

Autenticación con certificado

Como método alternativo de identificación se proporciona la autenticación con certificado electrónico de cliente.

En estos enlaces se puede consultar su significado y algún detalle técnico:

https://en.wikipedia.org/wiki/Transport_Layer_Security#Client-authenticated_TLS_handshake

https://en.wikipedia.org/wiki/Mutual_authentication

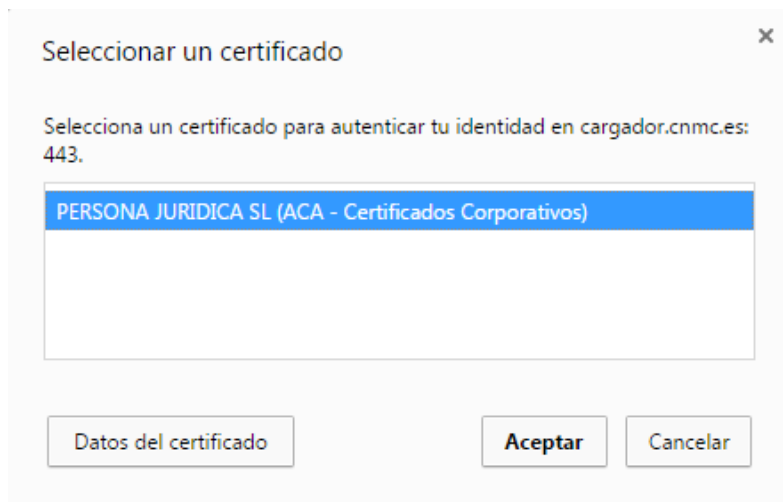
Este sistema permite identificar a la persona que se conecta al servicio, a diferencia el método OAuth que es una identificación de empresa. La única excepción son los certificados "de sello" o "no personales" que sólo incluyen el identificador de la empresa para la que están emitidos, aunque lleven información de contacto.

El API utiliza la identificación de persona física del certificado (NIF) para comprobar en el registro de habilitación de la CNMC la capacidad de operar de esa persona en el procedimiento elegido. Si el certificado es de representante, igualmente, se verificará la habilitación del NIF del representante. Si el certificado está emitido a una persona jurídica debe estar relacionado también como habilitado en dicha entidad jurídica.

Por lo tanto los campos indicados como nifPresentador y nifEmpresa del resto de llamadas al API deben estar relacionados con el certificado electrónico empleado en la identificación o se devolverá un mensaje de error de acceso "403 Forbidden". De nuevo, los certificados de sello al sólo identificar a la empresa sólo añaden esa restricción y se podrá utilizar cualquiera de los nifPresentador de los contactos asociados a dicha empresa.

La aplicación web de carga [Cargador](#) incluye esta funcionalidad, como se puede ver en las siguientes pantallas:

Paso 1. Solicitud del certificado del presentador:



Paso 2. Los campos nifPresentador y nifEmpresa son autocompletados a partir de la información del certificado.

