Una mirada sobre el futuro de la identidad descentralizada (v2)

Leo Sorokin

Tabla de contenidos

Resumen

La transformación digital se extiende globalmente y ha hecho un impacto en todos, desde ciudadanos y empleados hasta corporaciones y gobiernos. La identidad digital es uno de los pilares para el desarrollo de negocios en la economía digital. La identidad digital descentralizada es el próximo paso evolutivo de la identidad digital y ofrece la posibilidad de optimizar cómo las personas interactúan con otras instituciones, con objetos físicos y entre sí mismas. Este artículo aborda el posible futuro de la identidad descentralizada, los beneficios de la misma, su terminología, así como algunos casos de uso y ofrece una muestra de su implementación técnica a la vez que plantea algunas de las limitaciones de este modelo. Por otra parte, el lector encontrará información sobre el estado actual de las capacidades de la identidad descentralizada y un resumen de la evolución de la identidad digital del pasado al presente.

Introducción

A medida que las organizaciones se transforman, la identidad digital está alcanzando un estado crítico rápida y globalmente. La identidad juega un rol crucial en la transformación digital e impulsa que tanto gobiernos como negocios provean un acceso seguro y restringido a datos para cualquiera de las partes interesadas; ya sean empleados, socios, clientes o ciudadanos. En un mundo donde hay una gran proliferación de datos en un sinfín de dispositivos y donde cada vez es más complejo determinar un perímetro de red, la identidad digital se ha vuelto un elemento vital en la seguridad.

En el ámbito de la identidad, el concepto de *identidad descentralizada* es uno de los que está más activamente en desarrollo. La identidad descentralizada representa un cambio filosófico y técnico de las *credenciales basadas en cuentas* hacia las *credenciales verificables* e implica una transformación en la manera en que la información de identidad es obtenida y presentada. El *World Wide Web Consortium* (W3C) está trabajando en la publicación de estándares de *Credenciales Verificables* e *Identificadores Descentralizados*.[1],[2] Sin embargo y como ocurre con cualquier estándar tecnológico, para ser útil debe ser adoptado por gran parte de la comunidad.

Actualmente, la identidad digital de una persona, y los datos personales asociados a la misma, están repartidos entre varios servicios en línea que se acceden primariamente mediante un usuario y una contraseña. Este tipo de credencial basada en cuentas es típicamente provisto directamente por el proveedor de servicio o por un proveedor de identidades (IdP, por sus

[1] "Verifiable Credentials Data Model 1.0," W3C Recommendation, World Wide Web Consortium (W3C), 19 de noviembre de 2019, https://www.w3.org/TR/vc-data-model/.

[2] "Decentralized Identifiers (DIDs) v1.0," W3C Working Draft, World Wide Web Consortium (W3C), 27 de octubre de 2020, https://www.w3.org/TR/did-core/.

siglas en inglés) vasto y más bien centralizado como Google, Facebook o Twitter con el cual una aplicación proveedora de servicio se unirá para verificar la identidad. No obstante, este modelo federado basado en cuentas tiene algunas limitaciones importantes: el IdP puede dejar de ofrecer sus servicios a terceros; la identidad avalada por ese IdP puede verse comprometida y por lo tanto puede impactar en toda aplicación proveedora de servicio que use dicha identidad; el IdP puede rastrear las actividades de un individuo a través de múltiples servicios; y un IdP puede retirar el servicio de la cuenta siendo utilizada para la autenticación. El modelo federado de identidad plantea muchos desafíos, pero volver a los silos de la identidad donde cada proveedor de servicios provee y administra su propio set de credenciales para sus usuarios, provocando que los usuarios deban manejar decenas de credenciales basadas en cuentas, tampoco es ideal.

La identidad descentralizada pone al individuo en el centro de la experiencia de identidad digital, es decir en el centro del intercambio de datos de identidad. A grandes rasgos, la identidad descentralizada imita las billeteras y tarjetas físicas por medio de una representación digital de las mismas.

Hay quienes están muy entusiasmados con este modelo, así como quienes lo miran con escepticismo. Aunque la identidad descentralizada y los conceptos que la sustentan intentan solucionar los desafíos que ha habido con la identidad digital en las últimas décadas, aún es muy pronto para predecir cómo los individuos, gobiernos y corporaciones la abordarán y qué provecho sacarán de ella.

Los beneficios de la identidad descentralizada

Un sistema de identidad descentralizada puede reemplazar al tradicional sistema de “usuario y contraseña” durante una secuencia de *autenticación* típica. Este es el primer caso de uso en que se pensará al hablar de identidad descentralizada. Sin embargo, autenticar una identidad sin contraseña es posible hoy en día aún sin ninguno de los componentes de la identidad descentralizada. Por eso, el verdadero valor de la identidad descentralizada se comprende mejor durante la *autorización*. Durante la autorización, el proveedor de servicio puede reducir los riesgos al requerir que el individuo presente una o más acreditaciones firmadas digitalmente en proporción al nivel de riesgo y al nivel de valor que esa transacción específica implica. Esta capacidad aumenta el nivel de confianza entre las partes, optimiza la experiencia del individuo y reduce costos a los negocios.

El objetivo de la identidad descentralizada es otorgar el poder a los individuos para que sean dueños y controlen sus identidades digitales, así como la manera en que se acceden y utilizan sus datos de identidad. La identidad descentralizada se despega de la noción de usuario y contraseña y del tradicional modelo basado en cuentas. Una identidad digital no es otra cosa que un modelo de usuario y contraseña basado en cuentas provisto y mantenido por un tercero. Con un modelo de identidad descentralizada, el individuo puede ser autenticado y autorizado para ejecutar una transacción con un servicio y luego presentar la misma información de identidad a otra entidad con la cual el individuo prefiera interactuar. Sumado a

esto, el individuo puede ser su propio proveedor de identidad que es lo más difícil de conseguir con los modelos centralizados o federados que usamos hoy en día.

La identidad digital descentralizada y los *datos personales* asociados a la misma permiten que el individuo tenga más control sobre cómo sus datos son accedidos y utilizados. De esta filosofía se desprende que los datos personales deberían ser presentados por el propio individuo a los proveedores de servicio, según sea necesario, y con los términos de uso específicos que él decida. Este principio es la esencia de la identidad descentralizada. En un ecosistema de identidad descentralizada, no hay una autoridad central única; los valores son intercambiados de forma *peer-to-peer* (entre pares). Dado que los individuos controlan y poseen sus propios datos personales son ellos quienes habilitan a otras partes a accederlos, otorgándoles permisos específicos. Esto contrasta con la realidad de hoy en día en la que los datos personales pueden ser compartidos y almacenados por terceros que están por fuera del control del individuo quien no tiene forma de especificar bajo qué términos y condiciones de uso su información de identidad es compartida.

En un ambiente de identidad descentralizada, es posible poseer una tarjeta digital para una licencia de conducir, una tarjeta de crédito o incluso un pasaporte y tenerlos disponibles en un dispositivo móvil. Puede también ser útil cuando un individuo se encuentra de viaje y tiene que ver un médico. Actualmente compartir con un médico el historial médico y la medicación utilizada es muy engorroso y poco práctico, salvo a través de una explicación verbal. Sin embargo, un ecosistema saludable de identidad descentralizada de emisores y verificadores permitiría compartir información médica importante de forma digital y preservando la privacidad del individuo, permitiendo que el médico pueda tomar una mejor decisión médica y por lo tanto proveyendo al paciente una mejor atención.

Otro ejemplo de caso de uso de la identidad descentralizada es un banco hipotecario que necesita que el dueño de la propiedad provea pruebas de que su póliza de seguro de propiedad esté activa. Para ello, el propietario presenta información de su póliza de seguro de propiedad al banco hipotecario de modo que el banco puede verificar periódicamente el estado de la póliza de seguros cuando lo necesite sin la necesidad de que el propietario deba volver a presentar la documentación para su verificación. Si bien una identidad centralizada o federada puede permitir este tipo de caso de uso, la identidad descentralizada es más adecuada.

La identidad descentralizada puede promover nuevos modelos de negocio e intercambios de valores. Abre el camino para experiencias 100% digitales de modo que los individuos no necesitan presentarse personalmente para realizar transacciones de gran valor. La identidad descentralizada puede también optimizar la experiencia de usuario “física” en múltiples situaciones de forma que el individuo no necesite portar su billetera física. También ofrece potenciales beneficios a los negocios para mejorar cómo verificar y generar confianza con sus clientes. Existen todo tipo de beneficios potenciales en el uso de la identidad descentralizada, pero solo el mercado y el tiempo dirán si las grandes expectativas que tenemos se llevarán a cabo en la práctica a largo plazo.

Terminología de la identidad descentralizada

A continuación, se encuentran los conceptos básicos involucrados en una experiencia de identidad descentralizada.
Estas definiciones han sido simplificadas para mejorar la comprensión de cuáles son los actores involucrados y cómo interactúan entre sí:

- *Identidad auto-soberana:* Es un término que describe un movimiento digital que se basa en el principio de que un individuo debe poseer y controlar su identidad sin la necesidad de intervención por parte de autoridades administrativas.
- *Credenciales verificables:* Son atestaciones o acreditaciones que hace un emisor sobre un sujeto. Las credenciales verificables son firmadas digitalmente por el emisor.
- *Emisor:* Es la entidad que emite credenciales verificables sobre sujetos a propietarios o titulares. En general, los emisores son entidades gubernamentales o corporaciones, sin embargo, un emisor puede también ser una persona o un dispositivo.
- *Titular (Holder):* Es la entidad que posee credenciales verificables. Los Titulares son generalmente usuarios, pero también pueden ser organizaciones o dispositivos.
- *Verificador:* Es la entidad que verifica las credenciales verificables para poder proveer servicios a un propietario.
- *Presentaciones verificables:* Conjunto de credenciales verificables, atestaciones autogeneradas o cualquier artefacto que se presenta ante los verificadores para ser verificado. Las presentaciones verificables están firmadas digitalmente por el propietario y pueden contener toda la información que un verificador solicita en un solo paquete. Es también donde los propietarios delimitan las condiciones de uso específicas en las que una presentación debe usarse.
- *Agente de usuario o agente digital:* es el software que los titulares utilizan (típicamente una aplicación de teléfono móvil) que recibe las credenciales verificables de los emisores, las almacenan y las presentan a los verificadores para su verificación.
- *Hub de identidad o repositorio*: Es el lugar en el que los usuarios pueden almacenar la información relativa a su identidad encriptada. Un *hub* de identidad puede estar en cualquier lado -en el borde, en la nube o en tu propio servidor. Su propósito es almacenar datos personales. Algunas implementaciones pueden permitir que otras entidades accedan al *hub* de identidad de un usuario si el usuario específicamente concede dicho acceso. Se puede pensar los *hubs* de identidad como un almacén de datos personales de un individuo.
- *Identificador Descentralizado (DID, por sus siglas en inglés):* Es un identificador que es creado y anclado a un sistema descentralizado como una cadena de bloques (*blockchain*) y puede representar a una entidad en el ecosistema -un emisor, un propietario, un verificador o incluso un *hub* de identidad.
- *Tarjetas digitales:* Son las credenciales verificables que los usuarios recopilan con el tiempo y que están almacenadas como parte del agente o del *hub* de identidad del usuario. En cierta forma, es más sencillo referirse a ellas como tarjetas digitales que como credenciales verificables.

- *Billetera digital:* Es una metáfora digital que representa a una billetera física y que es en general representada por la combinación del agente de usuario y de las subyacentes capacidades del dispositivo informático, como el almacenamiento y enclave seguros en un teléfono móvil. La billetera digital contiene tarjetas digitales.
- *Infraestructura descentralizada de clave pública (dPKI, por sus siglas en inglés):* Es una infraestructura descentralizada de clave pública que generalmente se implementa mediante una cadena de bloques o un registro distribuido -un lugar donde los identificadores descentralizados pueden registrarse y ser buscados junto a las claves públicas asociadas al DID y sus metadatos. En términos generales, una dPKI puede ser descrita como un registro de datos verificables ya que la dPKI es solo una de las muchas formas de implementación de un registro de datos verificables que existen. Si bien este artículo se refiere a la infraestructura descentralizada de clave pública, el lector debe saber que un registro de datos verificables no debe ser necesariamente descentralizado.
- *Resolutor Universal:* Es un resolutor de identificadores que funciona con cualquier identificador descentralizado a través de los controladores del DID. El objetivo de un resolutor universal es entregar un documento DID con los metadatos DID ante determinado valor DID. Esta función es muy útil ya que los DID pueden ser anclados en una variedad de implementaciones disímiles de infraestructuras descentralizadas de clave pública.

La figura a continuación muestra a los principales actores y la relación entre ellos. También representa el escenario de caso modelo que abordaremos más adelante en este artículo.

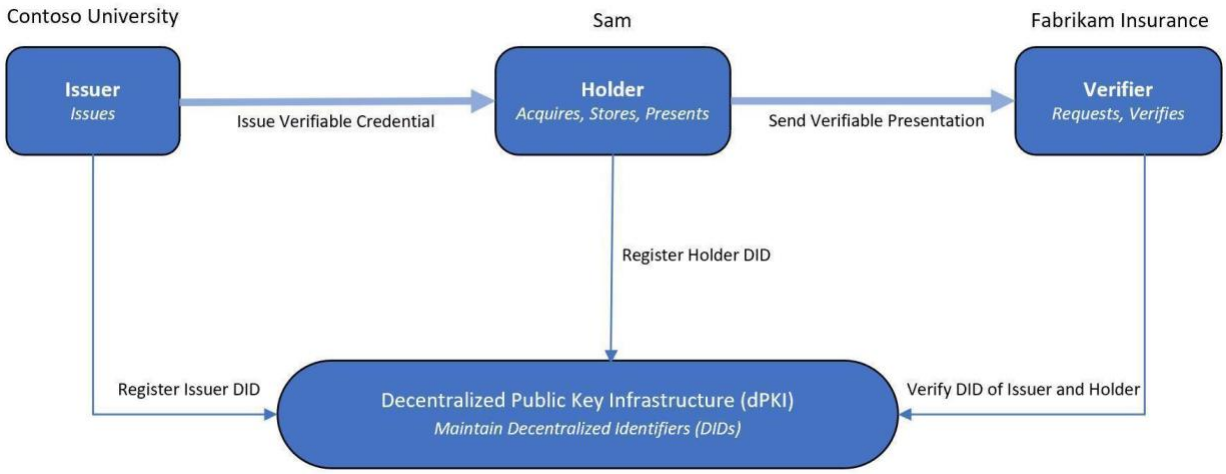

Figure 1 - Emisión y Presentación de Credenciales Verificables

Es fundamental destacar que ningún tipo de información personal debe ser almacenada en una infraestructura descentralizada de clave pública. La información personal de identidad debe ser almacenada como parte de la billetera digital o *hub* de identidad en una locación segura.

En general, el titular presenta las credenciales verificables a los verificadores durante una transacción en tiempo real, al igual que uno presenta su pasaporte ante el agente de migración al cruzar la frontera de un país. Sin embargo, en escenarios más avanzados, algunas implementaciones permitirían que el titular conceda un acceso específico a un verificador para que acceda datos en el *hub* de identidad del titular. De esta manera, el verificador puede acceder a la información que el individuo haya permitido en lugar de tener que presentar manualmente credenciales verificables al verificador cada vez que sea necesario. Dicho esto, el procedimiento más tradicional aún requiere que el titular presente credenciales verificables al verificador explícitamente pero el verificador tendrá el poder de verificar el estado de la credencial (como, por ejemplo, si ha sido revocada por el emisor) sin tener que molestar al titular.

Ahora que ya hemos asentado la terminología, pasaremos a un escenario caso modelo.

Escenario de identidad descentralizada

Mediante el caso modelo *end-to-end* (de principio a fin) detallado a continuación nos proponemos mostrar el valor y la utilidad de un ecosistema de identidad descentralizada. No se trata de una descripción exhaustiva de todas las posibilidades que ofrecen las identidades descentralizadas, sino que representa solo uno de los posibles flujos de la identidad descentralizada.

Supongamos que “Sam” quiere comprar a la “Aseguradora Ejemplo” un seguro para su vehículo, pero para conseguir un buen precio, la Aseguradora requiere que Sam demuestre que tiene un título universitario de “Una Universidad”. En nuestro escenario de identidad descentralizada los actores son los siguientes:

- Sam, como el sujeto y titular de la credencial verificable.
- Una Universidad, como el emisor de la credencial verificable.
- La Aseguradora Ejemplo como el verificador de la credencial verificable.

La siguiente secuencia de pasos representa el flujo donde el objetivo final es que Sam obtenga un diploma digital de Una Universidad y pueda luego presentarlo para su verificación a la Aseguradora Ejemplo con el fin de recibir el descuento en el seguro de su vehículo:

1. Sam recibe un email de Una Universidad felicitando a Sam por graduarse donde se le provee un código QR que Sam puede escanear con su móvil. Sam tiene una aplicación en su móvil que está registrada para manejar dicha solicitud. Esta aplicación representa la *billetera digital* de Sam y tiene todas las *tarjetas digitales* que fueron recogidas en el tiempo. Sam escanea el código QR, la aplicación de la billetera digital se inicia y Sam es informado que, para conseguir su diploma digital, Sam debe iniciar sesión en el sitio de Una Universidad.

2. En nuestro caso, Sam cliquea el enlace e ingresa sus credenciales existentes para autenticar su identidad en el sitio web de la Universidad, o en caso de que Sam no tenga dichas credenciales, es posible que se le solicite presentarse en persona en la Oficina de Alumnos con su documento de identidad para recibir sus credenciales digitales. Una vez que Sam provee sus credenciales existentes, Sam es informado que puede *aceptar* su tarjeta digital de Una Universidad. Una vez que Sam acepta su tarjeta, se le solicita que asegure esta operación de forma biométrica, como mediante el escaneo de su huella digital, su rostro o con un PIN. Luego de que Sam realiza esta acción, la tarjeta queda almacenada de forma segura en su billetera digital. Sam puede revisar la tarjeta, ver los datos que la tarjeta tiene sobre él (que fueron autenticados por la universidad), como su nombre completo, carrera, estado de sus estudios, fecha de graduación y fecha en la cual fue emitida. Sam puede también ver la actividad en la que se utilizó su tarjeta, como cuándo fue emitida, a quién fue presentada y cómo se utilizó - todo esto puede ser realizado desde la app de la billetera digital del móvil de Sam. Dichas actividades pueden ser consideradas como un *recibo digital* o *historial verificable* que Sam puede usar para rastrear quién ha accedido los datos de su tarjeta. Estos recibos digitales se almacenan localmente con la tarjeta en la billetera digital de Sam, que se encuentra siempre bajo el control de Sam. En términos generales, podemos referirnos a esta tarjeta digital como una *credencial verificable*.

3. Ahora, para reclamar su descuento, Sam navega al sitio web de la Aseguradora Ejemplo en su teléfono y ve el botón *Verificar Credenciales*. Es un enlace y cuando Sam lo cliquea, la aplicación de billetera digital se abre con una solicitud de permiso. La solicitud de permiso indica que para que Sam pueda recibir su descuento, la Aseguradora Ejemplo necesita recibir su tarjeta digital de exalumno de Una Universidad. Nótese que Sam no necesita autenticarse ante la Aseguradora Ejemplo con un usuario y contraseña ni utilizar un IdP federado. Sam simplemente presenta el diploma digital que se encuentra en su billetera digital. En nuestro escenario, Sam solo presenta su tarjeta digital de ex alumno de Una Universidad a la Aseguradora Ejemplo, pero también podría presentar en caso de que fuera necesario, otras tarjetas digitales que Sam tenga en su billetera digital y que demuestren que reside en determinado territorio o que demuestren su dirección actual. Una vez que Sam autoriza la solicitud de permiso con su información biométrica como por ej. escaneando su huella digital, la Aseguradora Ejemplo recibe la tarjeta digital y puede verificar que fue efectivamente emitida para Sam por parte de Una Universidad y que es en efecto Sam quien está presentando esta tarjeta digital a la Aseguradora Ejemplo. Una vez que la Aseguradora Ejemplo completa la verificación, puede otorgar el descuento a Sam. Sam puede ahora ver el recibo de esta tarjeta en la aplicación de su billetera digital, donde se indica que dicha tarjeta fue presentada a la Aseguradora Ejemplo en una fecha específica, con un objetivo concreto y con los términos y condiciones avalados por él. Algunas implementaciones pueden permitir que Sam *revoque* el acceso que tiene la Aseguradora Ejemplo para ver su tarjeta digital. Esta revocación puede generar un nuevo *recibo* que indica claramente la fecha y hora en la que Sam revocó el acceso de la Aseguradora Ejemplo a su tarjeta digital. Una vez más, Sam puede realizar todo esto desde la aplicación de su billetera

digital en su móvil y todas las tarjetas digitales que Sam genere a lo largo del tiempo así como los recibos asociados a las mismas, estarán bajo el control de Sam.

4. Sam puede recopilar en su billetera digital tantas tarjetas digitales como quiera y puede llegar a necesitar presentar varias tarjetas, como sería el caso si Sam quisiera ingresar a un curso avanzado de arquitectura empresarial en una academia, y tuviera que demostrar que es un ex alumno de Una Universidad y que es también un arquitecto de empresa certificado. La academia podría verificar ambas credenciales presentadas y habilitar a Sam para que acceda al material de entrenamiento avanzado.

Es importante aclarar que Sam es quien envía la *presentación verificable* a la Aseguradora Ejemplo. Esta presentación verificable contiene un artefacto que es la *credencial verificable* que Sam recibió de Una Universidad. De esta manera, la Aseguradora Ejemplo actúa como el verificador y puede verificar los siguientes dos elementos críticos:

- Basándose en la firma digital de la *credencial verificable*, la Aseguradora Ejemplo verifica que la credencial verificable es auténtica y que fue efectivamente emitida para Sam por Una Universidad.
- Basándose en la firma digital de la *presentación verificable*, la Aseguradora Ejemplo verifica que es efectivamente Sam quien está presentando la credencial.

Una vez que la Aseguradora Ejemplo ha verificado lo antedicho, puede otorgarle a Sam el descuento para el seguro de su vehículo con confianza.

Implementación técnica de la identidad descentralizada

La siguiente secuencia es la explicación técnica del escenario modelo presentado anteriormente. Destaca los pasos que deben seguirse para configurar la experiencia de identidad descentralizada, la emisión de la credencial verificable y el flujo de su presentación. Dicho esto, este escenario asume que la infraestructura descentralizada de clave pública (dPKI) ya está configurada por lo que eso no se explicará aquí.

Configuración

1. Una Universidad representa al emisor. Genera el Identificador Descentralizado (DID) enlazado a un par de claves pública/privada y registra sus DID en el dPKI. La clave privada es almacenada por el departamento TI de Una Universidad en una Bóveda de Claves o en un Módulo de Hardware de Seguridad. La correspondiente clave pública es publicada en un registro descentralizado como una cadena de bloques de modo que cualquiera pueda encontrarla.

2. El departamento TI de Una Universidad publica un documento DID que enlaza sus DID con el Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) registrado públicamente, como por ej. unauniversidad.edu. Esto representa el enlace del dominio a una credencial verificable. El departamento TI de Una Universidad hospeda en su sitio web este archivo que demuestra la propiedad del dominio y del DID específico. El verificador (como por ej. la Aseguradora Ejemplo) utiliza ese documento DID para

confirmar que Una Universidad es propietaria de dicho DID y para asegurarse de que la credencial verificable que recibe fue efectivamente emitida por Una Universidad y no por otro emisor que dice ser Una Universidad.

3. El departamento TI de Una Universidad desarrolla un contrato que describe los requisitos para la emisión de una credencial verificable. Por ejemplo, el departamento TI de Una Universidad especifica qué acreditaciones deben ser emitidas directamente por el usuario y qué otras credenciales verificables -si las hay- el individuo debe proporcionar primero. En nuestro escenario, el departamento TI requiere que el estudiante se autentique con un IdP federado que admita el protocolo *OpenID Connect*, con el fin de recibir un token de seguridad y extraer sus acreditaciones, como su nombre, apellido y número de estudiante. El emisor podrá entonces asignarle los atributos que emitirá en la credencial verificable. Es importante destacar que Una Universidad indicará el (los) patrón (es) a los que se ajustará la credencial verificable, de manera que otros verificadores de todo el mundo puedan utilizar el contenido de la credencial verificable que reciban.

4. Por último, los administradores de TI de Una Universidad pueden configurar y personalizar el diseño de las tarjetas de credenciales verificables que se emitirán, como el color de la tarjeta, los logos, iconos, imágenes y el texto útil. Los administradores pueden personalizar las cadenas de texto mediante los metadatos que conforman las tarjetas basadas en las certificaciones emitidas con los datos de la credencial. Esto permite diseñar la apariencia de las credenciales verificables de exalumnos emitidas por Una Universidad y garantiza que las tarjetas digitales emitidas reflejen la marca de la universidad. A futuro, estos elementos gráficos deberían estandarizarse para que los estudiantes disfruten de una experiencia visual consistente de la representación de la tarjeta digital, independientemente del proveedor que desarrolle el agente de usuario o del agente digital que el estudiante elija usar.

Emisión de las credenciales verificables

1. El flujo de la solicitud de emisión de credenciales comienza cuando Sam escanea un código QR usando su móvil. El propósito de la solicitud de emisión es que el agente de usuario de Sam recupere los requisitos para la emisión de credenciales dictados por el emisor y que muestre la experiencia de usuario (UX, por sus siglas en inglés) apropiada al usuario a través del agente de usuario. El código QR se muestra en el sitio web de Una Universidad y escanearlo abre la aplicación de la billetera digital de Sam, activando una operación de recuperación de la solicitud de emisión desde el agente de usuario a Una Universidad. Una vez que el agente de usuario recibe la solicitud de emisión de Una Universidad, comienza el flujo de emisión de la credencial. La solicitud de emisión está firmada digitalmente por Una Universidad y el agente de usuario puede verificar la autenticidad de dicha solicitud. La solicitud de emisión incluye una referencia al contrato que describe cómo el agente de usuario debe proveer la UX y qué información necesita Sam para que se le otorgue una credencial verificable de exalumno.

2. Una vez que el agente verifica que la solicitud es genuina, le presenta la UX a Sam. Dado el requisito específico que Una Universidad tiene para emitir tarjetas digitales a exalumnos en nuestro escenario, Sam necesita iniciar sesión en su cuenta preexistente de la Universidad, que a su vez emite un token de seguridad al agente de usuario que acredita el nombre y apellido de Sam, su título y fecha de graduación. (Nótese que durante la configuración mencionada aquí arriba, el emisor puede configurarse para aceptar tokens de seguridad de cualquier proveedor de identidad confiable de *OpenID Connect* de modo que el usuario de agente utilizará dicho proveedor de identidad durante el proceso de emisión.) Así, cuando el individuo cliquea "Iniciar sesión en Una Universidad" en el agente de usuario, el mismo redirige al individuo para que se autentique ante el IdP, y es allí donde el individuo realiza las tareas de autenticación estándar como ingresar su nombre de usuario y contraseña, llevando a cabo una Autenticación Multifactor (MFA, por sus siglas en inglés), y aceptando los términos y condiciones del servicio o pagando por su credencial. Toda esta actividad ocurre del lado del cliente a través del agente de usuario (por ej. una aplicación de móvil). Cuando el usuario finalmente recibe el token de seguridad del IdP, puede presentarlo al emisor quien puede extraer las acreditaciones de este, tal y como se mencionó anteriormente, e introducirlos como atributos en la credencial verificable resultante, enriqueciendo así las acreditaciones con información obtenida de otras fuentes. Asimismo, luego de que el individuo se autenticó ante el IdP, el agente de usuario puede mostrar campos adicionales de entrada de datos que el individuo puede escoger. Una vez que el individuo ha provisto toda la información requerida, el usuario de agente verifica que ha completado todos los requisitos del emisor y le pregunta a Sam si quiere aceptar la tarjeta.

3. En nuestro escenario, cuando Sam acepta la tarjeta se le solicita que realice una acción biométrica como escanear su huella digital. Esta acción genera un par de claves público/privado para el DID de Sam a través del cual la clave privada es almacenada en el móvil en un enclave seguro mientras que la clave pública es publicada en un registro distribuido.

4. Por último, el emisor recibe toda la información requerida junto con el DID de Sam y emite la tarjeta digital de Sam quien recibe la credencial verificable, que es un *JSON Web Token* (JWT) bajo el estándar W3C de credenciales verificables. El JWT incluye el DID del sujeto (Sam) y el DID del emisor (Una Universidad) así como el tipo de credencial y cualquier otra acreditación como nombre, apellido, carrera y fecha de graduación. También contiene una manera de saber el estatus de revocación de la credencial en el caso en que la credencial sea luego revocada por el emisor (Una Universidad). Esta credencial verificable está digitalmente firmada por el DID del emisor.

5. Una vez que el agente de usuario valida la credencial verificable recibida por Una Universidad, introduce esta tarjeta digital en la billetera digital de Sam quien ahora puede presentarla a organizaciones como la Aseguradora Ejemplo.

Presentación de credenciales verificables

1. Cuando Sam entra al sitio web de la Aseguradora Ejemplo en su móvil para recibir un descuento en el seguro para su vehículo, Sam cliquea el botón "Verificar Credenciales" del sitio web (que es un enlace profundo) o simplemente escanea un código QR generado por la Aseguradora Ejemplo. Esto genera una solicitud de presentación/verificación para Sam cuyo fin es verificar su estatus de ex alumno de Una Universidad. La solicitud describe el tipo de tarjeta(s) que Sam deberá presentar a la Aseguradora Ejemplo, como por ej. la tarjeta digital de ex alumno de Una Universidad. Dicha solicitud está digitalmente firmada por el DID del verificador que en nuestro caso es la Aseguradora Ejemplo. Esta solicitud de presentación puede incluir también los términos y condiciones de servicio de la Aseguradora Ejemplo.
2. Luego de que la firma de la solicitud es verificada por el agente de usuario, se presenta a Sam una interfaz de usuario en el agente de usuario que indica que la Aseguradora Ejemplo está solicitando permiso para ver la tarjeta de ex alumno de Sam de Una Universidad junto con un motivo, como por ej. la razón por la que la Aseguradora necesita verla (en este caso, para que Sam pueda recibir un descuento).
3. Una vez que Sam aprueba la solicitud mediante una acción biométrica, como el escaneo de su huella digital con su móvil, la respuesta de verificación, que es básicamente una presentación de una respuesta de credencial (también conocida como presentación verificable), es enviada a la Aseguradora Ejemplo. La respuesta está firmada digitalmente por la clave privada de Sam e incluye la credencial verificable emitida por Una Universidad a Sam que está alojada en un *JWT payload* (carga útil).
4. La Aseguradora Ejemplo intenta emparejar a la persona realizando la presentación de la credencial con el sujeto de la credencial verificable para asegurarse de que es en efecto Sam quien está presentándola a la Aseguradora Ejemplo y no otra persona. De esta forma, el DID de Sam está presente tanto en el *JWT payload* externo, ya que Sam está realizando la presentación de la credencial, como dentro del *JWT payload* alojado, ya que es el sujeto de la credencial verificable emitida por Una Universidad. Una vez que la Aseguradora Ejemplo confirma que el DID en la presentación se corresponde con el sujeto de la credencial emitida, Sam es autenticado por el sitio web de la Aseguradora Ejemplo así como autorizado para reclamar su descuento. Esto es mucho mejor que poseer un usuario y contraseña ya que mediante este mecanismo, la Aseguradora Ejemplo sabe que la persona presentando esta credencial es la misma persona a la que se le emitió la tarjeta. Con un sistema de usuario y contraseña, cualquier persona podría suplantar la identidad de Sam mientras que en este tipo de arquitectura es más complicado hacerlo: para poder usurpar su identidad, un usurpador tendría que tomar

control de la clave privada de Sam que está almacenada en el enclave seguro del móvil de Sam.

5. Por último, la Aseguradora Ejemplo puede extraer la información que necesita de la credencial verificable como el nombre de Sam, su apellido, su carrera, fecha de graduación, y puede ofrecer a Sam el descuento para el seguro de su vehículo.
6. El flujo de verificación de la credencial se completa cuando Sam almacena un recibo firmado digitalmente por la Aseguradora Ejemplo que estará asociado a la tarjeta en la billetera digital de Sam. Sam puede ahora ver en un único lugar todos los sitios web donde presentó su tarjeta de exalumno a lo largo del tiempo. En nuestro escenario, el recibo tiene información sobre la Aseguradora Ejemplo, como el motivo por el cual la Aseguradora Ejemplo necesitó recibir la tarjeta, los términos y condiciones bajo los cuales se presentó y la fecha en la que el recibo se generó. Este recibo firmado está asociado con la tarjeta de Sam en su billetera digital y será siempre propiedad de Sam.
7. Algunas implementaciones pueden también permitir que Sam revoque el acceso que la Aseguradora Ejemplo tiene a su tarjeta digital de ex alumno de Una Universidad. La Aseguradora deberá luego implementar las medidas de revocación correspondientes para ejecutar la solicitud de Sam. El verificador deberá entonces dejar de usar los datos de la tarjeta de Sam que le fue presentada. En caso de que sea necesario, Sam podría luego demostrar que emitió una solicitud de revocación lo cual favorece el cumplimiento de la Regulación General de Protección de Datos (GDPR, por sus siglas en inglés).

Resumen del escenario

En nuestro caso modelo sencillo, el emisor de una credencial verificable era Una Universidad pero en otros contextos, el emisor puede ser un empleador, una agencia de gobierno, un dispositivo, un programa residente (*daemon process*) o incluso el individuo. Del mismo modo, un verificador puede también ser cualquiera de los actores mencionados anteriormente. El ecosistema de identidad descentralizada es muy amplio y sus estándares ofrecen la posibilidad de desentrañar una forma más flexible, segura y que preserve mejor la privacidad en las interacciones digitales en una variedad de contextos.

Los componentes presentados en el flujo descrito anteriormente están basados en estándares abiertos. La emisión de credenciales verificables y los flujos de presentación dependen de las especificaciones fundacionales del Estándar de Credenciales Verificables W3C, y el sistema descentralizado, como cadenas de bloques o registros distribuidos, se basa en el trabajo de los Identificadores Descentralizados W3C. El objetivo de la tecnología de registro descentralizado es sustentar una infraestructura descentralizada de clave pública (dPKI). La dPKI ancla los DID a sus claves públicas permitiendo así que la propiedad de los DID sea validada sin tener que depender de unos pocos proveedores de identidad privilegiados o de autoridades de certificación.

La Fundación para la Identidad Descentralizada está al frente del trabajo sobre identidad descentralizada pero aún queda mucho por hacer.[3] Por ejemplo, la comunidad de la identidad descentralizada está discutiendo cómo permitir una mejor preservación de la identidad dándole el poder a Sam de presentar su edad de forma segura sin revelar innecesariamente su fecha de nacimiento exacta al verificador. También se está discutiendo cómo fortalecer a Sam para que pueda poseer una clave de recuperación propia en caso de que extravíe su móvil o que el mismo sufra daños, de modo que Sam pueda recuperar de forma sencilla todas sus tarjetas digitales previamente obtenidas y tenerlas en un nuevo dispositivo o en otro agente de usuario.

Las limitaciones de la identidad descentralizada

Si bien la identidad descentralizada tiene el potencial de mejorar la productividad de un individuo y de digitalizar procesos de negocio existentes de gobiernos y corporaciones, tiene limitaciones y áreas que requieren más investigación y profundización. Un ecosistema de identidad descentralizada solo puede ser exitoso si adquiere una masa crítica de uso por parte de gobiernos, negocios e individuos. Cuando Apple lanzó su primer iPhone, marcó el inicio de un cambio inmediato en la experiencia de usuario al momento en que el comprador tomaba posesión de su nuevo dispositivo. Por oposición, un individuo no podrá sacar gran beneficio de sus credenciales verificables otorgadas por un emisor a menos que puedan utilizarlas con varios verificadores. Por ejemplo, un pasaporte digital es útil únicamente si el ciudadano puede utilizarlo en la mayoría de las oficinas de migración de los aeropuertos del mundo. Las organizaciones pueden dudar sobre convertirse en emisores o verificadores de credenciales verificables a menos que ya haya un ecosistema saludable implementado, pero a su vez ese ecosistema no puede desarrollarse a menos que haya entidades dispuestas a emitir y verificar estas nuevas credenciales.

La identidad descentralizada es una identidad digital. Sin la tecnología necesaria para sostener una billetera digital, como un móvil o algún tipo de dispositivo informático, es muy difícil prometer el lanzamiento de la identidad digital para todos los individuos globalmente. Si un individuo pierde su dispositivo o decide compartir su dispositivo con otros sin las debidas precauciones, recuperar sus datos en un dispositivo diferente o demostrar quién realizó determinada acción puede ser un desafío. Esperar que una persona común entienda todo esto, así como proteger sus claves privadas, es aún uno de los grandes desafíos de la administración de claves descentralizadas.

En la mayoría de los casos modelo de identidad descentralizada, los desarrolladores asumen que todas las partes involucradas tienen acceso a Internet. Otros casos en los que el individuo no tiene acceso a Internet dejan abierta la pregunta de cómo se pueden verificar las credenciales verificables. La verificación de credenciales verificables requiere buscar la información en el dPKI. Cuando menos, verificar si una credencial presentada ha sido revocada

[3] Fundación para la Identidad Descentralizada (DIF, por sus siglas en inglés), [Online]. Disponible en: https://identity.foundation/.

requiere conectividad de red. En ambientes totalmente desconectados y offline, esto representa un desafío y un problema para la adopción de la identidad descentralizada en situaciones o contextos específicos.

La gran promesa de la identidad descentralizada es dar poder a los individuos para que sean propietarios y controlen su identidad digital y sus datos privados. Sin embargo, si una persona provee una credencial verificable que contiene datos personales al proveedor de servicio, el mismo podría copiar estos datos en sus propias bases de datos con fines de marketing o para poder continuar ofreciendo servicios a ese usuario. El individuo puede intentar revocar el acceso que el proveedor de servicio tiene a sus credenciales verificables, pero no hay garantías de que el proveedor de servicio obedecerá a la solicitud y eliminará todos los datos que tiene almacenados de este usuario. Esto genera un gran problema a resolver mediante medidas tecnológicas estrictas y requiere que haya marcos legales y de política implementados para garantizar que los datos personales de todos están protegidos, para asegurar que se conservan registros de auditoría y para establecer un proceso documentado para la gestión y resolución de disputas.

Palabras Finales

La identidad descentralizada abre un abanico de posibilidades para que nuevos negocios prosperen y otorga a los ciudadanos el control sobre sus identidades y datos personales. Actualmente, los administradores TI se ven obligados a realizar intercambios de claves criptográficas para establecer un marco de confianza entre dos entidades. Esto no escala cuando se realizan transacciones con decenas o cientos de otros negocios de forma ad-hoc. Hoy en día cuando un banco emite una tarjeta de crédito a un cliente, ese cliente puede hacer compras con prácticamente cualquier comerciante del mundo. En ese escenario, no es viable que cada comerciante intercambie claves criptográficas con cada banco que haya emitido una tarjeta de crédito. Un ecosistema de identidad descentralizada funcionaría de forma similar al de las tarjetas de crédito, introduciendo autoridades de gobernanza e infraestructuras para varias comunidades fiables en una amplia gama de industrias verticales. Como resultado, los comerciantes u otros verificadores evitarían tener que establecer múltiples federaciones de confianza: sencillamente solicitarían al emisor que presente pruebas adicionales que demuestren que el emisor es en efecto miembro de una autoridad de gobernanza específica con la cual el verificador ya tiene una relación de confianza establecida.

Uno de los mayores inconvenientes para implementar una cadena de bloques o registro distribuido en las empresas hoy en día es la falta de infraestructuras de identidad descentralizada. Después de todo, no tiene mucho sentido tener una red descentralizada de registro distribuido si todas las identidades que están allí dependen de cuentas controladas de forma centralizada. En un ecosistema de identidad descentralizada, los consumidores pueden rastrear más fácilmente qué sitios web visitan y con quién realizan transacciones. Pueden saber qué negocios tienen sus datos personales y podrían revocarles el acceso si así lo quisieran. En

lugar de compartir documentos en papel o tarjetas físicas, podrían compartir documentos y tarjetas de forma totalmente digital, que preserve su privacidad y que se puedan auditar. Esto reduce los riesgos asociados al Reglamento General de Protección de Datos (GDPR) para las organizaciones, ya que los datos personales estarían almacenados en el *hub* de identidad que está bajo control del individuo, mientras que la organización solo tendría acceso a los datos específicos otorgados por el usuario. Asimismo, el individuo puede revocar el acceso a sus datos lo cual facilita el cumplimiento del Reglamento General de Protección de Datos (GDPR) por parte de la organización y simplifica dichas solicitudes para el individuo. Asimismo, las organizaciones tendrían pruebas criptográficas que demuestran que el individuo les proveyó los datos específicos en cuestión.

Como se ha mencionado anteriormente, una billetera digital contiene un agente digital mediante el cual el usuario interactúa. En la mayoría de los casos, estos agentes digitales o agentes de usuario están basados en software abierto. El individuo puede descargar un usuario de agente de una corporación comercial o de una entidad gubernamental. Un individuo puede incluso desarrollar su propio agente de usuario a partir de software abierto preexistente. Conceptualmente, el individuo debe confiar en su agente de usuario y debe estar bajo su control.

Si bien es difícil predecir la evolución del panorama de la identidad descentralizada dado su estado prematuro, las tendencias actuales indican que los gobiernos están interesados en aliviar la carga que enfrentan los ciudadanos y negocios mediante tarjetas digitales emitidas por el gobierno. La pandemia del COVID-19 instó a los gobiernos a facilitar el acceso a servicios gubernamentales tanto para los ciudadanos como para los negocios. Asimismo, los requisitos cada vez mayores y estrictos del cumplimiento de las normas regulatorias, así como el reclamo de los individuos de tener experiencias de usuario mejores y más cómodas, impulsan la implementación de identidades digitales mediante el intercambio de credenciales verificables. Por último, las credenciales verificables son muy útiles a la hora de tener que presentar la misma credencial tanto para transacciones digitales como en interacciones personales dado que resultan en experiencias más eficientes para los negocios, así como más consistentes y sencillas para los usuarios.

Conclusión

La identidad descentralizada representa un cambio conceptual respecto a la manera en que la identidad y la administración del acceso ha sido abordada en el pasado y puede coexistir con el modelo de identidad basado en cuentas que ha existido durante décadas. La identidad descentralizada aporta un cambio significativo en las transacciones que requieren de un elevado nivel de confianza para tomar decisiones de autorización. Por otra parte, el hecho de que un individuo utilice el método de cuentas tradicional para autenticarse ante un sitio web no significa que no pueda también tener credenciales verificables para, por ejemplo, transferir una gran cantidad de dinero a otro individuo o a una organización. Esto habilita un sinfín de nuevas oportunidades para el comercio digital y permite que los consumidores, empleados y

ciudadanos del mundo entero puedan realizar transacciones en la web de forma más segura y que preserve su privacidad. Abre el camino para que las billeteras digitales con tarjetas digitales se utilicen de la misma forma que utilizamos las billeteras y tarjetas físicas hoy en día. Las credenciales verificables son sencillas de usar ya que son simplemente la representación digital de las tarjetas que llevamos en nuestros bolsillos cada día.

Nos encontramos todavía en los albores de la identidad descentralizada y no es una tecnología que una única empresa pueda lanzar al mercado sin más. Requiere estándares y la colaboración entre el sector público y privado para tener un ecosistema saludable de *emisores, titulares* y *verificadores*. Cuando se alcance una masa crítica que la adopte, las experiencias digitales podrán verse y sentirse muy diferentes a las de hoy en día. La identidad descentralizada es un avance fascinante del campo de la identidad digital y tiene el potencial de ofrecer experiencias digitales más confiables y generar valor para todos.

Registro de cambios

Fecha	Cambio
30-10-2020	V1 publicada
28-02-2022	Cambios editoriales únicamente (se cambiaron los nombres de los negocios-ejemplo por nombres no utilizados por Microsoft)

Biografía del autor

Leo Sorokin tiene más de 10 años de experiencia en soluciones de arquitectura y arquitectura de roles de negocios en grandes organizaciones de los sectores financieros, manufactureros y de software. Actualmente es Arquitecto de Soluciones en la Nube en Microsoft, colaborando con las organizaciones canadienses más importantes en la adopción de tecnología en la nube. Leo cuenta con amplia experiencia en identidad, arquitectura orientada al servicio, integración de aplicaciones, aplicaciones en la nube y arquitectura híbrida de nube, así como en arquitectura de software de seguridad. Leo es también un TOGAF® 9 Certificado, un Arquitecto de Soluciones Azure Certificado por Microsoft y es diplomado en informática de la Universidad de York. También ha impartido cursos de tecnología en diversas instituciones educativas.