Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1403

(09/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad (2) – Seguridad de tecnología de libro mayor distribuido

Directrices de seguridad para la utilización de la tecnología de libro mayor distribuido en la gestión descentralizada de identidades

Recomendación UIT-T X.1403

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	**X.1400–X.1429**
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1403

Directrices de seguridad para la utilización de la tecnología de libro mayor distribuido en la gestión descentralizada de identidades

Resumen

La tecnología de libro mayor distribuido (DLT) y sus aplicaciones específicas, como las cadenas de bloques, ofrecen una oportunidad sin precedentes para utilizar una infraestructura fiable y una plataforma que puede ser útil para facilitar una federación de confianza para el intercambio de atributos e información de identidades. En la Recomendación UIT-T X.1403 se exponen consideraciones relativas a la privacidad y la seguridad específicas de las telecomunicaciones para la utilización de los datos de DLT en la gestión de identidades.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1403	03-09-2020	17	11.1002/1000/14264

Palabras clave

Gestión de identidades, tecnología de libro mayor distribuido.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1403

Directrices de seguridad para la utilización de la tecnología de libro mayor distribuido en la gestión descentralizada de identidades

1 Alcance

La tecnología de libro mayor distribuido (DLT) proporciona una infraestructura fiable que resulta útil para crear sistemas descentralizados de gestión de identidades destinados al intercambio de atributos e información de identidades.

En la presente Recomendación se describe una visión general de la utilización de la DLT para la gestión descentralizada de identidades. El alcance es el siguiente:

– breve reseña de la utilización de los libros mayores distribuidos para la gestión de identidades y datos de identidades;

– análisis sobre las ventajas de la descentralización de identidades para la seguridad; y

– orientación relativa a los controles necesarios que deben imponerse para mitigar las amenazas a los datos de identidades.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad*.

[UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autentificación de entidad*.

[UIT-T X.1277] Recomendación UIT-T X.1277 (2018), *Marco de autentificación universal*.

[UIT-T X.1278] Recomendación UIT-T X.1278 (2018), *Cliente del protocolo autentificador/marco bifactor universal*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 declaración (*claim*) [UIT-T X.1252]: Formular una declaración, sin estar en condiciones de aportar pruebas.

3.1.2 credencial (*credential*) [UIT-T X.1252]: Conjunto de datos presentado como demostración de una identidad y/o unos derechos declarados.

3.1.3 documento DID [b-W3C-2]: Conjunto de datos que describen al titular del DID, que comprende mecanismos, como claves públicas y datos biométricos pseudónimos, que el titular del DID puede utilizar para autentificarse y demostrar su titularidad del DID.

3.1.4 entidad (*entity*) [UIT-T X.1252]: Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

3.1.5 federación (*federation*) [UIT-T X.1252]: Una asociación de usuarios, proveedores de servicios y proveedores de servicios de identidad.

3.1.6 proveedor de servicios de identidad (IdSP) (*identity service provider*) [UIT-T X.1252]: Entidad que verifica, mantiene, gestiona y puede crear y asignar información relativa a la identidad de otras entidades.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 identificador descentralizado (DID): Identificador único global que no requiere una autoridad central de registro porque emplea la tecnología de libro mayor distribuido (DLT) u otro tipo de sistema descentralizado.

NOTA – Basado en la definición de [b-W3C-2].

3.2.2 titular del DID: Entidad a la que se refiere el documento DID. Es decir, entidad identificada por el DID y descrita por el documento DID.

NOTA – Basado en la definición de [b-W3C-2].

3.2.3 portaclaves: Se refiere a la tarea de proteger el almacenamiento de claves privadas y datos en una unidad física fiable de un dispositivo.

3.2.4 extremo del servicio: Dirección de libro mayor distribuida en la que un servicio opera en nombre de un titular de DID. Entre los ejemplos de servicios específicos figuran los servicios de detección, las redes sociales, los servicios de almacenamiento de archivos y los servicios de depósito de declaraciones verificables. Los extremos del servicio también pueden proporcionarse mediante un protocolo de intercambio de datos generalizado, como el intercambio de datos extensible.

NOTA – Basado en la definición de [b-W3C-2].

3.2.5 marco de confianza: Conjunto de especificaciones, normas y acuerdos jurídicamente vinculantes que rigen un sistema de identidades.

3.2.6 cartera (cartera de identidad): Aplicación que permite principalmente al usuario ser titular de identificadores y credenciales mediante el almacenamiento de las correspondientes claves privadas en el dispositivo de usuario.

3.2.7 prueba de conocimiento cero: Prueba que utiliza una criptografía especial y un secreto maestro para permitir la divulgación selectiva de información en un conjunto de declaraciones. La prueba de conocimiento cero demuestra la veracidad de algunos o todos los datos de un conjunto de declaraciones sin revelar ninguna información adicional, incluida la identidad del verificador.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las siguientes abreviaturas y acrónimos:

DDO Documento DID (*DID document*)

DID Identificador descentralizado (*decentralized identifier*)

DIdAm Gestión descentralizada de identidades y accesos (*decentralized identity and access management*)

DLT Tecnología de libro mayor distribuido (*distributed ledger technology*)

IdAM Gestión de identidades y accesos (*identity access and management*)

IdSP Proveedor de servicios de identidad (*identity service provider*)

PKI Infraestructura de claves públicas (*public key infrastructure*)

PII Información de identificación personal (*personally identifiable information*)

RP Parte que confía (*relying party*)

SAML Lenguaje de marcaje de aserción de seguridad (*security assertion markup language*)

SSI Identidad autosoberana (*self-sovereign identity*)

SSO Inicio de sesión único (*single sign on*)

TI Tecnología de la información

URL Localizador uniforme de recursos (*uniform resource locator*)

5 Convenios

La presente Recomendación aplica las siguientes formas verbales de expresión del grado de obligatoriedad de las disposiciones:

a) el futuro de obligación "deberá" se utiliza para los requisitos;

b) el verbo modal "debe" se utiliza para recomendaciones;

c) el condicional "podría" indica que se da permiso;

d) el "puede" indica posibilidad y capacidad.

6 Hacia una identidad digital descentralizada

La tecnología de libro mayor distribuido desempeña un papel fundamental en la evolución y la consolidación de los sistemas de identidades descentralizados.

La proliferación de los dispositivos móviles y de la Internet de las cosas aumenta la presión sobre los sistemas tradicionales de gestión de identidades y accesos (IdAM) para que evolucionen hacia plataformas dinámicas e inteligentes capaces de dar soporte a sistemas móviles y basados en la nube.

Los sistemas tradicionales de gestión de identidades se fundamentan en autoridades centralizadas, por ejemplo, servicios de directorio empresariales, autoridades de certificación o registros de nombres de dominio. Cada una de estas autoridades centralizadas actúa como sus propios dominios de confianza. En un sistema IdAM tradicional, la autoridad centralizada podría constituir el punto débil global. La federación de identidades [UIT-T X.1252] surgió como una solución provisional que permite a los sistemas IdAM funcionar en distintos sistemas con diferentes organizaciones controlando cada una su dominio.

La aparición de la DLT ofrece una oportunidad para la creación de soluciones descentralizadas de gestión de identidades y accesos (DIdAm). La DLT ofrece la posibilidad de una gestión de la confianza sin una autoridad centralizada, evitando así cualquier punto de fallo único. Además, la DLT permite a cualquier entidad crear y gestionar sus propios identificadores mediante un número cualquiera de libros mayores distribuidos.

Los modelos de identidad digital han ido evolucionando para satisfacer las cambiantes necesidades de las empresas. Hay tres modelos de identidad básicos, que se describen a continuación en la cláusula 6.

6.1 Modelo centralizado de gestión de identidades

Este es el modelo de identidad digital más antiguo y actualmente el más utilizado [UIT-T X.1252]. En un modelo de identidad centralizado, las organizaciones actúan como proveedores de servicios de identidad (IdSP). En este modelo, la organización establece una relación de confianza punto a punto con cada uno de sus usuarios. Este es el modelo tradicional aislado, en el que cada organización expide credenciales para sus usuarios que les permite acceder a los servicios de esta organización.

En este modelo cada organización actúa como un IdSP. La organización gestiona la identidad digital del usuario y decide las relaciones de confianza aceptadas. La confianza entre el usuario y el IdSP se suele establecer mediante secretos compartidos, como un nombre de usuario y una contraseña. En algunos casos, los secretos compartidos se complementan con autentificaciones multifactor, como dispositivos físicos, biométricos o soluciones basadas en FIDO [UIT-T X.1277] y [UIT-T X.1278].

En el modelo centralizado, el IdSP puede almacenar y recopilar datos sobre los usuarios. Los datos pueden monetizarse, compartirse o venderse a otras partes dependiendo del modelo comercial del proveedor de servicios de identidad (IdSP). Los usuarios tienen que confiar en que el IdSP hará lo correcto en lo relativo a la gestión de sus datos. Aunque los usuarios finales se benefician de los servicios de la organización, en la mayoría de los casos no tienen control alguno sobre la gestión de sus propias identidades, datos personales o sus atributos de identidad personal. En este modelo, el IdSP es el propietario de la identidad de los usuarios. Los usuarios no tienen la posibilidad de transferir sus datos a otros proveedores.

El modelo de identidad centralizada requiere que el usuario cree y administre credenciales separadas para cada una de sus relaciones comerciales con cada IdSP. Cada organización requiere la creación de dichas credenciales antes de permitir al usuario acceder a sus recursos. Este modelo abruma al usuario con muchas identidades en línea. La falta de autenticación mutua en el momento del inicio de sesión hace que este modelo sea vulnerable a los ataques de *peska* y de *kosecha* de credenciales. El modelo insta al usuario a reutilizar las contraseñas, con los consiguientes riesgos y vulnerabilidades de seguridad.

El modelo centralizado impone una carga al IdSP en lo que respecta a la gestión del ciclo de vida de la identidad. En particular, el modelo exige que cada IdSP realice una verificación de identidad [UIT-T X.1254] durante la fase de inscripción de la identidad en la gestión del ciclo de vida de la identidad. La verificación de la identidad es necesaria para establecer un nivel de confianza en la identidad declarada. Este proceso puede repetirse durante todo el ciclo de vida de la identidad. Este paso es problemático desde la perspectiva del usuario, ya que el modelo centralizado requiere que el usuario pase por la etapa de verificación de la identidad por separado con cada proveedor de identidad. Además, la amenaza de filtración de datos aumenta los riesgos de apropiación de la cuenta debido a que las organizaciones dependen de registros de datos centralizados que son el blanco habitual de piratas informáticos.

6.2 Modelo federado de gestión de identidades

Las organizaciones han reparado en las limitaciones inherentes al modelo de identidad centralizado, descrito en la cláusula 6.1 y han elaborado un modelo federado de gestión de identidades para resolver esos problemas. El modelo federado tiene por objeto reducir los inconvenientes para el usuario al permitirle utilizar su identidad de un dominio en otro dominio. El lenguaje de marcaje de aserción de seguridad (SAML) [Rec. UIT-T X.1242] resulta más conveniente para las personas por cuanto dispone de la funcionalidad de inicio de sesión único (SSO).

Los sistemas federados de gestión de identidades pueden proporcionar capacidades de autentificación y autorización más allá de los límites de las organizaciones y sistemas. A tal efecto, es preciso establecer acuerdos comerciales y de confianza para que la identidad de un usuario de un proveedor sea reconocida por otros proveedores (miembros de la federación). En general, un acuerdo de confianza incluye también un acuerdo contractual sobre la propiedad de los datos, la utilización de la información de identificación personal (PII) y la conformidad [UIT-T X.1242].

El modelo federado resulta ventajoso para el usuario, ya que el proveedor de servicios de identidad suele proporcionar la función de inicio de sesión único. Así, se reduce el número de credenciales independientes que el usuario necesita adquirir y mantener. En este modelo, las partes que confían integrantes de la federación, incluidos sus usuarios, dependen de la disponibilidad de los servicios de un determinado IdSP y de su voluntad de permanecer en la federación.

Al igual que en el modelo centralizado, la autentificación en el modelo de federación no es mutua y adolece de idénticas limitaciones.

6.3 Modelo descentralizado de gestión de identidades

La identidad descentralizada podría implementarse utilizando la DLT u otras tecnologías emergentes basadas en normas como las declaraciones verificables [b-W3C-1] y los identificadores descentralizados (DID) [b-Sovrin], [b-W3C-1] y [b-W3C-2]. El modelo de identidad descentralizado puede basarse en un libro mayor distribuido (DLT) y en la relación entre el usuario y la organización [b-Sovrin] y [b-W3C-17]. En este modelo, el usuario y la organización son homólogos.

La identidad descentralizada permite a los usuarios asumir el control y la propiedad de sus identidades. El grado de propiedad puede variar según el modelo descentralizado. En particular, en el modelo de identidad autosoberana (SSI) se supone que las entidades podrían tener el control de su propia identidad digital.

En la actualidad, la mayoría de las soluciones de gestión de identidades admiten un limitado control de la identidad, la transparencia y la portabilidad, ya que esas soluciones las ofrecen proveedores de identidades con sistemas propietarios. Es posible que en un futuro próximo exista un sistema de gestión de identidades que cumpla plenamente un modelo SSI, pero ello no es óbice para excluir la necesidad de definir sus principios fundamentales conforme se indica en las cláusulas 6.3.1 y 6.3.2. En la cláusula 7 se examina más a fondo cómo utilizar la DLT para la gestión descentralizada de identidades.

6.3.1 Identificadores descentralizados

Los DID [b-W3C-2] son un tipo de identificador para sistemas verificables y descentralizados de gestión de identidades. El formato del DID permite estar bajo el control del titular del DID, lo que los hace independientes de cualquier registro centralizado, proveedor de identidad o autoridad de certificación. Los DID son localizadores uniformes de recursos (URL) que establecen la relación entre el titular del DID y medios con los que dicho titular puede efectuar interacciones fiables. Los elementos normalizados de un documento DID (DDO) [b-W3C-2] son:

1) DID (para autodescripción);
2) Serie de claves públicas (para verificación);
3) Conjunto de protocolos de autenticación (para la autenticación);
4) Conjunto de extremos del servicio (para la interacción);
5) Sello de tiempo (para el historial de la auditoría);
6) Firma (por integridad).

La tarea de resolver un DID [b-W3C-2] culmina en un DDO, que es un documento simple en el que se describe cómo utilizar ese DID concreto. Cada documento DID contiene por lo menos tres elementos: material criptográfico, conjuntos de autenticación y extremos de servicio. El material criptográfico combinado con los conjuntos de autenticación proporciona una serie de mecanismos para autentificar al titular DID (el usuario que es el titular de DDO). Ejemplos de opciones de autentificación son las claves públicas y los protocolos biométricos pseudónimos. Los extremos de servicio permiten la comunicación fiable con el sujeto DID.

Para utilizar el DID [b-W3C-2] con un libro mayor distribuido concreto es preciso definir un método DID. La especificación del método DID puede basarse en [b-RFC 8141]. El método DID especifica el conjunto de reglas que rigen la forma de registrar, resolver, actualizar y revocar un DID en una DLT específica. Todos los DID se especifican y resuelven en un libro mayor distribuido.

La utilización del DID basado en la DLT [b-W3C-2] reduce la dependencia de los registros centralizados para los identificadores, así como de las autoridades de certificación centralizadas para la gestión de las claves. Como los DID residen en un libro mayor distribuido, cada entidad puede servir como su propio dominio de confianza, lo que da lugar a una infraestructura de confianza descentralizada. De esta manera se crea un puente de interoperabilidad entre los mundos de identificadores centralizados, federados y descentralizados.

El DID consta de un par de claves criptográficas públicas y privadas [b-W3C-2]. La propiedad del DID se demuestra aplicando algoritmos criptográficos basados en una clave privada, que sólo el propietario del DID debe poseer. Por consiguiente, los DID pueden publicarse, modificarse, consultarse o suprimirse. Dado que cada DLT puede implementar su propio método DID, en la práctica habrá diferentes implementaciones de las operaciones "crear, leer, actualizar y borrar" (en inglés, *CRUD*) para el DID.

6.3.2 Credenciales verificables

La credencial verificable [b-W3C-1] resuelve el problema del intercambio de credenciales, como la licencia de conducir, justificante de edad, titulación educativa y datos sanitarios, por medio de una red de comunicación de una manera que sea verificable y que, a la vez, proteja la PII individual. En este planteamiento, las credenciales están compuestas por afirmación denominadas declaraciones verificables. Las declaraciones verificables [b-W3C-1] son útiles cuando una entidad necesita probar, por ejemplo, que:

- tiene más de una cierta edad;
- es capaz de conducir un vehículo motorizado particular;
- requiere un medicamento en particular;
- está formado y certificado como electricista;
- dispone de licencia profesional para ejercer la medicina;
- tiene autorización para viajar al extranjero.

El ecosistema de credenciales verificables está compuesto por cuatro funciones primarias:

1) El expedidor, que expide las credenciales verificables sobre un tema específico.
2) El portador, quien guarda las credenciales en nombre del titular. El portador suele ser también el titular de la credencial.
3) El verificador, que solicita un perfil del sujeto. El perfil contiene el conjunto específico de credenciales. El verificador confirma que las credenciales proporcionadas en el perfil son adecuadas para el fin previsto.
4) El registro de identificadores, que es el mecanismo utilizado para expedir identificadores para los titulares.

La declaración [b-W3C-1] es una afirmación sobre un titular, expresada como la relación titular-propiedad-valor. Las declaraciones pueden fusionarse para expresar un gráfico de información sobre un sujeto determinado.

Cuando un expedidor envía datos a un portador, agrupa el conjunto de declaraciones en una estructura de datos denominada credencial y firma digitalmente dicha estructura [b-W3C-1]. Cuando un verificador solicita datos a un portador, éste suele agrupar el conjunto de credenciales en una estructura de datos denominada perfil y firma digitalmente dicha estructura [b-W3C-1].

7 Identidad descentralizada mediante DLT

La identidad descentralizada puede concebirse como una identidad vinculada a una DLT. Según este planteamiento, la prueba de conocimiento cero [b-W3C-1] permite relacionar identidades de manera universalmente descubrible. La identidad descentralizada permite al usuario probar su identidad una sola vez a un tercero de confianza y almacenar la prueba de su identificador en una DLT. La DLT actúa como la caja fuerte fiable para la identidad. La DLT ofrece servicios de infraestructura de identidad para dar soporte, entre otras cosas, a las comunicaciones punto a punto, servicios de infraestructura de claves públicas (PKI) basados en la DLT y protocolos de intercambio de declaraciones verificables.

La identidad descentralizada permite a los usuarios acceder a los servicios mediante un proceso sencillo. Por ejemplo, el usuario interactúa con un IdSP que a su vez utiliza una DLT para crear el DID del usuario que apunta a una ubicación DLT que el usuario puede utilizar. Este paso es transparente para el usuario final y equivale a crear un par de claves privadas y públicas para el usuario. La clave privada se almacena con el usuario en algún tipo de cartera digital. La clave pública correspondiente se almacena en la DLT. La clave pública actúa como identificador de la cartera (denominada también identidad del usuario en la DLT) y se guarda en el libro mayor de forma segura. Como parte de los servicios que ofrece la DLT, los expedidores DLT pueden expedir y firmar declaraciones para determinado usuario y facilitárselas al usuario. Estas reclamaciones pueden almacenarse en la cartera del usuario.

En este modelo, el usuario puede acceder a un servicio presentando su identificador a un proveedor de servicios en la forma de un testigo. El proveedor de servicios verifica la identidad comparando los valores generadores (*hash*) de los identificadores con sus correspondientes registros generadores que se almacenan en la DLT. El proveedor de servicios concede o rechaza el acceso en función del resultado de la verificación.

7.1 Inicialización de la cartera

El estudio en [b-Sovrin] y [b-W3C-1] proporciona un ejemplo de interacciones para el servicio basado en identidades. El usuario decide interactuar utilizando los servicios de identidad descentralizados de un sistema fiable de identidades basado en la DLT. A este respecto, la DLT presta servicios para que el usuario final pueda establecer un DID y una relación con el libro mayor. La tarea de establecer el DID para el usuario concluye guardando la dirección de libro mayor para ese usuario y creando pares de claves públicas y privadas para interactuar con el usuario. El libro mayor también puede prestar servicios que pueden utilizarse para crear el documento DID y establecer los enlaces a los documentos necesarios, conforme a lo especificado por el usuario. El libro mayor proporciona servicios básicos de identidad que permiten a los servicios descubrir cómo interactuar con la cartera del usuario a fin de hacer consultas sobre las declaraciones disponibles bajo el control del usuario.

El acto de crear un DID en el libro mayor conduce a la creación de la cartera que utilizará el usuario para presentar reclamaciones verificadas a la parte que confía (RP). La cartera contiene las claves privadas, las claves públicas y otros perfiles de identidad del usuario, conforme a lo previsto por el método DID. Recurriendo a técnicas de conocimiento cero [b-Sovrin] se garantiza que las declaraciones puedan verificarse preservando la PII y en consonancia con la actual utilización de las credenciales y documentos tradicionales en papel. Por ejemplo, un usuario puede demostrar su edad con un permiso de conducir en un establecimiento sin necesidad de que la autoridad emisora del permiso de conducir participe en la transacción. La cartera puede ser una cartera virtual en la que una parte de la cartera se encuentra en el dispositivo móvil del usuario y otra parte en la nube. Esta configuración permite crear agentes que actúen en nombre del usuario y presten servicios sin necesidad de que éste participe directamente.

El proceso consta de las siguientes etapas:

1) Registro de DID: el usuario descarga la cartera asociada al proveedor de servicios DLT y registra su DID en el libro mayor. La DLT genera los pares de claves privadas y públicas asociadas a la cartera de identidad. Se crea una dirección y se almacena en la DLT durante el proceso de registro.

2) Inicialización de la identidad: para que una DLT se utilice en sistemas descentralizados de gestión de identidades, se supone que existe un marco de confianza que especifica la lista de servicios de identidad disponibles para los participantes. A este respecto, el usuario puede confiar en la disponibilidad de un expedidor (parte fiable) que pueda validar la identidad de los usuarios. Inicialmente, los usuarios pueden comenzar con declaraciones autoaseveradas. Luego, el usuario puede aprovechar las declaraciones iniciales de su cartera para reunir declaraciones adicionales de múltiples proveedores a fin de incluirlas en su cartera y mejorar la validez de su identidad dentro del sistema. Toda relación está protegida por un DID mutuo entre el expedidor, el titular (usuario) y el verificador.

3) Verificación: si un titular (usuario) desea acceder a un servicio ofrecido por una parte que confía (RP), el verificador de la RP solicitará al usuario que le dé acceso a las declaraciones disponibles en su cartera. El verificador consultará entonces con la DLT para validar las declaraciones firmadas utilizando las claves públicas correspondientes al DID, tal como se indica en la transacción. El sistema supone que la cartera es fidedigna en cuanto al conocimiento de las claves privadas del titular. Supone además que se ha producido una autentificación adecuada para garantizar que el propietario legítimo de la cartera es realmente la entidad que está efectuando la transacción.

4) Validación de la declaración: la parte dependiente utiliza las declaraciones proporcionadas por la cartera para verificar la identidad y el atributo del usuario mediante la firma DLT PKI y las técnicas de validación basadas en valores generadores.

5) Autorización: la parte dependiente determina los servicios a los que se puede acceder en función del resultado de las verificaciones de identidad.

7.2 Resolución DID y autentificación

El concepto DID [b-W3C-2] puede facilitar la creación de mecanismo resolutivo universal [b-DIF] para cualquier DID. Este mecanismo resolutivo universal puede participar en la capa de autentificación DID interoperativo. La autentificación del DID permite al titular de la identidad tomar control del DID cuando interactúa con una RP. Para ello, ésta ha de ejecutar las siguientes etapas:

1) La parte que confía resuelve el DID del titular de la entidad en una DLT a un documento DID.

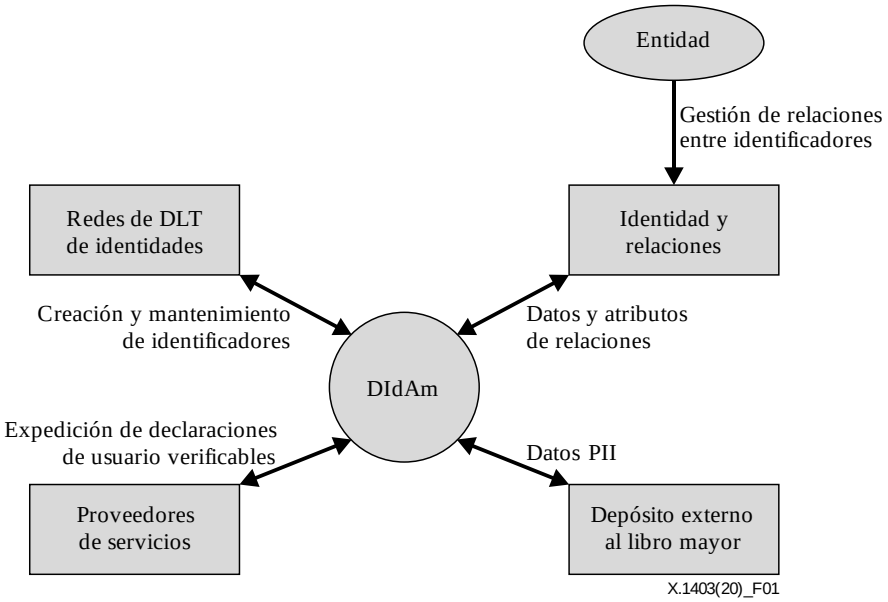
2) La parte que confía trata de autentificar al titular de la identidad utilizando objetos de autentificación contenidos en el documento DID en la DLT.

3) Los objetos de autentificación pueden incluir o remitir a objetos de clave pública, en casos en los que la prueba del titular de la identidad se establece mediante una firma criptográfica.

7.3 Ventajas de utilizar la DLT para el sistema de gestión descentralizada de identidades y accesos (DIdAm)

La utilización de la DLT como marco de confianza para los sistemas descentralizados de gestión e identidades allana el camino para que los proveedores diseñen marcos que les permitan actuar como una capa de abstracción intermedia entre el usuario y diversos libros mayores. Para poder efectuar estas interacciones, es indispensable que los sistemas tradicionales de gestión de identidades y accesos establezcan un marco adecuado que de soporte a los sistemas descentralizados. Básicamente, la fusión de los sistemas centralizados y descentralizados puede denominarse sistema de gestión descentralizada de identidades (DIdAm) [b-Angelov et al.]. A este respecto, un DIdAm [b-Angelov

et al.] es un sistema de sistemas que puede interactuar con muchas DLT que dan soporte a modelos de identidad descentralizados basados en DID. Esto se representa en la Figura 1.



DIdAm: Sistema de gestión descentralizada de identidades y accesos

Figura 1 – Marco de DIdAm

Los componentes de DIdAm que utilizan la DLT son los siguientes:

1) Propietario de identidades descentralizadas: entidad que gestiona sus identidades descentralizadas utilizando los servicios ofrecidos por la DIdAm en múltiples libros mayores.
2) Proveedores de servicios (SP): los expedidores que ofrecen servicios a los propietarios de identidades (identidad de inicialización). Por ejemplo, organismos gubernamentales como el departamento de vehículos motorizados o empresas privadas como instituciones financieras.
3) Depósito de identidad externa al libro mayor: se trata de una base de datos en la que se almacenan los atributos de identidades del usuario, las declaraciones y la información general. El usuario tiene el control del lugar donde deben almacenarse los datos. Normalmente se trata de datos sensibles PII y deben almacenarse fuera del libro mayor. El depósito debe proporcionar la capacidad de leer y escribir los datos a discreción del usuario.
4) Los sistemas de identidades basados en la DLT pueden considerarse sistemas de identidades independientes con diferentes límites de confianza y claves de criptografía. Por lo tanto, la DIdAm debe facilitar la interacción entre los libros mayores en nombre del usuario.

Los servicios DIdAm puede prestarlos internamente la empresa o por algún tercero.

7.3.1 Soporte de identidades descentralizadas a través de múltiples libros mayores DLT

A fin de poder dar soporte a las identidades descentralizadas utilizando DID a través de múltiples DLT es necesario que la interfaz cumpla muchos requisitos [b-Angelov et al.]. La dificultad surge debido a que requisitos del marco de confianza son diversos en función de, por ejemplo, el tipo de DLT, público o privado, etc. El sistema DIdAm debe poder dar soporte al usuario independientemente de las preferencias del usuario en cuanto al tipo de red de acceso utilizado. En la Figura 1 se muestra la DIdAm actuando de interfaz unificada para el propietario de la identidad, pudiendo operar en múltiples libros mayores.

El sistema DIdAm [b-Angelov et al.] actúa como una capa de abstracción para el usuario final. Permite al usuario interactuar con muchas DLT utilizando una única interfaz virtual. El DIdAm también actúa como capa de abstracción para la empresa, cuyos sistemas IdM tradicionales pueden interactuar con el DIdAm para funciones internas IdM centralizadas. Esta abstracción presenta la ventaja de que el usuario puede gestionar identidades en cualquier número de libros mayores, permitiéndole crear relaciones con los proveedores y tener un mejor control sobre su identidad.

7.3.2 Soporte de servicios de identidades

En los sistemas IdAm tradicionales, el proveedor de servicios de identidad puede dar fe de la identidad de un usuario a una parte que confía. El sistema DIdAm [b-Angelov et al.] debe poder dar soporte a esta función en particular para mantener la compatibilidad con los sistemas tradicionales. Las siguientes acciones pueden dar soporte a la necesidad de atestación:

1) El sistema DIdAm debe actuar como un asociado de confianza. Debe asegurarse de que el propietario de la identidad adquiera asertos precisos y válidos mediante procedimientos de declaración correctos y verificables para los expedidores.
2) Reducir la frustración relativa a la verificación de la identidad para los usuarios. Por lo general, el usuario tendrá que pasar por una etapa de verificación de la identidad con cada expedidor. Diseñar debidamente el sistema DIdAm puede ayudar al usuario a superar esta limitación al convertirse en un participante activo y de confianza en la interacción.
3) Validación de datos en tiempo real. La inexactitud de los datos es un problema en los sistemas tradicionales. Este problema puede resolverse mediante la DIdAm gracias a la oferta de servicios que ayuden a las partes que confían a determinar que los atributos del usuario no han quedado obsoletos.
4) Gestión del consentimiento. El consentimiento es una parte inherente a la conformidad. El DIdAm puede ofrecer servicios a los usuarios y a las partes que confían para garantizar que se tenga en cuenta la conformidad del consentimiento.

7.3.3 Gestión de portaclaves

El término portaclaves se refiere a la tarea de proteger el almacenamiento de las claves privadas relacionadas con una cartera en el dispositivo del usuario. Existe una correspondencia directa biunívoca entre el DID, la credencial verificable y el proveedor de servicios. El dispositivo puede ser un dispositivo móvil o un dispositivo con navegador. En el este modelo de seguridad actual, el acceso a las claves privadas se utiliza para validar la identidad del usuario. La tarea de proteger los pares de claves es crucial para impedir ataques por fraude de identidad. Al tener que manejar múltiples DID a través de muchas DLT, los usuarios tienen que proteger un conjunto de claves privadas que se utilizan para desbloquear sus identidades en todo el espacio identitario.

El portaclaves es la estructura en la que se almacenan de forma segura las claves privadas correspondientes a los DID del usuario. Es una estructura que pertenece al propietario de la identidad y que controla las claves privadas, lo que se traduce en la propiedad de los DID. Los sistemas DIdAm deben ser capaces de gestionar el portaclaves en nombre del usuario. En particular:

1) el usuario debe poder utilizar la funcionalidad del portaclaves y el almacenamiento mientras se encuentra dentro del dominio de la DIdAm;
2) la gestión de las claves debe estar bajo el control del usuario;
3) el acceso al portaclaves debe ser administrado y verificable;
4) el sistema DIdAm podría ofrecer servicios que autoricen al usuario a guardar y restaurar su cartera.

8 Directrices de seguridad para utilizar DLT para DIdAm

La identidad descentralizada resuelve algunos de los problemas fundamentales relacionados con los modelos de identidad centralizados y federados. La tecnología de libro mayor distribuido es vulnerable a riesgos de ciberseguridad, incluidos los resultantes de errores humanos, como los errores de programación de *software*.

En general, los DID del usuario no deben publicarse en un libro mayor sin permisos, aunque en algunos casos podría ser necesario poner a disposición de todos sus usuarios un ID único. Sin embargo, los datos que ayudan a los usuarios a confiar en el libro mayor, como las claves públicas de los IdSP, las listas de revocación y los datos que mejoran la interoperabilidad, como los esquemas de credenciales variables, pueden convertirse en información pública en los libros de contabilidad.

En esta cláusula se abordan las ventajas, los problemas y los riesgos de seguridad de los modelos de identidad descentralizados.

8.1 Consideraciones relativas a la seguridad del libro mayor distribuido

Hay dos grandes tipos de libros mayores distribuidos, que se clasifican en "sin permisos" y "con permisos". Los libros mayores sin permisos permiten a cualquier entidad acceder, ver, proponer nuevos datos o validar los datos existentes en el libro, siempre y cuando sigan los protocolos establecidos. El libro mayor garantiza la confidencialidad, integridad, disponibilidad y coherencia de los datos con los protocolos de consenso para crear confianza entre los participantes, que pueden no confiar entre sí. En general, los libros mayores sin permisos funcionan sin ninguna autoridad central.

Un libro mayor con permisos es un sistema compuesto por partes de confianza a las que se conceden derechos de utilización que dependen de su función en el marco de la confianza. En este modelo, determinados participantes pueden modificar los datos del libro. En función de los acuerdos de confianza, algunos libros mayores pueden permitir el acceso abierto en modo lectura.

El libro mayor sin permisos garantiza la confianza mediante protocolos de consenso que constituyen recursos de cómputo y tienen una repercusión directa en el caudal y el rendimiento del sistema de identidades que en ellos se ejecuta. Por otra parte, los libros mayores con permisos se basan en la confianza entre los creadores del libro para garantizar la seguridad de los datos del libro, incluidos los datos de identidad. Los libros de contabilidad con permisos suelen ser más rápidos y económicos que los libros sin permisos.

8.2 Ventajas de utilizar el DID para DLT

La identidad descentralizada ofrece las siguientes ventajas:

1) Portabilidad de la identidad: los DID descentralizados garantizan el control de las personas sobre sus identidades digitales. Eliminan la dependencia de los IdSP centralizados. En teoría, cada persona puede poseer, controlar y administrar sus propias identidades y sus relaciones.
2) Fomenta los servicios de identidad basados en relaciones: los DID permiten a las entidades crear identificadores digitales para casi todas las relaciones. Asimismo, los DID seudónimos preservan la PII.
3) Minimiza el riesgo de seguridad: el DID exige que los propietarios de un identificador demuestren que lo son al exigir que conozcan la clave privada relacionada con la clave pública correspondiente. La declaración se valida dinámicamente en la DLT en tiempo real. La validación puede realizarse sin necesidad de servidores centralizados, lo que reduce la exposición a ataques.
4) Distribución de costes: la validación de identidad en una DLT puede aprovechar la capacidad de utilizar DID para reutilizar las pruebas de identidad entre los participantes de la DLT. Esto reduce el coste y mejora la seguridad.

5) PII por diseño: los servicios descentralizados de DID soberanos distribuyen el riesgo resultante de utilizar almacenamiento central de datos para guardar la información de los usuarios y, por lo tanto, aumenta la dificultad para los atacantes.

6) Intercambio consentido y controlado de datos personales: los DID ofrecen la posibilidad de compartir datos entre usuarios y proveedores conforme a políticas acordadas, lo que mejora la capacidad del usuario de proteger sus datos.

7) Federación dinámica y mejorada: la utilización de DID dentro de una DLT extiende la confianza a todas las organizaciones que participan en el ecosistema. Los participantes pueden centrarse en la prestación de servicios en lugar de centrarse en los detalles de la federación y en la forma de establecerla.

8) Tolerancia a fallos: el carácter descentralizado de la DLT proporciona buena tolerancia a fallos y resiliencia de la infraestructura.

8.3 Amenazas y vulnerabilidades

Los libros mayores distribuidos disponen de capacidades inherentes que mitigan el riesgo de ciberseguridad de los sistemas de tecnologías de la información y la comunicación. Algunos ejemplos de características de seguridad mejoradas son:

1) Mayor resiliencia del sistema: la arquitectura distribuida de la DLT evita que exista un punto débil.

2) Mayor robustez: los mecanismos de consenso mejoran la integridad general de los libros mayores distribuidos, ya que se requiere el consenso entre los participantes antes de aceptar cualquier dato nuevo en el libro mayor.

3) Mayor transparencia: es más difícil que el *software* malicioso funcione dentro de la DLT, por cuanto el sistema cuenta con muchas capas de seguridad separadas a nivel de la infraestructura del libro mayor.

Los sistemas de identidad descentralizados basados en la DLT tendrán los riesgos de seguridad inherentes a esas tecnologías. Además, la utilización de la DLT para la gestión de identidades conlleva riesgos adicionales.

8.3.1 Gestión de datos de identidades

El término CRUD es el acrónimo de Crear, Leer, Modificar y Suprimir. Estas son las operaciones básicas de las bases de datos de almacenamiento tradicionales. En la DLT, concretamente en las cadenas de bloques con permisos, las entidades que la integran no pueden borrar las transacciones escritas en la cadena de bloques. Tampoco pueden modificarse las transacciones existentes, ya que son inmutables. Por consiguiente, las operaciones "CRUD" no pueden considerarse normales para la gestión de los datos de usuario.

En su lugar, las operaciones en la cadena de bloques pueden describirse como CRAB: Crear, Recuperar, Añadir y Quemar. La operación Añadir, que reemplaza al Modificar, significa que las entidades sólo pueden añadir nuevas transacciones a una tecnología de cadena de bloques, cambiando así el "estado global" (suma de todos los eventos/transacciones pasados hasta ese instante). La operación Quemar en CRAB significa que se tiran las claves de cifrado, por lo que no se pueden añadir nuevas transacciones ni introducir cambio alguno en el estado del libro mayor del activo.

Por consiguiente, es importante prestar mucha atención a la escritura de datos personales en una DLT o cadena de bloques, por cuanto los datos no pueden ser eliminados ni olvidados en el futuro. En este sentido, es mejor escribir los datos fuera de la cadena con punteros en la DLT a los datos exteriores. Sin embargo, el almacenamiento de datos fuera de la cadena también tiene sus inconvenientes. En particular:

- se reduce la transparencia, ya que los usuarios no sabrán si no están autorizados a acceder a los datos fuera de libro mayor;

- se menoscaba la titularidad de los datos de la cadena de bloques, ya que una vez que los datos están fuera del libro mayor, pueden pasar a ser propiedad de cualquier entidad que pueda acceder a ellos.

8.3.2 Posibilidad de vinculación de claves DID

Existe la posibilidad de que los DID estén correlacionados. Puede suceder si el mismo DID se utiliza en más de una relación. Los libros mayores DLT pueden mitigar este riesgo utilizando DID únicos para las relaciones. Es decir, cada par de DID utilizados es diferente para cada relación. En este caso, cada DID actúa como un pseudónimo [b-W3C-2]. Sólo se precisa compartir un pseudónimo DID con más de una parte cuando el titular DID autoriza explícitamente la correlación entre esas partes.

Cabe señalar que los DID pseudónimos pueden estar correlacionados [b-W3C-2] si los datos de los documentos DID correspondientes estuvieran correlacionados. Por ejemplo, el uso de nombres de extremos de servicio comunes en múltiples documentos DID puede utilizarse para correlacionar la información sobre el mismo DID. Por consiguiente, el documento DID para un pseudónimo DID también necesita utilizar claves públicas únicas por pares.

8.3.3 Protección de claves DID

La gestión de las claves privadas es importante. Si una clave maestra se almacena en un lugar que no es seguro, aunque sea en un solo dispositivo, es probable que se produzca un robo de identidad. Se debe exigir la utilización de funciones de almacenamiento seguras en los dispositivos.

8.3.4 Técnicas de preservación de la PII

Se recomienda no almacenar información confidencial en el libro mayor. Con el advenimiento de la computación cuántica se podrá piratear con el tiempo cualquier técnica de encriptación bidireccional, por lo que no se debe almacenar nunca información sensible en el libro mayor.

Aunque las funciones generadoras (*hashes*) son unidireccionales, pueden ser no obstante sensibles ya que los *hackers* disponen de un tiempo ilimitado para efectuar ataques por fuerza bruta. Por esta razón, no deben almacenarse valores generadores en el libro.

En lugar de almacenar datos en bruto en el libro mayor, como la fecha de nacimiento, las respuestas a las preguntas que indican, por ejemplo, que una persona es mayor de 21 años, se podría almacenar dentro de un contrato inteligente en el libro mayor. Puede considerarse como una declaración que reúne un requisito.

Se recomienda almacenar en la DLT sólo valores generadores de datos privados o sensibles. Los datos de PII no deben guardarse en el libro mayor, aunque estén encriptados. Los datos sensibles deben almacenarse fuera del libro y deben intercambiarse entre entidades autorizadas que necesiten utilizarlos. Este planteamiento reduce el riesgo de que una eventual filtración de la DLT cause la pérdida de datos sensibles. Se debe utilizar una tecnología segura para el intercambio de datos punto a punto que dan soporte al acceso fuera del libro mayor. Deben utilizarse técnicas adecuadas de almacenamiento de datos fuera del libro mayor, incluidos planes para el archivo y recuperación de datos. Por ejemplo, si el propietario de una identidad afirma que es un proveedor de seguros con licencia, esa afirmación puede ser verificada por la entidad que desempeñe el papel de proveedor fiable en el sistema de identidad descentralizado y la prueba se almacena en la DLT de forma de valor generador. La prueba puede ser el valor generador de la declaración firmada digitalmente por el titular. Debe garantizarse la seguridad del depósito fuera del libro mayor.

8.3.5 Dependencia del suministrador

Los libros mayores pueden estar normalizados, sin embargo, los componentes software son específicos de una determinada solución y podrían ser propietarios y no interoperables.

8.3.6 Ataques contra la identidad

El libro mayor distribuido es vulnerable a los ataques contra la identidad, similares a los dirigidos contra la infraestructura tradicional de las tecnologías de la información, como la suplantación de identidad y los ataques Sybil. Los agentes maliciosos pueden desplegar esos ataques para apoderarse de la mayoría de los nodos del libro mayor. Si tiene éxito, el atacante puede socavar las protecciones de validación de consenso y de arquitectura distribuida del libro mayor. Este riesgo puede mitigarse utilizando soluciones de autenticación sólidas para los servicios de directorio basados en la nube.

8.3.7 Efectos en la red de comunicaciones

La estructura distribuida de la DLT puede crear problemas operativos cuando participan muchos actores, cada uno con sus propias soluciones de protección de la infraestructura de comunicaciones. Esta estructura plantea problemas en la gestión de las identidades, el control de acceso, la configuración de la seguridad, el almacenamiento y la gestión de las claves PKI.

Las operaciones de la DLT requieren nodos de ejecución que utilizan diferentes topologías de red de comunicaciones, *software* y protocolos que pueden ser vulnerables a las amenazas a la seguridad. El impacto de estas amenazas varía según la naturaleza de la DLT (privada o pública). Por ello, los sistemas de gestión de identidades y los datos de identidad son vulnerables a los ataques a nivel de la red de comunicaciones que tienen como objetivo la DLT. Los ingenieros de sistemas de gestión de identidades deben tener en cuenta los siguientes aspectos a nivel de la red de comunicaciones:

1) Impacto sobre los datos de identidad en caso de que falle el algoritmo de consenso de la DLT.
2) Cómo hacer frente a la DLT o a las colisiones en la cadena de bloques.
3) Cuál es el plan de recuperación de datos de identidad en caso de catástrofe.
4) Cuáles son las amenazas para los datos de identidad en caso de que un pequeño grupo de participantes controle los mecanismos de consenso de la DLT.

8.3.8 Encriptado de datos de identidad

Los datos de identidad almacenados en el libro mayor se consideran confidenciales y privados para el propietario de la identidad. El usuario debe poder obtener ayuda del libro mayor para la codificación de los datos, ya sea en bloque o durante la transmisión, en particular cuando los datos se comparten entre varios proveedores.

8.3.9 Copias de seguridad

Existen riesgos para el usuario a la hora de proteger su dispositivo y su contenido mediante declaraciones verificables o de claves privadas y datos personales.

Es necesario recuperar y restaurar adecuadamente los datos de la cartera del usuario.

Además, el usuario necesitará una garantía de que sus datos están protegidos y con copia de seguridad en el libro mayor. El usuario final debe disponer de servicios que garanticen protección contra la corrupción o la pérdida de datos.

8.3.10 Contratos inteligentes

La utilización de contratos inteligentes puede resultar necesaria en la implementación de sistemas de identidad descentralizados. Los contratos inteligentes son redactados por ingenieros utilizando lenguajes de programación. Estos programas son susceptibles de errores de desarrollo y programación, especialmente cuando aumenta la complejidad de los contratos inteligentes. Las incertidumbres con respecto a la exactitud de los contratos inteligentes requieren la creación de un marco de gobernanza que ofrezca garantías de que los sistemas de identidad descentralizados disponen procesos y procedimientos adecuados para resolver cualquier limitación resultante de un contrato inteligente inexacto, ya sea deliberado o no.

8.3.11 Gestión de certificados DLT

Los sistemas de gestión de identidades se encargan de gestionar la identidad a lo largo de su ciclo de vida, incluidas las tareas de verificación. Las tareas relacionadas con la gestión de la identidad comprenden la creación, emisión, almacenamiento, revocación y sustitución de credenciales y la detección del fraude.

La utilización de certificados en los libros mayores plantea retos singulares a los profesionales de la seguridad. En los sistemas de identidad descentralizados, hay que pagar un precio más alto por la pérdida o extravío de claves privadas que en los sistemas de acceso tradicionales. Por ejemplo, si se pierden las claves privadas del monedero de un usuario, el acceso de éste a su DLT queda permanentemente desactivado. El daño será mayor si se roban las claves, ya que demostrar la posesión de las claves privadas equivale a un robo de identidad. La dificultad de los mecanismos de recuperación también está en función de la naturaleza de la DLT. Es más fácil tratar estas cuestiones en los libros mayores privados que en los libros sin permisos, que requieren un consenso en las transacciones.

Estas cuestiones deben incluirse en el diseño de los sistemas de gobernanza de la DLT, ya que no existe una autoridad central encargada del fraude o de las dificultades técnicas. A tal efecto, se requieren marcos que rijan la confianza y garanticen que todos los estados del ciclo de vida de la identidad estén protegidos desde el principio y que los participantes en la DLT acuerden de antemano procedimientos adecuados para los servicios de recuperación de identidad, tales como: gestión del ciclo de vida de las claves, qué partes de la carga útil del bloque están cifradas, cómo se revocan las claves, cómo se protegen y recuperan las claves privadas, y qué ocurre si se detecta un fraude.

Bibliografía

[b-RFC 8141] RFC 8141, *Uniform Resource Names (URNs)*, abril de 2017.

[b-Angelov et al.] Angel Angelov, Mihail Milkov, Markus Sørensen, *Decentralized Identity Management System for Self-Sovereign Identity*, https://projekter.aau.dk/projekter/files/281068659/Master_Thesis_ICTE4SER4.2.pdf

[b-Baars] Djuri Baars, *Towards Self-Sovereign Identity using Blockchain Technology*, https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

[b-Blog] Blockchain platforms, https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

[b-DIF] Decentralized Identity Foundation (DIF), https://identity.foundation/#wgs

[b-Gartner] Gartner, Blockchain, *Evolving Decentralized Identity Design*, publicado el 1 de diciembre de 2017 – ID G00324208, por Analysts Homan Farahmand.

[b-Sovrin] Sovrin Foundation, https://sovrin.org/

[b-W3C-1] W3C, *Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web*, https://www.w3.org/TR/2019/CR-vc-data-model-20190725/

[b-W3C-2] W3C, *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes*, agosto de 2019, https://w3c-ccg.github.io/did-spec/

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021