Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1154

(04/2013)

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

Aplicaciones y servicios con seguridad – Protocolos de seguridad

Marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad

Recomendación UIT-T X.1154

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	
Aspectos generales de la ciberseguridad	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 heurística 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.1154

Marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad

Resumen

Últimamente, muchos servicios de aplicación, en particular los servicios financieros, requieren métodos de autentificación más fiables o combinados, tales como la autentificación multifactorial debido al aumento de los robos de identidad (ID). Se utilizan, por ejemplo, métodos de autentificación de contraseña única y otros nuevos en lugar de la autentificación tradicional basada en contraseñas.

Las combinaciones de métodos de autentificación proporcionan a múltiples proveedores de servicio de identidad (IdSP) la capacidad de mejorar las garantías de autentificación. La Recomendación UIT-T X.1154 presenta un marco general sobre autentificación combinada en entornos con múltiples IdSP para un proveedor de servicio. En esta Recomendación, se consideran tres tipos de métodos de autentificación combinada: autentificación multifactorial, autentificación multimétodo y autentificaciones múltiples.

El marco de referencia de esta Recomendación describe los modelos, las operaciones básicas y los requisitos de seguridad para cada componente del modelo y para cada mensaje entre los componentes del modelo con el fin de mantener un nivel general de garantía de autentificación en situaciones en las que se combinan múltiples IdSP.

Además, el marco también describe modelos, operaciones básicas y requisitos de seguridad para soportar el servicio de autentificación que gestiona una combinación de múltiples IdSP.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1154	2013-04-26	17

Palabras clave

Autentificación combinada, autentificación de entidad, autentificación multifactorial.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de 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

Introducción

Últimamente, muchos servicios de aplicación, en particular los servicios financieros, requieren métodos de autentificación más fiables o combinados, tales como la autentificación multifactorial debido al aumento de los robos de identidad (ID). Se utilizan, por ejemplo, métodos de autentificación de contraseña única y otros nuevos en lugar de la autentificación tradicional basada en contraseñas.

Las Recomendaciones UIT-T relativas a la autentificación para el servicio de aplicación segura (véanse [b-UIT-T X.509] y [UIT-T X.1141]) están normalizados como marcos de autentificación. Estas Recomendaciones UIT-T consideran fundamentalmente que un proveedor de servicio y/o usuario pertenecen a un dominio de seguridad proporcionado por un IdSP, incluso cuando el proveedor de servicio y el usuario pertenecen a diferentes dominios de seguridad. Para lograr una mejora en la autentificación, los IdSP precisan la introducción de métodos de autentificación más robustos (por ejemplo, los métodos de [b-UIT-T X.1151], [b-UIT-T X.1084], [b-UIT-T X.1086] y [b-UIT-T X.1089]).

Por otra parte, ocurre a menudo que un usuario obtiene varias identidades de distintos IdSP y que un proveedor de servicio establece relaciones de confianza con diversos IdSP. En estos entornos de múltiples IdSP, puede hallarse una forma alternativa para mejorar la autentificación cuando el proveedor de servicio utiliza múltiples IdSP para autenticar al usuario.

Es más, incluso cuando el proveedor de servicio implementa una autentificación más estricta, se puede utilizar el proveedor intermediario del servicio de identidad para combinar múltiples IdSP.

Sin embargo, puesto que cada IdSP actúa con diferentes proveedores, una simple combinación de múltiples IdSP puede llevar al colapso de todo el nivel de autentificación.

Por lo tanto, se requiere un marco general para describir modelos, operaciones básicas y requisitos de seguridad para cada componente del modelo y cada mensaje entre los componentes del modelo con el fin de mantener el nivel global de garantía de autentificación en situaciones en las que se combinan múltiples IdSP.

Además, el requisito de una autentificación fiable más robusta acrecienta la complejidad de la implementación y/o de la gestión del sistema de autentificación. El resultado es que el servicio de autentificación, que gestiona una combinación de múltiples IdSP, se utiliza para autenticar al usuario en representación del servicio de aplicación. Este servicio de autentificación es necesario para gestionar una combinación de multiples IdSP que satisfaga las políticas de autentificación de cada servicio de aplicación.

También se requiere el marco para describir modelos, aplicaciones básicas y requisitos de seguridad que soporten el servicio de autentificación.

Recomendación UIT-T X.1154

Marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad

1 Alcance

La presente Recomendación proporciona un marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad (IdSP) para que el proveedor de servicio consiga una autentificación combinada como la autentificación multifactorial.

El marco de referencia en esta Recomendación describe modelos, operaciones básicas y requisitos de seguridad para cada componente del modelo y cada mensaje entre los componentes del modelo con el fin de mantener un nivel general de garantía de autentificación cuando se combinan múltiples IdSP.

Además, el modelo también describe modelos, operaciones básicas y requisitos de seguridad para soportar el servicio de autentificación que gestiona una combinación de múltiples IdSP.

2 Referencias

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

[UIT-T X.1141] Recomendación UIT-T X.1141 (2006), *Lenguaje de marcaje de aserción de seguridad (SAML 2.0)*.

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

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza los términos siguientes definidos en otros documentos:

3.1.1 aseveración (*assertion*) [b-UIT-T X.1252]: Declaración hecha (por una entidad) sin presentar evidencias de su validez.

3.1.2 nivel de garantía (*assurance level*) [b-UIT-T X.1252]: Expresión cuantitativa que indica el nivel de confianza en la vinculación entre una entidad y la información de identidad presentada.

3.1.3 autentificación (*authentication*) [b-UIT-T X.1252]: Proceso encaminado a lograr una confianza suficiente en la vinculación entre la entidad y la identidad presentada.

3.1.4 garantía de autentificación (*authentication assurance*) [b-UIT-T X.1252]: Confianza a la que se llega en el proceso de autentificación de que el asociado de la comunicación es la entidad que declara ser o se espera que sea.

NOTA – La confianza se basa en el grado de confianza del vínculo entre la entidad que comunica y la entidad a la que se presenta.

3.1.5 usuario final (*end user*) [b-UIT-T X.1141]: Persona física que aplica los recursos.

3.1.6 identificador (*identifier*) [b-UIT-T X.1252]: Uno o más de los atributos utilizados para identificar a una entidad dentro de un contexto.

3.1.7 identidad (*identity*) [b-UIT-T X.1252]: Representación de una entidad bajo la forma de uno o más elementos información que permiten distinguir suficientemente a las entidades dentro del contexto. A los efectos de la IdM, se entiende que el término identidad es una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

NOTA – Cada entidad está representada por una identidad holística, que comprende todos los posibles elementos de información que caracterizan a dicha entidad (los atributos). Sin embargo, la identidad holística es una cuestión teórica y elude cualquier descripción y utilización práctica, dado que el número de todos los atributos posibles es indefinido.

3.1.8 proveedor intermediario de servicio de identidad (*identity service bridge provider*) [b-UIT-T X.1252]: Proveedor de servicio de identidad que actúa como intermediario fiable entre otros proveedores de identidad.

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

3.1.10 parte confiante (*relying party*) [UIT-T X.1141]: Entidad del sistema que decide ejecutar una acción basándose en información de otra entidad del sistema. Por ejemplo, una parte confiante del SAML depende de las aserciones que recibe de una parte asertante (una autoridad del SAML) acerca de un sujeto.

3.1.11 proveedor de servicio (*service provider*) [UIT-T X.1141]: Cometido que asume una entidad del sistema para proporcionar servicios a los principales u otras entidades del sistema.

3.2 Términos definidos en esta Recomendación

Esta Recomendación define los términos siguientes:

3.2.1 factor de autentificación (*authentication factor*): Tipo de credencial. Existen tres tipos de factores de autentificación: factor de propiedad, factor de conocimiento y factor biométrico.

3.2.2 factor biométrico (*biometric factor*): Factor de autentificación que verifica algo que es o hace el usuario.

3.2.3 autentificación combinada (*combined authentication*): Autentificación que utiliza múltiples credenciales.

3.2.4 nivel de garantía vigente (*current assurance level*): Nivel de garantía de autentificación de cierta entidad en un determinado momento.

3.2.5 factor de conocimiento (*knowledge factor*): Factor de autentificación que verifica algo que el usuario conoce.

3.2.6 autentificación multifactorial (*multifactor authentication*): Autentificación que utiliza múltiples credenciales de dos o más de las tres categorías de factores de autentificación.

3.2.7 autentificación multimétodo (*multi-method authentication*): Autentificación que utiliza múltiples credenciales de diferentes métodos de autentificación.

3.2.8 autentificación múltiple (*multiple authentication*): Autentificación que utiliza múltiples credenciales de los mismos métodos de autentificación.

3.2.9 factor de propiedad (*ownership factor*): Factor de autentificación que verifica algo que posee el usuario.

3.2.10 nivel de garantía proporcionado (*provided assurance level*): Nivel de garantía que proporcionarán ciertos proveedores de servicio de identidad (IdSP) cuando el IdSP autentifica al usuario.

3.2.11 nivel de garantía requerido (*required assurance level*): Nivel de garantía que requerirá cierto proveedor de servicio para prestar su propio servicio.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las siguientes abreviaturas y acrónimos:

ID Identidad (*identity*)

IdM Gestor de identidad (*identity management*)

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

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

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

SP Proveedor de servicio (*service provider*)

5 Convenios

En esta Recomendación:

Las palabras "se requiere para" indican un requisito que debe seguirse estrictamente y del que no se permite ninguna desviación si se tiene que reclamar la conformidad con esta Recomendación.

Las palabras "se recomienda" indican un requisito que está recomendado pero que no es absolutamente requerido. Por lo tanto, este requisito no es necesario para exigir la conformidad.

Las palabras "se prohíbe" indican un requisito que debe seguirse estrictamente y del que no se permite ninguna desviación si se reclama la conformidad con esta Recomendación.

Las palabras "puede opcionalmente" indican un requisito facultativo que se puede permitir, sin implicar en ningún caso que esté recomendado. Este término no pretende que la implementación del fabricante tenga que proporcionar la opción y la característica puede incluirse facultativamente por cualquier proveedor de red/servicio. En cambio, esto significa que el fabricante puede proporcionar la característica de forma opcional y seguir reclamando conformidad con la presente Recomendación.

6 Tipos de autentificación combinada

En la presente Recomendación se consideran los tres tipos de autentificación combinada siguientes:

– Autentificación multifactorial que utiliza múltiples credenciales de dos o más de las tres categorías de factores de autentificación. Por ejemplo, (1) autentificación mediante un certificado de clave pública almacenado en una tarjeta inteligente, (2) autentificación mediante una autentificación de una sola contraseña que utiliza un dispositivo físico y (3) autentificación mediante la combinación de una autentificación de contraseña única y una autentificación biométrica.

– Autentificación multimétodo que utiliza múltiples credenciales provenientes de diferentes métodos de autentificación. Por ejemplo, (1) autentificación mediante una combinación de autentificación de contraseña única y de autentificación de frase contraseña y (2) autentificación mediante una combinación de autentificación con huella dactilar y autentificación con patrón venoso.

– Autentificación múltiple que utiliza múltiples credenciales provenientes de los mismos métodos de autentificación. Por ejemplo, (1) autentificación de contraseña doble y (2) autentificación de huella dactilar que utiliza múltiples dedos.

La diferencia entre los tres métodos de autentificación citados es la combinación de credenciales. Además, el "factor de autentificación" proporciona una categorización de las credenciales. Es más, existen tres tipos de factores de autentificación: factor de propiedad, factor de conocimiento y factor biométrico.

– El factor de propiedad es un factor de autentificación que verifica algo que el usuario posee. Son ejemplos las tarjetas inteligentes, el testigo de seguridad, el testigo de soporte físico, los teléfonos de línea fija y los teléfonos móviles.
– El factor de conocimiento es un factor de autentificación que verifica algo que el usuario conoce. Por ejemplo, una contraseña, una frase contraseña y el número de identificación personal (PIN).
– El factor biométrico es un factor de autentificación que verifica algo que el usuario es o hace. Las huellas dactilares, el patrón venoso y el iris son buenos ejemplos.

7 Modelos de autentificación en entornos con múltiples IdSP

7.1 Modelos básicos en lo que respecta al proveedor de servicio

Al considerar el modelo de autentificación desde el punto de vista del proveedor de servicio, se deben tener en cuenta los factores siguientes para los modelos de autentificación cuando un usuario recibe un servicio de aplicación:

– El modelo de autentificación suministrado por el IdSP es una autentificación con un único factor o una autentificación combinada.
– El modelo incluye un único IdSP o varios IdSP. Si el modelo incluye varios IdSP, estos proporcionan el mismo método o diferentes métodos. Si varios IdSP proporcionan diferentes métodos, podrán ser factores diferentes o el mismo factor.

  Por lo tanto, para lograr una autentificación combinada, hay ocho tipos de modelos funcionales, en función del número de SP y de IdSP, y un tipo de autentificación combinada (Cuadro 1). Además, si hay múltiples usuarios en entornos con múltiples IdSP, un usuario puede no tener una relación de confianza con todos los IdSP. En otras palabras, se pueden agrupar los IdSP desde el punto de vista del conjunto de usuarios que tenga una relación de confianza con ellos (Figura 1). En este caso, también se considera el factor siguiente.
– Los IdSP se clasifican en un grupo o en muchos grupos desde el punto de vista de una relación de confianza con los usuarios.

Si los IdSP se clasifican en un grupo, se pueden aplicar los modelos T-3 a T-8 del Cuadro 1.

Si los IdSP se clasifican en más de dos grupos, se pueden considerar los modelos T-9 a T-14 (véase el Cuadro 2).

Cuadro 1 – Modelos de autentificación básicos (si los IdSP se categorizan en un grupo)

	Número de IdSP	Número de tipos de métodos de autentificación	Tipo de método de autentificación suministrado por un IdSP	Número de grupos de IdSP	Método de autentificación suministrado por una combinación de IdSP
T-1	Uno	Uno	Factor único	Uno	Ninguno
T-2			Combinado	Uno	Combinado (Nota 1)
T-3	Múltiple	Uno	Factor único	Uno	Múltiple
T-4			Combinado	Uno	Combinado (Nota 1)
T-5		Múltiple (diferentes métodos)	Factor único	Uno	Múltiple, multimétodo (Nota 2)
T-6			Combinado (múltiple o multimétodo)	Uno	Múltiple, multimétodo (Nota 3)
T-7		Múltiple (diferentes factores)	Factor único	Uno	Múltiple, multimétodo, multifactorial (Nota 2)
T-8			Combinado	Uno	Combinado (Nota 3)

NOTA 1 − Se pueden proporcionar los tres tipos de autentificación combinada. Sin embargo, el método de autentificación suministrado depende del tipo de autentificación facilitado por un IdSP.

NOTA 2 − Se pueden proporcionar los tres tipos de autentificación combinada. Sin embargo, el modelo de autentificación suministrado depende de la selección de los IdSP.

NOTA 3 − Se pueden proporcionar los tres tipos de autentificación combinada. Sin embargo, el método de autentificación suministrado depende no sólo de los tipos de autentificación suministrados por los IdSP sino también de la selección de los IdSP.

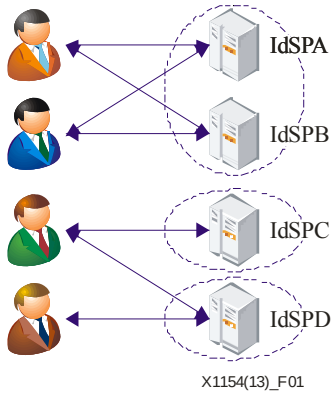

Figura 1 – Ejemplo de agrupamiento múltiple de IdSP desde el punto de vista de la relación de confianza con los usuarios

Cuadro 2 – Modelos de autentificación básicos (si los IdSP se categorizan en un grupo)

	Número de IdSP	Número de tipos de métodos de autentificación	Tipo de método de autentificación suministrado por un IdSP	Número de grupos de IdSP	Método de autentificación suministrado por una combinación de IdSP
T-9	Múltiple	Uno	Factor único	Múltiple	Múltiple
T-10			Combinado	Múltiple	Combinado (Nota 1)
T-11		Múltiple (diferentes métodos)	Factor único	Múltiple	Múltiple, multimétodo (Nota 2)
T-12			Combinado (múltiple o multimétodo)	Uno	Múltiple, multimétodo (Nota 3)
T-13		Múltiple (diferentes factores)	Factor único	Múltiple	Múltiple, multimétodo, multifactorial (Nota 2)
T-14			Combinado	Múltiple	Combinado (Nota 3)

NOTA 1 − Se pueden proporcionar los tres tipos de autentificación combinada. Sin embargo, el método de autentificación suministrado depende del tipo de autentificación facilitado por un IdSP.

NOTA 2 − Se pueden proporcionar los tres tipos de autentificación combinada. Sin embargo, el modelo de autentificación suministrado depende de la selección de los IdSP.

NOTA 3 − Se pueden proporcionar los tres tipos de autentificación combinada. Sin embargo, el método de autentificación suministrado depende no sólo de los tipos de autentificación suministrados por los IdSP sino también de la selección de los IdSP.

7.1.1 Modelo T-1

El modelo T-1 es el modelo que se utiliza cuando un IdSP proporciona una autentificación de factor único y cuando un IdSP, un proveedor de servicio y uno o más terminales están conectados entre sí a través de la red.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio solicita al IdSP que autentique al usuario. El IdSP que recibe la petición de autentificación desde el proveedor de servicio autentifica al usuario mediante un método de factor único. Si los resultados de la autentificación recibidos desde el IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo no puede proporcionar una autentificación combinada. Por lo tanto, este modelo se encuentra fuera del ámbito de la presente Recomendación.

7.1.2 Modelo T-2

El modelo T-2 es el modelo en el que un IdSP proporciona una autentificación combinada (autentificación múltiple, multimétodo o multifactorial) y en el que un IdSP, un proveedor de servicio o uno o más terminales están conectados entre sí a través de la red.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio solicita al IdSP que autentique al usuario. El IdSP, que recibe la petición de autentificación desde el proveedor de servicio, autentifica al usuario mediante un método de autentificación combinada. Si los resultados de la autentificación recibidos desde el IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de método de autentificación combinada aunque depende del tipo de método de autentificación facilitado por el IdSP.

7.1.3 Modelo T-3

El modelo T-3 es el modelo que se utiliza cuando múltiples IdSP proporcionan el mismo método de autentificación de factor único, y cuando múltiples IdSP, un proveedor de servicio o uno o más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-3 todos los usuarios tienen relaciones de confianza con todos los IdSP.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentifiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar un método de autentificación múltiple.

Cabe destacar que este modelo puede proporcionar una autentificación de factor único si el método de autentificación suministrado por un IdSP satisface la garantía de autentificación requerida. Sin embargo, la autentificación de factor único es un modelo que se encuentra fuera del ámbito de la presente Recomendación.

7.1.4 Modelo T-4

El modelo T-4 es el modelo que se utiliza cuando múltiples IdSP proporcionan el mismo método de autentificación combinada y cuando múltiples IdSP, un proveedor de servicio y uno o más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-4 todos los usuarios tienen relaciones de confianza con todos los IdSP.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona uno o múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de autentificación combinada aunque depende del tipo de autentificación combinada proporcionado por un IdSP y/o de la selección de los IdSP. (Se podrían realizar autentificaciones multifactoriales múltiples y autentificaciones multimétodo múltiples).

7.1.5 Modelo T-5

El modelo T-5 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación única, que son de diferentes tipos aunque utilizan el mismo factor, y cuando múltiples IdSP, un proveedor de servicio y uno o más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-5 todos los usuarios tienen relaciones de confianza con todos los IdSP.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentifiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede facilitar autentificación múltiple o autentificación multimétodo. Cabe destacar que el método de autentificación utilizado depende de la combinación de los IdSP.

Este modelo también puede proporcionar autentificación de factor único si el método de autentificación suministrado por un IdSP satisface la garantía de autentificación requerida. Sin embargo, la autentificación de factor único en este modelo se encuentra fuera del ámbito de la presente Recomendación.

7.1.6 Modelo T-6

El modelo T-6 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación combinada, que son de diferentes tipos pero utilizan el mismo factor (es decir, métodos de autentificación múltiple o multimétodo) y cuando múltiples IdSP, un proveedor de servicio y uno o más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-6, todos los usuarios tienen relaciones de confianza con todos los IdSP.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona uno o múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar autentificaciones múltiples o autentificaciones multimétodo aunque depende de la selección y combinación de los IdSP.

7.1.7 Modelo T-7

El modelo T-7 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación única, que utilizan diferentes factores, y cuando múltiples IdSP, un proveedor de servicio y uno o más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-7 todos los usuarios tienen relaciones de confianza con todos los IdSP.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona a los múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de autentificación combinada. Cabe destacar que el método de autentificación utilizado depende de la selección de los IdSP.

Este modelo también puede proporcionar una autentificación de factor único si el método de autentificación suministrado por un IdSP satisface la garantía de autentificación requerida. Sin embargo, la autentificación de factor único en este modelo se encuentra fuera del ámbito de la presente Recomendación.

7.1.8 Modelo T-8

El modelo T-8 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación combinada, que utilizan diferentes factores, y cuando múltiples IdSP, un proveedor de servicio y uno o más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-8 todos los usuarios tienen relaciones de confianza con todos los IdSP.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona uno o múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de método de autentificación combinada.

7.1.9 Modelo T-9

El modelo T-9 es el modelo que se utiliza cuando múltiples IdSP proporcionan el mismo método de autentificación de factor único y cuando múltiples IdSP, un proveedor de servicio y más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-9 uno o más usuarios no tienen relaciones de confianza con todos los IdSP.

NOTA – Este modelo puede existir con un IdSP que no tiene relaciones de confianza con ningún usuario en este modelo. No obstante, este modelo con este tipo de IdSP se encuentra fuera del ámbito de la presente Recomendación.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona a múltiples IdSP para satisfacer la garantía de autentificación requerida en un grupo de IdSP, que tenga relaciones de confianza con el usuario, y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar un método de autentificación múltiple.

Cabe destacar que este modelo también puede proporcionar una autentificación de factor único si el método de autentificación proporcionado por un IdSP satisface la garantía de autentificación requerida. Sin embargo, la autentificación de factor único en este modelo se encuentra fuera del ámbito de la presente Recomendación.

7.1.10 Modelo T-10

El modelo T-10 es el modelo que se utiliza cuando múltiples IdSP proporcionan el mismo método de autentificación combinada y cuando múltiples IdSP, un proveedor de servicio y más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-10 uno o más usuarios no tienen relaciones de confianza con todos los IdSP.

NOTA – El modelo T-10 existe cuando el IdSP no tiene una relación de confianza con todos los usuarios. No obstante, este modelo con este tipo de IdSP se encuentra fuera del ámbito de la presente Recomendación.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona uno o múltiples IdSP para satisfacer la garantía de autentificación requerida y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de autentificación combinada aunque depende del tipo de autentificación combinada facilitado por un IdSP y/o de la selección de los IdSP. Se podrían utilizar múltiples autentificaciones multifactoriales y múltiples autentificaciones multimétodo.

7.1.11 Modelo T-11

El modelo T-11 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación única, que son de diferentes tipos aunque utilizan el mismo factor, y cuando múltiples IdSP, un proveedor de servicio y más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-11 uno o más usuarios no tienen relaciones de confianza con todos los IdSP.

NOTA – El modelo T-11 existe cuando el IdSP no tiene una relación de confianza con todos los usuarios. No obstante, este modelo con este tipo de IdSP se encuentra fuera del ámbito de la presente Recomendación.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona a los múltiples IdSP para satisfacer la garantía de autentificación requerida en un grupo de IdSP, que tenga relaciones de confianza con el usuario, y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar autentificación múltiple o autentificación multimétodo. Cabe destacar que el método de autentificación utilizado depende de la combinación de IdSP.

Este modelo también puede proporcionar una autentificación de factor único si el método de autentificación proporcionado por un IdSP satisface la garantía de autentificación requerida. Sin embargo, la autentificación de factor único en este modelo se encuentra fuera del ámbito de la presente Recomendación.

7.1.12 Modelo T-12

El modelo T-12 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación combinada, que son de diferentes tipos aunque utilizan el mismo factor (es decir, métodos de autentificación múltiple o multimétodo) y cuando múltiples IdSP, un proveedor de servicio y más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-12 uno o más usuarios no tienen relaciones de confianza con todos los IdSP.

NOTA – El modelo T-12 existe cuando el IdSP no tiene relaciones de confianza con ningún usuario. No obstante, este modelo con este tipo de IdSP se encuentra fuera del ámbito de la presente Recomendación.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona uno o múltiples IdSP para satisfacer la garantía de autentificación requerida en un grupo de IdSP, que tenga relaciones de confianza con el usuario, y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar autentificación múltiple o autentificación multimétodo aunque depende de la selección y combinación de los IdSP.

7.1.13 Modelo T-13

El modelo T-13 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación única que utilizan diferentes factores y cuando múltiples IdSP, un proveedor de servicio y más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-13 uno o más usuarios no tienen relaciones de confianza con todos los IdSP.

NOTA – El modelo T-13 existe cuando el IdSP no tiene relaciones de confianza con ningún usuario. No obstante, este modelo con este tipo de IdSP se encuentra fuera del ámbito de la presente Recomendación.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona a los múltiples IdSP para satisfacer la garantía de autentificación requerida en un grupo de IdSP, que tenga una relación de confianza con el usuario, y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de autentificación múltiple. Cabe destacar que el método de autentificación utilizado depende de la selección de IdSP.

Este modelo también puede proporcionar una autentificación de factor único si el método de autentificación facilitado por un IdSP satisface la garantía de autentificación requerida. Sin embargo, la autentificación de factor único en este modelo se encuentra fuera del ámbito de la presente Recomendación.

7.1.14 Modelo T-14

El modelo T-14 es el modelo que se utiliza cuando múltiples IdSP proporcionan métodos de autentificación combinada que utilizan diferentes factores y cuando múltiples IdSP, un proveedor de servicio y más terminales están conectados entre sí a través de la red. En concreto, en el modelo T-14 uno o más usuarios no tienen relaciones de confianza con todos los IdSP.

NOTA – El modelo T-14 existe cuando el IdSP no tiene relaciones de confianza con ningún usuario. No obstante, este modelo con este tipo de IdSP se encuentra fuera del ámbito de la presente Recomendación.

Cuando el proveedor de servicio recibe una petición de servicio desde el terminal, el proveedor de servicio selecciona uno o múltiples IdSP para satisfacer la garantía de autentificación requerida en un grupo de IdSP, que tenga relación de confianza con el usuario, y solicita a los IdSP seleccionados que autentiquen al usuario respectivamente. Si todos los resultados de autentificación recibidos desde los IdSP indican que el usuario se ha autentificado con éxito, el proveedor de servicio presta su servicio al terminal.

Este modelo puede proporcionar cualquier tipo de método de autentificación combinada.

7.2 Modelo de ciclo de vida de autentificación de entidad

El modelo de ciclo de vida de autentificación de entidad es el modelo de transición de estados en la fase de autentificación de entidad definida en [UIT-T X.1254].

Existen dos tipos de modelo: el modelo de ciclo de vida desde el punto de vista del usuario y el modelo de ciclo de vida desde el punto de vista del SP.

7.2.1 Modelo de ciclo de vida desde el punto de vista del usuario

Durante el proceso de autentificación del modelo de ciclo de vida desde el punto de vista del usuario, el estado de autentificación pasa por cuatro instancias: "sin autentificación", "identificado", "verificado" y "finalizado" (Figura 2).

El estado inicial de autentificación es "sin autentificación".

Cuando el usuario envía una petición de autentificación y es identificado por el IdSP, el estado cambia de "sin autentificación" a "identificado".

Una vez que el usuario ha sido autentificado por el IdSP, el estado cambia de "identificado" a "verificado".

Además, si el usuario envía una petición de finalización o si ha transcurrido cierto tiempo después de que se autentificara al usuario con el estado en "verificado", el estado cambia de "verificado" a "finalizado".

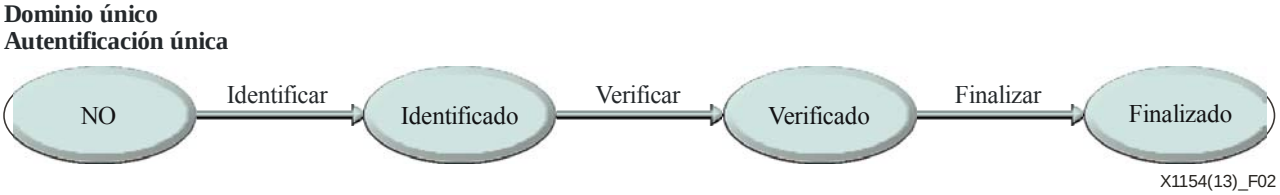

Figura 2 – Transición de estados de la autentificación de factor único

En el caso de autentificación combinada, la transición de estados de "identificado" a "verificado" es diferente (Figura 3).

Durante el proceso de autentificación combinada, el IdSP o el proveedor de servicio gestiona la garantía de autentificación vigente del usuario.

Cuando el usuario es autentificado con éxito mediante una autentificación de factor único, se actualiza la garantía de autentificación vigente y se comprueba si satisface la garantía de autentificación requerida.

Si la garantía de autentificación vigente satisface la garantía de autentificación requerida, el estado cambia de "identificado" a "verificado".

Además, si el usuario envía una petición de finalización o si ha transcurrido cierto tiempo después de que se autentificara al usuario con el estado en "verificado", el estado cambia de "verificado" a "finalizado".

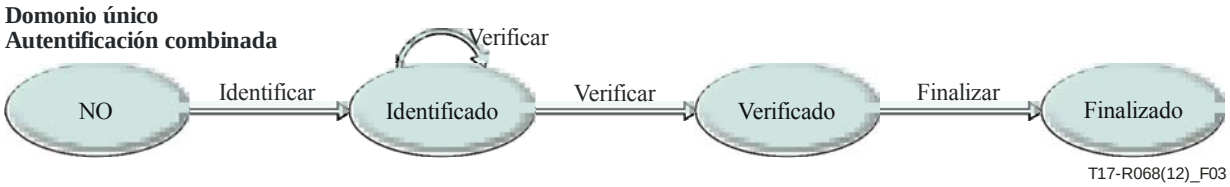

Figura 3 – Transición de estados de la autentificación combinada en un dominio único

La transición de estados se muestra en la Figura 4 en el caso de autentificación combinada en múltiples dominios que tienen requisitos de garantía de autentificación diferentes en los modelos T-4, T-6 y T-8.

Aunque la transición de estados en el primer dominio es la misma que la de la Figura 3, la transición de estados en otros dominios es diferente.

Cuando el estado en el primer dominio es "verificado para el primer dominio" y el usuario envía una petición de autentificación al segundo dominio, el estado en el segundo dominio cambia a "insuficiente para el segundo dominio" si el usuario es identificado en el segundo dominio. Si la garantía de autentificación vigente del usuario satisface la garantía de autentificación requerida en el segundo dominio, el estado cambia de "insuficiente para el segundo dominio" a "verificado para el segundo dominio".

En otro caso, el usuario es autentificado por el IdSP (o el proveedor de servicio) y se actualiza y evalúa la garantía de autentificación vigente, si satisface la garantía de autentificación requerida. Es más, si el usuario envía una petición de finalización a cualquier dominio, el estado en todos los dominios cambia de "verificado" a "finalizado".

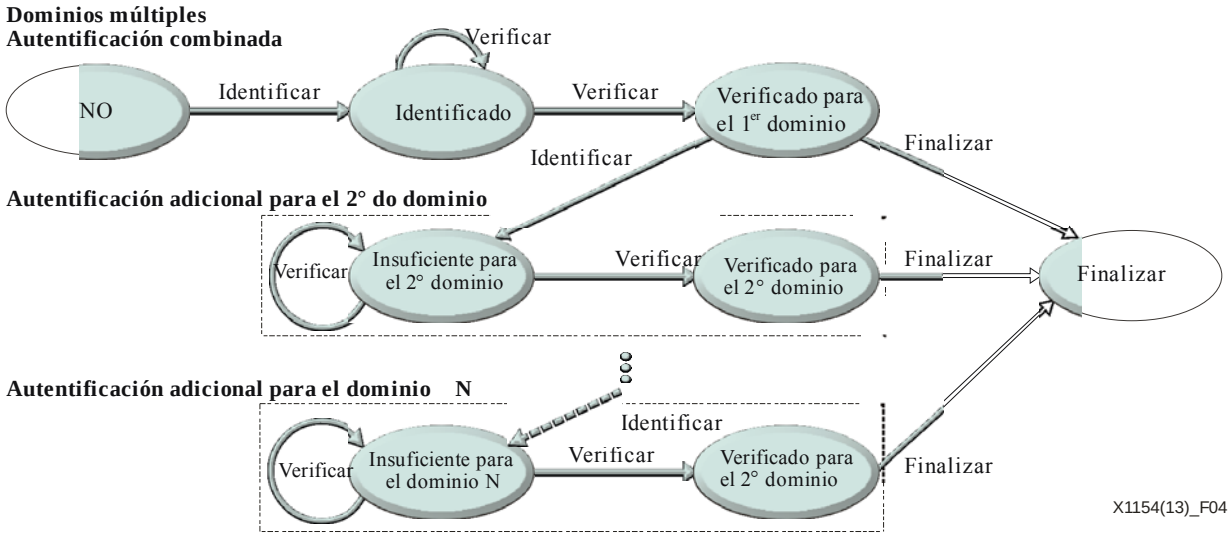

Figura 4 – Transición de estados de la autentificación combinada en múltiples dominios con diferentes requisitos de garantía

En la Figura 5 se muestra la transición de estados en el caso de autentificación combinada en dominios múltiples con federación. Es el mismo caso de autentificación combinada en dominios múltiples con diferentes requisitos de garantía de autentificación en los modelos T-4, T-6 y T-8.

La transición de estados en el primer dominio es la misma que en las Figuras 3 y 4.

Cuando el estado en el primer dominio es "verificado" y el usuario envía una petición de autentificación al segundo dominio, el estado no cambia aunque que se identifique al usuario en el segundo dominio.

Además, si el usuario envía una petición de finalización a cualquier dominio, el estado en todos los dominios cambia de "verificado" a "finalizado".

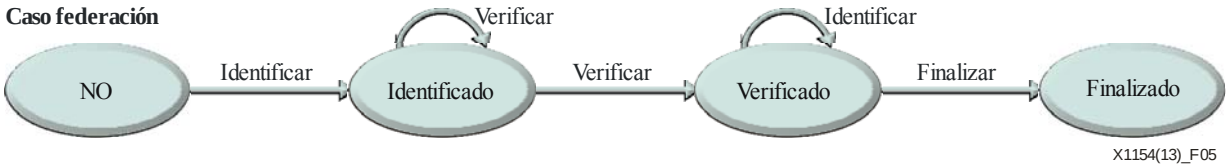

Figura 5 – Transición de estados de la autentificación combinada en dominios múltiples con federación

7.2.2 Modelo de ciclo de vida desde el punto de vista del proveedor de servicio

Durante el proceso de autentificación del modelo de ciclo de vida desde el punto de vista del SP, el estado de autentificación pasa también por cuatro instancias: "sin autentificación", "identificado", "verificado" y "finalizado" (Figura 6).

El estado inicial de autentificación es "sin autentificación".

Cuando el SP recibe una petición de autentificación e identifica quién es el usuario, el estado cambia de "sin autentificación" a "identificado". Posteriormente, el estado cambia de "identificado" a "verificado" cuando el usuario es autentificado por el IdSP,

Además, si el SP recibe una petición de finalización del usuario o si ha transcurrido cierto tiempo después de que se autentificara al usuario con el estado en "verificado", el estado cambia de "verificado" a "finalizado".

Figura 6 – Transición de estados de la autentificación de factor único

En el caso de autentificación combinada, la transición de estados de "identificado" a "verificado" es diferente.

Durante el proceso de autentificación combinada, el IdSP o el proveedor de servicio gestiona la garantía de autentificación vigente del usuario.

Cuando el usuario es autentificado con éxito por el IdSP, se actualiza la garantía de autentificación vigente y se comprueba si satisface la garantía de autentificación requerida.

Si la garantía de autentificación vigente satisface la garantía de autentificación requerida, el estado cambia de "identificado" a "verificado".

Además, si el usuario envía una petición de finalización o si ha transcurrido cierto tiempo después de que se autentificara al usuario con el estado en "verificado", el estado cambia de "verificado" a "finalizado".

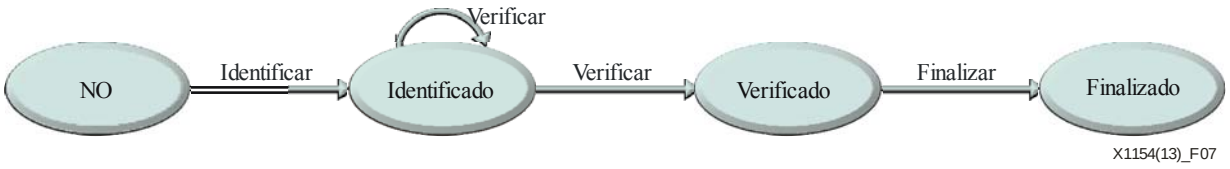

Figura 7 – Transición de estados de la autentificación combinada

Desde el punto de vista del SP, no existe ninguna diferencia con el caso de autentificación combinada aunque el usuario acceda a múltiples dominios y a dominios federados.

8 Operaciones en entornos de múltiples IdSP

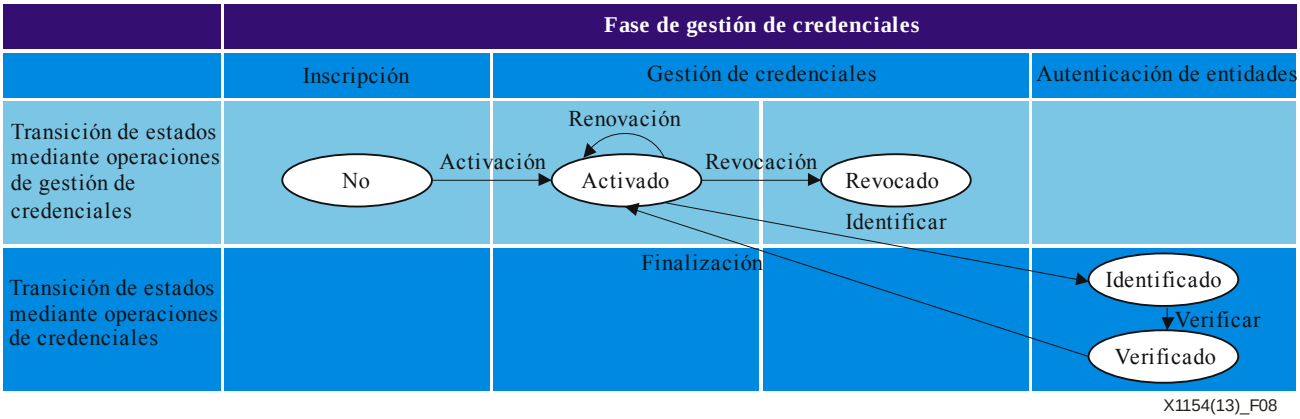

Figura 8 – Operaciones para el usuario

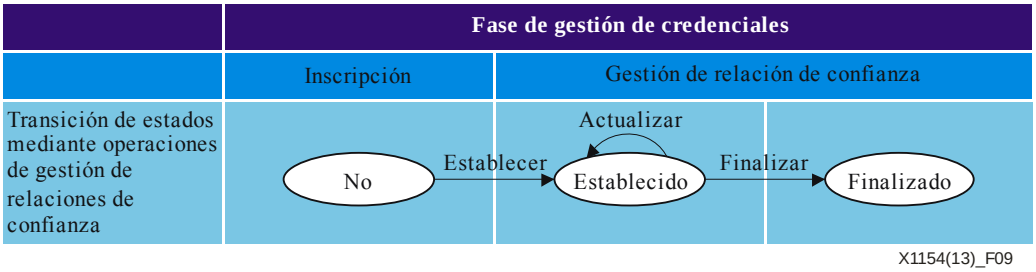

Figura 9 – Operaciones del proveedor de servicio

En los modelos que se muestran en la cláusula 7 se describen los diferentes tipos de operaciones IdSP siguientes:

1) operaciones de gestión de credenciales (Figura 8);
2) operaciones de uso de credenciales (Figura 8);
3) operaciones de gestión de relaciones de confianza con proveedores de servicio (Figura 9).

8.1 Operaciones de gestión de credenciales

Las operaciones de gestión de credenciales son operaciones para que el usuario gestione el ciclo de vida de sus credenciales de la forma siguiente:

1) Activar

   La operación activar realiza el proceso de activación de la credencial, que se define en [UIT-T X.1254], para especificar la credencial del usuario.

2) Renovar

   La operación renovar realiza el proceso de renovación de credenciales, que se define en [UIT-T X.1254], para especificar la credencial del usuario.

3) Revocar

   La operación revocar realiza el proceso de revocación de credenciales, que se define en [UIT-T X.1254], para especificar la credencial del usuario.

8.2 Operaciones de uso de credenciales

Cuando se activa la credencial, se pueden realizar las operaciones de uso. Las operaciones de uso de credenciales son operaciones para la identificación/verificación del usuario y para la expiración de la aseveración que emitió inicialmente la operación para verificar al usuario.

1) Identificar

   La operación identificar identifica al usuario.

   Esta operación se utiliza en la fase de autentificación de la entidad.

2) Verificar

   La operación verificar comprueba si los pares de comunicación son los reclamados por el usuario a partir de las credenciales presentadas. Una vez verificado el par se emite una aseveración al par de comunicación.

   Esta operación se utiliza en la fase de autentificación de la entidad.

3) Finalizar

   La aseveración concluye tras la operación de finalización.

   Esta operación se utiliza en la fase de uso.

8.3 Operaciones de gestión de relaciones de confianza con proveedores de servicio.

Las operaciones de gestión de relaciones de confianza con proveedores de servicio son operaciones para que los proveedores de servicio generen y eliminen la relación de confianza con proveedores de servicio.

1) Establecer

   La operación establecer crea una nueva relación de confianza con un determinado proveedor de servicio.

   Esta operación se utiliza en la fase de inscripción de relaciones de confianza.

2) Actualizar

   La operación actualizar renueva la relación de confianza existente con un determinado proveedor de servicio.

   Esta operación se utiliza en la fase de gestión de relaciones de confianza.

3) Terminar

   La operación terminar elimina la relación de confianza especificada con un determinado proveedor de servicio.

   Esta operación se utiliza en la fase de gestión de relaciones de confianza.

9 Marco general de autentificación combinada en entornos de múltiples proveedores de servicio de identidad

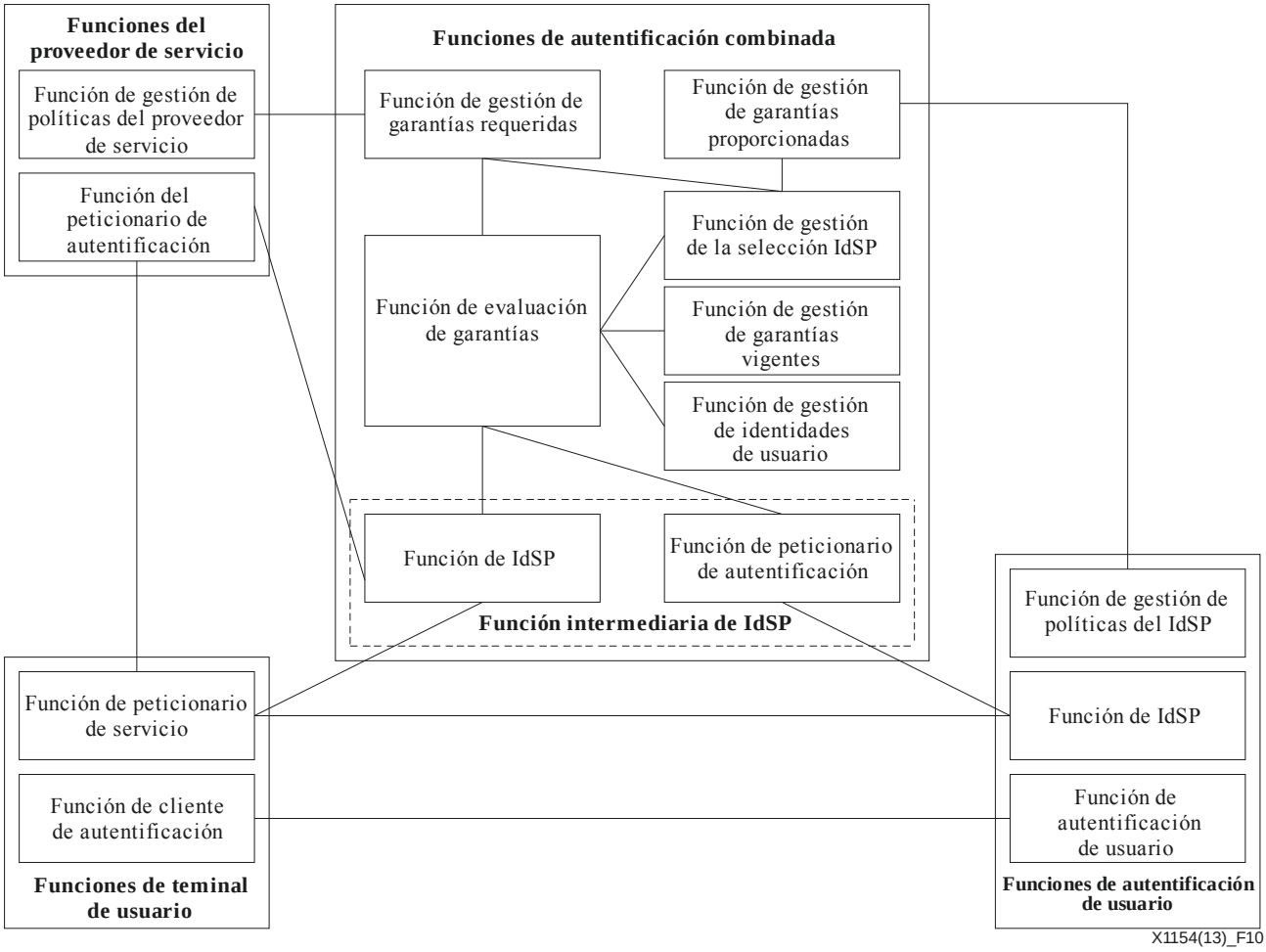

Figura 10 – Modelo del marco general de la autentificación combinada en entornos de múltiples proveedores de servicio de identidad

En la Figura 10 el marco de autentificación combinada incluye cuatro bloques de funciones lógicas: las funciones de autentificación de usuario, las funciones de proveedor de servicio, las funciones de terminal de usuario y las funciones de autentificación combinada.

9.1 Componentes lógicos

9.1.1 Funciones de autentificación de usuario

Las funciones de autentificación de usuario son tres: la función de autentificación de usuario, la función de IdSP y la función de gestión de políticas IdSP.

La función de autentificación de usuario es una función que se utiliza para realizar la operación de verificación y para autentificar a un usuario.

La función de IdSP es una función que se utiliza para recibir una petición de autentificación desde (o recibir una función de peticionario de autentificación de) las funciones de autentificación combinada y para realizar la operación de identificación. Además, la función de IdSP sirve para recibir una solicitud de finalización y realizar una operación de finalización.

La función de gestión de políticas de IdSP es una función que se utiliza para gestionar una política de autentificación de IdSP que incluye un tipo de método de autentificación y un nivel de garantía de autentificación facilitados por la función de autentificación de usuario.

9.1.2 Funciones de proveedor de servicio

Las funciones de proveedor de servicio son dos: función de peticionario de autentificación y función de gestión de políticas de proveedor de servicio.

La función de peticionario de autentificación es una función que se utiliza para enviar una petición de autentificación a (una función de IdSP de) las funciones de autentificación combinada.

La función de gestión de políticas de proveedor de servicio es una función que se utiliza para gestionar la política de autentificación del proveedor de servicio y que incluye un nivel de garantía de autentificación requerido para prestar un servicio.

9.1.3 Funciones de terminal de usuario

Las funciones de terminal de usuario son dos: la función de peticionario de servicio y la función de cliente de autentificación.

La función de peticionario del servicio es una función que se utiliza para enviar una petición de servicio a (una función de peticionario de autentificación de) las funciones de proveedor de servicio.

La función de cliente de autentificación es una función que se utiliza para comunicar con (una función de autentificación de usuario de) una función de autentificación de factor único para autentificar al usuario.

9.1.4 Funciones de autentificación combinada

Las funciones de autentificación combinada son ocho: la función de IdSP, la función de peticionario de autentificación, la función de gestión de garantía requerida, la función de garantía proporcionada, la función de gestión de garantía vigente, la función de gestión de identidad de usuario, la función de evaluación de garantía y la función de selección de IdSP.

La función de IdSP es una función que se utiliza para recibir una petición de autentificación desde (una función de peticionario de autentificación de) las funciones de proveedor de servicio y realizar la operación de identificación. Es más, la función de IdSP recibe una petición de terminación de servicio y realiza la operación de finalización.

La función de peticionario de autentificación es una función que se utiliza para enviar una petición de autentificación o una petición de finalización a (la función IdSP de) las funciones de autentificación de factor único.

La función de gestión de garantía requerida es una función que se utiliza para gestionar un nivel de garantía de autentificación requerido por cada función de proveedor de servicio mediante las operaciones establecer/actualizar/terminar.

La función de gestión de garantía proporcionada es una función que se utiliza para gestionar un tipo de método de autentificación y un nivel de garantía de autentificación proporcionado por cada función de autentificación de factor único mediante las operaciones establecer/actualizar/terminar.

La función de gestión de garantía vigente es una función que se utiliza para gestionar el nivel de garantía de autentificación vigente de cada usuario.

La función de gestión de identidad de usuario es una función que se utiliza para gestionar la información de identidad de cada usuario mediante la función crear/actualizar/revocar.

La función de evaluación de garantía es una función que se utiliza para verificar el resultado de la autentificación de usuario suministrada por una función IdSP de las funciones de autentificación de factor único, para evaluar el nivel de garantía vigente del usuario y comprobar si el nivel de garantía del usuario satisface el nivel de garantía requerido del proveedor de servicio.

La función de selección de IdSP es una función que se utiliza para seleccionar una o muchas funciones de autentificación de factor único para que el usuario satisfaga el nivel de garantía requerido del proveedor de servicio.

Cabe destacar que algunos marcos de gestión de identidad (IdM) existentes pueden utilizar otra función, la función de identificación de proveedor intermediario del servicio de identidad, en lugar de la función IdSP y de la función de peticionario de autentificación.

9.2 Comportamientos

9.2.1 Petición de servicio

La Figura 11 muestra un comportamiento básico de una petición de servicio en el marco general de autentificación múltiple en entornos con múltiples proveedores de servicio de identidad.

(1) Una función de petición de servicio envía una petición de servicio a la función de peticionario de autentificación en las funciones de proveedor de servicio.

(2) Cuando la función de peticionario de autentificación en las funciones de proveedor de servicio recibe la petición de servicio, envía una petición de autentificación a la función de IdSP en las funciones de autentificación combinada, si la función de peticionario de autentificación considera que se requiere que la función terminal de usuario se autentique para proporcionar el servicio de aplicación.

(3) Cuando la función de IdSP recibe la petición de servicio, envía una petición de autentificación a la función de evaluación de garantías.

(4) La función de evaluación de garantías extrae el nivel de garantía vigente del terminal de usuario mediante la función de gestión de garantías vigentes y envía una petición de selección de IdSP con la garantía vigente del terminal de usuario a una función de selección de IdSP.

(5) La función de selección de IdSP obtiene un nivel de garantía requerido del proveedor de servicio y proporciona el nivel de garantía de cada IdSP desde las funciones de gestión de garantías requeridas y de gestión de garantías proporcionadas, respectivamente. Posteriormente, el IdSP selecciona un IdSP de una lista de IdSP disponibles y envía el nombre a la función de evaluación de garantías.

(6) Si es preciso, la función de evaluación de garantías obtiene un identificador de terminal de usuario en el IdSP seleccionado mediante una función de gestión de identidades de usuario y envía una petición de autentificación a la función de peticionario de autentificación. Además, la función de peticionario de autentificación envía una solicitud de autentificación a la función de IdSP en las funciones de IdSP seleccionadas.

(7) La función de IdSP envía la solicitud de autentificación a la función de autentificación. Además, la función de autentificación realiza la autentificación del usuario con el cliente de autentificación en las funciones terminales de usuario.

(8) La función de autentificación entrega el resultado de la autentificación a la función de evaluación de garantías a través de la función IdSP en las funciones de IdSP y mediante la función peticionario de autentificación en las funciones de autentificación combinada.

(9) La función de evaluación de garantías analiza y actualiza la garantía vigente del terminal de usuario.

(10) Si el nivel de garantía vigente del terminal de usuario no es suficiente para prestar el servicio (es decir, es inferior a la garantía requerida), la función de evaluación de garantías solicita de nuevo una petición de selección de IdSP a la función de selección de IdSP. Posteriormente, se repiten los pasos (5) a (9).

(11) Si la garantía vigente del terminal de usuario es suficiente para prestar el servicio en (10), la función de evaluación de garantías envía un resultado de autentificación a la función de IdSP.

(12) La función de IdSP crea una aseveración y la envía al peticionario de autentificación en las funciones de proveedor de servicio.

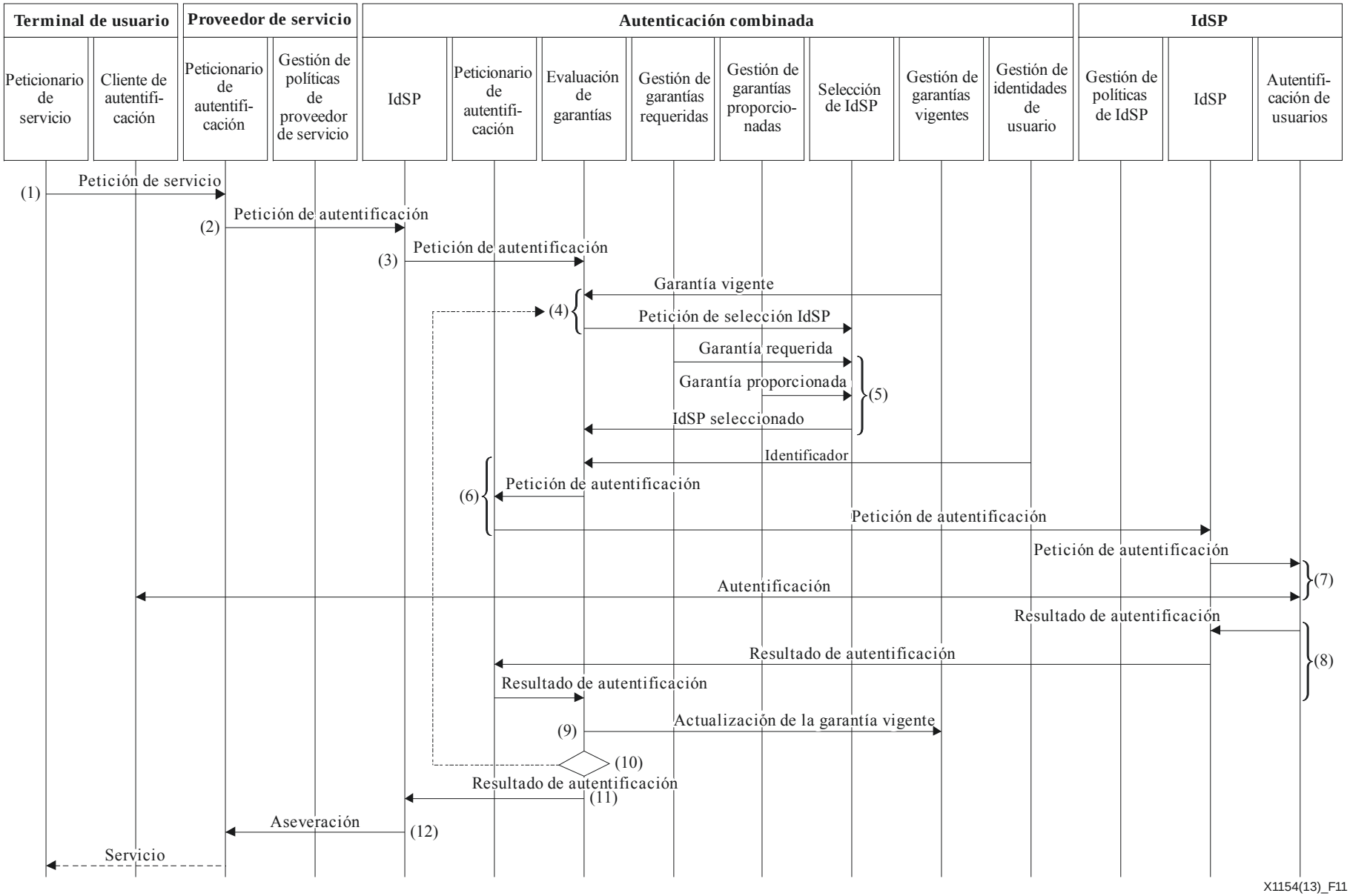

Figura 11 – Comportamiento general de la petición de servicio en el marco general de autentificación combinada en múltiples entornos de proveedor de servicio de identidad

9.2.2 Terminación del servicio

La Figura 12 muestra un comportamiento general de la terminación del servicio en el marco general de autentificación combinada en entornos con múltiples proveedores de servicio de identidad.

(1) Una función de peticionario de servicio envía una petición de terminación del servicio a la función de peticionario de autentificación en las funciones de proveedor de servicio.

(2) Cuando la función de peticionario de autentificación en las funciones de proveedor de servicio recibe la petición de terminación del servicio, envía una solicitud de finalización a la función IdSP en las funciones de autentificación combinada.

(3) Cuando la función IdSP recibe la petición de finalización, envía una petición de terminación a la función de evaluación de garantías.

(4) La función de evaluación de garantías recupera una lista de IdSP que el terminal de usuario registra y envía una petición de finalización a todas las funciones IdSP enumeradas mediante la función de peticionario de autentificación.

(5) La función de IdSP devuelve un resultado de finalización.

(6) Cuando la función de evaluación de garantías recibe el resultado de finalización, se actualiza la garantía vigente.

(7) Si la función de evaluación de garantías recibe todos los resultados de finalización, devuelve el resultado de terminación a la función de IdSP.

(8) La función de IdSP devuelve el resultado de finalización a la función de peticionario de autentificación.

(9) La función de peticionario de autentificación devuelve el resultado de terminación del servicio al peticionario del servicio.

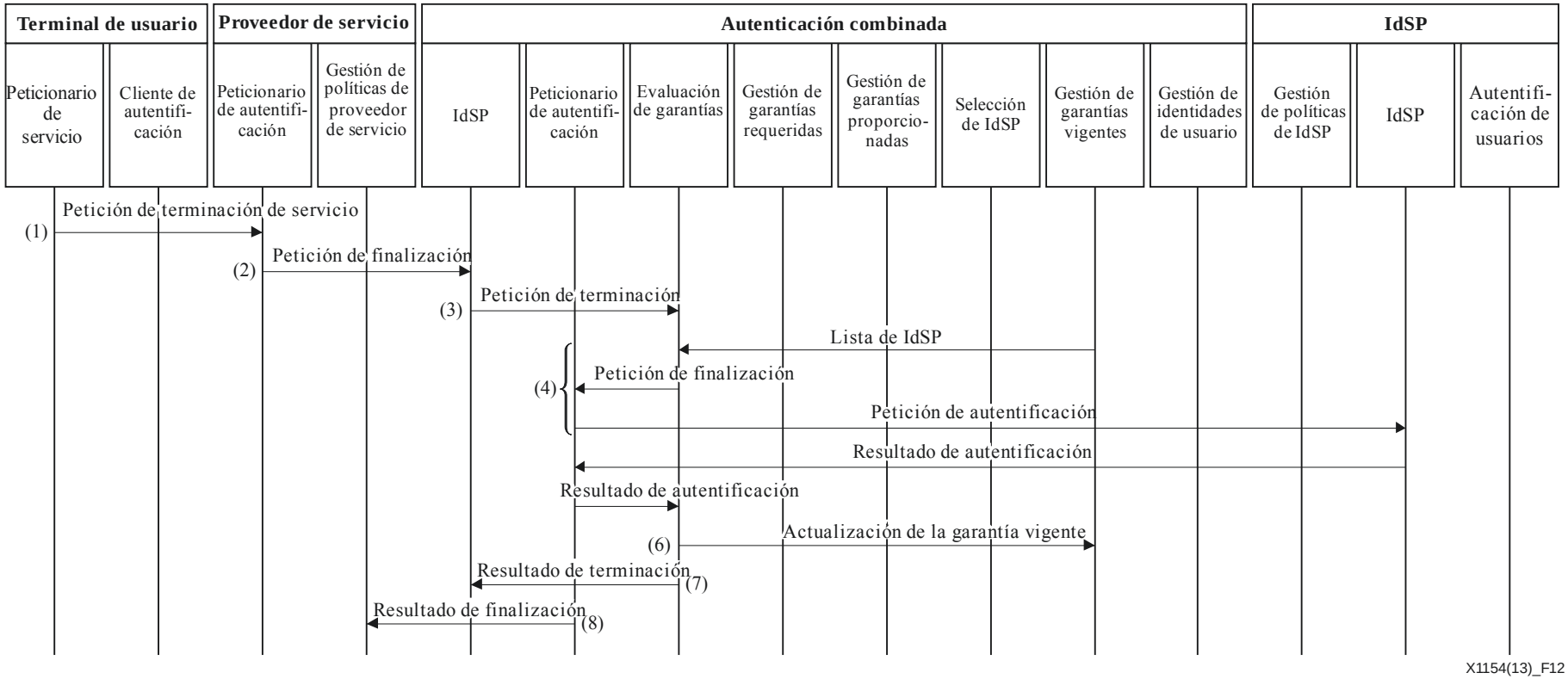

Figura 12 – Comportamiento básico de la terminación del servicio en el marco general de autentificación combinada en entornos con múltiples proveedores de servicio de identidad

9.2.3 Gestión de garantías requeridas de las funciones de proveedor de servicio

Para la gestión de las garantías requeridas de las funciones de proveedor de servicio en funciones de autentificación combinada se envía una garantía requerida desde la función de gestión de políticas de proveedor de servicio a la función de gestión de garantías requeridas mediante las operaciones establecer/actualizar/terminar.

9.2.4 Gestión de garantías proporcionadas de las funciones de IdSP

Para la gestión de las garantías proporcionadas de las funciones IdSP en funciones de autentificación combinada, se envía una garantía requerida desde la función de gestión de políticas del IdSP a la función de gestión de garantías proporcionadas mediante las operaciones establecer/actualizar/
terminar.

Anexo A

Consideraciones sobre la autentificación combinada

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

A.1 Obtención de la garantía de autentificación estimada

Puesto que la autentificación combinada es una autentificación que utiliza múltiples credenciales, se requieren diferentes credenciales para obtener una garantía de autentificación estimada. En otras palabras, una simple combinación de múltiples métodos de autentificación o de múltiples IdSP conducirá a un completo fracaso del nivel de garantía si se utiliza el mismo credencial.

Para conseguir una garantía de autentificación estimada, se requiere un proceso que verifique si las credenciales utilizadas en la autentificación combinada son realmente diferentes. Se recomienda que el proceso de verificación se realice antes de actualizar la garantía de autentificación vigente.

En el modelo en el que se implementan una función de autentificación combinada y funciones de autentificación de usuario en una entidad (por ejemplo, un IdSP proporciona una autentificación combinada), resulta sencillo efectuar el proceso de verificación en el IdSP. Es más, el proceso de verificación podría realizarse cuando es ejecutada la operación crear/actualizar.

Por otra parte, en el modelo en el que se implementan una función de autentificación combinada y funciones de autentificación de usuario en una entidad (por ejemplo, el SP utiliza múltiples IdSP que proporcionan una autentificación de factor único), se requiere para el proceso de verificación el intercambio de datos adicionales entre la función de autentificación combinada y la función de autentificación de usuario. Concretamente, se requiere en la función de autentificación de usuario una función que envíe los datos para identificar las credenciales. Es más, en la función de autentificación combinada se requiere una función para confirmar que se utilizan las diferentes credenciales comparando cada dato recibido desde las funciones de autentificación de usuario.

En el caso de aplicar el método de autentificación utilizando una infraestructura de clave pública (PKI) la función en la función de autentificación de usuario puede estar enviando una clave pública puesto que los datos que indican la credencial y la función en la función de autentificación combinada pueden comparar esos datos directamente.

Sin embargo, en el caso de aplicar el método de autentificación utilizando un secreto compartido (por ejemplo, una contraseña), la función en la función de autentificación de usuario tiene prohibido enviar el propio secreto compartido como parte de los datos que indican la credencial.

A.2 Selección de los IdSP

Cuando el proveedor de servicio reciba una petición de servicio desde el terminal, se requiere que la función de selección de IdSP descubra y seleccione IdSP adecuados.

Para seleccionar un IdSP apropiado, la función de gestión de garantías requeridas y la función de gestión de garantías proporcionadas deben estar implementadas en modo seguro.

Asimismo, se requiere que la función de gestión de garantías vigentes esté implementada en modo seguro en el IdSP (en el modelo en el que un IdSP proporciona una función de autentificación combinada) o en el SP (en el modelo en el que el SP proporciona la función de autentificación combinada).

Además, la función de evaluación de garantías debe recuperar la garantía de autentificación vigente, la garantía de autentificación requerida y la garantía de autentificación proporcionada de forma segura.

A.3 Garantía de autentificación efectiva

En algunos casos la garantía de autentificación efectiva puede ser inferior a la garantía de autentificación estimada debido a que la garantía de autentificación debido a diversos factores ambientales que pueden influir en ella.

En este caso, se precisa en el IdSP una función que envíe la garantía de autentificación efectiva. Asimismo, se requiere en el SP una función que actualice y evalúe la garantía de autentificación vigente del usuario a partir de la garantía de autentificación efectiva.

A.4 Consideraciones de seguridad para la autentificación multifactorial

Existen dos tipos de autentificación multifactorial: el primero utiliza una única credencial para la verificación y el segundo utiliza múltiples credenciales.

El primer tipo de autentificación se basa en un certificado de clave pública almacenado en la tarjeta inteligente o en una contraseña única que utiliza un dispositivo físico.

El segundo tipo de autentificación se basa en una combinación de una contraseña de un solo uso y factores biométricos.

El primer tipo de autentificación multifactorial es necesario cuando se usan equipos a prueba de manipulaciones para almacenar credenciales.

A.5 Consideraciones de seguridad para la autentificación multimétodo

En el caso de autentificación multimétodo se requiere que cada credencial no pueda derivarse (o no sea absorbida) por otras credenciales.

A.6 Consideraciones de seguridad para la autentificación múltiple

En el caso de múltiples autentificaciones, se requiere que cada credencial no se pueda obtener (ni sea extraída) por otras credenciales.

Apéndice I

Relación con normas conexas

(Este apéndice no forma parte integrante de la presente Recomendación.)

I.1 Relación con [UIT-T X.1141]

La Figura I.1 muestra la relación entre el modelo descrito en la presente Recomendación y el descrito en la cláusula 10 y en el lenguaje de marcaje de aseveración de seguridad (SAML 2.0) de [UIT-T X.1141]. Los recuadros grises son funciones definidas en SAML.

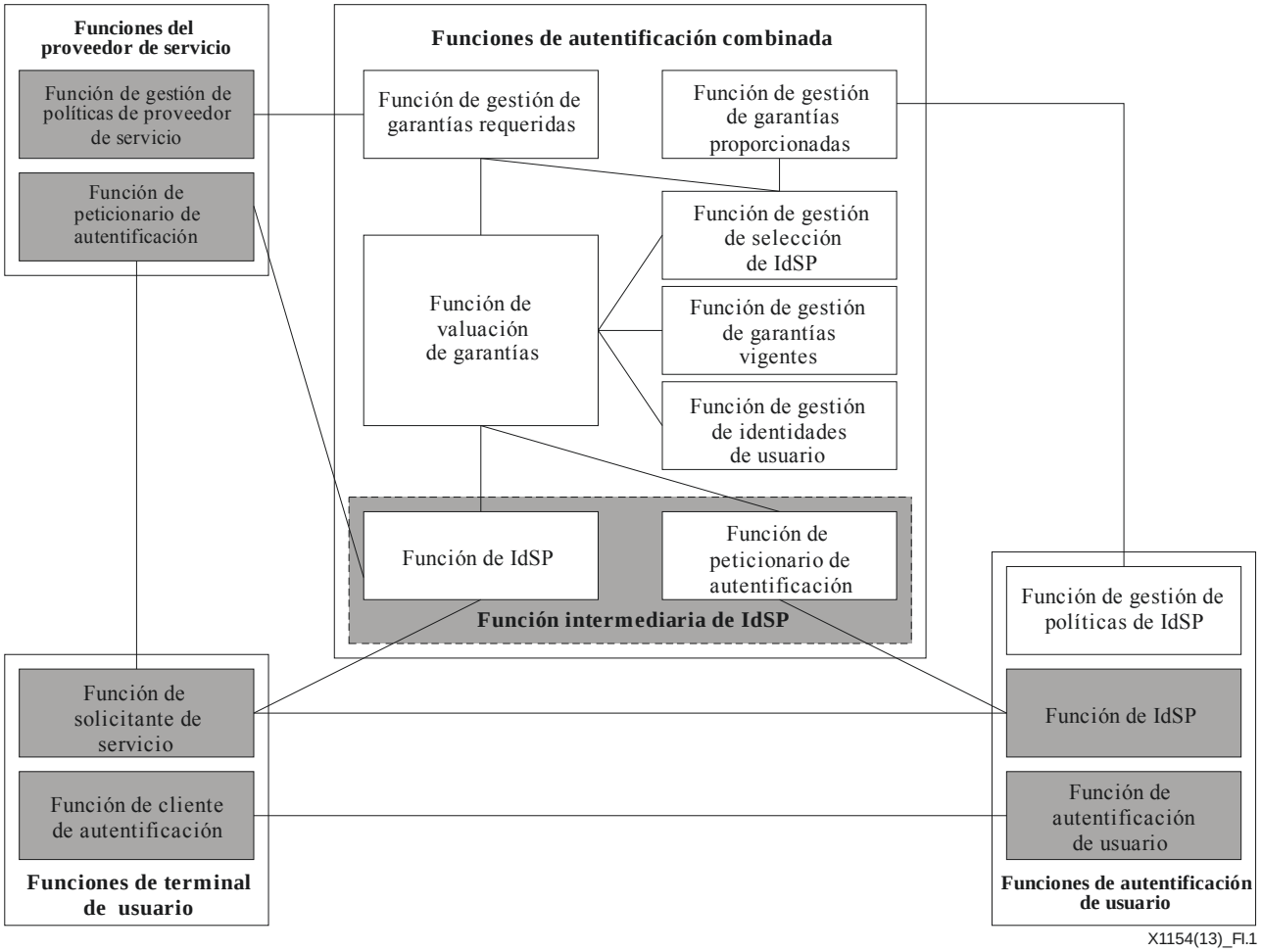

Figura I.1 – Relación con [UIT-T X.1141]

I.2 Relación con [UIT-T X.1254]

El marco en la presente Recomendación proporciona una autentificación combinada utilizando múltiples IdSP. Esto significa que este marco es una instancia para implementar la fase de autentificación, que se describe en [UIT-T X.1254], en entornos con múltiples IdSP.

Bibliografía

[b-UIT-T X.509] Recomendación UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

[b-UIT-T X.1084] Recomendación UIT-T X.1084 (2008), *Mecanismo del sistema de telebiometría – Parte 1: Protocolo general de autentificación biométrica y perfiles tipos para sistemas de telecomunicaciones.*

[b-UIT-T X.1086] Recomendación UIT-T X.1086 (2008), *Procedimientos de protección telebiométrica – Parte 1: Guía sobre las medidas técnicas y de gestión para la protección de la seguridad de los datos biométricos.*

[b-UIT-T X.1089] Recomendación UIT-T X.1089 (2008), *Infraestructura de autentificación de telebiometría (TAI).*

[b-UIT-T X.1151] Recomendación UIT-T X.1151 (2007), *Orientación sobre el protocolo de autentificación seguro basado en contraseña con intercambio de claves.*

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

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, 2014