

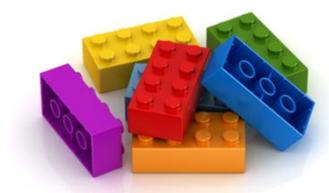


GOBIERNO
DE ESPAÑA

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

SECRETARÍA GENERAL
DE ADMINISTRACIÓN DIGITAL



IDENTIFICACION ELECTRONICA CL@VE 2.0

SOCINFO: Firma-e en la AAPP: estado actual y nuevas soluciones

19 de febrero de 2020

Contenidos

- Base legal
- Cl@ve 1.0
- Nodo eIDAS
- Cl@ve 2.0
- Datos de uso

Contenidos

- **Base legal**
- Cl@ve 1.0
- Nodo eIDAS
- Cl@ve 2.0
- Datos de uso

Normativa de identificación y firma aplicable en España

Normativa Europea y Estándares

- Reglamento 910/2014. eIDAS
- Nodos eIDAS.
- IMPLEMENTING DECISION (EU) 2015/1506. Formatos firma.
- IMPLEMENTING DECISION (EU) 2015/1505. TSL

Legislación Española

- Ley 39/2015 de Procedimiento Administrativo
- Ley 40/2015 de Régimen Jurídico
- Real Decreto 4/2010 del Esquema Nacional de Interoperabilidad.
- NTI de Política de firma
- Anteproyecto Ley Reguladora de los Servicios Electrónicos De Confianza
- Proyecto de Real Decreto por el que se desarrollan la Ley 39/2015, y la Ley 40/2015

Id y firma. Ley 39/2015

Preámbulo

*Por otro lado, este título [I] dedica parte de su articulado a una de las novedades más importantes de la Ley: **la separación entre identificación y firma electrónica y la simplificación de los medios para acreditar una u otra, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento del interesado [Artículo 11]. Se establece, con carácter básico, un conjunto mínimo de categorías de medios de identificación y firma a utilizar por todas las Administraciones.***

Id y firma. Ley 39/2015

Artículo 9. Sistemas de identificación de los interesados en el procedimiento.

1. Las Administraciones Públicas **están obligadas a verificar la identidad de los interesados** en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.
2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas **a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad**. En particular, serán admitidos, los sistemas siguientes:
 - a) **Sistemas basados en certificados electrónicos reconocidos o cualificados** de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados **los de persona jurídica y de entidad sin personalidad jurídica**.
 - b) Sistemas basados en **certificados electrónicos reconocidos o cualificados de sello electrónico** expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».
 - c) **Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan**.Cada Administración Pública podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos, si bien **la admisión de alguno de los sistemas de identificación previstos en la letra c) conllevará la admisión de todos los previstos en las letras a) y b) anteriores para ese trámite o procedimiento**.
3. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

Id y firma. Ley 39/2015

Artículo 10. Sistemas de firma admitidos por las Administraciones Públicas.

1. Los interesados podrán firmar a través de cualquier medio que permita **acreditar la autenticidad de la expresión de su voluntad y consentimiento**, así como la integridad e inalterabilidad del documento.
2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de **firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados** de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.

b) Sistemas de **sello electrónico reconocido o cualificado** y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración Pública, Organismo o Entidad podrá determinar si sólo admite algunos de estos sistemas para realizar determinados trámites o procedimientos de su ámbito de competencia.

3. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

4. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.

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.
- 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.

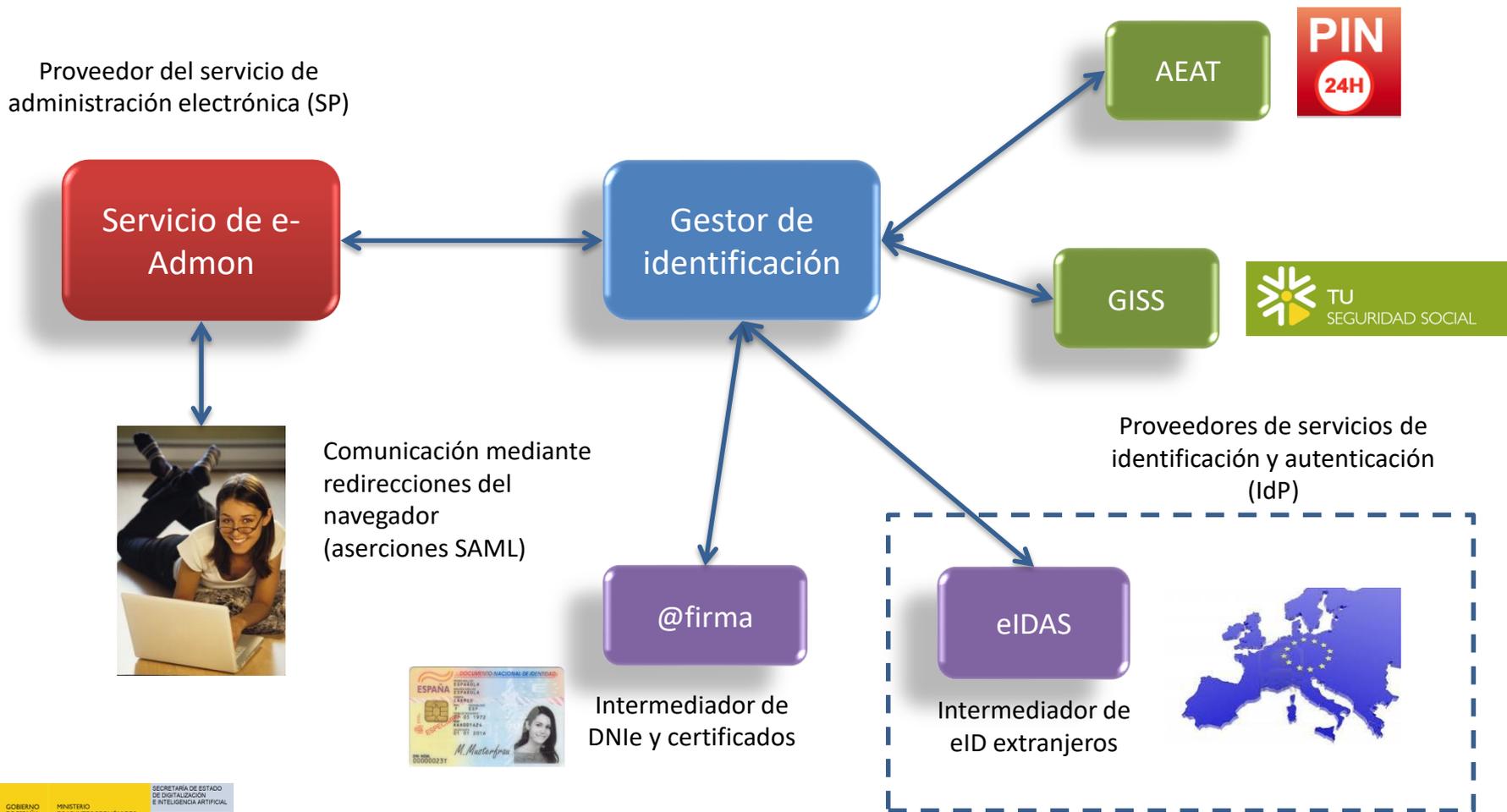
Contenidos

- Base legal
- **Cl@ve 1.0**
- Nodo eIDAS
- Cl@ve 2.0
- Datos de uso

Objetivos

- **Unifica y simplifica** el acceso electrónico a los servicios públicos
- **Complementa** sistemas actuales basados en **DNI-e** y **certificados electrónicos**
- Requiere registro previo: **presencial** u **online**
- Dos nuevas 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.
- Ofrece la **posibilidad de firmar en la nube** con certificados personales custodiados por la DGP.

Pasarela Cl@ve de autenticación



Cl@ve Pasarela



Seguridad Social



AEAT



... DGT



Ha sido redirigido a Cl@ve para identificarse en **Carpeta Ciudadana**

Elija el método de identificación

Si no transcurren más de 60 minutos entre autenticaciones y llamadas a Cl@ve, se le autenticará automáticamente de forma transparente.

 DNI-e / Certificado electrónico Acceder >	 Cl@ve PIN Acceder > Para usarlo es necesario registrarse	 Cl@ve permanente Acceder > Para usarlo es necesario registrarse	 Ciudadanos UE Acceder >
--	--	---	--------------------------------

Identificación por

- DNI-e
- Certificados electrónicos
- Clave PIN
- Clave Permanente
- Credenciales UE

© Gobierno de España · Cl@ve

Portal informativo

- Soporte a los **ciudadanos**
 - Portal informativo: <http://clave.gob.es>
 - Teléfono 060



Conoce Cl@ve

Identidad Electrónica para las Administraciones



¿Qué es?

Un sistema para identificarte electrónicamente en las relaciones con las Administraciones Públicas



¿Dónde puedo usarlo?

Cl@ve está pensado para usarlo con tu ayuntamiento, pedir cita médica, presentar tu declaración de impuestos...



¿Qué necesito para empezar?

Solamente tienes que registrarte en el sistema para obtener tus datos de acceso



¿Cómo funciona?

Rápido y sencillo, tu eliges cómo indentificarte en cada momento

Contenidos

- Base legal
- Cl@ve 1.0
- **Nodo eIDAS**
- Cl@ve 2.0
- Datos de uso

eIDAS: casos de uso de reconocimiento de eID transfronterizos

La red de nodos eIDAS de los Estados miembros de la UE da respuesta a dos casos de uso principales.

1

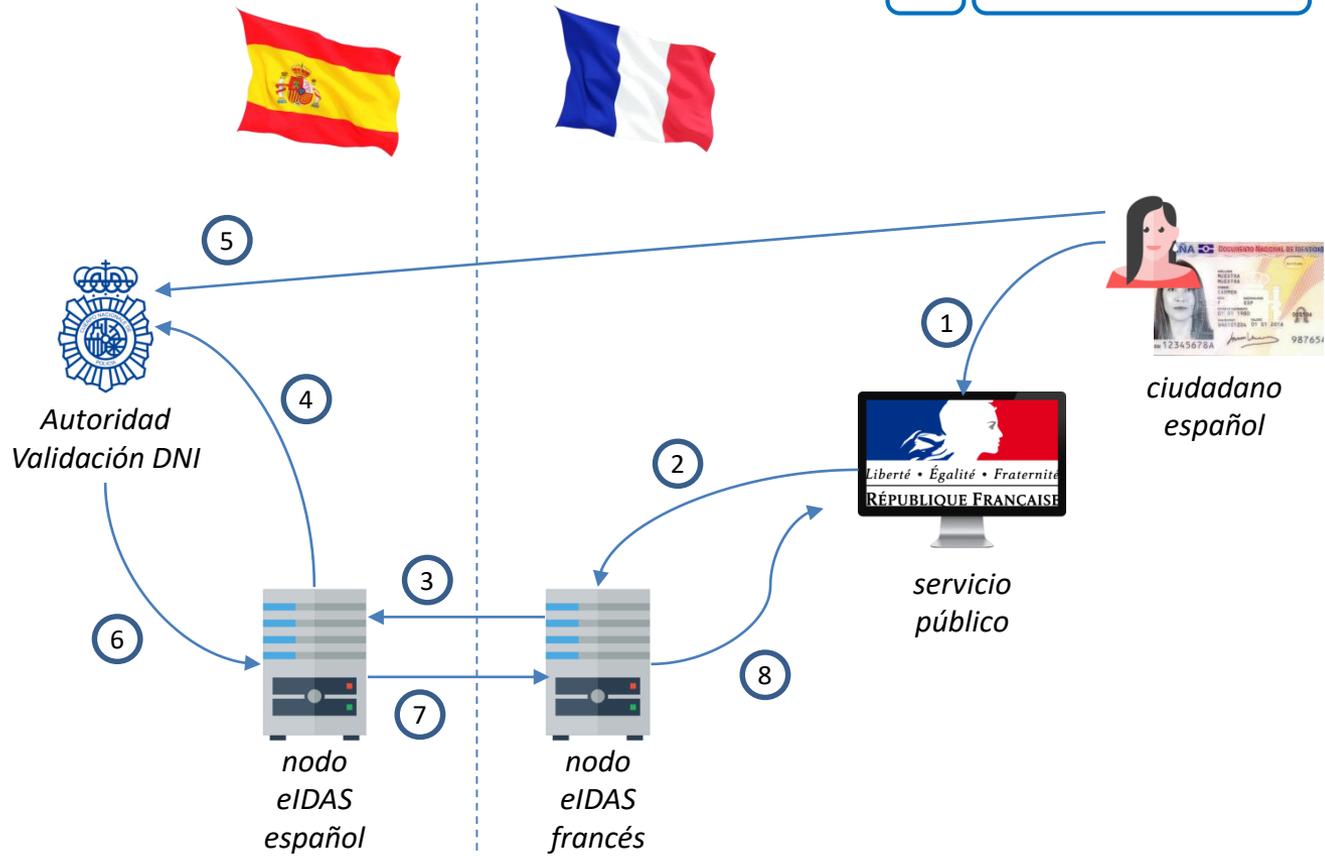
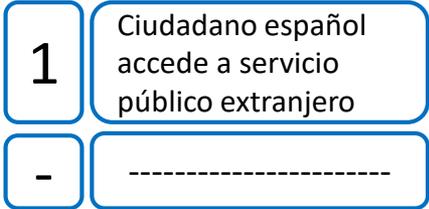
Identificar a un ciudadano nacional (*español*) que accede a un servicio público establecido en un EM extranjero

2

Identificar a un ciudadano de un EM extranjero que accede a un servicio público nacional (*español*)

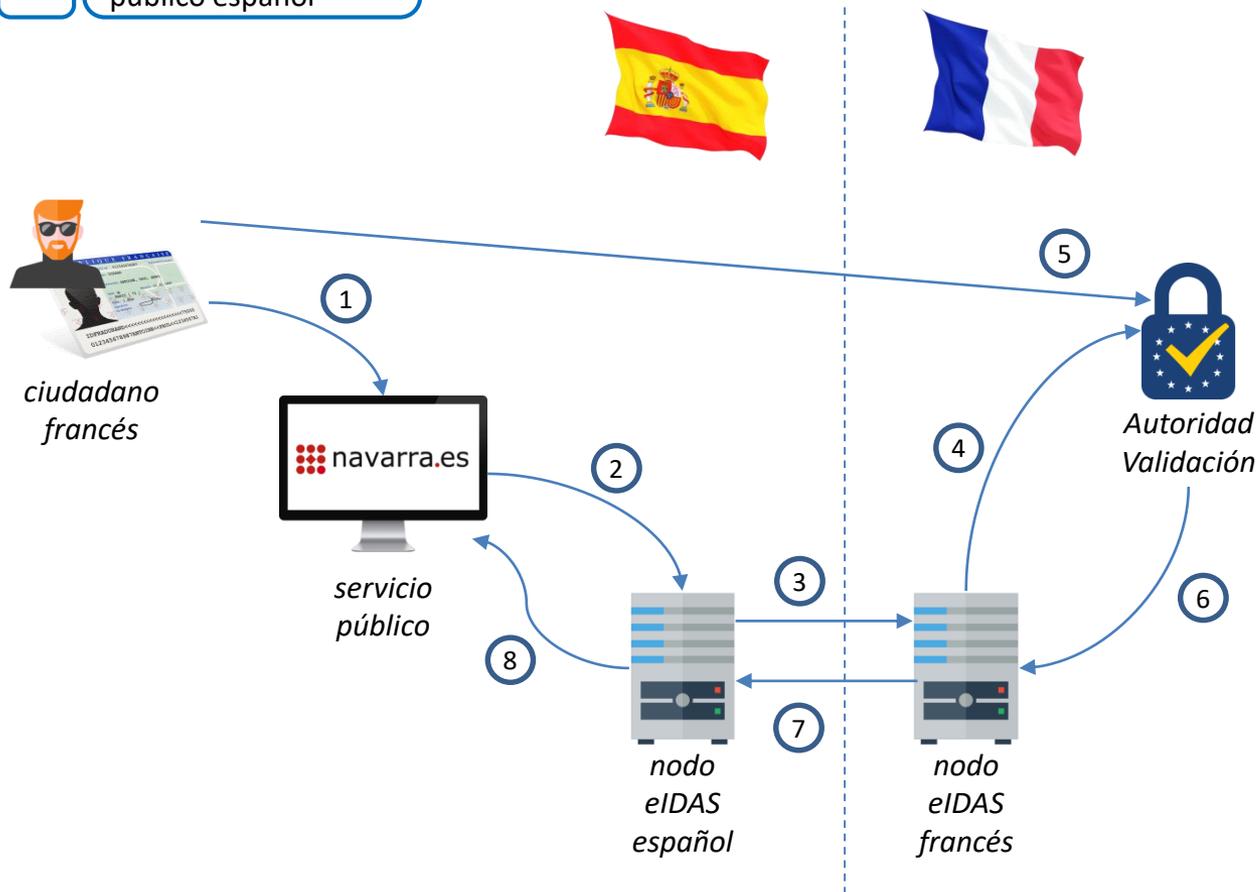
eIDAS: casos de uso de reconocimiento de eID transfronterizos

1. Ciudadano español accede a servicio público extranjero
2. Es redirigido al nodo eIDAS del país extranjero
3. Selecciona su país y es redirigido al nodo eIDAS español
4. Es redirigido a la autoridad que validará su identidad electrónica
5. El ciudadano presenta su identidad electrónica y ésta es verificada
6. El nodo eIDAS español recibe los datos de su identidad
7. Los datos de identidad se transmiten al nodo eIDAS extranjero
8. Los datos de identidad se transmiten al servicio público extranjero



eIDAS: casos de uso de reconocimiento de eID transfronterizos

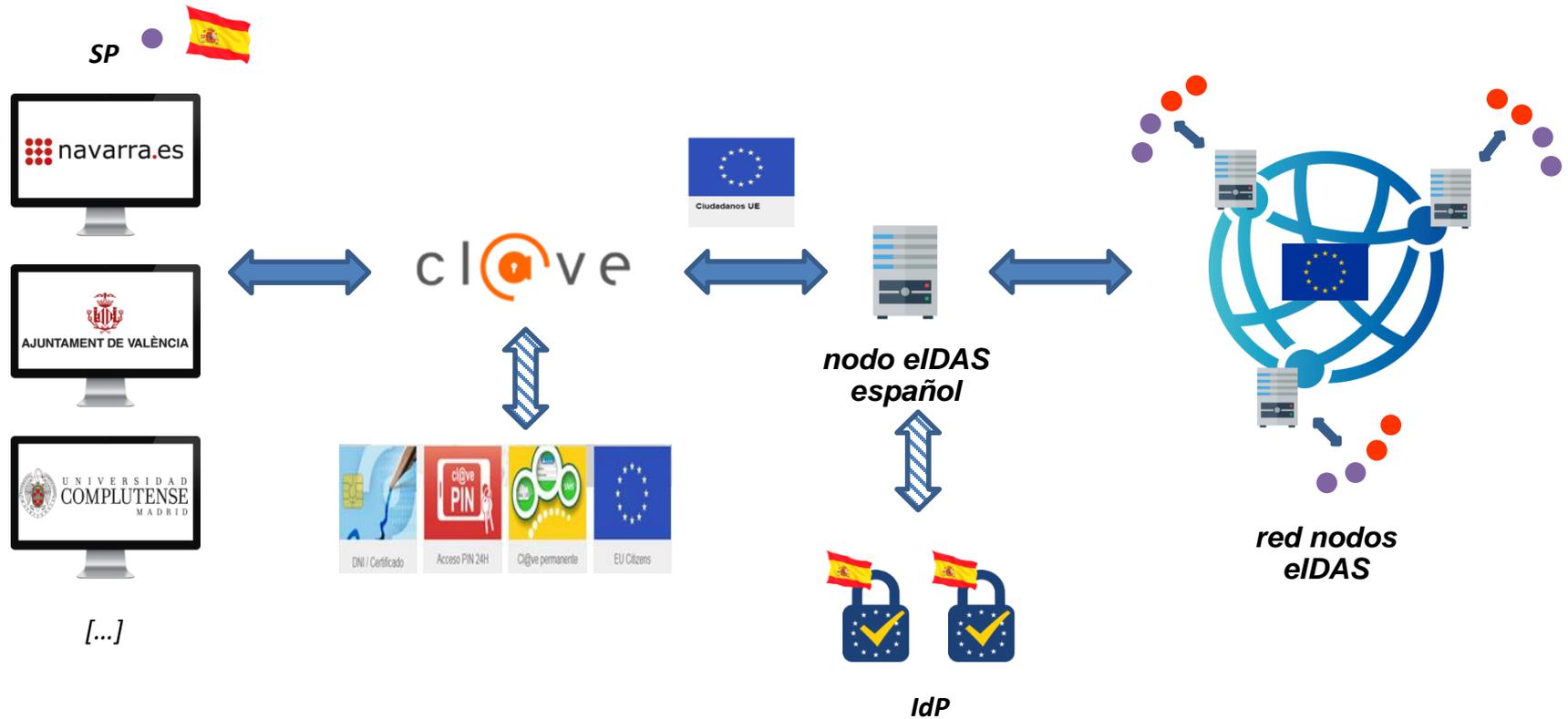
-
- 2 Ciudadano extranjero accede a servicio público español



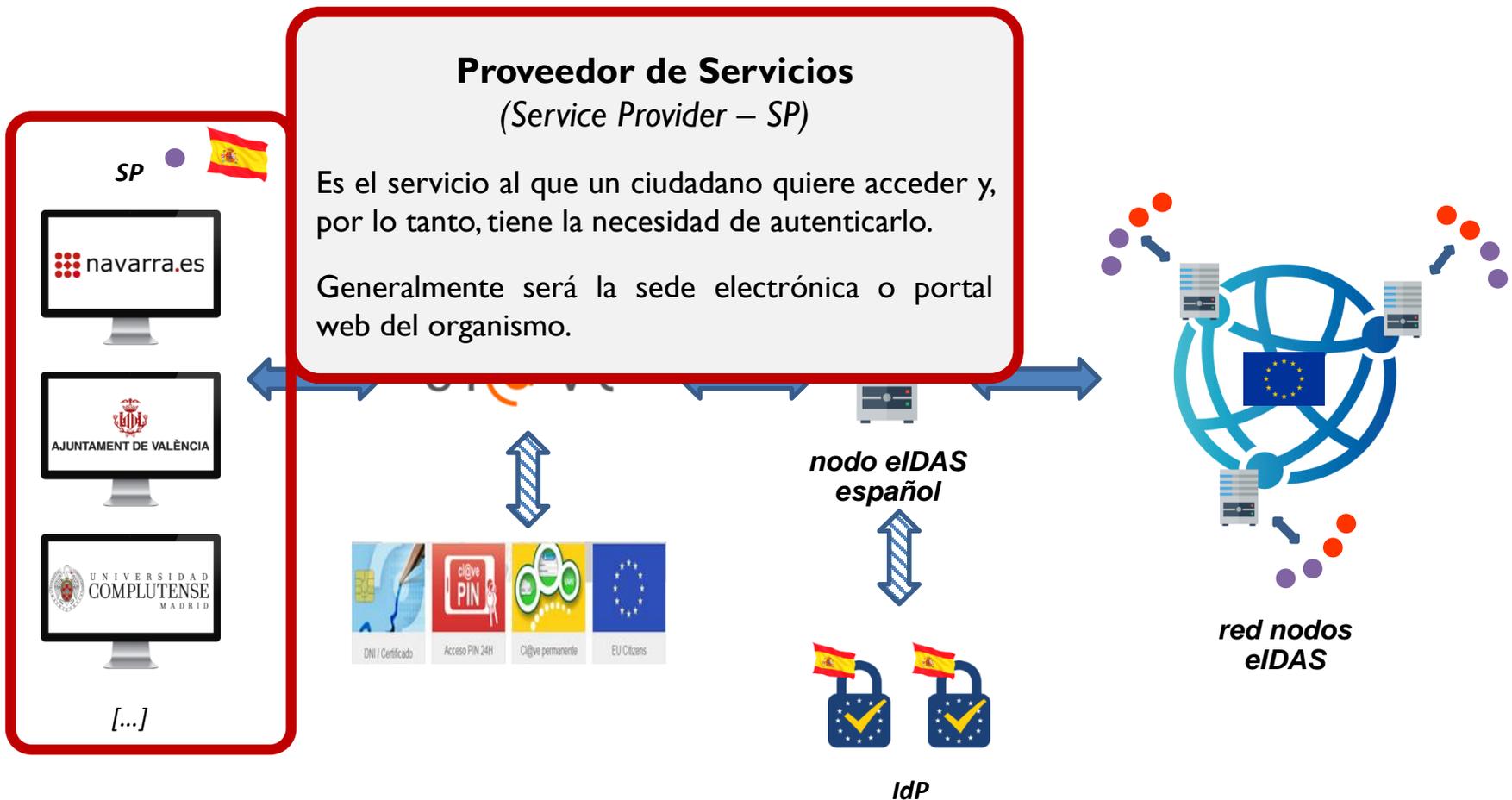
1. Ciudadano extranjero accede a servicio público español
2. Es redirigido al nodo eIDAS español
3. Selecciona su país y es redirigido a su nodo eIDAS extranjero
4. Es redirigido a la autoridad que validará su identidad electrónica
5. El ciudadano presenta su identidad electrónica y ésta es verificada
6. El nodo eIDAS extranjero recibe los datos de su identidad
7. Los datos de identidad se transmiten al nodo eIDAS español
8. Los datos de identidad se transmiten al servicio público español

Arquitectura de integración SPs- Nodo eIDAS

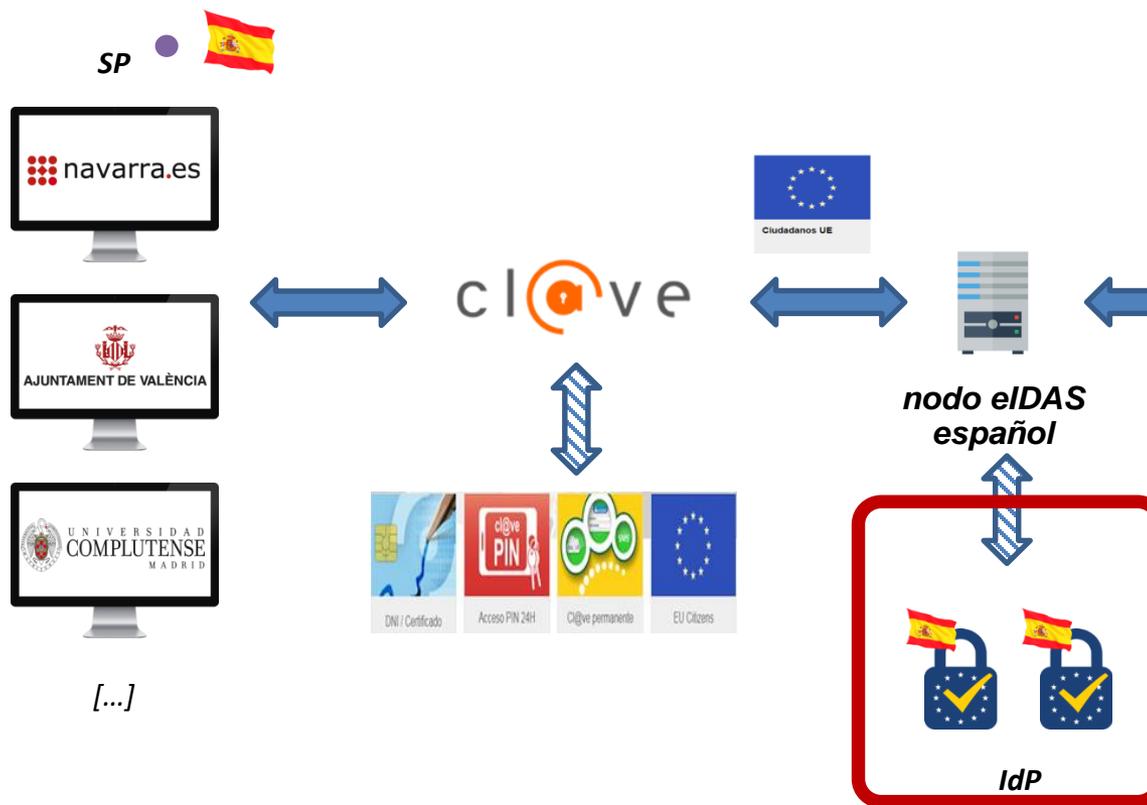
Los SPs del sector público se conectarán al nodo a través
Cl@ve 2.0.



Arquitectura de integración SPs- Nodo eIDAS



Arquitectura de integración SPs- Nodo eIDAS



Proveedor de Identidad (Identity Provider – IdP)

Es el elemento que valida la identidad electrónica de los ciudadanos de un país que se encuentran en el extranjero.

Cada país define los esquemas de identificación que desea usar y, en consecuencia, los proveedores de identidad que utilizará.

En el caso de España el esquema de identificación inicial es el DNI electrónico.

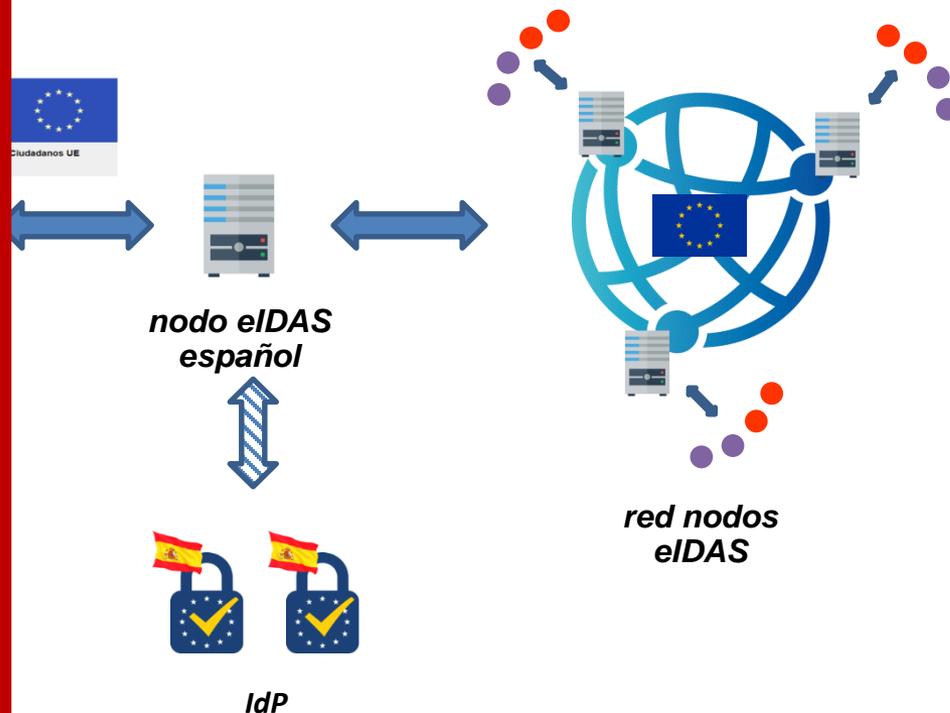
Arquitectura de integración SPs- Nodo eIDAS

Los SPs se conectarán al nodo a través

Nodo eIDAS

Es el elemento que hace de intermediación entre los SP e IdP del país donde está instalado y el resto de los nodos eIDAS extranjeros. Se divide en dos partes:

- i. **Conector.** Se comunica con los SPs del país donde está instalado (recibe las peticiones de autenticación de los SP nacionales, permite al ciudadano seleccionar su país, redirige al nodo extranjero, recibe la identidad y se la comunica al SP).
- ii. **Servicio (*proxy service*).** Se comunica con los IdPs del país donde está instalado (recibe las peticiones de autenticación de los nodos extranjeros, redirige al IdP, recibe la identidad y se la comunica al nodo original).



Arquitectura de integración SPs- Nodo eIDAS

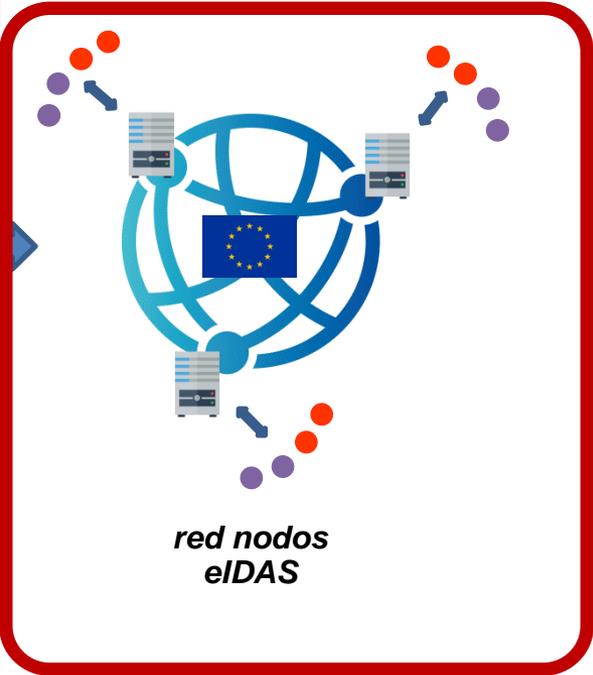


Red nodos eIDAS

Es la red de nodos eIDAS*, SPs e IdPs instalada en el resto de países de la Unión Europea.

No existe un elemento central, sino que se realiza una comunicación bidireccional entre todos los nodos eIDAS de la red.

**Nota: excepto para los países que optan por el modelo middleware comentado anteriormente.*



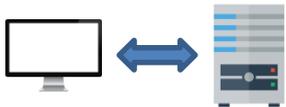
IdP

Las principales características de la comunicación entre los distintos elementos de la arquitectura son:



La comunicación entre los nodos se realiza mediante las especificaciones técnicas eIDAS¹ de la Unión Europea:

- Se intercambian mensajes SAML2² (*AuthnRequest* y *Response*).
- Cada nodo publica sus metadatos (*Metadata*) en una URL pública en https.
- Todos los mensajes van **firmados** por los nodos.
- Los datos personales de las respuestas van **encriptados**.
- Existe un paso inicial de intercambio de certificados para establecer la confianza entre los nodos.



Cada país define libremente la interfaz de comunicación entre los SPs ubicados en su territorio y su nodo eIDAS.

En el caso de España se ha optado por usar la misma comunicación que la que se realiza entre los nodos (SAML2 perfil eIDAS).



La interfaz de comunicación entre el nodo eIDAS y el IdP también puede ser definida libremente por cada país y normalmente dependerá del propio IdP (por ejemplo, mediante OCSP).

Cl@ve

Reconocimiento mutuo de esquemas de identificación eIDAS

Sep'18

Sep'19

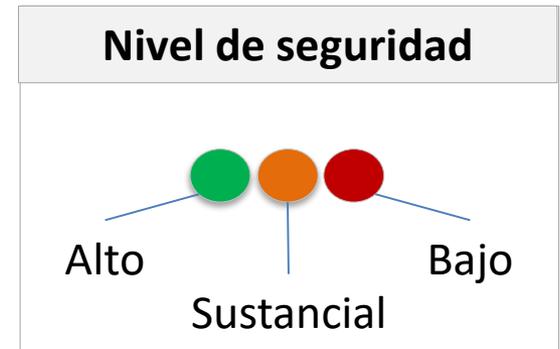
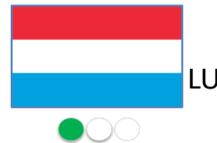
Nov'19

Dic'19

Feb'20

May'20

Sep'20



Contenidos

- Base legal
- Cl@ve 1.0
- Nodo eIDAS

- **Cl@ve 2.0**

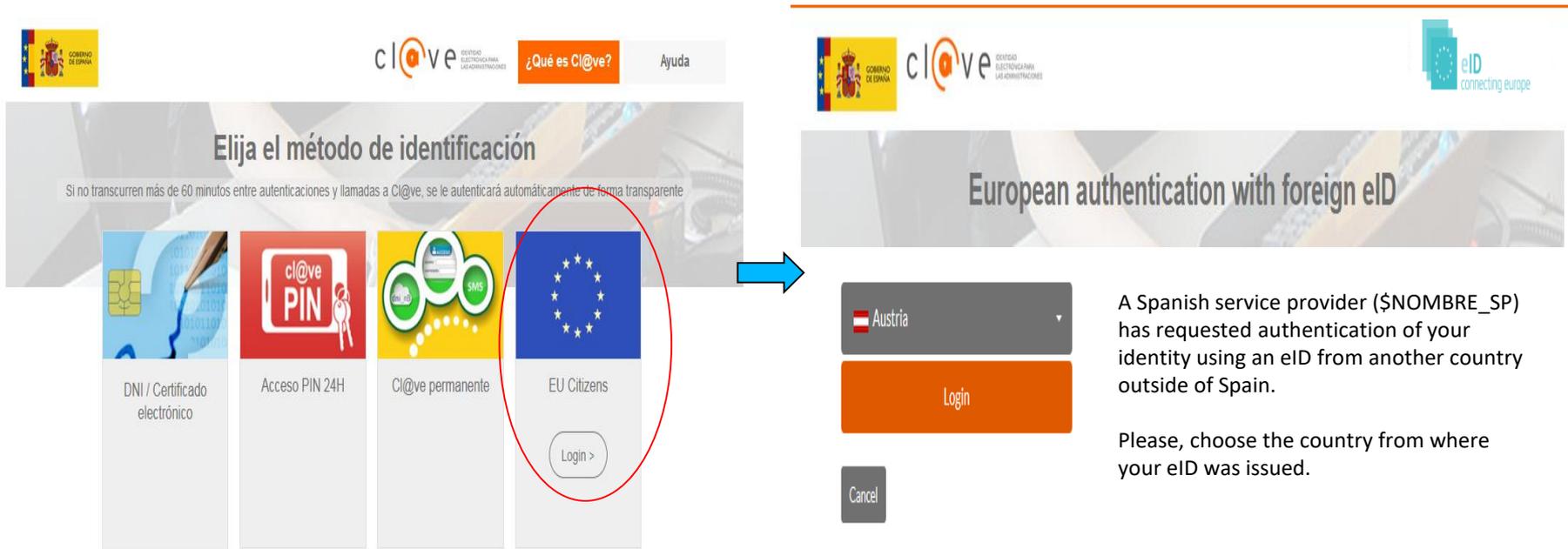
- Datos de uso

Arquitectura de integración

SPs- Nodo eIDAS



Desde Cl@ve 2.0 se ofrece al ciudadano la posibilidad de autenticarse mediante el acceso al nodo eIDAS como una opción adicional.



Reglamento eIDAS - Identificación

- Datos identificativos **obligatorios**:
 - Nombre - *CurrentGivenName*
 - Apellido - *CurrentFamilyName*
 - Identificador único - *PersonIdentifier*
 - Fecha de nacimiento – *DateOfBirth*
- El campo ***PersonIdentifier*** es de formato libre. Es **único**, pero **puede no ser persistente**.
- Aplicaciones de los SPs adaptadas a gestionar **NIF/NIE** (9 posiciones, formato rígido) como dato de identificación.

Cl@ve

Persistencia y datos opcionales eIDAS

Req	Atributo								
		DE	HR	EE	IT	LU	ES	PT	BE
✓	Nombre actual	●	●	●	●	●	●	●	●
✓	Apellido actual	●	●	●	●	●	●	●	●
✓	Fecha de nacimiento	●	●	●	●	●	●	●	●
✓	Identificador	●	●	●	●	●	●	●	●
-	Lugar de nacimiento	●	●	○	●	●	○	○	●
-	Nombre de nacimiento	●	○	○	○	○	○	○	○
-	Domicilio actual	●	●	○	●	●	○	●	
-	Género	○	●	○	●	●	○	●	●

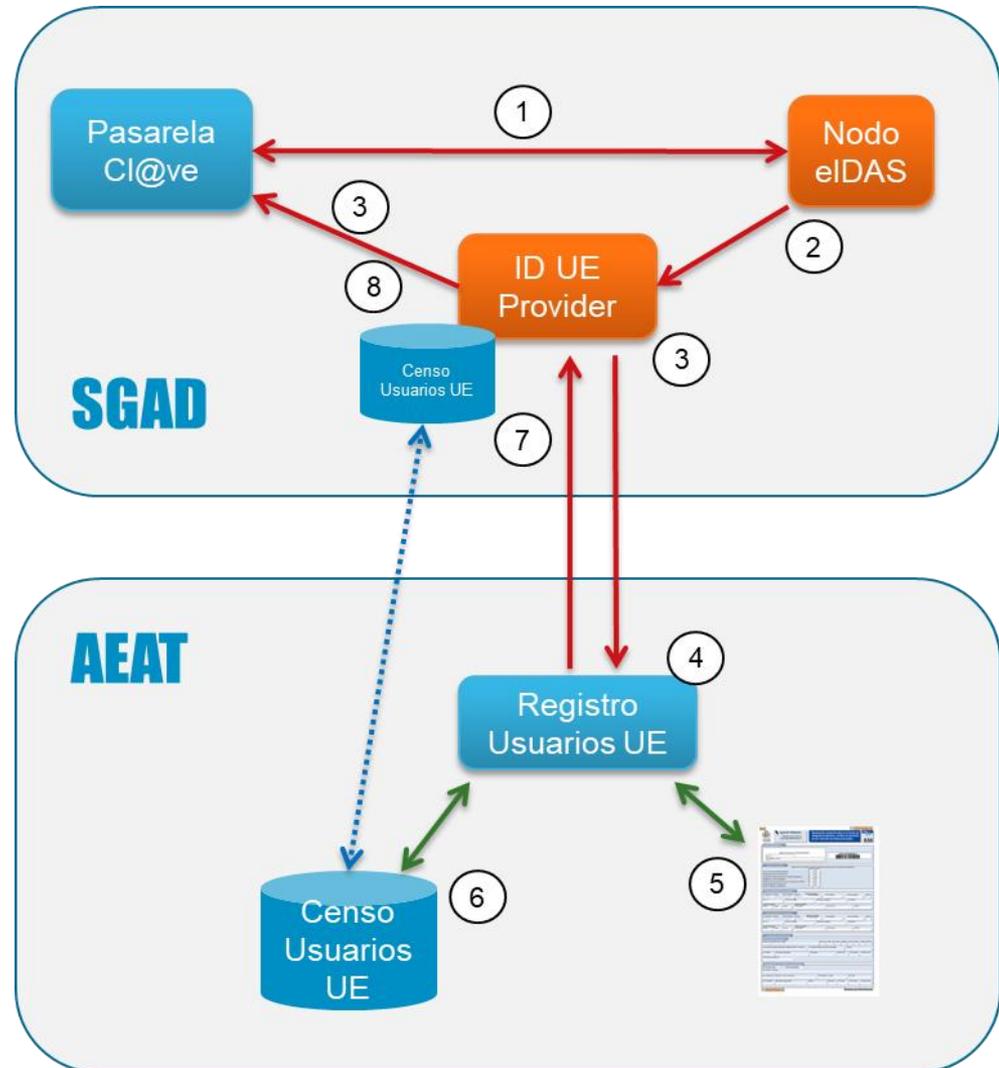
No persistentes

Reglamento eIDAS / tipología de usuarios

- Ciudadanos de otros países de la UE que no residen en España (**no tienen un NIE**) y quieren utilizar un mecanismo de identificación y autenticación notificado por otro país de la UE.
- Ciudadanos de otros países de la UE que viven en España (**tienen un NIE**) y quieren utilizar un mecanismo de identificación y autenticación notificado por otro país de la UE.
- Ciudadanos españoles (**tienen un DNI**) que viven en otros países de la UE y tienen un mecanismo de identificación y autenticación notificado del país de residencia.
- Ciudadanos españoles (**no tienen un DNI**) que viven en otros países de la UE y tienen un mecanismo de identificación y autenticación notificado del país de residencia.

Reglamento eIDAS / solución propuesta

- Ciudadanos españoles residentes en el extranjero sin DNI: Código con formato NIF cuyo primer carácter es “L”
- Ciudadanos extranjeros sin NIE: Código con formato NIF cuyo primer carácter es “M”



Contenidos

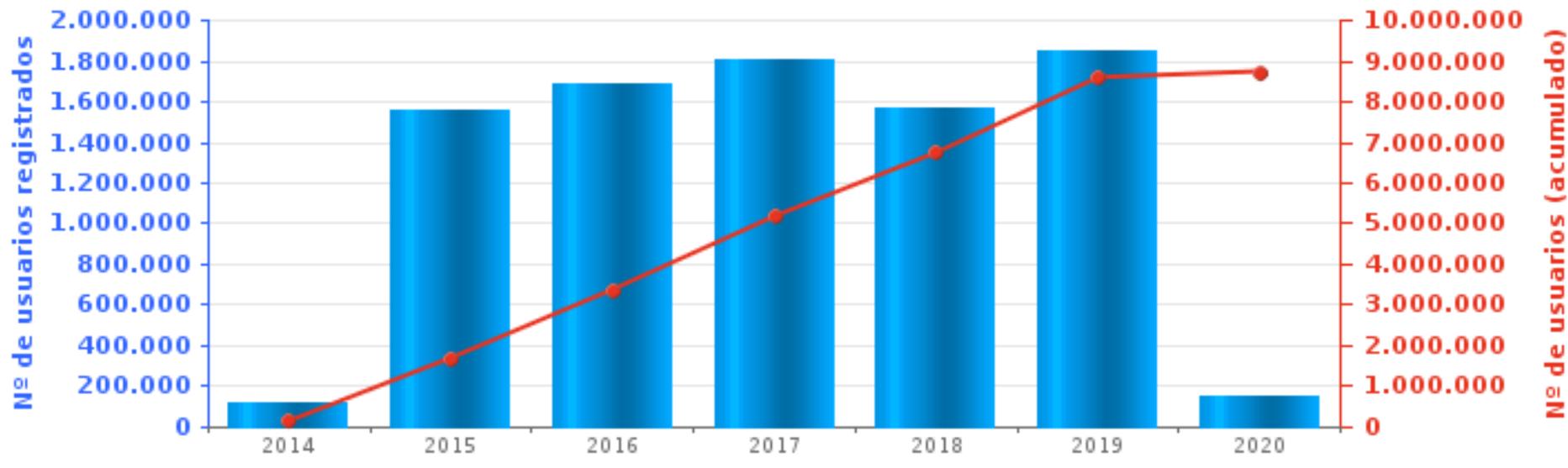
- Base legal
- Cl@ve 1.0
- Nodo eIDAS
- Cl@ve 2.0
- **Datos de uso**

Usuarios registrados

Datos acumulados desde 17/11/14 hasta 09/02/20

8.736.039

Cl@ve. Evolución anual del nº de usuarios registrados. Datos desde el 17/11/14 hasta 09/02/20 (inclusive)

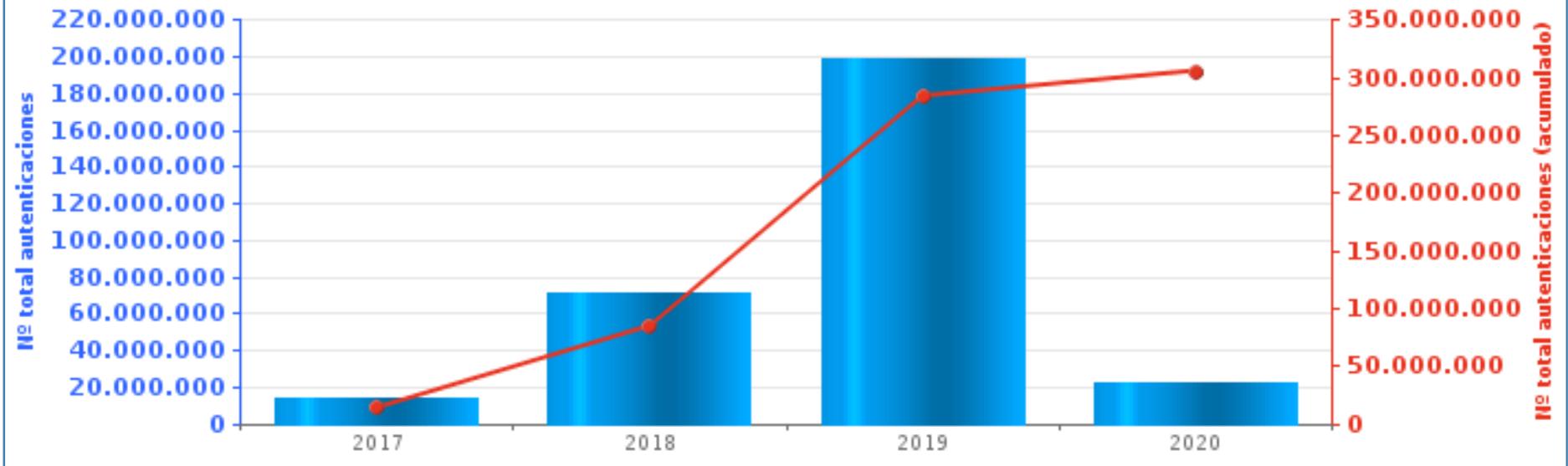


Número de Autenticaciones

Datos acumulados desde 01/06/17 hasta 16/02/20

305.513.615

Cl@ve. Evolución anual del nº Total autenticaciones.
Datos acumulados desde 01/06/17 hasta 16/02/20 (inclusive)



*Muchas
gracias*

fjavier.murillo@correo.gob.es

<http://administracionelectronica.gob.es/>

