ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1410 (03/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Aplicaciones y servicios seguros (2) – Seguridad de tecnología de libro mayor distribuido (DLT)

Arquitectura de seguridad para la gestión de la compartición de datos basada en la tecnología de libro mayor distribuido

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	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
Comunicaciones de emergencia	X.1300-X.1309
Seguridad en las redes de sensores ubicuos	X.1310-X.1319
Seguridad en redes eléctricas inteligentes	X.1330-X.1339
Correo certificado	X.1340-X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350-X.1369
Seguridad en los sistemas de transporte inteligentes (STI)	X.1370-X.1399
Seguridad en la tecnología de libro mayor distribuido (DLT)	**X.1400-X.1429**
Seguridad en las aplicaciones (2)	X.1450-X.1459
Seguridad en la web (2)	X.1470-X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

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

Recomendación UIT-T X.1410

Arquitectura de seguridad para la gestión de la compartición de datos basada en la tecnología de libro mayor distribuido

Resumen

En la Recomendación UIT-T X.1410 se especifica una arquitectura de seguridad de la gestión de la compartición de datos basada en tecnologías de libro mayor distribuido (DLT). Sobre la base de esta arquitectura, la presente Recomendación especifica las interfaces entre las entidades funcionales y los procedimientos de la gestión de la compartición de datos basada en DLT. La tecnología de libro mayor distribuido (DLT) está transformando las industrias con soluciones innovadoras y cambiando la manera en que trabajan los gobiernos, las instituciones y las empresas. Ofrece una solución para replicar, compartir y sincronizar datos de manera segura en una red informática distribuida, teniendo en cuenta sus funciones de descentralización y no manipulación. Los métodos actuales para compartir datos comerciales e información de identificación personal (PII) con empresas y plataformas digitales han dado paso a vulnerabilidades de privacidad por piratería informática o mala gestión de datos. La adopción de las DLT o la cadena de bloques para la gestión de la compartición de datos permite a las personas o a las empresas mantener un control más directo sobre su propia información confidencial. En la solución basada en DLT, solo los datos que no son PII, por ejemplo, los valores de datos compendiados, se almacenan en la cadena. Los datos PII sobre el propietario de los datos se almacenan fuera de la cadena. Una solución basada en DLT proporciona un método que mejora la trazabilidad, la verificabilidad y la posibilidad de cambiar la situación de los datos.

Historia*

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	UIT-T X.1410	03-03-2023	17	11.1002/1000/15109

Palabras clave

Arquitectura de seguridad, compartición de datos, DLT.

* Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 propiedad intelectual, protegida por patentes/derechos de autor de *software*, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios 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.1410

Arquitectura de seguridad para la gestión de la compartición de datos basada en la tecnología de libro mayor distribuido

1 Alcance

En esta Recomendación se especifica una arquitectura de seguridad para la compartición de datos basada en tecnologías de libro mayor distribuido (DLT). La presente Recomendación abarca:

– el diseño de la arquitectura de seguridad para la compartición de datos basada en DLT;

– la especificación de las funciones lógicas de la arquitectura de seguridad de la compartición de datos;

– la especificación de las interfaces entre las funciones lógicas de la arquitectura de seguridad;

– la especificación de los procedimientos para la compartición de datos basada en DLT.

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. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias son objeto de revisión, por lo que se alienta a los usuarios de la presente Recomendación a utilizar la edición más reciente de las Recomendaciones y demás referencias que se indican 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.1408] Recomendación UIT-T X.1408 (2021), *Amenazas y requisitos de seguridad para el acceso y la compartición de datos basados en la tecnología de libro mayor distribuido*.

3 Definiciones

3.1 Términos definidos en otros textos

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

3.1.1 dirección [b-UIT-T FG DLT D1.1]: Identificador de una o varias entidades que realizan operaciones u otras acciones en una cadena de bloques o una red de libro mayor distribuido.

3.1.2 cadena de bloques [b-UIT-T X.1400]: Tipo de libro mayor distribuido que está formado por datos registrados por medios digitales dispuestos en forma de una cadena de bloques cada vez mayor, en la que cada bloque se vincula criptográficamente y se refuerza contra la manipulación y la revisión.

3.1.3 autoridad de certificación (CA) [b-UIT-T X.509]: Autoridad a la que una o más entidades han confiado la creación y firma digital de certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios.

3.1.4 proveedor de datos [b-ISO/CEI/IEEE 15939]: Persona u organización que constituye la fuente de los datos.

3.1.5 identidad [b-ISO/CEI 29100]: Conjunto de atributos que permiten identificar al titular de la información de identificación personal.

3.1.6 fuera de la cadena [b-ISO 22739]: Relacionado con un sistema de cadena de bloques, pero ubicado, realizado o ejecutado fuera de ese sistema de cadena de bloques.

3.1.7 en la cadena [b-ISO 22739]: Ubicado, realizado o ejecutado dentro de un sistema de cadena de bloques.

3.1.8 información de identificación personal (PII) [b-ISO/CEI 29100]: Toda información que a) puede utilizarse para identificar el titular de la información de identificación personal (IIP) con quien está relacionada esa información, o b) está o puede estar relacionada directa o indirectamente con el titular de la PII.

NOTA – Para determinar si un titular de la IIP es identificable, se deben tener en cuenta todos los medios utilizables, razonablemente, por el interesado en la privacidad que posea los datos, o por cualquier otra parte, para identificar a esa persona física.

3.1.9 infraestructura de clave pública (PKI) [b-UIT-T X.509]: Infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio.

3.1.10 contrato inteligente [b-UIT-T X.1400]: Un programa escrito en el sistema del libro mayor distribuido, que codifica la normativa aplicable a ciertos tipos de operaciones en dicho sistema, con miras a su validación y activación en condiciones específicas.

3.1.11 sistema de encriptación simétrico [b-ISO/CEI 18033-1]: Técnica criptográfica utilizada para proteger la confidencialidad de los datos, que consta de tres procesos (un algoritmo de cifrado, un algoritmo de desencriptación y un método para generar claves), en cuyo marco los algoritmos de cifrado y desencriptación utilizan la misma clave.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se define el siguiente término:

3.2.1 consumidor de datos: Usuario que lee los datos y a continuación los procesa de manera que se revelan los límites léxicos o de codificación.

NOTA – Adaptado de [b-ISO/CEI 20944-1].

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

API Interfaz de programación de aplicaciones (*application programming interface*)

CA Autoridad de certificación *(certification authority)*

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

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

PKI Infraestructura de clave pública *(public key infrastructure)*

5 Convenios

En esta Recomendación:

La expresión **"se recomienda"** indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para declarar la conformidad.

La expresión **"puede"** y **"opcionalmente"** indica que el requisito se permite, sin que ello signifique que se recomienda. El uso de este término no implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

El uso de la *cursiva* en esta Recomendación indica las funciones.

6 Arquitectura de compartición de datos basada en DLT

La tecnología de libro mayor distribuido proporciona una solución para replicar, compartir y sincronizar datos de manera segura en una red informática distribuida, teniendo en cuenta sus funciones de descentralización y no manipulación. Los métodos actuales para compartir datos comerciales e información de identificación personal (PII) con empresas y plataformas digitales han dado paso a vulnerabilidades de privacidad por piratería informática o mala gestión de datos. La adopción de las DLT o la cadena de bloques para la gestión de la compartición de datos permite a las personas o a las empresas mantener un control más directo sobre su propia información confidencial. En la solución basada en DLT, solo los datos que no son PII, por ejemplo, los valores de datos compendiados, se almacenan en la cadena. Los datos PII sobre el propietario de los datos se almacenan fuera de la cadena. Una solución basada en DLT proporciona un método que mejora la trazabilidad, la verificabilidad y la posibilidad de cambiar la situación de los datos. En este contexto, la presente Recomendación especifica la arquitectura de seguridad de la gestión de la compartición de datos basada en las DLT. La gestión de la compartición de datos utiliza un sistema de encriptación simétrico en el que los algoritmos de cifrado y desencriptación utilizan las mismas claves. Las amenazas contra la seguridad se describen en la [UIT-T X.1408].

Esta Recomendación se ha elaborado sobre la base de la [UIT-T X.1408]. Mientras que la [UIT-T X.1408] se elaboró desde un punto de vista conceptual, la presente Recomendación se ha preparado desde el punto de vista de la aplicación. En el Cuadro 1 se indican las correspondencias de la terminología utilizada en esta Recomendación y en la [UIT-T X.1408].

Cuadro 1 – Correspondencia de los términos utilizados en esta Recomendación y en la [UIT-T X.1408]

Esta Recomendación	[UIT-T X.1408]
Proveedor de datos	Agente de compartición de datos (propietario de los datos)
Consumidor de datos	Cliente consumidor de datos (procesador de datos)
Servidor de almacenamiento de claves	Servidor de gestión de claves
Servidor de almacenamiento de datos	Servidor de almacenamiento de datos (proveedor de servicios de almacenamiento de datos)
Gestión de la compartición de datos basada en DLT	Intermediario de datos

6.1 Visión general de la arquitectura funcional

La Figura 1 ilustra la arquitectura funcional de la gestión de la compartición de datos basada en DLT desde el punto de vista de la implementación. Está en consonancia con la arquitectura del acceso y compartición de datos basados en DLT que se muestra en la Figura B.1 de la [UIT-T X.1408]. Este último diseño se hizo desde un punto de vista conceptual y se trata de una arquitectura de alto nivel. La arquitectura funcional que se expone en la Figura 1 consta de cinco componentes funcionales azules y tres componentes funcionales grises.

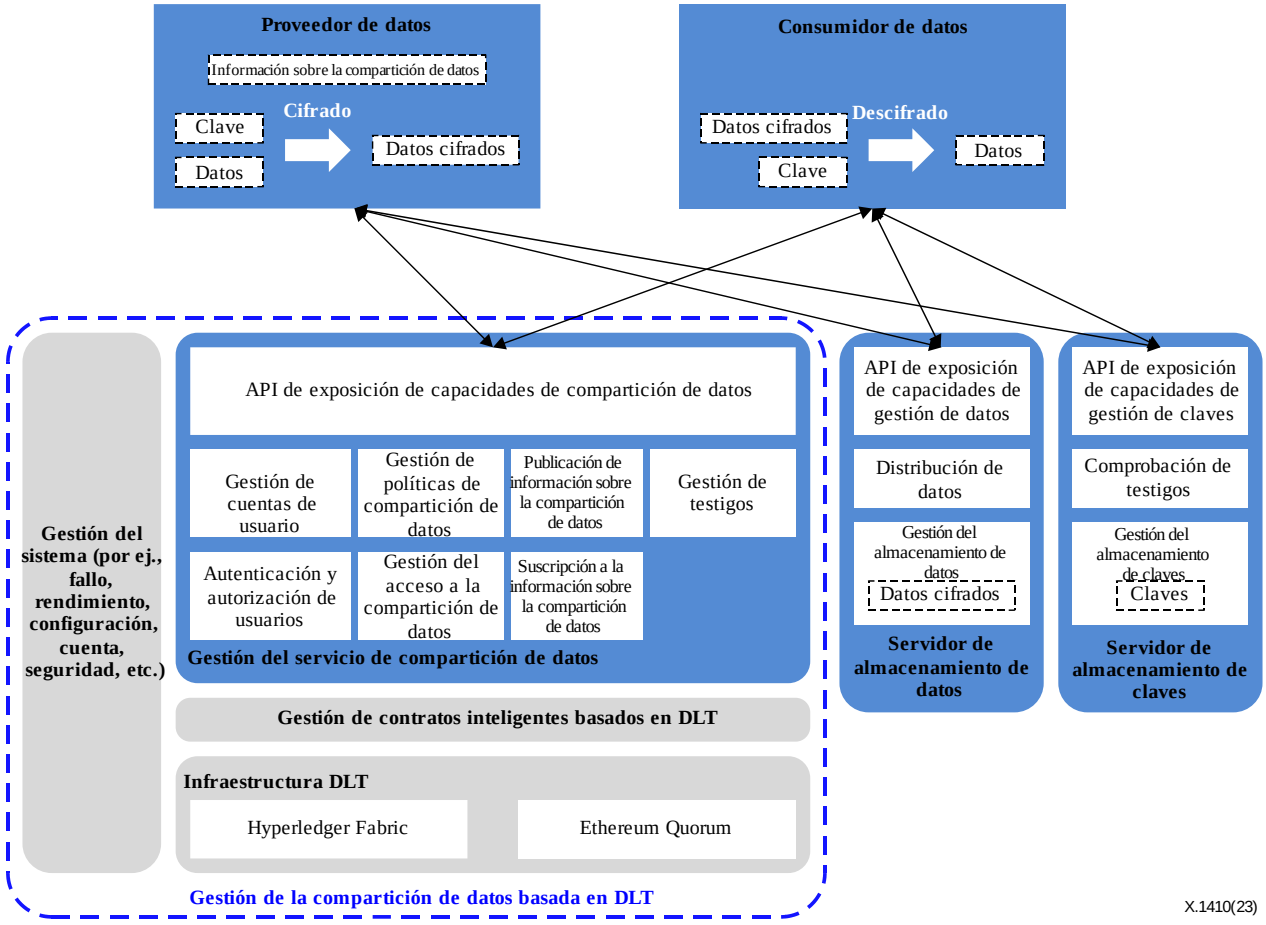

Figura 1 – Arquitectura funcional de la gestión de compartición de datos basada en DLT

A continuación, se describen dichos componentes:

– Los cinco componentes funcionales azules son el proveedor de datos, el consumidor de datos, la gestión del servicio de compartición de datos, el servidor de almacenamiento de claves y el servidor de almacenamiento de datos, que se describen y definen de manera detallada en la cláusula 6.2.

– Los tres componentes funcionales grises son *la infraestructura DLT, la gestión de contratos inteligentes basada en DLT y la gestión del sistema (por ejemplo, fallo, configuración, rendimiento, cuenta, seguridad)*, que reutilizan las plataformas DLT de código abierto existentes (por ejemplo, Hyperledger Fabric) y quedan fuera del alcance de la presente Recomendación.

En el Anexo A se describen los procedimientos de gestión de la compartición de datos basada en DLT.

6.2 Componentes funcionales

6.2.1 Proveedor de datos y consumidor de datos

En esta Recomendación se presentan dos tipos de usuario: el proveedor de datos (es decir, los usuarios que comparten sus datos) y el consumidor de datos (es decir, los usuarios que consumen los datos compartidos por otros usuarios). Ambos tipos comparten las mismas capacidades:

1) obtener certificados digitales (incluidas las claves públicas) y las correspondientes claves privadas de la autoridad de certificación (CA);

2) almacenar los certificados digitales obtenidos y las correspondientes claves privadas de manera segura;

3) comunicarse con el servidor de gestión de la compartición de datos basada en DLT;

4) obtener y almacenar los certificados digitales, los parámetros de red y las configuraciones de red de los nodos de la red DLT;

5) recibir notificaciones de la gestión de la compartición de datos basada en DLT;

6) utilizar un sistema de encriptación simétrico.

El proveedor de datos y el consumidor de datos tienen sus propias capacidades específicas, como se indica a continuación.

– Un *proveedor de datos* tiene las siguientes capacidades:

  1) recopilar datos brutos y desensibilizarlos (por ejemplo, haciendo que los datos sean anónimos, retirando la información sensible como el nombre, el número de teléfono móvil o los datos de la tarjeta de crédito), sin incidir negativamente en la calidad de los datos que se van a compartir;

  2) generar una clave para un sistema de encriptación simétrico;

  3) cifrar datos con la clave que utiliza el sistema de encriptación simétrico;

  4) almacenar el texto cifrado y la correspondiente clave de cifrado en el servidor local o remoto;

  5) garantizar una autenticación mutua con la gestión de la compartición de datos basada en DLT;

  6) proporcionar a la gestión de la compartición de datos basada en DLT información relativa a la compartición de datos, que abarca el identificador del proveedor de datos, la clave pública del proveedor de datos, el identificador del texto cifrado y su dirección de almacenamiento, el identificador de la clave de cifrado y su dirección de almacenamiento, las industrias a las que se autorizará el acceso, los usuarios a los que se autorizará el acceso, y otros atributos de los datos (por ejemplo, la categoría de datos, la introducción de los datos, la utilización y el precio);

  7) combinar información sobre la compartición de datos con otra información para formar una política de compartición de datos, y a continuación firmar la política de compartición de datos con la clave privada;

  8) enviar la política de compartición de datos con la correspondiente firma digital a la gestión de la compartición de datos basada en DLT;

  9) recibir notificaciones de la gestión de la compartición de datos basada en DLT acerca de la creación del contrato inteligente para la compartición de datos;

  10) gestionar la política de compartición de datos, como las consultas y las actualizaciones.

– Un *consumidor de datos* tiene las siguientes capacidades:

  1) suscribirse a los mensajes publicados relativos a la compartición de datos;

  2) garantizar una autenticación mutua con la gestión de la compartición de datos basada en DLT;

  3) obtener información relativa a la compartición de datos;

  4) enviar información sobre el consumidor de datos (por ejemplo, la identidad del consumidor de datos o la clave pública del consumidor de datos) e información sobre los datos compartidos (por ejemplo, la identidad del proveedor de datos, la clave pública del proveedor de datos, el identificador del texto cifrado y el identificador de la clave de cifrado) junto con la firma digital (hecha con la clave privada del consumidor de datos) a la gestión de la compartición de datos basada en DLT;

5) recibir notificaciones de la gestión de la compartición de datos basada en DLT, en que se incluya información sobre los datos compartidos, la dirección de almacenamiento de claves, la dirección de almacenamiento del texto cifrado y el testigo de acceso;

6) enviar el testigo de acceso al servidor de almacenamiento de claves a fin de obtener la clave de encriptación de datos correspondiente a la dirección de almacenamiento de claves;

7) obtener el texto cifrado correspondiente a la dirección de almacenamiento de datos;

8) descifrar el texto cifrado con la clave obtenida del sistema de encriptación simétrico para que los datos se muestren en forma de texto sin formato;

9) gestionar los registros para acceder a los datos compartidos.

6.2.2 Gestión del servicio de compartición de datos

A continuación se describen las capacidades de cada componente de la gestión del servicio de compartición de datos.

– ***La gestión de cuentas de usuario*** tiene las capacidades de gestionar las cuentas de usuario, como las de creación, actualización, consulta y supresión.

– ***La autenticación y autorización de usuarios*** tienen las siguientes capacidades:

1) realizar la autenticación mutua con los usuarios (es decir, el proveedor de datos y el consumidor de datos);

2) autorizar a los usuarios a compartir los datos y acceder a los datos compartidos.

– ***La gestión de la política de compartición de datos*** tiene las siguientes capacidades:

1) recibir información sobre la compartición de datos y políticas de compartición de datos junto con la firma digital correspondiente de cada proveedor de datos;

2) crear una operación DLT con arreglo a la información recibida del proveedor de datos;

3) presentar la operación DLT a los componentes subyacentes (es decir, *la infraestructura DLT y la gestión de contratos inteligentes*) a fin de crear un contrato inteligente de compartición de datos, que se distribuirá a los nodos de la red DLT;

4) comunicar al *proveedor de datos* y a la *publicación de información sobre la compartición de datos* que se ha creado el contrato inteligente de compartición de datos;

5) permitir a los proveedores de datos gestionar sus datos compartidos.

– ***La gestión del acceso a la compartición de datos*** tiene las siguientes capacidades:

1) recibir solicitudes de acceso a los datos (en particular, la información sobre el consumidor de datos, la información sobre los datos compartidos y la correspondiente firma digital) del consumidor de datos y comprobar si este está autorizado a acceder a los datos con arreglo a la política de compartición de datos (por ejemplo, solo el consumidor de datos de la industria o país indicado podría acceder a los datos compartidos);

2) crear una operación DLT con arreglo a la información recibida del consumidor de datos;

3) presentar la operación DLT a los componentes subyacentes (por ejemplo, la *infraestructura DLT*) a fin de registrar el acceso a los datos, que se distribuirán a los nodos de la red DLT;

4) comunicar a la *gestión de testigos* que se ha creado la operación de acceso a los datos y que debe crearse un testigo de acceso;

5) recibir el testigo de acceso de la *gestión de testigos*;

6) enviar información relativa al acceso a la compartición de datos (por ejemplo, el testigo de acceso, la dirección de almacenamiento de claves, la dirección de almacenamiento de datos, etc.) al consumidor de datos;

7) permitir al consumidor de datos gestionar sus registros de acceso a la compartición de datos.

– La ***publicación de información sobre la compartición de datos*** tiene las siguientes capacidades:

1) recibir notificaciones de la *gestión de políticas de compartición de datos*, que contienen información nueva sobre la compartición de datos;

2) publicar información nueva sobre la compartición de datos;

3) comunicar a la s*uscripción de información sobre la compartición de datos* que se ha publicado información nueva sobre la compartición de datos.

– La ***suscripción de información sobre la compartición de datos*** tiene las siguientes capacidades:

1) recibir notificaciones de la *gestión de información sobre la compartición de datos*, que contienen información nueva sobre la compartición de datos;

2) enviar información nueva sobre la compartición de datos a los suscriptores.

– La ***gestión de testigos*** tiene las siguientes capacidades:

1) recibir notificaciones de la *gestión del acceso a la compartición de datos* para crear un testigo de acceso;

2) crear el testigo de acceso;

3) enviar el testigo de acceso creado a la *gestión del acceso a la compartición de datos.*

– La ***interfaz de programación de aplicaciones (API) de exposición de capacidades de compartición de datos*** permite a los usuarios gestionar y acceder a los servicios de compartición de datos expuestos anteriormente.

6.2.3 Servidor de almacenamiento de claves

A continuación se describen las capacidades de cada componente del servidor de almacenamiento de claves.

– La ***gestión del almacenamiento*** de claves tiene las siguientes capacidades:

1) recibir solicitudes del *proveedor de datos* para almacenar la clave;

2) autenticar al *proveedor de datos*;

3) almacenar la clave de manera segura, por ejemplo, en un texto cifrado y/o en un dispositivo de almacenamiento aislado;

4) comunicar al *proveedor de datos* que la clave se ha almacenado;

5) recibir notificaciones de la *comprobación de testigos*, en que se indique el resultado de la comprobación del testigo de acceso;

6) enviar la clave al *consumidor de datos*.

– La ***comprobación de testigos*** tiene las siguientes capacidades:

1) recibir el testigo de acceso del consumidor de datos;

2) comprobar el testigo de acceso recibido;

3) enviar el resultado de la comprobación a la *gestión del almacenamiento de claves*.

– Una ***API de exposición de capacidades de gestión de claves*** permite a los usuarios gestionar y acceder a la clave de cifrado de los datos.

6.2.4 Servidor de almacenamiento de datos

A continuación se describen las capacidades de cada componente del servidor de almacenamiento de datos.

– La ***gestión del almacenamiento de datos*** tiene las siguientes capacidades:
  1) recibir solicitudes del *proveedor de datos* para almacenar el texto cifrado;
  2) autenticar al *proveedor de datos*;
  3) almacenar el texto cifrado;
  4) comunicar al *proveedor de datos* que el texto cifrado se ha almacenado.
– La ***distribución de datos*** tiene las siguientes capacidades:
  1) recibir la solicitud de un *consumidor de datos*;
  2) autenticar al *consumidor de datos*;
  3) enviar el texto cifrado al *consumidor de datos*.
– Una ***API de exposición de capacidades de gestión de datos*** permite a los usuarios gestionar y acceder a los datos compartidos.

7 Arquitectura de seguridad de la gestión de compartición de datos basada en DLT

Según la arquitectura funcional que se ilustra en la Figura 1, los consumidores de datos solicitan y reciben una clave de cifrado de datos, con la que a continuación desencriptan los datos en el texto cifrado y por último obtienen los datos compartidos en forma de texto sin formato. Tras ello, los datos compartidos en forma de texto sin formato no pueden ser controlados por la gestión de la compartición de datos basada en DLT. Es posible que los consumidores de datos reenvíen los datos compartidos en forma de texto sin formato a otros usuarios que no tengan permiso para acceder a ellos.

A fin de ayudar a los proveedores de datos a compartir datos con otros de manera segura y evitar que los consumidores de datos reenvíen los datos compartidos en forma de texto sin formato a otros usuarios, la arquitectura funciona que se ilustra en la Figura 1 necesita funciones de seguridad avanzada, que se muestran en la Figura 2.

7.1 Visión general de la arquitectura de seguridad

En la Figura 2 se describe la arquitectura de seguridad de la gestión de compartición de datos basada en DLT, que garantiza que:

– las comunicaciones entre los componentes funcionales que se muestran en la Figura 1 sean seguras;
– los proveedores de datos encripten los datos y también establezcan los permisos necesarios para acceder a ellos antes de compartirlos con terceros;
– los consumidores de datos desencripten los datos compartidos en texto cifrado con arreglo a los permisos de acceso antes de acceder a ellos;
– los consumidores de datos encripten los datos compartidos de la misma manera que lo hacen los proveedores de datos tras terminar de acceder a los datos, y de este modo almacenen los datos compartidos en texto cifrado;
– los consumidores de datos solo reenvíen los datos compartidos en texto cifrado a terceros.

De esta manera, incluso si los usuarios reciben los datos compartidos reenviados por otros, deben solicitar un permiso de acceso para acceder a ellos a la gestión de compartición de datos basada en DLT.

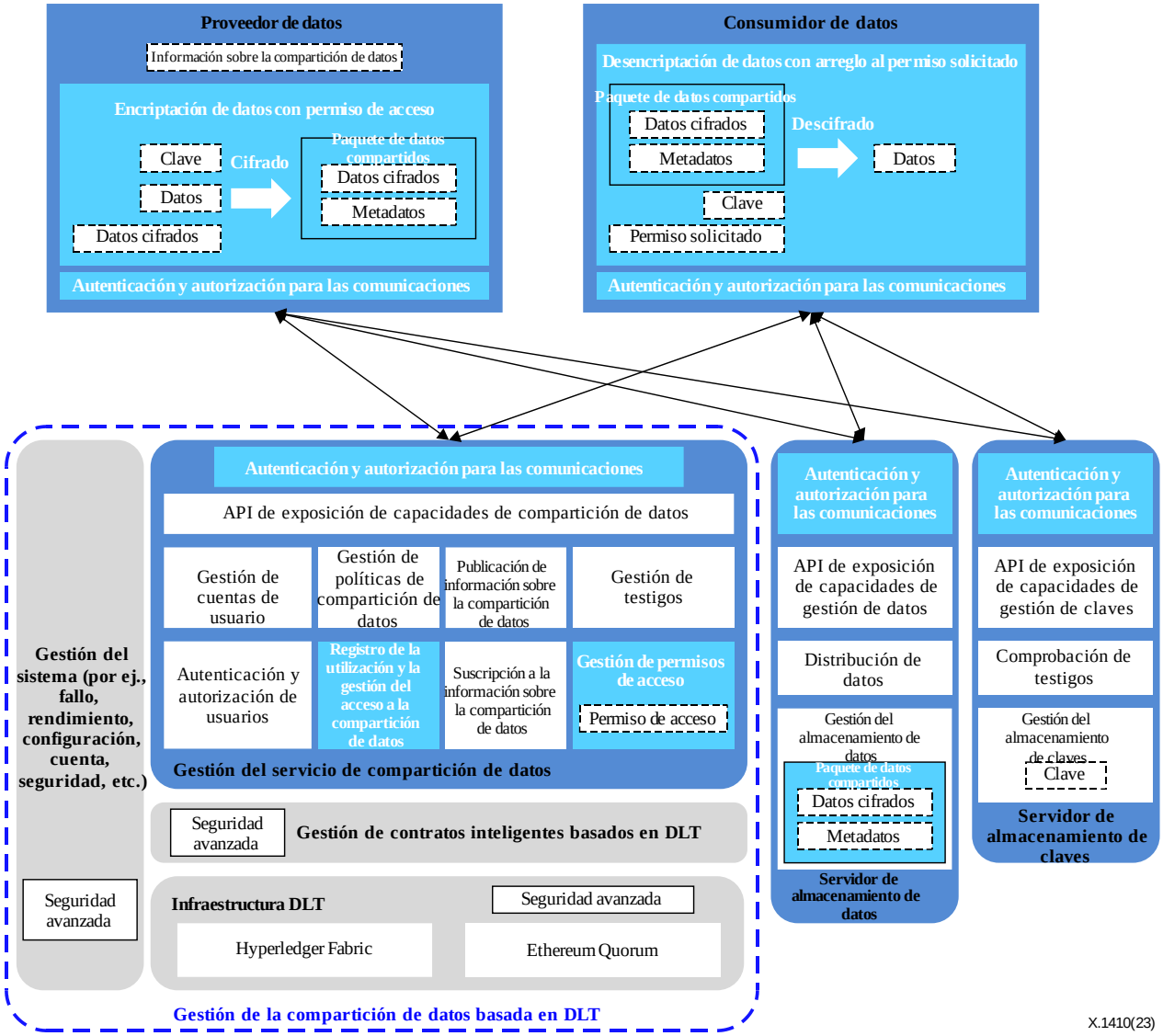

Figura 2 – Arquitectura de seguridad de la gestión de compartición de datos basada en DLT

A diferencia de la Figura 1, la Figura 2 contiene componentes funcionales con un fondo azul claro que corresponden a funciones lógicas de seguridad, que se describen detalladamente en la cláusula 7.2.

En esta Recomendación no se describe la seguridad avanzada correspondiente a los tres componentes funcionales grises que se ilustran en la Figura 2; véase [b-UIT-T X.1402].

7.2 Componentes funcionales de seguridad

7.2.1 Encriptación de datos con permiso de acceso

A fin de ayudar a los usuarios a definir permisos de acceso respecto de los datos que van a compartir, el *proveedor de datos* que se ilustra en la Figura 1 debe mejorar introduciendo una nueva función lógica de seguridad, la *encriptación de datos con permiso de acceso*, que tiene las capacidades siguientes:

– generar una clave de un sistema de encriptación simétrico que se utilice para cifrar los datos que se van a compartir;

– comunicarse con el *servidor de almacenamiento de claves* a fin de registrar el identificador de una clave y la dirección para obtenerlo;

– comunicarse con el s*ervidor de almacenamiento de datos* a fin de registrar el identificador de un paquete de datos compartidos y la dirección para obtenerlo;
– definir un permiso de acceso respecto de los datos que se van a compartir, que incluya los tiempos de acceso, el plazo de expiración, la función de solo lectura, el identificador de la clave y su dirección de almacenamiento, el identificador del paquete de datos compartidos y su dirección de almacenamiento;
– generar metadatos, que incluyan un identificador del paquete de datos compartidos, un identificador del proveedor de datos, la clave pública del proveedor de datos y la firma de la información anterior;
– generar un paquete de datos compartidos, que incluya los datos cifrados y los metadatos;
– cargar la clave en el *servidor de almacenamiento de claves* mediante un canal de transmisión seguro;
– cargar el paquete de datos compartidos en el *servidor de almacenamiento de datos* mediante un canal de transmisión seguro;
– cargar el permiso de acceso en la *gestión del servicio de compartición de datos* mediante un canal de transmisión seguro.

7.2.2 Desencriptación de datos con arreglo al permiso solicitado

A fin de ayudar a los usuarios a acceder a los datos compartidos con arreglo al permiso solicitado, el *consumidor de datos* que se ilustra en la Figura 1 debe mejorar introduciendo una nueva función lógica de seguridad, la *desencriptación de datos con arreglo al permiso solicitado*, que tiene las capacidades siguientes:

– obtener la dirección para ejecutar el contrato inteligente de compartición de datos;
– comunicarse con la *gestión del servicio de compartición de datos*, ejecutar el contrato inteligente de compartición de datos y obtener el permiso solicitado, que incluye los tiempos de acceso, el plazo de expiración, la función de solo lectura, el identificador de la clave y su dirección de almacenamiento, el identificador del paquete de datos compartidos y su dirección de almacenamiento;
– comunicarse con el *servidor de almacenamiento de claves* para obtener la clave de cifrado;
– comunicarse con el *servidor de almacenamiento de datos* para obtener el paquete de datos compartidos, que incluye los datos cifrados y los metadatos;
– validar el paquete de datos compartidos recibido sobre la base de la firma en los metadatos;
– desencriptar los datos cifrados sobre la base de la clave de cifrado;
– presentar los datos compartidos en forma de texto sin formato a los usuarios con arreglo al permiso solicitado;
– encriptar los datos compartidos de la misma manera que lo hacen los proveedores de datos tras terminar de acceder a los datos.

7.2.3 Gestión de permisos de acceso

A fin de ayudar a los usuarios a definir los permisos de acceso respecto de los datos compartidos o ayudar a los usuarios a acceder a tales datos con arreglo al permiso solicitado, la *gestión del servicio de compartición de datos* que se ilustra en la Figura 1 debe mejorar mediante la introducción de una nueva función lógica de seguridad, la *gestión de permisos de acceso*, que tiene las capacidades siguientes:

– ayudar a los usuarios a definir los permisos de acceso respecto de los datos que se van a compartir;
    • recibir de la gestión de políticas de compartición de datos los permisos de acceso definidos por el proveedor de datos;

- almacenar los permisos de acceso;
- enviar la respuesta a la *gestión de políticas de compartición de datos*;

– ayudar a los usuarios a acceder a los datos compartidos con arreglo al permiso solicitado:
- recibir *del registro de la utilización y la gestión del acceso a la compartición de datos* el permiso solicitado por el *consumidor de datos*;
- generar el permiso solicitado;
- enviar el permiso solicitado al *registro de la utilización y la gestión del acceso a la compartición de datos*.

7.2.4 Registro de la utilización y la gestión del acceso a la compartición de datos

A fin de ayudar a los usuarios a rastrear la utilización de sus datos compartidos, el *registro de la utilización y la gestión del acceso a la compartición de datos* que se ilustra en la Figura 2 debe mejorarse con las siguientes capacidades:

– comunicarse con la *gestión de permisos de acceso* a fin de obtener el permiso solicitado;

– registrar la utilización de los datos compartidos sobre la base del permiso solicitado.

7.2.5 Autenticación y autorización para las comunicaciones

Para que las comunicaciones sean seguras, los cinco componentes funcionales que se ilustran en la Figura 1 (a saber, *el proveedor de datos*, *el consumidor de datos, la gestión del servicio de compartición de datos, el servidor de almacenamiento de claves* y *el servidor de almacenamiento de datos*) deben mejorar mediante la introducción de una nueva función lógica de seguridad, la *autenticación y autorización para las comunicaciones.*

Cuando el proveedor de datos o el consumidor de datos envían el mensaje de solicitud a la *gestión del servicio de compartición de datos,* al *servidor de almacenamiento de claves* o al *servidor de almacenamiento de datos*, la *autenticación y autorización para las comunicaciones* puede dar soporte a lo siguiente:

– la autenticación del *proveedor de datos/consumidor de datos* por parte de la *gestión del servicio de compartición de datos/el servidor de almacenamiento de claves/el servidor de almacenamiento de datos*, sobre la base del certificado [b-IETF RFC 4306] [b-IETF RFC 5246] o la clave precompartida [b-IETF RFC 4279] [b-IETF RFC 4306];

– la autenticación de la *gestión del servicio de compartición de datos/el servidor de almacenamiento de claves/el servidor de almacenamiento de datos* por parte *del proveedor de datos/consumidor de datos*, sobre la base del certificado [b-IETF RFC 4306] [b-IETF RFC 5246];

– la autorización del *proveedor de datos/consumidor de datos* por parte de la *gestión del servicio de compartición de datos/el servidor de almacenamiento de claves/el servidor de almacenamiento de datos*, sobre la base de una lista blanca/lista negra [b-IETF RFC 5782] [b-IETF RFC 5851] o una lista de control de acceso [b-IETF RFC 4314] [b-IETF RFC 4949];

– la generación de la clave de sesión, que se utilizará para proteger las comunicaciones entre el *proveedor de datos/consumidor de datos* y la *gestión del servicio de compartición de datos/el servidor de almacenamiento de claves/el servidor de almacenamiento de datos.*

7.3 Procedimientos para compartir datos de manera segura

7.3.1 El procedimiento utilizado por los proveedores de datos para compartir datos con el establecimiento de permisos de acceso

En la Figura 3 se ilustra el procedimiento para que los proveedores de datos compartan datos estableciendo permisos de acceso.

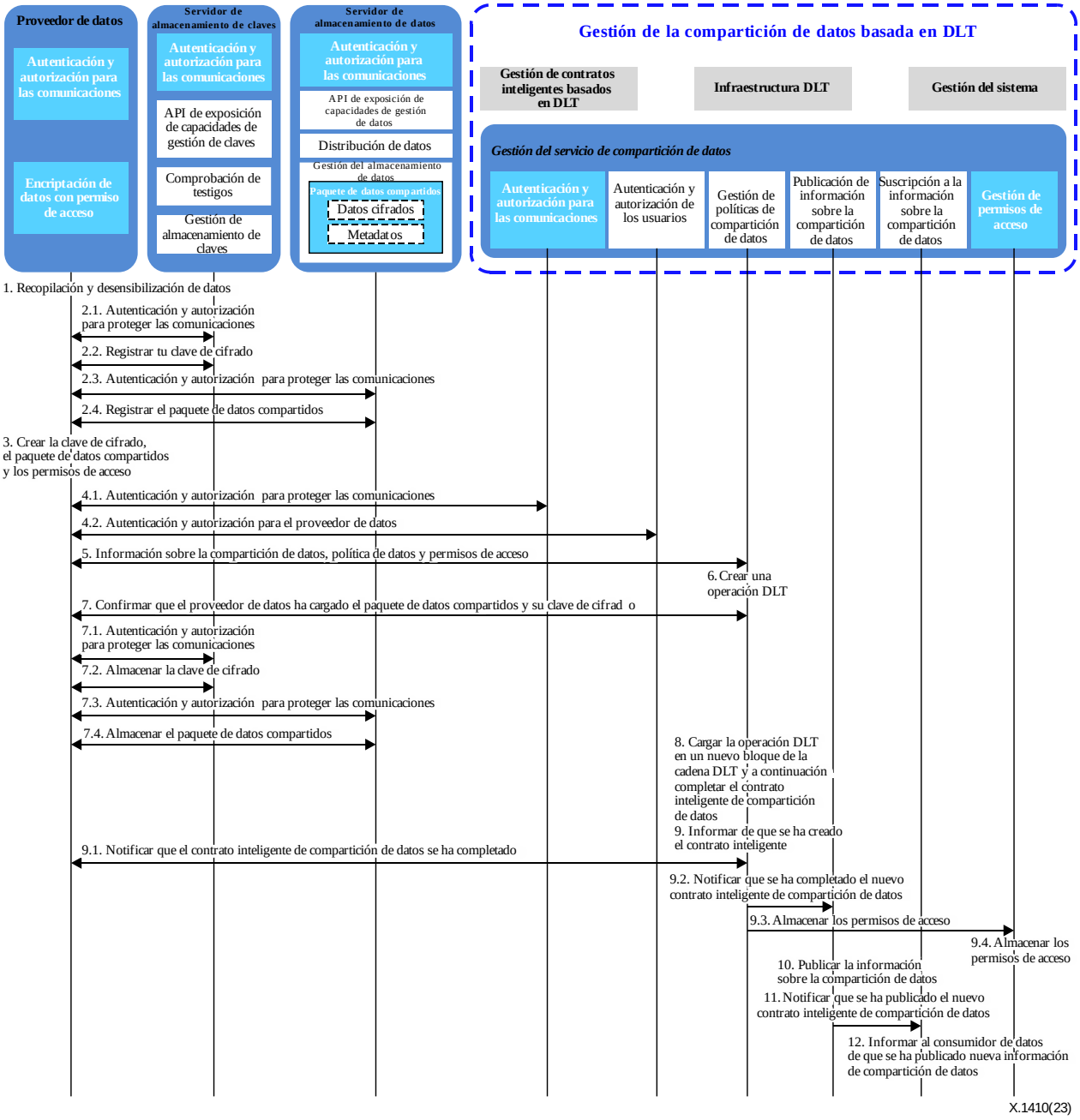

Figura 3 – Procedimiento para que los proveedores de datos compartan datos estableciendo permisos de acceso

Como se ilustra en la Figura 3, el procedimiento es el siguiente:

1) El *proveedor de datos* recopila los datos originales y los desensibiliza sin incidir negativamente en la calidad de los datos que se van a compartir.

2) El *proveedor de datos* registra el paquete de datos compartidos y su clave en el servidor de almacenamiento de claves y en el servidor de almacenamiento de datos, locales o remotos, del siguiente modo:

   2.1) El *proveedor de datos* y *la autenticación y autorización para las comunicaciones* del *servidor de almacenamiento de claves* llevan a cabo una autenticación mutua y obtienen una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

   2.2) El *proveedor de datos* se conecta al *servidor de almacenamiento de claves* y registra un identificador de clave y la dirección para obtenerla.

2.3) El *proveedor de datos* y la *autenticación y autorización para las comunicaciones* del *servidor de almacenamiento de datos* llevan a cabo una autenticación mutua y obtienen una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

2.4) El *proveedor de datos* se conecta al *servidor de almacenamiento de datos* y registra un identificador de paquete de datos compartidos y la dirección para obtenerlo.

3) El *proveedor de datos* crea la información sobre la compartición de datos, que incluye el identificador del proveedor de datos, la clave pública del proveedor de datos, el identificador del paquete de datos compartidos y su dirección de almacenamiento, el identificador de clave y su dirección de almacenamiento, las industrias a las que se autorizará el acceso, los usuarios a los que se autorizará el acceso, y otros atributos de datos (por ejemplo, la categoría de datos, la introducción de datos, la utilización y el precio).

El *proveedor de datos* genera una clave que se utiliza para encriptar los datos que se van a compartir.

El *proveedor de datos* establece el permiso de acceso respecto de los datos, que incluye los tiempos de acceso, el plazo de expiración, la función de solo lectura, el identificador de la clave y su dirección de almacenamiento, el identificador del paquete de datos compartidos y su dirección de almacenamiento que se va a compartir.

El *proveedor de datos* genera metadatos, que incluyen un identificador del paquete de datos compartidos, un identificador del proveedor de datos, la clave pública del proveedor de datos y la firma de la información anterior.

El *proveedor de datos* genera un paquete de datos compartidos, que incluye los datos cifrados y los metadatos.

4) Antes de publicar los datos que se van a compartir, es necesario que:

4.1) El *proveedor de datos* y la *autenticación y autorización para las comunicaciones* de la *gestión del servicio de compartición de datos* lleven a cabo una autenticación mutua y obtengan una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

4.2) El *proveedor de datos* y la *autenticación y autorización de los usuarios* de la *gestión del servicio de compartición de datos* lleven a cabo una autenticación mutua. Una vez que se haya realizado correctamente la autenticación mutua, el componente de *autenticación y autorización de los usuarios* comprueba si el proveedor de datos tiene derecho a publicar los datos que se van a compartir.

5) El *proveedor de datos* proporciona la información sobre la compartición de datos con arreglo a los requisitos recibidos de la *gestión de políticas de compartición de datos* de la *gestión del servicio de compartición de datos.* El *proveedor de datos* crea una política de compartición de datos con la compartición de datos y otra información. El *proveedor de datos* envía la información sobre la compartición de datos, la política de compartición de datos, los permisos de acceso y su firma digital a la *gestión de políticas de compartición de datos*.

6) Tras recibir la información sobre la compartición de datos, la política de compartición de datos, los permisos de acceso y la correspondiente firma digital del *proveedor de datos*, la *gestión de políticas de compartición de datos* comprueba la firma digital y a continuación crea una operación DLT.

7) La *gestión de políticas de compartición de datos* confirma con el *proveedor de datos* que la clave y el paquete de datos compartidos se han almacenado en el *servidor de almacenamiento de claves* y el *servidor de almacenamiento de datos*, respectivamente. De lo contrario, deberán adoptarse las siguientes medidas:

7.1) El *proveedor de datos* y *la autenticación y autorización para las comunicaciones* del *servidor de almacenamiento de claves* llevan a cabo una autenticación mutua y obtienen una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

7.2) El *proveedor de datos* se conecta al *servidor de almacenamiento de claves* y almacena en él la clave.

7.3) El *proveedor de datos* y la *autenticación y autorización para las comunicaciones* del *servidor de almacenamiento de datos* llevan a cabo una autenticación mutua y obtienen una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

7.4) El *proveedor de datos* se conecta al *servidor de almacenamiento de datos* y almacena en él el paquete de datos compartidos.

8) La *gestión de políticas de compartición de datos* envía una o varias operaciones DLT junto con sus firmas digitales a los componentes subyacentes de la *infraestructura DLT* y la *gestión de contratos inteligentes basada en DLT* para formar un nuevo bloque que contenga uno o más contratos inteligentes para la compartición de datos. El bloque de nueva creación se distribuye a los nodos DLT asociados. La carga de las operaciones DLT en la cadena DLT depende de la tecnología de implementación específica subyacente (por ejemplo, Hyperledger Fabric, Ethereum Quorum), que queda fuera del alcance de la presente Recomendación.

9) La *gestión de políticas de compartición de datos* informa a los componentes pertinentes de que se ha creado el contrato inteligente para la compartición de datos:

9.1) La *gestión de políticas de compartición de datos* comunica al *proveedor de datos* que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente.

9.2) La *gestión de políticas de compartición de datos* comunica a la *publicación de información sobre la compartición de datos* que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente y la información sobre la compartición de datos.

9.3) La *gestión de políticas de compartición de datos* comunica a la *gestión de permisos de acceso* que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente y los permisos de acceso.

9.4) La *gestión de permisos de acceso* almacena el permiso de acceso.

10) Tras recibir la notificación de la *gestión de políticas de compartición de datos*, la *publicación de información sobre la compartición de datos* publica la nueva información sobre compartición de datos recibida.

11) La *publicación de información sobre la compartición de datos* informa a la *suscripción a información sobre la compartición de datos* de que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente y la nueva información sobre la compartición de datos.

12) Tras recibir la notificación de la *publicación de información sobre la compartición de datos*, la *suscripción a información sobre la compartición de datos* envía a los suscriptores la dirección para firmar el contrato inteligente y la nueva información sobre la compartición de datos.

7.3.2 El procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos con arreglo al permiso solicitado

En la Figura 4 se muestra el procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos con arreglo al permiso solicitado.

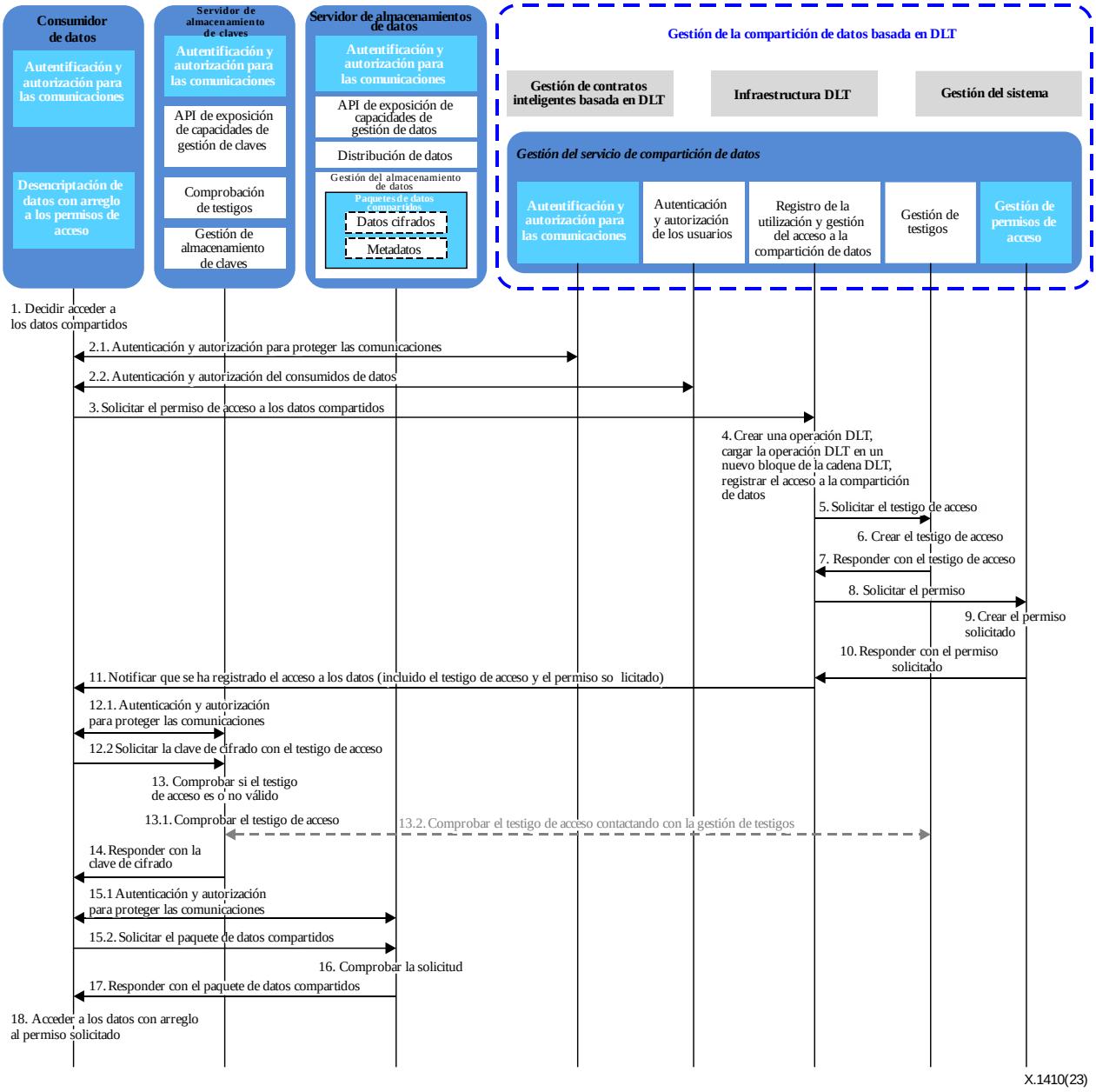

Figura 4 – Procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos con arreglo al permiso solicitado

Como se muestra en la Figura 4, el procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos con arreglo al permiso solicitado es el siguiente:

1) El *consumidor de datos* obtiene la información sobre la compartición de datos buscando en la *publicación de información sobre la compartición de datos* o suscribiéndose a la información publicada o siendo informado por terceros. El consumidor de datos decide acceder a los datos compartidos y firma el contrato inteligente de compartición de datos.

2) Antes de firmar el contrato inteligente de compartición de datos para acceder a los datos compartidos, se llevan a cabo las siguientes operaciones:

2.1) El *consumidor de datos* y la *autenticación y autorización para las comunicaciones* de la *gestión del servicio de compartición de datos* lleven a cabo una autenticación mutua y obtengan una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

2.2) El *consumidor de datos* garantiza que haya una autenticación mutua con el componente de *autenticación y autorización de los usuarios* de la *gestión del servicio de compartición de datos.* Una vez que se haya realizado correctamente la autenticación mutua, el componente de *autenticación y autorización de los usuarios* comprueba si el consumidor de datos tiene derecho a acceder a los datos compartidos.

3) El *consumidor de datos* envía su información de identidad (por ejemplo, el identificador, la clave pública) y la información sobre la compartición de datos junto con su firma digital al *registro de utilización y gestión del acceso a la compartición de datos.*

4) Tras recibir la información de identidad del *consumidor de datos*, la información sobre la compartición de datos y su firma digital, el *registro de utilización y gestión del acceso a la compartición de datos* verifica la firma digital y a continuación comprueba si el consumidor de datos está autorizado a acceder a los datos con arreglo a la política de compartición de datos (por ejemplo, solo un consumidor de datos de una industria o país determinado puede acceder a los datos compartidos). Si se cumplen todos los requisitos para acceder a los datos compartidos, el *registro de utilización y gestión del acceso a la compartición de datos* crea una operación DLT con arreglo a la información recibida del consumidor de datos. El *registro de utilización y gestión del acceso a la compartición de datos* envía una o varias operaciones DLT junto con su firma digital a los componentes subyacentes de *infraestructura DLT* y *gestión de contratos inteligentes basada en DLT* a fin de formar un nuevo bloque que contenga uno o varios registros de acceso a los datos. El bloque de nueva creación se distribuye a los nodos de red DLT asociados. La carga de las operaciones DLT en la cadena DLT depende de la tecnología de implementación específica subyacente (por ejemplo, Hyperledger Fabric, Ethereum Quorum), que queda fuera del alcance de la presente Recomendación.

5) El *registro de utilización y gestión del acceso a la compartición de datos* informa a la *gestión de testigos* para crear un testigo de acceso.

6) Tras recibir la notificación del *registro de utilización y gestión del acceso a la compartición de datos*, la *gestión de testigos* crea un testigo de acceso.

7) La *gestión de testigos* envía el testigo de acceso creado al *registro de utilización y gestión del acceso a la compartición de datos.*

8) El *registro de utilización y gestión del acceso a la compartición de datos* informa a la *gestión de permisos de acceso* para crear el permiso solicitado.

9) Tras recibir la notificación del *registro de utilización y gestión del acceso a la compartición de datos*, la *gestión de permisos de acceso* crea el permiso solicitado.

10) La *gestión de permisos de acceso* envía el permiso solicitado al r*egistro de la utilización y la gestión del acceso a la compartición de datos.*

11) Tras recibir el testigo de acceso y el permiso solicitado, el *registro de utilización y gestión del acceso a la compartición de datos* registra la utilización de los datos compartidos y envía el testigo de acceso, el permiso solicitado, la información clave (por ejemplo, el identificador y su dirección de almacenamiento), la información del paquete de datos compartidos (por ejemplo, el identificador y su dirección de almacenamiento), otra información (por ejemplo, los certificados digitales del *servidor de almacenamiento de claves* y el *servidor de almacenamiento de datos*) al *consumidor de datos*.

12) Tras recibir el testigo de acceso, el permiso solicitado, la información clave y la información del paquete de datos compartidos del *registro de utilización y gestión del acceso a la compartición de datos*, el *consumidor de datos* lleva a cabo las siguientes operaciones:

12.1) El *consumidor de datos* y la *autenticación y autorización para las comunicaciones* del *servidor de almacenamiento de claves* llevan a cabo una autenticación mutua y obtienen una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

12.2) El *consumidor de datos* envía el testigo de acceso a la *comprobación de testigos* del *servidor de almacenamiento de claves* con arreglo a la dirección de almacenamiento de claves para obtener la clave de cifrado.

13) La *comprobación de testigos* del *servidor de almacenamiento de claves* comprueba si es válido el testigo de acceso:

13.1) La *comprobación de testigos* del *servidor de almacenamiento de claves* recibe el testigo de acceso del *consumidor de datos* y a continuación verifica el testigo de acceso.

13.2) Opcionalmente, la *comprobación de testigos* tal vez tenga que comunicarse con la *gestión de testigos* de la *gestión de compartición de datos basada en DLT* al comprobar el testigo de acceso.

14) La *comprobación de testigos* envía el resultado de la comprobación a la *gestión del almacenamiento de claves* del *servidor de almacenamiento de claves.* Tras recibir el resultado de la comprobación realizada por la *comprobación de testigos*, la *gestión del almacenamiento de claves* del *servidor de almacenamiento de claves* envía la clave al *consumidor de datos.*

15) Tras recibir la clave de la *gestión del almacenamiento de claves* del *servidor de almacenamiento de claves*, el *consumidor de datos* realiza las siguientes operaciones:

15.1) El *consumidor de datos* y la *autenticación y autorización para las comunicaciones* del *servidor de almacenamiento de datos* llevan a cabo una autenticación mutua y obtienen una clave de sesión que se utilizará para proteger las ulteriores comunicaciones entre ellos.

15.2) El *consumidor de datos* envía la solicitud al *servidor de almacenamiento de datos* a fin de obtener el paquete de datos compartidos.

16) Tras recibir la solicitud del *consumidor de datos*, la *distribución de datos* del *servidor de almacenamiento de datos* autentica al *consumidor de datos*.

17) La *distribución de datos* del *servidor de almacenamiento de datos* envía el paquete de datos compartidos al *consumidor de datos.*

18) El *consumidor de datos* accede a los datos con arreglo al permiso solicitado. El *consumidor de datos* encripta los datos compartidos de la misma manera que lo hace el *proveedor de datos* tras terminar de acceder a los datos.

Anexo A

Procedimientos relativos a la gestión de la compartición de datos basada en DLT

(El presente anexo es parte integrante de la Recomendación.)

En este anexo se describen dos procedimientos principales: 1) el utilizado por los proveedores de datos para publicar los datos que se compartirán sobre la base de DLT; y 2) el utilizado por los consumidores de datos para acceder a los datos compartidos sobre la base de DLT.

Antes de describir los procedimientos relativos a la gestión de la compartición de datos basada en DLT, se supone que se reúnen las siguientes condiciones:

– cada usuario (por ejemplo, *proveedor de datos*, *consumidor de datos*), ha obtenido un certificado digital y su correspondiente clave privada, generada por él mismo o por una autoridad de certificación;
– cada usuario ha realizado las correspondientes configuraciones correctas (como el certificado digital del nodo DLT, los parámetros de conexión a la red DLT, la configuración de la red);
– los usuarios tienen a su disposición sistemas de encriptación simétricos (por ejemplo, proveedor de datos, consumidor de datos). Estos ofrecen un nivel de seguridad criptográfica suficiente para garantizar la confidencialidad de los datos;
– la *infraestructura DLT* y la *gestión de contratos inteligentes basada en DLT* funcionan adecuadamente;
– la red DLT funciona adecuadamente;
– el *servidor de almacenamiento de claves* y el *servidor de almacenamiento de datos* funcionan adecuadamente.

A.1 El procedimiento utilizado por los proveedores de datos para publicar los datos que se compartirán sobre la base de DLT

En la Figura A.1. se muestra el procedimiento utilizado por los proveedores de datos para publicar datos que se compartirán sobre la base de DLT.

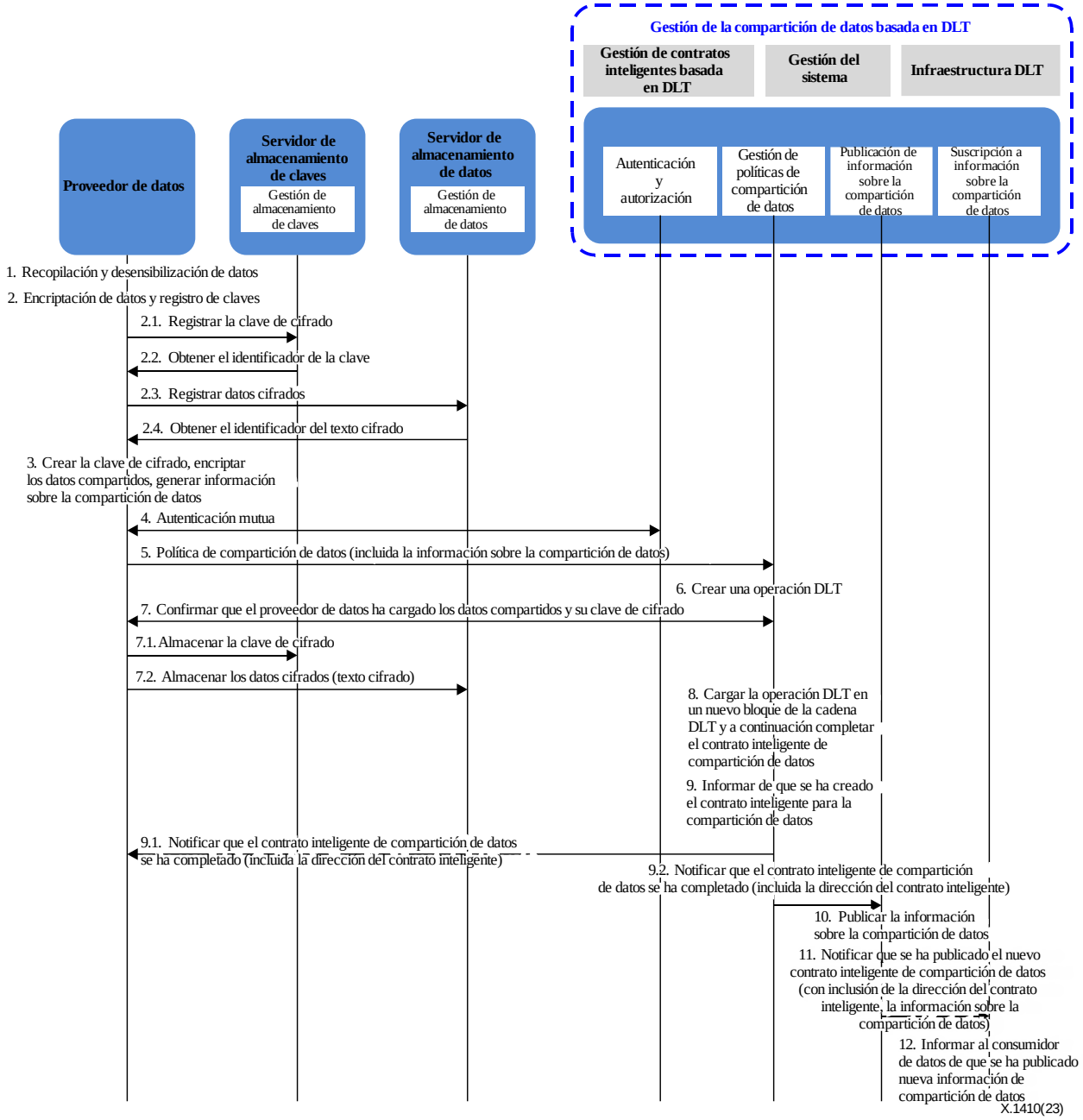

Figura A.1 – Procedimiento utilizado por los proveedores de datos para publicar los datos que se compartirán sobre la base de DLT

Como se ilustra en la Figura A.1, el procedimiento es el siguiente:

1) El *proveedor de datos* recopila los datos originales y los desensibiliza sin incidir negativamente en la calidad de los datos que se van a compartir.

2) El *proveedor de datos* registra los datos que se van a compartir y una clave de un sistema de encriptación simétrico en el servidor de almacenamiento de claves y el servidor de almacenamiento de datos, locales o remotos, de la siguiente manera:

   2.1) generar una clave de cifrado de datos utilizada para un sistema de encriptación simétrico;

   2.2) el *proveedor de datos* obtiene del *servidor de almacenamiento de claves* el identificador de la clave y su dirección de almacenamiento;

2.3) encriptar los datos con la clave que utiliza el sistema de encriptación simétrico, y registrar los datos encriptados, es decir, el texto cifrado;

2.4) el *proveedor de datos* obtiene del *servidor de almacenamiento de datos* el identificador del texto cifrado y su dirección de almacenamiento.

3) El *proveedor de datos* genera una clave de cifrado de datos y encripta los datos que se van a compartir con la clave de cifrado de datos generada. Los datos encriptados constituyen el texto cifrado. El *proveedor de datos* crea información sobre la compartición de datos, que incluye el identificador del proveedor de datos, la clave pública del proveedor de datos, el identificador del texto cifrado y su dirección de almacenamiento, el identificador de la clave de cifrado de datos y su dirección de almacenamiento, las industrias a las que se autorizará el acceso, los usuarios a los que se autorizará el acceso, y otros atributos de datos (por ejemplo, la categoría de datos, la introducción de datos, la utilización, el precio).

4) Antes de publicar los datos que se van a compartir, el *proveedor de datos* garantiza que haya una autenticación mutua con el componente de *autenticación y autorización de los usuarios* de la *gestión de compartición de datos basada en DLT.* Para la autenticación mutua podría utilizarse un certificado digital de credencial. Una vez que se haya realizado correctamente la autenticación mutua, el componente de *autenticación y autorización de los usuarios* comprueba si el proveedor de datos tiene derecho a publicar los datos que se van a compartir.

5) Una vez que se hayan realizado correctamente la autenticación y la autorización, el *proveedor de datos* proporciona la información sobre la compartición de datos con arreglo a los requisitos de la *gestión de políticas de compartición de datos* de la *gestión de la compartición de datos basada en DLT.* El *proveedor de datos* crea una política de compartición de datos con la compartición de datos y otra información. El *proveedor de datos* envía la política de compartición de datos y su firma digital a la *gestión de políticas de compartición de datos.*

6) Tras recibir la política de compartición de datos y la correspondiente firma digital del *proveedor de datos*, la *gestión de políticas de compartición de datos* comprueba la firma digital y a continuación crea una operación DLT.

7) La *gestión de políticas de compartición de datos* confirma con el *proveedor de datos* que la clave y el texto cifrado se han almacenado en el *servidor de almacenamiento de claves* y el *servidor de almacenamiento de datos* respectivamente. De lo contrario, deberán adoptarse las siguientes medidas:

7.1) el *proveedor de datos* almacena la clave en el *servidor de almacenamiento de claves*;

7.2) el *proveedor de datos* almacena el texto cifrado en el *servidor de almacenamiento de datos.*

8) La *gestión de políticas de compartición de datos* envía una o varias operaciones DLT junto con su firma digital a los componentes subyacentes de la *infraestructura DLT* y la *gestión de contratos inteligentes basada en DLT* para formar un nuevo bloque que contenga uno o más contratos inteligentes para la compartición de datos. El bloque de nueva creación se distribuye a los nodos DLT asociados. La carga de las operaciones DLT en la cadena DLT depende de la tecnología de implementación específica subyacente (por ejemplo, Hyperledger Fabric, Ethereum Quorum), que queda fuera del alcance de la presente Recomendación.

9) La *gestión de políticas de compartición de datos* informa a los componentes pertinentes de que se ha creado el contrato inteligente para la compartición de datos.

9.1) La *gestión de políticas de compartición de datos* comunica al *proveedor de datos* que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente.

9.2) La *gestión de políticas de compartición de datos* comunica a la *publicación de información sobre la compartición de datos* que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente y la información sobre la compartición de datos.

10) Tras recibir la notificación de la *gestión de políticas de compartición de datos*, la *publicación de información sobre la compartición de datos* publica la nueva información sobre compartición de datos recibida.

11) La *publicación de información sobre la compartición de datos* informa a la *suscripción a información sobre la compartición de datos* de que se ha completado el contrato inteligente para la compartición de datos. En la notificación se incluye la dirección para firmar el contrato inteligente y la nueva información sobre la compartición de datos.

12) Tras recibir la notificación de la *publicación de información sobre la compartición de datos*, la *suscripción a información sobre la compartición de datos* envía la dirección para firmar el contrato inteligente y la nueva información sobre la compartición de datos al suscriptor.

A.2 El procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos sobre la base de DLT

En la Figura A.2. se muestra el procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos sobre la base de DLT.

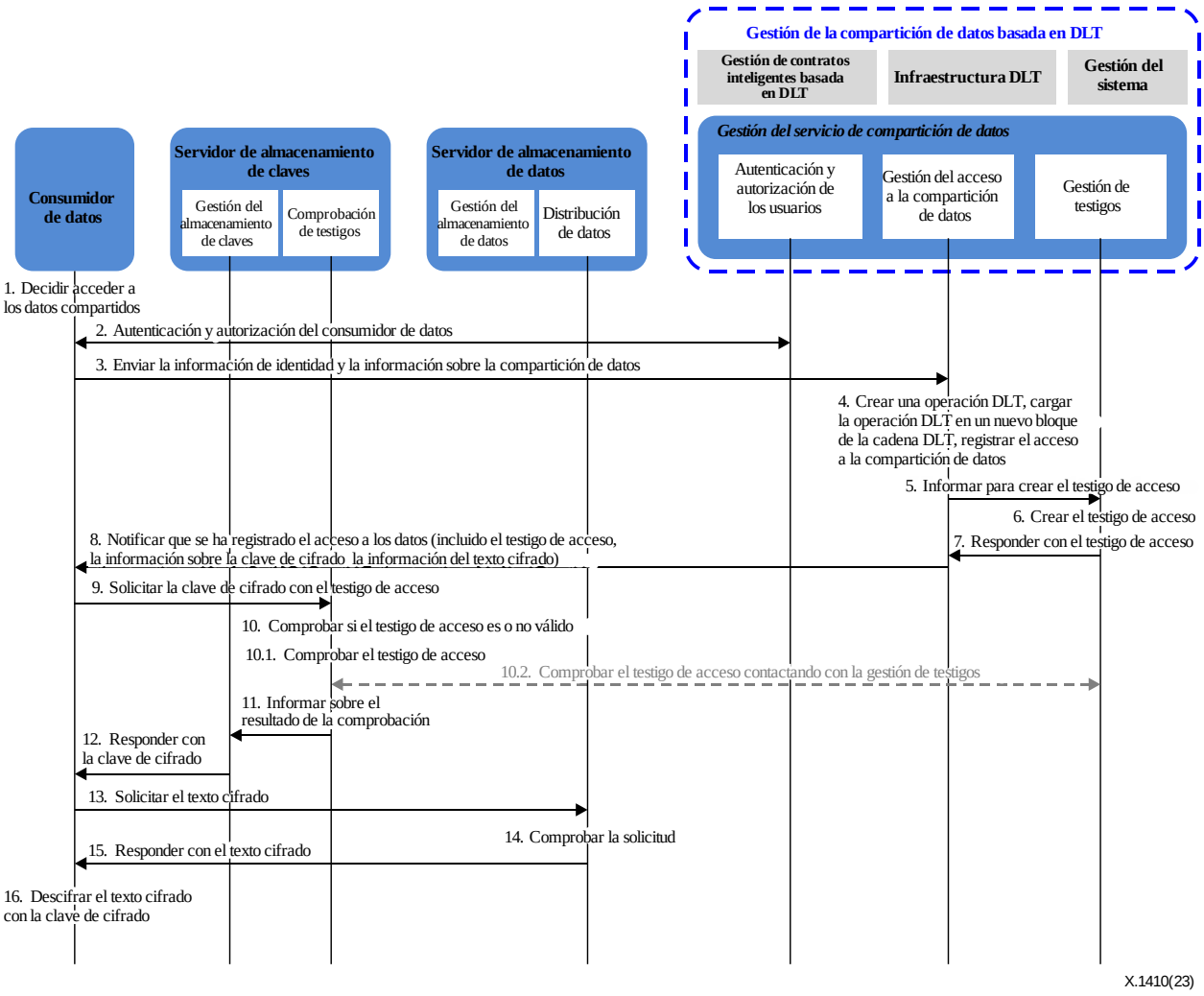

Figura A.2 – Procedimiento utilizado por los consumidores de datos para acceder a los datos compartidos sobre la base de DLT

Como se ilustra en la Figura A.2, el procedimiento es el siguiente:

1) El *consumidor de datos* obtiene la información sobre la compartición de datos buscando en la *publicación de información sobre la compartición de datos* o suscribiéndose a la información publicada o siendo informado por terceros. El consumidor de datos decide acceder a los datos compartidos y firma el contrato inteligente de compartición de datos.

2) Antes de firmar el contrato inteligente de compartición de datos para acceder a los datos compartidos, el *consumidor de datos* garantiza que haya una autenticación mutua con el componente de *autenticación y autorización de los usuarios* de la *gestión de compartición de datos basada en DLT.* Para la autenticación mutua se recomienda utilizar un certificado digital de credencial. Una vez que se haya realizado correctamente la autenticación mutua, el componente de *autenticación y autorización de los usuarios* comprueba si el consumidor de datos tiene derecho a acceder a los datos compartidos.

3) Una vez que se hayan realizado correctamente la autenticación y autorización, el *consumidor de datos* envía su información de identidad (por ejemplo, el identificador, la clave pública) y la información sobre la compartición de datos junto con su firma digital a la *gestión del acceso a la compartición de datos.*

4) Tras recibir la información de identidad del consumidor de datos, la información sobre la compartición de datos y su firma digital, la *gestión del acceso a la compartición de datos* verifica la firma digital y a continuación comprueba si el consumidor de datos está autorizado a acceder a los datos con arreglo a la política de compartición de datos (por ejemplo, solo un consumidor de datos de una industria o país determinado puede acceder a los datos compartidos). Si se cumplen todos los requisitos para acceder a los datos compartidos, la *gestión del acceso a la compartición de datos* crea una operación DLT con arreglo a la información recibida del consumidor de datos. La *gestión del acceso a la compartición de datos* envía una o varias operaciones DLT junto con sus firmas digitales a los componentes subyacentes de *infraestructura DLT* y *gestión de contratos inteligentes basada en DLT* a fin de formar un nuevo bloque que contenga uno o varios registros de acceso a los datos. El bloque de nueva creación se distribuye a los nodos de red DLT asociados. La carga de las operaciones DLT en la cadena DLT depende de la tecnología de implementación específica subyacente (por ejemplo, Hyperledger Fabric, Ethereum Quorum), que queda fuera del alcance de la presente Recomendación.

5) La *gestión del acceso a la compartición de datos* informa a la *gestión de testigos* para crear un testigo de acceso.

6) Tras recibir la notificación de la *gestión del acceso a la compartición de datos*, la *gestión de testigos* crea un testigo de acceso.

7) La *gestión de testigos* envía el testigo de acceso creado a la *gestión del acceso a la compartición de datos*.

8) Tras recibir el testigo de acceso, la *gestión del acceso a la compartición de datos* envía el testigo de acceso, la información clave (por ejemplo, el identificador y su dirección de almacenamiento), la información del texto cifrado (por ejemplo, el identificador y su dirección de almacenamiento), otra información (por ejemplo, los certificados digitales del *servidor de almacenamiento de claves* y el *servidor de almacenamiento de datos*) al *consumidor de datos*.

9) Tras recibir el testigo de acceso, la información clave y la información del texto cifrado de la *gestión del acceso a la compartición de datos,* el *consumidor de datos* envía el testigo de acceso a la *comprobación de testigos* del *servidor de almacenamiento de claves* con arreglo a la dirección de almacenamiento de claves a fin de obtener la clave, que se utiliza para descifrar el texto cifrado.

10) La *comprobación de testigos* comprueba si es válido el testigo de acceso.

10.1) La *comprobación de testigos* del *servidor de almacenamiento de claves* recibe el testigo de acceso del consumidor de datos y a continuación verifica el testigo de acceso.

10.2) Opcionalmente, la *comprobación de testigos* tal vez tenga que comunicarse con la *gestión de testigos* de la *gestión de compartición de datos basada en DLT* al comprobar el testigo de acceso.

11) La *comprobación de testigos* envía el resultado de la comprobación a la *gestión del almacenamiento de claves.*

12) Tras recibir el resultado de la comprobación realizada por la *comprobación de testigos,* la *gestión del almacenamiento de claves* envía la clave de cifrado al *consumidor de datos*.

13) Tras recibir la clave de cifrado de la g*estión del almacenamiento de claves,* el *consumidor de datos* envía una solicitud al *servidor de almacenamiento de datos* para obtener el texto cifrado.

14) Tras recibir la solicitud del *consumidor de datos,* la *distribución de datos* del *servidor de almacenamiento de datos* autentica al *consumidor de datos*.

15) La *distribución de datos* del *servidor de almacenamiento de datos* envía el texto cifrado al *consumidor de datos.*

16) El *consumidor de datos* desencripta el texto cifrado con la clave de cifrado y a continuación accede a los datos compartidos en forma de texto sin formato.

Bibliografía

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

[b-UIT-T X.1400] Recomendación UIT-T X.1400 (2020), *Términos y definiciones utilizados en la tecnología de libro mayor distribuido.*

[b-UIT-T X.1402] Recomendación UIT-T X.1402 (2020), *Marco de seguridad para la tecnología de libro mayor distribuido.*

[b-UIT-T FG DLT D1.1] Especificación técnica UIT-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions.*

[b-ISO/CEI 18033-1] ISO/CEI 18033-1(2021), *Seguridad de la información – Algoritmos de encriptación – Parte 1: Disposiciones generales.*

[b-ISO/CEI 20944-1] ISO/CEI 20944-1:2013, *Tecnología de la información – Interoperabilidad y vínculos de los registros de metadatos (MDR-IB) – Parte 1: Marco, vocabulario común y disposiciones comunes a efectos de conformidad.*

[b-ISO/CEI 29100] ISO/CEI 29100: 2011, *Tecnología de la información – Técnicas de seguridad – Marco de privacidad.*

[b-ISO/CEI/IEEE 15939] ISO/CEI/IEEE 15939:2017, *Ingeniería de sistemas y soporte lógico – Proceso de medición.*

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Conjuntos de cifrado de claves previamente compartidas para la seguridad de la capa de transporte (TLS).*

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Protocolo de intercambio de claves de Internet -Versión 2 (IKEv2).*

[b-IETF RFC 4314] IETF RFC 4314 (2005), *Ampliación de la lista de control de acceso IMAP4.*

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Glosario sobre la seguridad de Internet, versión 2*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *El protocolo de seguridad de la capa de transporte (TLS): versión 1.2.*

[b-IETF RFC 5782] IETF RFC 5782 (2010), *Listas negras y listas blancas del DNS*

[b-IETF RFC 5851] IETF RFC 5851 (2010), *Marco y requisitos del mecanismo de control de nodos de acceso en las redes multiservicios de banda ancha.*

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

Publicado en Suiza
Ginebra, 2023