Resumen de Protocolos:

El servidor del registro se identifica mediante un certificado de servidor emitido por VeriSign, Inc.

Todas las comunicaciones entre el servidor del registro y el navegador del cliente se realizan encriptadas bajo protocolo SSL (Secure Socket Layer). Dicho protocolo está dividido en dos capas: el SSL Handshake y el SSL Record, cuyos cometidos son los siguientes:

SSL Record: Es el protocolo de bajo nivel que se ocupa de la formación de los paquetes de datos.

SSL Handshake: Es el protocolo de alto nivel en el que se negocian las características de la comunicación, a través de las siguientes fases:

Inicio: El cliente y el servidor establecen los algoritmos que se van a usar en la transmisión.

Determinación de la clave: se genera la clave simétrica y se intercambia entre cliente y servidor encriptándola mediante un algoritmo de clave pública.

Verificación: cliente y servidor verifican la integridad de la información transmitida hasta ese momento.

Intercambio de datos: la información a transmitir circula por el canal seguro, encriptada mediante la clave simétrica previamente intercambiada.

Finalización: el cliente finaliza la sesión SSL, el navegador advierte que la comunicación ha dejado de ser segura.

Seguridad de las transacciones:

Por cada transacción se genera una nueva clave de encriptación que se descarta al finalizar la transacción de forma que el conocimiento de la clave de una transacción no permite desencriptar otras.

Toda transacción realizada en el registro telemático produce un documento de respuesta con sello electrónico de Administración Pública, conforme al artículo 18 de la ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos

Dicho documento de respuesta incluye la solicitud presentada por el usuario