Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1251

(09/2009)

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

Seguridad en el ciberespacio – Gestión de identidades

Marco para el control de la identidad digital por el usuario

Recomendación UIT-T X.1251

UIT-T

Unión Internacional de Telecomunicaciones

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	
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	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Overview of cybersecurity	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

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

Recomendación UIT-T X.1251

Marco para el control de la identidad digital por el usuario

Resumen

La Recomendación UIT-T X.1251 define un marco para mejorar el control y el intercambio por parte del usuario de la información relativa a su identidad digital. Se definen asimismo capacidades de usuario y funcionales para el intercambio de información sobre la identidad digital. Esto incluye dotar al usuario de la capacidad de controlar la divulgación de información de identificación personal.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T X.1251	2009-09-25	17

Palabras clave

Cliente de identidad digital, contrato digital, gestión de identidades, identidad, identidad digital, intercambio de identidades, servidor de identidades.

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 [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, 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 la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1251[1]

Marco para el control de la identidad digital por el usuario

1 Alcance

En la presente Recomendación se define un marco para mejorar el control y el intercambio por parte del usuario de la información relativa a su identidad digital.

Se definen asimismo capacidades para el intercambio de información sobre la identidad digital. Esto incluye dotar al usuario de la capacidad de controlar la divulgación de información de identificación personal.

NOTA – En la presente Recomendación, la palabra "identidad" referida a la gestión de identidades (IdM, *identity management*) no debe interpretarse en sentido estricto y no supone por tanto ninguna validación positiva de una persona.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de 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 en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[UIT-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad*.

[UIT-T X.1250] Recomendación UIT-T X.1250 (2009), *Capacidades básicas para una mejor gestión y compatibilidad de identidades a escala mundial*.

3 Términos y definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 credencial [b-UIT-T X.1252]: Conjunto de datos presentado como prueba de la identidad y/o los derechos declarados.

3.1.2 entidad [b-UIT-T X.1252]: Cualquier cosa que tenga una existencia independiente y distinta y pueda ser identificada en contexto.

NOTA – Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de éstos. En el contexto de las telecomunicaciones cabe citar como ejemplos de identidades los puntos de acceso, los abonados, los usuarios, los elementos de red, las redes, las aplicaciones informáticas, los servicios, los dispositivos, las interfaces, etc.

3.1.3 federación [b-UIT-T X.1252]: Una asociación de usuarios, proveedores de servicio y proveedores de servicio de identidad.

---

[1] La presente Recomendación podría no ser de aplicación en algunos países debido a su legislación nacional.

3.1.4 identificador [b-UIT-T X.1252]: Uno o varios atributos utilizados para identificar a una entidad en un contexto.

3.1.5 identidad [b-UIT-T X.1252]: Representación de una entidad en forma de uno o varios elementos de información que permiten que la entidad o entidades se distingan suficientemente en un contexto. A los fines de la IdM, el término identidad se entiende como identidad contextual (subconjunto de atributos), esto es, la variedad de atributos está limitada por un marco con condiciones limítrofes definidas (el contexto) en el que la entidad existe e interactúa.

NOTA – Cada entidad está representada por una identidad holística, que comprende todos los posibles elementos de información que caracterizan dicha entidad (los atributos). Sin embargo, la cuestión de la identidad holística es teórica y evita toda descripción y uso práctico debido a que el número de todos los posibles atributos es infinito.

3.1.6 gestión de identidad (IdM) [b-UIT-T Y.2720]: Conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y vinculación, cumplimiento de una política, autentificación y asertos) que se utilizan para:

- garantizar la información de identidad (por ejemplo, identificadores, credenciales, atributos);
- garantizar la identidad de una entidad (por ejemplo, usuarios/abonados, grupos, dispositivos de usuario, organizaciones, proveedores de red y servicios, elementos y objetos de red, y objetos virtuales);
- habilitar aplicaciones de negocios y de seguridad.

3.1.7 proveedor de servicio de identidad (IdSP) [b-UIT-T X.1252]: Entidad que verifica, mantiene, gestiona y puede crear y asignar información sobre la identidad de otras entidades.

3.1.8 información que identifica a la persona (IIP) [b-UIT-T Y.2720]: Información perteneciente a cualquier persona que permite su identificación (entre otras, la información capaz de identificar una persona cuando se combina con otra información, incluso cuando aquélla no identifique con claridad a la persona).

3.1.9 parte confiante [b-UIT-T Y.2720]: Entidad que confía en una representación o declaración de identidad de una entidad solicitante/acertante en algún contexto de petición.

3.1.10 usuario [b-UIT-T X.1252]: Cualquier entidad que utilice un recurso, por ejemplo un sistema, equipo, terminal, proceso, aplicación o red institucional.

3.1.11 centrado en el usuario [b-UIT-T X.1252]: Sistema de IdM que puede facilitar al usuario (IdM) capacidad para controlar la aplicación, y obligar al cumplimiento, de diversas políticas de privacidad y seguridad que rigen el intercambio de la información de identidad, incluida la IIP, entre entidades.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 círculo de confianza: Conjunto de criterios fijados para que una organización pueda ingresar en una federación a fin de que cada una de ellas tenga acceso fiable a los recursos de las demás. Cabe señalar que un círculo de confianza es también el resultado final de la suma de organizaciones en una federación.

3.2.2 contrato digital: Contrato en formato digital firmado por las dos entidades entre las que se ha alcanzado un acuerdo.

3.2.3 identidad digital: Representación digital de la información conocida sobre un particular, grupo u organización específicos.

3.2.4 cliente de identidad digital: Programa cliente que facilita al usuario la gestión de su autentificación y de sus credenciales, el intercambio de su identidad y el servicio de protección de su privacidad.

3.2.5 fraude de identidad: Delito por el que un impostor obtiene piezas clave de la información de identificación personal (IIP), tales como el número de afiliación a la seguridad social y el del permiso de conducir, para utilizarlos en beneficio propio.

3.2.6 información de identidad: Información que identifica a un usuario, incluidas las direcciones fiables (generadas por la red) y/o no fiables (generadas por el usuario).

3.2.7 intercambio de identidades: Proceso de divulgación de la información de identidad del usuario entre un proveedor de servicio de identidad y una parte confiante a través de un cliente de identidad digital.

3.2.8 selector de identidad: Componente de software de un cliente de identidad digital a disposición del usuario para que controle y despache sus identidades digitales

3.2.9 servidor de identidades: Servidor que gestiona las credenciales y la información de identidad del usuario y la facilita a un cliente de identidad digital.

3.2.10 sincronización de identidades: Proceso de actualización de la información de la identidad de usuario divulgada a una parte confiante cuando se modifica la fuente de la información de identidad en el proveedor de servicio de identidad.

3.2.11 terminación de identidad: Proceso de eliminación de la información de identidad de usuario de un almacén cuando su validez expira.

3.2.12 testigo de identidad: Modelo de datos de la identidad digital, que puede contener la IIP y la información de credenciales de un usuario.

3.2.13 suplantación de identidad (*phishing*): Proceso delictivo y fraudulento de intentar adquirir información sensible tal como nombres de usuario, contraseñas y detalles de las tarjetas de crédito, haciéndose pasar por una entidad digna de confianza en una comunicación electrónica.

3.2.14 política de privacidad: Declaración política que define las normas de protección del acceso y divulgación de información personal de carácter privado.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas:

CoT Círculo de confianza (*circle of trust*)

DIC Cliente de identidad digital (*digital identity client*)

DIIF Marco de intercambio de identidades digitales (*digital identity interchange framework*)

IdM Gestión de identidades (*identity management*)

IdS Servidor de identidades (*identity server*)

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

IIP Información de identificación personal

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

RP Parte confiante (*relying party*)

SP Proveedor de servicios (*service provider*)

XML Lenguaje de marcaje extensible (*eXtensible markup language*)

5 Convenios

Ninguno.

6 Capacidades generales

En esta Recomendación se define el siguiente conjunto de capacidades. Las capacidades funcionales y de usuario especificadas a continuación son de carácter obligatorio a menos que se indique lo contrario.

6.1 Capacidades de usuario

Para satisfacer las capacidades de usuario se necesita lo siguiente:

1) Soporte de mecanismos de autentificación mutua.
2) Facilitación de una interfaz de autentificación sólida que soporte diversos mecanismos de autentificación con un cliente de identidad digital (DIC).
3) Facilitación de un selector de identidad que permita al usuario elegir la credencial utilizada para la autentificación. La elección de la credencial utilizada para la autentificación puede estar restringida por los requisitos de algunos sitios web. Para comodidad del usuario, la elección del método de autentificación y la credencial correspondiente puede delegarse en el proveedor de servicio de identidad (el usuario sólo podrá elegir un proveedor de servicio de identidad y no la credencial concreta que se utilizará para la autentificación con ese proveedor de servicio de identidad).
4) Facilitación de una interfaz intuitiva y sólida para gestionar la información de las credenciales del usuario con la máxima seguridad.
5) Soporte de inscripción o suscripción automática a un sitio web para minimizar la interacción del usuario con el sitio, manteniendo el usuario el pleno control para activar y desactivar tales mecanismos. Este requisito es facultativo.
6) Facilitación de la información de identidad siempre que el usuario lo desee, y permitirle que conserve el pleno control del intercambio de identidades mediante un mecanismo de protección de la privacidad adecuado.
7) Facilitación de actualizaciones automáticas de la información de identidad compartida cuando se modifica la información original bajo pleno control del usuario.
8) Facilitación al usuario de control total sobre el establecimiento de políticas de seguridad y privacidad y sobre su aplicación a fin de controlar el intercambio de identidades antes de compartir la información de identidad de manera que el usuario tenga influencia directa en el establecimiento y aplicación de la política.
9) Facilitación a los usuarios de la visión de los detalles de la información de identidad que comparten con cada entidad.
10) Soporte de capacidades de gestión de sesión de autentificación para evitar que el usuario haya de reautentificarse sistemáticamente ante un proveedor de servicio de identidad para acceder a los sitios web.

6.2 Capacidades funcionales

A continuación se definen las capacidades funcionales del marco de intercambio de identidades digitales. Estas capacidades funcionales se requieren para ofrecer las funciones mínimas necesarias para el marco de intercambio de identidades digitales.

1) Soporte de gestión de credenciales integrada que pueda gestionar la información de credenciales de usuario para la autentificación.

2) Soporte de gestión de enlaces de intercambio de identidad para que el usuario conozca detalladamente las entidades con que se conecta para el intercambio de identidad.

3) Soporte de múltiples mecanismos de autentificación que puedan incluir autentificaciones basadas en la contraseña, basadas en la PKI y basadas en los datos biométricos.

4) Soporte de mecanismos de intercambio de identidades que puedan establecer un enlace bidireccional para compartir la información de identidad del usuario entre entidades que empleen DIC.

5) Soporte de un mecanismo de contrato digital que establezca un contrato para el intercambio de identidades que se empleará para aplicar las políticas de seguridad y privacidad sobre divulgación de IIP.

6) Soporte de la sincronización de información de identidad para actualizar la información de identidad distribuida y compartida de manera coherente cuando se modifica la fuente de información de identidad divulgada. La información de identidad que ha de sincronizarse se limita a la IIP que modifica directamente el usuario.

7) Soporte de transformación de testigo universal para que el marco sea compatible con los sistemas de gestión de identidad existentes.

8) Hacer que el marco sea lo más independiente posible al proceso de autentificación para evitar dependencias entre el DIC y los mecanismos de autentificación soportados en los proveedores de servicio de identidad (o, al menos, que el marco soporte fácilmente todos los mecanismos de autentificación, en particular los específicos del operador de telecomunicaciones).

9) Soporte de mecanismos que permitan al proveedor de servicio de identidad interactuar con el usuario durante el proceso de autentificación y facilitar su propia interfaz de autentificación (GUI).

10) Soporte del almacenamiento de testigos de identidad en diversos medios (lápiz USB, tarjeta SIM, servicio de almacenamiento en red, etc.) con una capa de almacenamiento bien definida que utilizará DIC.

6.3 Directrices de seguridad

A fin de elaborar un DIIF seguro, se recomienda seguir las siguientes directrices de seguridad:

– La seguridad de la comunicación DIIF dependerá del modelo de confianza subyacente, que normalmente se basa en una infraestructura de gestión de claves (por ejemplo, PKI o clave secreta).

– Se debería utilizar algún tipo de protocolo de seguridad de la capa de transporte para asegurar la integridad y confidencialidad de los datos (por ejemplo, por encriptación) cuando el mensaje se transporta por la red.

– El contrato digital debería llevar la firma digital de las partes en el acuerdo. De ser necesario, puede estar encriptado.

– Los datos, incluida la información de identidad, almacenados en el DIC deberían llevar una firma digital y estar encriptados durante el almacenamiento.

– Dado que los usuarios pueden trasladar su testigo de identidad de un dispositivo a otro, ha de haber una política de mantenimiento de la seguridad de los datos mientras se encuentren en tránsito.

7 Control de usuario mejorado del intercambio de identidades digitales

7.1 Introducción

La federación de identidades [b-LA-FF] se constituye para conectar la información de identidades distribuida entre un proveedor de servicio de identidad (IdSP) y un proveedor de servicios (SP). Si el SP quiere garantizar la información de autentificación del IdSP, deberá existir una relación de confianza entre ambas partes. Este dominio de confianza se denomina círculo de confianza (CoT) y puede incluir uno o más IdSP y SP. En un CoT, si el usuario se autentifica en un IdSP, se permite el acceso a los SP dentro del CoT sin proceder a más autentificaciones. Así, el usuario sólo se ha de autentificar una vez en el CoT.

Sin embargo el número de autentificaciones a que se ha de someter el usuario aumenta conforme crece el número de CoT. En esta situación, el usuario tiene que autentificarse ante el CoT cada vez que lo visita. Esto significa que el usuario ha de gestionar la información de credenciales de un IdSP en un CoT, lo que a menudo causa que el usuario olvide la contraseña o la escriba, aumentando así el riesgo de divulgación no autorizada. La federación dentro de un CoT es una manera cómoda de intercambiar la información de identidad de usuario, aunque la compartición de información de identidad entre CoT requiere que se disponga previamente de un acuerdo comercial, lo cual suele llevar bastante tiempo debido a los procedimientos legales que ello implica. Cuando el dominio para la gestión de identidades se limita al entorno de la empresa, la tecnología de federación funciona adecuadamente; pero si el dominio del sistema de gestión de identidades (IdM) se extiende a Internet, resulta difícil cerrar acuerdos comerciales entre empresas para todas las federaciones.

En los sistemas de IdM a gran escala centrados en la aplicación puede ocurrir que los servicios y políticas de identidad estén diseñados para satisfacer los requisitos de los IdSP y los SP y estén optimizados para satisfacer los requisitos de las aplicaciones (por ejemplo, configuración de la información de cuenta de usuario). Cuando un servicio de identidad se configura para el usuario, el intercambio de identidades suele llevarse a cabo entre un IdP y un SP directamente. En este caso, el usuario tiene un control limitado sobre la divulgación de su información de identidad.

Dado que hay un flujo y reflujo de información de identidades entre las entidades empresariales sin intervención del usuario, el control de la privacidad y su consiguiente protección pueden dejarse de lado. El problema se presenta cuando dos entidades intentan compartir la información de identidad de un usuario que a su vez pertenece a éste. Dado que las dos entidades tienen que utilizar la identidad del usuario, necesitan establecer un acuerdo comercial y de política de privacidad previo. Cuando una entidad sólo necesite compartir la identidad del usuario con el propietario original, cada identidad sólo necesitará concluir un contrato con el propietario (o con la entidad que gestiona su identidad) y establecer una política de seguridad y privacidad para la utilización de su información de identidad.

Para resolver este problema, se define en la presente Recomendación un marco que permite mejorar el control y el intercambio por parte del usuario de la información relativa a su identidad digital.

7.2 Amenazas contra la seguridad

Cabe suponer que la mayor parte de las amenazas que aparecen en el ciberespacio existen también en los sistemas de IdM. Las amenazas generales contra la seguridad en el ciberespacio se describen en [UIT-T X.1205].

En los sistemas de IdM, hay varias amenazas contra la seguridad que los hacen vulnerables o comprometen su seguridad de tal manera que la organización queda expuesta al peligro. La suplantación de identidad es uno de los tipos más comunes de amenazas contra la seguridad que existen en el entorno IdM.

El robo de identidad constituye una cuestión de seguridad de la mayor gravedad, especialmente para las organizaciones que almacenan y gestionan grandes volúmenes de información de identificación personal. No se trata tan sólo del riesgo de que se produzca una pérdida de datos personales que socave la confianza de los clientes y de las instituciones y ocasione costosos daños para la reputación de las organizaciones, sino de que la fuga de datos pueda resultar también enormemente costosa para las organizaciones desde el punto de vista económico. En la actualidad el robo de identidad puede realizarse mediante suplantación de identidad o *phishing*.

La suplantación de identidad es un intento por parte de un tercero de solicitar información confidencial a un individuo, un grupo o una organización haciéndose pasar por, o simulando ser, una marca específica generalmente conocida, casi siempre con ánimo de lucro. Un sitio web de suplantación de identidad es aquel que está diseñado para hacerse pasar por un sitio web legítimo de la organización cuya marca está siendo suplantada. El atacante intenta engañar a los usuarios para que muestren sus datos personales tales como los números de sus tarjetas de crédito, sus credenciales bancarias en línea y otra información sensible que pueden utilizar para cometer actos fraudulentos. En los sistemas de IdM, la suplantación de identidad constituye una seria amenaza debido a que una vez captada por el atacante la información de autentificación de la víctima, u otra que permite identificar a la persona, puede ser utilizada para el robo de su identidad o para otra actividad fraudulenta.

7.3 Modelo conceptual para el intercambio de identidades digitales

En este modelo conceptual, el marco de intercambio de identidades digitales (DIIF) emplea el concepto de cliente de identidad digital (DIC) que puede controlar el intercambio de información de la identidad digital. El control que se otorga al usuario para que controle la divulgación de información de identidad puede reducir sustancialmente las amenazas contra la seguridad que se describen en la cláusula anterior (véase la cláusula 7.2).

En la figura 1 se ilustra el modelo conceptual para el intercambio de identidades digitales.

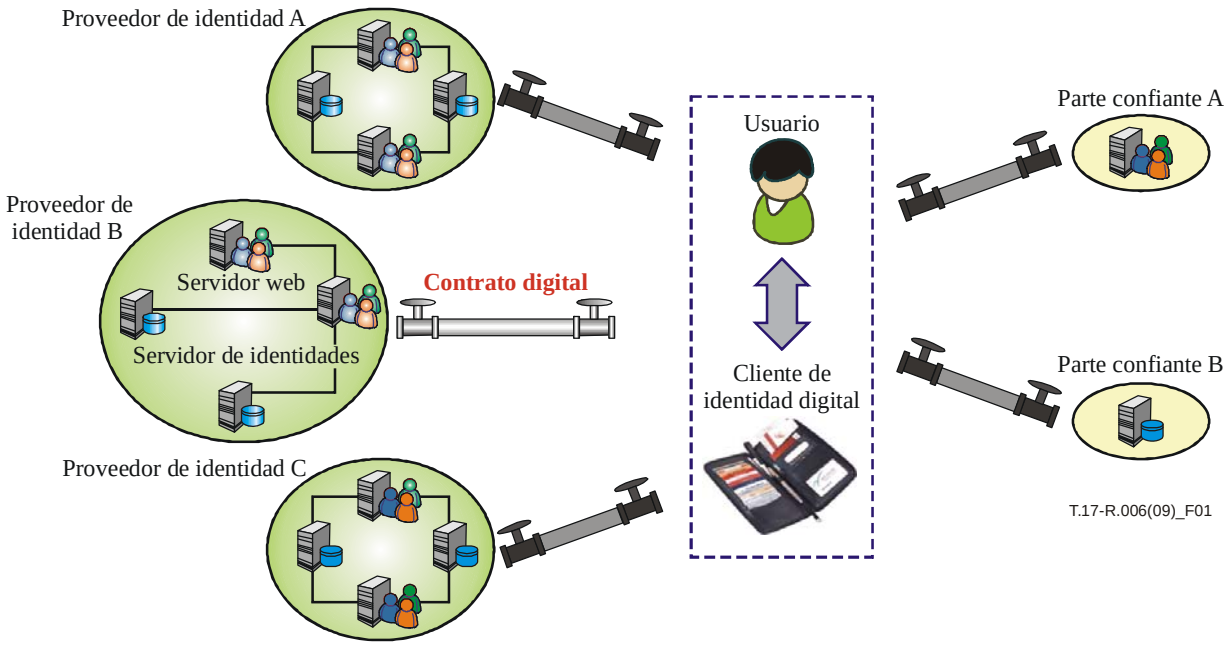

Figura 1 – Modelo conceptual de intercambio de identidades digitales

7.3.1 Servidor de identidad

El servidor de identidad (IdS) es el principal servidor que da información de identidad de los usuarios a las entidades que lo solicitan o que solicita al DIC información de identidad para los servicios web. El IdS puede ser un proveedor de servicio de identidad si suministra información de identidades; de lo contrario, puede ser una parte confiante (RP) si utiliza la información de identidad proporcionada por el usuario. Puede ocurrir que la función de un IdS sea tanto la de proveedor de servicio de identidad como la de parte confiante. En este caso, el IdS difunde su propia información de identidad para algunos servicios web mientras que exige la información de identidad del usuario para otros servicios web. Un servidor web puede solicitar al IdS que suministre información sobre la identidad del usuario a fin de proporcionar un servicio web.

7.3.2 Cliente de identidad digital

El cliente de identidad digital es un programa que facilita al usuario la gestión de la autentificación, las credenciales y la sesión, el intercambio de identidades y el servicio de protección de la privacidad. Cuando necesita compartir información de identidades con un IdSP o RP, el DIC establece un enlace con el IdS en un dominio. El DIC puede formalizar un contrato con el IdS que describa los términos y condiciones que afectan al servicio de intercambio de identidades para mejorar la seguridad y privacidad del intercambio de información de identidad. Cada una de las informaciones de identidad del usuario pasa por el DIC, de modo que el usuario en cuestión puede controlar la compartición de la información de su identidad. En particular, dependiendo de la política acordada entre el usuario y la entidad, el usuario controla por completo cuáles son los datos de identidad que se intercambian, con qué entidades, en qué momento y con qué objeto. El descubrimiento de la información de identidad del usuario no es necesario dado que el cliente tiene toda la información del enlace necesaria para enviar y recuperar la información de identidad.

7.3.3 Proveedor de servicio de identidad

El proveedor de servicio de identidad (IdSP) es la entidad que gestiona la información de identidad del usuario, ofrece servicios de autenticación y autorización y presta servicios de intercambio de identidades para los servidores web. El IdSP es el modelo de función conceptual que puede asignarse a la entidad que gestiona la identidad del usuario y proporciona dicha información cuando el DIC la solicita. El IdSP gestiona la información de identidad sometida por el usuario o generada por él.

7.3.4 Parte confiante

La parte copiante (RP) es otro modelo de función conceptual que está asignado a la entidad que solicita a un DIC la identidad de un usuario y presta un servicio utilizando la información de identidad recibida. La RP no confía en el IdSP para realizar la autentificación. Los usuarios harán de emplear el DIC para autentificarse ante la RP.

7.3.5 Usuario

La definición de usuario se encuentra en la cláusula 3. En el modelo conceptual, usuario se refiere generalmente a una persona o abonado en un contexto de IdM centrado en el usuario. El usuario es el usuario extremo que posee y ejecuta un DIC.

7.4 El contrato digital

La información de identificación personal (IIP) que fluye entre un proveedor de servicio de identidad y una parte confiante debe pasar por un cliente de identidad digital en un entorno de gestión de identidades centrada en el usuario. Esto ofrece al usuario la posibilidad de controlar la utilización de su información de identificación personal. Un contrato digital se establece únicamente entre un usuario y un IdSP o entre un usuario y una parte confiante. No se permite establecer contratos multipartitos, pues podrían complicar las cuestiones de gestión a las que debe enfrentarse el usuario. El contrato digital constituye el componente central que puede proporcionar

el control minucioso, por parte del usuario, de los flujos de información de identificación personal. En la figura 2 se representa la estructura de un contrato digital.

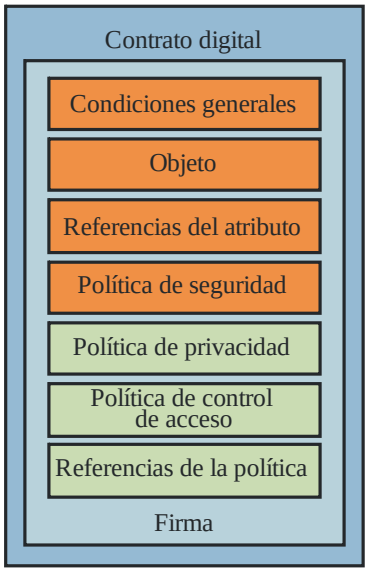

Figura 2 – Estructura del contrato digital

Entre los tipos de controles que pueden definir los contratos digitales se encuentran las políticas necesarias para mediar en una relación de intercambio de identidades. Dependiendo de la reglamentación y demás requisitos de política, es posible que el contrato digital no sea necesario en todos y cada uno de los intercambios de identidad, sino tan sólo cuando sea necesario controlar el flujo o almacenamiento en memoria intermedia de la IIP compartida. Este componente es tan flexible y ampliable como los contratos en la vida real (por ejemplo, los acuerdos sobre confidencialidad). Además, dado que los contratos digitales pueden consistir en documentos XML, pueden ordenar su propia revisión, modificación y supresión (es decir, exactamente como los contratos en la vida real). Entre los elementos del contrato se incluyen los siguientes:

1) Condiciones generales: Describen la versión, fecha del acuerdo y fecha de validación así como los posibles avisos a los usuarios. Este elemento tiene carácter obligatorio.

2) Objeto: Uso al que se destina la información de IIP del usuario. Se trata de un elemento obligatorio.

3) Referencias del atributo: Indican qué atributos de una entidad están contemplados en el contrato. Se trata de un elemento obligatorio.

4) Política de seguridad: Este elemento ha de contener la política de seguridad de la información y de la autentificación que especifique cómo pueden autentificarse dos entidades y cómo se asegura la información. Este elemento tiene carácter obligatorio.

5) Política de privacidad: Este elemento puede contener cualquier tipo de declaración de política de privacidad. En él pueden especificarse la sincronización y la terminación de la IIP del usuario divulgada. Ha de garantizarse la protección de la privacidad de conformidad con la legislación sobre privacidad regional/nacional en materia de privacidad aplicable. Este elemento tiene carácter opcional.

6) Política de control de acceso: Este elemento puede describir cualquier política de control de acceso o política de autorización. Este elemento tiene carácter opcional.

7) Referencias de la política: Pueden especificarse aquí las referencias a políticas definidas externamente. Este elemento tiene carácter opcional.

8) Firma: Los contratos pueden concertarse por dos entidades que llegan a un acuerdo acerca del contenido del contrato digital. Sin embargo, el contrato puede tener un máximo de dos firmas digitales, que representan a las dos entidades que celebran el contrato. Sin embargo, por los motivos aducidos en el primer párrafo de esta cláusula, no puede haber más de dos firmas. Para su validez e integridad es necesario que lo firmen las dos entidades. Al firmar el contrato, el usuario da su consentimiento. El ámbito de una firma preceptiva abarca desde las condiciones generales a las referencias de política como se muestra en la figura 2. Este elemento tiene carácter obligatorio.

7.5 Tres capas para el intercambio de identidades

En esta cláusula se definen tres capas: la de aplicación, la de intercambio de identidades y la de comunicación.

7.5.1 Capa de aplicación

La capa de aplicación puede consistir en la típica aplicación web que se ejecuta en Internet o en un entorno de comunicaciones móviles. Por ejemplo, el usuario utiliza un navegador web para solicitar a un servidor web un servicio web. Cuando una entidad de la aplicación necesite solicitar una autentificación o el servicio de identidades, llamará al servicio indicado en la capa de intercambio de identidades. Lógicamente, el DIC se encuentra tanto en la capa de aplicación como en la de intercambio de identidades conectando ambas capas para ofrecer al usuario servicios relativos a la identidad, sin solución de continuidad. Cada vez que el usuario intenta conectarse a un sitio web, llama al selector de identidades, que es un componente del gestor de la interfaz de usuario en el cliente, para seleccionar un testigo que equivale a una identidad para autentificarse en el sitio web. Cuando una aplicación web necesita compartir la información de identidad del usuario para satisfacer la petición de servicio de éste, puede llamar a uno de los servicios de intercambio de identidades especificados en la capa de intercambio de identidades. En la capa de intercambio de identidades se incluye la ubicación de la descripción de servicio para la administración de la aplicación web.

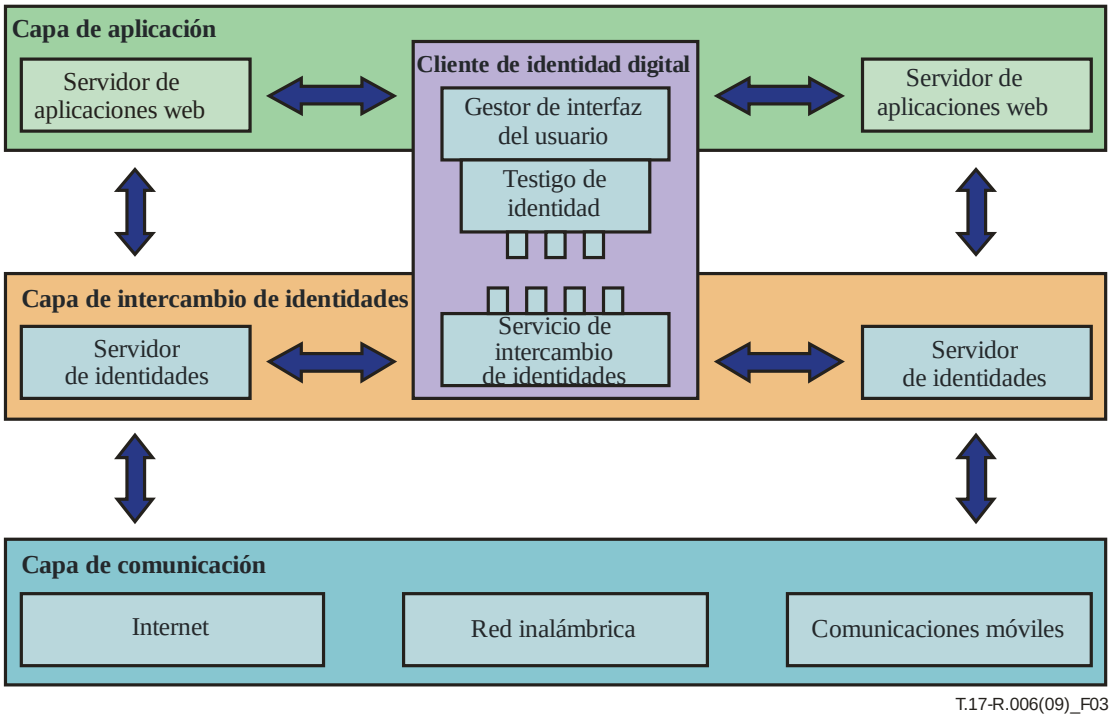

Figura 3 – Capa de intercambio de identidades

7.5.2 Capa de intercambio de identidades

La capa de intercambio de identidades se comporta como una capa de enlace de intercambio de identidades transparente que facilita el intercambio de identidades entre entidades y otorga al usuario pleno control para aplicar su política de seguridad y privacidad.

Gracias a esta capa, la compartición de la información de identidades entre diversas entidades puede desarrollarse e implantarse con independencia de la aplicación, ya que una aplicación no necesita conocer en detalle la operación del intercambio de identidades. Además, la capa de intercambio de identidades puede ofrecer diversas funciones relacionadas con el intercambio de identidades a las soluciones IdM existentes que no dispongan de capacidades de intercambio de identidades. En la cláusula relativa al contrato digital se ofrece una descripción detallada de cómo la capa de intercambio de identidades facilita el cumplimiento de la política de seguridad y privacidad (véase la cláusula 7.4).

7.5.3 La capa de comunicación

La capa de comunicación es una capa independiente responsable del transporte de datos entre dispositivos.

8 Marco de intercambio de identidades digitales

8.1 Principios de diseño

Para poder ofrecer el intercambio de identidades sin solución de continuidad entre entidades en cualquier entorno informático, incluso móvil y ubicuo, este marco se ha inspirado en los siguientes principios de diseño:

- **Independencia** – Este marco no está vinculado a ninguna aplicación ni entorno de red específico. Dicho de otro modo, el propio marco debe ser adaptable a cualquier entorno, siempre que sea necesario.
- **Capacidad de integración** – En un entorno informático móvil o ubicuo, el usuario puede utilizar varios dispositivos para su trabajo o entretenimiento. En este caso, lo que el usuario necesita es la información de identidad esencial que pueda establecer su identidad. Esta información debe diseñarse para ajustarse a cualquier dispositivo de modo que el usuario sólo tenga que integrar la información de su identidad en el dispositivo para utilizarla.
- **Flexibilidad** – Este marco debe diseñarse con la suficiente flexibilidad para acoplarse a cualquier dispositivo, desde una estación de trabajo a un pequeño dispositivo informático portátil. El marco debe ser lo suficientemente maleable como para poder configurarse de modo que se adapte a distintos entornos informáticos.
- **Capacidad evolutiva** – Este marco tiene que poder utilizarse tanto en un dominio sencillo como entre dominios, sin que se necesite una sobrecarga de comunicación o computación para integrarlo en un sistema existente.

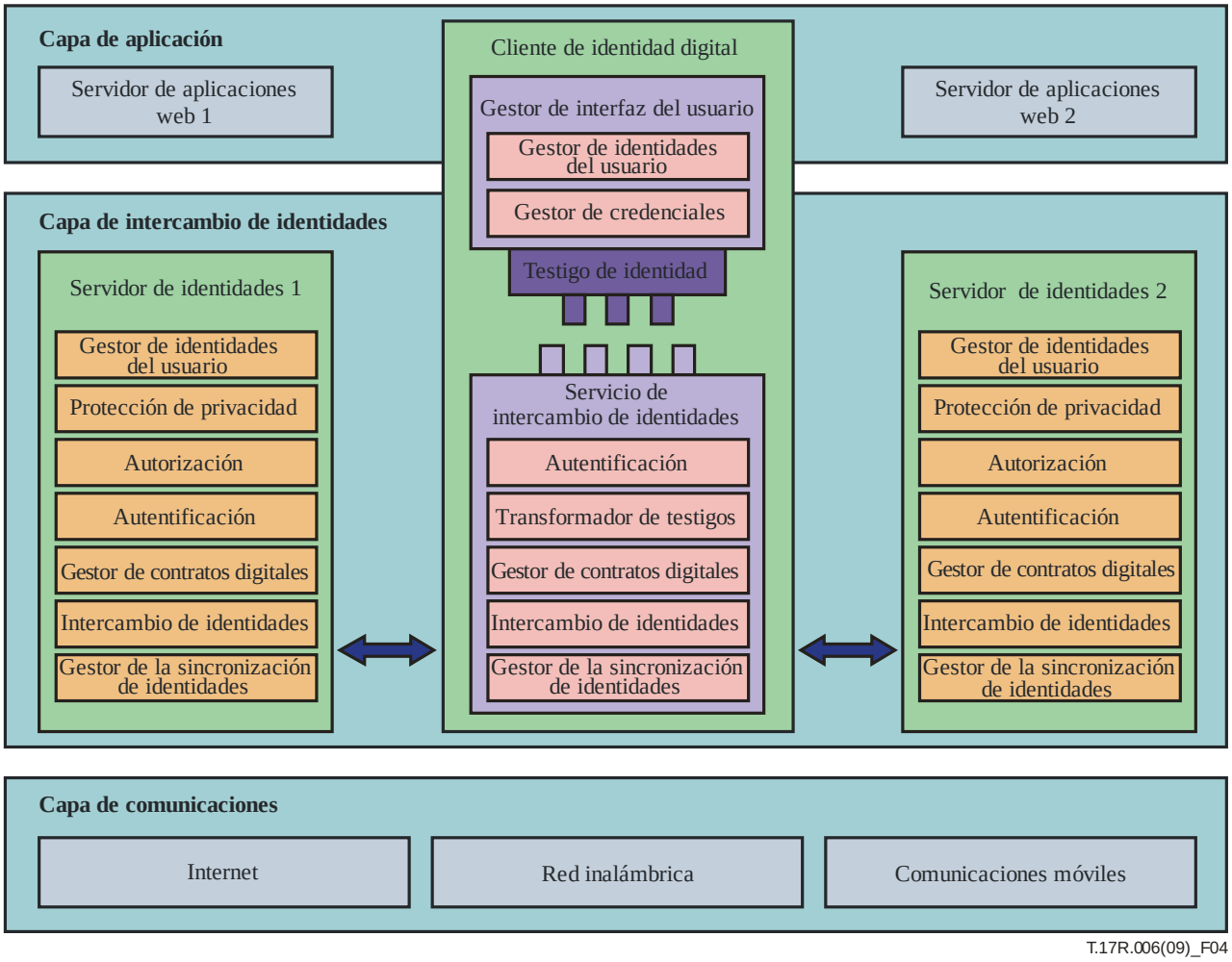

Figura 4 – Marco de intercambio de identidades digitales

8.2 Componentes de este marco

El DIC es el componente central de este marco y facilita el enlace de identidades conectando a todos los proveedores de servicio de identidad de usuario y partes confiantes. Un usuario puede recuperar y actualizar su información de identidad cada vez que lo necesite, utilizando el enlace preestablecido.

El DIC consta de tres partes: gestor de la interfaz del usuario, servicio de intercambio de identidades y testigo de identidad.

En la figura 4 se representan los componentes funcionales de este marco.

8.2.1 Gestor de identidades del usuario

Este componente gestiona la información de identidad del usuario que se compartirá con otras entidades. En el IdS, la gestión de identidades se centra principalmente en el almacenamiento. Por otra parte, la gestión de identidades en el DIC intenta centrase en la interfaz gráfica del usuario que presenta la información de identidad.

8.2.2 Protección de la privacidad

Éste es el componente que gestiona la función de privacidad que protege la información de identidad del usuario. Efectúa un seguimiento de la información de auditoría de la utilización y fin de la identidad del usuario. Esta función también cumple los requisitos de privacidad descritos en el contrato digital siempre que se utilice la identidad del usuario, ya sea involuntariamente o a

propósito. Ha de garantizarse la protección de la privacidad de conformidad con la legislación regional/nacional en materia de privacidad aplicable.

8.2.3 Autorización

El servicio de autorización está diseñado para la toma de decisiones relativas a los derechos de acceso del usuario y para hacer cumplir las decisiones de autorización correspondientes a los privilegios del usuario. La autorización es un servicio opcional. Sólo se suministra cuando hay que controlar el acceso a los recursos en función de los derechos del usuario.

8.2.4 Autentificación

Este componente proporciona un marco de autentificación genérico que soporta diversos tipos de mecanismos de autentificación. El servicio de autentificación comprende la autentificación mutua entre clientes y servidores

8.2.5 Gestor de contratos digitales

Éste es el componente que gestiona la lista de contratos digitales concluidos entre el usuario y el proveedor de servicio de identidad para la autentificación, control de acceso y protección de la privacidad. El gestor determina el periodo de vigencia de los contratos digitales suscritos con firmas digitales.

8.2.6 Intercambio de identidades

Éste es el componente central que proporciona el servicio de intercambio de identidades. El intercambio de identidades se divide en dos servicios: recuperación y actualización. Si la información de identidad se almacena en una entidad, el DIC puede recuperar su identidad de la entidad, y viceversa. Si se modifica la información de identidad almacenada en la entidad, ésta puede actualizar o introducir en el DIC la información de identidad modificada, y viceversa. La descripción detallada de este componente queda fuera del alcance de la presente Recomendación.

8.2.7 Gestor de sincronización de identidades

Éste es el componente que gestiona el proceso de sincronización de identidades en el DIC. Cuando se modifica la información de identidad almacenada en el IdSP, éste actualiza en el DIC la identidad modificada. En el DIC, este componente lleva a cabo la operación de actualización de identidades en la función de intercambio de identidades para cada parte confiante con la que el DIC haya compartido la identidad del usuario. Obsérvese que sólo podrá recibir la identidad actualizada la parte confiante para la que el DIC haya introducido alguna vez su identidad.

8.2.8 Gestor de la interfaz del usuario

Éste es el componente que representa la interfaz gráfica del usuario para la identidad del usuario y la información de sus credenciales. Por lo general, este componente guarda una estrecha relación con el servidor de aplicaciones web cuando el usuario necesita autentificarse para conectarse o compartir la información de su identidad para algún servicio.

8.2.9 Gestión de credenciales

Éste es el componente que gestiona la información de las credenciales de autentificación generada por la entidad o por el sitio. Un usuario puede tener varias credenciales tales como la contraseña, el certificado X.509 y sus datos biométricos. Para que el usuario tenga siempre la misma percepción, se define una representación gráfica común de la información de sus credenciales.

8.2.10 Testigo de identidad

El testigo de identidad es un modelo de datos para la identidad digital. Puede integrarse en un cliente de identidad digital a fin de conectar el gestor de la interfaz del usuario al servicio de intercambio de identidades para permitir el funcionamiento del DIC. La representación lógica del testigo puede realizarse cuando se conecta el gestor de la interfaz del usuario. Por ejemplo, para que un usuario conecte el entorno de trabajo de su ordenador personal a un teléfono móvil, sólo necesitará llevar consigo el testigo e integrarlo en el teléfono móvil. El soporte físico del testigo puede ser una tarjeta inteligente, un dispositivo USB, etc.

8.2.11 Servicio de intercambio de identidades

Ésta es la parte del servicio responsable de la sincronización e intercambio de identidades. Dependiendo de la red o plataforma de comunicaciones en la que se utilice, se requiere la modificación de esta parte para adaptarla al entorno. Por ejemplo, el módulo de servicio de intercambio de identidades en un ordenador personal es totalmente distinto del de un teléfono móvil.

8.2.12 Transformador de testigos

Éste es el componente que transforma un testigo emitido por otro sistema IdM en un testigo que pueda ser comprendido y procesado en el DIIF. Éste es el componente de pasarela para interactuar con otros sistemas IdM para el intercambio de diversos testigos (por ejemplo, el de identidad y el de seguridad). Este componente tiene carácter opcional.

Apéndice I

Directrices de implementación de referencia para un marco de control de la identidad digital por parte del usuario utilizando WS-Confianza y la tecnología de tarjeta de información

(Este apéndice no es parte integrante de la presente Recomendación)

NOTA – En este apéndice se presenta un ejemplo de correspondencia entre WS-Confianza [b-WS-TRUST] y la tarjeta de información [b-IS-INTEROP] con las capacidades de la presente Recomendación.

I.1 Introducción

En este apéndice se describe cómo se satisfacen los requisitos descritos en la presente Recomendación mediante WS-Confianza y la tecnología de tarjeta de información que se describen en [b-CARDSPACE].

I.2 Antecedentes

I.2.1 El cliente de identidad digital

En la cláusula 7.3.2 se describe "el concepto de cliente de identidad digital que puede controlar el intercambio de identidades digitales".

I.2.2 La capa de intercambio de identidades

En la cláusula 7.5.2 se describe la "capa de intercambio de identidades para facilitar el intercambio de identidades entre entidades y otorgar a una entidad el pleno control para imponer sus políticas de seguridad y privacidad".

I.2.3 WS-Confianza

La especificación WS-Confianza es una ampliación de WS-Seguridad destinada a ofrecer un marco para la solicitud y emisión de testigos de seguridad y para mediar en las relaciones de confianza. El solicitante, normalmente en representación de una entidad, envía un mensaje de petición de testigo de seguridad (RST, *RequestSecurityToken*) al servicio de testigos de seguridad (STS, *security token service*) y recibe una respuesta a la petición de testigo de seguridad (RSTR, *RequestSecurityTokenResponse*) que suele contener un testigo de seguridad. El testigo de seguridad contiene un conjunto de declaraciones y puede enviarse a un servicio web como prueba de identidad del solicitante. Opcionalmente puede enviarse una RST a un servicio de testigos de seguridad con una petición de validar o cancelar un testigo de seguridad previamente emitido. Estas interacciones se representan en la figura I-1.

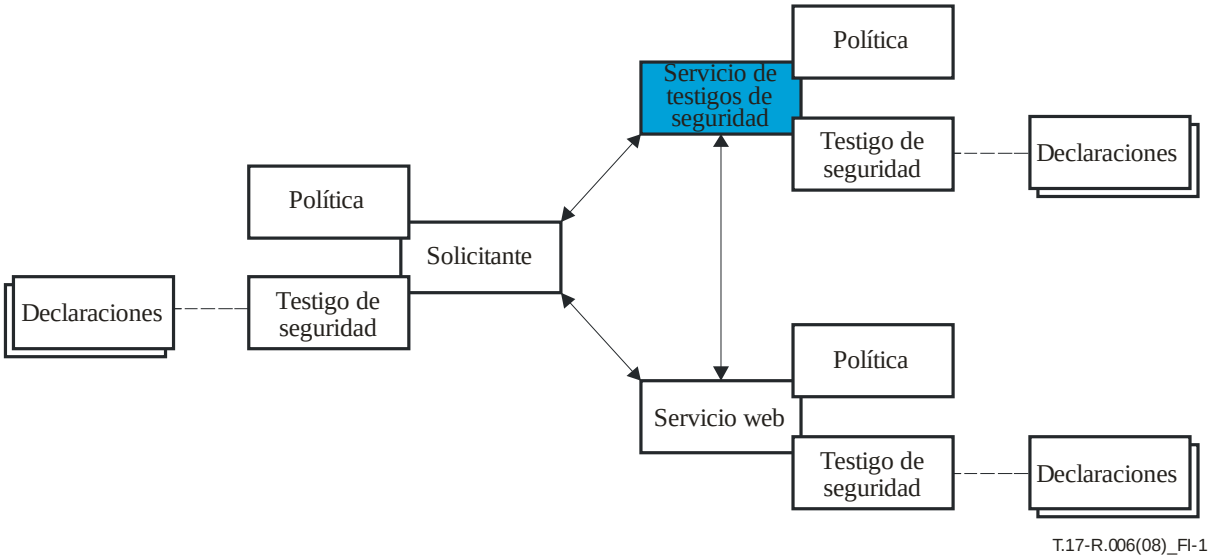

Figura I.1 – Confianza directa con WS-Confianza

Puede utilizarse WS-Confianza para implementar una diversidad de modelos además del modelo de confianza directa sencillo. En ciertos casos se utilizará un modelo indirecto cuando el IP/STS (proveedor de servicio de identidad/servicio de testigos de seguridad) envíe una RST a otro STS para satisfacer la RST original, como se representa en la figura I-2.

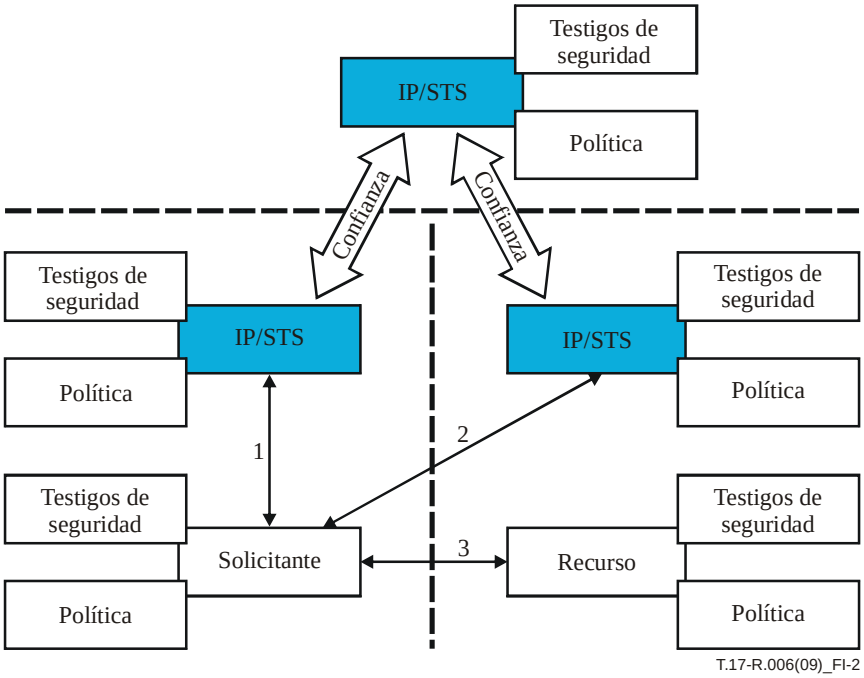

Figura I.2 – Confianza indirecta con WS-Confianza

I.2.4 La tarjeta de información

La tecnología de tarjeta de información se describe en el perfil de interoperabilidad del selector de identidades [b-IS-INTEROP]. Con la tecnología de tarjeta de información, un selector de identidades y los componentes del sistema de identidades asociado permiten a las entidades gestionar sus identidades digitales procedentes de distintos proveedores de servicio de identidad, y emplearlas en diversos contextos para acceder a servicios en línea.

Cuando las entidades establecen una relación con los IdSP, reciben tarjetas de información, las cuales contienen metadatos que describen los testigos de seguridad potenciales que pueden solicitarse mediante un WS-Confianza así como los mecanismos de seguridad utilizados para proteger y autentificar el intercambio de mensajes. Lo normal es que una entidad instale sus tarjetas de información en un almacén de tarjetas accesible desde su selector de identidades. La política de seguridad de la parte confiante se especifica mediante WS-política de seguridad [b-WS-SECURITY] y puede recuperarse de diversos modos, entre ellos por inserción en páginas web. Lo normal es que la política de seguridad especifique mecanismos definidos en WS-Seguridad para la autentificación y protección de mensajes. El selector de identidades evalúa la política de la parte confiante y el conjunto de tarjetas de información instaladas en el almacén de tarjetas de usuario y permite que la entidad seleccione de entre el conjunto de tarjetas de información que concuerdan (es decir que sean capaces de obtener un testigo de seguridad conforme con la política). El selector de identidades solicita a continuación a la entidad la información de autentificación y, de ser necesario, envía una RST al STS especificado en la tarjeta de información seleccionada. El testigo de seguridad del RSTR resultante puede, a continuación, adjuntarse a un mensaje y enviarse a la parte confiante. En el caso en el que la parte confiante sea un sitio web, puede publicarse el testigo de seguridad como respuesta al formulario que contenía la política [b-IS-GUIDE].

I.3 Capacidades del DIIF

En el presente apartado se definen una vez más las capacidades del DIIF y se describe cómo puede utilizarse WS-Confianza y/o la tecnología de tarjeta de información para satisfacerlas.

I.3.1 Capacidades generales

I.3.1.1 Capacidades del usuario

El DIIF debe conseguir los siguientes objetivos:

1) *Facilitación de un selector de identidad que permita al usuario elegir la credencial utilizada para la autentificación*

El selector de identidades descrito en la tarjeta de información proporciona una experiencia de entidad segura, intuitiva y coherente, y permite que la entidad seleccione tarjetas de información en representación de una diversidad de identidades proporcionada por distintos IdSP con una diversidad de mecanismos de autentificación.

2) *Facilitación de una interfaz intuitiva y sólida para gestionar la información de las credenciales del usuario con la máxima seguridad*

El selector de identidades descrito en la tarjeta de información proporciona una experiencia de entidad segura, intuitiva y coherente.

3) *Soporte de inscripción o suscripción automática a un sitio web para minimizar la interacción del usuario con el sitio, manteniendo el usuario el pleno control para activar y desactivar tales mecanismos. Este requisito es facultativo.*

Los valores de declaración, incluidos en el testigo de seguridad, utilizados conjuntamente con el selector de identidades descrito en la tarjeta de información pueden proporcionar la información que, normalmente, introduciría la entidad para registrarse.

4) *Facilitación de la información de identidad siempre que el usuario lo desee, y permitirle que conserve el pleno control del intercambio de identidades mediante un mecanismo de protección de la privacidad adecuado*

La hipótesis que se maneja con la tecnología de tarjeta de información es que un IdSP sólo proporciona la información de identidad en respuesta a una petición de la entidad. La política de

privacidad de la parte confiante y del IdSP se encuentra disponible en la interfaz de usuario del selector de identidades seguro durante la selección de la tarjeta de información.

5) *Facilitación de actualizaciones automáticas de la información de identidad compartida cuando se modifica la información original bajo pleno control del usuario*

Los valores de declaración incluidos en el testigo de seguridad utilizados conjuntamente con el selector de identidades descrito en la tarjeta de información pueden proporcionar la información que, normalmente, introduciría la entidad en el registro. Dado que los mismos valores de declaración del testigo de seguridad pueden ser solicitados por la parte confiante en cada visita, la modificación de estos valores se propaga con facilidad.

6) *Facilitación al usuario de control total sobre el establecimiento de políticas de seguridad y privacidad y sobre su aplicación a fin de controlar el intercambio de identidades antes de compartir la información de identidad de manera que el usuario tenga influencia directa en el establecimiento y aplicación de la política*

La política de seguridad de la parte confiante y del IdSP se encuentra disponible en la interfaz de usuario del selector de identidades seguro descrito en la tarjeta de información durante la selección de tarjeta de información.

I.3.1.2 Capacidades funcionales

1) *Soporte de gestión de credenciales integrada que pueda gestionar la información de credenciales de usuario para la autentificación*

La tecnología de tarjeta de información comprende un selector de identidades y una interfaz de usuario de gestión de la tarjeta.

2) *Soporte de gestión de enlaces de intercambio de identidad para que el usuario conozca detalladamente las entidades con que se conecta para el intercambio de identidad*

Cuando un IdSP devuelve un testigo de seguridad que representa una sesión, el IdSP puede suministrar una interfaz para que la entidad pueda ver el conjunto de sesiones establecidas.

3) *Soporte de múltiples mecanismos de autentificación que puedan incluir autentificaciones basadas en la contraseña, basadas en la PKI y basadas en los datos biométricos*

WS-Confianza y WS-Seguridad proporcionan un protocolo coherente e intuitivo que soporta diversos mecanismos de autentificación. Las implementaciones de la tecnología de tarjeta de información proporcionan API intuitivas para iniciar el proceso de autentificación.

4) *Soporte de mecanismos de intercambio de identidades que puedan establecer un enlace bidireccional para compartir la información de identidad del usuario entre entidades que empleen DIC*

Con la tecnología de tarjeta de información el selector de identidades y el almacén de tarjetas ejecutan la funcionalidad asociada a un DIC.

5) *Soporte de un mecanismo de contrato digital que establezca un contrato para el intercambio de identidades que se empleará para aplicar las políticas de seguridad y privacidad sobre divulgación de IIP*

La política de seguridad de la parte confiante y de IdSP están disponibles en la interfaz de usuario del selector de identidades seguro descrito en la tarjeta de información durante la selección de tarjeta de información.

6) *Soporte de la sincronización de información de identidad para actualizar la información de identidad distribuida y compartida de manera coherente cuando se modifica la fuente de información de identidad divulgada. La información de identidad que ha de sincronizarse se limita a la IIP que modifica directamente el usuario.*

Los valores de declaración incluidos en el testigo de seguridad utilizados junto con el selector de identidades descrito en la tarjeta de información pueden proporcionar información que normalmente introduciría la entidad para registrarse. Como estos mismos valores de declaración del testigo de seguridad pueden ser solicitados por la parte confiante en cada visita, la modificación de estos valores se propaga con facilidad.

7) *Soporte de transformación de testigo universal para que el marco sea compatible con los sistemas de gestión de identidad existentes*

WS-Confianza proporciona un mecanismo de intercambio de testigos. El mensaje RST puede incluir uno o más testigos de seguridad así como una indicación de la identidad de la parte confiante. El RSTR puede incluir un testigo de seguridad adecuado para la parte confiante.

I.3.2 Capacidades adicionales

El DIIF debe proporcionar mecanismos de ampliación para que el selector de identidades y protocolos asociados den soporte a la entrada y transmisión de una diversidad de mecanismos de autentificación e información relacionada con la garantía de la misma.

Esto comprende (entre otras cosas) el soporte de lectores de tarjetas inteligentes y de dispositivos de entrada de datos biométricos, así como los formatos de datos asociados a éstos tales como los descritos en [b-NIST].

Bibliografía

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-UIT-T Y.2091] Recomendación UIT-T Y.2091 (2008), *Términos y definiciones aplicables a las redes de la próxima generación*.

[b-UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad para las redes de la próxima generación, versión 1*.

[b-UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), *Marco general para la gestión de identidades en la red de la próxima generación*.

[b-CARDSPACE] Microsoft (2006), *Introducing Windows CardSpace.*

[b-ETSI 133 980] ETSI TR 133 980 V8.0.0 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Liberty Alliance and 3GPP security interworking.*

[b-IS-INTEROP] Microsoft (2007), *Identity Selector Interoperability Profile V1.0.*

[b-IS-GUIDE] Microsoft (2007), *A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers.*

[b-LA-FF] *Liberty Alliance, Liberty ID-FF Protocols and Schema Specification (ver 1.2).*

[b-NIST] National Institute of Standards and Technology (2006), *FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employess and Contractors.*

[b-WS-SECURITY] OASIS (2007), *WS-SecurityPolicy 1.2.*

[b-WS-TRUST] OASIS (2007), *WS-Trust 1.3.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2011