

Anexo Técnico

1. Chips del documento nacional de identificación civil

A nivel electrónico, el documento de identificación de los mayores de edad posee dos chips, uno visible, de contacto, y uno no visible, para uso sin contacto. El chip de contacto contiene aplicaciones destinadas a realizar identificación electrónica de las personas, pensadas para su uso en contextos de servicios electrónicos. En este sentido, el chip de contacto permite (i) leer electrónicamente todos los datos del titular del documento; (ii) confrontar electrónicamente la huella digital de una persona contra la almacenada, para verificar si la huella corresponde al dueño de la cédula (*Match-On-Card*), y (iii) utilizar un par de llaves y un certificado electrónico para realizar autenticación y firma electrónica avanzada de personas físicas.

2. Procedimiento para la equivalencia con la identificación presencial

Cuando un usuario tiene que autenticarse con el documento de identidad electrónico con niveles de seguridad altos, debe utilizarse el certificado digital almacenado en el documento de identidad electrónico.

El sistema informático que requiere autenticación para el acceso (sistema solicitante) **debe** iniciar el flujo por medio de una solicitud al dispositivo criptográfico, para que éste genere la firma de un ticket que actúa como desafío de autenticación. El sistema informático deberá verificar el ticket firmado, para decidir la autorización o denegación de acceso.

En este proceso ocurre una autenticación de doble factor, ya que para acceder al certificado de firma se solicita ingresar el PIN del documento de identidad electrónico (factor de conocimiento, "algo que sé") y luego se realiza una firma electrónica avanzada con el certificado que tiene el usuario almacenado en el documento de identidad electrónico (factor de posesión, "algo que tengo"). De este modo este procedimiento cumple con el nivel superior (AE3) de autenticación referido en la Política de Identificación Digital, sección 4.4, y con el nivel superior de registro (RID3) referido en la sección 4.1 de dicha política; por lo tanto, resulta equivalente a una identificación presencial.

En este escenario no se realiza federación de identidades, ya que el propio sistema solicitante resuelve la autenticación interactuando con el documento de identidad electrónico.