Partiendo del certificado enviado por el servidor al cliente, éste puede validar el mismo comparando el resumen integrado en el certificado, firmado por la clave privada de la CA, con el calculado por él mismo a partir del certificado.

Se ilustra este proceso a continuación:



