El reglamento europeo eIDAS

Un nuevo marco para la identificación electrónica en la Unión Europea

El **Reglamento (UE) Nº 910/2014** del Parlamento Europeo y del Consejo, de 23 de julio de 2014[1], relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS) establece las condiciones en que **los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro**, así como las normas para los servicios de confianza y un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

En lo que respecta a la identificación electrónica, **el reglamento establece la obligación de reconocer, en septiembre de 2018**, los esquemas de identificación notificados por otros Estados miembros para el acceso electrónico de los ciudadanos (personas físicas y jurídicas) a los servicios

[1] https://www.boe.es/doue/2014/257/L00073-00114.pdf

públicos. En la práctica, esto significa que, una vez que un Estado miembro haya comunicado su intención de que un determinado sistema de identificación electrónica sea reconocido por el resto, los ciudadanos de ese Estado podrán utilizar el sistema de identificación (p.ej. el DNI-e en el caso de España) para el acceso a los servicios públicos online ofrecidos por los otros Estados en condiciones equivalentes a las que esos Estados ofrecen a sus propios ciudadanos. Asimismo, aunque el reglamento obliga a los servicios públicos a este reconocimiento, permite también, con carácter opcional, que las entidades privadas se incorporen al sistema y posibiliten el uso de los sistemas de identificación notificados por otros países para acceder a sus servicios electrónicos.

El marco de interoperabilidad de eIDAS

Para que la obligación de reconocimiento de medios de identificación electrónica de otros países pueda llevarse a cabo, el reglamento y su legislación de desarrollo establecen un **marco de interoperabilidad**[2] al que deben ajustarse las infraestructuras nacionales de identificación electrónica de los Estados miembros.

Este marco de interoperabilidad contiene los siguientes elementos:

[2] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOL_2015_235_R_0001

- Referencia al acto de ejecución de **niveles de seguridad**[3]
- Interconexión de los nodos del sistema
- Protección de datos y confidencialidad
- Integridad y autenticidad de los datos en la comunicación
- Formato de los mensajes
- Gestión de la información de seguridad y los metadatos
- Estándares para la seguridad de la información
- Datos de identificación de las personas (físicas y jurídicas)
- Especificaciones técnicas

En cuanto a las especificaciones técnicas, estas han sido ya aprobadas[4] y constan de 4 documentos:

- Arquitectura de interoperabilidad
- Perfil de atributos SAML
- Formato de los mensajes

[3] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOL_2015_235_R_0002

[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+eIDAS+profile

- Requisitos criptográficos

El sistema eIDAS se basa en la comunicación segura que se establece entre los **nodos de interoperabilidad** operados por los distintos Estados miembros (**nodos eIDAS**), de manera que son esos nodos de interoperabilidad los que se comunican entre sí en las transacciones transfronterizas, y conectan a nivel nacional con los servicios electrónicos que desean usar un medio de autenticación emitido por otro país para la identificación de ciudadanos extranjeros, y con los sistemas de identificación nacionales para el acceso de los ciudadanos de ese Estado miembro a los servicios electrónicos ofrecidos por otros países.

En este sentido, las especificaciones técnicas de eIDAS regulan únicamente la comunicación que se establece entre los nodos de interoperabilidad de los Estados miembros en las transacciones transfronterizas, **dejando libertad a cada país de implementar sus propios mecanismos de conexión a nivel nacional**.

La arquitectura de interoperabilidad definida para eIDAS permite dos posibilidades de implementación, mediante un servicio proxy (servicio operado en el Estado miembro emisor del sistema de identificación y autenticación electrónicas) o mediante un servicio middleware (servicio operado en el Estado miembro receptor de la autenticación); en el caso de España, se ha optado por una arquitectura basada en un servicio proxy.

Esta arquitectura de interoperabilidad se refleja en el siguiente diagrama:

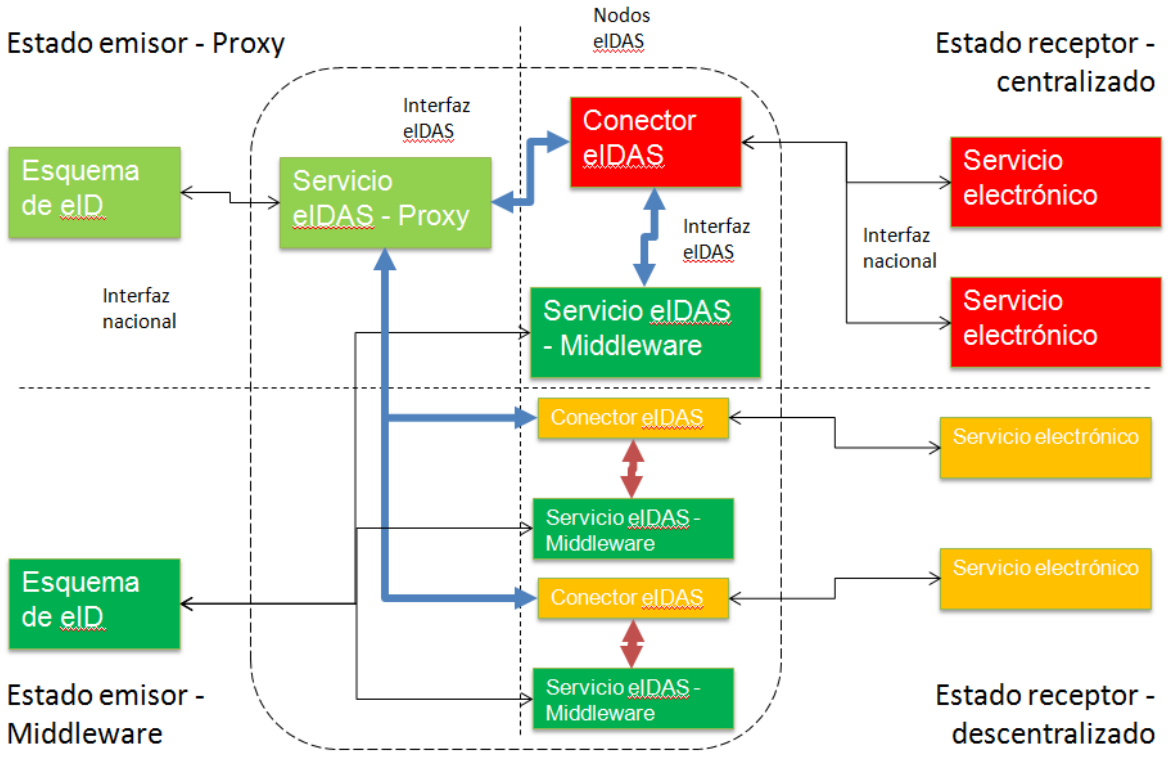

Ilustración 1. Diagrama de conexión nodo eIDAS

Como se observa, los servicios electrónicos conectados a la plataforma eIDAS se integran con el nodo eIDAS de su país mediante una conexión, implementada con una interfaz definida a nivel nacional, con el conector eIDAS del nodo. A través de esta interfaz realizan sus solicitudes de autenticación, y reciben las respuestas a las mismas.

Los niveles de seguridad

Un elemento esencial en el marco de interoperabilidad del reglamento eIDAS es el **nivel de seguridad de la autenticación**. El nivel de seguridad caracteriza el grado de confianza de un medio de identificación electrónica para establecer la identidad de una persona, garantizando así que la persona que afirma poseer una identidad determinada es de hecho la persona a quien se ha atribuido dicha identidad. El nivel de seguridad depende del grado de confianza que aporte este medio de identificación electrónica sobre la identidad pretendida o declarada por una persona, teniendo en cuenta los procedimientos técnicos, (por ejemplo, prueba y verificación de la identidad, autenticación), las actividades de gestión (como la entidad que expide los medios de identificación electrónica, el procedimiento para expedir dichos medios) y los controles aplicados.

El reglamento eIDAS establece **tres niveles de seguridad**, de menor a mayor grado de confianza: **bajo, sustancial y alto**. De acuerdo con el reglamento, cuando un proveedor de servicios envía una solicitud de autenticación al sistema eIDAS, debe especificar en esa solicitud, en función de la naturaleza del servicio, el nivel de seguridad (bajo, sustancial o alto) que desea para esa autenticación. El sistema eIDAS gestionará la petición de manera que solamente le entregará una identificación y autenticación válidas cuando el medio de identificación utilizado tenga un nivel de seguridad igual o superior al requerido.

Datos de identificación previstos en eIDAS

El marco de interoperabilidad del reglamento eIDAS especifica los datos de identificación que deben incluirse, tanto de manera obligatoria como opcional, en los mensajes de respuesta a las solicitudes de autenticación. Estos datos deberán provenir del esquema de identificación utilizado por el ciudadano para la autenticación.

En el caso de las **personas físicas**, el marco de interoperabilidad establece:

- Un conjunto de **4 datos obligatorios** que deben proporcionarse en todos los casos. Estos datos son:
    - **Identificador de unicidad**: Se trata de un identificador vinculado de manera única a una persona determinada, que permite asociar a la misma persona autenticaciones sucesivas. Se debe hacer notar que este identificador garantiza que no habrá dos personas con el mismo identificador, pero no que la misma persona tenga siempre el mismo identificador, ya que no es completamente persistente en todos los países (una persona puede tener identificadores distintos a lo largo de su vida).
    - **Nombre** (en general uno o varios nombres, según la costumbre de cada país)

- **Apellido** (en general un único apellido, como es lo habitual en el resto de países europeos)
- **Fecha de nacimiento**

- Un conjunto de **5 datos opcionales** que el país emisor de la autenticación puede decidir proporcionar o no, para facilitar la asociación de los datos de identificación del ciudadano en autenticaciones sucesivas cuando el identificador de unicidad no es persistente. Estos datos opcionales son:
  - Nombre al nacer
  - Apellido al nacer
  - Lugar de nacimiento
  - Dirección actual
  - Género

En el caso de las **personas jurídicas**, el esquema es similar al de personas físicas, con un conjunto de datos obligatorios y un conjunto de datos opcionales:

- El conjunto de **datos obligatorios** que deben proporcionarse en todos los casos está formado por:
  - **Identificador de unicidad** (equivalente al caso de las personas físicas, pudiendo no ser persistente)
  - **Nombre legal** (equivalente al nombre y apellidos de la persona física)
- El conjunto de **datos opcionales**, que el país emisor puede proporcionar o no en función de si son necesarios para vincular a una misma persona jurídica autenticaciones sucesivas, está formado por:
  - Dirección actual
  - Número de registro de IVA
  - Número de referencia fiscal
  - El identificador relacionado con el artículo 3, apartado 1, de la Directiva 2009/101/CE del Parlamento Europeo y del Consejo (registro de sociedades)
  - El identificador de entidades jurídicas (LEI)
  - El número de registro e identificación de operadores económicos (número EORI)

- Número de impuestos especiales

En el caso de las personas jurídicas, es importante hacer notar que el marco de interoperabilidad exige que cuando se envíen datos de identificación de la persona jurídica, se envíen también los datos de la persona física que actúa en su nombre.

Integración de los servicios públicos españoles con eIDAS

En el caso de España, la solución que se ha previsto para posibilitar que los servicios públicos cumplan la obligación de reconocimiento de medios de identificación electrónica de otros países prevista en el reglamento eIDAS **se apoya en la existencia del sistema Cl@ve**, cuyo diseño se llevó a cabo de forma totalmente alineada con el reglamento (contemplando tanto la gestión de niveles de seguridad como el uso de medios de identificación electrónica de otros países europeos, inicialmente a través de la plataforma STORK).

Según este diseño, **los servicios públicos españoles** no se conectarán al nodo eIDAS directamente para solicitar la autenticación de ciudadanos extranjeros, sino que **accederán a través de Cl@ve**. De esta manera, mediante una única interfaz, tendrán a su disposición no solamente los sistemas de identificación notificados por los distintos Estados miembros tal como establece el reglamento eIDAS, sino también los sistemas de identificación de alcance nacional integrados en Cl@ve. Para que ello sea posible, la interfaz con Cl@ve se está evolucionando de manera que permita soportar todos los datos de

identificación previstos en el reglamento eIDAS, así como un conjunto de datos adicionales que faciliten la gestión de la identificación por parte de los proveedores de servicios públicos.

Conclusiones

La obligación de reconocimiento mutuo de medios de identificación electrónicos que establece el reglamento eIDAS constituye un importante impulso hacia la consolidación del mercado único digital en la Unión Europea, toda vez que una identificación electrónica segura constituye una de las piezas fundamentales para la confianza en el mundo digital, y en consecuencia, para la aceptación de los servicios electrónicos por parte de los ciudadanos.

Para que el cumplimiento de esta obligación sea posible, es necesario el despliegue de infraestructuras de administración electrónica a nivel nacional conforme al marco de interoperabilidad definido por el reglamento; esto supone tanto el desarrollo de nuevos servicios como la adaptación de los sistemas existentes.

Aunque la integración con eIDAS de todos los servicios públicos electrónicos nacionales, tal como exige el reglamento, constituye un reto nada desdeñable, el hecho de que en España dicha integración se realice a través del sistema Cl@ve, que ha sido diseñado con el reglamento eIDAS en mente y por tanto en completa alineación con su marco de interoperabilidad, y que ya

están utilizando numerosas entidades, facilitará notablemente la implantación del reglamento en el sector público español.

Autor: Carlos Gómez Muñoz

Subdirección General de Coordinación de Unidades TIC

Secretaría General de Administración Digital

Ministerio de Hacienda y Función Pública