Estudio de la nueva estrategia de la Unión Europea de regulación de identidad electrónica soberana y servicios de confianza

Nuria de Antonio Casadevall

Trabajo final del Máster Universitario en Ciberseguridad y Privacidad

Blockchain

Nombre Tutor de TF
Pau del Canto Rodrigo
Profesor responsable de la asignatura
Víctor García Font

13/06/2023

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio de la nueva estrategia de la Unión Europea de regulación de identidad electrónica soberana y servicios de confianza*
Nombre del autor:	*Nuria de Antonio Casadevall*
Nombre del tutor:	*Pau del Canto Rodrigo*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	*13/06/2023*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	*Blockchain*
Idioma del trabajo:	*Castellano*
Palabras clave	*Blockchain* *eIDAS* *self-sovereign identity* *trust services*

Resumen del Trabajo

La finalidad del trabajo es una revisión del proceso actual de cambio de paradigma de los servicios de confianza en la Unión Europea, regulados por el Reglamento eIDAS vigente, una norma europea en pleno proceso de renovación.

Los nuevos servicios de confianza, además de un marco legal, deberán dotarse de un marco teórico y tecnológico, que habilite en su conjunto un marco de confianza, para su despliegue en la Unión Europea de forma homogénea y bajo el principio de la interoperabilidad entre los Países miembros.

El Trabajo en primer lugar introduce una serie de conceptos e ideas, relacionados con el marco de estudio, para posteriormente analizar y sintetizar el marco teórico que se está elaborando para la implantación de los servicios de confianza. En particular se selecciona como eje central del estudio el caso de uso de la Identidad Digital Europea y la EUDI Wallet.

Posteriormente se estudia el marco tecnológico propuesto, para la estandarización en la Unión Europea del caso de uso seleccionado, y se analizan las distintas tecnologías incluidas.

Además, se resume el marco de cumplimiento de los servicios de confianza, y se revisa el marco de confianza de la Identidad Digital Europea, objeto de estudio en los

apartados anteriores, para el caso de uso Identidad Digital Soberana (SSI) implementado en la plataforma pública europea EBSI, basada en tecnología blockchain.

Finalmente, se realiza un estudio funcional de una solución existente de una wallet conformada para EBSI.

Abstract

The purpose of this work is to review the paradigm shift process of trust services in the European Union, regulated by the current eIDAS Regulation, a European standard currently undergoing renewal.

In addition to a legal framework, the new trust services need to establish a theoretical and technological framework that enables a comprehensive trust framework, for their deployment in the European Union in a consistent manner and under the principle of interoperability among Member States.

Firstly, this work introduces concepts and ideas related to the study framework, and then analyzes and synthesizes the theoretical framework being developed for the implementation of trust services. In particular, the study focuses on the use case of the European Digital Identity and the EUDI Wallet.

Subsequently, the proposed technological framework for standardization of the selected use case in the European Union is examined, and the different technologies included are analyzed.

Furthermore, the compliance framework of trust services is summarized, and the trust framework of the European Digital Identity, which was the subject of study in previous sections, is reviewed for the use case of Self-Sovereign Identity (SSI) implemented on the European public platform EBSI, based on blockchain technology.

Finally, a functional study of an existing wallet solution conformed for EBSI is conducted.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación

Los servicios de confianza en la Unión Europea, definidos y regulados por el Reglamento (UE) n ° 910/2014 vigente, en adelante Reglamento eIDAS, han significado un gran avance en la seguridad de las transacciones electrónicas y la gestión de la identidad electrónica.

En estos últimos años, desde la publicación de la regulación actual, han surgido nuevos modelos de computación, tales como el Cloud Computing, que hacen necesaria una revisión de los servicios de confianza, por ejemplo, la incorporación de la firma electrónica remota o de los registros electrónicos.

Además, para la mayoría de los servicios electrónicos, existe una tendencia mundial de cambio de paradigma a modelos descentralizados, en especial con la aparición de las tecnologías de cadenas de bloques (DLT) y blockchain.

Sin duda, tanto el movimiento open source como los nuevos modelos descentralizados, han influido en la aparición del concepto de identidad soberana, un modelo que permite el control y gestión propia de tus datos personales, evitando el caos actual.

En este nuevo entorno, aproximadamente desde el año 2020, la Unión Europea ha iniciado el camino para seguir avanzando en la regulación de los servicios de confianza, además de incorporar un modelo de identificación transfronteriza, basada en el modelo de identidad soberana: la Identidad Digital Europea.

Por tanto, es necesario un cambio de enfoque para los servicios de confianza, pero este cambio requiere un marco de confianza que apoye y asegure la nueva estrategia de implantación en la Unión Europea. Por otro lado, es muy importante un trabajo de estandarización y homogenización, para garantizar la seguridad e interoperabilidad entre los distintos servicios de confianza que ya existen o se van a desplegar durante los próximos años.

Así que se considera un tema relevante y se plantea como hipótesis principal para este TFM estas dos cuestiones:

- ¿Existe un marco de confianza (teórico, legal y tecnológico) suficiente para la estandarización e implantación en Europa de los servicios de confianza y la Identidad Digital Europea?
- ¿Existen soluciones públicas o privadas que cumplan este marco?

También es interesante estudiar el planteamiento inicial de regulación de los libros de registro electrónicos y de la incorporación en el análisis de la adopción en la Unión Europea de modelos descentralizados y tecnología blockchain.

En resumen, el objeto de estudio del TFM abarca un escenario abierto hace relativamente pocos años, en una fase inicial de definición, clave para el éxito en la implementación e implantación.

El alcance puede ser muy amplio, se ha acotado en relación con la hipótesis definida y también en base al caso de uso de la implementación de un modelo de identidad soberana en toda la Unión Europea.

Posiblemente este trabajo puede ser el punto de partida de otros trabajos futuros, en el apartado 11.2 se han definido nuevas líneas de estudio que no se han podido incluir debido a los temas relacionados aún pendientes de definir o implementar.

1.2. Objetivos

El objetivo principal es el estudio y análisis del marco europeo: legal, conceptual y tecnológico, respecto a los servicios de confianza y la gestión de la identidad soberana, como apoyo a la estrategia de estandarización e implantación en la Unión Europea.

Además, se apoya en los siguientes objetivos más específicos:

- Realizar un estudio del arte previo respecto a la hipótesis planteada.
- Estudiar conceptos y analizar el cambio de paradigma de los servicios de confianza y la gestión de la identidad.
- Definir el marco conceptual: Estudiar y analizar el marco teórico y legal.
- Definir el marco tecnológico: Estudiar y analizar el marco tecnológico (incluye requisitos, arquitectura, protocolos y tecnologías propuestas como estándar) elaborado para el despliegue en la Unión Europea.
- Realizar un resumen del marco de confianza (incluye el marco conceptual y tecnológico) elaborado para el despliegue en la Unión Europea.
- Analizar el modelo de cumplimiento existente para los servicios de confianza, los estándares que le aplican y cómo van a evolucionar.
- Analizar el cumplimiento del marco de confianza para una solución existente: EBSI
- Estudiar, desde un punto de vista funcional, una solución wallet existente.
- Exponer conclusiones y acciones futuras.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Los servicios de confianza electrónicos contribuyen a la implementación de proyectos tecnológicos que pueden estar relacionados con el medio ambiente, el desarrollo sostenible y el cumplimiento de los derechos humanos. Por tanto, la mejora y adaptación de los servicios de confianza y la existencia de nuevos modelos pueden tener impacto en todos los Objetivos de Desarrollo Sostenible [71], en adelante ODS, principalmente en función del caso de uso.

La iniciativa de estandarización afecta en primer lugar a las instituciones públicas europeas e impacta en la mejora de las Instituciones y la reducción de desigualdades. Además, los modelos descentralizados pueden mejorar la confianza en el funcionamiento de las instituciones, permitir un mayor control y representar un avance en la gestión de la privacidad y seguridad de la información.

En particular la mejora de la privacidad y el control de los datos personales, y el aumento de transparencia y control en las instituciones, puede ubicarse en los ODS 10 y 16 [71] respectivamente, respecto a la reducción de desigualdades y la promoción de sociedades justas, pacíficas e inclusivas.

2. Metodología

2.1. Estrategia

La estrategia para cumplir los objetivos del TFM es la observación de la información, oficial y/o fiable, relacionada con el objeto de estudio. Además del uso de técnicas de análisis cuantitativo y cualitativo, según el tipo de datos relacionados observados.

2.2. Recursos

Los recursos necesarios para realizar el proyecto son:

- Buscadores de Internet y repositorios varios académicos.
- Fuentes oficiales de instituciones españolas y europeas.
- Otras fuentes, oficiales y/o fiables, relacionadas con el objetivo.
- Herramientas electrónicas para trabajo colaborativo y gestión de proyectos: correo electrónico, Trello.
- Suite de office para creación de documentos, hojas de cálculo y creación de presentaciones.
- Soluciones existentes relacionadas con los estándares objeto de estudio: EBSI y VID Wallet.

2.3. Actividades y Planificación

Las distintas etapas o fases, y las tareas de cada una, han sido:

- Etapa previa: (PEC1)
    - Revisar el estado del arte de la hipótesis planteada.
    - Elaborar el Plan de Trabajo.
- Primera etapa: (PEC2)
    - Estudiar conceptos y analizar el cambio del paradigma de los servicios de confianza y la gestión de la identidad.
    - Definir el marco conceptual: Estudiar y analizar el marco teórico y legal.
    - Definir el marco tecnológico: Estudiar y analizar el marco tecnológico, incluyendo requisitos, arquitectura, protocolos y tecnologías propuestas como estándar.

- Realizar un resumen del marco de confianza elaborado para el despliegue en la Unión Europea.

- Segunda etapa: (PEC3)
  - Analizar el modelo de cumplimiento existente, los estándares que le aplican y cómo van a evolucionar.
  - Analizar el cumplimiento del marco de confianza para una solución existente: EBSI.
  - Estudio funcional de una solución wallet de identidad soberana: VID Wallet.
- Memoria final: (PEC4)
  - Cierre de conclusiones y siguientes líneas de trabajo.

A continuación, se realiza un desglose en actividades y la planificación del TFM:

Actividades TFM	**Fecha inicio**	**Horas estimadas**	**Duración en días**	**Fecha fin**
1. Revisar el estado del arte de la hipótesis planteada	01/03/2023	14	7	07/03/2023
2. Elaborar el Plan de Trabajo.	08/03/2023	36	7	14/03/2023
3. Estudiar conceptos y analizar el cambio del paradigma de los servicios de confianza y la gestión de la identidad.	15/03/2023	9	3	17/03/2023
4. Recopilar y estudiar el marco teórico y legal.	18/03/2023	12	4	21/03/2023
5. Analizar y definir el marco teórico y legal.	22/03/2023	16	5	26/03/2023
6. Recopilar y estudiar el marco tecnológico, incluyendo requisitos, arquitectura, protocolos y tecnologías propuestas como estándar.	27/03/2023	16	7	02/04/2023
7. Analizar y definir el marco tecnológico.	03/04/2023	16	7	09/04/2023
8. Realizar un resumen del marco de confianza elaborado para el despliegue en la UE.	10/04/2023	6	2	11/04/2023
9. Analizar el modelo de cumplimiento existente, los estándares que le aplican y cómo van a evolucionar.	12/04/2023	25	10	21/04/2023
10. Analizar el cumplimiento del marco de confianza para una solución existente: EBSI.	22/04/2023	40	14	05/05/2023
11. Estudio funcional de una solución wallet de identidad soberana.	06/05/2023	10	4	09/05/2023
12. Definir conclusiones y líneas de trabajo futuro.	10/05/2023	15	7	16/05/2023

13. Redacción final de la memoria.	17/05/2023	60	28	13/06/2023

Tabla 1. Desglose de actividades

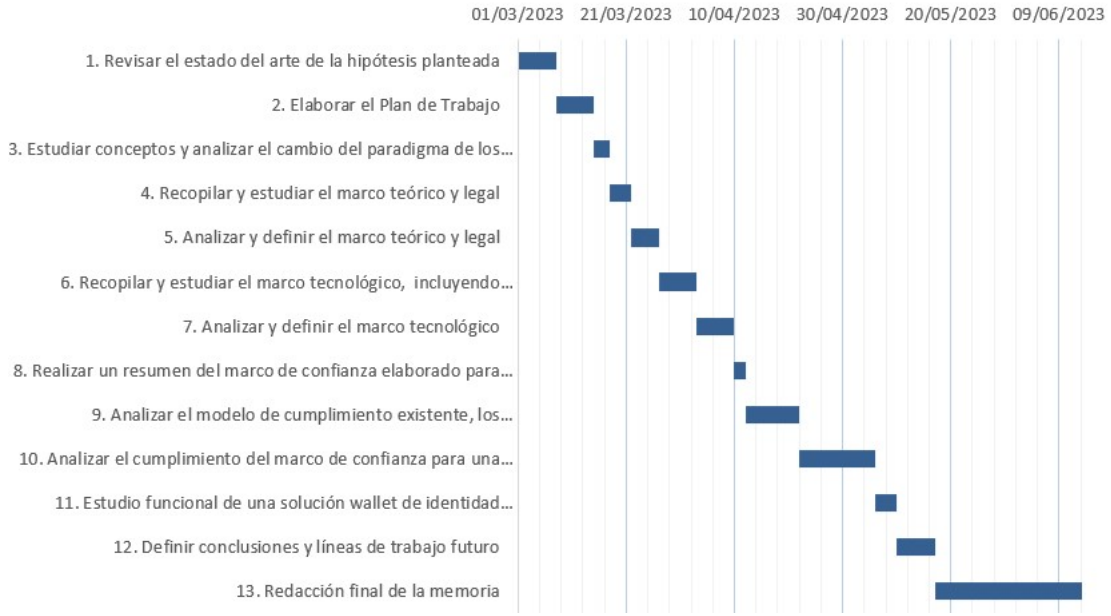


Figura 1. Diagrama de Gantt TFM

3. Estado del arte

En primer lugar, he realizado un estudio del arte en base a las palabras claves de la ficha del trabajo. La búsqueda la he centrado en fuentes fiables: artículos científicos, trabajos académicos y otros informes realizados por instituciones, consultorías o grupos de investigación reconocidos, mediante el uso de los buscadores Google, Google Scholar y Web of Science, además de la Biblioteca de la UOC.

Se han obtenido varias entradas relacionadas, sobre todo para el caso de la gestión de la identidad y el concepto de identidad soberana, un tema de estudio en crecimiento, principalmente desde el año 2022, en cuanto a número de referencias.

Los distintos resultados abarcan varios temas de la identidad soberana tales como análisis del marco conceptual, aspectos varios sobre una implementación segura y casos reales de implementación tanto a nivel europeo como mundial. También se han encontrado análisis del Reglamento eIDAS, tanto de aspectos legales como de estudios de implantación a nivel europeo, además de algún análisis de lo propuesta de renovación presentada por la Comisión Europea en el año 2021.

Por otro lado, no se han encontrado referencias que se centren únicamente en las propuestas de la Comisión Europea en cuanto a la estandarización de los servicios de confianza, probablemente porque son muy recientes y es necesario un tiempo para su elaboración. Por el contrario, sí existen análisis en blogs y redes sociales, canales que permiten una publicación más rápida, pero se han considerado fuentes de opinión y no fuentes científicas confiables.

La mayoría de las referencias me han ayudado a entender y centrar el objeto de estudio, incluso algunas han sido objeto de estudio y se nombran directamente en los distintos apartados del trabajo.

4. Estudiar conceptos y analizar el cambio del paradigma de los servicios de confianza y la gestión de la identidad.

4.1. Servicios de confianza

La definición de confianza es '*la esperanza firme que se tiene de alguien o algo*' [69]. En el caso de este estudio la confianza en algo o alguien es la esperanza en la veracidad de una identidad o de un dato registrado, algo imposible de garantizar únicamente en base a su existencia. Es necesario un marco aceptado que garantice dicha existencia, incluyendo terceros de confianza y/o mecanismos que permitan verificar pruebas de este "algo o alguien", y, por tanto, garantías que sustenten la 'esperanza firme' que avale la confianza.

En España la definición inicial de los servicios de confianza, en un contexto digital, se puede localizar en el Reglamento eIDAS. Estos servicios de confianza definidos son necesarios para garantizar las interacciones seguras electrónicas. Gracias al Reglamento eIDAS vigentes se ha conseguido un marco conceptual y legal de confianza.

Los servicios de confianza actuales, tales como la firma electrónica, el sello electrónico o el sello de tiempo, se basan en un modelo centralizado. Existen unos proveedores de estos servicios que cumplen una serie de requisitos estipulados que incluyen la capacidad técnica de soportarlos.

En España existe una lista de confianza actualizada de prestadores cualificados de servicios Electrónicos de confianza [12].

El servicio de confianza actual que garantiza la existencia de una identidad es el certificado digital, es un servicio que permite tanto la identificación y autenticación como la posibilidad de poder realizar una firma digital.

El certificado digital se puede obtener a partir de un proveedor cualificado incluido en la lista especificada, de manera centralizada, y de manera más habitual mediante un proceso de identificación a partir de un documento oficial que identifica a una persona física, por ejemplo, el Documento Nacional de Identidad.

Actualmente la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, complementa la regulación de los servicios de confianza establecidos por el Reglamento (UE) n.º 910/2014 en España.

En la propuesta de modificación del Reglamento eIDAS [7] se incluyeron dos nuevos servicios de confianza: de forma directa el registro de libros electrónicos mayores e indirectamente, a través del concepto de atributos y EUDI Wallet, un servicio de confianza de gestión de la identidad que se aproxima al concepto de identidad soberana.

4.2. Identidad

En términos legales, sin entrar en planteamientos filosóficos, la identidad de una persona depende de su nacionalidad y de la acreditación de esta por parte de su país. En el caso de España es acreditable mediante el Documento Nacional de Identidad, según se especifica en la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. No solo es un derecho, también es un deber, se debe disponer de dicha acreditación a partir de una edad mínima. Por tanto, en el mundo físico la acreditación está definida y es algo tangible que permite la identificación directa mediante observación.

En el mundo electrónico también es necesario en algunos casos acreditar la identidad mediante un mecanismo de identificación, al igual que en el mundo físico. Un dato importante es que el mismo Documento Nacional de Identidad puede ser también, de forma voluntaria, un certificado electrónico que habilita la identificación cualificada, por tanto, con un grado de confianza muy elevado, además de otros servicios de confianza tales como la firma electrónica.

Un aspecto importante de la gestión de la identidad en el mundo electrónico, al igual que en el mundo físico, es el ámbito de la validez. En el caso del DNI físico este es válido en primer lugar en España, pero también en otros países, principalmente de la Unión Europea. Estos países se informan en la página web del Ministerio del Interior [41].

En el resto de los casos si nos desplazamos físicamente a otro país que no permita la identificación mediante el DNI, entonces será necesario tramitar otros documentos que acrediten nuestra identidad. Existen varios marcos de confianza entre países respecto a la gestión de la identidad transfronteriza.

En el mundo digital las fronteras no son tan claras y, además, podemos acceder inmediatamente a servicios fuera de nuestro país y/o realizar transacciones electrónicas con personas de otro país. Por tanto, debe existir un marco legal que de validez a los certificados y a las firmas electrónicas. Dentro de la Unión Europea se consigue mediante el Reglamente eIDAS, fuera de esta, existen otros marcos legales que regulan también a los prestadores de servicios de confianza y la validez de los certificados y firmas, este estudio se considera fuera del alcance de este trabajo.

Según indica el Real Decreto 203/2021, existe un nodo de interoperabilidad para el reconocimiento mutuo de identidades electrónicas entre los Estados miembros de la Unión Europea, creado según se especifica en el Reglamento eIDAS, esto permite el uso del DNI electrónico en otras administraciones europeas. Por tanto, existe un reconocimiento legal de la identidad por parte de un país, algo que requiere un grado de confianza muy elevado y un marco regulatorio.

Es muy interesante el análisis del artículo [10] que revisa el grado de implantación de varios países europeos sobre cuestiones de cumplimiento transfronterizo e interoperabilidad relacionadas con el Reglamento eIDAS.

La identidad digital no se reduce únicamente a una identidad acreditada por un país o un tercero de confianza, mediante un certificado digital válido. Existen otras identidades digitales en el ciberespacio, estas suelen requerir un grado de confianza menor, que se generan partir de un registro de datos, normalmente como requisito previo necesario al uso de servicios digitales que ofrecen terceros. Todos estos registros crean múltiples identidades con varios datos personales, la mayoría de las veces más datos de los necesarios. Todas estas identidades digitales las gestionan de forma centralizada varias empresas y probablemente, pasado un tiempo, habrá una pérdida de control de la gestión de nuestros propios datos.

Además, no únicamente gestionan nuestros datos de registro. Algo más preocupante es el registro de nuestra huella de uso de los servicios ofrecidos. Todos estos datos por si solos o mediante el cruce con otros datos que intercambian con otros terceros, nos convierten en un objetivo comercial. Nuestros datos son valiosos, nos perfilan y hacen negocio con nosotros, es el capitalismo de los datos.

En la Unión Europea se ha creado un marco legal que dota a los ciudadanos europeos de más derechos relacionados con la privacidad y la gestión de sus datos de carácter personal. El problema es que la gran mayoría de nuestros datos, en especial los que recopilan terceros y requieren menor grado de confianza, residen fuera de la Unión Europea y por tanto se complica la aplicación de un marco regulatorio de protección, especialmente por parte de grandes tecnológicas.

Pasados unos años una persona que sea usuaria del ciberespacio puede acumular cientos de registros que ni recuerde, perder el conocimiento de todos los registros realizados y de todos los datos personales acumulados en varios servidores repartidos por todo el mundo. Actualmente, como solución a este problema, existen herramientas que permiten realizar búsquedas de las empresas que disponen de nuestros datos, a partir de un dato que suela usarse recurrentemente como por ejemplo un correo electrónico.

En resumen, la gestión de la identidad digital, desde sus inicios ha evolucionado de la siguiente manera [16][9]:

- En primer lugar, la gestión se implementó mediante un modelo centralizado, originando como principales problemas la pérdida de poder de la persona y el concepto de la balcanización de los datos.
- Posteriormente surgió la idea de la identidad federada, se añade el concepto de servicio de proveedor de identidad, para permitir a los usuarios utilizar la misma identidad digital en múltiples sitios.
- Finalmente ha surgido la idea de la identidad centrada en el usuario y específicamente el concepto de identidad soberana.

El paradigma actual, centralizado o federado, es un modelo caótico e insostenible, muy alejado de la persona. Es importante que los datos vuelvan a la persona que es la que tiene que gestionarlos. Es algo básico que la gestión de la identidad sea personal,

se compartan los datos mínimos y haya control sobre los datos personales que se comparten.

Probablemente es el mejor momento de reiniciar el modelo actual e implantar un modelo nuevo: la identidad soberana o también denominada SSI (self-sovereign identity).

4.3. Libros de registro

Un libro de registro es un '*Documento de carácter obligatorio que deben cumplimentar las personas físicas y jurídicas que desarrollan actividades empresariales y profesionales y en el que se hacen constar los datos relevantes a efectos fiscales de dicha actividad, tales como ingresos, gastos, facturas expedidas, facturas recibidas y cualesquiera otros exigidos por la normativa de cada impuesto.*' [43]

Es por tanto un contenedor de datos que se deben o quieren almacenar, en un libro de registro físico, o bien mediante un registro de tipo electrónico en un libro de registro electrónico.

Además, es necesario garantizar la confianza. Los datos que se registran deben ser confiables, no puede existir manipulación, y además se debe conocer el momento exacto del registro y la persona que lo realiza.

El paradigma actual es un modelo centralizado basado en certificados digitales y servicios de confianza, firma electrónica y sellado de tiempo, ofrecidos por terceros de confianza. Estos servicios de confianza se regulan a nivel de la Unión Europea en el Reglamento eIDAS, gracias a la firma y sello electrónico cualificado. El sello electrónico de tiempo cualificado se define como un servicio de confianza que aporta un tercero de confianza, por ejemplo, en España la FNMT-RC.

El conocimiento y la confianza en el tiempo de creación del registro es esencial pero también es importante poder verificar las distintas partes que han intervenido, el no repudio tanto de origen como de destino, y la integridad del registro realizado.

Actualmente estas garantías se consiguen a partir de un modelo centralizado de PKI, una infraestructura basada en sistemas criptográficos, que permiten a terceros dar servicios de confianza de firma digital con fecha, gracias a un tercero de confianza denominado Autoridad de Fechado Digital (TSA), de autenticación de las partes y de integridad.

En el artículo 24 del Reglamento eIDAS se especifican los requisitos para los prestadores cualificados de servicios de confianza en la Unión Europea.

4.4. Modelo centralizado vs descentralizado

La definición de centralizar '*Hacer depender de un centro común o de un poder central*' [69] es un modelo de estructura jerárquica en el que se basan muchos sistemas actuales, por ejemplo, puede ser un modelo jerárquico de los roles de una empresa, o un modelo centralizado de un proceso de desarrollo y comercialización de un producto.

En contraposición a la centralización existe una tendencia a modelos descentralizados que suponen mayor transparencia, aumento del trabajo colaborativo y una mayor responsabilidad de los integrantes de un sistema.

Existe una conexión del movimiento de open source y la identidad soberana, dos tendencias con un nexo común: la descentralización. Ambas implican un mayor control de los ciudadanos gracias al conocimiento de los algoritmos que tratan nuestros datos, la capacidad de selección libre del software que ejecutamos o bien del retorno del poder de la gestión de nuestros propios datos, ahora en poder de varias empresas o instituciones. [16]

El movimiento cypherpunk en los 80 y 90, defensor de la privacidad digital y de una moneda independiente, también se considera una probable inspiración del manifiesto de Bitcoin de Satoshi Nakamoto, origen de la tecnología blockchain y DLT.[16][18]

Remarcar la conclusión [16]: *'El hilo común desde la creación de la criptografía de clave pública hasta los criptógrafos emprendedores académicos, los cypherpunks, los pioneros de las criptomonedas y la comunidad SSI es proporcionar a las personas más herramientas para preservar la privacidad en la era digital'.*

Es significante nombrar la denominada "Ley de Johnston" que concluyó en el año 2014 "*Todo lo que se pueda descentralizar se descentralizará*" [14]. David Jhonston ha contribuido al crecimiento del desarrollo de aplicaciones descentralizadas, remarcar su escrito de la teoría general de las aplicaciones descentralizadas del año 2013 [15].

Además de teorizar con el modelo descentralizado también se ha avanzado en un marco conceptual a nivel mundial y en el avance de varias tecnologías que permiten su implementación. Es un hito la creación de Bitcoin, la primera transacción real entre dos personas se registró en enero del 2009.

Las tecnologías base para su desarrollo han sido en primer lugar la criptografía (de clave pública, funciones de hash y firmas digitales), base principal de la confianza que permite la descentralización de los sistemas, además de otras tecnologías subyacentes tales como:

- Estructuras de datos: Listas enlazada combinadas con el uso de funciones de hash y estructuras tipo Merkle-tree para validación de transacciones.
- Algoritmos de consenso que se encargan de la gobernanza, sin necesidad de centralizar la toma de decisiciones.

- Arquitecturas de red descentralizadas: redes P2P que constan de varios nodos interconectados que comparten la información de la red. Es una red completamente descentralizada y tolerante a fallos, incensurable. No existe un nodo o nodos centrales, si caen unos nodos estos serán sustituidos por otros y la información permanecerá replicada en toda la red.
- Otros protocolos descentralizados, tales como IPFS, un almacenamiento descentralizado muy importante para la implementación de la web3 descentralizada.

Aunque se pueden considerar tecnologías con una evolución relativamente reciente, se ha avanzado a nivel mundial en la estandarización de la tecnología blockchain y DLT [70]

4.5. Identidad soberana

La identidad soberana es una concepción descentralizada de la gestión de la identidad. La idea principal es preservar la confianza pero que la gestión de la identidad esté centrada en el usuario, el usuario decidirá si quiere o no compartir la identidad y los datos a compartir, La privacidad es el pilar de la gestión.

Los artículos pioneros de Christopher Allen, referencia fundamental para la revisión del concepto y la definición de los principios que definen la identidad soberana, ubican las primeras referencias a la idea en 2012 y a la aparición del término actual “identidad soberana” en el año 2016. [9]

También son una referencia importante las publicaciones de Kim Cameron en las que reflexiona sobre la falta de gestión de la identidad en Internet y los problemas que podría conllevar [19].

La falta de gestión de la identidad en Internet, juntamente con la aparición y evolución de la tecnología blockchain, han derivado en varias iniciativas relacionadas con la identidad soberana. Sin duda hay un movimiento a nivel mundial relacionado con la conceptualización, estandarización e implementación de la identidad soberana, o al menos de una gestión de la identidad bastante próxima a este concepto. Existen varias organizaciones y grupos de trabajo a nivel mundial, relacionadas o no con la tecnología blockchain, algunos ejemplos pueden ser:

- International Association for Trusted Blockchain Applications
- The EU Blockchain Observatory & Forum
- European SSI Framework [eSSIF]
- Internet Identity Workshop (IIW)
- Digital identity unConference Europe
- https://www.w3.org/community/credentials/
- ID2020 Alliance

- Open Identity Exchange

En el año 2016 Christopher Allen, a partir de diversas fuentes existentes hasta ese momento, definió 10 principios como punto de partida de la definición de lo que es la identidad soberana:[9]

1. Existencia: Los usuarios deben tener una existencia independiente, una identidad soberana simplemente hace públicos y accesibles algunos aspectos limitados del "yo" que ya existe.
2. Control: Los usuarios deben controlar sus identidades.
3. Acceso: Los usuarios deben tener acceso a sus propios datos.
4. Transparencia: Los sistemas y algoritmos deben ser transparentes. Los sistemas utilizados para administrar y operar una red de identidades deben ser abiertos, tanto en su funcionamiento como en su gestión y actualización. Los algoritmos deben ser gratuitos, de código abierto, bien conocidos y lo más independientes posible de cualquier arquitectura en particular; cualquiera debería poder examinar cómo funcionan.
5. Persistencia: Las identidades deben ser duraderas. Preferiblemente, las identidades deben durar para siempre, o al menos durante el tiempo que el usuario desee. Posiblemente la duración estará limitada por los cambios tecnológicos de la gestión de la identidad. No puede contradecir el derecho al olvido de la persona.
6. Portabilidad: La información y los servicios sobre la identidad deben ser transportables, este principio también posibilita el principio anterior.
7. Interoperabilidad: Las identidades deben ser tan ampliamente utilizables como sea posible, siempre bajo el control del usuario.
8. Consentimiento: Los usuarios deben aceptar el uso de su identidad.
9. Minimización: Se debe usar la cantidad mínima de datos en cada solicitud de datos al usuario.
10. Protección: Se deben proteger los derechos del usuario. Para garantizar esto, la autenticación de identidad debe ocurrir a través de algoritmos independientes que sean resistentes a la censura y que se ejecuten de manera descentralizada.

Más adelante en el año 2020, la fundación Sovrin define un total de 12 principios base para el concepto de SSI, se pueden consultar en la web [13]:

- 4 principios relacionados con el sistema:
    - Representación
    - Delegación
    - Equidad e inclusión,
    - Usabilidad, accesibilidad y consistencia
- 4 principios relacionados con la autonomía:

    - Participación
    - Descentralización
    - Interoperabilidad
    - Portabilidad
- 4 principios relacionados con la integridad:
    - Seguridad
    - Verificabilidad y autenticidad
    - Privacidad y minimización de datos
    - Transparencia

Aunque el cambio ya está en marcha, se indican tres desafíos para impulsar el proceso de cambio [16]: Por un lado, la necesidad de afianzar la construcción del ecosistema SSI a nivel global, se han iniciados proyectos y pilotos, pero la infraestructura está en vías de construcción y de aceptación por parte de gobiernos, grandes industrias y corporaciones. Por otro lado, la mejora de la gestión de claves descentralizada y finalmente la posibilidad de acceso sin conexión con las garantías necesarias para la acreditación de la identidad.

En el caso de la Unión Europea: se han iniciado los pasos para la implementación de la EUDI Wallet y los proyectos piloto que se van a llevar a cabo, no se considera imprescindible ni prioritaria una gestión de claves descentralizadas, probablemente se utilizarán infraestructuras PKI centralizadas, y se está trabajando en la implementación con características off-line de la EUDI Wallet.

Además, se aprobará una nueva versión del Reglamento eIDAS para confeccionar un marco conceptual y legal al nuevo concepto de Identidad Digital Europea.

En otros países también están avanzando en la implantación de la identidad digital, por ejemplo, en el caso de Estados Unidos a través de la agencia de estandarización NIST, con el proyecto 'A*ccelerate adoption of digital identities on mobile devices*', publicado en marzo del 2023. [20]

4.6. Libros de registro electrónico

La tecnología blockchain ha introducido un cambio de paradigma centralizado de los libros de registro electrónicos a otro de tipo descentralizado. La propia tecnología habilita la posibilidad de conocimiento de las partes y el tiempo, además de asegurar la integridad de un registro que se añade a una blockchain, sin la necesidad de que existan terceros de confianza que lo aseguren, la propia tecnología lo garantiza.

En la propuesta de modificación del Reglamente eIDAS [7] se definió el concepto de libro mayor electrónico, se añadió como un nuevo servicio de confianza y se introdujo una nueva sección en la que se definieron los libros mayores electrónicos cualificados.

En la última propuesta presentada [8] en febrero del 2023 se toma la decisión de eliminar el libro mayor electrónico como servicio de confianza, además de su definición de la sección '*Definitions'* y la propia sección 11, dedicada en exclusiva a la regulación del concepto de registro de libro electrónico.

El 13 de marzo del 2023 un conjunto de organizaciones tales como INATBA o EU Digital Identity Wallet Consortium, solicitó mediante una carta abierta [21] reponer las referencias eliminadas relacionadas con los libros mayores electrónicos. La idea principal de la petición se basa en que el concepto es importante para fortalecer la confianza digital en Europa y que puede ser neutral tecnológicamente, puede tener distintas implementaciones tanto centralizadas como descentralizadas, y definirse y regularse únicamente como un servicio de confianza genérico.

Se elimina el estudio del libro mayor de registro electrónico como servicio de confianza y el estudio de su implantación en la Unión Europea, centrando los objetivos en la implantación de la identidad soberana. Se incluirá en las Conclusiones y próximas líneas de trabajo el seguimiento futuro de la regulación y estrategia de implantación de los libros mayores electrónicos en la Unión Europea en los próximos años.

5. Definir el marco conceptual: Estudiar y analizar el marco teórico y legal

5.1. Marco teórico identidad soberana (SSI)

El movimiento Self-Sovereign Identity,(SSI), consta de una serie de principios que se han descrito en la apartado anterior. Es un movimiento relativamente joven y su nacimiento principalmente se debe a una carencia, la gestión de la identidad en Internet, además del avance en la sociedad de los derechos relacionados con la privacidad de los datos personales de los usuarios en Internet.

Aproximadamente desde el año 2016 se han ido definiendo los principales conceptos, objeto de estudio de este apartado. No podemos olvidar los conceptos de descentralización, tecnología DLT y blockchain, también relacionados con SSI, posiblemente estos garantizan un cumplimiento más purista de los principios del SSI.

A continuación, se van a definir siete conceptos que, bajo una visión totalmente descentralizada, conformarían los bloques básicos de una SSI [16, capítulo 2]:

1. Identificadores descentralizados: DID's. Una forma sólida, segura y escalable para que los titulares de identidades y sus agentes demuestren la propiedad de sus claves públicas. [22]
2. Verificable credentials(VC), las pruebas criptográficas de varios tipos, incluidas las pruebas de conocimiento cero (ZKP), desempeñan un papel fundamental en las credenciales verificables.
3. Trust triangle: El denominado triángulo de la confianza, define los principales actores que participan en un sistema SSI:
   - Issuers (o emisor): es la fuente de credenciales.
   - Holders (o titular): solicitar VC y los mantiene en la wallet.
   - Verifiers (o verificador): solicitar pruebas de los tenedores/proveedores de las credenciales.

   El paso crítico en este proceso es la verificación de la firma digital del emisor, normalmente mediante un DID (basado en el nivel de confianza que el verificador tiene en el emisor). Existe un W3C Verifiable Claims Working Group para los tres roles involucrados en el intercambio de VC.
4. Wallets digitales: Es un elemento que está en vías de estandarización, Centraliza las operaciones entre los actores, el intercambio de credenciales y otros datos privados, para garantizar la portabilidad debe implementar estándares abiertos.
5. Agentes digitales. Son las aplicaciones o módulos de software que nos permiten utilizar nuestras wallets digitales para obtener y presentar credenciales, administrar conexiones y comunicarnos e intercambiar credenciales verificables de manera segura con otros agentes digitales. Solo el titular (generalmente el titular de la identidad) puede acceder a los VC almacenados y las claves criptográficas. Siguiendo las instrucciones de sus propietarios, los agentes "hablan" entre sí a través de Internet para establecer conexiones e intercambiar credenciales. Específicamente se indica en

protocolo de mensajería seguro y descentralizado (DIDComm) para la comunicación privada entre agentes digitales. Existen distintos tipos: '*edge agents'*, se ejecutan en el perímetro de la red, en una red local, y '*cloud agents*' que se ejecutan de forma remota en un servidor o agente en la nube.

6. Blockchains y otros registros verificables de datos: Un DID puede registrarse con cualquier tipo de red descentralizada o registro de datos verificables (este es el término formal utilizado en las especificaciones del W3C Verifiable Credentials Data Model and Decentralized Identifier)—o incluso intercambiarse peer-to-peer sin depender de una autoridad central confiable y sin estar sujeta a puntos únicos de fallo o ataques.
7. Marcos de gobernanza, marcos de confianza. La entidad que crea y administra un marco de gobierno se conoce como autoridad de gobierno. Algunos ejemplos son:
    - El verificador puede verificar si el emisor está autorizado bajo un marco de gobierno en el que el verificador confía.
    - El verificador puede verificar si el emisor está autorizado bajo un marco de gobierno en el que el verificador confía.
    - Especifica las políticas y los procedimientos que los emisores deben seguir para emitir una credencial.
    - especifican los términos y condiciones que los titulares deben aceptar para obtener credenciales, o que los verificadores deben aceptar para verificar las credenciales.

Un ejemplo de implementación de los siete componentes básicos sería el modelo Trust over IP (ToIP), donde se define una arquitectura de cuatro capas para una infraestructura SSI [23].

5.2. Marco teórico de la Identidad Digital Europea

En el año 2020 La Unión Europea, con la publicación del documento '*Communication: Shaping Europe's digital future'* [24], en el que presentaba la estrategia de transformación digital con el objetivo también de avanzar en una sociedad más abierta, democrática y sostenible, planteaba las siguientes ideas:

• El control por parte de la persona de su identidad digital.

• Un identificador digital (eiD) público para que la persona tenga acceso a sus datos y pueda usar servicios de forma segura con mayor control de sus datos personales

En marzo del año 2021 la comunicación '*Brújula Digital 2030: el enfoque de Europa para el Decenio Digital*' [25] ya apunta al año 2030 como hito temporal para un despliegue amplio de la bautizada como Identidad Digital Europea (EUDI: European Digital Identity).

Es curioso ver que en la comunicación [25] también se hace referencia a una infraestructura europea de servicios de cadena de bloques que sea ecológica, segura y plenamente acorde con valores y marco jurídico de la UE. Parece que la intención en

ese momento era regular incluso los servicios de cadena de bloques, probablemente también se pensaba en una implementación de la identidad soberana más orientada a este tipo de servicios.

En junio del año 2021, la Comisión europea propone un framework o marco para la Identidad Digital Europea que incorpora la identificación digital nacional que se reconocerá en toda la Unión Europea y la EUDI Wallet.[26].

En febrero del año 2022 [2] se publica el esquema '*European Digital Identity Architecture and Reference Framework – Outline*' que avanza en la comprensión de la EUDI Wallet. Se definen objetivos, roles y requisitos del estado actual en ese momento del trabajo realizado por el grupo de expertos de eIDAS responsable del proyecto.

Finalmente, en enero del año 2023 se publica la versión 1.0.0 del documento '*The European Digital Identity Wallet Architecture and Reference Framework'* [1], documento central de estudio de este TFM, en el que también se definen aspectos del marco teórico de la Identidad Digital Europea.

En primer término, para entender el marco teórico, es importante conocer los conceptos que se introducen en el documento de referencia [1]. Los siguientes conceptos aparecen también en la propuesta de modificación del Reglamento eIDAS [8]:

Concepto	**Definición Reglamento eIDAS [8]**
Atributo (attribute)	Rasgo, característica o cualidad de una persona física o jurídica o de una entidad.
PID: Person identification data	Un conjunto de datos, emitido de conformidad con las leyes nacionales de cada estado miembro, que habilita la identidad de una persona.
Fuente auténtica (Authentic source)	Un sistema, que puede gestionar tanto el sector público como el privado, y contiene atributos sobre una persona que se consideran la fuente principal de esa información y que así se reconoce por el derecho de la UE o el nacional.
EAAs (Electronic Attestation of attributes)	'Attestation' es la certificación electrónica de atributos que permite la presentación y autenticación de atributos.
(Q)EEA (Qualified Electronic	Certificación emitida por un proveedor de servicios de

Attestation of attributes provider)	confianza cualificado y que cumple con los requisitos establecidos en el Anexo V del eIDAS
QSCD (Qualified Signature Creation Device)	Dispositivo cualificado de creación de firmas electrónicas que cumpla los requisitos establecidos en el Anexo II
Servicio de confianza (Trust service)	Un servicio de confianza en el marco del eIDAS, especificado en el artículo 1.
Proveedor de servicio de confianza (Trust service provider)	Persona física o jurídica que presta uno o más servicios (proveedor) de confianza cualificados o no cualificados.
QTSP (Qualified Trust Service Provider)	Proveedor de servicios de confianza que proporciona uno o más servicios de confianza cualificados y el organismo supervisor le otorga el estatus cualificado.
Parte que confía (Relying party)	La parte que recibe la información de identificación electrónica o de atributos procedente de EUDI Wallet.
User (Usuario)	Es una persona física o jurídica que utiliza una EUDI Wallet

Tabla 2. Conceptos EUDI Wallet y eIDAS

Otras definiciones propias del documento de referencia [1] son:

National Accreditation Bodies (NAB)	Los Organismos Nacionales de Acreditación según el Reglamento (CE) nº 765/2008 son los organismos de los Estados miembros que realizan la acreditación de Organismos de Evaluación de Conformidad con autoridad derivada del Estado.
Emisor (Issuer)	Un proveedor de datos de identificación de persona (PID) o de servicios de confianza que emite atributos (Q)EAA. En la arquitectura propuesta pueden existir varios emisores.

Proveedor de PID (PID Provider)	Estado miembro o entidad jurídica que proporciona datos de identificación de la persona a los usuarios como fuente primaria.
PKI Public Key Infraestructure	Una infraestructura de clave pública de la EUDI Wallet para gestionar las claves públicas. Una PKI emite certificados que contienen la clave pública y gestiona la confianza en esta. Es un sistema centralizado de gestión de las claves.
Divulgación selectiva (Selective Disclosure)	Capacidad de la EUDI Wallet que permite al usuario presentar un subconjunto de atributos de entre los que figuran en los PID o en los (Q)EAA.
Confianza (Trust) OASIS open standard ws-trust 1.4	Trust framework: Conjunto jurídicamente exigible de normas y acuerdos operativos y técnicos que rigen un sistema de múltiples intervinientes diseñado para realizar determinados tipos de transacciones entre una comunidad de participantes y sujeto a un conjunto común de requisitos. En el estudio del marco teórico se revisan estos requisitos. Trust model: Conjunto de normas que garantizan la legitimidad de los componentes y las entidades que intervienen la Identidad Digital Europea. Trusted List: Repositorio de información sobre entidades dotadas de autoridad en un determinado contexto legal o contractual que proporciona información sobre su estado actual e histórico. Las listas de confianza pueden implementarse de diferentes maneras.
EUDI Wallet Solution	Solución (Solution):

	Producto que ofrece los servicios de una EUDI Wallet, que puede ser certificada como conforme por un CAB. Instancia (Instance): Instancia de una solución de EUDI Wallet perteneciente a un Usuario y que está bajo su control. Proveedor (Provider): Organización, pública o privada, responsable del funcionamiento de una solución de EUDI Wallet compatible con eIDAS que puede instanciarse, por ejemplo, mediante su instalación e inicialización.

Tabla 3. Conceptos EUDI Wallet

A continuación, vamos a definir los distintos aspectos que definen el marco conceptual de la Identidad Digital Europea [1]:

Roles:

En el sistema van a participar los siguientes roles:

-Roles principales:

Usuario Role 1	Este role es el centro del sistema, el principal objetivo del nuevo sistema de gestión de la identidad es permitir a los usuarios el control de su identidad digital. Es el usuario de la EUDI Wallet que recibirá, guardará y presentará certificaciones de tipo PID, QEAA o EAA. También le será posible crear firmas tipo QES
Proveedores	(Role 3) Proveedores del PID: Entidades de confianza responsables de verificar la identidad (PID) del usuario, tiene que cumplir requisitos de tipo LoA high requirements. (Role 5) Proveedores de QEAA: Mantendrán interfaces para intercambio de QEAA, incluyendo autenticación mutua con la EUDI Wallet, e interfaces con Authentic sources para verificar los atributos. No puede almacenar información del uso de los servicios a los que puede acceder con una QEAA un usuario.

	(Role 6) Proveedores de EAA: Será necesario cumplir las especificaciones técnicas para conectar la EUDI Wallet con otros atributos, dependerá de las normas de cada sector, no será posible guardar información del uso de los atributos por parte del usuario. (Role 7) Proveedores de QES
Parte que confía (Role 9)	Podrán conectar con la EUDI Wallet, tendrán que informar el uso y finalidad a los estados miembros implicados. Es necesario una interfaz con la EUDI Wallet con autenticación mutua para las peticiones.

Tabla 4. Roles principales de la EUDI Wallet

-Roles de gobernanza:

Organismo de evaluación de conformidad (Role 10) (Conformity Assessment bodies (CAB))	Serán los organismos, públicos o privados, responsables de auditar la conformidad de las EUDI Wallets y los proveedores de servicios de confianza cualificados.
Organismo supervisor (Role 11) (Supervisory bodies)	Los Estados miembros deben notificar a la Comisión Europea la designación de estos organismos de supervisión de los proveedores de servicios de confianza no cualificados.
Proveedores de esquema (Q)EAA (Role 13)	Los proveedores de esquemas (Q)EAA publican esquemas y vocabularios que describen su estructura y semántica. La Comisión Europea establece las especificaciones técnicas, normas y procedimientos mínimos.
Organismo Nacional de Acreditación (Role 14) (National Accreditation bodies):	Organismos de los estados miembros que acreditan las CABs.

Tabla 5. Roles de gobernanza de la EUDI Wallet

-Otros roles del sistema:

Proveedor EUDI Wallet (Role 2) (Trusted list Provider)	Estados miembros UE u organizaciones reconocidas por estos. Están pendientes los términos y condiciones del reconocimiento por parte de cada país. Estos proveedores serán responsables del acompliance de la EUDI Wallet.
Lista de Confianza de proveedores (Role 4)	Se plantea su uso para verificar el estado de un role de la Identidad Digital Europea, por ejemplo, un proveedor de (Q)EAA
Fuentes auténticas (Role 8) (Authentic sources)	Tendrán que proveer interfaces para los proveedores de QEAA o EAA.
Fabricante de dispositivo (Role 12)	Las EUDI Wallet dispondrán de varias interfaces con los dispositivos en los que se basen, la nueva propuesta eIDAS establece restricciones respecto a dispositivos.

Tabla 6. Otros roles de la EUDI Wallet

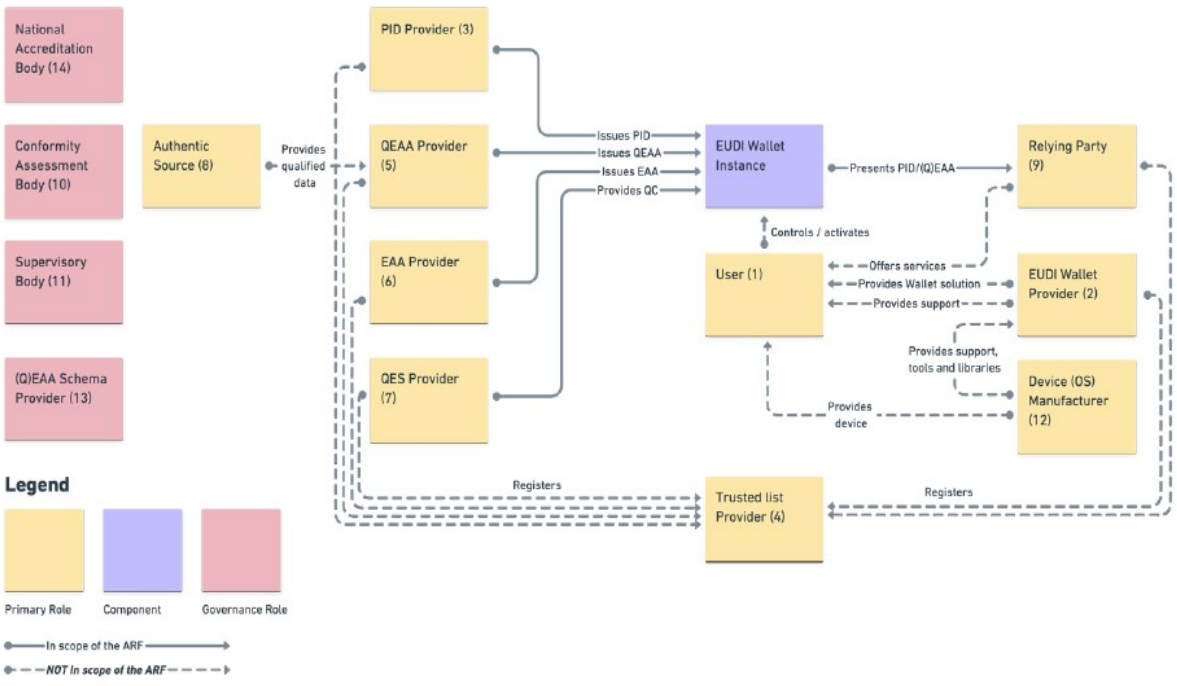


Figura 2. Roles EUDI Wallet [1]

Alcance:

En la primera versión de este documento de referencia el alcance definido es el siguiente (flujos con línea no discontinua de la Figura 2):

- A partir de una instancia de una EUDI Wallet, que gestionará un usuario, se definirán las interacciones de esta con los proveedores (PID, QEAA, EAA y QES) y con las partes que confían.

Estados y casos de uso:

Dentro del alcance, se especifican requisitos y se definen distintos estados para algunos elementos del sistema:

- Solución de EUDI Wallet:
    - Los estados posibles son: candidato, válido, suspendida o retirada.
    - El estado 'válido' se origina a partir de la certificación positiva de la Solución.
    - Un estado miembro puede suspender temporalmente una Solución.
    - Una suspensión temporal se puede cancelar y devolverla al estado válido.
    - Una solución puede retirarse y por tanto cancelarse por completo.
- Ciclo de vida de atributos PID/QEAA :
    - Los estados posibles son: preemitido, válido, revocado o expirado.
    - Existen dos transiciones posibles desde el estado 'válido': o bien expira automáticamente, por superarse la 'fecha de fin de validez, o se revoca.
    - Una vez revocado o expirado no puede volver al estado 'válido', debe volver a emitirse.
- Instancia de la EUDI Wallet:
    - Los estados posibles son: operativa, válida y desactivada.
    - El primer estado, una vez se haya instalado y activado, es 'operativa'. En este estado podría utilizarse ya para funciones no específicas de EUDI Wallet, para almacenar certificados que no exijan la vinculación a un PID.
    - Pasa a estado 'válida' al añadir un PID válido y reconocido por un proveedor de PID.
    - En el caso de que un proveedor revoque el PID la instancia pasa de nuevo al estado 'operativa'.
    - Únicamente el usuario puede desactivar la instancia de EUDI Wallet, ya que esta se podrá usar para otros tipos de atributos que no son el PID

ni (Q)EAA, el uso de estos dos tipos de atributos si dependerán de otros roles y requisitos que se especifican la EUDI Wallet.

Arquitectura lógica y definición de flujos:

A nivel conceptual, con el fin de aislar las distintas funcionalidades que realizará la EUDI Wallet, se propone una arquitectura lógica con los siguientes bloques funcionales:

- Dispositivo criptográfico seguro de la wallet: es un entorno aislado y seguro para gestión de claves criptográficas y datos.
- Componente de almacenamiento de datos: es un entorno seguro para almacenar claves y datos tales como el PID y otros atributos.
- Aplicación de creación de wallet (WCA - Wallet Creation Application); es una interfaz interna de la EUDI Wallet
- Aplicación de control de wallet(WDA, Wallet Driving Application): Interfaz de usuario de la EUDI Wallet.
- Interfaz con la parte que confía: interfaz de la Cartera IDUE proveedores, partes que confían y otras fuentes de EEA.

Se definen 4 tipos de flujos:

- Flujo 1 y 2: los dos primeros flujos son casos de proximidad, la parte que confía y el usuario se encuentran físicamente cerca y usan protocolos de proximidad. El primer flujo se define como supervisado, los atributos verificables se presentan bajo la supervisión de una persona, en el segundo caso se denomina no supervisado, se presentan los atributos directamente a una máquina.
- Flujo 3 y 4: en estos dos flujos el intercambio se realiza a través de Internet. En el caso del tercero que se denomina flujo remoto entre dispositivos, el usuario consume un servicio en un dispositivo distinto al de la EUDI Wallet que únicamente realiza la autenticación. En el caso del flujo 4 se denomina flujo remoto del dispositivo y tal como indica su nombre el servicio se consume en el mismo dispositivo que el EUDI Wallet.

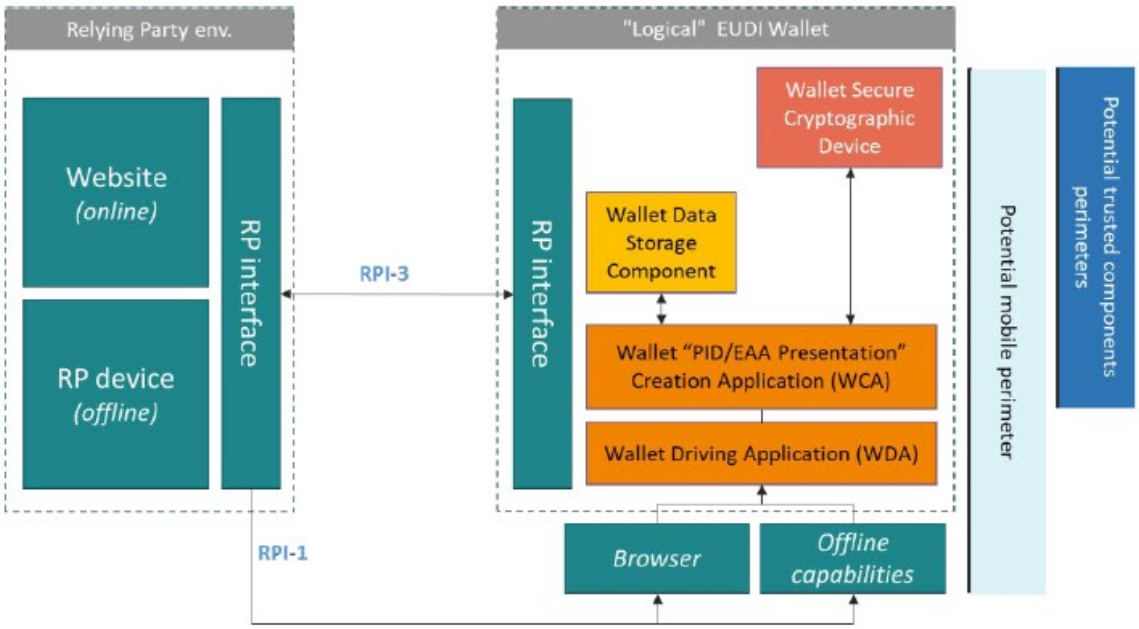


Figura 3. Arquitectura lógica EUDI Wallet [1]

A nivel conceptual también es importante remarcar la posibilidad del uso offline de la EUDI Wallet, tanto del usuario como de la parte que confía.

El detalle de la configuración propuesta de la EUDI Wallet y los distintos procolos, estándares y tecnologías, se revisarán en el apartado 6.

5.3. Comparativa marcos teóricos SSI vs Identidad Digital Europea

En comparación con el marco teórico de la SSI se constata que:

- Existe el concepto de wallet digital.
- El concepto 'Trust triangle' de la SSI puede ser análogo al conformado por los roles principales de la Identidad Digital Europea, con la siguiente correspondencia en los actores:

Actores SSI	Actores Identidad Digital Europea
Holder	Usuario
Issuers	Proveedores
Verifiers	Partes que confían

Tabla 7. Comparativa roles SSI vs EUDI Wallet

- Aunque los actores principales correspondientes al 'Trust Triangle' son similares, en el caso de la Identidad Digital Europea también existen otros roles

en el modelo de confianza propuesto, por ejemplo: las Fuentes auténticas o la Lista de Confianza de proveedores.

- Los avances en SSI tienden a modelos más descentralizados, con la mayoría de las propuestas enfocadas a blockchain. No es el caso de la propuesta de la Comisión Europea, que al menos en esta versión no parece basarse en blockchain.
- En ambos casos es necesario el concepto de marco de gobernanza en los roles especificados como tales.

5.4. Marco legal

El Reglamento eIDAS vigente [6] regula la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior de la Unión Europea.

Existen diferencias en su implantación en los distintos países de la UE. En el artículo '*eIDAS Interoperability and Cross-Border Compliance Issues'* [10], publicado en enero del año 2023, se realiza un análisis de la implementación del Reglamento eIDAS en una muestra de estados miembros: Bélgica, Croacia, Luxemburgo y España. Todos estos países notificaron esquemas de identificación electrónica, con niveles de seguridad altos, basada en sus tarjetas de identidad nacionales electrónicas.

En el caso de España algunas de las conclusiones son:

- La autoridad de control de los servicios de confianza proporciona también servicios de confianza no cualificada, en este caso el Ministerio de Asuntos Económicos y Transformación Digital.
- El uso de la firma electrónica en la AAPP: El artículo 10 de la Ley 39/2015 permite varias opciones, no se ha impuesto la firma electrónica con carácter general, salvo en los supuestos específicamente previstos en Artículo 11 (Procedimiento Administrativo). Las firmas electrónicas son obligatorias únicamente en el Esquema Nacional de Seguridad, en el Anexo II, Sección 5.7.4., para los sistemas de información de categoría altal en las dimensiones de integridad y autenticidad.
- En el caso del acceso comercial a la Red eIDAS: El Real Decreto 203/2021, de 30 de marzo, regula el Nodo de Interoperabilidad de Identificación Electrónica de España, que sólo está dirigido a entidades del sector público, excepto cuando las entidades privadas actúen en nombre de una Administración Pública. Un caso diferente sería el uso del enfoque de middleware, pero sólo sería válido para aquellos medios de identificación electrónica que lo hayan implementado.
- Respecto al uso de la biometría, de conformidad con la Ley 6/2020 y la Orden ETD/465/2021, de 6 de mayo, se regulan métodos de identificación remota por video para la emisión de certificados electrónicos cualificados

La publicación del documento 'Communication: Shaping Europe's digital future' en el año 2020, comentado en el inicio de apartado anterior, incorporaba también la siguiente idea relacionada con el marco legal [24]:

- Revisión del Reglamento eIDAS para mejorar su eficacia, extender sus beneficios al sector privado y promover identidades digitales confiables para todos los europeos.

En el capítulo '*24 From eIDAS to SSI in the European Union''* [16], cuya fecha aproximada de publicación es similar a la propuesta de modificación del Reglamento eIDAS [7] por parte de la Comisión Europea, se apuntan a los siguientes aspectos respecto al Reglamento eIDAS y su avance a un cambio de modelo SSI:

- El Reglamento eIDAS vigente es el principal marco de confianza en la Unión Europea. Este permite dos de los enfoques respecto a los distintos modelos de gestión de identidad: la infraestructura de clave pública (PKI) y la gestión de identidad federada (FIM), ambos modelos implantados o en proceso de implantación actualmente.
- Las PKI están formadas por autoridades de certificación (CA) que emiten certificados digitales que vinculan una clave pública con una entidad identificada, estos son documentos electrónicos emitidos que vinculan el nombre de una persona física o jurídica (y cualquier otro atributo de identidad relevante) a la clave pública de esa persona. Los certificados de clave pública están regulados como un servicio de confianza específico por el Reglamento eIDAS.
- Una PKI es una infraestructura que podría ser parte de una SSI, específicamente para el ciclo de vida de gestión de credenciales verificables (VC). Esto permite que la infraestructura SSI aproveche más de 20 años de normalización internacional en organizaciones como el Sector de Normalización de Telecomunicaciones de la UIT (UIT-T), el Grupo de Trabajo de Ingeniería de Internet (IETF) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI).
- El Reglamento eIDAS definió un vocabulario específico para comparar y evaluar los esquemas de identidad nacional y federarlos a nivel de la UE.
- Además, plantea los siguientes escenarios para la adopción de la EU SSI:
    - Mantener los Nodos tipo proxy actuales y usar SSI detrás del nodo, en esta propuesta el punto fuerte es que la transición sería rápida y sin necesidad de cambios legislativos.
    - Un modelo de middleware, El segundo escenario que plantean desarrollaría un modelo de middleware, sustituyendo los nodos proxy eIDAS por los protocolos y artefactos operativos SSI. En este caso se especifica que se debería ampliar el eIDAS para poder ampliar a cualquier tipo de credencial verificable.

Es muy interesante el análisis y propuesta del grupo de expertos de SSI, en el contexto del año de publicación, sobre la implantación de un modelo SSI en la actual infraestructura de la Unión Europea y la posible adaptación del Reglamento eIDAS.

Como reflexión es importante remarcar dos ideas:

- El grupo de expertos de SSI, con un enfoque totalmente orientado a modelos muy descentralizados, apunta a la ventaja del uso de la PKI para su desarrollo en la Unión Europea.
- Finalmente, la Unión Europea ha iniciado una estrategia ambiciosa de cambio respecto a la gestión de la identidad, con un marco temporal amplio, y que por supuesto implica un cambio importante en el Reglamento eIDAS vigente actualmente.

En junio del 2021 la Comisión Europea publica una propuesta de modificación del Reglamento eIDAS vigente, con el objetivo de establecer un marco legal para una Identidad Digital Europea. [7]

El 7 de febrero del 2023 la Comisión presenta el último texto consolidado de la propuesta de modificación del eIDAS presentada en junio de 2021.[8]

En el último texto consolidado de la propuesta de modificación del eIDAS [8] se pueden destacar los siguientes cambios respecto al Reglamento eIDAS vigente:

- Se añaden en el artículo 1 nuevos servicios de confianza, tales como la certificación de atributos, además se añade un apartado para la EUDI Wallet, remarcando la interoperabilidad y validez en toda la Unión Europea.
- En el artículo 2 se añade como alcance del eIDAS las EUDI Wallets.
- En el artículo 3 se añaden los nuevos conceptos del marco teórico de la Identidad Digital Europea [1], además de:
    - Mayor especificación de la definición de '*authentication'* con nuevas definiciones de '*identification'*, '*validation'* y '*zero knowledge proof*'.
    - Se añaden nuevos servicios de confianza.
    - Se añade el concepto de '*remote qualified signature creation device*'.
    - A partir de la definición 42 se añaden nuevos conceptos:
        - European Digital Identity Wallet'
        - Attribute
        - electronic attestation of attributes
        - qualified electronic attestation of attributes
        - authentic source
        - electronic archiving
        - qualified electronic archiving service
        - EU Digital Identity Wallet Trust Mark
        - strong user authentication

        - user account
        - identity matching
        - offline service
- En al artículo 6 se introduce le EUDI Wallet y se regulan los siguientes aspectos:
    - Cada estado miembro de la UE debe al menos poner a disposición una EUDI Wallet, temporalmente se da un plazo de 18 meses desde la aprobación.
    - El código fuente debe ser Open Source.
    - Define los servicios que obtendrá el usuario
    - Define los protocolos e interfaces que debe tener
    - Principio privacidad desde el diseño
    - Gratuito para personas físicas y jurídicas.
    - Aspectos relacionados con las partes que confían, estas deberán realizar un registro e informar de los servicios y datos que se usarán.
    - Se regula la certificación de la EUDI Wallet y la lista oficial que mantendrá la Comisión Europea de la wallets aceptadas y activas.
    - Actuación antes brechas de seguridad
    - Reconocimiento transfronterizo vs cooperación.
- Se añade una sección 9 en el capítulo 3 de Servicios de confianza relativo a certificación de atributos, con los siguientes artículos:
    - Efectos jurídicos de la certificación electrónica de atributos.
    - Certificación electrónica de atributos en los servicios públicos.
    - Requisitos para la certificación electrónica cualificada de atributos.
    - Verificación de atributos contra fuentes auténticas.
    - Normas adicionales para la prestación de servicios de certificación electrónica de atributos
- En esta última propuesta se elimina la sección 11, añadida en la primera propuesta de modificación del año 2021, respecto a los libros electrónicos mayores.
- Se añade un capítulo de Gobernanza que incluye:
    - Autoridades nacionales competentes y ventanilla única.
    - Tareas de las autoridades nacionales competentes.
    - Consejo Europeo del Marco de Identidad Digital (EDIFB): creación y tareas de este nuevo Consejo de apoyo a la Identidad Digital Europea.

En Resumen, en el nuevo Reglamento eIDAS propuesto, se establece un marco legal para la certificación electrónica de atributos y se establecen las condiciones para la emisión, gestión y reconocimiento de EUDI Wallets, garantizando su interoperabilidad y su uso transfronterizo en toda la Unión Europea.

Es significativo el artículo '*eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI'* [27] que revisa la propuesta eIDAS y se plantea las siguientes cuestiones: ¿Cuáles son los retos y oportunidades de eIDAS2? ¿Y cuáles son los principales focos y necesidades de la normalización (europea)?

El artículo es del año 2022, anterior a la última propuesta del eIDAS [8] y al documento sobre la arquitectura y framework de referencia de la EUDI Wallet [1], ambos del año 2023.

Las principales ideas del artículo son:

- La normalización será clave para garantizar la interoperabilidad a nivel de la Unión Europea, se garantizará a través de la certificación.
- El principio SSI de control total del dueño sobre su identidad, con toda la información de identidad almacenada de forma descentralizada y en la que el titular decidirá a quién dará acceso o transmitirá la información de identificación, se plantea en el artículo mediante el uso de un modelo descentralizado con tecnología DLT, como una PKI descentralizada, hace referencia al planteamiento de ENISA plasmado en el documento '*Leveraging the Self-Sovereign Identity (SSI)'* [28].
- Se requerirá que se notifique al menos un esquema de identidad de cada estado miembro.
- Se especifican los requisitos para que cada estado miembro proporcione una EUDI Wallet para la gestión de la identificación electrónica de un gobierno La EUDI Wallet será publicada: por el estado miembro o bajo la autoridad del estado miembro o reconocida por el estado miembro.
- La EUDI Wallet contendrá la identidad central que será la identificación electrónica de un gobierno, además de atributos adicionales o credenciales verificables, en el artículo se específica que las credenciales cumplan los estándares W3C.
- eIDAS2 cumple el '*Trust Triangle*' como concepto del SSI.
- Se añade a la EUDI Wallet la creación de firmas electrónicas cualificadas.
- Los detalles técnicos y requisitos de seguridad para la EUDI Wallet se están definiendo en un proceso de estandarización en curso de ETSI y CEN.
- El usuario decidirá las partes que confían con la que interactuar.
- Con la nueva propuesta del Reglamento eIDAS se le da seguridad jurídica al SSI, realmente a la Identidad Digital Europea, pero una desventaja a la que se apunta es que no es posible una descentralización completa con credenciales creadas por uno mismo e independientes de cualquier tercero de confianza

- Así bajo el eIDAS se limita la descentralización, siempre es necesario un tercero de confianza, eIDAS2 requiere la notificación de la eID emitida por el gobierno, así como la certificación del esquema de identificación privada por parte de CAB; lo mismo con EUDI Wallet.
- Se hace posible la ejecución de los principios de SSI sobre seguridad, autenticidad y verificabilidad
- Si se debe tener la certeza de que la persona física o jurídica es realmente lo que parece ser, es fundamental una identificación verificada y segura. Este procedimiento, sin embargo, establecería un requisito de entrada para la participación en el ecosistema.
- La nueva propuesta del Reglamento eIDAS es tecnológicamente neutral. Ni para las certificaciones (cualificadas), ni para el esquema de identificación ni para los medios de identificación se requiere una infraestructura concreta. No se necesita obligatoriamente ninguna DLT. SSI es un concepto de gestión de acceso e identidad donde, por un lado, el titular de la identidad decide a quién le dará qué parte de su información de identidad y, por otro lado, no tiene que dar la información de identidad completa en todos los casos, sino solo la necesaria.
- La estandarización debe centrarse especialmente en los esquemas de eID, EUDI Wallet y certificación de atributos primero.
- En W3C, el trabajo relacionado con DID-resolver está en curso, una colaboración sería significativa para identificar temas relevantes para Europa y garantizar la viabilidad internacional de la estandarización europea SSI.

En Resumen, la idea principal del artículo sería que la nueva propuesta del Reglamento eIDAS se basa en los principios SSI pero pone límites a la descentralización a cambio de lograr confianza legal y la soberanía de los datos. Si un titular no puede confiar en una identidad, emisor o verificador, no puede actuar con soberanía propia.

Por otro lado, la propuesta que analiza este artículo incluía los libros electrónicos mayores como servicios de confianza, y al respecto se analizan algunos problemas:

- DLT actualmente carece de una identificación clara y legalmente compatible de las partes que participan en la red, así como de evidencia única de autenticidad e integridad de sus transacciones.
- Con respecto al hecho de que DLT es inmutable por diseño, esta propiedad principal está en contradicción con la ley de privacidad y derechos de la persona tales como el derecho de borrado o derecho de corrección. Lo mismo ocurre con la falta de estándares para la interoperabilidad en DLT, lo que limita el derecho a la portabilidad de datos según GDPR.
- No contiene el requisito de estandarización en Europa para los libros mayores de registro.

Este último análisis por el momento pierde sentido al eliminar los libros electrónicos mayores como servicio de confianza, pero al revisar alguno de las carencias indicadas quizás se comprenda la eliminación de estos en la última propuesta presentada en febrero del año 2023.

6. Definir el marco tecnológico: Estudiar y analizar el marco tecnológico, incluyendo requisitos, arquitectura, protocolos y tecnologías propuestas como estándar

6.1. Arquitectura

En el documento principal de referencia de este estudio [1], se proponen los siguientes componentes para la arquitectura de la EUDI Wallet:

1. Sistema de gestión de claves criptográficas: se encarga de gestionar y almacenar información criptográfica.

2. Protocolo de intercambio de certificaciones:
   - Define cómo solicitar y presentar los datos de PID y las certificaciones de (Q)EAA de forma segura y preservando la privacidad.
   - Autenticación entre la instancia de EUDI Wallet y la parte que confía, en particular el mecanismo a través del cual la parte que confía puede solicitar la identificación a través de la EUDI Wallet.

3. Protocolo de emisión:
   - define cómo deben expedirse los PID y los certificados (Q)EAA y en qué formatos.

4. Modelo de datos:
   - El modelo de datos define y describe los elementos de datos y cómo interactúan entre sí y sus propiedades.

5. Esquemas PID/(Q)EAA:
   - contiene la estructura y la organización lógica de los datos que definen las propiedades de la certificación, los atributos del Usuario e información adicional como por ejemplo los mecanismos de verificación

6. Formatos PID/(Q)EAA:
   - se utilizan para representar la característica, cualidad, derecho o permiso de una persona física o jurídica o de un objeto, en forma de credenciales firmadas electrónicamente y verificables.

7. Formatos de firma:
   - Especificación del formato de firma, destinada a demostrar la autenticidad de un documento digital, su integridad, autenticar al autor de un documento y, opcionalmente, también a su destinatario.

8. Modelos de confianza:

- Conjunto de normas que garantizan la legitimidad de los componentes y las entidades que intervienen en la infraestructura de EUDI Wallet para la:
    - Autenticación de usuarios.
    - Identificación del emisor.
    - Registro de emisores.
    - Modelos de datos y esquemas reconocidos.
    - Registro y autenticación de las partes Informadas.
    - Mecanismos para establecer la confianza en un escenario multidominio.

9. Suites y mecanismos criptográficos: aseguran el intercambio de datos en términos de confidencialidad e integridad.

10. Identificadores de entidad: Identificadores únicos para todos los elementos del modelo de datos.

11. Comprobación del estado de validez: Mecanismo para publicar y obtener información sobre el estado de validez del PID, (Q)EAA, certificados destinados a realizar firmas o sellos electrónicos, etc.

6.2. Requisitos marco tecnológico

Teniendo en cuenta la idea introducida en el apartado anterior sobre que La estandarización debe centrarse primero en los esquemas de PID, EUDI Wallet y certificación de atributos, en el documento principal de referencia de este estudio [1] justo se han centrado en definir estos requisitos, relacionados con la implementación y marco tecnológico.

En el propio documento [1] también se informa que en futuras versiones posiblemente añadirán otros requisitos relacionados por ejemplo con emisores o partes que confían.

Además, se han definidos dos tipos de EUDI Wallet, en función del nivel de aseguramiento. El Tipo 1 está enfocada a garantizar un nivel de aseguramiento de la entidad LoA High para permitir la identificación transfronteriza mediante el PID. No obstante, el Tipo 2 flexibiliza los requisitos para uso de certificados que vayan a necesitar características adicionales.

Los requisitos definidos siguen la recomendación RFC 2119 en relación con los niveles de requerimiento [33].

1. **Requisitos de expedición del PDI, a efectos de comprobación de validez, autenticidad, validación, políticas, modelo de datos y formatos; en relación con la información que se incluye en el certificado:**

Requisito	Descripción
DEBE (OBLIGATORIO)	
INFO.01	Contener la información para identificar al proveedor
INFO.02	Contener la información para realizar una comprobación de integridad de datos
INFO.03	Contener la información para verificar su autenticidad
INFO.04	Contener la información para comprobar el estado de validez de las certificaciones
INFO.05	Contener la información para verificar la vinculación del titular por una parte que confía
INFO.06	Emitirse para ser presentada de acuerdo tanto con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021 como con el Modelo de datos de credenciales verificables v1.1 del W3C
INFO.07	Codificarse como CBOR y en formato JSON
INFO.08	Permitir la divulgación selectiva de atributos mediante el uso del esquema "Selective Disclosure for JWTs (SD-JWT)" y "Mobile Security Object (ISO/IEC 18013-5)" de acuerdo con el modelo de datos (Permiso de conducir en el móvil)
INFO.09	Utilizar firmas electrónicas y formatos de cifrado tal y como se detalla en la RFC 8812 Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms.
INFO.10	Utilizar algoritmos de firma y cifrado de conformidad con la norma SOG-IS ACM (Agreed Cryptographic Mechanism) [68]

Tabla 8. Requisitos de expedición del PDI

2. Requisitos de expedición del (Q)EAA, a efectos de comprobación de validez, autenticidad, validación, políticas relacionadas con la gestión de claves, el modelo de datos y los formatos; en relación con los certificados de (Q)EAA:

Requisito	Descripción
DEBE (OBLIGATORIO)	
CERT.01	Contener la información para identificar al emisor
CERT.02	Contener la información para realizar una comprobación de integridad de datos

CERT.03	Contener la información para verificar su autenticidad
CERT.04	Contener la información para comprobar el estado de validez de las certificaciones
CERT.07	Expedirse de conformidad con una de las especificaciones del modelo de datos: la norma de codificación de permiso de conducir: I"SO/IEC 18013-5:2021", o "Verifiable Credentials Data Model v1.1" (Modelo de datos de credenciales verificables 1.1) del W3C.
DEBERÍA (RECOMENDADO)	
CERT.06	Contener la información para verificar la vinculación del titular por una parte que confía
CERT.08	Codificarse como uno de los siguientes formatos: CBOR o JSON según el modelo de datos utilizado para la certificación. Ver RFC 8812, RFC 8152, RFC 9052, RFC 9053
CERT.10	Permitir la Revelación Selectiva de atributos utilizando bien "Selective Disclosure for JWTs" (Revelación Selectiva para JWTs) (SD-JWT) o bien el esquema "Mobile Security Object" (Objeto de Seguridad Móvil) de la norma sobre permiso de conducir (ISO/IEC 18013-5)
CERT.11	Utilizar uno de los siguientes formatos de firma y cifrado según se detalla en las normas del IETF, RFC relativas a JOSE (Javascript Object Signing and Encryptio), y RFCs relativas a COSE (CBOR Object Signing and Encryption)
CERT.12	Utilizar algoritmos de cifrado de conformidad con la norma SOG-IS ACM (Agreed Cryptographic Mechanism) [68]
CERT.13	Emitirse de acuerdo con el protocolo OpenID4VCI (OpenID for Verifiable Credential Issuance)
PUEDE (OPCIONAL)	
CERT.09	Codificarse como JSON-LD (JSON for Linking Data)

Tabla 9. Requisitos de expedición del (Q)EAA

3. Requisitos de configuración de la EUDI Wallet Tipo 1:

***** Componente EUDI Wallet definido en el apartado 6.1

Requisito	*****	**Descripción**

DEBE (OBLIGATORIO)		
EUW1.01	1	Se proponen 3 componentes para almacenar y gestionar claves criptográficas: elemento seguro integrado, dispositivo externo y un servidor Aplicar medidas de seguridad para evitar la exportación de secretos criptográficos
EUW1.02	2	soportar OpenID4VP como protocolo de intercambio de certificados para flujos remotos. Cuando se solicita autenticación pseudónima, los parámetros de solicitud DEBERÍAN especificarse de acuerdo con la especificación OpenID SIOPv2 soportar el protocolo detallado en la norma ISO/IEC 18013-5:2021 para flujos de proximidad Poder realizar una prueba de posesión Soportar la Divulgación Selectiva de atributos tal y como se especifica en la norma ISO/IEC 18013-5:2021 Soportar la Divulgación Selectiva de atributos como se especifica en la especificación SD-JWT
EUW1.03	3	Admitir OpenID4VCI como protocolo de emisión. (Los Estados miembros son libres de incluir alternativas adicionales al protocolo de emisión en sus soluciones nacionales)
EUW1.04	4	Admitir certificados emitidos de conformidad con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021 Soportar certificados emitidos de acuerdo con el modelo de datos especificado en la especificación W3C Verifiable Credentials Data Model 1.1
EUW1.05	6	Soportar certificados en formato JWT y SD-JWT Admitir certificados en formato CBOR
EUW1.06	7	Soportar formatos de firma electrónica y cifrado de acuerdo con las especificaciones JOSE (JWT) Soportar formatos de firma y cifrado de acuerdo con las especificaciones COSE.
EUW1.07	9	Soportar suites criptográficas y mecanismos utilizados para atributos detallados en SOG-IS Agreed Cryptographic Mechanisms Version 1.2.

DEBERÍA (RECOMENDADO)		
EUW1.08	2	Realizar comprobaciones para hacer cumplir la vinculación de sesión
PUEDE (OPCIONAL)		
EUW1.09	2	Soportar alternativas de protocolo de intercambio de certificados (Cabe destacar la API REST de mdoc, tal y como se detalla en el borrador de la norma ISO/IEC 23220-4)
EUW1.10	6	Soportar certificados en formato JSON-LD
NO PUEDE (PROHIBICIÓN)		
EUW1.11	7	Admitir formatos de firma y cifrado de acuerdo con las especificaciones LD-Proof.

Tabla 10. Requisitos de configuración de la EUDI Wallet Tipo 1

4. Requisitos de configuración de la EUDI Wallet Tipo 2:

***** Componente EUDI Wallet definido en el apartado 6.1

Requisito	*****	**Descripción**
DEBE (OBLIGATORIO)		
EUW2.01	3	Admitir OpenID4VCI como protocolo de emisión. (Los Estados miembros son libres de incluir alternativas adicionales al protocolo de emisión en sus soluciones nacionales
DEBERÍA (RECOMENDADO)		
EUW2.02	1	Se proponen 3 componentes para almacenar y gestionar claves criptográficas: elemento seguro integrado, dispositivo externo y un servidor Aplicar medidas de seguridad para evitar la exportación de secretos criptográficos
EUW3.03	4	Admitir certificados emitidos de conformidad con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021. Soportar certificados emitidos de acuerdo con el modelo de datos

		especificado en la especificación W3C Verifiable Credentials Data Model 1.1.
EUW4.04	9	Soportar suites criptográficas y mecanismos utilizados para atributos detallados en SOG-IS Agreed Cryptographic Mechanisms Version 1.2.
PUEDE (OPCIONAL)		
EUW5.05	2	Soportar OpenID4VP como protocolo de intercambio de certificados para flujos remotos. Cuando se solicita autenticación pseudónima, los parámetros de solicitud DEBERÍAN especificarse de acuerdo con la especificación OpenID SIOPv2 Soportar el protocolo detallado en la norma ISO/IEC 18013-5:2021 para flujos de proximidad Poder realizar una prueba de posesión Soportar la Divulgación Selectiva de atributos tal y como se especifica en la norma ISO/IEC 18013-5:2021 Soportar la Divulgación Selectiva de atributos como se especifica en la especificación SD-JWT Realizar comprobaciones para hacer cumplir la vinculación de sesión Soportar alternativas de protocolo de intercambio de certificados (Cabe destacar la API REST de mdoc, tal y como se detalla en el borrador de la norma ISO/IEC 23220-4)
EUW2.06	6	Soportar certificados en formato JWT y SD-JWT. Admitir certificados en formato CBOR
EUW3.07	7	Soportar formatos de firma electrónica y cifrado de acuerdo con las especificaciones JOSE (JWT) Soportar formatos de firma y cifrado de acuerdo con las especificaciones COSE Admitir formatos de firma y cifrado de acuerdo con las especificaciones LD-Proof.

Tabla 11. Requisitos de configuración de la EUDI Wallet Tipo 2

6.3. Protocolos y tecnologías propuestas como estándar

El documento principal de referencia [1] elaborado por el grupo de expertos '*eIDAS Expert Group'*, tal como se define, es un documento vivo que se complementará y actualizará para la implementación de la '*toolbox'* para la EUDI Wallet.

Como apoyo a la implantación de la Identidad Digital Europea, la Comisión Europea también ha licitado un conjunto de proyectos denominados LSP que se ejecutarán durante un periodo de dos años, finalizarán en el año 2024.

Por tanto, en primer lugar, este documento [1] es una base común para la ejecución de los LSP, cuya experiencia también influirá en la evolución de lo definido hasta el momento.

Se han propuesto los siguientes protocolos y tecnologías sobre la arquitectura y requisitos tecnológicos:

Protocolos y tecnologías	**id/nombre elemento arquitectura EUDI Wallet**
ISO/IEC 18013-5:2021	2/ Protocolo de intercambio de certificaciones para flujos de proximidad 4/Modelo de datos
Mobile Security Object (ISO/IEC 18013-5)	2/Protocolo de intercambio de certificaciones para divulgación selectiva de atributos
OpenID4VP	2/Protocolo de intercambio de certificaciones para flujos remotos
OpenID SIOPv2	2/Protocolo de intercambio de certificaciones para flujos remotos con autenticación pseudónima
JWT y Selective Disclosure for JWTs (SD-JWT)	2/Protocolo de intercambio de certificaciones para divulgación selectiva de atributos
OpenID4VCI	3/Protocolo de emisión
modelo de datos de credenciales verificables v1.1 del W3C	4/Modelo de datos
CBOR y formato JSON	5/Formatos PID/(Q)EAA
JSON-LD (JSON for Linking Data)	5/Formatos PID/(Q)EAA
CBOR, COSE, JOSE	7/Formatos de firma
SOG-IS ACM	9/Suites y mecanismos de confianza

Tabla 12. Protocolos y tecnologías estándares EUDI Wallet

En resumen, principalmente se ha definido [Figura 4]:

- Las normas que regulan el canal seguro de intercambios de certificaciones:
  - OpenID4VP (o OpenID SIOPv2) para flujos remotos
  - ISO/IEC 1813-5 para flujos cercanos

- Los formatos de los contenedores de certificaciones:
  - W3C VC con JSON + JWT[SD-JWT]
  - ISO/IEC 18013-5:2021 con CBOR + MSO

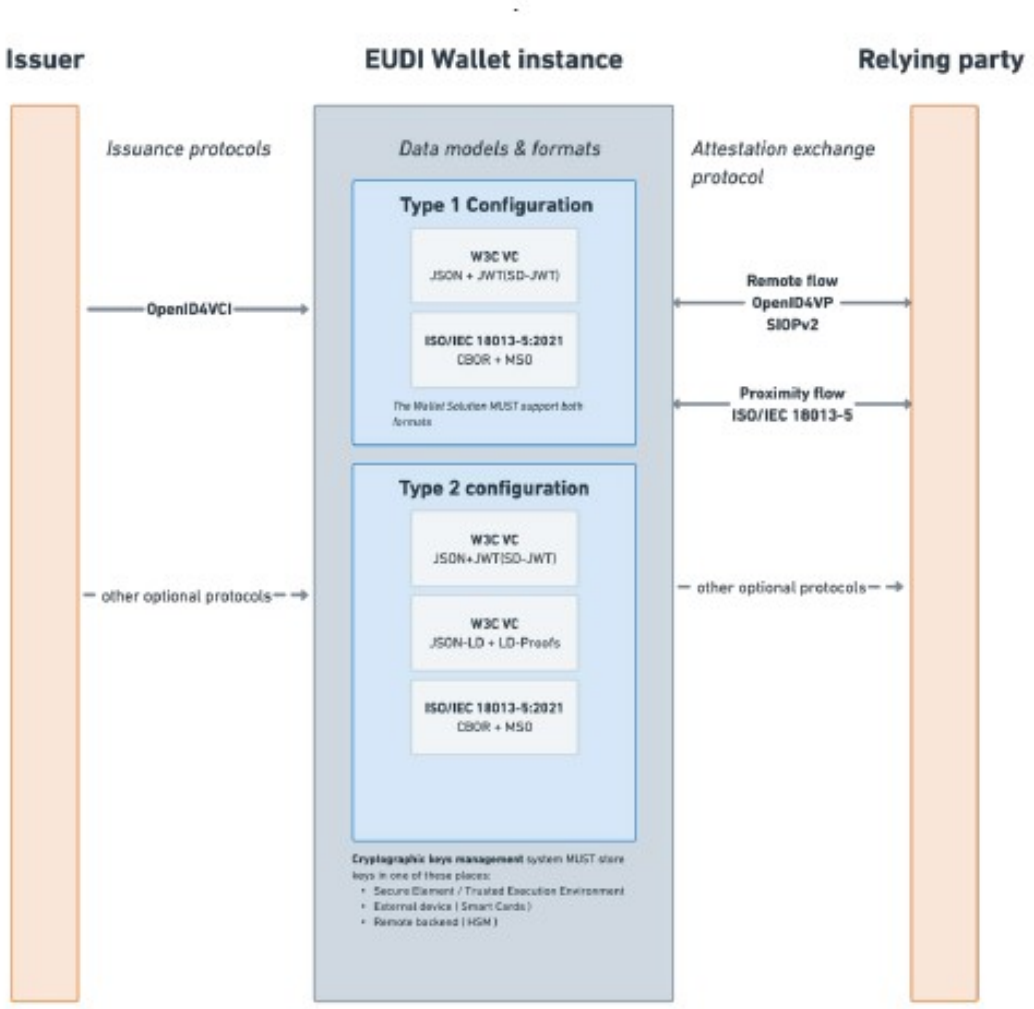


Figura 4. Configuración EUDI Wallet [1]

A continuación, se definirán las tecnologías principales:

OpenID

En el acta de constitución de OpenID se especifica que esta es una organización sin fines de lucro que entre otras tareas trabajan en la creación de un conjunto de estándares para establecer transacciones de identidad más seguras a través de Internet, centradas en el usuario y abiertas.

Las especificaciones de los estándares de OpenID se encuentran publicadas y accesibles en su página web [35].

En la *'toolbox'*, para el intercambio de certificaciones de atributos para conexiones a través de Internet, se ha seleccionado: OpenID4VP y OpenID SIOPv2.

OpenID4VP: OpenID para emisión de credenciales verificables

Tal como se define en el Abstract de la especificación [29], es un protocolo para solicitar y presentar Credenciales Verificables.

El formato puede ser cualquiera, incluidos los dos formatos de los contenedores de la toolbox: W3C VC e ISO/IEC 18013-5:2021.

El protocolo base es OAuth 2.0, al que se le añade un mecanismo para solicitar y presentar credenciales verificables.

En la especificación se definen dos diagramas de flujo, uno para el caso en el que el usuario final presenta una credencial a un verificador que interactúa con el usuario final con el mismo dispositivo en el que residen la billetera, el otro en el caso de ser un dispositivo distinto.

En los anexos de la especificación se definen los siguientes casos relacionados con la toolbox:

- A1: Esta sección define la presentación de una credencial verificable W3C basada en JWT
- A3: Esa sección define la presentación de una credencial de licencia de conducir móvil (mDL) utilizando un modelo de datos y conjuntos de datos definidos en la norma ISO.18013-5 y codificados como CBOR. El identificador de formato de Credencial es mso_mdoc.
- A4. En esta sección se muestra la combinación de OpenID y SIOP para presentar credenciales verificables y autenticar de forma seudónima a un usuario final, utilizando claves controladas por el usuario.

OpenID SIOPv2: Self-Issued OpenID Provider v2

Esta especificación [30] extiende el concepto de conexión OpenID con el concepto de un proveedor de OpenID autoemitido (OP autoemitido), los usuarios pueden autenticarse con tokens de identificación autoemitidos y presentar peticiones autocertificadas a las partes que confían que las soliciten. También pueden presentar

peticiones verificables criptográficamente emitidas por terceros en los que confían las partes que confían.

Un OP autoemitido permite al usuario final determinar los identificadores y afirmaciones emitidos a la parte que confía.

ISO/IEC 1813-5:2021

La norma no se puede consultar en un formato abierto. También se denomina mDL estándar (*Mobile driving license*).

En la '*toolbox'* se usa tanto para el protocolo de comunicación, en el caso de flujos cercanos, como para el modelo de datos especificado en la norma para los atributos.

Se encuentra una referencia a la norma en el documento de análisis de esta, en comparación con W3C VC [31]. En relación con los requisitos revisados se indica que:

- La versión actual de ISO/IEC 18013-5, únicamente cubre los casos de uso en los que el titular presenta físicamente el certificado del atributo o credencial a un lector administrado por un verificador. Por lo tanto, no permite que un verificador remoto interactúe directamente con este certificado, a través de Internet
- Los objetivos principales de ISO/IEC 18013-5 son la interoperabilidad, la extensibilidad, la seguridad y la privacidad.
- El estándar mDL admite la divulgación selectiva (*selective disclosure*) de elementos de datos, el consentimiento informado del usuario y la minimización de datos.
- El estándar especifica los requerimientos de la credencial mDL, pero es posible usarlos para otros tipos usando la norma.
- En el apartado 3.4.1 [31] se define el modelo de datos:
    - Los elementos que conforman el atributo tienen un identificador y están codificados en CBOR (RFC 8949) o JSON (RFC 8259).
    - Los elementos de una credencial mDL se definen dentro de un espacio de nombres con el valor '*org.iso.18013.5.1'*.
    - Si se cumple el estándar se pueden se pueden crear otras credenciales, además de mDL, definiendo un espacio de nombres diferente y nuevos elementos de datos dentro de ese espacio de nombres.
    - Además de un nombre de espacio o 'namespace', existe el concepto de 'documents types', con una notación parecida, en el caso de mDL es '*org.iso.18013.5.1.mDL'*.
- En el apartado 3.4.2 [31] se define el protocolo de comunicación:

- El estándar especifica dos tipos de interfaces: una entre la credencial y el lector de la credencial directamente, y otra entre el lector de la credencial y una autoridad de confianza (emisor de la credencial).
- Según el estándar, las tecnologías que se pueden utilizar son los QR o NFC. Ambos son de corto alcance y necesitan la colaboración del usuario, esto reduce el riesgo de que se obtengan datos mDL sin el conocimiento y consentimiento del titular.
- El lector de credenciales debe admitir las tecnologías de transmisión BLE y NFC.
- En caso de poder comunicar con una autoridad emisora, la credencial incluye un token y una URL, el token no está estandarizado en esta norma pero se recomienda que sea de un solo uso y una validez corta.
- La norma estandariza la estructura de las solicitudes y respuestas intercambiadas entre todos los componentes del sistema de protocolo.
- El lector de mDL debe incluir explícitamente el identificador de cada dato del elemento que quiere recibir en la solicitud. El mDL y/o su titular puede decidir para cada uno de los elementos de datos solicitados si liberarlo o no.

W3C VC + JSON + JWT[SD-JWT]

Es una especificación de W3C, de consulta abierta [32].

Esta especificación es relativa a credenciales que se pueden presentar en la Web de forma segura, gracias a la criptografía, respetuosas con la privacidad y además verificables por una máquina.

En particular, teniendo en cuenta que la toolboox adopta esta especificación para el formato de los contenedores de certificaciones, específicamente en la sección 6.3.1 se define el JSON Web Token y la codificación de la VC en JWT.

Hay que destacar el grupo colaborativo de W3C ‘W3C Credentials Community Group’ con meetings abiertos. [36]

Respecto al modelo de datos de ISO/IEC 1813-5:2021 indicar que:

- No se han especificado para un tipo de credencial el particular, por tanto, no contiene una lista de elementos más definidos como el caso de mDL, los modelos los puede crear cualquier persona, aunque sí existen algunos elementos genéricos tales como emisor o credentialSubject.
- En cada implementación se definen los atributos propios, el identificador de un atributo es una URI. Cada URI es única a nivel mundial. Para facilitar el uso de URIs se puede añadir un contexto a una credencial.
- No exige una codificación concreta, existen ejemplos con JSON-LD, YAML o CBOR.

CBOR (Concise Binary Object Representation) + MSO (Mobile Security Object)

Para los formatos de los contenedores de certificaciones con ISO/IEC 18013-5:2021 se especifica el uso de CBOR para la codificación de los elementos y MSO para la divulgación selectiva de atributos

CBOR es un estándar de Internet para codificación de datos que se define en la RFC 8949 [38]. Algunas de sus características son [37]:

- Se basa en JSON, por tanto, en un intercambio de datos no es necesario crear un esquema.
- En JSON los datos binarios se codifican en base64, CBOR está codificado en binario, lo que ahorra volumen y optimiza el procesamiento.
- Tienen un modelo de datos básico, pero es extensible a través de las etiquetas

El estándar RFC 8152 [40] define la firma y el cifrado de objetos CBOR.

MSO se define en la especificación ISO/IEC 1813-5:2021, define una estructura de datos con un valor hash para cada elemento. El verificador validará el hash y la firma sobre el MSO a través de un certificado incluido en los metadatos del MSO.

7. Resumen del marco de confianza elaborada para el despliegue en la Unión Europea

El marco de confianza elaborado para el despliegue en la Unión Europea, en este caso de la Identidad Digital Europea, engloba todo lo comentado en los apartados anteriores: el marco teórico y el marco legal, revisados en el apartado 5, y el marco tecnológico, resumido y analizado en el apartado 6.

En resumen, el marco de confianza comprende:

Marco teórico	- Conceptos propios de la Identidad Digital Europea definidos en: • Documento principal de referencia del TFM [1] • Última propuesta de revisión del Reglamento eIDAS por parte de la Comisión Europea [8] - Los principales conceptos definidos para el sistema de gestión de la identidad propuesto en el marco de confianza son: • Conceptos • Roles • Alcance • Estados y casos de uso • Arquitectura lógica y definición de flujos
Marco legal	- Es importante definir el marco teórico del sistema, pero sin una cobertura legal no sería posible su implementación. Esto no será realizable hasta que se aprueben las modificaciones en el Reglamento eIDAS, las últimas en la fecha de realización de este estudio son las de febrero del año 2023 [8]. - Una vez aprobado el nuevo Reglamento eIDAS se deberá esperar y conocer el marco legal relacionado que puede aprobarse en España y otros países de la Unión Europea.
Marco tecnológico	-Posiblemente, tanto el marco teórico, como el marco tecnológico, no deberían avanzar hasta que estuviera aprobado el nuevo Reglamento eIDAS, pero al ser un cambio profundo del sistema actual, que puede alargarse en el tiempo, se han iniciado avances en ambos marcos de referencia de forma paralela. - En el caso del marco tecnológico, el documento principal de análisis de este estudio [1] se publicó en enero del año 2023, es muy reciente. Este define principalmente los componentes del sistema EUDI Wallet y específicamente los requisitos y tecnologías para los esquemas de PID, EUDI Wallet y certificación de atributos.

Tabla 13. Marco de confianza de la Identidad Digital Europea

8. Analizar el modelo de cumplimiento existente, los estándares que le aplican y cómo van a evolucionar

8.1. Modelo de cumplimiento existente

La definición de cumplimiento es 'llevar a efecto algo' [69]. En este caso un modelo de cumplimiento o compliance puede describirse como un conjunto de reglas y procedimientos que se establecen para un sistema y que deben realizarse para su correcto funcionamiento.

El modelo de cumplimiento actual se define en el Reglamento eIDAS, encargado de regular los servicios de confianza en la UE. Se destacan los siguientes aspectos principales:

- Respecto a la identificación electrónica, los estados miembros notificarán a la Comisión Europea el sistema de identificación implantado. En el artículo 9 se especifica que la Comisión Europea publicará en el Diario Oficial de la UE los sistemas notificados y la información de estos.
- En el artículo 17, perteneciente a la sección de servicios de confianza, se indica que los Estados miembros designarán un organismo de supervisión y que será el responsable de las funciones de supervisión que el reglamento establece para el Estado miembro. Las funciones principales serán:
    - Garantizar el cumplimiento del reglamento por parte de los prestadores cualificados de servicios de confianza y los servicios que prestan.
    - Conceder o retirar la cualificación necesaria a los prestadores cualificados de servicios de confianza y comunicarlo al organismo responsable de la lista de confianza especificada en el artículo 22.
    - Cooperar con otros organismos de supervisión y la Comisión Europea.
- En el artículo 20, ubicado en la sección de servicios de confianza cualificados, se describe que debe llevarse a cabo una supervisión de los prestadores cualificados de servicios de confianza, que deben ser auditados para confirmar que, tanto ellos como los servicios que prestan, cumplen los requisitos establecidos en el Reglamento. Pueden ser auditados por un organismo de supervisión o por un organismo de evaluación de la conformidad. El Reglamento eIDAS señala los servicios de confianza que necesitan certificación, esto son:
    - Servicio de expedición de certificados electrónicos cualificados de firma electrónica.
    - Servicio de expedición de certificados electrónicos cualificados de sello electrónico.

- Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web.
- Servicio de expedición de sellos electrónicos cualificados de tiempo.
- Servicio cualificado de validación de firmas electrónicas cualificadas.
- Servicio cualificado de validación de sellos electrónicos cualificados.
- Servicio cualificado de conservación de firmas electrónicas cualificadas.
- Servicio cualificado de conservación de sellos electrónicos cualificados.
- Servicio cualificado de entrega electrónica certificada.

- Cada Estado miembro mantendrá una Lista de confianza con la información relativa a los proveedores cualificados de servicios de confianza y de los servicios de confianza cualificados que prestan. Se especifica que se deben mantener, establecer y publicar de forma segura mediante firmas o sellos electrónicos. Las listas de confianza se especifican en el artículo 22.

  La Decisión de Ejecución (UE) 2015/1505 de la Comisión establece las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22 del Reglamento eIDAS [64].

- En el artículo 24 se definen los requisitos que deben cumplir los prestadores cualificados de servicios de confianza.
- En el artículo 30, 31 y 34, dentro de la sección de firma electrónica, se detalla la certificación de los dispositivos cualificados de creación de firmas electrónicas, la lista de dispositivos cualificados de creación de firmas electrónicas y el servicio de conservación de firmas electrónicas. Para el caso de los sellos electrónicos se establece también una certificación y una lista de dispositivos cualificados.

En resumen, en el modelo de cumplimiento se establecen al menos los siguientes roles:

- Comisión Europea
- Organismos de supervisión de los estados miembros de la UE.
- Organismos de evaluación de conformidad (CAB), que podrían ser un organismo de supervisión.
- Lista de prestadores cualificados de servicios de confianza y de los servicios cualificados que prestan

8.2. Estándares del modelo de cumplimiento existente

ENAC es el Organismo Nacional de Acreditación designado por el Estado miembro español en aplicación del Reglamento (CE) nº765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación

y vigilancia del mercado relativos a la comercialización de los productos [53]. Este reglamento promueve un enfoque armonizado para la acreditación en los Estados miembros de la UE.

Es interesante nombrar al European Accreditation (EA), la infraestructura oficial europea de acreditación, asociación encargada de gestionar la acreditación a nivel europeo. Los Estados miembros de la UE deben aceptar los resultados emitidos por los organismos de evaluación de la conformidad acreditados por cualquiera de los signatarios de EA MLA. Además, los mismos organismos de acreditación son evaluados por sus pares de forma transparente por todos.

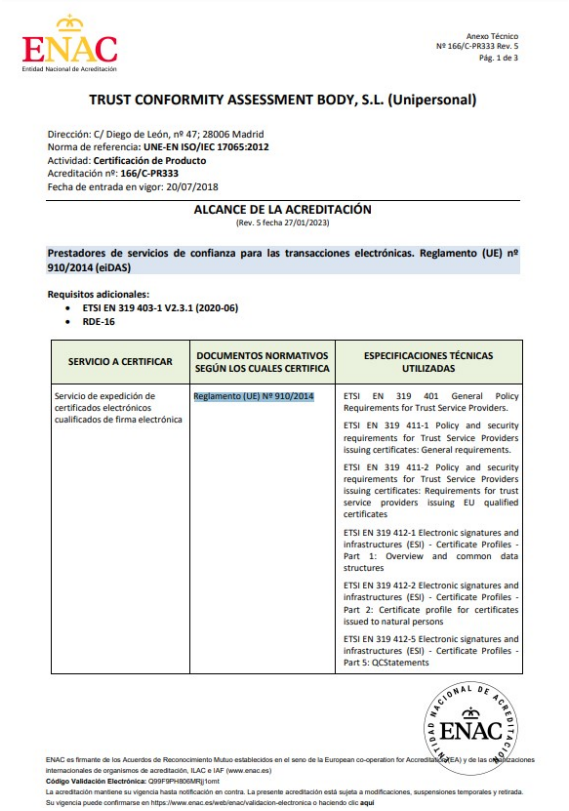
EA mantiene un directorio de las entidades de acreditación y sus evaluaciones [55].

Para establecer el compliance con la normativa europea, ENAC acredita los esquemas relacionados con el cumplimiento del Reglamento eIDAS, tanto de la acreditación de la CAB como de los servicios de confianza que esta ofrecerá. Los estándares y especificaciones que se revisan en la acreditación son los elaborados por ETSI, como, por ejemplo [52]:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI): General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
- ETSI TS 119 511 Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

Específicamente el estándar europeo ETSI EN 319 403 indica los requisitos necesarios para que ENAC pueda realizar la acreditación: Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers, además de los requisitos establecidos en las normas UNE EN ISO/IEC 17065 [54].

En la siguiente figura se muestra un ejemplo acreditación emitida por la ENAC a un proveedor de servicios de confianza cualificado.



ENAC
Entidad Nacional de Acreditación

Anexo Técnico
Nº 166/C-PR333 Rev. 5
Pág. 1 de 3

TRUST CONFORMITY ASSESSMENT BODY, S.L. (Unipersonal)

Dirección: C/ Diego de León, nº 47; 28006 Madrid
Norma de referencia: **UNE-EN ISO/IEC 17065:2012**
Actividad: **Certificación de Producto**
Acreditación nº: **166/C-PR333**
Fecha de entrada en vigor: 20/07/2018

ALCANCE DE LA ACREDITACIÓN
(Rev. 5 fecha 27/01/2023)

Prestadores de servicios de confianza para las transacciones electrónicas. Reglamento (UE) nº 910/2014 (eIDAS)

Requisitos adicionales:
- **ETSI EN 319 403-1 V2.3.1 (2020-06)**
- **RDE-16**

SERVICIO A CERTIFICAR	DOCUMENTOS NORMATIVOS SEGÚN LOS CUALES CERTIFICA	ESPECIFICACIONES TÉCNICAS UTILIZADAS
Servicio de expedición de certificados electrónicos cualificados de firma electrónica	Reglamento (UE) Nº 910/2014	ETSI EN 319 401 General Policy Requirements for Trust Service Providers. ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates: General requirements. ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates ETSI EN 319 412-1 Electronic signatures and infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures ETSI EN 319 412-2 Electronic signatures and infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons ETSI EN 319 412-5 Electronic signatures and infrastructures (ESI) - Certificate Profiles - Part 5: QCStatements

ENAC es firmante de los Acuerdos de Reconocimiento Mutuo establecidos en el seno de la European co-operation for Accreditation (EA) y de las organizaciones internacionales de organismos de acreditación, ILAC e IAF (www.enac.es)
Código Validación Electrónica: Q99F9PH806MRJ1omt
La acreditación mantiene su vigencia hasta notificación en contra. La presente acreditación está sujeta a modificaciones, suspensiones temporales y retirada. Su vigencia puede confirmarse en https://www.enac.es/web/enac/validacion-electronica o haciendo clic **aquí**

Figura 5. Ejemplo de Acreditación de ENAC
https://www.enac.es/documents/7020/6aa99e14-7f23-443c-92c5-1bb61512dc2c

En conformidad con el Reglamento eIDAS y la Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015, en España, el Ministerio de Ministerio de Asuntos Económicos y Transformación Digital gestiona y mantiene pública una Lista de confianza de prestadores de servicios electrónicos de confianza (TSL) de los prestadores que proporcionan servicios electrónicos de confianza cualificados establecidos y supervisados en España [12].

Actualmente en el caso de las listas de confianza es necesario el uso del estándar X.509 para infraestructuras de claves públicas PKI. Es un modelo centralizado que requiere la existencia de organizaciones tales como una Autoridad certificadora o AC que es la responsable de emitir los certificados o una Autoridad de Registro o AR que es la responsable de identificar al solicitante de un certificado.

Sobre los requisitos de seguridad aplicables a los prestadores de servicios de confianza, hay que destacar la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, en adelante NIS2 [67], que:

- Deroga el artículo 19 del Reglamento eIDAS ya que los servicios prestados por prestadores de servicios de confianza se encuentran en el ámbito de NIS2.
- Las obligaciones en materia de ciberseguridad de NIS2 son complementarias a los requisitos establecidos en el Reglamento eIDAS que se imponen a los prestadores de servicios de confianza. Los requisitos aplicables a los

prestadores cualificados de servicios de confianza establecidos en el artículo 24 del Reglamento eIDAS siguen siendo de aplicación.

8.3. Evolución a un nuevo modelo de cumplimiento

En el nuevo marco de confianza propuesto, tanto en el marco legal a partir de la nueva propuesta del Reglamento eIDAS, como en el marco teórico establecido en el documento de referencia principal de estudio [1], se perfila la siguiente evolución del modelo de cumplimiento definido:

- Los roles de gobernanza y otros roles definidos [1] describen por un lado roles ya existentes en el modelo actual, y que por tanto implicaría cambios funcionales en estos, y, por otro lado, roles nuevos a crear y añadir al modelo:

Organismo de evaluación de conformidad (Conformity Assessment bodies (CAB))	Ya existe este role actualmente, se los debería habilitar para poder auditar la conformidad de las EUDI Wallets y los proveedores de servicios de confianza cualificados para los nuevos servicios.
Organismo supervisor (Supervisory bodies)	Ya existe este role actualmente, estos organismos de supervisión de los proveedores de servicios de confianza no cualificados ahora deberán tener en cuenta los futuros cambios normativos.
Proveedores de esquema (Q)EAA	Es un nuevo role que deberá incluirse en el modelo de cumplimiento, publicarán esquemas y vocabularios que describen la estructura y semántica de los (Q)EAA.
Organismo Nacional de Acreditación (National Accreditation bodies)	Ya existe este role, deberá incluir nuevas acreditaciones y revisar esquemas existentes.
Proveedor EUDI Wallet (Trusted list Provider)	Es un role nuevo que debe añadirse al modelo de cumplimiento. Probablemente serán organizaciones reconocidas por los Estados miembros. Están pendiente los términos y condiciones del reconocimiento por parte de cada país. Estos proveedores serán responsables del compliance de la EUDI Wallet según la certificación que establece la modificación propuesta del reglamento eIDAS.
Lista de Confianza de proveedores	Este role ya existe, deberá ampliarse a nuevos proveedores y servicios de confianza
Fuentes auténticas (Authentic sources)	Nuevo role a definir en el modelo de cumplimiento, estas tendrán que proveer interfaces para los

	proveedores de QEAA o EAA.
Fabricante de dispositivo	La nueva propuesta eIDAS establece restricciones respecto a dispositivos. No se especifica si se deberá realizar una evaluación de dispositivos y crear una lista de confianza.

Tabla 14. Revisión roles de gobernanza EUDI Wallet vs modelo de cumplimiento

- Se añade una nueva certificación que realizará el CAB, respecto a la solución wallet.
- La norma de referencia será el nuevo reglamento eIDAS, pero se debe avanzar, por parte de ETSI o CEN, en la elaboración de nuevos estándares y especificaciones para su uso en las auditorías de conformidad. Algunas de las especificaciones en elaboración relacionadas con el nuevo modelo, de las que es posible consultar el programa de trabajo en ETSI, son:
    - ETSI TS 119 462 EUDI Wallet -Wallet interfaces for trust services and electonic signatura [56]
    - ETSI TS 119 471 Policy and Security requirements for Attribute Attestation Services [57]
    - ETSI TS 119 472 Profiles for Attribute Attestations [58]
- La EUDI Wallet deberá estar certificada para garantizar las evaluaciones de conformidad y demostrar el cumplimiento un nivel de seguridad alto. El uso de un sistema de certificación de la ciberseguridad debería aportar un nivel armonizado de confianza en la seguridad de la EUDI Wallet. Se espera que el almacenamiento seguro de material criptográfico también esté sujeto a la certificación de ciberseguridad.
- El proceso de certificación de los proveedores de carteras IDUE debe aprovechar, basarse y exigir el uso de los sistemas de certificación pertinentes y existentes del Reglamento sobre la Ciberseguridad: Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación
- La propuesta legal de reforma del reglamento EIDAS establece restricciones (por ejemplo, el cumplimiento de Nivel de Aseguramiento Alto – “LoA high”) respecto a qué tipos de dispositivos y servicios se pueden utilizar con el fin de emitir la EUDI Wallet.
- En el nuevo sistema propuesto es necesaria la gestión de nuevas listas de confianza, por ejemplo: proveedores de wallets, las partes que confían o los catálogos de esquemas de los certificados de los proveedores.

9. Analizar el cumplimiento del marco de confianza para una solución existente: EBSI

9.1. Introducción a EBSI

En el año 2018 los estados miembros de la UE crean la asociación European Blockchain Partnership, en adelante EBP. En la declaración de su formación [59] se detalla como objetivo principal el desarrollo de una infraestructura basada en la tecnología de cadena de bloques para transformar los servicios digitales en la UE. Hay que destacar las siguientes ideas incluidas en la declaración:

- Respecto a las tecnologías indican que estas tienen el potencial de cambiar la forma en que los ciudadanos y las organizaciones colaboran, comparten información, ejecutan transacciones, organizan y entregan servicios.
- El enfoque es que estas tecnologías permitirán crear más servicios descentralizados, confiables y centrados en el usuario, proporcionando un mejor control de los datos por parte de los ciudadanos.
- Mediante esta asociación se quiere evitar la fragmentación en el desarrollo de estas tecnologías y hacer realidad además de la implantación de estas, la interoperabilidad entre los Estados miembros.
- Se quiere crear una infraestructura con altos estándares de seguridad, confidencialidad y cumplimiento de las normativas europeas, que ofrezca un marco confiable que proporcione también igualdad de condiciones y fomentar la competencia en las empresas. Esta infraestructura podría utilizarse para respaldar servicios digitales confiables en Internet.

Por tanto, la European Blockchain Services Infrastructure, en adelante EBSI, surge como iniciativa de la Comisión Europea y la EBP para la creación de una plataforma blockchain pública permisionada en la UE.

Actualmente para su financiación, EBSI se incluye en el Programa Europa Digital (DIGITAL), específicamente en la licitación '*Accelerating best use of technologies (DIGITAL-2022-DEPLOY-02)*' [60] bajo el tema '*DIGITAL-2022-DEPLOY-02-EBSI-SERVICES*'.

He de informar que esta licitación también incluye estas dos líneas, relacionadas con el objeto de estudio:

- El tema '*DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID'*, que articula los LSP propuestos en la estrategia de implantación de la Identidad Digital Europea, Además, establece como requisito el cumplimiento de los estándares establecidos en el documento de referencia '*The European Digital Identity Wallet Architecture and Reference Framework'* [1].

- El tema '*DIGITAL-2022-DEPLOY-02-BLOCKCHAIN-STANDARD'* para avanzar en la UE en la estandarización de las tecnologías blockchain.

EBSI es una red P2P que consta de varios nodos distribuidos por los estados miembros de la UE. Cualquier organización de uno de los países que componen la EBP puede crear un nuevo nodo, para esto es necesario el aval del miembro de la EBP de su país, además de cumplir las condiciones que se establecen a un '*Node operator'*, tales como reglas operativas, requisitos técnicos y SLA's mínimos. [61]. El miembro de la EBP del país que acepta el aval también será el encargado de la supervisión del cumplimiento de las condiciones establecidas al nuevo operador.

Dentro de EBSI existen distintos entornos: un entorno piloto para pruebas de usuario. Los entornos de preproducción y producción para el proceso de aceptación y finalmente el propio entorno de EBSI real. Todos los nodos de la red pueden realizar transacciones que actualizarán el libro mayor, además cada nodo mantiene una copia idéntica de este libro mayor.

La arquitectura de EBSI se compone de cinco capas [62]:

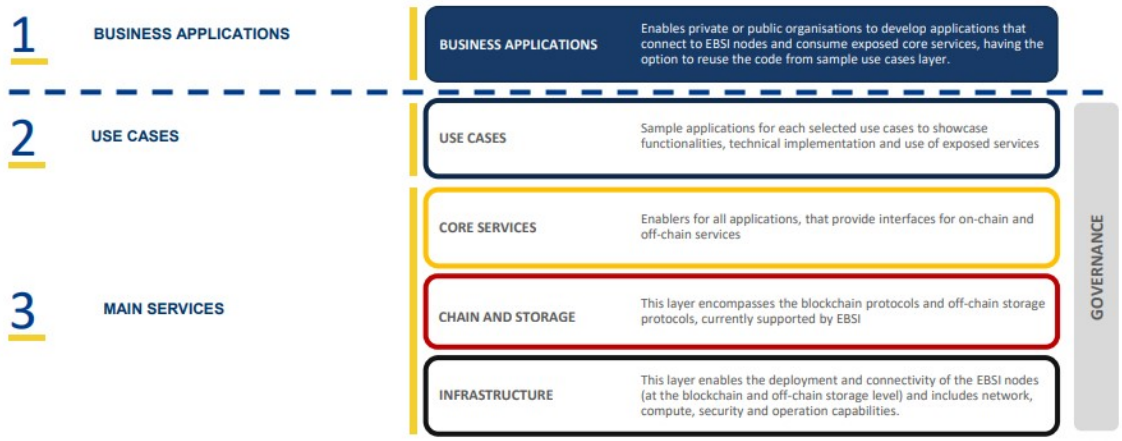


Figura 6. Arquitectura EBSI

De abajo a arriba son:

- Infraestructura: Esta capa se encarga del despliegue y conectividad de los nodos. Utiliza tecnología de contenedores mediante el uso de imágenes. Se realizan tareas de automatización, monitorización y configuración/orquestación.
- Chain and storage: Esta capa se encarga de la gestión de los protocolos de la cadena de bloques y los soportados fuera de la cadena de bloques. Utiliza la blockchain Hyperledger Fabric [50] pero puede integrarse con otras blockchain como Consortium Ethereum mediante el cliente Hyperledger Besu [52]. Contiene los smart contracts y servicios off-chain de almacenaje de ficheros, datos relacionales, clave/valor o big data. El tipo de almacenaje puede ser distribuido por los nodos, privado en un nodo o incluso externo, por ejemplo, en un proveedor de cloud.

- Core services: Habilita interfaces para conectar con los servicios de las capas inferiores, permite abtraerse de la implementación de estas. Actualmente existen trece tipos de APIs que integran varios servicios: Authorisation, DID Registry, Ledger, Notifications, Proxy Data Hub, Storage, Timestamp, Trusted Apps Registry, Trusted Issuers Registry, Trusted Ledgers & Smart Contracts Registry, Trusted Policies Registry, Trusted Schemas Registry y Users Onboarding.

- Use Cases: Para un conjunto de casos de uso propuestos se ejemplifican aplicaciones para mostrar las funcionalidades, implementación técnica y uso de los servicios. Por el momento existen tres dominios con distintos servicios [43]:
    - Track and trace: SMEs Financing y Document Traceability.
    - Verificable credentials: SSI, Social security y Diploma
    - Trusted data exchange: Asylum process management y Trusted Data Sharing.
- Business applications: Esta capa no está realizada por EBSI, serán las aplicaciones que pueden realizar tanto organismos públicos como empresas privadas para el uso de los servicios core ofrecidos por EBSI. Los casos implementados en la capa inferior pueden reusarse para los desarrollos.

9.2. Caso de uso SSI en EBSI

El caso de uso SSI de Verificable Credentials, desarrollado en EBSI, se ajusta con bastante similitud a los conceptos definidos en el apartado 5.1, relativos al marco teórico de la identidad soberana.

EBSI define estos tres conceptos como los principales:

- Las credenciales verificables, definidas en la especificación '*EBSI W3C Verifiable Credentials (VCs) and W3C Verifiable Presentations (VPs)*' [42][43]
- Wallets digitales
- Blockchains para almacenar DIDs y Listas de confianza

Y además EBSI también contiene los siguientes conceptos:

- La existencia del '*Trust triangle'* conformado por *Issuers*, *Holders* y *Verifiers*.
- El uso de los W3C Decentralised Identifier (DID) [44]
- Marco de gobernanza que establece la confianza en la red y el caso de uso de la SSI.

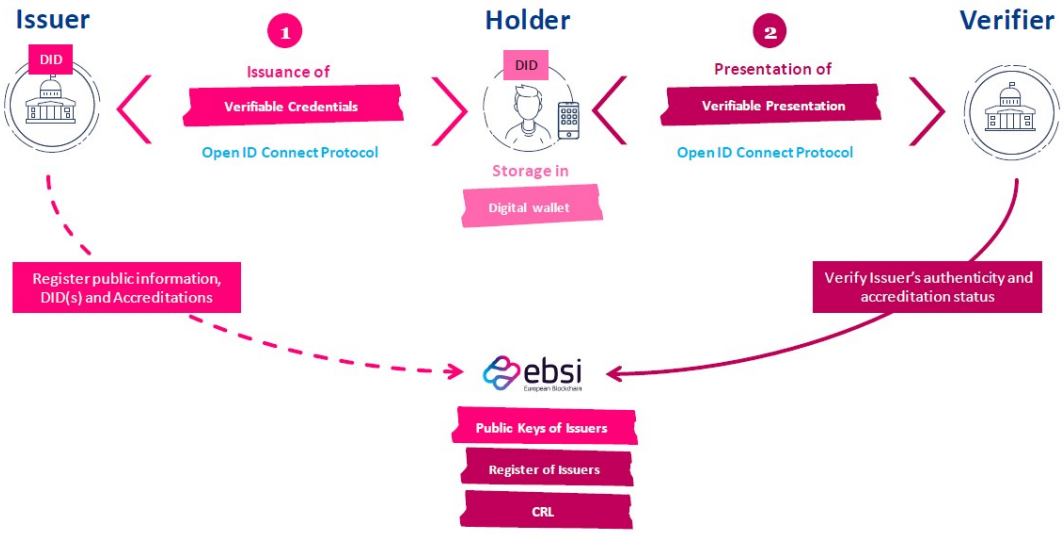


Figura 7 Escenario SSI [42]

En relación con las capas definidas en la arquitectura EBSI, la siguiente imagen es un ejemplo del flujo de una transacción [62]:

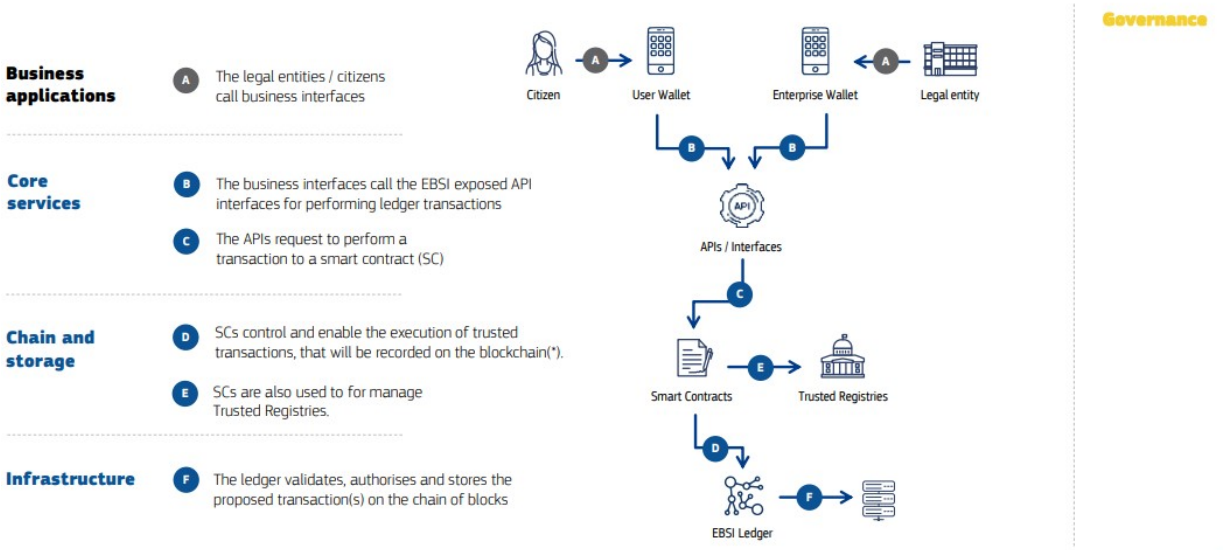


Figura 8 Flujo transacción SSI [62]

A continuación, se detallarán los principales conceptos en EBSI relacionados con el caso de uso SSI:

- Credenciales Verificables
- W3C Decentralised Identifier (DID)

- Modelo de confianza y gobernanza en EBSI
- Wallet

Credenciales Verificables

Las credenciales verificables son una implementación segura de una credencial, se basan en el estándar VC de W3C reconocido a nivel global para la presentación de credenciales en Internet.

Existen principalmente dos tipos: EBSI W3C Verifiable Credentials (VCs) and W3C Verifiable Presentations (VPs). En EBSI se han definido distintos esquemas de credenciales específicos para los distintos casos de uso y algunos generales de base. Es posible definir nuevos esquemas en función de las nuevas necesidades de credenciales. Existe una jerarquía, unos extienden a otros en el nivel superior.

Los distintos esquemas de modelos de datos se administran en la blockchain de EBSI, en el TSR, accesible a través de la API.

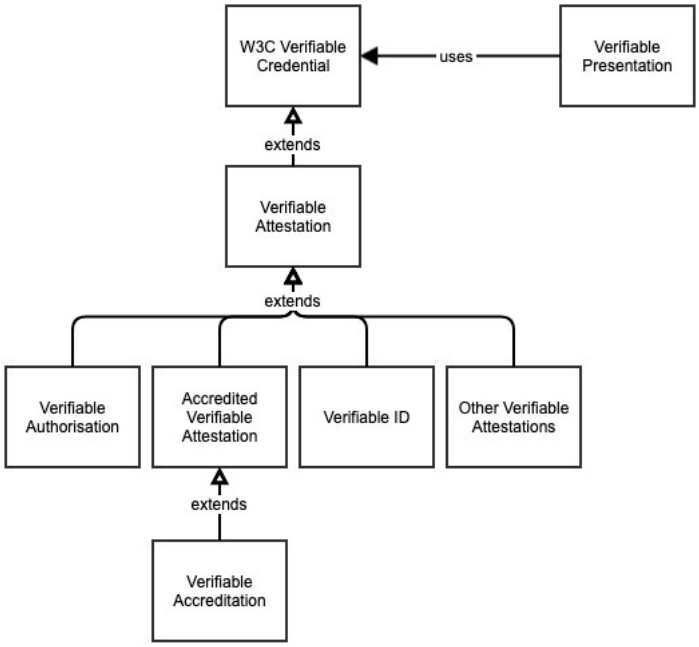


Figura 9 Esquema de datos de EBSI y jerarquía entre ellos

Una credencial contiene:

- Metadatos de la credencial: DID del Issuer y campos para el estado de la credencial tales como fechas y estado.
- Claims, se denomina así a las distintas afirmaciones de atributos del Holder que han proporcionado los Issuer's. contiene el DID del Holder.

- Firma del Issuer (Proof): prueba digital de la autenticidad e integridad de la credencial.

El formato de las credenciales es JWT (token web JSON) y JSON-LD (datos vinculados JSON), depende de los requisitos del caso de uso y la necesidad de diferentes tipos de firma.

W3C Decentralised Identifier (DID) [44]

El identificador DID se utiliza para garantizar la autenticidad de los Holders e Issuers de una credencial verificable.

El identificador por sí solo no contiene información respecto a una persona física o jurídica. El formato de un identificador DID es una cadena larga que sigue el estándar W3C, se compone de tres partes:

- Empieza por la cadena '*did*'
- A continuación, contiene un identificador
- Y por último un número aleatorio que se crea según el método indicado en la especificación.

Un ejemplo sería:

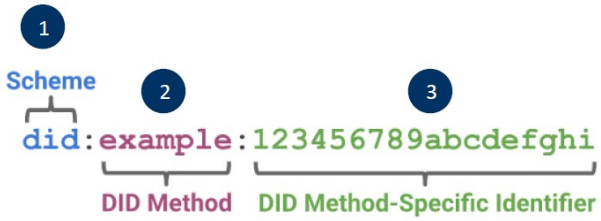


Figura 10 Formato DID

En EBSI existen dos métodos distintos:

- DID method specification v1 orientado a personas jurídicas y que se almacena en la red blockchain.
- DID method specification v2 orientado a personas físicas y que, por razones de privacidad y cumplimiento normativo de las leyes de protección de datos, se almacena únicamente en la wallet.

Modelo de confianza y gobernanza en EBSI

EBSI crea un modelo de confianza totalmente distribuido a partir de la tecnología blockchain y el estándar DID.

El marco de gobernanza establece un conjunto de reglas, cada sector o Estado miembro será el responsable de definir y gestionar el emisor de acreditaciones sin necesidad de una autoridad central. Únicamente se requiere dos roles de gobernanza en EBSI:

- Trusted Accreditation Organisation (TAO): Encargado de verificar, acreditar y administrar a las Trusted Issuers para poder emitir ciertos tipos de VC. También se encargan de regitrar los esquemas asociados al VC. Pueden existir distintos niveles jerárquicos de TAO's y denominarse root TAO o sub-TAO en función del nivel que ocupen.
- Trusted Issuer (TI): Issuer de confianza que emitirá el VC.

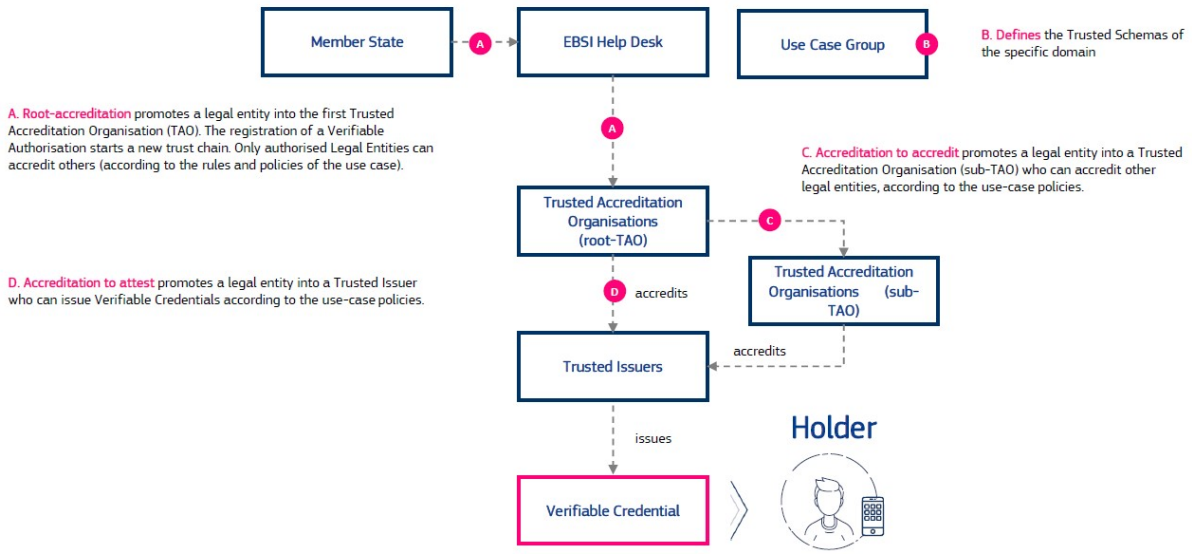


Figura 11 Cadena de confianza en EBSI [46]

En la blockchain de EBSI se almacena la siguiente información: Claves públicas de los Issuers, Registro de Issuers y Registro de los esquemas de certificados. El role Verifier puede consultar esta información en la blockchain EBSI para comprobar la validez de los datos del VC.

En la blockchain también se almacena un documento DID de las TAO's, la autorización (Verifiable Authorisation) y la acreditación (Verifiable Accreditation).

En la blockchain se almacena un documento DID del Issuer, debido a que por razones de seguridad el Issuer puede actualizar sus claves criptográficas en el tiempo, existen

varias versiones del documento DID almacenados. La información de la versión correcta se almacenará en el VC para que el Verifier pueda consultar el documento correcto.

Wallet

Para el funcionamiento de la plataforma EBSI y específicamente el caso de uso SSI, es necesario el uso de aplicativos informáticos tales como aplicaciones web o apps móviles, para que los distintos roles participantes puedan ejecutar las funcionalidades del sistema SSI y conectar también con las APIs de EBSI.

Una wallet en el contexto de EBSI permite a su usuario el almacenamiento y seguimiento seguro de su información digital, tal como certificados digitales e información de identidad digital. Para poder interactuar con el sistema EBSI una wallet debe ser conforme, es decir que debe superar los '*Wallet Conformance Test'*, en adelante WTC.

Los documentos publicados en EBSI respecto a la conformidad en la versión 3 son:

- Verifiable Credential Issuance Guidelines: Define la especificación de emisión de VC en conformidad con el protocolo OIDC 4 Verifiable Credential Issuance [65]. El flujo lo puede iniciar el Issuer, por ejemplo, un servicio que ofrece desde su página web, o el propio Holder o usuario, por ejemplo, una petición al Issuer desde su wallet.

- Veriable Presentation Exchange Guidelines. Define la especificación para los intercambios de VP en conformidad con OpenID for Verifiable Presentations [29]. Se indica que la principal diferencia con OpenID4VP es que el flujo lo inicia la wallet.

- Providers and Wallets Metadata

- Accredit and Authorise Functional Flows, Define los flujos del módulo 'Accredit 'y 'Authorise' para realizar la prueba de conformidad.

- Issue to Holder Functional Flows: Para el testeo de la emisión de VC, se simula fuera de EBSI con una interfaz de usuario para la conformidad.

- Holder Wallet Functional Flows: Test específicos para la prueba de conformidad de los flujos de la wallet.

- Verifier Functional Flows: Test específicos para la prueba de conformidad de los flujos del Verifier.

Y en la versión 2:

- Credential Issuance Guidelines: Define la especificación de emisión de credenciales en conformidad con el protocolo OIDC 4 Verifiable Credential Issuance [65].

- Veriable Presentation Exchange Guidelines: Define la especificación para los intercambios de VP con OpenID Connect for Verifiable Presentations [29] y OpenID Connect Self-issued OpenID provider V2 [30]

En la página web de EBSI se publican con total transparencia las wallets conformes con la información de las pruebas realizadas y los casos de uso que estas cubren del ecosistema EBSI.

Sobre la wallet, EBSI está pendiente de publicar en breve:

- Capítulo 7 de la colección de guías '*EBSI Verifiable Credentials explained*' dedicado a la wallet,
- Test de conformidad v3 de la wallet '*Verify*'

9.3. Análisis Marco de confianza y cumplimiento en EBSI

A continuación, se va a revisar en EBSI el marco conceptual y tecnológico, definido en los apartados 5 y 6, para la Identidad Digital Europea.

En el marco teórico definido en el apartado 5.2 se revisaron los siguientes temas:

1. Conceptos
2. Roles
3. Alcance
4. Estados y casos de uso
5. Arquitectura lógica y definición de flujos

1. Comparativa conceptos Identidad Digital Europea vs EBSI

Concepto	**Definición Reglamento eIDAS [8]**	**EBSI**
Atributo (attribute)	Rasgo, característica o cualidad de una persona física o jurídica o de una entidad.	Tiene el mismo significado, no se define directamente en EBSI pero se nombra en la documentación EBSI [43][45]. También al referirse a los VC, en las especificaciones de W3C se nombran, se especifica que un VC contiene: "Información relacionada con atributos o propiedades específicas que afirma la autoridad emisora sobre el tema (por ejemplo, la nacionalidad, las clases de vehículos con derecho a conducir o la fecha de nacimiento)" [32]

PID: Person identification data	Un conjunto de datos, emitido de conformidad con las leyes nacionales de cada estado miembro, que habilita la identidad de una persona.	En la especificación 'Data Models and Schemas' se define un tipo especial de VC 'Verifiable ID-Natural Person'. En la documentación [42] se indica que la VC se puede complementar con una identidad digital de confianza del ciudadano. La VC de EBSI soporta el formato DID v2 que en el caso del Holder se almacena en la wallet y no en la blockchain.
Fuente auténtica (Authentic source)	Un sistema, que puede gestionar tanto el sector público como el privado, y contiene atributos sobre una persona que se consideran la fuente principal de esa información y que así se reconoce por el derecho de la UE o el nacional.	Este concepto es similar en EBSI, se encuentra en la documentación [42] [46]
EAAs (Electronic Attestation of attributes)	'Attestation' es la certificación electrónica de atributos que permite la presentación y autenticación de atributos.	EBSI W3C Verifiable Credentials (VCs) and W3C Verifiable Presentations (VPs).
(Q)EEA (Qualified Electronic Attestation of attributes provider)	Certificación emitida por un proveedor de servicios de confianza cualificado y que cumple con los requisitos establecidos en el Anexo V del eIDAS.	EBSI W3C Verifiable Credentials (VCs) and W3C Verifiable Presentations (VPs).
QSCD (Qualified Signature Creation Device)	Dispositivo cualificado de creación de firmas electrónicas que cumpla los requisitos establecidos en el Anexo II	Concepto definido en el eIDAS. EBSI soporta advanced electronic signatures (AdES). La firma qualificada es una firma avanzada, pero con otros requisitos añadidos tales como QSCD y certificados cualificados.

Servicio de confianza (Trust service)	Un servicio de confianza en el marco del eIDAS, especificado en el artículo 1.	Mismo significado, vigente en el eiDAS actual. La modificación propuesta añade la atestación de atributos como servicio de confianza.
Proveedor de servicio de confianza (Trust service provider)	Persona física o jurídica que presta uno o más servicios (proveedor) de confianza cualificados o no cualificados.	Mismo significado en EBSI que usa también criptografía de clave pública. Al ser la atestación un nuevo servicio de confianza también será el rol Trust Issuer.
QTSP (Qualified Trust Service Provider)	Proveedor de servicios de confianza que proporciona uno o más servicios de confianza cualificados y el organismo supervisor le otorga el estatus cualificado.	Mismo significado en EBSI que usa también criptografía de clave pública. Al ser la atestación un nuevo servicio de confianza también será el rol Trust Issuer.
Parte que confía (Relying party)	La parte que recibe la información de identificación electrónica o de atributos procedente de EUDI Wallet.	Verifier
User (Usuario)	Es una persona física o jurídica que utiliza una EUDI Wallet	Holder
National Accreditation Bodies (NAB)	Los Organismos Nacionales de Acreditación según el Reglamento (CE) nº 765/2008 son los organismos de los Estados miembros que realizan la acreditación de Organismos de Evaluación de Conformidad con autoridad derivada del Estado.	TAO
Emisor (Issuer)	Un proveedor de datos de identificación de persona (PID) o de servicios de confianza que emite atributos (Q)EAA. En la arquitectura propuesta pueden existir varios	Issuer

	emisores.	
Proveedor de PID (PID Provider)	Estado miembro o entidad jurídica que proporciona datos de identificación de la persona a los usuarios como fuente primaria.	Issuer específico que gestiona el Estado miembro responsable de la identificación.
PKI Public Key Infraestructure	Una infraestructura de clave pública de la EUDI Wallet para gestionar las claves públicas. Una PKI emite certificados que contienen la clave pública y gestiona la confianza en esta. Es un sistema centralizado de gestión de las claves.	Mismo significado en EBSI, En la documentación se explica el modelo actual centralizado [45]
Divulgación selectiva (Selective Disclosure)	Capacidad de la EUDI Wallet que permite al usuario presentar un subconjunto de atributos de entre los que figuran en los PID o en los (Q)EAA.	En el estándar W3C se usa '*Zero-Knowledge Proofs*', es un método criptográfico para poder demostrar que conoce un valor sin revelar el valor real de este.
Confianza (Trust) OASIS open standard ws-trust 1.4	Trust framework: Conjunto jurídicamente exigible de normas y acuerdos operativos y técnicos que rigen un sistema de múltiples intervinientes diseñado para realizar determinados tipos de transacciones entre una comunidad de participantes y sujeto a un conjunto común de requisitos. En el estudio del marco teórico se revisan estos requisitos. Trust model: Conjunto de normas que garantizan la legitimidad de los componentes y las entidades que intervienen la Identidad Digital Europea. Trusted List: Repositorio de información sobre entidades dotadas de autoridad en un determinado contexto legal o contractual que proporciona	Definido en el Modelo de confianza y gobernanza en EBSI: Issuers Trusted Accreditation Organisation (TAO) Trusted Issuer (TI) Listas de confianza y esquemas en la blockchain de EBSI

	información sobre su estado actual e histórico. Las listas de confianza pueden implementarse de diferentes maneras.	
EUDI Wallet Solution	Solución (Solution): Producto que ofrece los servicios de una EUDI Wallet, que puede ser certificada como conforme por un CAB. Instancia (Instance): Instancia de una solución de EUDI Wallet perteneciente a un Usuario y que está bajo su control. Proveedor (Provider): Organización, pública o privada, responsable del funcionamiento de una solución de EUDI Wallet compatible con eIDAS que puede instanciarse, por ejemplo, mediante su instalación e inicialización.	Están pendiente de publicación para el Q2 del 2023 las pruebas de EBSI para la conformidad a la versión 3: '*Verify*'. Por el momento se han publicado '*Accredit and Authorise*', '*Holder Wallet*' y '*Issue to Holder*' Por el momento hay más de 30 wallets certificadas en EBSI, esta guarda el Holder DID, VC y contraseñas.

Tabla 15. Comparativa conceptos Identidad Digital Europea vs EBSI

2. Comparativa roles Identidad Digital Europea vs EBSI

-Roles principales:

Concepto	**Definición**	**EBSI**
Usuario	Este role es el centro del sistema, el principal objetivo del nuevo sistema de gestión de la identidad es permitir a los usuarios el control de su identidad digital. Es el usuario de la EUDI Wallet que recibirá, guardará y presentará certificaciones de tipo PID, QEAA o EAA. También le será posible crear firmas tipo QES	Holder
Proveedores	(Role 3) Proveedores del PID: Entidades de confianza responsables de verificar la identidad (PID) del usuario, tiene que cumplir requisitos de tipo LoA high requirements.	Issuers, es necesario la identificación de estos y la autenticación, con LoA o HoA, en función de si es un issuer de un eID o de un atributo menor.

	(Role 5) Proveedores de QEAA: Mantendrán interfaces para intercambio de QEAA, incluyendo autenticación mutua con la EUDI Wallet, e interfaces con Authentic sources para verificar los atributos. No puede almacenar información del uso de los servicios a los que puede acceder con una QEAA un usuario. (Role 6) Proveedores de EAA: Será necesario cumplir las especificaciones técnicas para conectar la EUDI Wallet con otros atributos, dependerá de las normas de cada sector, no será posible guardar información del uso de los atributos por parte del usuario. (Role 7) Proveedores de QES	Los Trust Issuers almacenan en la blockchain de EBSI sus acreditaciones y documentos DID's. Una vez aceptado el esquema, este se almacenará en la blockchain de EBSI por parte de la TAO. La generación de firmas QES no se encuentra en el alcance de EBSI
Parte que confía (Role 9)	Podrán conectar con la EUDI Wallet, tendrán que informar el uso y finalidad a los estados miembros implicados. Es necesario una interfaz con la EUDI Wallet con autenticación mutua para las peticiones.	Verifier

Tabla 16. Comparativa roles principales Identidad Digital Europea vs EBSI

-Roles de gobernanza:

Concepto	**Definición**	**EBSI**
Organismo evaluación conformidad (CAB)	Serán los organismos, públicos o privados, responsables de auditar la conformidad de las EUDI Wallets y los proveedores de servicios de confianza cualificados	En EBSI la conformidad de las wallets la gestiona propiamente EBSI, es necesario pasar los tests publicados en la página web. TAO para el caso de la conformidad a los Trust Issuers.
Organismo supervisor	Los Estados miembros deben notificar a la Comisión Europea la designación de estos organismos de supervisión de los proveedores de servicios de confianza no cualificados.	En el caso de EBSI las TAO´s y sub-TAO`s son las que se encargan en función del dominio y credencial aceptado por EBSI y el Estado miembro.

Proveedores esquema (Q)EAA	Los proveedores de esquemas (Q)EAA publican esquemas y vocabularios que describen su estructura y semántica. La Comisión Europea establece las especificaciones técnicas, normas y procedimientos mínimos.	Las TAO's se encargan de registrar esta información en la EBSI blockchain.
Organismo Nacional de Acreditación	Organismos de los estados miembros que acreditan las CABs.	Root TAO

Tabla 17. Comparativa roles de gobernanza Identidad Digital Europea vs EBSI

-Otros roles del sistema:

Concepto	**Definición**	**EBSI**
Proveedor EUDI Wallet	Estados miembros UE u organizaciones reconocidas por estos. Están pendiente los términos y condiciones del reconocimiento por parte de cada país. Estos proveedores serán responsables del acompliance de la EUDI Wallet.	Conformidad en EBSI de la wallet
Lista de Confianza de proveedores	verificar el estatus de un role de la Identidad Digital Europea	Se almacenan en la blockchain de EBSI los registros de Issuers y sus estados, así como sus claves públicas.
Fuentes auténticas (Authentic sources)	Tendrán que proveer interfaces para los proveedores de QEAA o EAA.	Fuera de EBSI, el Issuer conecta con estas fuentes.
Fabricante de dispositivo	Las EUDI Wallet dispondrán de varias interfaces con los dispositivos en los que se basen, la nueva propuesta eIDAS establece restricciones respecto a dispositivos.	No encuentro en EBSI especificaciones de los dispositivos.

Tabla 18. Comparativa otros roles principales Identidad Digital Europea vs EBSI

3. Comparativa Alcance Identidad Digital Europea vs EBSI

En EBSI el alcance de definición es mayor, el estado de madurez está más avanzado y además de las interacciones entre Issuers-Holder-Verifiers se definen por ejemplo los DIDs y la implementación de las listas de confianza en la blockchain. El ecosistema

EBSI es una plataforma que como producto viable ya puede implementar casos de uso en su totalidad.

En el caso de la Identidad Digital Europea hay pendiente de definir temas tan importantes como la implementación del marco de gobernanza y probablemente la revisión de protocolos y tecnologías propuestas, también en función de la implementación los próximos meses de los LSP.

4. Comparativa Estados y casos de uso Identidad Digital Europea vs EBSI

En el caso de la solución wallet, EBSI es la responsable de aceptar el uso de una wallet en la plataforma. EBSI publica en la página web un listado de las wallets conformadas indicando tipo de dispositivo, que puede ser móvil y escritorio, y los casos de uso certificados.

EBSI únicamente recomienda aquellas wallets que han pasado las últimas versiones de las pruebas de conformidad, el resto se informa que se consideran obsoletas y que pueden no disponer de algunas funcionalidades y se podrían dejar de fabricar. No consta información sobre el estado de la solución wallet de forma parecida a lo especificado para la Identidad Digital Europea.

En cuanto al ciclo de vida y estados de los PID/(Q)EAA, en el caso de EBSI, el esquema 'Verifiable Attestation' dispone tanto de campos para poder comprobar las fechas de vigencia de la credencial como de campos para el control del estado. Y el caso de poder ser revocado por el proveedor también es posible tal como se especifica en los flujos definidos para la conformidad a la versión 3 de la wallet, específicamente el flujo '*Issue CTRevocable Credential and revoke it'* de la prueba '*Accredit and Authorise Functional Flows'.*

5. Comparativa Arquitectura lógica y definición de flujos Identidad Digital Europea vs EBSI

EBSi no define una arquitectura lógica específica que deba cumplir una wallet, para conseguir la conformidad en EBSI, es necesario cumplir los WTC. Estas pruebas verifican que la billetera cumpla con ciertos estándares de rendimiento y funcionalidad. El WCT evalúa la capacidad de la billetera para manejar las credenciales asignadas por un emisor simulado y devolverlas a un verificador simulado

En EBSI se soportan los flujos 3 y 4 definidos en la Identidad Digital Europea.

Para los casos de los flujos 1 y 2, relativos a casos de proximidad, en la documentación de EBSI se define el flujo 'Cross-*device flow - Agent to agent*' en el que el Verifier no tienen un punto de entrada en Internet, sino que dispone de una aplicación móvil y el Agente SSI del Holder capturará el código QR que genere dicha aplicación móvil, aunque en este caso ambos deben tener acceso a la API de EBSI y

por tanto conexión a Internet, aunque no es necesario que el Verifier disponga de un punto de entrada en Internet. En la documentación se especifica que este caso de uso no permite presentación off-line y parece que sigue bajo revisión.

A continuación, se va a revisar en EBSI el marco tecnológico para la Identidad Digital Europea definido en el apartado 6.

1. Requisitos de expedición del PDI.

En la documentación de EBSI se define los data models y esquemas de los certificados. En el caso del PID el modelo correspondiente en EBSI sería el '*VerifiableID Natural Person*', este cumple los estándares y recomendaciones del reglamento eIDAS, el eidas Minimum Dataset definido por SEMIC [66], el modelo de W3C y el formato de fecha/hora RFC 3339.

En la documentación se definen varios modelos y su jerarquía al extender uno de otros. El '*VerifiableID Natural Person*' extiende a '*Verifiable Attestation'* que extiende a la especificación W3C VC.

En el caso de '*Verifiable Attestation'* se añaden las propiedades necesarias para la certificación verificable de una identificación: formatos, fechas, issuer, datos del sujeto, datos del estado, datos del esquema, etc.

Y para cada requisito definido para el PID:

Requisito	**Descripción**	**EBSI**
DEBE (OBLIGATORIO)		
INFO.01	Contener la información para identificar al proveedor	La credencial contiene el DID del Issuer
INFO.02	Contener la información para realizar una comprobación de integridad de datos	Los DIDs garantizan la autenticidad de los Issuers y Holders: v1 legal persons y v2 natural persons. En la EBSI se almacena: Issuer public key, Registro de issuers, CRL: Listado de revocaciones de issuers keys. En la wallet se guardarán las de tipo v2. Para asegurar la autenticidad/integridad se usa firma electrónica sistema de claves privadas y públicas: -Al crear un VC este lo firma el Issuer con su clave privada y en el documento DID del Issuer en la blockchain EBSI se
INFO.03	Contener la información para verificar su autenticidad	

		almacena la clave pública de este. - Al presentar una VP la firma el Holder mediante su clave privada, y el Verifier la chequea usando la clave pública de este, almacenada en el DID Holder.
INFO.04	Contener la información para comprobar el estado de validez de las certificaciones	La credencial contiene valores relacionadas con el estado y campos de fecha para la validez: issuanceDate, validFrom, validUntil, credentialStatus
INFO.05	Contener la información para verificar la vinculación del titular por una parte que confía	La credencial contiene el DID del Subject
INFO.06	Emitirse para ser presentada de acuerdo tanto con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021 como con el Modelo de datos de credenciales verificables v1.1 del W3C	EBSI por el momento no soporta el modelo de datos ISO/IEC 18013-5:2021
INFO.07	Codificarse como CBOR y en formato JSON	Se codifica como JWT en JSON
INFO.08	Permitir la divulgación selectiva de atributos mediante el uso del esquema "Selective Disclosure for JWTs (SD-JWT)" y "Mobile Security Object (ISO/IEC 18013-5)" de acuerdo con el modelo de datos (Permiso de conducir en el móvil)	En el estándar W3C para JWT es posible usar '*Zero-Knowledge Proofs*', es un método criptográfico para poder demostrar que conoce un valor sin revelar el valor real de este.
INFO.09	Utilizar firmas electrónicas y formatos de cifrado tal y como se detalla en la RFC 8812 Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE) and JSON Object Signing and	EBSI usa para la firma electrónica: • JWS (obligatorio al menos soportar ES256) • JAdES (ADeS para JSON)

	Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms.	
INFO.10	Utilizar algoritmos de firma y cifrado de conformidad con la norma SOG-IS ACM (Agreed Cryptographic Mechanism) [68]	EBSI fomenta el uso de algoritmos criptográficos aprobados por SOG-IS, como mínimo requiere soporte para claves públicas y privadas de Elliptic Curve NIST P256.

Tabla 19. Requisitos de expedición del PID vs EBSI

Por tanto, los requisitos obligatorios no se cumplen en su totalidad en EBSI, Una implementación en EBSI para la expedición del PID requeriría adaptaciones en EBSI.

2. Requisitos de expedición del (Q)EAA

En el caso de un (Q)EAA el modelo correspondiente en EBSI debería ser alguno de los que existen ya diseñados específicamente para los casos de uso definidos, como por ejemplo el '*Verifiable Attestation for ID'* para el caso de uso del Diploma de un estudiante, o bien uno de los esquemas tipo de confianza: '*Accredited Verifiable Attestation'*, '*Verifiable Accreditation'* o '*Verifiable Authorisation'*. También es posible definir nuevos modelos para futuros casos de uso.

Los modelos comentados anteriormente extienden al esquema base '*Verifiable Attestation'* que extiende a su vez de la especificación W3C VC.

Y para cada requisito definido para una (Q)EAA:

Requisito	**Descripción**	**EBSI**
DEBE (OBLIGATORIO)		
CERT.01	Contener la información para identificar al emisor	Igual a lo especificado para el PID
CERT.02	Contener la información para realizar una comprobación de integridad de datos	Igual a lo especificado para el PID
CERT.03	Contener la información para verificar su autenticidad	

CERT.04	Contener la información para comprobar el estado de validez de las certificaciones	Igual a lo especificado para el PID
CERT.07	Expedirse de conformidad con una de las especificaciones del modelo de datos: la norma de codificación de permiso de conducir: l"SO/IEC 18013-5:2021", o "Verifiable Credentials Data Model v1.1" (Modelo de datos de credenciales verificables 1.1) del W3C.	Cumple uno de los dos modelos indicados, el modelo de datos credenciales VC del W3C
DEBERÍA (RECOMENDADO)		
CERT.06	Contener la información para verificar la vinculación del titular por una parte que confía	La credencial contiene el DID del Subject
CERT.08	Codificarse como uno de los siguientes formatos: CBOR o JSON según el modelo de datos utilizado para la certificación. Ver RFC 8812, RFC 8152, RFC 9052, RFC 9053	JSON
CERT.10	Permitir la Revelación Selectiva de atributos utilizando bien "Selective Disclosure for JWTs" (Revelación Selectiva para JWTs) (SD-JWT) o bien el esquema "Mobile Security Object" (Objeto de Seguridad Móvil) de la norma sobre permiso de conducir (ISO/IEC 18013-5)	Igual a lo especificado para el PID para JWT
CERT.11	Utilizar uno de los siguientes formatos de firma y cifrado según se detalla en las normas del IETF, RFC relativas a JOSE (Javascript Object Signing and Encryptio), y RFCs relativas a COSE (CBOR Object Signing and Encryption)	EBSI usa para la firma electrónica: • JWS (obligatorio al menos soportar ES256) • JAdES (ADeS para JSON)
CERT.12	Utilizar algoritmos de cifrado de conformidad con la norma SOG-IS ACM (Agreed Cryptographic Mechanism)	EBSI fomenta el uso de algoritmos criptográficos aprobados por SOG-IS, como mínimo requiere soporte para

	[68]	claves públicas y privadas de Elliptic Curve NIST P256.
CERT.13	Emitirse de acuerdo con el protocolo OpenID4VCI (OpenID for Verifiable Credential Issuance)	EBSI utiliza este protocolo para la emisión de credenciales
PUEDE (OPCIONAL)		
CERT.09	Codificarse como JSON-LD (JSON for Linking Data)	El formato de las credenciales es JWT (token web JSON) y JSON-LD (datos vinculados JSON), se especifica en el campo '*context*'

Tabla 20. Requisitos de expedición del (Q)EAA vs EBSI

Por tanto, los requisitos obligatorios se cumplen en EBSI, una implementación en EBSI para la expedición del (Q)EAA parece plausible.

A continuación, se revisarán para EBSI los requisitos específicos para los dos tipos de EUDI Wallet:

3. Requisitos de configuración de la EUDI Wallet Tipo 1:

***** Componente EUDI Wallet definido en el apartado 6.1

Requisito	*****	**Descripción / revisión EBSI**
DEBE (OBLIGATORIO)		
EUW1.01	1	Se proponen 3 componentes para almacenar y gestionar claves criptográficas: elemento seguro integrado, dispositivo externo y un servidor Aplicar medidas de seguridad para evitar la exportación de secretos criptográficos
		EBSI: Por el momento el alcance de EBSI no incluye la gestión de QES. Cada implementación de wallet debe contemplar la seguridad de las claves privadas (EBSI Security considerations: Private keys)

EUW1.02	2	soportar OpenID4VP como protocolo de intercambio de certificados para flujos remotos. Cuando se solicita autenticación pseudónima, los parámetros de solicitud DEBERÍAN especificarse de acuerdo con la especificación OpenID SIOPv2 soportar el protocolo detallado en la norma ISO/IEC 18013-5:2021 para flujos de proximidad Poder realizar una prueba de posesión Soportar la Divulgación Selectiva de atributos tal y como se especifica en la norma ISO/IEC 18013-5:2021 Soportar la Divulgación Selectiva de atributos como se especifica en la especificación SD-JWT
		EBSI: Soporta OpenID4VP y OpenID SIOPv2, no soporta la norma ISO/IEC 18013-5:2021 Es posible realizar una prueba de possession (proof of possession en openid [65]), además de también poder soportar la divulgación selectiva de atributos.
EUW1.03	3	Admitir OpenID4VCI como protocolo de emisión. (Los Estados miembros son libres de incluir alternativas adicionales al protocolo de emisión en sus soluciones nacionales)
		EBSI: Admite OpenID4VCI como protocolo de emisión
EUW1.04	4	Admitir certificados emitidos de conformidad con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021 Soportar certificados emitidos de acuerdo con el modelo de datos especificado en la especificación W3C Verifiable Credentials Data Model 1.1
		EBSI: No permite el modelo ISO/IEC 18013-5:2021
EUW1.05	6	Soportar certificados en formato JWT y SD-JWT Admitir certificados en formato CBOR
		EBSI: Soporta certificados en formato JWT. No usa formato CBOR, de todas formas, la especificación VC W3C sí lo permite [32]. Zero-Knowledge Proofs para JWT
EUW1.06	7	Soportar formatos de firma electrónica y cifrado de acuerdo con las

		especificaciones JOSE. Soportar formatos de firma y cifrado de acuerdo con las especificaciones COSE.
		EBSI: No se usa JOSE por el momento en EBSI, la especificación VC W3C sí lo permite [32] pero no nombra COSE.
EUW1.07	9	Soportar suites criptográficas y mecanismos utilizados para atributos detallados en SOG-IS Agreed Cryptographic Mechanisms Version 1.2.
		EBSI: fomenta el uso de suites criptográficas y mecanismos aprobados por SOG-IS.
DEBERÍA (RECOMENDADO)		
EUW1.08	2	Realizar comprobaciones para hacer cumplir la vinculación de sesión
		EBSI: Authorisation API para el acceso de las wallets conformadas a los servicios de EBSI, sistema de tokens con un tiempo de validez para el envío de peticiones.
PUEDE (OPCIONAL)		
EUW1.09	2	Soportar alternativas de protocolo de intercambio de certificados (Cabe destacar la API REST de mdoc, tal y como se detalla en el borrador de la norma ISO/IEC 23220-4)
EUW1.10	6	Soportar certificados en formato JSON-LD
		EBSI: El formato de las credenciales es JWT (token web JSON) y JSON-LD (datos vinculados JSON), se especifica en el campo '*context*'
NO PUEDE (PROHIBICIÓN)		
EUW1.11	7	Admitir formatos de firma y cifrado de acuerdo con las especificaciones LD-Proof.
		EBSI: Utiliza pruebas de conocimiento cero (ZKP) en JWT

Tabla 21. Requisitos de configuración de la EUDI Wallet Tipo 1 vs EBSI

Por tanto, los requisitos obligatorios no se cumplen en EBSI, una wallet conformada con EBSI en principio no podría usarse para la EUDI Wallet en los casos que se requiera una wallet de Tipo 1.

4. Requisitos de configuración de la EUDI Wallet Tipo 2:

***** Componente EUDI Wallet definido en el apartado 6.1

Requisito	*****	**Descripción**
DEBE (OBLIGATORIO)		
EUW2.01	3	Admitir OpenID4VCI como protocolo de emisión. (Los Estados miembros son libres de incluir alternativas adicionales al protocolo de emisión en sus soluciones nacionales
		EBSI: Admite OpenID4VCI como protocolo de emisión
DEBERÍA (RECOMENDADO)		
EUW2.02	1	Se proponen 3 componentes para almacenar y gestionar claves criptográficas: elemento seguro integrado, dispositivo externo y un servidor Aplicar medidas de seguridad para evitar la exportación de secretos criptográficos
		EBSI: Por el momento el alcance de EBSI no incluye la gestión de QES. Cada implementación de wallet debe contemplar la seguridad de las claves privadas (EBSI Security considerations: Private keys)
EUW2.03	4	Admitir certificados emitidos de conformidad con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021. Soportar certificados emitidos de acuerdo con el modelo de datos especificado en la especificación W3C Verifiable Credentials Data Model 1.1.
		EBSI: No permite el modelo ISO/IEC 18013-5:2021
EUW2.04	9	Soportar suites criptográficas y mecanismos utilizados para atributos detallados en SOG-IS Agreed Cryptographic Mechanisms Version 1.2.
		EBSI: fomenta el uso de suites criptográficas y mecanismos aprobados por

		SOG-IS.
PUEDE (OPCIONAL)		
EUW2.05	2	Soportar OpenID4VP como protocolo de intercambio de certificados para flujos remotos. Cuando se solicita autenticación pseudónima, los parámetros de solicitud DEBERÍAN especificarse de acuerdo con la especificación OpenID SIOPv2 Soportar el protocolo detallado en la norma ISO/IEC 18013-5:2021 para flujos de proximidad Poder realizar una prueba de posesión Soportar la Divulgación Selectiva de atributos tal y como se especifica en la norma ISO/IEC 18013-5:2021 Soportar la Divulgación Selectiva de atributos como se especifica en la especificación SD-JWT Realizar comprobaciones para hacer cumplir la vinculación de sesión Soportar alternativas de protocolo de intercambio de certificados (Cabe destacar la API REST de mdoc, tal y como se detalla en el borrador de la norma ISO/IEC 23220-4)
		EBSI: EBSI: Soporta OpenID4VP y OpenID SIOPv2, NO soporta la norma ISO/IEC 18013-5:2021 Es posible realizar una prueba de posesión (proof of possession en openid [65]), además de también poder soportar la divulgación selectiva de atributos.
EUW2.06	6	Soportar certificados en formato JWT y SD-JWT. Admitir certificados en formato CBOR
		EBSI: Soporta certificados en formato JWT. No usa formato CBOR, de todas formas, la especificación VC W3C sí lo permite [32]. Zero-Knowledge Proofs para JWT
EUW2.07	7	Soportar formatos de firma electrónica y cifrado de acuerdo con las especificaciones JOSE (JWT) Soportar formatos de firma y cifrado de acuerdo con las especificaciones COSE Admitir formatos de firma y cifrado de acuerdo con las especificaciones LD-Proof.

		EBSI: No se usa JOSE por el momento en EBSI, la especificación VC W3C sí lo permite [32] pero no nombra COSE.

Tabla 22. Requisitos de configuración de la EUDI Wallet Tipo 2 vs EBSI

Por tanto, los requisitos obligatorios si se cumplen en EBSI, una Wallet conformada con EBSI en principio podría usarse para la EUDI Wallet para las credenciales válidas para la de Tipo 2.

9.4. Resumen revisión marco de confianza en EBSI

Los conceptos y roles del marco teórico de la Identidad Digital Soberana Europea son muy similares en EBSI.

El alcance y los estados y casos de uso en la Identidad Digital Europea se encuentran en un proceso de definición inicial, no se aborda todo el sistema ni casuísticas de este. Se esperan nuevas versiones que completen lo realizado, además de las aportaciones durante la ejecución de los LSP propuestos.

Por el contrario, la arquitectura lógica y definición de flujos es más concreta en el caso de la Identidad Digital Europea. En EBSI una wallet debe cumplir unos tests de conformidad, sin especificar aspectos concretos de la arquitectura de la wallet.

En cuanto a los requisitos obligatorios que se indican para la implementación de la Identidad Digital Europea, en EBSI:

- No se cumplen en su totalidad para la expedición del PID.
- Sí se cumplen para la expedición del (Q)EAA.
- No se cumplen para la wallet Tipo 1.
- Sí se cumplen para la wallet Tipo 2.

Respecto a los protocolos y tecnologías, principalmente hay que destacar como puntos de incumplimiento que:

- Para el canal seguro de intercambios de certificaciones EBSI no soporta la norma ISO/IEC 1813-5 para flujos cercanos.
- Para los formatos de los contenedores de certificaciones EBSI no soporta ISO/IEC 18013-5:2021 con CBOR + MSO

En resumen, aunque nos encontramos en un momento inicial del proceso de regulación y definición de la Identidad Digital Europea, según el marco definido hasta hoy, EBSI sí podría ser una implementación posible para algunos de los casos que requieren menos nivel de aseguramiento, pero no es una solución válida para el PID o los certificados para los que se exija vinculación a un PID.

EBSI, además de poder evolucionar para poder ser compatible con los requisitos que se han establecido para la Identidad Digital Europea y los casos que requieran mayor nivel de aseguramiento, ya contempla soluciones de implementación óptimas y viables de algunas de las funcionalidades requeridas, tales como las listas de confianza o el uso de flujos OpenID.

10. Análisis funcional de una wallet

10.1. Selección de una solución de wallet

La Comisión Europea ha licitado [75] el desarrollo de un primer prototipo de EUDI Wallet que cumpla los requisitos especificados hasta el momento. Este se actualizará en función de los casos de uso que se desarrollarán a través de la los LSP, en el marco del Digital Europe Programme,

Será la primera implementación según los requisitos de la toolbox [1] elaborada por la Comisión Europea en colaboración con los Estados miembros. En el roadmap para la elaboración del prototipo se estima que esté finalizado en septiembre de 2023. Además, será open source y podrá ser reutilizado por los Estados miembros y otros interesados.

Los cuatro proyectos que componen los LSP se iniciaron en abril del 2023. Los proyectos se articulan a través de Consorcios que aglutinan en total más de 250 organizaciones públicas y privadas de 25 Estados miembros y Noruega, Islandia y Ucrania.

En total se implementarán 11 casos de uso:

1. Acceso a servicios de Gobierno Electrónico
2. Apertura de una Cuenta Bancaria
3. Registro para SIM móvil
4. Licencia de conducir móvil
5. Firma Electrónica Calificada Remota
6. Receta electrónica
7. Credenciales de viaje digitales
8. Identidades digitales organizacionales
9. Pagos (Cuenta a Cuenta, Basados en Tarjeta, Posiblemente basados en Token)
10. Credenciales educativas (diplomas) y calificaciones profesionales
11. Documento Portátil A1 (PDA1) y Tarjeta Sanitaria Europea (TSE)

Los cuatro consorcios y los casos de uso que implementarán las organizaciones españolas que lo componen son:

- POTENTIAL: Casos de uso: 4. Licencia de conducir móvil y 6. Receta electrónica
- NOBID: No participan organizaciones españolas.
- DC4EU: Caso de uso 10: Credenciales educativas (diplomas)

- EWC: Caso de uso 7: Credenciales de viaje digitales

Respecto a soluciones wallet conformadas en la versión v3 de EBSI y que además estén desarrolladas por organizaciones que formen parte de los Consorcios de los LSP, destacan:

- Gataca. Incluida en el consorcio DC4EU [72]:

  https://www.gataca.io/products/wallet/

- Validate ID: Incluida en el consorcio EWC [73]:

  https://www.validatedid.com/es/vidchain/vidwallet

Las dos soluciones están disponibles en la App Store y la Google Play, para IOS y Android respectivamente.

Además, las dos soluciones de wallet participaron en pilotos de EBSI presentados en el EBSI Demo Day realizado el 31 de mayo del año 2022 [74].

- Transcript of Records:

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Transcript+of+records

- Municipality Credentials:

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Municipality+Credentials

Tal como se puede ver en los pilotos de EBSI, las dos wallets son muy parecidas, disponen del mismo volumen de descargas (+ 100), el uso es muy parecido y únicamente existe alguna variación en la interfaz. Gataca simplifica las pantallas, sería necesario un estudio de usabilidad pero quizás es más sencilla para un usuario sin conocimientos avanzados de SSI, no es el caso de este estudio y selecciono VID Wallet para describir funcionalmente un caso de uso.

10.2. VID Wallet

Para el estudio funcional en primer lugar es necesario disponer de un teléfono móvil, en este caso un dispositivo con Android, e instalar la solución de wallet seleccionada desde la Google Play.

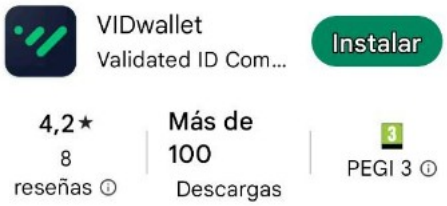
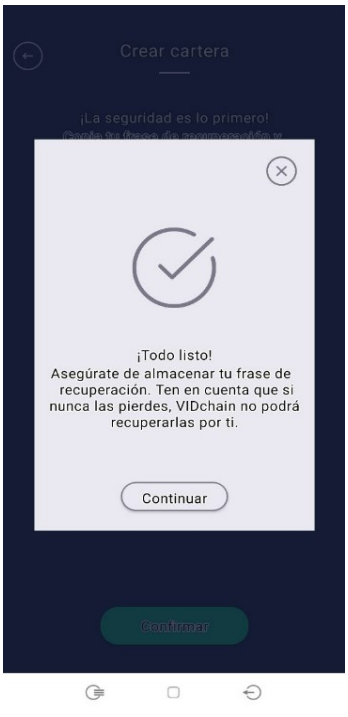


Figura 12. VID Wallet en la Google Store

Una vez instalada, se inicia una configuración muy básica en la que se informa la frase de recuperación y se solicita por razones de seguridad el tipo de desbloqueo del dispositivo al iniciar la aplicación. A continuación, se indican unas pantallas informativas de inicio y finalmente ya es posible acceder al entorno de VID Wallet, que se compone de 5 pantallas principales:

- Credenciales: Se crean y visualizan las credenciales del usuario.
- Selector de identificador: DID's del usuario, es posible crear DID's de distinto tipo: Ethereum, DID KEY, DID JWK, EBSI y Alastria.
- Escanear código QR: Código de entrada QR para validar DID's y credenciales desde sitios externos al dispositivo móvil.
- Mensajes: Intercambio de mensajes del usuario con los Issuers y Verifiers.
- Configuración: Datos generales de configuración de la aplicación móvil



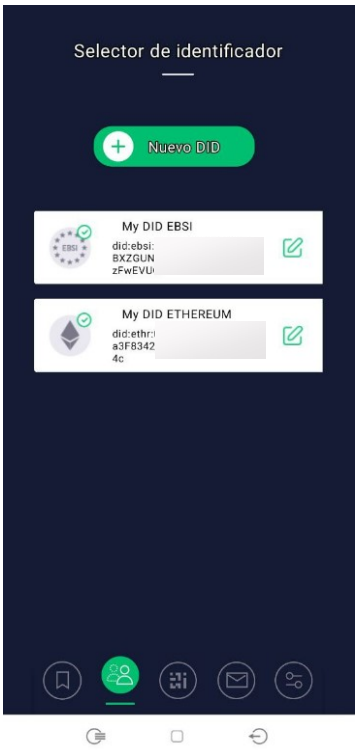

Elige cómo desbloquear tu cartera
Usa tus datos biométricos
Usa contraseña


¡Enhorabuena
ya tienes tu cartera de identidad!


Tu identidad, siempre protegida
VIDchain es un servicio diseñado para ayudarte a recuperar el control sobre tu identidad digital.


Controla cómo compartes tus datos
Comparte y descarga credenciales digitales de forma segura y privada.


Credenciales
Nueva credencial
Tienes 0 credenciales
Todos mis dids
Visita la demo de VIDchain para ver cómo funciona. 🔥
https://try.vidchain.net/demo


Selector de identificador
Nuevo DID
My DID EBSI
My DID ETHEREUM

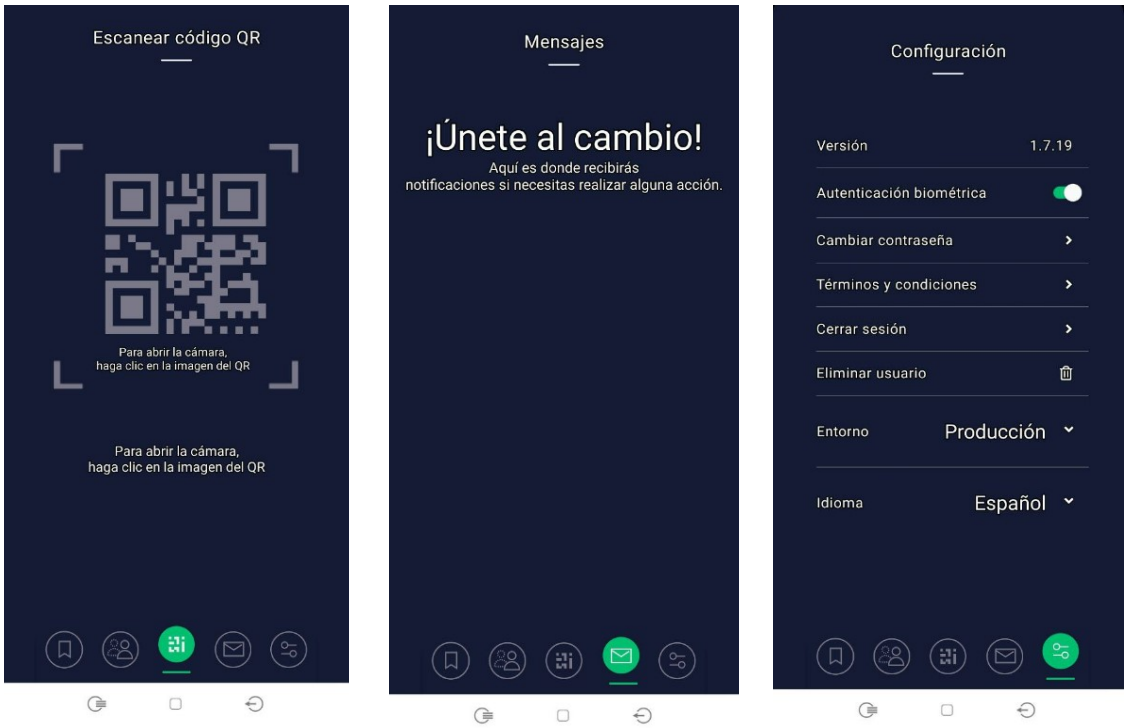


Figura 13: Configuración VID Wallet

10.3. Caso de uso VID Wallet

A continuación, para entender el funcionamiento de una wallet, explicaré un caso de uso.

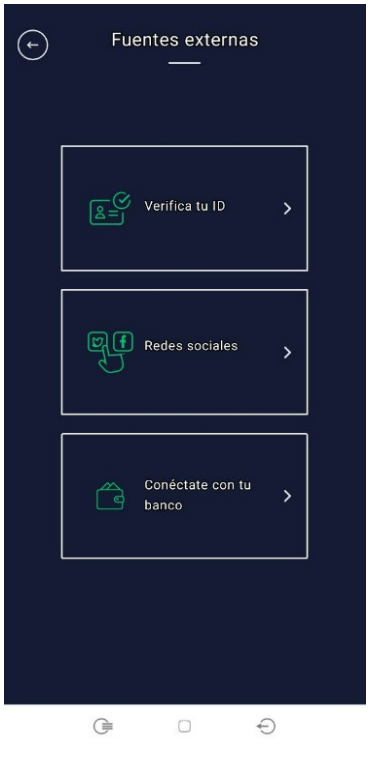
En primer lugar, voy a crear una credencial verificable que nos permita identificarnos para la ejecución del caso de uso. Si extrapoláramos a la EUDI Wallet el identificador podría tratarse del PID y el proveedor sería el Estado miembro de tu nacionalidad.

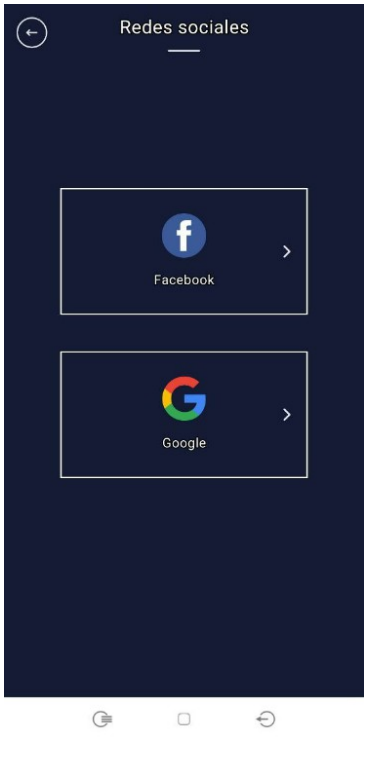
Para este ejemplo voy a crear una credencial verificable a partir de mi perfil en Google.

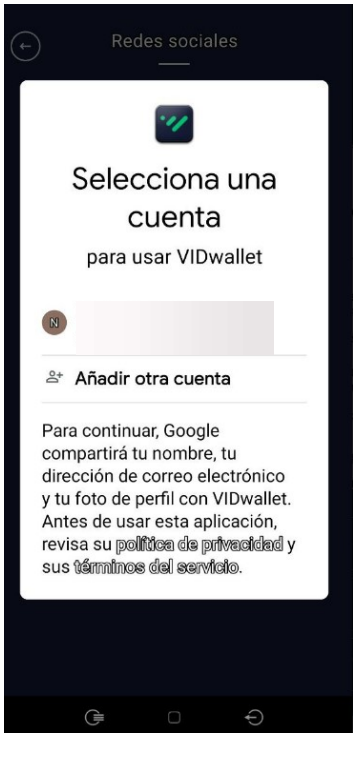

Credenciales
Nueva credencial
Tienes 0 credenciales
Todos mis dids
Visita la demo de VIDchain para ver cómo funciona. 🔥
https://try.vidchain.net/demo


Nueva credencial
Elige un DID para esta operación
My DID EBSI
My DID ETHEREUM


Nueva credencial
Conecta tu número de teléfono
Conecta tu Email
Conectar con fuentes externas


Fuentes externas
Verifica tu ID
Redes sociales
Conéctate con tu banco


Redes sociales
Facebook
Google


Redes sociales
Selecciona una cuenta
para usar VIDwallet
Añadir otra cuenta
Para continuar, Google compartirá tu nombre, tu dirección de correo electrónico y tu foto de perfil con VIDwallet. Antes de usar esta aplicación, revisa su política de privacidad y sus términos del servicio.

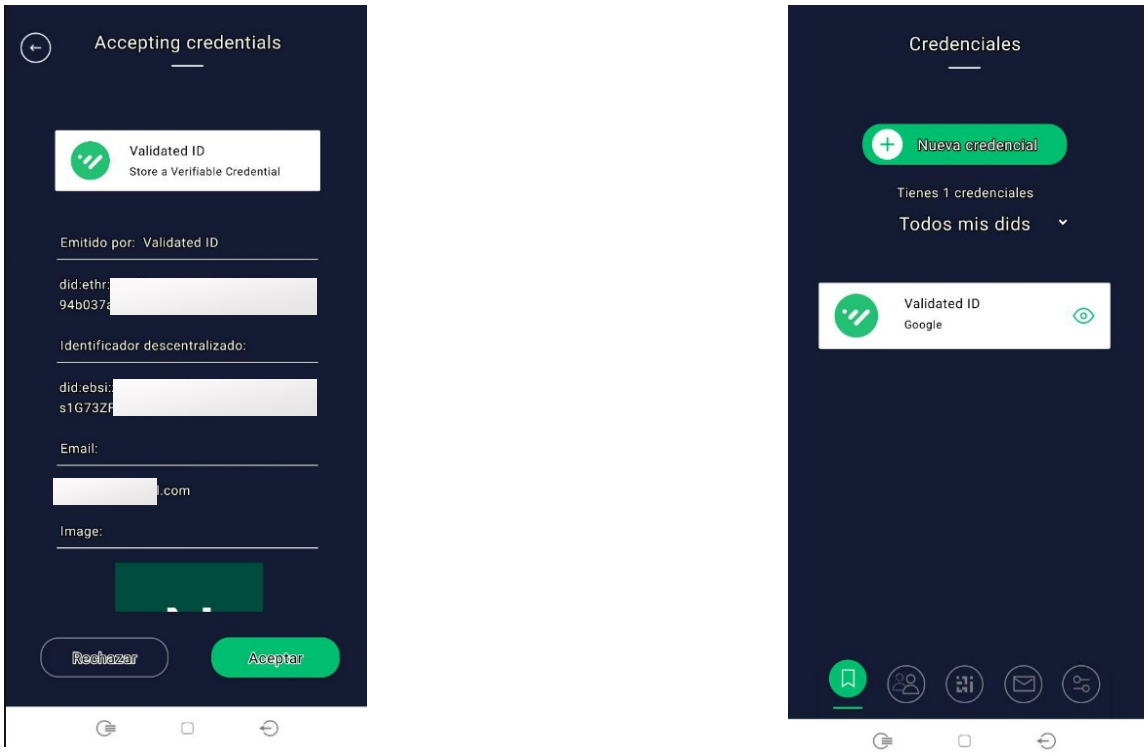


Figura 14: Creación una credencial en VID Wallet

Una vez creada la credencial verificable, esta nos permitirá identificarnos, y autenticarnos en sitios de Internet que a su vez nos ofrecen otros servicios, tales como nuevas credenciales.

En este caso de uso accederé a una web denominada Freedonia, que ofrece varios servicios a sus miembros a los que denomina ciudadanos. En primer lugar, me identificaré en la página principal a través de la wallet, mediante el siguiente flujo:

1. Acceso desde un PC a la página web de Freedonia

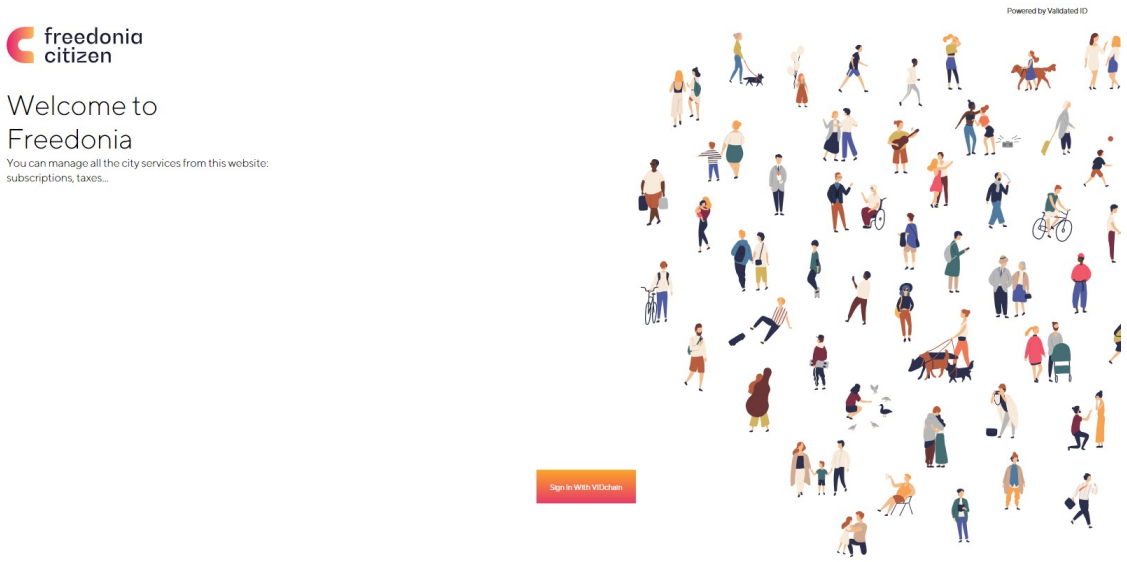


Figura 15. Página de inicio de Freedonia
https://try.vidchain.net/demo/government

2. Pulsando el botón 'Sig in with VIDchain' solicito la identificación. Se informa de que es necesario: el DID y una credencial verificable tipo Id Credential.

Figura 16. Página de autenticación SSI Freedonia

3. A continuación, desde mi app de VID Wallet:
    - Escaneo el código desde la ventana de 'Escanea código QR'
    - VID Wallet solicita mi permiso para aceptar compartir la credencial (Id Credential de Google) con el Verifier (Freedonia).

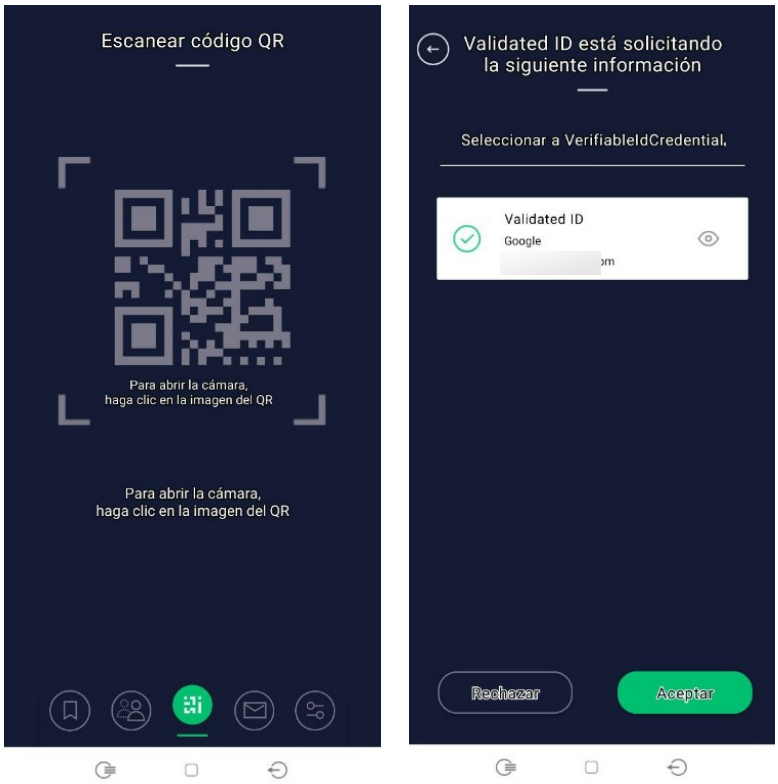


Figura 17. Proceso autenticación con VID Wallet

4. Accedo al contenido de Freedonia

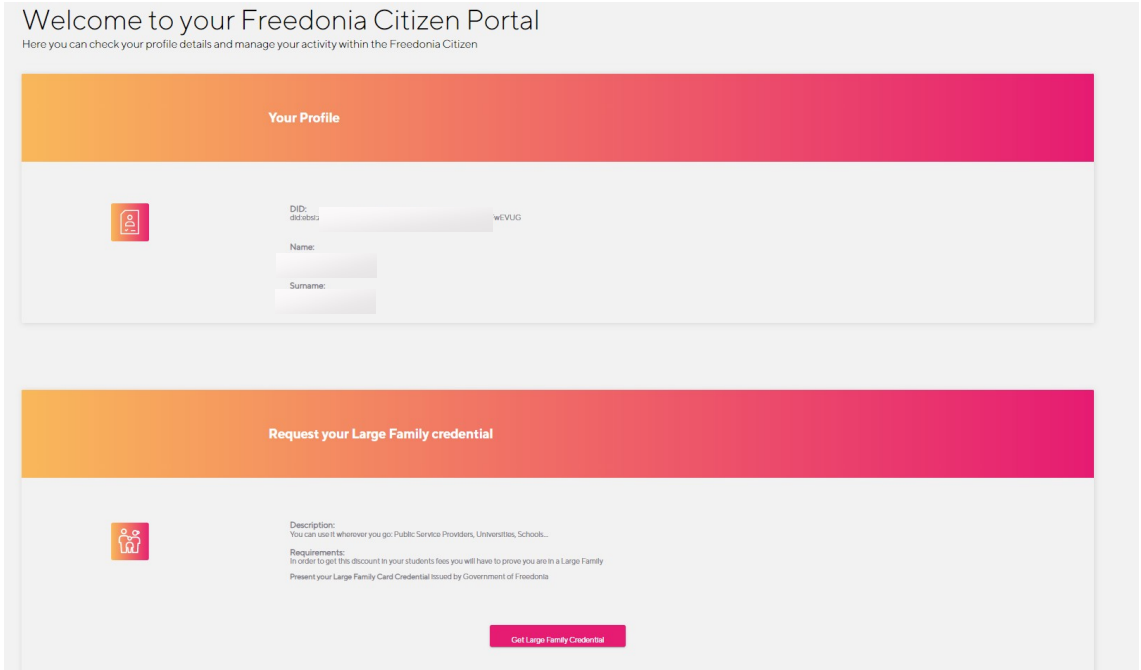


Figura 18. Página Freedonia con autenticación

5. Freedonia me ofrece la posibilidad de solicitar la ‘Large Family credential’, esta credencial se puede almacenar en la wallet y permitirá obtener descuentos por ser familia numerosa. Pulso el botón ‘Get Large Family Credential’ y desde mi VID Wallet:
    - Se solicita mi permiso para aceptar la nueva credencial (tipo Verifiable Credential) de Freedonia.
    - Puedo ver la nueva credencial en la ventana ‘Credenciales’ y ver el detalle de esta.

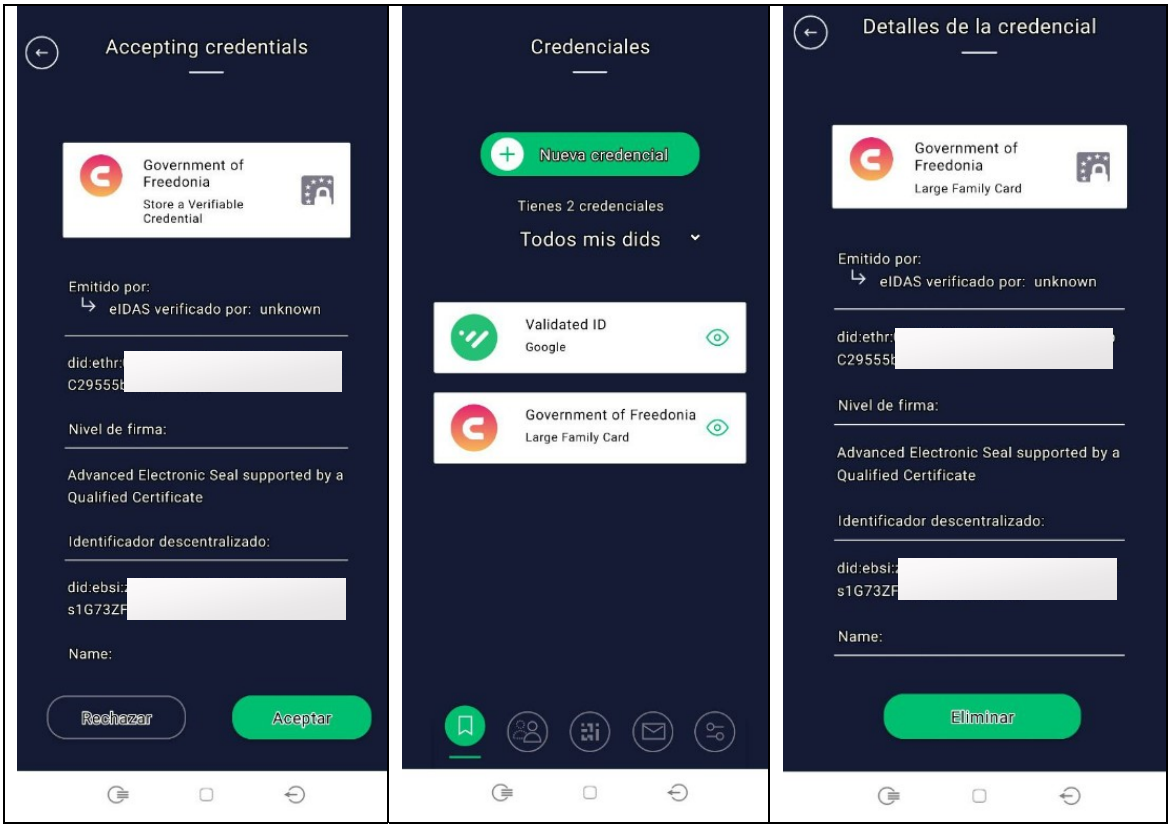


Figura 19. Petición credencial que ofrece Freedonia

10.4. Conclusiones del funcionamiento de una EBSI Wallet

Para un usuario sin participación o acceso a sistemas privados de SSI o pilotos existentes, la primera conclusión es que es muy difícil actualmente poder acceder a un caso real de uso de una wallet SSI.

Por el momento, después de probar wallets reales y ver distintos pilotos de casos de uso y páginas de prueba preparadas por cada wallet, considero que es una mejora sustancial en el control de tus datos. Se evitan múltiples registros en distintos sitios de Internet y permite, además de identificarte, poder probar, a través de distintos tipos de credenciales, títulos de educación y aspectos tales como ser familia numerosa, mayor de edad, etc.

Como contras, aunque el uso puede considerarse bastante fácil y asequible para la mayoría de la población, es necesario:

- Disponer de un dispositivo móvil
- Pedagogía para que la mayoría de la población entienda qué es y cómo se usa. Hoy en día parte de la ciudadanía no entiende conceptos tales como certificado digital, firma digital e implementaciones específicas como el eDNI y Cl@ve. Es necesario un esfuerzo y cambio de estrategia en la difusión y formación de la EUDI Wallet.

11. Conclusiones y líneas de trabajo futuras

11.1. Conclusiones

En este trabajo, que reúne información que se encuentra dispersa y en su mayoría en inglés, se han explicado los conceptos e ideas que se consideran pueden ayudar a entender el cambio de paradigma de los nuevos servicios de confianza en la Unión Europea, y específicamente se ha profundizado en la implantación de la nueva Identidad Digital Europea.

El estudio realizado se ha enfocado como una revisión del planteamiento de cambio propuesto en la Unión Europea y el proceso actual en el que se encuentra, intentando realizar comparativas con conceptos, estándares y soluciones existentes, lo que permite visualizar el futuro que nos espera en un horizonte aproximado de cinco años.

Además, se obtienen las siguientes conclusiones:

- Existe un movimiento de cambio de paradigma de la gestión de las identidades a nivel mundial, centrada en el concepto de identidad soberana. La Unión Europea está encabezando, mediante la identidad Digital Europea, un marco de confianza que puede dotar a este nuevo paradigma del impulso necesario para la implantación masiva en sus Estados miembros.

- El pilar del marco de confianza es el marco legal y la regulación que va a sustentar la Identidad Digital Europea. Para que la implantación sea masiva, además del nuevo reglamento eIDAS, son muy importantes otras iniciativas tales como la obligación regulatoria en grandes plataformas tecnológicas, que permita a los ciudadanos identificarse y autenticarse sin la dependencia actual de compartir sus datos.

- En cuanto a los estándares y tecnologías que compondrán la nueva Identidad Digital Europea, estamos en una fase temprana, con la publicación de la primera versión de la arquitectura y estándares de la EUDI Wallet por parte de la Comisión Europea. De esta primera versión se concluye que:
    - Faltan temas importantes por definir.
    - Los estándares y tecnologías seleccionados por el momento ya existen, son reconocidos a nivel mundial, lo que parece indicar un planteamiento de interoperabilidad fuera de la Unión Europea.
    - Hace falta una estandarización por parte de organismos europeos, actualmente se está en proceso de elaboración.
    - Se esperan a futuro nuevas versiones, en especial en función de la implementación real que se realizará con los LSP y las aportaciones de los Estados Miembros.
- Se están realizando en paralelo varias tareas tales como: la regulación, la definición de la arquitectura y las tecnologías, la estandarización y los prototipos de

implementación mediante los LSP. Esto es debido a la necesidad de acelerar la implantación de la Identidad Digital Europea, se pretende llegar al 80% de la población en 2030.

- Hay que destacar que, aunque la tecnología blockchain está muy presente en los movimientos mundiales de descentralización y SSI, además de ser la tecnología base de muchas soluciones existentes de identidad digital soberana, el marco de confianza establecido hasta el momento por la Unión Europea no hace referencia directa a esta tecnología.

11.2. Líneas de trabajo futuras

La principal línea de trabajo futura es seguir con el estudio iniciado y realizar un análisis de los trabajos pendientes de su publicación, tales como:

- Nueva versión del Reglamento eIDAS
- Ampliaciones y revisiones de la arquitectura, estándares y tecnologías de la EUDI Wallet.
- Resultados de los LSP.
- Prototipo de EUDI Wallet que se espera en septiembre de 2023: funcionamiento e implementación open source.
- Avance en los distintos Estados miembros en cuanto a nueva regulación propia y desarrollos específicos.
- Seguimiento estrategia respecto a la regulación de los libros de registro electrónico como servicio de confianza en la Unión Europea.

Además, otras líneas de estudio relacionadas que se proponen son:

- Uso de tecnología blockchain en la EUDI Wallet, casos particulares de implementación en los Estados miembros.
- Adaptaciones de EBSI relacionadas con la EUDI Wallet.
- Estrategias de implantación en cada Estado miembro, comparativas y casos de éxito.
- Estudios de nuevos casos de uso además de la identidad digital soberana y los propuestos en los LSP.

Finalmente, quiero mencionar que una línea interesante de estudio podrían ser las interrelaciones que puedan surgir entre la EUDI Wallet y la wallet para el Euro Digital.

12. Glosario

Definición de los términos y acrónimos más relevantes utilizados en la Memoria.

AAPP	Administraciones públicas
AC	Autoridad certificadora
AR	Autoridad de Registro
Blockchain	Tecnología de cadena de bloques
CAB	Organismos de evaluación de conformidad
CBOR	Concise Binary Object Representation
CEN	European Committee for Standardization
COSE	Object Signing and Encryption
DID	Identificador descentralizado
DIDComm	Decentralized identity communication
DLT	Distributed Ledger Technology
DNI	Documento Nacional de Identidad
EA	European Accreditation
EBP	European Blockchain Partnership
EDIFB	Consejo Europeo del Marco de Identidad Digital
eID	Identificador digital
eIDAS	electronic IDentification, Authentication and trust Services
ENAC	Organismo Nacional de Acreditación
ETSI	The European Telecommunications Standards Institute
EUDI Wallet	European Digital Identity Wallet
FNMT-RC	Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
JSON-LD	JSON for Linking Data

LD-Proof	Linked Data Proofs
LoA	Levels of assurance
LSP	Large Scale Pilots
mDL	Mobile driving license
Merkle-tree	Estructura de valores en forma de árbol con criptografía hash
MSO	Mobile Security Object
NFC	Near field communication
NIS2	Directiva (UE) 2022/2555
ODS	Objetivos de Desarrollo Sostenible
OpenID	estándar de identificación digital descentralizado
OpenID4VCI	OpenID para emisión de credenciales verificables
PKI	Public key infraestructura, infraestructura de clave pública.
QR	Quick response (QR) codes
red eIDAS	Red a la que están conectadas los sistemas de cada país y permite a los ciudadanos realizar transacciones interfronterizas
eIDAS	Reglamento (UE) n.º 910/2014
SD-JWT	Selective Disclosure for JWT
SEMIC	Comunidad de Interoperabilidad Semántica (UE)
SIOPv2	Self-Issued OpenID Provider v2
SLA	Service Level Agreement (Acuerdo de Nivel de Servicio)
SOG-IS ACM	Agreed Cryptographic Mechanism
SSI	Self-sovereign identity o identidad soberana
UE	Unión Europea
VC	Verificable credentials
W3C	World Wide Web Consortium
WTC	Wallet Conformance Test EBSI

13. Referencias

[1] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Famework. The European Digital Identity Wallet Architecture and Reference Framework. January 2023. Version 1.0.0
https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[2] European Digital Identity Architecture and Reference Framework. Outline. 22 February 2022
https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

[3] eIDAS Architecture Reference Framework 1.0 –comments and first analysis. Epicenter.works.12 February 2023. Thomas Lohninger and Kai Wagner
https://en.epicenter.works/documents

[4] EUROPEAN COMMISSION RECOMMENDATION of 3.6.2021, on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework

[5] Digital Identity. Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust. ENISA. January 2022

[6] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014
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
https://www.boe.es/doue/2014/257/L00073-00114.pdf

[7] Propuesta del REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea
Bruselas, 3.6.2021, COM(2021) 281 final , 2021/0136 (COD)

[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity
7 February 2023

[9] [22] Christopher Allen, artículos:
First version the Path to Self-Sovereign Identity, Apr 26, 2016
Self-Sovereign Identity Principles 1.0, Oct 23, 2016
Characteristics-of-sovereign-identity, 2018
lifeID Self-Sovereign Identity Bill of Rights, 2018
https://github.com/WebOfTrustInfo/self-sovereign-identity

[10] eIDAS Interoperability and Cross-Border Compliance Issues
Marko Hölbl, Boštjan Kežmah and Marko Kompara
Faculty of Electrical Engineering and Computer Science, University of Maribor, 2000 Maribor, Slovenia

[11] Portal DNIe
https://www.dnielectronico.es/PortalDNIe/

[12] Lista de confianza de prestadores cualificados de servicios electrónicos de confianza
https://sede.serviciosmin.gob.es/prestadores/paginas/inicio.aspx

[13] Principios SSI. Sovrin
https://sovrin.org/principles-of-ssi

[14] Johnston's law
https://www.johnstonslaw.org/

[15] The General Theory of Decentralized Applications,
Dappshttps://github.com/DavidJohnstonCEO/DecentralizedApplications

[16] Self-sovereign identity : decentralized digital identity and verifiable credentials / Alex Preukschat, Drummond Reed ; foreword by Doc Searls.
Preukschat, Alex, author.; Reed, Drummond, author.; Searls, Doc, writer of foreword.
2021 Biblioteca UOC

[17] Principios Open Source
https://opensource.com/open-source-way

[18] Manifiesto Satoshi Nakamoto
https://bitcoin.org/bitcoin.pdf

[19] Cameron, Kim. 2005. “The Laws of Identity.” Kim Cameron’s Identity Weblog.
https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[20] ACCELERATE ADOPTION OF DIGITAL IDENTITIES ON MOBILE DEVICES. Indetity Management. March 2023. NIST
https://csrc.nist.gov/publications/detail/white-paper/2023/03/15/accelerate-adoption-of-digital-identities-on-mobile-devices/draft

[21] Open Letter for the preservation of the Electronic Ledger’s provisions in eIDAS 2
https://inatba.org/news/savesection11-eidas2-trusted-electronic-ledgers-open-letter/

[22] Especificación W3C DID
https://www.w3.org/TR/did-core/

[23] Trust Over IP Stack SSI infraestructure. TRUST Over IP Foundation
https://trustoverip.org/toip-model/

[24] Communication: Shaping Europe’s digital future’. 19 february 2020
https://commission.europa.eu/publications/communication-shaping-europes-digital-future_en

[26] Commission proposes a trusted and secure Digital Identity for all Europeans
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[27] eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI
Steffen Schwalm1, Daria Albrecht2, Ignacio Alamillo

[28] DIGITAL IDENTITY Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust ENISA enero 2022.

[29] referencia OpenID4VP
https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[30] referencia OpenID SIOPv2: Self-Issued OpenID Provider v2
https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

[31] ISO/IEC 1813-5:2021 vs W3C VC
https://collateral-library-production.s3.amazonaws.com/uploads/asset_file/attachment/36416/CS676613_-_Digital_Credentials_promotion_campaign-White_Paper_R3.pdf

[32] Especificación W3C VC
https://www.w3.org/TR/vc-data-model/

[33] RFC 2119 Palabras clave a utilizar en RFC para Indicar Niveles de Requerimiento
https://www.rfc-es.org/rfc/rfc2119-es.txt

[34] Página web Comisión Europea Identidad Digital
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en#key-principles

[35] OpenID especificaciones
https://openid.net/developers/specs/

[36] W3C Credentials Community Group
https://w3c-ccg.github.io

[37] Página de referencia de CBOR
https://cbor.io/

[38] RFC 8949
https://www.rfc-editor.org/rfc/rfc8949

[39] RFC 8812
CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms
https://www.rfc-editor.org/rfc/rfc8812.html]

[40] COSE RFC 8152
https://www.rfc-editor.org/rfc/rfc8152

[41] Ministerio del Interior, página web con información de validez del DNI en otros países https://www.interior.gob.es/opencms/en/servicios-al-ciudadano/tramites-y-gestiones/dni/paises-a-los-que-puede-viajar-con-su-dni-en-vigor/index.html

[42] Chapter 1 EBSI Verifiable Credentials explained. EBSI Verifiable credentials. June 2002 - European Commission, ebsi https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained

[43] Chapter 2 EBSI Verifiable Credentials explained. EBSI Verifiable credentials in action. June 2002 - European Commission, ebsi https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained

[44] Chapter 3 EBSI Verifiable Credentials explained. EBSI DIDs June 2002 - European Commission, ebsi https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained

[45] Chapter 4 EBSI Verifiable Credentials explained. EBSI digital identity. June 2002 - European Commission, ebsi https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained

[46] Chapter 5 EBSI Verifiable Credentials explained. Issuers trust model. June 2002 - European Commission, ebsi https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained

[47] Chapter 6 EBSI Verifiable Credentials explained. Open ID Connect for Verifiable Credentials. June 2002 - European Commission, ebsi https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained

[48] Página web principal EBSI https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

[49] Hyperledger foundation web https://www.hyperledger.org/

[50] Hyperledger fabric documentation https://hyperledger-fabric.readthedocs.io/en/latest/

[51] Hyperledger Besu https://besu.hyperledger.org/en/stable/

[52] ETSI Página web, buscador de estándares
https://www.etsi.org/standards/get-standards#Pre-defined%20Collections

[53] Reglamento (CE) nº 765/2008
https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-81669

[54] UNE-EN ISO/IEC 17065
https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?Tipo=N&c=N0050466

[55] EA -DIRECTORY OF EA MEMBERS AND MLA SIGNATORIES
https://european-accreditation.org/ea-members/directory-of-ea-members-and-mla-signatories/

[56] ETSI- Details of 'DTS/ESI-0019462' Work Item
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63566

[57] ETSI- Details of 'DTS/ESI-0019471' Work Item
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63664

[58] ETSI- Details of 'DTS/ESI-0019472' Work Item
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63560

[59] Creación EBP Comisión Europea
https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership

[60] Accelerating best use of technologies (DIGITAL-2022-DEPLOY-02)- Comisión Europea
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-deploy-02-ebsi-services

[61] EBSI's Node Operators
https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Node+Operators

[62] EBSI Architecture, explained, CEF Digital Connecting Europe Final draft 10/06/2021
https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/447687044/%28210610%29%28EBSI_Architecture_Explained%29%28v1.02%29.pdf

[63] APIs EBSI
https://api-pilot.ebsi.eu/docs/apis

[64] DECISIÓN DE EJECUCIÓN (UE) 2015/1505 DE LA COMISIÓN
de 8 de septiembre de 2015
https://www.boe.es/doue/2015/235/L00026-00036.pdf

[65] OpenID for Verifiable Credential Issuance
https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-10.html

[66] SEMIC Support Center
https://joinup.ec.europa.eu/collection/semic-support-centre

[67] Directiva NIS2
https://www.boe.es/doue/2022/333/L00080-00152.pdf

[68] SOG-IS ACM https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[69] Diccionario de la lengua española de la Real Academia Española https://www.rae.es/

[70] Appendix A: Reference architecture comparison: functions of standards in knowledgeintensive industries
https://www3.weforum.org/docs/WEF_AppendixA_Reference_architecture_comparison.pdf

[71] Naciones Unidas Objetivos de desarrollo sostenible
https://www.un.org/sustainabledevelopment/es/development-agenda/

[72] Consorcio DC4EU
https://www.dc4eu.eu/consortium/

[73] Consorcio EWC
https://eudiwalletconsortium.org/

[74] EBSI Demo Day
https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Demo+Day

[75] Belgium-Brussels: Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet
https://ted.europa.eu/udl?uri=TED:NOTICE:668669-2022:TEXT:EN:HTML&tabId=1