Validated ID

Always be yourself

La historia de la identidad auto soberana

Introducción

Iván Basart, CTO de Validated ID

La historia del concepto de la identidad auto soberana (Self-Sovereign Identity, SSI por sus siglas en inglés) es relativamente corta. Al principio, la identidad descentralizada era un tema que preocupaba únicamente a profesionales muy especializados.

Este grupo estaba preocupado por los problemas de privacidad relacionados con las identidades digitales centralizadas. Este temor dio lugar a formas de gestión de la identidad basadas en la criptografía.

El interés por este fenómeno creció más allá de esta comunidad, porque coincidió con un aumento de las violaciones de datos, que expusieron los datos de millones de personas a hackers que los habían robado de grandes empresas como Yahoo, Equifax, eBay, Uber y otras.

Más tarde, llegó la tecnología blockchain con su capacidad de crear sistemas resistentes al fraude y más seguros que los creados por humanos. Esto llevó al impulso de la descentralización de la identidad.

La preocupación pública por la privacidad y la seguridad alcanzó tal nivel que los gobiernos comenzaron a regular este ámbito con leyes como el Reglamento General de Protección de Datos (RGPD) en Europa o la Ley de Privacidad del Consumidor de California (CCPA).

A pesar de que la identidad auto soberana ha sido un paradigma que en sus inicios ha estado muy alejado de los entes reguladores finalmente se ha convertido en la base de la nueva regulación de identidad en Europa (eIDAS 2.0).
En esta sección vamos a revisar la evolución del mundo de la identidad en los últimos años para entender el momento actual.

Las siete leyes de la identidad

Uno de los primeros hitos en la conceptualización de la identidad digital fueron **Las siete leyes de identidad**[1], escritas en 2005 por Kim Cameron, entonces arquitecto de sistemas en Microsoft.

Kim era un gurú sobre este tema y, lamentablemente, falleció hace unos meses. Siempre se le ha considerado una de las figuras clave en la evolución de la identidad descentralizada. La teoría de las leyes de identidad describe cómo debe ser un modelo de identidad moderno, flexible y seguro. Son las siguientes:

1. **Control y consentimiento del usuario:** los sistemas de identidad digital deben revelar información identificando a un usuario sólo con su consentimiento.
2. **Acceso limitado, para uso limitado:** la solución que muestre la menor información posible y que mejor limite su uso es la más estable en el largo plazo.
3. **La ley de las mínimas partes** (The Law of Fewest Parties): los sistemas de identidad digital deben diseñarse de manera que la divulgación de la información se limite a las partes que tienen una relación de identidad necesaria y justificable.
4. **La ley de la identidad dirigida (Directed Identity):** un metasistema universal de identidad debe soportar identificadores omnidireccionales para el uso de entidades públicas e identificadores unidireccionales para entidades privadas. Facilitando así el descubrimiento, pero previniendo el "lanzamiento" innecesario de correlación.
5. **Pluralismo de operadores y tecnologías:** un sistema universal (o metasistema) debe canalizar y permitir la interacción de múltiples tecnologías y múltiples proveedores de identidad.
6. **Integración humana:** el nuevo sistema de identidad debe cambiar profundamente la experiencia del usuario humano para que sea lo suficientemente predecible e inequívoca como para permitirle tomar decisiones informadas.
7. **Experiencia consistente en diferentes contextos:** un metasistema unificado debe proveer una experiencia de uso simple y consistente al mismo tiempo que permite la separación de contextos a través de múltiples operadores y tecnologías.

[1] https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Hubo varias iniciativas de crear un modelo de identidad en internet en ese momento. La más relevante fue OpenID, que conocemos como los modelos de "Login con Facebook y Google" que tenemos hoy en día. Estos modelos tienen varios fallos: por un lado, la falta de privacidad y, por otro, la falta de verificación de identidad que afectan tanto a los usuarios como a las empresas.

Al mismo tiempo, se desarrolló el modelo oficial según el reglamenteo eIDAS y basado en certificados digitales. Al contrario del modelo anterior, este modelo cuenta con un nivel elevado de seguridad y privacidad, pero con un uso prácticamente residual por parte de la mayoría de los ciudadanos debido a la gran complejidad de uso.

Los principios de la identidad auto soberana

Es fundamental dar crédito a los pioneros del concepto de identidad auto-soberana o descentralizada y mencionar que este término ya fue conceptualizado en 2011 por Devon Leffretto y utilizado en la lista VRM.

Posteriormente, la explosión de la tecnología Blockchain generaría un fuerte impacto en el sector de la identidad digital y este concepto sería retomado por Christopher Allen, en 2016, en su artículo **The Road to Self Sovereign Identity**[2]. En este artículo, Christopher Allen explica los principios que deben guiar cualquier identidad auto-soberana:

1. **Existencia:** el usuario debe tener una existencia independiente. Toda identidad auto soberana está basada, en última instancia, en el concepto del "yo" en el corazón de la identidad, que, inevitablemente, nunca podrá existir como tal en formato digital. La identidad auto soberana simplemente hace pública y accesible algunos aspectos del "yo" que ya existe.
2. **Control:** el usuario debe controlar su identidad. A pesar de que la identidad del usuario está sometida al tratamiento por parte algoritmos que la validan, el usuario debe ser la máxima autoridad de su propia identidad. Siempre deberá poder consultarla, actualizarla o, incluso, esconderla.
3. **Acceso:** el usuario debe poder acceder a sus propios datos. No puede haber datos ocultos o información inaccesible para el dueño de la identidad. Sin embargo, esto no implica que el usuario pueda cambiar todos los aspectos y declaraciones asociadas a su identidad. Para proteger la soberanía de los demás usuarios, un individuo sólo debe tener acceso a su propia identidad y no a las de los demás.
4. **Transparencia:** los algoritmos y los sistemas deben ser transparentes. Los sistemas que administran y operan la red de identidades deben ser abiertos, tanto sobre su funcionamiento como en su gestión. Los algoritmos deben ser libres, open-source, independientes de la arquitectura y accesibles para su consulta.
5. **Persistencia:** las identidades deben ser longevas. A ser posible, deberían durar para siempre o, como mínimo, hasta cuando el usuario quiera. Esto no puede contradecir el "derecho al olvido": el usuario debe poder eliminar una identidad si así lo desea. Para ello, se necesita una fuerte separación entre una identidad y sus partes.

6. **Portabilidad:** la información y los servicios relacionados con la identidad deben ser fácilmente transportables. Según Allen, la información y los servicios deben ser fácilmente transportables y no pueden estar en manos exclusivas de una tercera entidad centralizada. Aunque la tercera entidad trabaje en beneficio del usuario, el problema del punto de fallo único (Single Point Of Failure, SPOF por sus siglas en inglés) sigue existiendo. La portabilidad garantiza que la identidad de un usuario puede ser transferida y almacenada en múltiples lugares, a su propia discreción.

7. **Interoperabilidad:** la identidad puede utilizarse de la forma más amplia posible. Las identidades tienen poco valor si solo funcionan en entornos nicho. Por tanto, el objetivo de crear un sistema de identidad digital es que la información esté disponible en todo el mundo, sin que el usuario pierda el control de su identidad.

8. **Consentimiento:** el usuario debe consentir el uso de su identidad. Para compartir datos de la identidad de una persona es crucial contar con el consentimiento del usuario. Aunque otros usuarios, como la empresa en la que trabaja, el seguro médico o un amigo pueden presentar datos, el usuario siempre tiene que dar el consentimiento para que estos datos sean válidos.

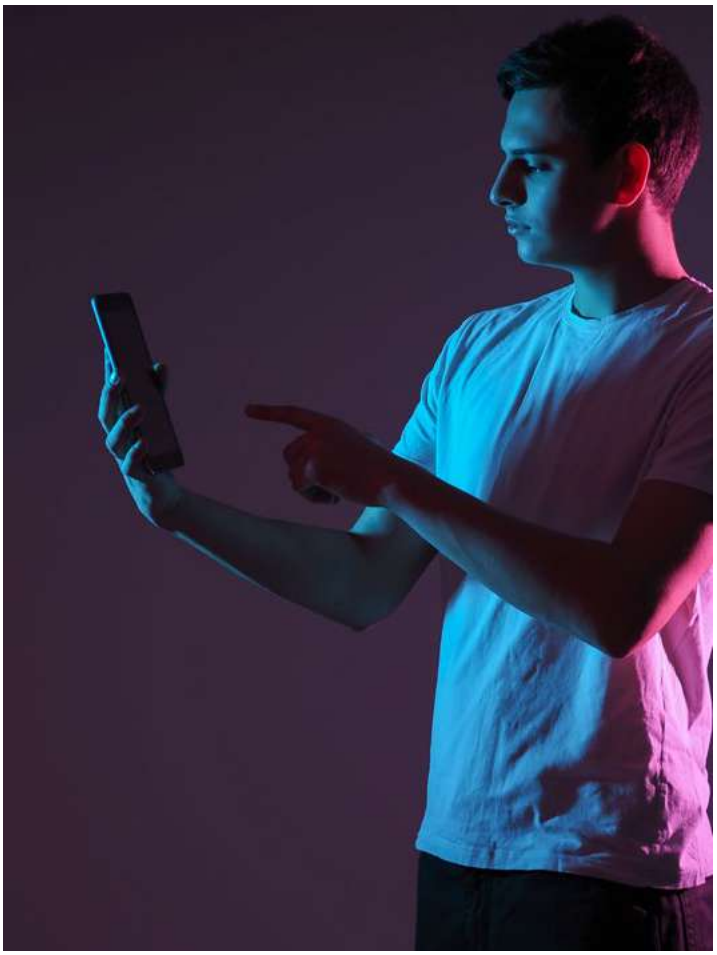
9. **Minimización:** la divulgación de los datos propios debe ser mínima. Cuando se comparten datos de un usuario, la divulgación de la información debe incluir la menor cantidad posible de información para poder llevar a cabo la transacción. Por ejemplo, si se requiere la edad mínima de un usuario para una transacción, no se puede exigir que proporcione la fecha exacta de su nacimiento, sino simplemente que cumple la condición. Según Allen, mediante la aplicación de la divulgación selectiva, las pruebas de alcance y otras técnicas de conocimiento cero, los desarrolladores pueden facilitar la minimización para apoyar mejor la privacidad. Fundamentalmente, la minimización activa permite una mayor protección de la privacidad en las interacciones entre usuarios y sistemas.

10. **Protección:** los derechos de los usuarios deben ser respetados. Allen afirma que, cuando hay un conflicto entre las necesidades de la red de identidad y los derechos de los usuarios, la red debe errar en favor de preservar las libertades y derechos de las personas. Para garantizar esto, la autenticación de la identidad debe ocurrir a través de algoritmos independientes, resistentes a la censura y ejecutados de forma descentralizada.

[2] http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Pretty good privacy

En 1991, el programa Pretty Good Privacy (PGP) de Phil Zimmermann fue una de las primeras implementaciones de un esquema de cifrado basado en clave pública. Christopher Allen fue uno de sus grandes impulsores.



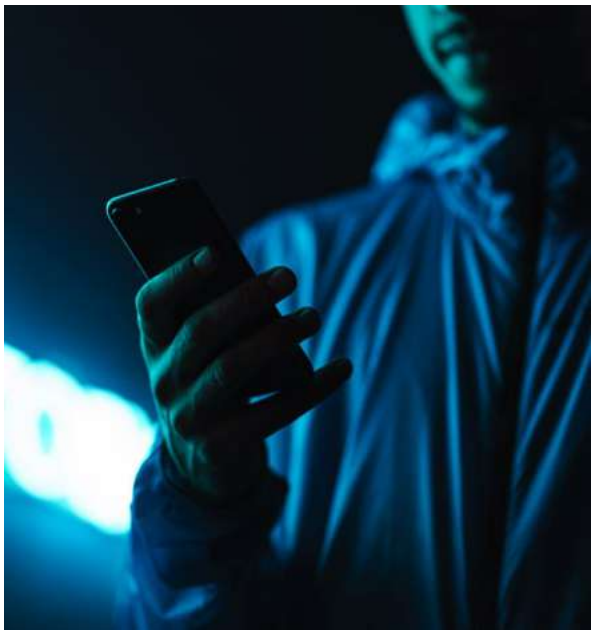
Para enviar mensajes cifrados, el PGP requiere que los usuarios intercambien claves criptográficas antes de comunicarse. En el PGP, este intercambio de claves se realiza a través de una red de confianza: cada usuario distribuye su clave pública a sus amigos y asociados, que, a su vez, distribuyen sus propias claves públicas a sus amigos y asociados y así sucesivamente. Este proceso eliminaba la necesidad de un tercero para el intercambio de la información.

Este proceso construye gradualmente una red de confianza que puede utilizarse para distribuir claves de forma segura. Cuantas más personas firmen la clave de una persona, mayor será la probabilidad de que la clave sea segura. Este concepto es el de Web Of Trust (red de confianza).

El PGP llegó a alcanzar tal nivel de popularidad que incluso se celebraban fiestas con el objetivo de conocer gente e intercambiar claves.

Este sistema, previo al uso masivo de internet, era muy poco escalable. Sin embargo, sentó las bases del concepto de modelo de confianza descentralizado sobre el que se basan las identidades auto soberanas.

Rebooting web of trust: la primera iniciativa para organizar a la industria



Cristopher Allen decidió organizar una serie de eventos llamados **RWOT** [3] (Rebooting Web Of Trust) con el objetivo de crear la siguiente generación de sistemas de identidad basados en el concepto de una red de confianza descentralizada. Para ello, la idea era crear una serie de whitepapers como resultado de las conversaciones de estos eventos. Por ejemplo, el primer paper que resultó de primer evento, celebrado en noviembre de 2015, se tituló **"Rebranding the Web of Trust"**[4], que redefine el término y crea un nuevo modelo para los elementos de confianza con una definición más moderna.

Al inicio en estos eventos participaba gente que venía sobretodo del mundo del Blockchain. Como anécdota, en los primeros eventos del RWOT participó Vitalik Buterin, el creador de Ethereum, una celebridad en el mundo Blockchain. Participó en la elaboración del paper **"Decentralized Publick Key Infrastructure"**[5].

El RWOT son unas jornadas que se hacen en distintos puntos del mundo, normalmente cada seis meses y donde se juntan ahí técnicos, pero también filósofos, abogados y perfiles muy variados para tratar temas de todo tipo alrededor de la identidad. Desde protocolos técnicos a temas de diversidad y sostenibilidad.

Se puede acceder a la lista de todos los whitepapers publicados en este enlace: **https://www.weboftrust.info/papers.html**[6]

[3] https://www.weboftrust.info

[4] https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/rebranding-web-of-trust.pdf

[5] https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf

[6] https://www.weboftrust.info/papers.html

DIF: el gran think tank del mundo SSI

Además del RWOT, el IIW (Identity Internet Workshop) era el principal foro de la industria de la identidad. Esta organización se centra en la identidad basada en el usuario. **El primer tallerą** se celebró en octubre de 2005, con el objetivo de contar con un foro en el que se pudieran tratar los temas de arquitectura, gobernanza, etc. para los servicios de identidad en internet y sus filosofías subyacentes.

Como resultado de estos eventos, surgió la necesidad de organizar a los distintos pensadores de la industria sobre temas de SSI. Así pues, tanto el RWOT como el IIW sirvieron de base para crear el DIF (Decentralized Identity Foundation) en 2017.

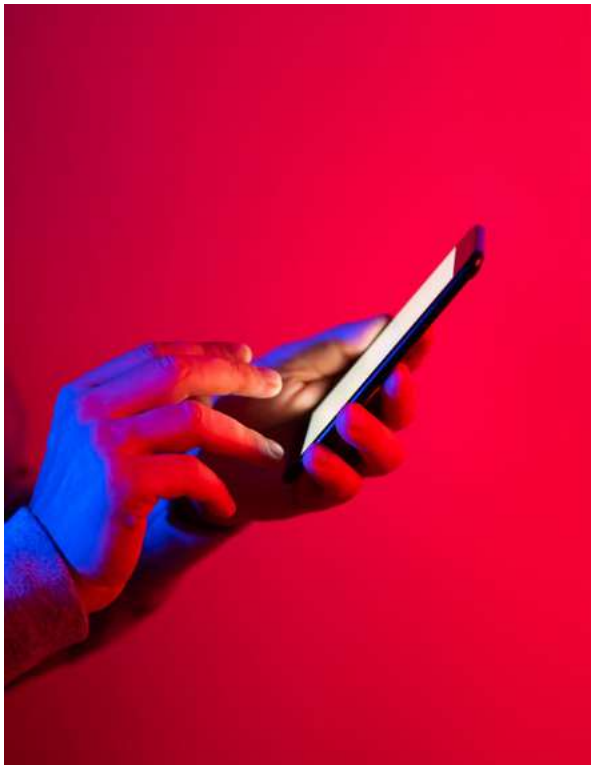
Desde su creación ha sido y es uno los think tanks más relevantes en el mundo del SSI. Actualmente hay centenares de empresas que participan, como Microsoft, Accenture, Sovrin y Validated ID entre otras.

DIF[8] impulsa el desarrollo del sector de la identidad a través de sus grupos de trabajo (Working Groups), que se dividen en áreas funcionales (como "Identificadores y descubrimiento" "Autenticación DID", "Credenciales", etc) donde se debaten desde temas más conceptuales a temas más técnicos que después tratan los comités de estandarización correspondientes.

[7] https://identitywoman.net/announcing-the-internet-identity-workshop-iiw2005/

[8] https://identity.foundation

INATBA: la asociación europea para temas de blockchain



En 2019, la Unión Europea impulsa la creación de la alianza internacional blockchain **INATBA**[9] (International Association of Trusted Blockchain Applications), con el objetivo de tratar los temas relacionados con Blockchain. El objetivo de la asociación es promover el uso de la tecnología Blockchain, reuniendo a entidades públicas y privadas del sector, así como a creadores de políticas, organizaciones internacionales, reguladores, la sociedad civil y organismos de establecimiento de estándares de toda Europa.

Actualmente cuenta con más de un centenar de miembros, como Accenture, Everis, Fujitsu, IBM, Deutsche Telekom, Telefónica, BBVA, IOTA, Ripple, Sovrin o ConsenSys.

Cuentan con un **grupo de trabajo**[10] específico que trata lo relacionado con el sector de la identidad. Cabe destacar el whitepaper "**Decentralised Identity: What's at Stake?**[11], publicado en noviembre de 2020.

También se pueden consultar **la respuestaàá** que INATBA preparó a la consulta pública sobre el borrador del reglamento eIDAS 2, en la que se incluye una propuesta de mejoras.

[9] https://inatba.org

[10] https://inatba.org/identity-working-group/

[11] https://inatba.org/wp-content/uploads/2020/11/2020-11-INATBA-Decentralised-Identity-001.pdf

[12] https://inatba.org/wp-content/uploads/2021/10/INATBA-Response-to-the-EU-Commission-Open-Public-Consultation-response-on-the-eIDAS-Regulatory-Framework-1.pdf

Sovrin: la primera gran red SSI

sovrin

En paralelo a las labores de definición de conceptos, protocolo y estándares internacionales, surgen varias iniciativas y proyectos alrededor de SSI.

La red de **Sovrin**[13] es una red distribuida, pública y con permisos, construida específicamente para la identidad. Sovrin fue la primera gran red de SSI para identidad y que ha tenido mucha influencia en el modelo actual. En la red participan toda una serie de Stewards (stakeholders que mantienen los nodos de la red). En España, el único nodo de Sovrin que hay lo aloja Validated ID.

En 2020, como resultado de la colaboración entre empresas en los foros internacionales, surge **Trust Over**[14] IP (ToIP). La idea se gestó durante 2019, como una confluencia de múltiples esfuerzos en los espacios de identidad digital, credenciales verificables, tecnología blockchain y comunicaciones seguras por parte de personas que vieron la necesidad de converger y crear una arquitectura interoperable para la confianza digital descentralizada. Más de 300 organizaciones e individuos miembros forman parte de la Fundación ToIP, como Accenture, Avast, British Columbia, IBM, MasterCard, entre otros.

[13] https://sovrin.org

[14] https://trustoverip.org/about/about/

ALASTRIA: la gran iniciativa nacional

En España, la principal red en el sector de la identidad descentralizada es Alastria. Fundada en 2017, se presentó como "la primera red nacional regulada basada en blockchain en el mundo. Respaldada por grandes entidades españolas como BBVA, Banco Santander, Iberdrola, Repsol, entre muchas otras, nace con el objetivo de acelerar la creación de ecosistemas digitales poniendo a disposición una plataforma colaborativa común.

Esta iniciativa trata más allá del ámbito de la identidad, aunque con foco importante en la misma. Basada en la tecnología Ethereum, es la primera iniciativa que le da un foco específico al tema legal.

ALASTRIA

Europa y el eIDAS bridge

Todos los actores mencionados, excepto tal vez Alastria, están muy alejados del mundo regulatorio. A pesar de que hay muchas carteras de credenciales en desarrollo y de que varias empresas como nosotros esperan este destacado paradigma, la realidad es que el marco legal está aún poco maduro. Por el momento contamos con el reglamento eIDAS, centrado sobre todo en las PKIs y los certificados tradicionales.

En junio de 2021, la Comisión Europea aprobó un nuevo borrador de este reglamento que establece que las nuevas identidades de los ciudadanos europeos se basarán en los principios SSI y estarán respaldadas por carteras de identidad. Sin embargo, esta normativa aún debe ser aprobada y desarrollada formalmente, es decir, aún no existe un marco de confianza establecido. Por ello, el proyecto eIDAS Bridge ha surgido como un paso intermedio.

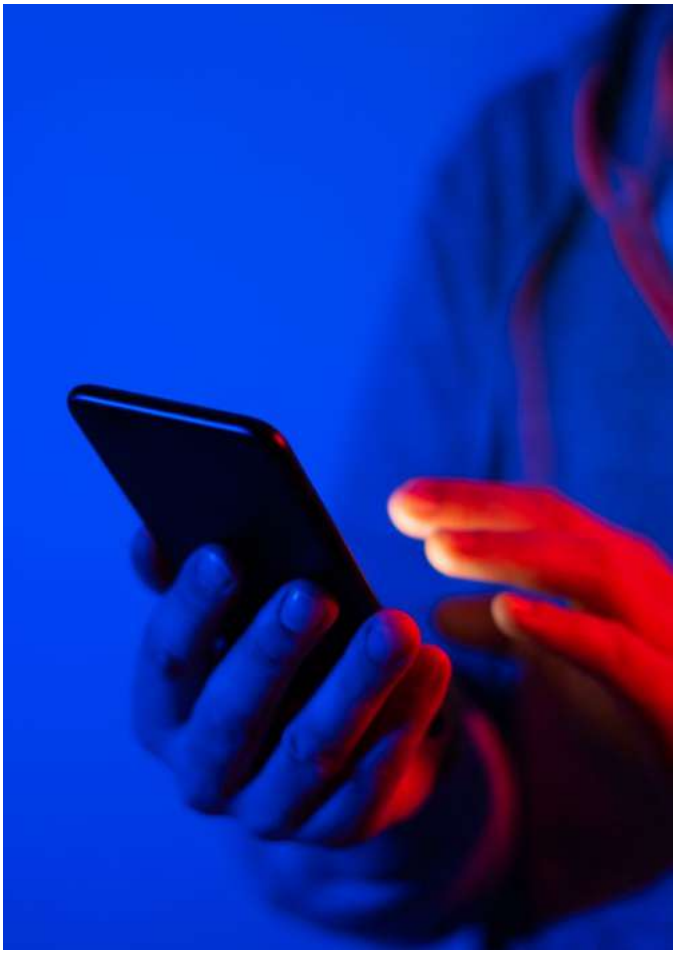
El proyecto eIDAS Bridge es una iniciativa de la Comisión Europea (CE) dentro del programa ISA2. La CE desarrolló eIDAS Bridge para promover eIDAS como marco de confianza para el ecosistema SSI. Este proyecto trata de dar solución a uno de los retos más urgentes a los que se enfrenta la SSI: disponer de un marco de confianza en el que confiar.

Más adelante, **eSSIF Lab**[15], otro proyecto financiado por la UE cuyo objetivo es proporcionar un ecosistema interoperable, abrió un programa para hacer evolucionar eIDAS Bridge.

El objetivo principal de este nuevo programa es proporcionar una implementación de eIDAS Bridge y probar la interoperabilidad entre diferentes implementaciones de proveedores.

Los entregables técnicos, desarrollados por Validated ID, consisten en utilizar claves vinculadas de certificados cualificados para operaciones SSI. Se pueden consultar en el siguiente enlace: **https://joinup.ec.europa.eu/collection/ssi-eidas-bridge**[16]

Los entregables legales, elaborados por Nacho Alamillo, exponen las partes de la regulación actual que necesitan ser modificadas para dar cabida a este nuevo modelo de identidades, que posteriormente resuelve el eIDAS 2.0.



eIDAS

[15] https://essif-lab.eu

[16] https://joinup.ec.europa.eu/collection/ssi-eidas-bridge

EBSI: el gran proyecto europeo

La **(EBSI)**[17] es una iniciativa conjunta de la Comisión Europea y la European Blockchain Partnership. Nace en 2020 para aprovechar la tecnología blockchain para acelerar la creación de servicios transfronterizos para que las administraciones públicas y sus ecosistemas verifiquen la información y hagan que los servicios sean más fiables.

En el marco del programa EBSI Early Adopters, buscaban enfrentar a los diferentes proyectos del sector de la industria a probar un piloto en un entorno real multiuniversitario, con el fin de probar la interoperabilidad de las soluciones con otros actores clave del ecosistema para permitir el intercambio de credenciales verificables.

Desde 2020, EBSI ha desplegado una red de nodos distribuidos en toda Europa, apoyando aplicaciones centradas en casos de uso seleccionados. Ha sido el proyecto de referencia en Europa en el mundo del SSI.

EBSI y eIDAS 2 se han creado de manera independiente y los gestionaban grupos diferentes, aunque parece que están en periodo de confluencia.

[17] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

eIDAS 2.0: el horizonte final de SSI

El Reglamento eIDAS, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, se publicó en julio de 2014. Esta iniciativa europea fue un hito clave en la regulación de la identificación en las transacciones electrónicas. Esta regulación tenía como objetivo aumentar la confianza de las transacciones electrónicas para promover el comercio online y se basaba en los certificados, sellos y la firma electrónica de documentos (servicios de confianza).

El primer reglamento eIDAS es un referente mundial que sienta las bases regulatorias replicadas en los reglamentos de países de fuera de la Unión Europea. A pesar de su gran nivel de aceptación en lo referente a los servicios de confianza, casi una década más tarde, la adopción de sistemas de identificación electrónica en las administraciones públicas es aún muy baja.

Por ello, en junio de 2021 se publica **una nueva propuesta**[18] para modificar el Reglamento eIDAS (conocido como eIDAS 2). Este reglamento quiere que los ciudadanos europeos cuenten con una identidad digital para todo el territorio de la UE, que sirva para poder compartir la información personal en una amplia variedad de contextos, incluido el entorno privado.

EIDAS 2 está basado en los conceptos de la tecnología SSI. Dado el recorrido de la tecnología de la identidad descentralizada, no deja de ser sorprendente que, con orígen en un mundo tan alternativo como el Blockchain, este modelo haya servido de base para la nueva regulación de identidad europea.

El siguiente gran hito es el Toolbox, una serie de protocolos y herramientas comunes, en la que está trabajando tanto la EC como los estados miembros y que está previsto que su primera versión vea la luz en septiembre.

[18] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

Validated ID

Always be yourself

Barcelona
C/ Aragó 179, 4° piso
08011 Barcelona
Tel: +34 900 828 948

Madrid
Paseo de las Delicias, 30 planta 7
28045 Madrid
Tel: +34 900 828 948

info@validatedid.com
validatedid.com