# Cuestiones sobre RFP N28:

Encriptación y desencriptación de TOKEN-REQUEST y TOKEN-REPLY:

Se índice que el algoritmo tiene que ser 3DES, pero hay que especificar de forma detallada el padding del algoritmo. De igual forma hay que especificar lo mismo en el algoritmo DES de generación de MAC (e indicar también el modo CBC o ECB).

Asimismo, hay que sincronizar esta parte con la CARM para que los algoritmos de codificación sean simétricos en ambas aplicaciones para asegurar la correcta transmisión de datos.

Longitud MAC generado para CCT:

Aclarar si la longitud del MAC generado para el cálculo del CCT tiene que ser 8 o 16, ya que existen discrepancias en varios documentos.

Datos de Prueba:

Obtención de un recibo real para la comprobación de los algoritmos de cifrado.

Validaciones:

Especificar sobre que datos enviados por la CARM en el TOKEN\_REQUEST se ha de efectuar la validación para controlar el correcto envío.

BBDD:

Tablas afectadas y campos a añadir en su caso (CCT).