

El DNI electrónico carece de prestaciones para el cifrado de mensajes, salvo las necesarias para realizar los procesos internos de firma electrónica. La razón hay que buscarla en las etapas de decisión del alcance del proyecto; los diseñadores concluyeron que dicha prestación quedaba fuera del ámbito deseable para un documento de identidad, más aún teniendo en cuenta la complejidad que supondría la gestión de las claves de decenas de millones de ciudadanos. Esa gestión incluye la necesidad de mantener accesible para el titular su clave privada aun en caso de destrucción o pérdida del soporte; dicha pérdida supone la imposibilidad de recuperar el contenido cifrado lo cual obligaría a mantener una infraestructura de recuperación de claves. La relación de esta actividad con el ente encargado de la gestión del DNIE, el Cuerpo Nacional de Policía, sería considerada sin duda antinatural.

La finalidad del ejercicio que se propone en este documento no es otra que simular un escenario en el que un ciudadano pueda transmitir la confianza de la Autoridad de Certificación del DNIE a una pareja de claves propia. En otras palabras, se trata de convertir cada DNIE en una AC subordinada “*en miniatura*”, vector de transmisión de la confianza en AC-RAIZ-DNIE.

Es necesario establecer una serie de asunciones para delimitar el ámbito de aplicación de los conceptos y del resultado que se proponen. En primer lugar, la Ley [59/2003](#) en su artículo 3, siguiendo pautas establecidas en la Directiva [1999/93/CE](#), define la firma electrónica reconocida como *una firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*. Puesto que no cabe duda de lo que en la Ley se define como certificado reconocido “de firma” y de las características que debe tener (con especial referencia a la descrita en el artículo 11.2.h), para evitar efectos indeseados proponemos hacer uso en este ejercicio del certificado “de identidad” en lugar del certificado “de firma”; esta medida implica que el resultado de la firma obtenida no expresa conformidad con el contenido, habida cuenta de que el certificado de identidad sólo tiene habilitado el bit 0 del atributo *KeyUsage*, conocido como *digitalSignature*, a diferencia del certificado de firma que presenta activo el bit 1 etiquetado como *non-Repudiation*. Para más información sobre este aspecto técnico sugerimos un estudio detallado de los documentos [RFC-5280](#) y [RFC-3739 \(4. Security Considerations\)](#). Se ha considerado que, puesto que la finalidad del ejercicio es dotar de identidad a una clave pública, parece más adecuado el uso del certificado de identidad.

Dentro del marco del ciclo de talleres organizado conjuntamente por INTECO y Red.es, se decidió incluir este ejercicio con la única finalidad de servir de argumento a la necesidad de certificar las aplicaciones de firma que hagan uso del DNIE; el esquema descrito sugiere una transmisión de confianza entre un proveedor de servicios de certificación, la DGPGC, y una entidad aceptante, en este caso el ciudadano, mediante la firma de una clave pública. A pesar de que el esquema pueda parecer robusto y confiable y de que efectivamente se transforma cada DNIE en una *mini-AC*, es necesario resaltar que el eslabón débil es precisamente la aplicación que invoca la funcionalidad de firma. Se pone así de manifiesto el hecho cierto de que una certificación, por ejemplo EAL4+, tiene unos límites físicos y lógicos; dichos límites se establecen precisamente en la definición del TOE de dicha certificación. Sólo la aplicación de unos perfiles de protección y la superación del correspondiente proceso de certificación dotan a los productos del halo de seguridad necesario.

Insistimos en que se trata de un mero ejercicio conceptual, sin utilidad práctica más allá del simple experimento de laboratorio. Cualquier utilización que se quiera hacer de los principios e ideas que se exponen a continuación deberá llevarse a cabo asumiendo las responsabilidades y obligaciones inherentes al uso del DNIE y de la información que contiene, en especial las relacionadas con la reglamentación vigente en materia de protección de datos.

El programa que se facilita junto a este documento incorpora el conjunto de comandos necesarios para simplificar este proceso; está profusamente comentado para garantizar la comprensión de un lector con unos mínimos conocimientos de programación; a veces se ha recurrido a estructuras redundantes para garantizar la comprensión del proceso, incluso por personas sin conocimiento de la programación orientada a eventos. Se publica en forma de código fuente por lo que para poder ejecutarlo será necesario que el usuario disponga del entorno de desarrollo Gambas y las dependencias que concurran en su sistema. Las operaciones criptográficas han sido delegadas en el producto OpenSSL y los accesos al DNIE se hacen mediante invocación de herramientas incorporadas a opense: *pkcs11-tool*, *pkcs15-tool* y *pkcs15-crypt*.

---

El desarrollo se realizó en un equipo con el siguiente software:

[Ubuntu](#) 9.10 (Karmic Koala).

[GNOME](#) 2.28.1

[Gambas](#) 2.13

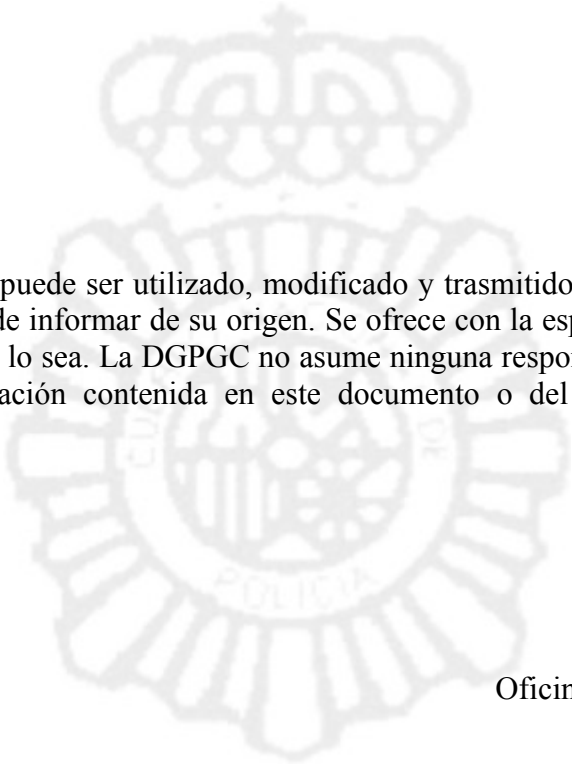
[opense](#) 0.11.8

[opense-dnie](#) 1.4.7-1

[openssl](#) 0.9.8

[pcscd](#) 1.5.3

El contenido del programa puede ser utilizado, modificado y transmitido por cualquiera sin ninguna limitación y sin necesidad de informar de su origen. Se ofrece con la esperanza de que sea útil pero sin ninguna garantía de que lo sea. La DGPGC no asume ninguna responsabilidad por el uso que se pueda hacer de la información contenida en este documento o del programa al que se hace referencia.



Oficina Técnica del DNIE.