe que no está en el fichero **users** definido no es posible conectarnos a la red Wi-Fi.





1. WEBGRAFÍA.

**DNIe**

<https://drive.google.com/drive/folders/1tArlmfmwXLazmNixgPJaqmlC1wlFCYJc>

<http://oa.upm.es/1602/1/PFC_SERGIO_YEBENES_MORENO.pdf>

<http://seguridadxredes.blogspot.com/2015/12/vpn-ipsec-ii-autentificando-con-dnie-o.html>

<https://www.eduardocollado.com/2017/07/24/conexion-a-mikrotik-via-radius/>