Se trata de que el terminal y la tarjeta realicen la Autenticación Mutua.

Ahora que ya tenemos configurada la tarjeta con las claves vamos a realizar un script que autentique la tarjeta y el terminal. Se va a realizar la autenticacion Mutua con triple DES, según la página 28 del manual de la tarjeta ACOS3. Tambien se ha explicado en clase en la diapositiva 36 del documento cifrado-autenticacion-secure-messaging.

Hay que hacer un script que realice la autenticación mutua y nos saque por pantalla trazas de lo que va haciendo, imprimiendo al final la clave de sesión e indicando con un mensaje si la autenticación ha tenido éxito o no.

Las claves de la tarjeta y del terminal están escritas en la tarjeta: ver la actividad de inicializacion del fichero de claves.

La tarjeta tiene un límite de 8 intentos de autenticación fallidos a partir de los cuales se bloquea el proceso de autenticación y ya no es posible llevarlo a cabo (por seguridad, para que la gente no empiece a probar claves a la fuerza bruta). Es decir la tarjeta queda inútil.

Para realizar el script y no bloquear la tarjeta con pruebas, se recomienda no probar con la tarjeta hasta que no estemos seguros de que ya está resuelto y funciona.

Es decir la técnica sería: cuando la tarjeta tenga que enviar una respuesta, por ejemplo un aleatorio, definirlo nosotros en el script como una variable y utilizarlo como si hubiera venido de la tarjeta.

Cuando la tarjeta tenga que devolver un cifrado, hacerlo nosotros en el script como si lo hubiera hecho la tarjeta y utilizarlo como si hubiera venido de la tarjeta.
Cuando el script funcione se van substituyendo las funcionalidades "simuladas" por las respuestas reales de la tarjeta.

Para dudas consultarme.

Subir al servidor web el script que realiza la Autenticacion Mutua 3DES.

Disponible en: viernes, 20 de febrero de 2015, 16:00
Fecha límite de entrega: sábado, 28 de febrero de 2015, 20:00

Borrador del envío

Aún no se han enviado archivos

Subir un archivo (Tamaño máximo: 10Mb)

Choose File No file chosen
Subir este archivo