27.06.2022

Documento de conclusiones sobre el desarrollo y los resultados de las pruebas del proyecto Dalion presentado por los promotores Inetum España, Banca March, Banco Santander, CaixaBank, Unicaja Banco, Línea Directa Aseguradora, Mapfre España, Repsol y Grupo Generali España

Departamento de Funciones Horizontales
Dirección General de Supervisión

1 Antecedentes

La Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero (en adelante, Ley 7/2020) regula un entorno controlado de pruebas que permite llevar a la práctica proyectos tecnológicos de innovación en el sistema financiero.

Con fecha 22 de febrero de 2021, Inetum España, Banca March, Banco Santander, CaixaBank, Unicaja Banco, Línea Directa Aseguradora, Mapfre España, Repsol y Grupo Generali España, en adelante los Promotores, presentaron una solicitud para acceder al espacio controlado de pruebas conforme a un proyecto piloto, "Dalion" (en adelante, el "Proyecto"), cuyo objeto es la utilización de la tecnología *blockchain* para facilitar a los usuarios de las entidades financieras compartir, bajo su propio control, información de carácter personal[1] con otras entidades, financieras o no.

Con fecha 14 de mayo de 2021 la Secretaría General del Tesoro y Financiación Internacional publicó en su sede electrónica la lista de proyectos que recibieron una evaluación previa favorable para acceder a dicho entorno de pruebas en la que figura incluido el Proyecto. Asimismo, en la lista se contemplaba que el Banco de España (en adelante, el "Supervisor") sería la Autoridad Supervisora encargada de la monitorización de las pruebas.

Con fecha 4 de agosto de 2021 se suscribió el Protocolo de Pruebas en el que se recogen los términos en los que se realizarían las pruebas del Proyecto piloto presentado, al objeto de permitir al Promotor la realización –de manera controlada y delimitada– de las pruebas incluidas en el Proyecto.

Las pruebas previstas en el Protocolo se iniciaron el 14 de agosto de 2021 y finalizaron el 7 de enero de 2022.

[1] Esta información podrá ser generada por el usuario o acreditada por un tercero.

Con fecha 7 de febrero de 2022, los Promotores remitieron al Banco de España la Memoria, requerida por el apartado 1 del artículo 17 de la Ley 7/2020, con la evaluación de los resultados de las pruebas y del conjunto del Proyecto piloto.

El apartado 3 del artículo 17 de la Ley 7/2020 establece que la autoridad que haya sido responsable del seguimiento de las pruebas elaborará un documento de conclusiones sobre su desarrollo y resultados. Dichas conclusiones se tendrán en cuenta a efectos de lo previsto en los artículos 25 (el Informe anual sobre transformación digital del sistema financiero elaborado por la Secretaría General del Tesoro y Financiación Internacional) y 26 (las autoridades supervisoras incluirán en su memoria anual un informe sobre la aplicación de la innovación de base tecnológica a sus funciones supervisoras). Las conclusiones se podrán publicar con las reservas necesarias de conformidad con lo previsto en la Ley 7/2020 y en los protocolos suscritos con los Promotores.

En cumplimiento de lo establecido en el citado apartado 3 del artículo 17 de la Ley 7/2020, se elabora el presente Informe, en el que se recogen las conclusiones sobre el desarrollo de las pruebas y sus resultados.

2 Descripción del Proyecto

El Proyecto Dalion es una solución descentralizada de identidad auto gestionada basada en tecnología *blockchain*, donde el usuario es propietario y mantiene el control sobre sus propios datos personales, que gestiona mediante su teléfono móvil, sin depender de terceros y gestionándolos directa y autónomamente tanto para compartirlos como para recuperarlos. El usuario podrá enriquecer sus datos mediante la acreditación de los mismos por las empresas participantes.

Dalion es una implementación completa del Modelo de Identidad Alastria[2] ID[3] y sigue por tanto el estándar UNE 71307-1:2020, primer estándar formal de gestión de identidad basada en *blockchain*. Los elementos software que conforman el Proyecto son los siguientes:

- ***Wallet* de usuario MIIO**: Aplicación móvil, desarrollada únicamente para móviles Android, que permite al usuario: almacenar sus datos en forma de credenciales, autogestionar dichas credenciales recibidas y las presentaciones compartidas con terceros y realizar las comunicaciones con el resto de los actores y la *blockchain*. Esta aplicación se puso a disposición de los probadores a través de Google Play como aplicación en "prueba cerrada"[4].
- ***Wallet* de entidad:** Comprende un conjunto de elementos software que permiten a las entidades emitir credenciales, revocarlas, recibir presentaciones de credenciales, comprobar el estado de validez o revocación de las credenciales y revocaciones en *blockchain*, así como configurar las reglas de negocio necesarias. Incluye los repositorios de datos que se utilizarán para dichas funciones. Los elementos software del *wallet* de entidad se pueden agrupar de la siguiente manera:

[2] Alastria es una asociación sin ánimo de lucro, de la que son socios, entre otros, todos los Promotores del Proyecto Dalion, que fomenta la economía digital a través del desarrollo de tecnologías de registro descentralizadas/blockchain.

[3] Alastria ha definido el modelo e implementado algunas de sus piezas, fundamentalmente los *Smart Contracts* y la librería que facilita su uso. De modo complementario, Alastria ha realizado una implementación de referencia o demostración del resto de las piezas software clave del modelo, que son el *wallet* de usuario y el *wallet* de entidad de Alastria.

[4] Una "prueba cerrada" de Google Play permite crear listas de probadores usando la dirección de correo electrónico de modo que solo los usuarios de las listas pueden descargar la aplicación.

- ***Backend***: conjunto de módulos que interactúan con la *blockchain* y el *wallet* de usuario MIIO y tienen la lógica para realizar todas las acciones mencionadas.
- **Portal de administración de las entidades:** donde se realiza la configuración de las reglas de negocio para emitir y recibir credenciales, y se visualiza la información relativa a las mismas.
- **SDK[5]:** pieza de software que se integra en las aplicaciones web de las entidades para permitir al usuario iniciar la emisión y presentación de credenciales, entre otras acciones.

- **Red *blockchain*:** es la red en la que se registran los DID[6] (y clave pública) de los usuarios y entidades, así como las acciones de emisión, recepción y revocación de credenciales y presentaciones. Se utiliza la Red T de Alastria[7].
- **Servicios *Core* Dalion:** Es el conjunto formado por el *wallet* de entidad, *wallet* de usuario MIIO y la red *blockchain*, así como las comunicaciones entre estos elementos, entre las que se incluyen el canal SSE[8] y el módulo BSS[9].
- **Sistemas corporativos:** Son los servicios de autenticación, firma y CRM[10] propios de cada entidad, con los que se integra el *wallet* de entidad. Durante las pruebas del *Sandbox* se utilizaron implementaciones mínimas de estos tres sistemas, con la funcionalidad necesaria para llevar a cabo las pruebas.

Para la realización de las pruebas se configuraron dos *wallets* de entidad simulando un banco, Banco Dalion, y una aseguradora, Aseguradora Dalion, mientras que todos los probadores instalaron el *wallet* de usuario MIIO en sus móviles de empresa.

3 Desarrollo de las pruebas

3.1 Información remitida por los Promotores sobre el desarrollo de las pruebas

Las pruebas se llevaron a cabo entre los días 14 de agosto de 2021 y 7 de enero de 2022, con una duración de 4 meses y tres semanas.

Fueron ejecutadas por 30 empleados de los Promotores, a los que se denominó probadores, que utilizaron datos ficticios siguiendo una guía de pruebas. Los probadores comenzaron a ejecutar las pruebas la semana del 22 de noviembre de 2021 y finalizaron el día 5 de enero de 2021, dentro del plazo establecido.

Las pruebas llevadas a cabo por los probadores, o *customer journey*[11], fueron las siguientes:

- **Prueba 1.** Creación de la identidad Alastria ID utilizando el *wallet* de usuario MIIO y emisión por parte del Banco Dalion de la credencial[12] IBAN.

[5] Un kit de desarrollo de software (S*oftware Development Kit* o SDK por sus siglas en inglés) es un conjunto de herramientas de desarrollo de software que permite a un desarrollador crear una aplicación informática para un sistema concreto.
[6] Los identificadores distribuidos (*Decentraliced Identifiers* o DID por sus siglas en inglés) son identificadores que permiten una identidad digital verificable y descentralizada.
[7] Red T de Alastria es una red *blockchain* público-permisionada. Es la red *blockchain* de acceso público más grande y con mayor estabilidad disponible en España. Al ser permisionada garantiza que los operadores de todos los nodos que participan en dicha red son conocidos, y siguen unas políticas aceptadas por todos.
[8] El canal *Server-Sent Events* (SSE) se utiliza en el SDK web de Dalion, integrado en la web de la entidad, para comunicarse con el *wallet* de entidad para entregar asíncronamente información a la página web
[9] El módulo *Blockchain Synchro Service* (BSS) es el módulo encargado de comunicarse con la red *blockchain* y escuchar sus eventos.
[10] CRM (del inglés *Customer Relationship Management*) es el software para la administración y gestión de la relación con los clientes.
[11] *Customer Journey* es el camino o pasos que va a recorrer el probador para realizar las pruebas que se le solicitan. Es un término utilizado en marketing para definir el proceso por el que pasa una persona para realizar una compra.
[12] Una credencial es un archivo digital con una o más declaraciones acerca de un sujeto, como el nombre, la edad, etc., emitida por el sujeto o un tercero que acredita su veracidad.

- **Prueba 2.** Desde la web de la Aseguradora Dalion, realización del cambio de la cuenta de cargo mediante la presentación del IBAN de la nueva cuenta bancaria acreditada por el Banco Dalion a través del *wallet* de usuario MIIO.
- **Prueba 3.** Revocaciones de las presentaciones de credenciales por parte de los probadores (prueba 3.1) y revocaciones de las credenciales tanto por parte de Banco Dalion (prueba 3.2) como por parte de los probadores (prueba 3.3).

3.2 Seguimiento supervisor del desarrollo de las pruebas

A lo largo de las pruebas, el Supervisor y los Promotores mantuvieron una serie de reuniones de seguimiento periódicas para tratar, principalmente, el grado de avance de las pruebas. Además, a petición del Supervisor, los Promotores realizaron demostraciones específicas en las que se pudo observar el flujo interno de cada prueba en los portales de administración de los *wallets* de entidad, así como los cambios en la red *blockchain*.

3.3 Valoración supervisora del desarrollo de las pruebas

El desarrollo de las pruebas ha cumplido los objetivos que se marcaron en el Protocolo de Pruebas, ya que ha permitido comprobar que Dalion proporcionaría eficiencia para entidades y usuarios. Adicionalmente, las demostraciones realizadas por los Promotores han sido muy enriquecedoras para los supervisores.

Por otra parte, no se han materializado riesgos durante las pruebas.

4 Próximos pasos

4.1 Información remitida por los Promotores

Entre los próximos pasos del Proyecto Dalion se incluyen actuaciones a corto plazo para realizar pilotos más complejos con las entidades asociadas y a medio plazo para realizar pilotos internos con casos de uso reales. Esto puede sufrir cambios y priorizaciones a lo largo de los próximos meses.

Las conclusiones obtenidas junto con la experiencia ganada en otros pilotos realizados por los socios de Dalion, servirán para determinar aspectos pendientes de mayor concreción, tales como:

- La calificación del servicio que se va a prestar, dado que consideran que éste podría enmarcarse como servicio de la sociedad de la información regulado por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico o incluso en un futuro como servicio de confianza, en caso de ampliarse el alcance del Reglamento eIDAS.
- La necesidad o conveniencia de constituir una figura jurídica que preste el servicio.
- La figura o figuras que gestionarán los derechos ARSO-POL[13] de los usuarios y darán cumplimiento a las obligaciones exigibles conforme a la normativa de protección de datos.
- La existencia de términos y condiciones únicos u homogéneos.

[13] Los derechos ARSO-POL, contemplados en el reglamento general de protección de datos (RGPD), persiguen la protección de los datos personales de los ciudadanos. Actualmente han quedado definidos 7 derechos: acceso, rectificación, supresión (cancelación), oposición, portabilidad, olvido y limitación del tratamiento.

4.2 Valoración supervisora sobre los siguientes pasos del Proyecto

Para llevar a cabo el Proyecto fuera del entorno del *Sandbox*, los Promotores no harán uso de la pasarela de acceso a la actividad a la que se refiere el artículo 18 de la Ley 7/2020, ya que no es necesario solicitar autorización para implantar este Proyecto.

Se advierte de que el Banco de España no ha llevado a cabo una valoración del cumplimiento del principio de responsabilidad proactiva en el tratamiento de datos personales, toda vez que dicha valoración excede del ámbito competencial de esta Institución.

5 Barreras regulatorias identificadas por los Promotores

Según indican los Promotores en su Memoria, el marco regulatorio actual presenta una serie de incertidumbres que condicionan la viabilidad del Proyecto y su desarrollo a escala comercial. A continuación, se detalla el análisis de las barreras e incertidumbres regulatorias llevado a cabo por los Promotores.

Reglamento General de Protección de Datos.
En primer lugar, los Promotores indican que es necesario que la Agencia Española de Protección de Datos confirme que el DID no debe considerarse como un dato de carácter personal, y si, en su caso, la inscripción del DID junto con la clave publica en la *blockchain* puede ocasionar algún tipo de incumplimiento normativo. Asimismo, debe tenerse en consideración y concretarse si la posibilidad de identificar el estado de la credencial (enviado, recibido, etc.) afecta al tratamiento de ésta como dato personal.

En segundo lugar, en relación con los mecanismos técnicos que garantizan la privacidad del usuario y el ejercicio sencillo y autónomo de sus derechos ARSO-POL en la red *blockchain,* sería necesario aclarar si son adecuados para poder lanzar el producto al mercado sin asumir riesgos de un posible incumplimiento normativo.

Valor probatorio del servicio Dalion.
Ante la ausencia de una legislación específica que regule el valor probatorio de los datos existentes en una red *blockchain* o criterios jurisprudenciales a los que acudir, los Promotores sostienen que sería necesaria una manifestación por parte de la Administración reconociéndolo de manera expresa.

Reconocimiento de firmas y certificados digitales basados en tecnología *blockchain* como válidos en el Reglamento eIDAS.
Los datos de validación de firma basada en claves tipo *blockchain* se corresponden con la clave pública que cada individuo posee junto a su clave privada. Las credenciales verificables, con datos y atributos de identidad, proporcionan los datos que confirman la identidad de la persona física. El DID tiene como objetivo relacionarse con la identidad para poder asegurar la confianza en la interacción.

Si se considera una acreditación con la combinación de estos documentos que están vinculados en la tecnología *blockchain*, los Promotores manifiestan que se debería interpretar que cumple con el objetivo de la declaración definida en el artículo 3 del Reglamento eIDAS.

La manifestación expresa por parte de la Administración de esta interpretación respecto a la firma y el certificado digital basado en tecnología *blockchain*, permitiría garantizar la seguridad jurídica de todos los actores que utilicen este tipo de firma y certificados.

Compatibilidad con Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

Los Promotores sostienen que debe validarse que la solución técnica utilizada cumple los criterios y recomendaciones en materia de seguridad, conservación y normalización de la información establecidos en el Esquema Nacional de Interoperabilidad por tal de asegurar su compatibilidad con el sistema público.

El Esquema Nacional de Seguridad establece los aspectos y metodologías comunes relativos a la seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, y, deberá corroborarse que Dalion cumple con los principios básicos y requisitos mínimos que se recogen en el mismo.

SEPBLAC

Según los Promotores, si bien las alternativas de identificación no presencial actualmente autorizadas por el SEPBLAC suponen un avance importante tanto en tiempo como en costes respecto a la identificación presencial, sigue siendo necesario el envío de documentación original o la repetición del proceso de identificación en cada una de las entidades en las que un cliente desea abrir una cuenta.

Para que no sea necesario repetir el proceso de identificación ante otras entidades, los Promotores consideran que el SEPBLAC debería autorizar la presentación de credenciales del cliente ante otro sujeto obligado con garantías suficientes para darse de alta y posteriormente realizar operaciones financieras.

6 Conclusiones

6.1 Conclusiones remitidas por los Promotores

Según indican los Promotores en su memoria, las pruebas efectuadas cumplieron todos los criterios de éxito incluidos en el Protocolo de pruebas, salvo los derivados de un pequeño problema funcional, detectado durante las mismas y que ya ha sido resuelto y probado.

La puesta en producción de esta solución se ve dificultada por algunas incertidumbres y barreras regulatorias que se agrupan en distintos ámbitos: la legislación en materia de protección de datos, el valor probatorio de los registros distribuidos, la validez legal de los esquemas de firma electrónica y certificados digitales basados en tecnología *blockchain*, y también de las credenciales verificables y las presentaciones de credenciales, entre otras.

Según los Promotores, las pruebas efectuadas en el *Sandbox* han servido para verificar el funcionamiento del Piloto como Producto Mínimo Viable, así como la viabilidad de la puesta en marcha del Proyecto siempre que se resuelvan las barreras regulatorias identificadas.

El impulso decidido de esta y otras iniciativas, que han aprovechado las ventajas que el *Sandbox* ofrece, servirá para mantener el liderazgo del ecosistema *blockchain* español en Europa, en particular en el área de identidad digital, que constituye la base para la soberanía tecnológica europea en un entorno de adopción masiva de la digitalización, tanto en el ámbito personal como en el empresarial y en el de las Administraciones Públicas.

6.2 Conclusiones supervisoras

Se trata de un Proyecto prometedor, que podría aportar grandes ganancias de eficiencia para las entidades de crédito, así como para los usuarios. Sin embargo, los Promotores deberán evolucionar su solución de cara a una eventual puesta en producción.

Existen una serie de riesgos prudenciales relacionados con el uso de redes *blockchain* para identidad digital que se describen a continuación, como pueden ser los derivados de incertidumbres legales, cumplimiento regulatorio, la falta de una gobernanza adecuada, dependencia de terceras partes, responsabilidades inciertas y riesgo tecnológico.

En cuanto a las incertidumbres legales o potenciales problemas de incumplimiento regulatorio se encuentran, entre otros, los relativos a la ausencia de regulación acerca del valor probatorio de la red *blockchain* y los relacionados con el cumplimiento de la legislación vigente en materia de protección de datos personales.

La ausencia de una gobernanza adecuada de la red *blockchain* podría tener un impacto negativo que conllevase riesgos operacionales y reputacionales. Este riesgo podría quedar mitigado por el hecho de que el Proyecto hace uso de una red público-permisionada con unas políticas de gobierno y operación de la red, definidas por los socios de Alastria, que deben ser conocidas y aceptadas para proceder a la incorporación de un nodo en la red y empezar a usarla.

Por otro lado, existe un riesgo de dependencia de terceros, ya que el Proyecto está desplegado sobre la red *blockchain* de Alastria y si bien los Promotores son miembros del consorcio, la red *blockchain* o la propia Alastria podrían desparecer o la *blockchain* funcionar o evolucionar de forma diferente a las expectativas de los Promotores. Debido a la naturaleza distribuida de una red *blockchain,* podría ser difícil asignar las responsabilidades en caso de materializarse algún riesgo.

En lo relativo al riesgo tecnológico, este podría aumentar potencialmente si los datos sensibles no se protegieran adecuadamente en tránsito y en almacenamiento, aun no almacenándose en la *blockchain*. Asimismo, los *wallets* de usuario podrían ser atacados para obtener las credenciales, lo que constituye otro vector de ataque que podría dar lugar a suplantaciones de identidad. Adicionalmente, debido a que la red *blockchain* está formada por un número indeterminado de nodos, aquellos nodos con un menor nivel de seguridad podrían ser usados para conseguir acceder a la red *blockchain* de manera ilegítima.

Si finalmente se eliminaran las barreras regulatorias, este Proyecto alcanzaría su máximo potencial una vez identificados los casos de uso más apropiados y conseguido un efecto de red[14], ya que son necesarios tanto un elevado número de usuarios como de empresas que acepten y emitan credenciales para tener un crecimiento satisfactorio. En relación a esto último, será necesario que los Promotores tengan en cuenta el incremento del volumen de eventos de la *blockchain* que deberá escuchar y, en su caso, procesar el módulo BSS, para dimensionarlo de manera adecuada.

En lo relativo a dispositivos móviles, en primer lugar, el Proyecto solo funciona en la actualidad para dispositivos Android, por lo que, en una eventual puesta en producción, los

[14] Se dice que ocurren efectos de red cuando el valor de un bien o servicio depende del número de personas que lo utilizan. En general, cuando existe un efecto de red, mientras mayor sea el número de usuarios, mayor valor o utilidad tendrá ese bien o servicio. Ejemplo de ello es WhatsApp, la plataforma de mensajería con más usuarios registrados en todo el mundo y, por consiguiente, la que más usuarios nuevos atrae.

Promotores deberán trabajar en la compatibilidad del *wallet* de usuario MIIO con otros sistemas operativos.

También relacionado con los dispositivos móviles, el Proyecto piloto probado en el *Sandbox* no ha abordado la problemática de la pérdida, avería o robo del dispositivo donde está instalado el *wallet* de usuario MIIO y las implicaciones que estas situaciones podrían tener en la recuperación y/o la revocación de las credenciales almacenadas en el *wallet*. Sería necesario por tanto que los Promotores implementen los procedimientos relativos a la recuperación de credenciales y/o la realización de copias de seguridad del *wallet*.

Conforme a lo dispuesto en el artículo 5 de la Ley 7/2020, el Proyecto debía aportar potencial utilidad o valor añadido. A este respecto, el Supervisor concluye que el Proyecto podría suponer un eventual beneficio para los usuarios de servicios financieros en términos de mejora de la calidad o de las condiciones de acceso, así como un aumento de la eficiencia de entidades o mercados.

La innovación probada en el Proyecto no proporciona mecanismos para el mejor ejercicio de la función supervisora, por lo que no sería necesaria la inclusión de la evaluación del Proyecto en el informe para la Memoria de Supervisión al que hace referencia el artículo 26 de la Ley 7/2020.

Por delegación de la Comisión Ejecutiva
B.O.E. de 27.12.2019

[F] Mª MERCEDES OLANO LIBRAN

Firmado digitalmente por [F] Mª MERCEDES OLANO LIBRAN

Mercedes Olano
Directora General de Supervisión