Signata y el Framework de Protección de Identidad y Anonimidad para el futuro de los sistemas de control de acceso

Congruent Labs, marzo del 2021

Resumen

Los desarrolladores de los servicios online gastan horas innumerables de su tiempo en la construcción de sistemas para recopilar la información privada durante la identificación de sus usuarios, luego deben gastar más de su tiempo en mantener cada uno de estos sistemas para cumplir con las leyes y normas locales e internacionales. Además, al recibir el pago por servicios solamente sirve para aumentar esta carga, ya que las organizaciones deben pagarles y cederles el control a los terceros proveedores de servicios quienes son los encargados de proporcionar servicios seguros y resistentes al fraude para recopilar y administrar la información sobre los pagos.

En este documento, explicaremos cómo el servicio Signata podrá unir la siguiente generación de las identidades: éstas siendo identidades que se mantendrán anónimas de los proveedores de servicios, y presentaremos el Framework de Protección de Identidad y Anonimidad – o el Identity Guard & Anonymity Framework (IdGAF) - como una solución on y off-chain descentralizado para la identificación, autorización, y administración durante el ciclo de vida de la identidad moderna. Al mismo tiempo, presentaremos cómo los usuarios podrán autodesignar sus identidades a los chains a través de los contratos inteligentes, además de los proveedores de servicios que tendrán la habilidad de validar y mantener las identidades ya conocidas mediante soluciones off-chain.

Asimismo, hablaremos sobre las capacidades ya existentes con Signata para el manejo de los monederos y las interacciones con los blockchains. Del mismo modo, presentaremos las siguientes etapas del producto para incorporar el IdGAF como una plataforma integral de identidad para los pagos, presentaremos el nuevo token SATA que apoyará estos sistemas, y explicaremos cómo estos servicios proveerán la primera prueba de concepto para la integración independiente de los otros servicios que trabajarán dentro de este Framework.

Tabla de Contenido

Introducción

El mundo del manejo de la identidad se encuentra en un constante estado de cambio. Los proveedores de identidad centralizados (tales como Google, Facebook, y Okta) están procurando liderar la lucha con sistemas de autenticación centralizados que ofrecen un manejo simplificado, lo que nos lleva a pensar que la época de la contraseña se está volviendo cada vez más obsoleta. No obstante, el manejo centralizado de la identidad requiere que los usuarios les cedan todo el control de su identidad y el acceso a los proveedores de servicios que manejan sus identidades, en vez de mantener el control de sus propias capacidades individuales de autenticación y las designaciones de identidad. Típicamente, estos proveedores centralizados se financian por cultivar datos – a niveles sin precedentes – sobre los individuos, de esta forma observando el uso de las identidades *dentro* de sus servicios además de *fuera* de ellos a través de una red cada vez más grande de sistemas de seguimiento online.

Signata[1] es una plataforma construida por Congruent Labs[2] para revelar la verdadera capacidad de tarjeta inteligente de los Yubico[3] YubiKeys para vincular las identidades de los individuos con su contenido digital y para interactuar con los blockchains. Actualmente, la capacidad clave de Signata es proveer un monedero de hardware para almacenar las criptomonedas, sin embargo la tecnología que forma la base de los YubiKeys también se puede emplear para proveer la capacidad de autenticar, firmar contenido de manera digital, y unir las identidades a los factores de la autenticación.

Asimismo, Signata emplea las capacidades ya establecidas de tarjeta inteligente de los YubiKeys para crear un camino natural de expansión del servicio, de esta manera integrando más funcionalidades como la autenticación y las firmas digitales, pero también expandiendo a integrar las identidades de los usuarios sobre los blockchains en vez de simplemente interactuar con ellos.

El presente documento propone introducir un nuevo token ERC-20[4] para Signata que se llama SATA. Este token servirá para una variedad de propósitos. En los lanzamientos futuros de la plataforma, los tokens SATA se utilizarán para interactuar con una plataforma de servicios de identidad descentralizada basada en los contratos inteligentes. Actualmente, Signata está desarrollando estos servicios como capacidades internas claves del producto, pero adicionalmente como sistemas de preservación de anonimato on y off-chain que los servicios externos podrán integrar y consumir para construir un ecosistema de identidad no ligado a las autoridades centrales. Esta nueva plataforma será conocida como el Framework de Protección de Identidad y Anonimidad (IdGAF por sus siglas en inglés).

[1] https://signata.net
[2] https://congruentlabs.co
[3] https://yubico.com
[4] https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

Nosotros creemos que las capacidades existentes de manejo de identidad en los blockhains intentan realizar protocolos y sistemas que fueron diseñados para sistemas no basados en los blockchains. Por ende, Signata ofrecerá una plataforma que mantiene los principios centrales de los blockchains:

- Identificaciones de los individuos anónimas pero criptográficamente confiables,
- Designaciones descentralizadas de contenido, y
- Pagos asegurados por servicios o interacciones en el chain.

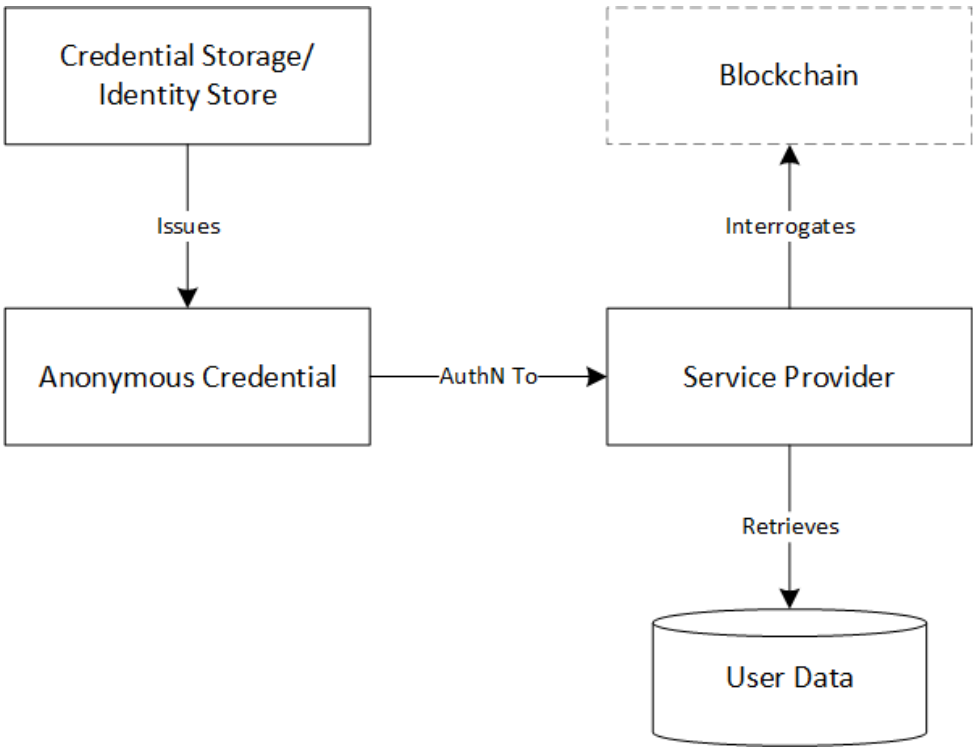

Figure 1 - Interaction Overview

Los proveedores de servicios que utilizan el IdGAF (incluyendo a Signata como la primera prueba de concepto) podrán autenticar y autorizar los usuarios de manera segura con credenciales anónimas, el cual se logrará al combinar la verificación de datos on-chain suministrada por el poseedor de la credencial (asegurando propiedad de la credencial), la verificación on-chain de las autorizaciones, y la verificación off-chain de la información que se tiene dentro del servicio mismo (asegurando que la credencial recibe su debida autorización).

Esta capacidad permitirá que los proveedores de servicios puedan autenticar los usuarios, recolectar los pagos, y proveer control de acceso a los sistemas sin conocer dato alguno sobre el usuario que lo podría identificar – a no ser que quieran recopilar esa información ellos mismos y el usuario les ceda el permiso para la recolección de dicha información.

Descripción del producto

La Criptomoneda Signata

La Cripto Signata (conocida como Signata) es un servicio actualmente en operación y disponible en línea a la dirección https://signata.net que les permite a los usuarios registrados:

- Agregar uno o más YubiKeys a su cuenta, estableciendo el embedded applet PIV[5] con una clave de codificación.
- Agregar o Importar direcciones de BTC, ETH, XRP, DASH y DOGE a su cuenta, todas encriptadas por sus YubiKeys.
- Agregar notas seguras a su cuenta que son encriptadas por sus YubiKeys.

Signata opera como un servicio de cero conocimiento para todos los secretos almacenados en el sistema. Los usuarios deben configurar un BIP39[6] mnemónica *contraseña de recuperación* para mantener la capacidad de recuperar su cuenta en caso de perder sus YubiKeys. La clave de codificación que reside en su YubiKeys se queda en el YubiKey del usuario almacenado en una tarjeta inteligente inexportable y una versión encriptada se almacena dentro del servicio de Signata como copia de seguridad. Para asegurar que Signata no se convierta en objeto de ataque, la mnemónica nunca se envía al almacenamiento que opera el sistema.

Para que los usuarios puedan interactuar con sus direcciones, simplemente tienen que conectar su YubiKey, proveer su PIN (parecido al sistema de autorizar un pago con una tarjeta de crédito, pero solo el YubiKey y el usuario conocen el PIN), y las claves se desencriptan para ser utilizadas por el usuario. A diferencia de los monederos de hardware comunes, las claves no se residen en el YubiKey – solamente la clave de codificación reside allí. La clave de codificación se protege del uso no autorizado por el PIN del usuario (que no lo conoce Signata), y los intentos fallidos repetidos terminarán en el bloqueo del YubiKey para asegurar que el acceso por fuerza bruta no se pueda lograr.

[5] https://www.nist.gov/topics/identity-access-management/personal-identity-verification-piv
[6] https://en.bitcoin.it/wiki/BIP_0039

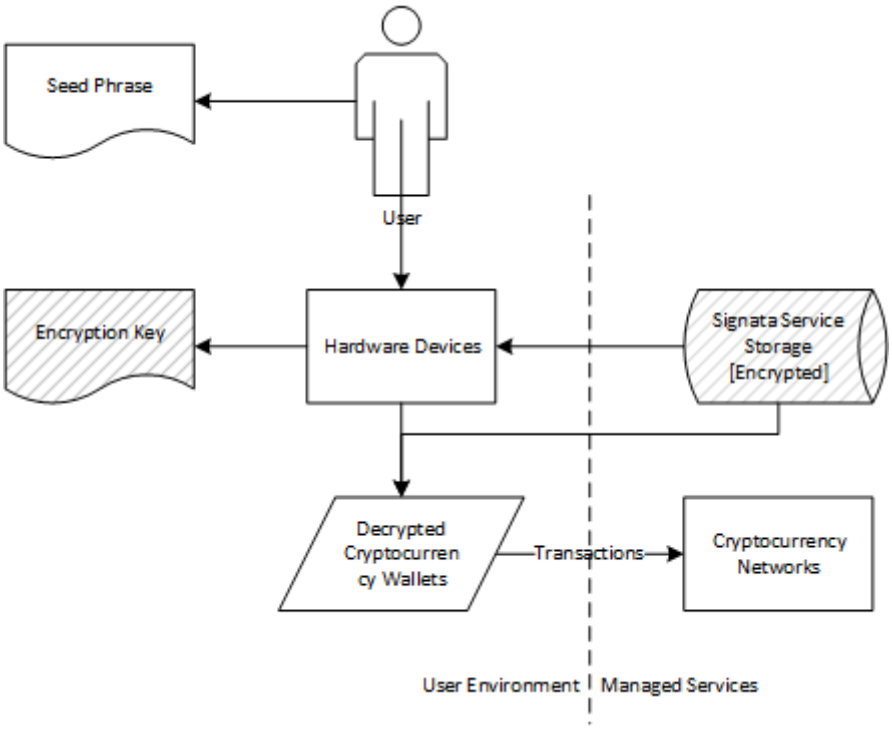

Figure 2 - Signata Crypto Overview

IdGAF – Framework de Protección de Identidad y Anonimidad

El Framework de Protección de Identidad y Anonimidad se lanzará como un conjunto de contratos *on-chain* y sistemas *off-chain* para proveer un servicio de autenticación integral para las aplicaciones. Este framework proveerá varios subsistemas claves, cada uno atado o relacionado con las capacidades criptográficas de las direcciones, registros, e interacciones de blockchain.

Cada vez que se construyen y se lanzan estos sistemas, serán entregados dentro de un mercado de identidad abierta, aunque cabe mencionar que la naturaleza open-source de estos componentes no se restringirá al acceso exclusivo a través de este Marketplace.

Autoridades de Identidades Autodesignadas

Cada individuo establecerá una credencial anclaje dentro de su dispositivo de preferencia. Esta credencial anclaje se retendrá para aprobar la ligada de direcciones agregadas o importadas de otros sistemas y de esta manera provee a los usuarios la habilidad de autodesignar la aprobación de material criptográfico para ser utilizado con la autenticación y la autorización. Los usuarios no tienen restricciones para la emisión de sus propias credenciales de autoridad, tampoco las hay en el número de credenciales emitidas por las autoridades para que de este modo puedan adaptar sus identidades a los contextos específicos en los cuales las están designando.

En las operaciones normales, puede suceder que los usuarios pierdan acceso, o sus identidades puedan ser comprometidas. En el caso de una afectación identificada, el individuo o puede autodesignar la cancelación de su propia autoridad de identidad (suponiendo que mantienen el control sobre ella) o reemplazar su identidad con una nueva (y de esta forma realizar la re-designación de la nueva autoridad a los proveedores conectados). Las autoridades de identidades son quienes introducen el vector más grande de ataque de los terceros – si se compromete la autoridad uno puede denegar el servicio o asumir la identidad de la autoridad robada.

Una manera de mitigar este ataque vector será la imposición de un almacenamiento de claves basado en hardware, que será vital en la manera en la que los usuarios interactúan con el IdGAF, siendo muy parecido a como el Universal 2nd Factor (U2F[7]) provee protección basada en hardware al uso de las credenciales de autenticación. No todos los sistemas de autenticación pueden interactuar con los dispositivos de hardware (incluyendo muchos dispositivos móviles que son limitados por las interfaces físicas y las políticas de sistemas operativos), entonces se implementará también una capacidad de delegación de credenciales para facilitar la creación de credenciales emitidas con capacidades restringidas para asegurar que los usuarios puedan acceder a los sistemas que necesitan sin exponer sus credenciales a un riesgo innecesario dentro de los dispositivos de menor seguridad.

[7] https://fidoalliance.org/specs/u2f-specs-master/fido-u2f-overview.html

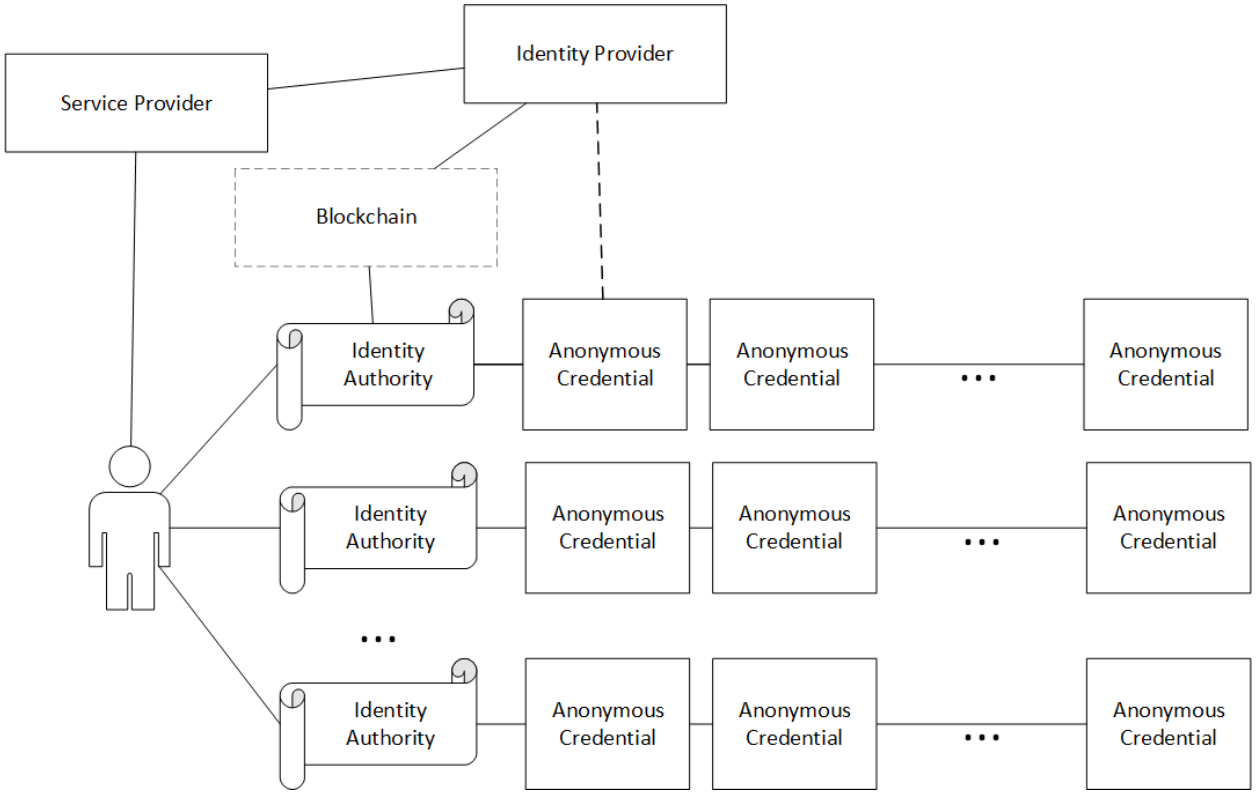

Figure 3 - Las autoridades de identidad y sus conexiones

Proveedores de Identidad Anonimizadas (DeREx)

En el mercado actual de Proveedores de Identidad, la mayoría de los proveedores ofrece alguna combinación de un tipo de solución persistente de la colección de identidad, la capacidad de single sign-on, el manejo de sesiones en varios dispositivos, y para las generaciones más avanzadas, soluciones de riesgo adaptativas para la observación de comportamiento inesperado de los usuarios.

A diferencia de lo anterior, los proveedores de servicios conectados al IdGAF podrán proveer la capacidad clave de las identidades persistentes, pero al mismo tiempo manteniendo la anonimidad, al igual que ofrecer la capacidad de capturar y manejar los servicios de pagos que están directamente vinculados al proveedor de identidad. Mediante este método integrado, los desarrolladores de sistemas no tendrán que integrar dos sistemas dispares para lograr el mismo resultado para sus productos – los usuarios pueden autenticarse de manera segura y pagar por servicios dentro del mismo conjunto de transacciones, y sin tener que ceder información que los identifique personalmente al proveedor de servicios.

Asimismo, los proveedores de servicios pueden liberarse de la responsabilidad de capturar y almacenar la información de identidad y pagos, de esta manera quitando una posible exposición de datos que los podría identificar una vez un sistema haya sufrido una filtración de información.

Los proveedores conectados se presentarán como el Exchange de Derechos Descentralizados, o el Decentralized Rights Exchange (DeREx) y así se proveerá una plataforma unificada para que los terceros puedan integrar y consumir estos servicios.

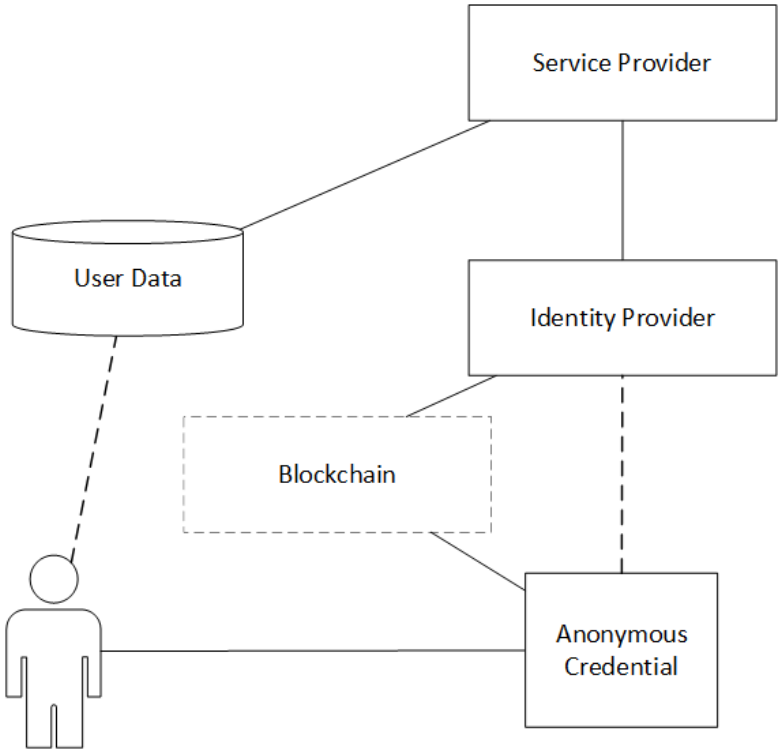

Figure 4 - Resumen del Proveedor de Identidad Anonimizada

Descentralizado X.509 (Dex509)

Los sistemas de Infraestructura de Clave Pública (PKI systems en inglés) han sido construidos y han evolucionado de manera natural para adaptarse a operaciones *sobre* los blockchains. Entonces, al considerar las capacidades clave de las autoridades de certificaciones, los controles de seguridad impuestos para protegerlos están diseñados para replicar efectivamente las características que los blockchains ahora ofrecen de manera inherente – almacenan una secuencia de eventos inmutables muy parecidos a los blocks y las transacciones que se manejan en el chain.

De manera importante, los servicios que habilitan el IdGAF que interactúan con las certificaciones de autenticación, firma, y codificación podrán, adicionalmente, empujar y traer los registros de certificaciones en los chains. Las designaciones de estado de autoridad/firma de las claves públicas permitirán a los proveedores de servicios a confiar de manera inherente las designaciones hechas por autoridades específicas como un modelo de confianza transitivo pero anónimo, similar a los dentro del ecosistema de los PKI.

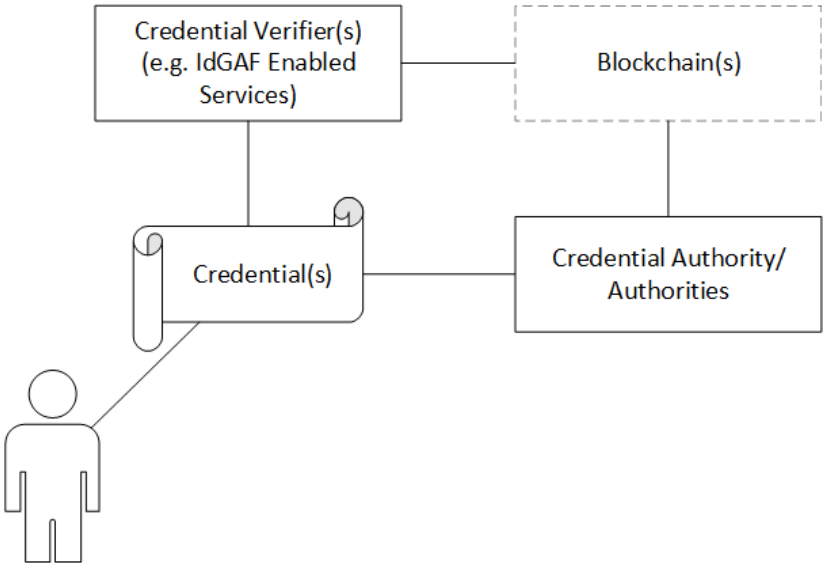

Figure 5 - Resumen del Dex509

Hoja de Ruta del Producto

Al lanzar y lograr la adopción exitosa del SATA Airdrop, Congruent Labs establecerá tres ejes de desarrollo para cumplir con cada producto clave. El primer eje de desarrollo contempla el desarrollo de aplicaciones claves de Signata. El segundo eje se encarga del desarrollo de la aplicación del Dex509. Finalmente, el tercer eje desarrolla la aplicación de IdGAF.

El penúltimo servicio que Congruent Labs lanzará involucra la convergencia de todos los tres ejes de desarrollo en un solo producto y framework unificado que facilitará el uso de monederos de hardware en combinación con el manejo descentralizado de la identidad y el pago de productos y suscripciones ligados a estas identidades.

T2 2021 Lanzamiento

Lanzamiento del Token y Distribución de Liquidez - El token SATA, en conjunto con el presente whitepaper, se lanzará en el mainnet de Ethereum y se distribuirá a todos los exchanges centrales (donde se acepta) para establecer la liquidez del token.

T4 2021 Lanzamiento

Interacción total de contratos ERC-20 - Mientras Signata se conecta actualmente a Infura como un proveedor de Ethereum, está limitado todavía a puras transacciones con la moneda ETH en esta etapa. El producto se extenderá para permitir la interacción con contratos en la red ETH, incluyendo la capacidad de intercambiar los tokens ERC-20 dentro de las direcciones ETH.

Integración directa con los Exchanges - Para facilitar depósitos y retiros más sencillos de los exchanges de criptomonedas, se establecerán conexiones directas para permitir que los usuarios puedan mover las monedas de manera sencilla y rápida entre Signata y los exchanges, ofreciendo un almacenamiento más seguro.

Integración expandida de hardware – El servicio de Signata de manejo de dispositivos se extraerá y se expandirá para incluir conectividad directa con las aplicaciones web, de esta manera permitiendo una interacción más amplia con las claves privadas almacenadas en hardware para la firma de transacciones y la distribución entre plataformas.

Ligada de identidades – Actualmente, Signata emite certificados de codificación a los YubiKeys del usuario para encriptar todos sus datos. Esta habilidad se mejorará y se utilizará la plataforma PKI de Congruent Labs para la emisión de certificados de confianza para los YubiKeys de los usuarios.

Primeros Lanzamientos de Dex509 y DeREx – La nueva integración de IronSign de Signata incluirá la capacidad de ligar la información de identidades a las direcciones criptográficas, de esta manera estableciendo la capacidad de identificar, validar, y asegurar los niveles de seguridad de las monederas. La nueva plataforma Descentralizada del Manejo de la Identidad y el Acceso

de Signata se lanzará para el uso del público, y el primer servicio consumidor de ella será la misma aplicación Signata. Adicionalmente, se lanzará la primera versión del mercado.

2022 Lanzamiento

Adopción del mercado – Todas las capacidades lanzadas estarán disponibles dentro del mercado, y la inclusión de proveedores se priorizará para aumentar la adopción del producto.

Anonimidad de Signata – Las capacidades del nuevo Dex509 y DIdAM serán aprovechados por Signata para incluir el acceso anónimo al servicio mientras se permite que el usuario mantenga el control sobre su monedero de hardware.

Hardware alternativo – Los dispositivos diferentes de YubiKeys, como el PIV tarjeta inteligente genérica, se integrarán como una alternativa más rentable que los YubiKeys para interactuar con el servicio de Signata, de esta forma reduciendo costos para los usuarios.

Sobre nosotros

Este whitepaper fue desarrollado por Congruent Labs Pty Ltd, una empresa australiana de software registrada desde el año 2017.

Descargo de Responsabilidad

Los planes, estrategias, e implementación de los detalles descritos en el presente whitepaper están sujetos al cambio y lo más probable es que evolucionen, e incluso, puede que nunca sean adoptados. Por ende, Congruent Labs Pty Ltd se reserva el derecho de desarrollar o buscar planes, estrategias, o detalles de implementación alternativos o adicionales que se asocian con la plataforma Signata.

Los tokens SATA están siendo distribuidos por Congruent Labs Pty Ltd conforme a los términos y condiciones (los “términos”) del token disponibles en https://sata.technology/. Para más detalles, revisa los términos. Los tokens SATA no son valores, inversiones, ni dinero, y no se venden ni se promocionan de esta manera. La participación en la colección de los tokens SATA implica riesgos tecnológicos y sistémicos considerables. La distribución de los tokens SATA no está abierta a los ciudadanos de los Estados Unidos y Canadá. El periodo, duración, y tarificación de la distribución, además de otras provisiones, pueden cambiar tal como se estipula en los términos. Los tokens SATA no representan, de ninguna manera, la participación accionaria, la participación, el derecho, el título, ni ningún interés en Congruent Labs Pty Ltd, sus respectivos afiliados, ni ninguna otra compañía, empresa, o iniciativa; poseer tokens SATA tampoco le da promesa alguna de pagos, dividendos, ingresos, ganancias, ni rendimiento de inversiones, y tampoco se pretenden constituir valores en Australia ni en cualquier jurisdicción relevante.

La distribución del token SATA conlleva riesgos tanto conocidos como desconocidos, incertidumbres, y otros factores que pueden causar que la funcionalidad, utilidad, o niveles de uso de los tokens SATA sean materialmente diferentes de cualquier resultado, uso, funcionalidad o utilidad futuros proyectados que hayan sido expresados o implicados por Congruent Labs Pty Ltd en los términos.