El reglamento europeo eIDAS y su impacto en la identificación electrónica

III Foro de Identidad Red IRIS

2 de junio de 2016

Objetivos de eIDAS

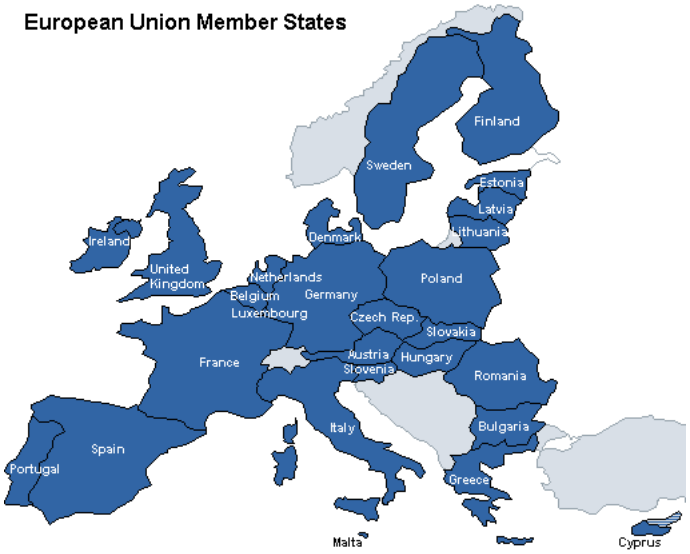
eIDAS: Regulation on Electronic identification and trust services for electronic transactions in the internal market (eIDAS)

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A LA IDENTIFICACIÓN ELECTRÓNICA Y LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS EN EL MERCADO INTERIOR Y POR LA QUE SE DEROGA LA DIRECTIVA 1999/93 CE

- Reforzar el Mercado Único europeo impulsando la confianza y la conveniencia en transacciones electrónicas transfronterizas seguras y sin fisuras

¿Cómo se logran los objetivos?

1. Asegurando que las personas y las empresas pueden usar y aprovechar sus eID nacionales de manera transfronteriza para acceder al menos a servicios públicos en otros países de la UE
   - Reconocimiento mutuo de identificación electrónica



¿Cómo se logran los objetivos?

2. Eliminando las barreras al mercado único para firmas electrónicas y los servicios de confianza online relacionados

→ Asegurando que los servicios de confianza tienen el mismo valor legal que en los procesos tradicionales en papel

- Firma electrónica
- Sello electrónico
- Dimensión transfronteriza de
  - Sello de tiempo electrónico
  - Servicio de entrega electrónica certificada
  - Documento electrónico
  - Autenticación de sitios web




eIDAS - Identificación

- Asegurar que es posible el acceso online a servicios ofrecidos por otro Estado Miembro mediante eID seguros.
  - **eID de personas físicas**
  - **eID de personas jurídicas**
- Obligación de los Estados Miembros de reconocer los **eID notificados** en servicios públicos
  - Opcional el uso en servicios privados
- Creación de un marco de interoperabilidad
  - Requisitos de interoperabilidad
  - Niveles de seguridad
- Prevé un mecanismo de cooperación entre Estados Miembros para la seguridad y la interoperabilidad técnica

Calendario

- Entró en vigor el **17 de septiembre de 2014**
- Lleva asociados una serie de actos de ejecución que desarrollan el reglamento
  - Especificaciones técnicas mínimas, normas y procedimientos con referencia a los cuales se especificarán los **niveles de seguridad** bajo, sustancial y alto de los medios de identificación electrónica
  - Circunstancias, formatos y procedimientos relativos a la **notificación**
  - Modalidades de procedimiento necesarias para facilitar la **cooperación** entre los Estados miembros
  - **Marco de interoperabilidad**
- Reconocimiento mutuo obligatorio 3 años después de la aplicación de los actos de implementación (en **2018**)
- Grupo de expertos para la elaboración de los actos de implementación creado en abril 2014.

Niveles de seguridad

- Los **niveles de seguridad** deben caracterizar **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.
- Referencias para determinar los niveles
  - Proyecto piloto a gran escala STORK
  - Norma ISO 29115
  - Respecto al nivel de seguridad alto, los requisitos en relación con la acreditación de identidad para la expedición de certificados cualificados.
- **Los requisitos que se establezcan deberán ser tecnológicamente neutros**. Debe ser posible cumplir los requisitos de seguridad necesarios mediante diversas tecnologías.
- El Reglamento define **3 niveles de seguridad** en la identificación y autenticación
  - **Básico** - reducir el riesgo de uso indebido o alteración de la identidad
  - **Sustancial** - reducir sustancialmente el riesgo de uso indebido o alteración de la identidad
  - **Alto** - cuyo objetivo es evitar el uso indebido o alteración de la identidad
- El **proveedor del servicio define el nivel de calidad** en la autenticación que requiere para su servicio
- Cada país decide qué mecanismos de identificación incorpora al sistema
  - **Notificación** del mecanismo
  - Asignación del nivel de calidad

Niveles de seguridad

Elementos a tener en cuenta para determinar los niveles de seguridad

- Inscripción
  - Solicitud y registro
  - Prueba y verificación de la identidad (persona física)
  - Prueba y verificación de la identidad (persona jurídica)
  - Vinculación entre persona física y jurídica
- Gestión de medios de identificación
  - Características y diseño de los medios
  - Expedición, entrega y activación
  - Suspensión, revocación y reactivación
  - Renovación y sustitución
- Autenticación
  - Mecanismo de autenticación
- Gestión y organización
  - Disposiciones generales
  - Avisos publicados e información del usuario
  - Gestión de la seguridad de la información
  - Conservación de la información
  - Instalaciones y personal
  - Controles técnicos
  - Cumplimiento y auditoría

Reconocimiento mutuo

- Obligatorio únicamente para **servicios públicos**
- Se refiere únicamente a la **autenticación a efectos de un servicio en línea**.
- **El sistema de identificación electrónica** del Estado miembro que efectúa la notificación **cumple las condiciones de notificación y esta se ha publicado** en el Diario Oficial de la Unión Europea.
- **El acceso a estos servicios en línea y su prestación final al solicitante deben estar estrechamente vinculados al derecho a recibir dichos servicios en las condiciones fijadas por la legislación nacional**.
- Niveles de seguridad
  - Se refiere únicamente a los **medios cuyo nivel de seguridad de la identidad corresponde a un nivel igual o superior al exigido** para el servicio en línea de que se trate.
  - **Habrá de aplicarse** únicamente cuando el organismo del sector público en cuestión emplee **el nivel de seguridad «sustancial» o «alto»** en lo tocante al acceso a dicho servicio en línea
- **La autenticación transfronteriza deberá ser gratuita** cuando se realice en relación con **un servicio en línea prestado por un organismo del sector público**.

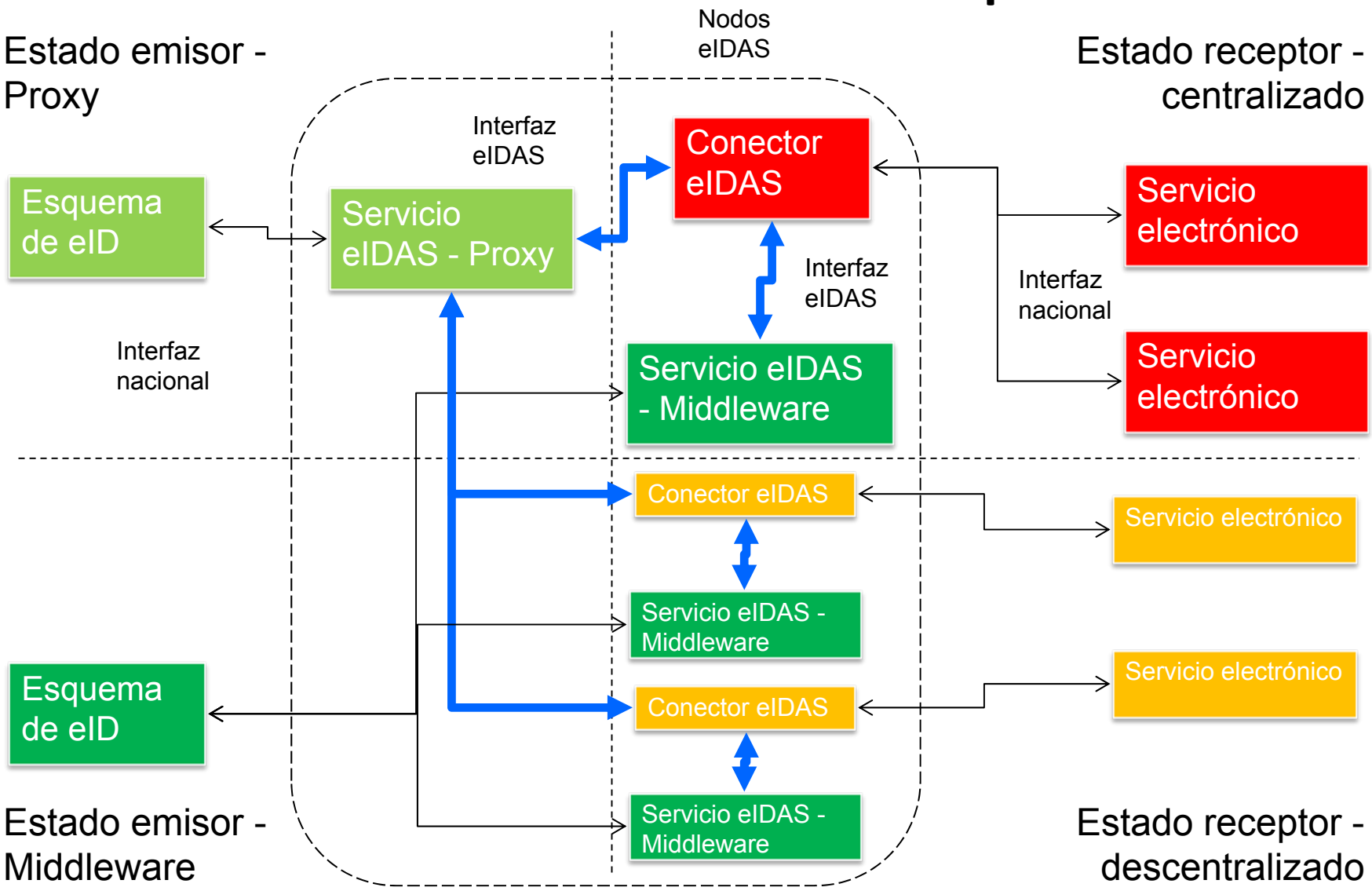
Reconocimiento mutuo

- El Reglamento **no se propone intervenir en los sistemas** de gestión de la identidad electrónica e infraestructuras conexas **establecidos en los Estados miembros**.
  - Los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de identificación electrónica, medios de acceder a los servicios en línea.
- **Los Estados miembros no deben estar obligados a notificar sus sistemas** de identificación electrónica a la Comisión.
- Sector privado
  - Puede intervenir en la provisión de los medios de identificación
  - Los Estados miembros **deben fomentar que el sector privado utilice voluntariamente** los medios de identificación electrónica amparados en un sistema notificado
  - **Mismas condiciones** de uso para las partes usuarias del sector privado establecidas fuera del territorio de un Estado miembro que las aplicadas a las partes usuarias del sector privado establecidas dentro de dicho Estado miembro.
  - El Estado miembro que efectúa la notificación podrá definir **condiciones de acceso** a los medios de autenticación.
    - Esto incluye la posibilidad de que esas condiciones supongan un coste para las partes usuarias del sector privado

Arquitectura de interoperabilidad

- Especificaciones técnicas
  - Disponibles en https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10
  - Cuatro documentos
    - Arquitectura de interoperabilidad
    - Perfil de atributos SAML
    - Formato de los mensajes
    - Requisitos criptográficos
- Interfaz eIDAS
  - Mensajes SAML firmados
  - TLS
  - HTTP Post binding o HTTP Redirect binding
  - Confianza basada en intercambio de metadatos
  - Aserciones encriptadas
- Información manejada
  - **Datos de identificación**
  - Nivel de seguridad
  - Características del servicio electrónico que solicita la identificación
    - Sector público / privado, para verificar las condiciones de acceso

Arquitectura de interoperabilidad



Personas físicas

- Datos obligatorios
  - Identificador de unicidad (no persistente en todos los países)
  - Nombre
  - Apellido
  - Fecha de nacimiento
- Datos no obligatorios
  - Nombre al nacer
  - Apellido al nacer
  - Lugar de nacimiento
  - Dirección actual
  - Género
- Semántica
  - Datos mapeados a los ISA Core Vocabularies
    - Vocabulario para personas
- Posibilidad de extender la información con atributos opcionales
  - Todavía por definir (p. ej. grado obtenido, suplemento del título)

Personas físicas

Identificador	Nombre	Apellido	Fecha de nacimiento	Dirección actual
UK/ES/a34dtfte19384	John	Smith	4-03-1965	12, Abbey Road

Servicio electrónico

¿Es la misma persona?

Identificador	Nombre	Apellido	Fecha de nacimiento	Dirección actual
UK/ES/2rft465i982389	John	Smith	4-03-1965	7, Downing Street

Personas jurídicas

- Datos obligatorios
  - Identificador de unicidad
  - Nombre legal
- Datos no obligatorios
  - 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
- Semántica
  - Datos mapeados a los ISA Core Vocabularies
    - Vocabulario para organizaciones registradas
- Atributos adicionales opcionales

Personas físicas representando personas jurídicas

Identificador de persona física	Nombre	Apellido	Fecha de nacimiento	Dirección actual
UK/ES/a34dtfte19384	John	Smith	4-03-1965	12, Abbey Road

Servicio electrónico

Identificador de persona jurídica	Nombre legal	Número de referencia fiscal
UK/ES/234t589yhf459	Marks and Spencer plc	04578932456

Identificación de personas físicas en España

- **Real Decreto 2393/2004**, de 30 de diciembre, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.
- **Artículo 101. Número de identidad de extranjero.**
  - 1. Los extranjeros que obtengan un documento que les habilite para permanecer en territorio español, aquellos a los que se les haya incoado un expediente administrativo en virtud de lo dispuesto en la normativa sobre extranjería y **aquellos que por sus intereses económicos, profesionales o sociales, se relacionen con España serán dotados, a los efectos de identificación, de un número personal, único y exclusivo, de carácter secuencial**.
  - 2. **El número personal será el identificador del extranjero**, que deberá figurar en todos los documentos que se le expidan o tramiten, así como en las diligencias que se estampen en su pasaporte o documento análogo.
- ¿Se usa el NIE como identificador en TODOS los servicios públicos?
- ¿Hay algún otro identificador alternativo (pasaporte, número de identificación de su país de origen …)?

Identificación de personas jurídicas en España

- Las personas jurídicas constituidas en España tienen como identificador único el NIF
  - En principio, todas las personas jurídicas españolas deben tener uno
- El NIF se puede asignar también a personas jurídicas y entidades extranjeras
  - Letras N y W
- ¿Es la situación del NIF equivalente a la del NIE?
  - ¿Todas las entidades extranjeras que se relacionen con España deben tener un NIF?
- ¿ Hay algún otro identificador alternativo (nombre legal, número de identificación de su país de origen …)?

Reconciliación de identidades

Identificador	Nombre	Apellido	Fecha de nacimiento	Dirección actual
UK/ES/a34dtfte19384	John	Smith	4-03-1965	12, Abbey Road

Servicio electrónico

¿Es la misma persona?

Expediente	Fecha de inicio	NIE	Nombre	Apellido	Estado
34567823	4-01-2016	X0123768K	John	Smith	Iniciado

Reconciliación de identidades

Identificador	Nombre	Apellido	Fecha de nacimiento
PT/ES/3456892	João	Gomes	14-08-1975

Servicio electrónico

¿Es la misma persona?

Αντώνης Στασής

Antonis Stasis

Христо Стоичков

Hristo Stoichkov

Expediente	Fecha de inicio	NIE	Nombre	Apellido	Fecha de nacimiento
32356744	14-01-2016	X0694768T	Joao	Gomes	14-08-1975

Identificación frente a firma

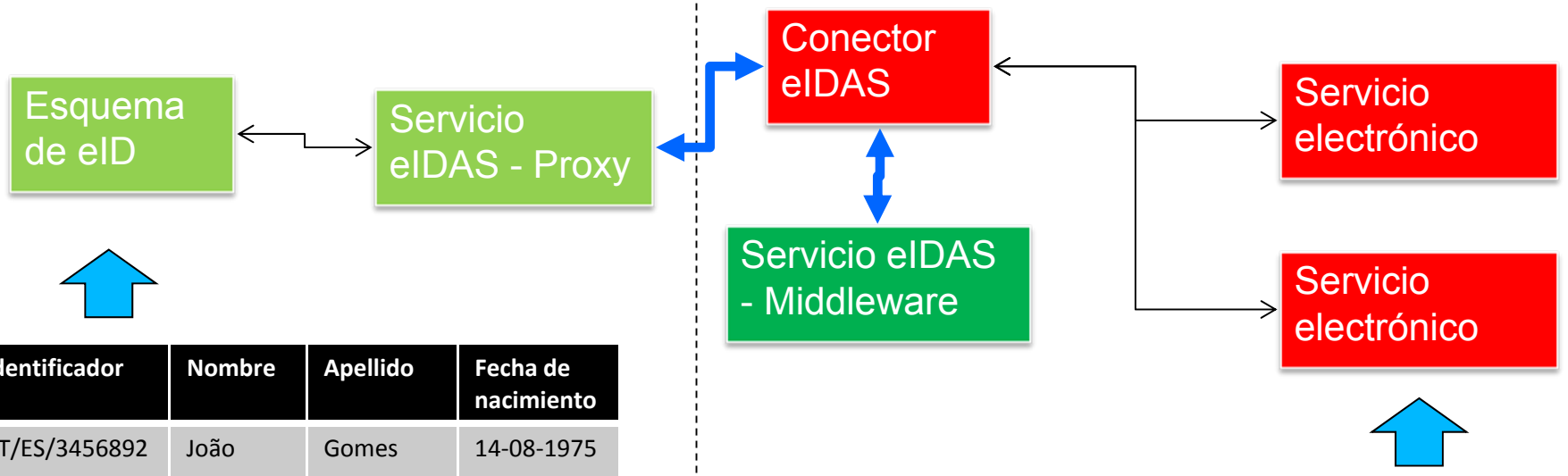
- Identificación
  - Verificar la identidad
- Firma
  - Constatación de la voluntad
  - Debe estar ligada a una identidad
- Según eIDAS
  - La identificación la respalda el Estado Miembro directamente
  - La firma indirectamente, a través de un prestador autorizado
- Transacción con identificación y firma
  - ¿La persona que se identificó es la misma que firmó?

Identificación frente a firma

- Personas físicas
  - Los certificados cualificados de firma electrónica contendrán:
    - c) al menos el **nombre del firmante o un seudónimo**; si se usara un seudónimo, se indicará claramente
- Personas jurídicas
  - Los certificados cualificados de sello electrónico contendrán:
    - c) al menos, el **nombre del creador del sello y, cuando proceda, el número de registro**, tal como se recojan en los registros oficiales

Estrategias de adaptación

Envío directo



Identificador	Nombre	Apellido	Fecha de nacimiento
PT/ES/3456892	João	Gomes	14-08-1975

Identificador	Nombre	Apellido	Fecha de nacimiento
PT/ES/3456892	João	Gomes	14-08-1975

Estrategias de adaptación

Servicio común

Identificador eIDAS	Nombre eIDAS	Apellido eIDAS	Fecha de nacimiento	NIE	Nombre	Apellido
PT/ES/3456892	João	Gomes	14-08-1975	X-0694768-T	Joao	Gomes

Servicio de mapeo

NIE	Nombre	Apellido
X-0694768-T	Joao	Gomes

Esquema de eID

Servicio eIDAS - Proxy

Conector eIDAS

Servicio electrónico

Servicio electrónico

Servicio eIDAS - Middleware

Identificador	Nombre	Apellido	Fecha de nacimiento
PT/ES/3456892	João	Gomes	14-08-1975

Implantación y operación del nodo eIDAS en España

- El marco de interoperabilidad exige que haya **un único nodo nacional** que establece la confianza respecto al esquema de eID
  - Servicio eIDAS – Proxy
  - Servicio eIDAS – Middleware
- En STORK España adoptó la **configuración Proxy** en lugar de Middleware
  - En principio se va a mantener
  - Facilita la utilización de varios eID
- Podría haber varios conectores eIDAS para enlazar con los servicios
- El operador del nodo nacional eIDAS será la DTIC, de acuerdo con el Real Decreto 802/2014
  - Corresponde a la DTIC
    - "ñ) la identificación, diseño y ejecución de programas y proyectos para el desarrollo de la administración digital en el ámbito de la Administración General del Estado y sus Organismos Públicos y, en su caso, de **la Unión Europea**, de las Administraciones de las Comunidades Autónomas y de las Entidades Locales, mediante la **implantación y explotación de infraestructuras tecnológicas, sistemas, redes de comunicación y servicios comunes**."
- La Comisión ha liberado una implementación de referencia del nodo eIDAS que cumple con las especificaciones técnicas, dentro del marco del programa CEF
- La DTIC está trabajando ya en la instalación de esa implementación de referencia y su integración con la infraestructura nacional de administración electrónica

Cl@ve y eIDAS

cl@ve
IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

- **Proyecto colaborativo** promovido por la DTIC y alineado con las medidas CORA
- Gobernanza
  - Grupo de trabajo reducido: Entidades responsables del sistema: DTIC, AEAT, GISS, DG Policía + DG Tráfico
  - Grupo de trabajo extendido
- Formalizado por el **Acuerdo de Consejo de Ministros del 19 de septiembre de 2014**
  - Cl@ve es la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, abierta a su utilización por parte de todas las Administraciones Públicas.
  - Uso obligatorio para el Sector Público Administrativo Estatal a finales de 2015
- Técnicamente se apoya en los resultados del proyecto europeo STORK
  - Especificaciones: perfil
  - Implementación del SW (PEPS, paquetes de integración)
- Empezó a operar el 17 de noviembre de 2014

Cl@ve y eIDAS

- Sistema orientado a **unificar y simplificar el acceso electrónico** de los ciudadanos a los servicios públicos
  - Principal objetivo: un ciudadano puede identificarse y autenticarse frente a una entidad pública usando claves concertadas, sin tener que recordar claves diferentes para acceder a servicios distintos
- **Complementa los sistemas actuales** basados en DNI-e y certificados electrónicos
- Requiere **registro previo**
  - Presencial
  - Online: Certificado electrónico / datos conocidos por ambas partes (información tributaria)
- **Dos modalidades** de identificación electrónica basada en claves concertadas
  - **Cl@ve PIN**: Usuario (NIF) + contraseña formada por dos partes, una de ellas elegida por el ciudadano, la otra un código enviado a su teléfono móvil por SMS con validez limitada en el tiempo. Destinado a usuarios que acceden a los servicios de forma esporádica.
  - **Cl@ve permanente**: Usuario (NIF) + contraseña definida y custodiada por el ciudadano, reforzada (si se requiere) por un código enviado por SMS al móvil.
- Ofrecerá la posibilidad de **firmar en la nube** con certificados personales custodiados en servidores remotos.

Cl@ve y eIDAS

Alineamiento con eIDAS

- Integración con **eID extranjeros**
  - Soporte de la futura obligación de reconocimiento de eID de otros EEMM
  - Ahora mediante STORK
- El proveedor del servicio define el **nivel de aseguramiento** de la autenticación que exige para acceder a su servicio
- Niveles de aseguramiento basados en
  - La fase de **registro** (con datos conocidos por ambas partes, certificado o presencial)
  - La fase de **autenticación** (tipo de credencial usada)
- Niveles alineados con los que están previstos en eIDAS
  - **Bajo** (Registro débil, Clave Permanente sin SMS)
  - **Sustancial** (Clave PIN y Clave Permanente reforzado, certificado SW)
  - **Alto** (DNI-e, certificado HW)

Cl@ve y eIDAS

Proveedor del servicio de administración electrónica (SP)

Interfaz adaptada
Interfaz Cl@ve

Servicio de e-Admon

Gestor de identificación

AEAT

GISS

Cl@ve PIN

Cl@ve Permanente

Comunicación mediante redirecciones del navegador (aserciones SAML)

Proveedores de servicios de identificación y autenticación (IdP)

@firma

Intermediador de DNIe y certificados

Conector eIDAS

Intermediador de eID extranjeros