Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2721

(09/2010)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Redes de la próxima generación – Seguridad

Requisitos de gestión de identidad en las NGN y ejemplos de utilización

Recomendación UIT-T Y.2721

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	**Y.2700–Y.2799**
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999

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

Recomendación UIT-T Y.2721

Requisitos de gestión de identidad en las NGN y ejemplos de utilización

Resumen

En esta Recomendación se describen ejemplos de utilización de la gestión de identidad (GId) y los requisitos para las redes de la próxima generación (NGN) y sus interfaces. Las funciones y capacidades de GId se utilizan para aumentar la confianza en la información de identidad y para mejorar y dar soporte a las aplicaciones empresariales y de seguridad, incluidos los servicios basados en la identidad.

Los requisitos prescritos en la presente Recomendación están destinados a las NGN (es decir, a redes de paquetes gestionadas), como se definen en la Recomendación UIT-T Y.2001.

Los objetivos y requisitos especificados en la presente Recomendación se basan en el marco GId de la Recomendación UIT-T Y.2720 y en un análisis de los ejemplos de utilización en las NGN. Estos ejemplos se presentan a título informativo y su base documental puede encontrarse en los apéndices a la presente Recomendación.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T Y.2721	2010-09-16	13

Palabras clave

Identidad federada, gestión de identidad, red de la próxima generación, seguridad.

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

Página

Recomendación UIT-T Y.2721

Requisitos de gestión de identidad en las NGN y ejemplos de utilización

1 Alcance

En esta Recomendación se presentan los objetivos, requisitos, directrices y ejemplos de utilización de la gestión de identidad (GId) en las redes de la próxima generación (NGN, *next generation network*) y sus interfaces. Las funciones y capacidades de GId se emplean para aumentar la confianza en la información de identidad y para mejorar y dar soporte a las aplicaciones empresariales y de seguridad, incluidos los servicios basados en la identidad.

Esta Recomendación comprende objetivos, requisitos, directrices y ejemplos de utilización relativos a:

- El aumento de la confianza en la información de identidad de una entidad NGN (por ejemplo, usuario, grupo, dispositivo de usuario, proveedor de servicio, empresa, federación, elemento de red y objeto).
- La gestión segura del ciclo de vida (por ejemplo, registro, validación, revocación) de la información de identidad, previo consentimiento específico e informado del usuario.
- La GId como habilitador de aplicaciones empresariales (por ejemplo, procedimiento de inicio y cierre de sesión único para múltiples servicios de aplicación) y de seguridad (por ejemplo, controles de acceso), incluidos los servicios basados en la identidad (por ejemplo, autentificación, aseveración e identidad federada).
- El descubrimiento e intercambio seguros de la información asociada con la identidad o identidades de una entidad NGN, previo consentimiento específico e informado del usuario. Esto comprende la información que pueda estar ubicada en una NGN y en varios dominios administrativos o federaciones diferentes.
- El interfuncionamiento/la compatibilidad entre los sistemas y capacidades de GId dentro de un dominio de proveedor NGN (es decir, dentro de la red).
- El interfuncionamiento/la compatibilidad de los sistemas y capacidades de GId entre diversos dominios de proveedor o federaciones diferentes, previo consentimiento específico e informado del usuario (por ejemplo, entre proveedores NGN, proveedores de servicios web y proveedores de contenido).
- La imposición de la política aplicable (por ejemplo, protección de la información de identificación personal) asociada con la identidad de una entidad o con su información de identidad.
- La seguridad de los sistemas, funciones, capacidades, datos y comunicaciones de GId.

Los objetivos y requisitos prescritos por esta Recomendación están destinados a las NGN (es decir, redes de paquetes gestionadas), como se definen en [UIT-T Y.2001], *Visión general de las NGN*.

Los objetivos y requisitos de esta Recomendación se basan en el marco de GId de [UIT-T Y.2720] y en un análisis de ejemplos de utilización, cuya documentación puede encontrarse en los apéndices a la presente Recomendación.

NOTA 1 – En esta Recomendación, el término "identidad", en relación con la GId, no tiene un valor absoluto. En concreto, no implica la validación positiva de una persona.

NOTA 2 – En esta Recomendación, el término "usuario" designa una persona, un grupo, una empresa, una persona jurídica o cualquier entidad que recurra a servicios NGN.

NOTA 3 – En esta Recomendación, el término "NGN/proveedor de servicio de identidad (NGN/PSId)" se utiliza para denominar a un proveedor NGN o tercero que ofrece servicios de GId.

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 Recomendación.

[UIT-T E.107] Recomendación UIT-T E.107 (2007), *Servicio de telecomunicaciones de emergencia (ETS) y marco de interconexión para implementaciones nacionales del ETS*.

[UIT-T X.811] Recomendación UIT-T X.811 (1995) | ISO/IEC 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación*.

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

[UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación*.

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2010), *Arquitectura y requisitos funcionales de las redes de próxima generación*.

[UIT-T Y.2201] Recomendación UIT-T Y.2201 (2009), *Requisitos y capacidades de las redes de próxima generación del UIT-T*.

[UIT-T Y.2205] Recomendación UIT-T Y.2205 (2008), *Redes de próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas*.

[UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autentificación y autorización en las redes de próxima generación versión 1*.

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

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 anonimato [UIT-T X.1252]: Situación en la que una entidad no puede ser identificada dentro de un conjunto de entidades.

NOTA – El anonimato impide el rastreo de entidades o de su comportamiento, como por ejemplo la localización del usuario, la frecuencia de utilización de un servicio, y así sucesivamente.

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

3.1.3 atributo [UIT-T X.1252]: Información relacionada con una entidad que especifica una característica de la entidad.

3.1.4 autentificación [UIT-T X.1252]: Proceso utilizado para obtener una confianza suficiente en la vinculación entre la entidad y la identidad presentada.

NOTA – En el contexto de la gestión de identidad (GId) se entiende que el término autentificación se refiere a la autentificación de una entidad.

3.1.5 garantía de autentificación [UIT-T X.1252]: Grado de confianza al que se llega en el proceso de autentificación del 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 de la relación entre la entidad que comunica y la entidad que está presente.

3.1.6 autorización [UIT-T X.1252]: Concesión de derechos y, sobre la base de esos derechos, concesión de acceso.

3.1.7 vinculación [UIT-T X.1252]: Una asociación, atadura o lazo explícitamente establecido.

3.1.8 declaración [UIT-T X.1252]: Declarar que es el caso, sin estar en condiciones de proporcionar pruebas.

3.1.9 declarante [UIT-T X.1252]: Entidad que es la principal o la representa a los efectos de la autentificación.

NOTA – Un declarante desempeña las funciones necesarias para participar en intercambios de autentificación en nombre de un principal.

3.1.10 contexto [UIT-T X.1252]: Entorno con fronteras definidas en el cual existen e interactúan las entidades.

3.1.11 credencial [UIT-T X.1252]: Conjunto de datos presentado como evidencia de una identidad y/o unos derechos declarados.

3.1.12 delegación [UIT-T X.1252]: Acción mediante la cual se asigna una autoridad, responsabilidad o función a otra entidad.

3.1.13 descubrimiento [UIT-T Y.2720]: El acto de localizar una descripción procesable mediante máquina de un recurso relacionado con una red que puede haberse desconocido previamente y que satisface ciertos criterios funcionales. Entraña la correspondencia de un conjunto de criterios funcional y de otro tipo con un conjunto de descripciones de recursos. La idea es encontrar un recurso idóneo relacionado con el servicio.

3.1.14 entidad [UIT-T X.1252]: Cualquier cosa que tenga una existencia autónoma y bien definida 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 estos elementos. En el contexto de las telecomunicaciones, como ejemplos de entidades cabe mencionar puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc.

3.1.15 telecomunicaciones de emergencia (ET, *Emergency Telecommunications*) [UIT-T Y.2205]: Todo servicio de emergencia que necesita de las NGN un tratamiento especial en comparación con otros servicios. Comprende los servicios de emergencia autorizados por el Estado y los servicios de seguridad pública.

3.1.16 servicio de telecomunicaciones de emergencia (ETS, *Emergency Telecommunications Service*) [UIT-T E.107]: Servicio nacional que proporciona telecomunicaciones prioritarias a los usuarios autorizados en situaciones de catástrofe y emergencia.

3.1.17 federación [UIT-T X.1252]: Una asociación de usuarios, proveedores de servicios y proveedores de servicios de identidad.

3.1.18 identidad federada [UIT-T Y.2720]: Identidad que puede utilizarse para acceder a un grupo de servicios o aplicaciones limitado por las políticas y condiciones de una federación.

3.1.19 identificador [UIT-T X.1252]: Uno o más de los atributos utilizados para identificar a una entidad dentro de un contexto.

NOTA – En el contexto de las NGN, según la definición que figura en [b-UIT-T Y.2091], un identificador es una serie de dígitos, caracteres y símbolos, o cualquier otro tipo de dato utilizado para identificar abonados, usuarios, elementos de red, funciones, entidades de red que proporcionan servicios/aplicaciones, u otras entidades (objetos físicos o lógicos).

3.1.20 identidad [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 gestión de identidad (GId), 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.

3.1.21 garantía de identidad [UIT-T X.1252]: El grado de confianza en el proceso de demostración de identidad utilizado para determinar la identidad de la entidad para la cual se expide la credencial, y el grado de confianza en que la entidad que utiliza la credencial es la entidad a la cual se le expidió o asignó la credencial.

3.1.22 gestión de identidad [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.

3.1.23 pauta de identidad (*identity pattern*) [UIT-T X.1252]: Una expresión estructurada de atributos de una entidad (por ejemplo, el comportamiento de una entidad) que podría utilizarse en algunos procesos de identificación.

3.1.24 proveedor de identidad (IdP, *identity provider*): Véase proveedor de servicio de identidad (PSId).

NOTA – El término "proveedor de identidad (IdP)" se utiliza en [UIT-T Y.2720] y en otras especificaciones de otras organizaciones. Ahora bien, para evitar confusión entre la entidad proporciona identidades y la entidad que gestiona identidades, en la presente Recomendación se utiliza el término proveedor de servicio de identidad (PSId).

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

3.1.26 red de próxima generación [UIT-T Y.2001]: Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios.

3.1.27 información de identificación personal (IIP, *personally identifiable information*) [UIT-T X.1252]: 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).

3.1.28 presencia [UIT-T Y.2720]: Conjunto de atributos que caracterizan una entidad en relación con la situación presente.

3.1.29 principal [UIT-T X.811]: Entidad cuya identidad puede ser autentificada.

3.1.30 privacidad [UIT-T X.1252]: Derecho de los particulares de controlar la información personal relacionada con ellos que se puede compilar, gestionar, retener y utilizar o distribuir, o de influir en dicha información.

3.1.31 parte dependiente (RP, *relying party*) [UIT-T X.1252]: Entidad que confía en la representación o declaración de identidad de una entidad solicitante/aseverante en un contexto de petición.

3.1.32 dominio de seguridad [UIT-T X.1252]: Un conjunto de elementos, una política de seguridad, una autoridad responsable de la seguridad y un conjunto de actividades relacionadas con la seguridad cuyos elementos se gestionan de conformidad con la política de seguridad.

3.1.33 confianza (*trust*) [UIT-T X.1252]: Firme creencia en la fiabilidad y veracidad de la información, o en la habilidad y disposición de una entidad para actuar adecuadamente dentro de un contexto especificado.

3.1.34 usuario (*user*) [UIT-T X.1252]: Entidad que utiliza un recurso, por ejemplo sistemas, equipos, terminales, procesos, aplicaciones o redes empresariales.

NOTA – En el contexto de las NGN, según la [b-UIT-T Y.2091], comprende al usuario final, persona, abonado, sistema, equipo, terminal (por ejemplo, fax, PC), entidad (funcional), proceso, aplicación, proveedor o red empresarial.

3.1.35 verificador [UIT-T X.1252]: Entidad que es o representa a la entidad que requiere una identidad autentificada. Un verificador incluye las funciones necesarias para intervenir en intercambios de autentificación.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Siglas y acrónimos

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

3G 3ª Generación (*3rd generation*)

AKA Acuerdo de autentificación y clave (*authentication and key agreement*)

ANI Interfaz aplicación-red (*application-to-network interface*)

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

BSS Sistema de soporte de negocio (*business support system*)

CDC Centro de distribución de claves (*key distribution centre*)

CSP Proveedor de servicios de comunicaciones (*communications service provider*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DeviceID Identidad de dispositivo (*device identity*)

DoS Denegación de servicio (*denial of service*)

EAG Pasarela de aplicación externa (*external application gateway*)

EV-DO Evolución por optimización de datos (*evolution data optimized*)

FE Entidad funcional (*functional entity*)

FTTX Fibra hasta X (*fibre-to-the-X*)

GBA Arquitectura de inicialización genérica (*generic bootstrapping architecture*)

GId Gestión de identidad (*identity management*)

HSS Servidor de abonado residencial (*home subscriber server*)

IBGC-FE Entidad funcional de control de pasarela de frontera de interconexión (*interconnection border gateway control functional entity*)

IdMCC-FE Entidad funcional de coordinación y control de IdM (*IdM coordination and control functional entity*)

IDPS Sistemas de detección y prevención de intrusión (*intrusion detection and prevention systems*)

ID-WSF Marco de servicios web de identidad (*identity web services framework*)

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

IMS Subsistema multimedios IP (*IP multimedia subsystem*)

IP Protocolo Internet (*Internet protocol*)

ISC Control de servicio IMS (*IMS service control*)

LS Servidor de ubicación (*location server*)

LTE Evolución a largo plazo (*long term evolution*)

MNO Operador de red móvil (*mobile network operator*)

MSISDN Número director del servicio integrado de abonado móvil (*mobile subscriber integrated service director number*)

NACF Funciones de control de anexión a la red (*network attachment control functions*)

NGN Red de la próxima generación (*next generation networks*)

NNI Interfaz red-red (*network-to-network interface*)

OAM&P Operación, administración, mantenimiento y configuración (*operation, administration, maintenance and provisioning*)

OSS Sistema de soporte de operaciones (*operations support system*)

PC Computador personal (*personal computer*)

P-CSC-FE Entidad funcional de control de sesión de llamada por intermediario (*proxy call session control functional entity*)

PDA Agenda digital (*personal digital assistant*)

POTS Sistemas telefónico convencional (*plain old telephone system*)

PS Servidor de presencia (*presence server*)

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

QoS Calidad de servicio (*quality of service*)

RACF Funciones de control de recursos y admisión (*resource and admission control functions*)

RFID Identificación por radiofrecuencias (*radio-frequency identification*)

RP Parte dependiente (*relying party*)

RTPC Red telefónica pública conmutada (*public switched telephone network*)

SAA-FE Entidad funcional de autentificación y autorización de servicio (*service authentication and authorization functional entity*)

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

S-CSC-FE Entidad funcional de control de sesión de llamada de servicio (*serving call session control functional entity*)

SCT Servidor de concesión de tique (*ticket granting server*)

SDE Servicio de directorio de empresa (*enterprise directory service*)

SIM Módulo de identidad de abonado (*subscriber identity module*)

SIP Protocolo de inicio de sesión (*session initiation protocol*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SN Nodo de servicio (*service node*)

SNI Interfaz servidor-red (*server-to-network interface*)

SP Proveedor de servicio (*service provider*)

STE Servicio de telecomunicaciones de emergencia (*emergency telecommunications service*)

SUP-FE Entidad funcional de perfil de usuario de servicio (*service user profile functional entity*)

TE Telecomunicaciones de emergencia (*emergency telecommunications*)

TI Tecnología de la información (*information technology*)

TVIP Televisión IP (*IP television*)

UE Equipo de usuario (*user equipment*)

UICC Tarjeta universal de circuito integrado (*universal integrated circuit card*)

UNI Interfaz usuario-red (*user-to-network interface*)

URI Identificador uniforme de recursos (*uniform resource identifier*)

UserID Identidad de usuario (*user identity*)

VoD Vídeo a la carta (*video-on-demand*)

VoIP Voz a través del protocolo Internet (*voice over Internet protocol*)

WiFi Fidelidad inalámbrica (*wireless fidelity*)

WiMAX Interoperabilidad mundial por acceso de microondas (*worldwide interoperability for microwave access*)

WLAN Red inalámbrica de área local (*wireless local area network*)

WS Servidor web (*web server*)

WSG Pasarela de servicio web (*web services gateway*)

xDSL Bucle de abonado digital x (*x digital subscriber loop*)

5 Convenios

En esta Recomendación:

La expresión "**se le exige que**" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si el documento pretende reclamar su conformidad.

La expresión "**se recomienda**" indica un requisito recomendado pero que no se exige con carácter taxativo. Por ello no es necesario cumplir este requisito para reclamar su conformidad.

La expresión "**se le prohíbe**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si el documento pretende ser conforme.

La expresión "**puede opcionalmente**" indica un requisito opcional admisible que no reviste en absoluto el carácter de recomendación. Esta expresión no pretende dar a entender que la implementación del fabricante deba suministrar una opción o característica que puedan ser activadas opcionalmente por el operador de red o proveedor del servicio. Más bien significa que el fabricante puede proporcionar opcionalmente esta característica sin menoscabo de su derecho de reclamar la conformidad con esta Recomendación.

En la parte principal de esta Recomendación, los anteriores requisitos podrán expresarse por medio de tiempos verbales o la utilización del verbo deber (formulación afirmativa o negativa). La utilización de tales tiempos o expresiones en los apéndices o partes explícitamente *informativas* no tendrá propósito normativo.

6 Visión general de la gestión de identidad (GId)

6.1 Consideraciones generales

En la Recomendación [UIT-T Y.2720] se presenta el marco general de gestión de identidad. Las funciones y capacidades de GId se utilizan para aumentar la confianza en la información de identidad de las entidades y soportar las aplicaciones empresariales y de seguridad (por ejemplo, control de acceso y autorización), incluidos los servicios basados en la identidad. Se considera que las entidades tienen una existencia distinta e independiente y que pueden identificarse unívocamente en un determinado contexto. Como ejemplos de entidades, en el contexto de la GId, pueden citarse los abonados, los usuarios, los elementos de red, las redes, las aplicaciones de software, los servicios y los dispositivos.

Las NGN soportarán una amplia gama de servicios de aplicación para los abonados usuarios finales, los gobiernos y las empresas privadas. A fin de asegurar la integridad y protección de los servicios de aplicación, se recomienda que las NGN admitan las funciones y capacidades necesarias para garantizar la identidad y los datos conexos asociados con una entidad en un contexto específico. Puede consultarse la definición de gestión de identidad en [UIT-T X.1252].

A definir los requisitos de gestión de identidad se tienen en cuenta los ejemplos de utilización que se presentan en los siguientes apéndices:

- Apéndice I – Casos generales de utilización de la GId
- Apéndice II – Casos de utilización de la GId para las aplicaciones NGN
- Apéndice III – Casos de utilización de la GId en el servicio de telecomunicaciones de emergencia (STE)
- Apéndice IV – Casos de utilización en el entorno móvil

Además, para definir los requisitos de GId se tienen en consideración los siguientes factores relacionados con la identidad del usuario en el entorno NGN:

- Con cada vez más frecuencia los usuarios finales utilizan múltiples identidades
- Una identidad puede estar asociada a diferentes contextos y privilegios de servicio

- Una identidad puede identificar solo parcialmente a un usuario final
- La entidad puede consistir en un pseudónimo
- Las identidades pueden utilizarse en cualquier lugar, en cualquier momento y desde cualquier dispositivo.
- Es posible que las identidades no sean compatibles entre distintos proveedores NGN.

6.2 Relaciones de gestión de identidad

En la figura 1 se presenta un esquema general de las relaciones de gestión de identidad basado en el marco de [UIT-T Y.2720].

Figura 1 – Relaciones de GId

Las entidades van desde los usuarios humanos individuales a las grandes organizaciones, como las empresas, y los objetos virtuales, como las aplicaciones electrónicas. La información de identidad asociada con cada entidad puede tener diversos grados de sensibilidad, desde datos relativamente públicos, por ejemplo el número de teléfono que aparece en la guía pública, hasta datos identificadores altamente sensibles, como las contraseñas, los certificados digitales y otros autentificadores privados.

Una entidad puede tener una o varias identidades. Estas identidades pueden utilizarse para múltiples papeles (ciudadano, cónyuge, pariente, cliente y paciente, por ejemplo) y se utilizan en transacciones específicas, tanto para actividades comerciales como sociales. Una persona puede estar asociada con múltiples identidades digitales en diferentes contextos, como se ve en la figura 1. Además, la persona a quien pertenecen las identidades digitales puede ser reconocida por otras bajo

varias personalidades asumidas o presentadas en público o en sociedad, o de acuerdo con la función (por ejemplo, en representación de un servicio de emergencia) que le asigna u otorga una autoridad.

En la figura 1 se puede ver lo siguiente:

a) Entidades:

En un entorno NGN, donde los servicios se basan en contextos y funciones y que pueden ser accesibles desde cualquier lugar, en cualquier momento y desde cualquier dispositivo, es posible que una entidad tenga asociadas múltiples formas de información de identidad. Además, una entidad puede poseer una o más entidades en función del contexto. Como ejemplos de entidades se pueden citar:

- Los usuarios y abonados.
- Los dispositivos de usuario, los elementos de red y los objetos.
- Las organizaciones, los grupos, las empresas privadas y las empresas públicas.
- La red y los proveedores de servicio.
- Los objetos virtuales.

b) Información de identidad:

La información de identidad asociada con una entidad puede dividirse en las siguientes categorías:

- Identificadores (por ejemplo, cuenta del abonado, direcciones de elementos de red, identificador del proveedor de servicios).
- Atributos (por ejemplo, dirección de correo electrónico, números de teléfono, URI, direcciones IP, papeles, declaraciones, privilegios, métodos de autentificación, pautas, ubicación).
- Credenciales (por ejemplo, testigos y certificados digitales).

c) Funciones y capacidades de GId:

Las funciones y capacidades de GId se utilizan para garantizar la información de identidad, garantizar la identidad o identidades de una entidad; y soportar y mejorar aplicaciones de negocios y de seguridad que incluyen servicios basados en la identidad. Las funciones y capacidades de GId son:

- Gestión del ciclo de vida de la identidad.
- Organización, correlación y vinculación de la información de identidad.
- Autentificación, garantía de autentificación y aseveración.
- Descubrimiento e intercambio de información de identidad.
- Funciones y capacidades para vincular diversos sistemas de GId para facilitar la compatibilidad.

d) Aplicaciones de negocios y de seguridad:

Las funciones y capacidades de GId soportan y mejoran las aplicaciones empresariales y de seguridad que incluyen servicios basados en la identidad.

Como ejemplo de aplicaciones empresariales se pueden citar:

- Servicios federados (por ejemplo, acceso a servicios de un proveedor de servicio a otra o a través de diferentes proveedores de NGN).
- Inicio y término de sesión únicos (por ejemplo, acceso a múltiples aplicaciones y servicios, sin necesidad de autentificar individualmente cada plataforma de aplicaciones o servicios).

Como ejemplo de aplicaciones de seguridad se pueden citar:

- Control de acceso.
- Autorización y gestión de privilegios.
- Protección de la información de identificación personal (IIP).

Como ejemplo de los servicios basados en la identidad se pueden citar:

- Servicios de identificador, credenciales y atributo.
- Servicios de vinculación (correspondencia e interfuncionamiento de la información de identidad en un entorno heterogéneo).
- Servicios de información pauta.

La gestión de identidad comprende los procesos de gestión del ciclo de vida, además de las funciones y capacidades de descubrimiento y obtención de fuentes de identidad que puedan utilizarse para verificar y validar las identidades. Los servicios y capacidades de GId permiten a las entidades usuarias/abonadas controlar cómo se utiliza y divulga su información de identidad. La GId ofrece a las entidades (por ejemplo, partes dependientes) la información necesaria para adoptar decisiones relativas a la autentificación y tener confianza en las transacciones y comunicaciones correspondientes. La GId también permite que los miembros de una federación (por ejemplo, diversos proveedores NGN, empresas privadas o empresas públicas) compartan y utilicen la información de identidad federada para en el marco de sus servicios. Por ejemplo, los servicios de identidad federada permitirían a las entidades autorizadas por miembros de la federación acceder a los recursos de acuerdo con las funciones y privilegios conformes con las normas y políticas de la federación sin necesidad de registrar y autentificar a cada uno de los miembros de la federación.

6.3 Factores y motivaciones

Dado que muchos servicios y capacidades NGN conllevan un servicio basado en la identidad y preferencias del abonado, al que se puede acceder desde cualquier dispositivo, en cualquier momento y lugar, las soluciones de GId han de poder responder en tiempo real a un número cada vez más complejo de interacciones, a medida que los usuarios pasan de un dispositivo, tecnología de acceso, método de pago e, incluso, identidad a otro. Además, los usuarios finales piden que las capacidades sean fáciles de utilizar y, lo que es más importante, que las capacidades les permitan controlar la privacidad y la información de identificación personal (IIP).

Los factores y motivaciones de la GId proceden de los usuarios finales (por ejemplo, abonados a aplicaciones y servicios), los proveedores NGN, las empresas privadas y públicas, pues todos ellos quieren que las aplicaciones de GId se ajusten a sus intereses y necesidades. A la hora de definir los requisitos de GId en las NGN hay que tener en cuenta los siguientes factores:

- Los usuarios finales/abonados necesitan controlar y proteger su información de identidad, desean disponer de métodos flexibles y uniformes de acceso a los recursos y necesitan equilibrar los beneficios de las redes sociales con la exposición de información personal.
- Los proveedores NGN (proveedores de red y de servicios) necesitan proteger sus recursos de infraestructura, servicios y aplicaciones de red, habilitar los servicios federados, fomentar la utilización e servicios de abono ampliamente disponibles y ajustarse a las necesidades de los usuarios finales en materia de privacidad y protección de la información de identificación personal (IIP).
- Las empresas privadas necesitan proteger sus intereses comerciales, confiar en la capacidad de garantía de identidad para las transacciones y proteger los datos de identidad de sus clientes.
- Las empresas y los usuarios profesionales necesitan proteger sus intereses comerciales, confiar en las capacidades de autentificación para las transacciones comerciales y la protección de los datos sobre la identidad de sus asociados comerciales.

- La protección de la infraestructura de red contra los ciberataques y la protección de los datos privados.
- Las organizaciones gubernamentales que ofrecen servicios públicos electrónicos, servicios de seguridad pública, servicios de alerta temprana, servicios de telecomunicaciones de emergencia (STE) y otros servicios nacionales.

6.4 Entorno federado con múltiples proveedores de servicio

En un entorno federado con múltiples proveedores de servicio, los servicios y capacidades de GId se utilizan para descubrir y comunicar información destinada a crear confianza en la identidad o identidades de las entidades. Por ejemplo, un proveedor de servicio de identidad, considerado como fiable por la parte dependiente, podría verificar los identificadores, credenciales y atributos asociados a una identidad y comunicarlos, mediante aseveraciones, a una parte dependiente (por ejemplo, un usuario o un proveedor de servicio) a los efectos de autentificación para el control de acceso, las decisiones comerciales y la aplicación de la política pertinente (por ejemplo, privacidad y protección de información de identificación personal).

Por otra parte, puede haber diferentes soluciones de GId independientes que despierten la necesidad de compatibilidad entre proveedores de servicio.

6.5 Proveedor de servicio de identidad (PSId)

En esta Recomendación no se imponen restricciones relativas al prestatario de servicios de proveedor de servicio identidad (PSId).

Un PSId es una entidad que mantiene, gestiona y puede crear información de identidad fiable de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios basados en la identidad asentados en relaciones de confianza, comerciales o de otro tipo.

En un entorno con múltiples proveedores de servicio, es posible que un proveedor NGN sea un PSId y ofrezca servicios de gestión de identidad (es decir, servicios basados en la identidad) a otros proveedores.

En esta Recomendación, el término "PSId /NGN" implica que un proveedor NGN o una tercera parte pueden ofrecer servicios GId.

6.6 Gestión de identidad en el contexto de las arquitecturas NGN y los modelos de referencia

6.6.1 Relación con la arquitectura funcional NGN

En el contexto del modelo de arquitectura NGN de referencia definido en [UIT-T Y.2012], es posible que las funciones de GId residan en diferentes planos (por ejemplo, usuario, control y gestión) y en diferentes estratos de la arquitectura distribuida (por ejemplo, estrato de servicio y estrato de transporte). Desde el punto de vista de la realización o aplicación, el soporte de los servicios y capacidades GId pueden conllevar la utilización de los elementos de red existentes o la utilización de elementos de red adicionales (por ejemplo, servidores de aplicación especializados) en una NGN.

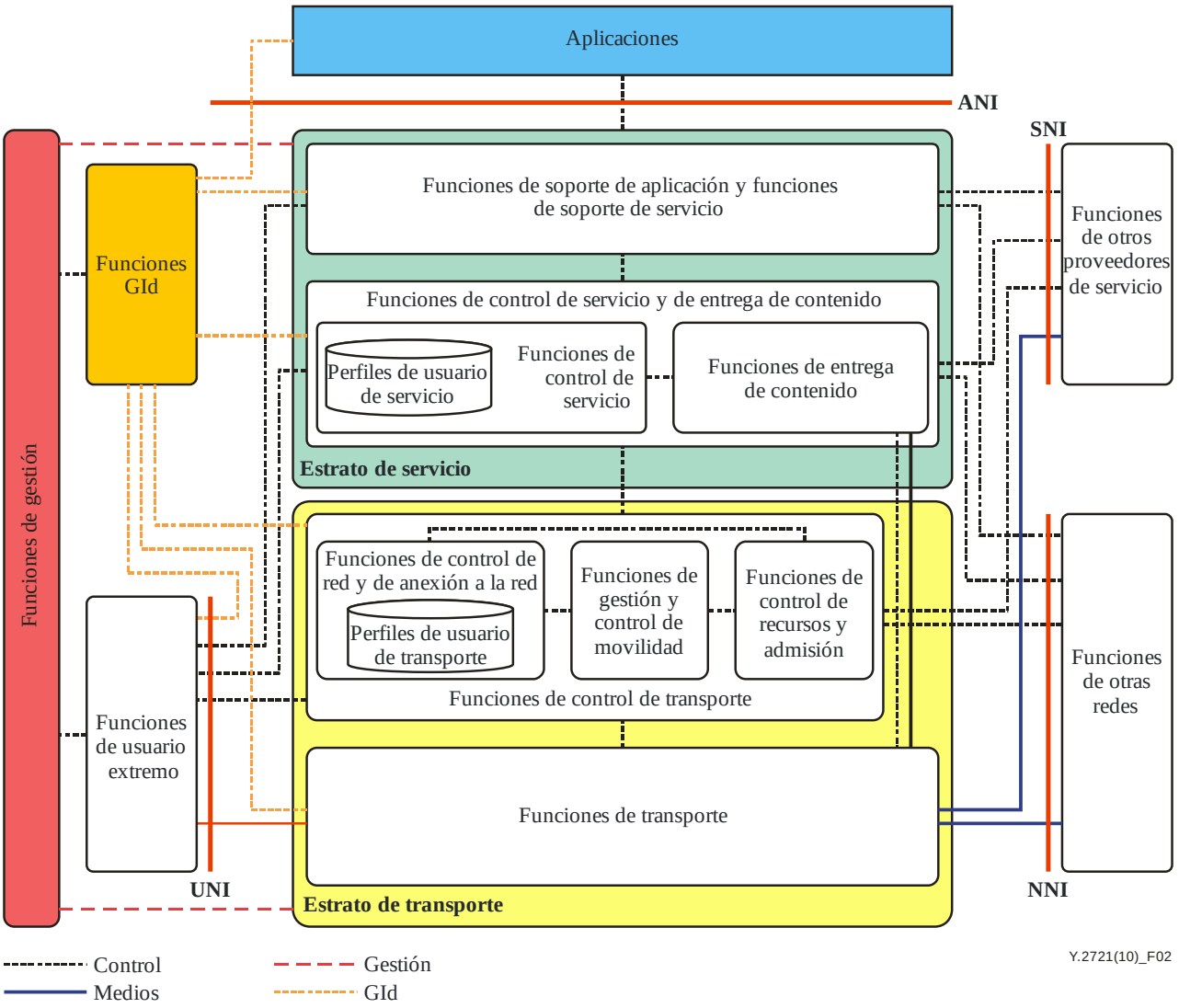


Figura 2 – Arquitectura general de la NGN

La figura 2 se basa en la figura 7-1 de [UIT-T Y.2012] y consta de un bloque funcional que representa funciones GId en la arquitectura funcional NGN. La figura 7-1 de [UIT-T Y.2012] ejemplifica los conceptos generales según los cuales el soporte de los servicios y capacidades GId puede conllevar la interacción con entidades funcionales (FE, *functional entities*) específicas que facilitan y soportan los servicios, incluidos los de identidad. Esto puede incluir las interacciones con las FE en los siguientes bloques funcionales, en función del servicio o capacidad GId específico que se soporta y del diseño de aplicación:

– aplicaciones;

– estrato de servicio: funciones de soporte de aplicación y funciones de soporte de servicio, funciones de control de servicio y funciones de entrega de contenido;

– estrato de transporte: funciones de control de transporte y funciones de transporte;

– funciones de usuario final;

– funciones de gestión.

En la arquitectura funcional NGN, las funciones de GId pueden residir en diferentes planos (por ejemplo, usuario, control y gestión) y en diferentes estratos de la arquitectura distribuida (por ejemplo, estrato de servicio y estrato de transporte). Aunque las funciones de GId se muestran como un grupo independiente de funciones, no se pretende imponer limitaciones o diseños concretos a los

sistemas GId. Las funciones GId deben cumplir las políticas aplicables, tales como reglamentos nacionales y regionales y la legislación en materia de protección de datos de identidad (por ejemplo, IIP). Concretamente, al crear y utilizar de funciones GId se debe velar por que guarden conformidad con las políticas pertinentes para cumplir los siguientes principios básicos de protección de datos:

- vinculación de los datos a un objetivo específico;
- no compartición de datos entre aplicaciones para fines distintos;
- limitación de los datos al mínimo necesario para un objetivo específico;
- derecho de las personas a controlar su IIP.

NOTA – En determinados reglamentos nacionales, lo anterior se traduce en crear funciones GId separadas en los diferentes estratos de las NGN.

6.6.2 Interfaces externas y comunicaciones de GId

Las interfaces normalizadas definidas en [UIT-T Y.2012] se utilizan para intercambiar datos de identidad entre distintos dominios administrativos y federaciones, y pueden incluir, según el caso:

- la interfaz usuario-red (UNI);
- la interfaz red-red (NNI);
- la interfaz aplicación-red (ANI);
- la interfaz servidor-red (SNI).

La interfaz escogida dependerá de factores tales como la aplicación específica y las necesidades de servicio (por ejemplo, tiempo real por oposición a tiempo casi real), el protocolo (por ejemplo, SAML, Diameter, RADIUS, SIP) y los mecanismos y métodos.

En el apéndice VI se muestra un ejemplo de utilización de la GId donde se ve cómo pueden utilizarse las interfaces NGN externas.

6.6.3 Modelos transaccionales

En [b-UIT-T X.1250] se presentan modelos transaccionales con múltiples partes (por ejemplo, usuarios, PSId y partes dependientes). En el apéndice V se resumen los modelos transaccionales descritos en [b-UIT-T X.1250].

7 Objetivos de la gestión de identidad

A continuación se enumeran los objetivos generales de la gestión de identidad:

1) Facilitar la toma de decisiones con confianza entre entidades.
2) Permitir soluciones GId que minimicen las consecuencias para los usuarios/abonados.
3) Ofrecer soluciones con nuevas capacidades que propiciarán una transición adecuada.
4) Admitir soluciones de GId compatibles dentro del dominio de proveedor NGN. Por ejemplo, compatibilidad entre productos de distintos fabricantes que soportan múltiples servicios de aplicación (por ejemplo, VoIP, TVIP, Vídeo y Datos).
5) Permitir soluciones de GId compatibles en diversos dominios y federaciones de proveedor NGN y proveedor de servicio, basadas en acuerdos y relaciones comerciales aplicables y en aplicación de los reglamentos y políticas en materia de protección de IIP.
6) Permitir la vinculación de sistemas GId y federaciones heterogéneos. Por ejemplo, la capacidad de poder vincular los sistemas GId del proveedor NGN con otros tipos de sistemas GId (por ejemplo servicios web, contenido y sistemas GId de proveedores terceros) sobre la base de los acuerdos y relaciones comerciales aplicables y en aplicación de los reglamentos y políticas en materia de protección de IIP.

7) Permitir a los usuarios finales/abonados interactuar y utilizar servicios de aplicación fácilmente y de manera intuitiva, conservando el control de sus datos personales durante todo su ciclo de vida, lo que comprende cómo y cuándo la información se utiliza y quién la utiliza.

8) Permitir que los usuarios finales/abonados revelen la información estrictamente necesaria para establecer una confianza mutua y realizar transacciones basadas en las políticas aplicables.

9) Lograr que los usuarios finales/abonados puedan verificar la autenticidad de la entidad que solicita los datos de identidad y la IIP. El usuario/abonado tiene por objetivo utilizar múltiples identificadores en función del contexto.

10) Conseguir que los usuarios finales/abonados actúen de manera anónima, pseudónima o conocida en función del contexto de aplicación y las políticas aplicables.

8 Requisitos de gestión de identidad

En esta cláusula se describen los requisitos de GId aplicables a las NGN, de acuerdo con los requisitos de alto nivel de las NGN descritos en [UIT-T Y.2201].

8.1 Requisitos generales

A continuación se presentan los requisitos generales de gestión de identidad:

R-1 El PSId/NGN ha de poder soportar funciones y capacidades para gestionar la identidad de los diversos tipos de entidades que soportan las NGN, entre los que se cuentan:

a) Los usuarios/grupos.

b) Las organizaciones/federaciones/empresas/ proveedores de servicio.

c) Los dispositivos/elementos de red/sistemas.

d) Los objetos (por ejemplo, proceso de aplicación, contenido, datos).

R-2 El PSId/NGN está obligado a soportar:

a) La gestión segura del ciclo de vida (es decir, desde la expedición hasta la revocación) de identidades.

b) El descubrimiento e intercambio seguros de la información de identidad, lo que comprende el descubrimiento e intercambio de la información de identidad que pueda estar ubicada en una NGN y en diferentes dominios administrativos.

R-3 El PSId/NGN debe soportar la aplicación de las políticas pertinentes asociadas a la información de identidad o identidades de una entidad.

R-4 El PSId/NGN debe soportar las funciones y capacidades de GId para las aplicaciones en tiempo real (por ejemplo, VoIP y TVIP) y en tiempo casi real (por ejemplo, transacciones de datos por la web).

R-5 El PSId/NGN debe soportar las funciones y capacidades de GId para permitir la aseveración anónima de la información de identidad (por ejemplo, identidad y atributos), en función de la política aplicable.

R-6 El PSId/NGN debe soportar el interfuncionamiento seguro de la GId entre los elementos de la red dentro del dominio del proveedor NGN (es decir, dentro de la red) y entre diferentes dominios de proveedor (por ejemplo, con otro proveedor NGN, proveedores de servicios web).

R-7 El PSId/NGN debe soportar servicios y características de fácil utilización para los usuarios finales, como:

a) Inicio y término de sesión únicos para múltiples servicios de aplicación.

b) Servicios convergentes (por ejemplo, convergencia fijo-móvil).

c) Control y protección de información de identificación personal (IIP).

R-8 El PSId/NGN debe soportar el inicio de sesión único en aplicaciones que utilizan credenciales vinculadas a un dispositivo de abonado (por ejemplo, credenciales UICC) o vinculadas a un usuario/abonado (por ejemplo, credenciales Digest SIP) según proceda, de acuerdo con los requisitos de seguridad de las aplicaciones. Concretamente:

- Deberá poder utilizar credenciales de abonado (por ejemplo, credenciales Digest SIP) para el inicio de sesión único con el fin de acceder a aplicaciones desde dispositivos móviles.
- Deberá poder utilizar credenciales de abonado (por ejemplo, credenciales Digest SIP) para el inicio de sesión único con el fin de acceder a aplicaciones desde dispositivos fijos.

8.2 Requisitos de gestión del ciclo de vida de la identidad

La gestión del ciclo de vida de la identidad comprende los procesos y procedimientos de afiliación y expedición de información de identidad (por ejemplo, identificadores, credenciales y atributos).

R-9 El PSId/NGN debe establecer y aplicar las políticas pertinentes para la gestión del ciclo de vida de la identidad, lo que incluye los procesos, procedimientos y políticas para la demostración, incorporación, expedición y revocación de información de identidad.

8.2.1 Afiliación y expedición

La afiliación de una entidad (por ejemplo, abonado, dispositivo, organización, proveedor NGN u objeto), en un contexto comienza con la demostración de la identidad o credencial y su afiliación. Ésta consiste en dar de alta una entidad en un contexto, registrar su identidad y posiblemente asignarle atributos específicos (por ejemplo, identificadores, credenciales o papeles). En el caso de los abonados usuarios finales, se trata del proceso mediante el cual un particular solicita su conversión en abonado a un PSId o proveedor NGN.

La demostración comprende la verificación y validación de los atributos, y posiblemente de sus credenciales.

R-10 El PSId/NGN debe verificar y validar la identidad de la entidad al realizar la afiliación, con arreglo a los requisitos del contexto. El registro de la identidad de la entidad y asignarle identificadores, credenciales y atributos para un determinado contexto está supeditado a la confirmación de que se cumplen los criterios y políticas de demostración aplicables.

Los procesos y políticas de demostración se basarán en el valor de los recursos (por ejemplo, servicios, transacciones, información y privilegios) autorizados a la identidad y de los riesgos asociados a la obtención y utilización de la identidad por parte de una entidad no autorizada. En concreto, se necesitan tomar medidas para garantizar lo siguiente:

- Existe una entidad (por ejemplo, persona física, organización o persona moral) con los atributos reclamados, que son adecuados para identificar a la entidad con suficiente exactitud según las necesidades del contexto.
- El solicitante cuya identidad se registra es, de hecho, la entidad a quien pertenece la identidad.
- Resulta difícil para una entidad que ya ha utilizado la identidad y credenciales registradas repudiar más adelante la inscripción/incorporación y poner en tela de juicio la autentificación.

Una vez completado con éxito el proceso de incorporación y demostración, se registra la entidad, y quizá también sus credenciales y/o atributos asignados, que servirán para autentificarla en el futuro.

R-11 Es necesario que la información de identidad (por ejemplo, identificadores, credenciales y atributos) relativa a una entidad sólo se expida una vez haya quedado demostrada la identidad de la entidad.

En algunos casos, también puede ser necesario registrar y expedir credenciales electrónicas, como los certificados digitales y los testigos vinculados a la identidad o a la declaración (es decir, atributo) relativa a la identidad. Dependiendo del tipo de testigo que se utilice, el PSId/NGN creará un nuevo testigo y lo entregará al abonado, o le exigirá que registre uno de los testigos que ya posee o ha creado recientemente.

R-12 En cualquier caso, el mecanismo de transporte del testigo desde su punto de origen hasta la otra parte ha de ser seguro a fin de garantizar la confidencialidad y la integridad del nuevo testigo.

8.2.2 Mantenimiento y actualización

Después de que una identidad, incluida cualquier información de identidad (identificador, credenciales y atributos) se haya registrado y expedido, tanto el PSId/NGN como el abonado tienen responsabilidades durante la fase operativa y de utilización a fin de mantenerla segura.

R-13 El PSId/NGN debe gestionar y mantener de manera segura los datos y el estado de los datos (por ejemplo, identificadores, credenciales, atributos) asociados a una identidad.

R-14 El PSId/NGN debe gestionar y registrar de manera segura las actualizaciones o modificaciones de las identidades.

R-15 El PSId/NGN debe validar periódicamente el estado de la identidad y sus datos asociados (por ejemplo, identificadores, credenciales y atributos).

R-16 El PSId/NGN debe soportar procedimientos de notificación de la actualización o modificación de una identidad o de cualquiera de sus datos asociados a los sistemas y elementos de red que han de conocer las actualizaciones o modificaciones.

R-17 El PSId/NGN debe facilitar funciones para informar al usuario sobre los datos de su identidad y para modificarlos o suprimirlos.

El abonado también es responsable de la seguridad de las credenciales asignadas de conformidad con los acuerdos comerciales y políticos contraídos con el PSId/NGN. Por ejemplo, el abonado tiene la responsabilidad de gestionar sus credenciales electrónicas (por ejemplo, testigos) y mantenerlas seguras.

R-18 El PSId/NGN debe tomar medidas de acuerdo con los acuerdos comerciales y contractuales con el fin de garantizar que la entidad (por ejemplo, el abonado u otro PSId/NGN) pueda gestionar y utilizar de manera segura las credenciales expedidas (por ejemplo, certificados digitales o testigos) para una identidad, de acuerdo con las políticas y reglamentos aplicables.

8.2.3 Revocación

La revocación de identidad es el proceso por el cual se rescinden una identidad y las credenciales asociadas a la misma. La parte o sistema (por ejemplo, el PSId/NGN) que gestiona la identidad o credenciales es responsable de su terminación o anulación. La revocación es necesaria para impedir que se siga utilizando una identidad o una credencial que ha dejado de ser válida o tiene un fallo de seguridad.

R-19 El PSId/NGN debe establecer y aplicar las políticas pertinentes para revocar una identidad. En concreto, deberá soportar las capacidades para terminar o destruir las credenciales (por ejemplo, certificados digitales o testigos) asociadas con una identidad cuando éstas han dejado de ser válidas o tienen un fallo de seguridad.

R-20 El PSId/NGN debe soportar procedimientos de notificación de la revocación o terminación de una identidad o cualquiera de sus datos relativos a la entidad y a los sistemas y elementos de la red que han de conocer esta información (es decir, todos los sistemas y procesos con los que se puede utilizar la identidad para tener acceso han de recibir una notificación de que la identidad ha dejado de ser válida).

8.3 Funciones OAM&P de gestión de identidad

8.3.1 Modelo y esquema de datos

Cada proveedor NGN, federación o empresa deberá tener su propio formato, esquema, definiciones o semántica de representación y compartición de la información y los datos de identidad. En la cláusula 8.2.1 de [UIT-T Y.2720] se describe la necesaria compatibilidad entre sistemas GId heterogéneos que emplean distintos modelos, estructuras y esquemas de datos.

R-21 El PSId/NGN debe soportar funciones y capacidades para permitir la compatibilidad entre sistemas de GId heterogéneos que emplean diferentes modelos, estructuras y esquemas de datos, según proceda.

8.3.2 Gestión de los datos de identidad

En la cláusula 8.2 de [UIT-T Y.2720] se describe la necesaria gestión de los datos de identidad (por ejemplo, gestión de identificadores, credenciales y atributos). Los detalles de los requisitos de gestión de los datos de identidad quedan fuera del alcance de la presente Recomendación.

En una NGN, los distintos datos de identidad (por ejemplo, identificadores como las direcciones de correo electrónico, los números de teléfono, los UIR y las direcciones IP) pueden estar gestionados por diversos sistemas de gestión y procesos operativos (por ejemplo, sistema de soporte de operaciones (OSS)/sistema de soporte de negocios (BSS)). Los siguientes requisitos generales están destinados a un contexto en el que se emplea un método estructurado y coordinado de interacción entre diversos sistemas de gestión y sistemas de atención al cliente para soportar los servicios y capacidades de GId.

R-22 El PSId/NGN ha de soportar una interfaz normalizada (por ejemplo, portal de clientes) para que los usuarios finales/abonados puedan interactuar con los sistemas y procesos de gestión de la NGN que soportan las transacciones de gestión de los datos de identidad de los usuarios finales/abonados (por ejemplo, modificaciones y actualizaciones), con sujeción a los reglamentos y políticas aplicables en materia de protección de datos.

R-23 El PSId/NGN debe soportar la interfaces, funciones y capacidades necesarias para facilitar la coherencia de las transacciones y flujos de trabajo entre los distintos sistemas y procesos de gestión relacionados con la gestión de los datos de identidad (por, ejemplo, modificaciones y actualizaciones que han de pasar por diversos OSS/BSS, sistemas de atención al cliente y plataformas de servicios de aplicación), según proceda, con sujeción a los reglamentos y políticas aplicables en materia de protección de datos.

R-24 El PSId/NGN debe soportar funciones y capacidades de registro y almacenamiento (por ejemplo, copia de seguridad) de las transacciones relacionadas con la gestión de los datos de identidad, con sujeción a los reglamentos y políticas aplicables en materia de protección de datos.

R-25 El PSId/NGN debe soportar funciones y capacidades para sincronizar las modificaciones y actualizaciones de los datos de identidad entre los distintos sistemas y procesos de gestión, según proceda, con sujeción a los reglamentos y políticas aplicables en materia de protección de datos.

R-26 El PSId/NGN debe soportar funciones y capacidades de verificación de los vínculos entre los datos de identidad asociados a una entidad (por ejemplo, abonado) y los servicios

contraídos (por ejemplo, acceso, voz, datos, vídeo), con sujeción a los reglamentos y políticas aplicables en materia de protección de datos.

8.4 Funciones de señalización y control

8.4.1 Descubrimiento de la información de identidad

En un entorno NGN distribuido, la información de identidad puede residir en diversos elementos de la red (por ejemplo, servidor de abonado, servidor de ubicación, servidor de presencia, servidor de abonado residencial, etc.) para que una aplicación pueda utilizar la información de identidad, necesita saber que existe y dónde se encuentra.

R-27 El PSId/NGN debe soportar funciones y capacidades de descubrimiento de las fuentes de información de identidad dentro de un dominio PSId/NGN. Por ejemplo, las funciones y capacidades para que un servidor de gestión de identidad descubra la existencia de información de identidad en otros elementos de la red, como los servidores de ubicación, presencia o abono o para que un servicio/aplicación descubra la gestión e identidad u otros servidores donde se encuentran datos de identidad.

R-28 El PSId/NGN debe soportar funciones y capacidades que utilizan interfaces y protocolos normalizados para descubrir las fuentes de información de identidad en diversos dominios de PSId/NGN. Por ejemplo, la utilización de interfaces y protocolos normalizados para el descubrimiento de fuentes de información de identidad en otros dominios PSId/NGN de conformidad con los acuerdos entre redes aplicables.

R-29 El PSId/NGN debe soportar capacidades de protección de las capacidades y mecanismos de descubrimiento.

8.4.2 Control de acceso a la información de identidad

Los datos de identidad sólo han de ser accesibles a las entidades autorizadas a acceder a la información.

R-30 Es necesario que la información de identidad sólo sea accesible para las entidades autorizadas de acuerdo con los reglamentos y políticas aplicables. En concreto:

- El PSId/NGN debe autentificar la entidad (por ejemplo, parte dependiente) que solicita datos de identidad o realizar una autentificación mutua.
- El PSId/NGN debe autentificar la entidad (por ejemplo, parte dependiente o parte solicitante) que solicita datos de identidad, y verificar y validar su autorización antes de conceder acceso a la información o que solicita el intercambio de datos de identidad.

8.4.3 Comunicaciones de gestión de identidad

Los sistemas y elementos de red han de establecer sesiones de comunicación para intercambiar informaciones de identidad (por, ejemplo, identificadores, credenciales y atributos) ubicados en diversos sistemas de red (por ejemplo, servidor de gestión de identidad, servidor de abonado, servidor de ubicación, servidor de presencia, etc.) que pueden correlacionarse y verificarse (es decir, mediante un servidor de aplicación GId que realiza las funciones de autentificación y correlación) para ofrecer capacidades de garantía de identidad.

Los PSId/NGN pueden comunicar aseveraciones de identidad y de atributos asociados (por ejemplo, declaraciones y privilegios) a las partes dependientes, por ejemplo para que puedan adoptar decisiones de control de acceso. Esto permite que diversos servicios de aplicación (es decir, de plataformas de proveedores diferentes) utilicen un servicio de GId disponible común, en lugar de soluciones independientes y autónomas. Las relaciones de comunicación que se han de considerar, entre otras, son:

- Intrarred: Comunicaciones dentro de un dominio de proveedor NGN (por ejemplo, entre elementos de red).

- Interred: Comunicaciones entre dos proveedores NGN diferentes.
- Federación: Comunicaciones entre miembros de una federación.

8.4.3.1 Comunicaciones en tiempo real y tiempo casi real

La solución que se utilice para descubrir e intercambiar información de identidad deberá tener en cuenta si se necesitan comunicaciones en tiempo real o en tiempo casi real. Esto dependerá de las aplicaciones específicas que se soportan. Determinadas aplicaciones (por ejemplo, VoIP y TVIP) pueden necesitar la validación de la identidad del usuario/abonado solicitante y la autorización para el servicio de aplicación. Otras aplicaciones (por ejemplo, servicios de mensajería y datos) pueden necesitar solamente sesiones de comunicación en tiempo casi real para validar la identidad del usuario/abonado solicitante y la autorización para el servicio de aplicación.

R-31 El PSId/NGN debe soportar capacidades de establecimiento de sesiones de comunicación conformes con los requisitos específicos del servicio de aplicación a fin de intercambiar información de identidad en tiempo real o casi real. Esto incluye las sesiones de comunicación para intercambiar información de identidad dentro de un dominio de proveedor NGN, entre dos proveedores NGN distintos y entre miembros de una federación.

La información de atributo puede limitarse, aunque no es obligatorio, a la situación del miembro, la función de afiliado (facturación, operaciones), los atributos utilizados por otros servicios (como el servicio de directorio o de certificado), lo que permite a la parte dependiente facilitar a los usuarios información y contenidos adaptados a sus atributos.

R-32 El PSId/NGN y la parte dependiente han de poder intercambiar aseveraciones asociadas con la identidad de una entidad, lo que comprende la aseveración de las declaraciones de atributos.

8.4.4 Correlación y vinculación

La información de identidad (por ejemplo, identificadores, credenciales y atributos) pueden correlacionarse para establecer una vinculación que garantice la identidad de una entidad. Por ejemplo, la información de identidad asociada a un abonado (por ejemplo, ID de usuario), un dispositivo de abonado (por ejemplo, ID de dispositivo) y otra información conexa, como la ubicación y los datos de pauta pueden estar correlacionados para establecer una vinculación que ofrezca un mayor grado de garantía a la identidad del abonado (es decir, confianza en la validez de la identidad).

R-33 El PSId/NGN debe soportar capacidades para correlacionar múltiples datos de identidad (por ejemplo, ubicación y pauta) y establecer la adecuada vinculación con la identidad de la entidad, con sujeción a los reglamentos y políticas aplicables en materia de protección de datos. Para utilizar estas capacidades se requiere el consentimiento explícito e informado del usuario.

NOTA – Algunos reglamentos y políticas nacionales en materia de protección de datos podrían limitar este requisito.

8.4.5 Requisitos de autentificación

La autentificación es el proceso mediante el cual se establece la confianza en la relación entre una identidad y la entidad. Un medio de garantizar la autentificación es describir los objetivos y directrices necesarios para cuantificar los riesgos que existen de que una entidad sea quien o lo que declara ser. Esto comprende la determinación de qué identificadores de entidad son más importantes que otros en el proceso de identificación y por qué determinados identificadores utilizados en la autentificación no han de tener el mismo valor autentificativo.

Véanse los requisitos de autentificación en las NGN en [UIT-T Y.2702].

A continuación se enumeran los requisitos de seguridad para la autentificación en la gestión de identidad:

R-34 Se podrá realizar la autentificación mutua entre entidades (por ejemplo, usuario, PSId/NGN, parte dependiente).

R-35 La parte dependiente ha de poder enviar solicitudes al PSId/NGN para la autentificación de una entidad (por ejemplo, usuario/abonado).

R-36 El PSId/NGN deberá admitir la autentificación de una entidad (por ejemplo usuario/abonado) y enviar aseveraciones a la parte dependiente.

R-37 La parte dependiente debe poder solicitar que se vuelva a autentificar una entidad especificando si se ha de utilizar el método en vigor u otro alternativo.

8.4.6 Garantía de autentificación

La garantía de autentificación es el grado de confianza alcanzado durante la autentificación en que la parte con la que se comunica es la entidad que declara ser o esperada. La confianza se basa en el grado de confianza en dicha relación entre la entidad comunicante y la identidad que se presenta. Cada entidad (usuario, servicio de aplicación, etc.) puede tener necesidades distintas en cuanto a garantías de autentificación en función del contexto. Hay casos en que se necesitará un mayor o menor grado de autentificación en función de la sensibilidad y el valor de la información y las transacciones. En estos casos, las partes dependientes (por ejemplo, usuarios, PSId/NGN) necesitarán más detalles de los habituales (por ejemplo métodos de autentificación, número de factores de autentificación, contextos de autentificación, etc.) para lograr la garantía de autentificación esperada. Para ello es necesario evaluar los posibles riesgos asociados con las consecuencias que tendrían los errores de autentificación y determinar el justo nivel de garantía de la identidad de una entidad. Cuando los errores de autentificación tengan peores consecuencias potenciales, se necesitarán mayores niveles de garantía.

R-38 El PSId/NGN debe soportar los métodos de autentificación apropiados, dependiendo del nivel de garantía necesario.

R-39 La parte dependiente ha de poder indicar al PSId/NGN el nivel de garantía necesario para la autentificación de una entidad.

R-40 El PSId/NGN, la parte dependiente y la entidad que se autentifica han de poder negociar el nivel de garantía.

8.4.6.1 Garantía de la identidad e integridad del dispositivo de usuario

Las NGN soportarán diversos dispositivos de usuario (por ejemplo, teléfonos fijos, teléfonos inalámbricos, computadores personales, agendas digitales, descodificadores TVIP). Los componentes de hardware y software de los dispositivos anexos a las NGN van de simples a complejos y, de ser robados o puestos en peligro, pueden utilizarse para orquestar diversos ataques. Se reconoce que las NGN también requerirán dispositivos complementarios (tales como terminales "mudos" o dispositivos POTS), que son incapaces de proporcionar el grado de protección necesario.

R-41 El PSId/NGN ha de poder soportar dispositivos de usuario final con capacidades de seguridad y datos encriptados de gestión de identidad (por ejemplo, contraseñas, claves digitales y certificados) en los componentes de hardware a prueba de ataques.

R-42 El PSId/NGN ha de poder comunicar con las capacidades de seguridad de los componentes de hardware a prueba de ataques de un dispositivo de usuario final utilizando interfaces normalizadas a fin de soportar los servicios de aplicación de seguridad basados en componentes hardware a prueba de ataques para identificar unívocamente y garantizar la identidad del dispositivo de usuario final.

Las aplicaciones que se ejecutan en los dispositivos de abonado para permitirles interactuar con los servicios y características de dispositivo locales pueden poner en peligro la integridad del dispositivo. Algunas aplicaciones de Internet populares, como los navegadores web y el correo electrónico, también pueden alterar la integridad de los dispositivos de abonado. Las descargas de software y ficheros, en especial si proceden de fuentes no fiables, exponen los dispositivos de abonado a códigos malignos, gusanos, virus y caballos de Troya. Podría diseñarse e incorporarse a los dispositivos de usuario final un componente de hardware especializado resistente a los ataques para verificar la integridad del dispositivo. Por ejemplo, este componente de hardware especializado resistente a los ataques podría contener algoritmos y funciones específicos del fabricante para realizar verificaciones de integridad. El componente de hardware especial podría incluir un modelo de referencia con una serie de valores de integridad, que se sabe son adecuados, para identificar el código correcto y facilitar valores de referencia para el dispositivo. Los valores de integridad definidos se compararán con los valores reales de la configuración a fin de determinar si la unidad se ajusta a las normas definidas.

R-43 El PSId/NGN ha de poder soportar dispositivos de usuario final con componentes de hardware especializados resistentes a los ataques a fin de realizar verificaciones de integridad y confirmar la adecuada integridad a las aplicaciones y servicios.

R-44 El PSId/NGN ha de poder comunicar con las capacidades de seguridad del componente de hardware resistente a los ataques de los dispositivos de usuario final a través de interfaces normalizadas que soporte los servicios de aplicación de seguridad dependientes de las verificaciones de integridad y la confirmación de la integridad de los dispositivos.

La pérdida o el robo de un dispositivo con IIP y otros datos sensibles podría acarrear serias consecuencias para los particulares, las empresas privadas y las públicas. El componente de hardware especializado diseñado para identificar unívocamente y confirmar la integridad de los dispositivos fiables también podría soportar capacidades de encriptación y protección de la IIP y otros datos sensibles en los dispositivos de usuario final.

R-45 El PSId/NGN ha de poder soportar dispositivos de usuario final con componentes de hardware especializados resistentes a los ataques para encriptar y proteger la IIP y otros datos sensible en los dispositivos de usuario final.

8.4.7 Soporte de servicios que requieren prioridad

Los sistemas y capacidades de GId de las NGN deben dar soporte a servicios de aplicación y sesiones de comunicación que requieren prioridad con respecto a otros servicios. En [UIT-T Y.2205] se describen las telecomunicaciones de emergencia (TE) que necesitan un trato especial en las NGN. Como ejemplo específico puede citarse el servicio de telecomunicaciones de emergencia (STE) definido en [UIT-T E.107]. El STE aprovecha las capacidades de GId utilizadas para los servicios ordinarios (por ejemplo, garantía de identidad y descubrimiento de identidades fiables). Por consiguiente, los sistemas de GId deben soportar las funciones y capacidades necesarias para reconocer y dar prioridad al establecimiento y mantenimiento de una llamada/sesión del STE, de conformidad con las normas y políticas nacionales aplicables. En [UIT-T E.107] y [UIT-T Y.2205] puede encontrarse información sobre los servicios y capacidades que requieren prioridad.

R-46 Los sistemas de GId del PSId/NGN deben soportar las funciones y capacidades necesarias para reconocer y dar prioridad al establecimiento y mantenimiento de una llamada/sesión del STE, de conformidad con las normas y políticas nacionales aplicables.

R-47 Los elementos de red y bases de datos de GId utilizadas para soportar las llamadas/sesiones del STE han de otorgar prioridad de conformidad con las normas y políticas nacionales aplicables, lo que incluyen, aunque no únicamente:

- Las comunicaciones de GId intrarred (por ejemplo, interacciones con un sistema GId de proveedor NGN).

- Las comunicaciones de GId entre redes (por ejemplo, interacciones entre dos sistemas de proveedor NGN basadas en acuerdos bilaterales y políticas).
- Las comunicaciones de GId federadas (por ejemplo, interacciones entre los miembros de las federaciones basadas en las reglas y políticas de identidad de la federación aplicables).

Véanse en el apéndice III ejemplos de casos de uso relacionados con el STE.

8.5 Funciones de identidad federadas de gestión de identidad

La federación conlleva el establecimiento de una relación entre dos o más entidades o la creación de una asociación que comprende cualquier número de proveedores de servicio y proveedores de servicios de identidad. El concepto general de federación supone permitir que cada uno de sus miembros permanece independiente al tiempo que facilita la compartición de información de identidad específica que permite la prestación de servicios federados. Por ejemplo, cierta información de identidad de un usuario/abonado (por ejemplo, subconjunto de un perfil de abonado) puede estar federada (es decir, disponible para los miembros de la federación) de acuerdo con las políticas y condiciones de la federación y los reglamentos y políticas de protección de datos. La identidad federada permite la portabilidad y transmisión de información de identidad a través de dominios de seguridad autónomos de acuerdo con las políticas y condiciones de la federación y con sujeción a las normas, reglamentos y políticas aplicables. La identidad federada permite a los usuarios de un dominio acceder de manera segura a los datos o sistemas de otro dominio sin redundancia en la administración de usuarios.

R-48 Los miembros de una federación han de poder descubrir e intercambiar información de identidad federada, de conformidad con las normas, reglamentos y políticas aplicables.

R-49 El PSId/NGN debe soportar capacidades que permitan a un abonado facilitar la autorización necesaria para federar sus identidades.

R-50 El PSId/NGN debe soportar capacidades para dar al abonado la opción de poner término a su participación en todos o algunos servicios y aplicaciones de identidad federados y terminar la federación de sus identidades.

R-51 El PSId/NGN debe soportar capacidades que permitan al abonado definir permisos y prohibiciones en relación con su información de identidad federada. Los abonados han de poder controlar qué datos personales se dan a quién y para qué fines.

NOTA – Los requisitos de protección de la IIP estipulados en la cláusula 8.6 son igualmente aplicables a las identidades federadas.

En general, cada proveedor NGN, empresa o miembro de una federación dispondrá de sus propios formatos, esquemas, definiciones o semántica para representar y compartir la información y los datos de identidad. Por ejemplo, la misma información, como la fecha de nacimiento, puede representarse de manera diferente en dos sistemas distintos. Asimismo, la semántica, los esquemas, las tecnologías y los mecanismos utilizados para representar, solicitar e intercambiar información de identidad pueden ser diferentes, lo que puede dar origen a problemas de compatibilidad. Por consiguiente, será necesario contar con las capacidades adecuadas que permitan la vinculación y la compatibilidad entre federaciones fiables.

R-52 Ha de ser posible la vinculación y la compatibilidad entre federaciones fiables que utilizan sistemas de GId, semántica, esquemas, mecanismos y tecnologías diferentes. Por ejemplo, las partes dependientes en distintos dominios (por ejemplo, dominio NGN y servicios web/Internet), que utilizan diferentes tecnologías y capacidades GId, han de poder interfuncionar y ser compatibles. En concreto, se ha de garantizar la transmisión segura de la información de identidad federada.

8.6 Funciones de usuario/abonado y protección de la IIP

Los usuarios finales/abonados han de disponer de interfaces intuitivas y capacidades para controlar su IIP y poseer la información necesaria para poder tomar decisiones relativas a sus datos personales. Los usuarios finales/abonados han de poder expresar sus políticas y preferencias en cuanto a la privacidad y negociar los términos de divulgación de sus datos con el PSId/NGN.

Sólo se divulgarán datos personales a las entidades autorizadas de conformidad con las políticas aplicables (por ejemplo, consentimiento del usuario/abonado, normas reglamentarias estatales). Además, se recopilará, almacenará y utilizará la IIP lo menos posible y respetando las políticas aplicables.

R-53 El PSId/NGN debe proporcionar servicios GId y proteger la confidencialidad de la IIP con arreglo a los reglamentos, políticas y normas aplicables.

R-54 Los usuarios finales/abonados habrán de tener la posibilidad de comunicar al PSId/NGN sus preferencias en cuanto a sus datos personales (por ejemplo, preferencias de privacidad definidas), de acuerdo con los reglamentos y políticas aplicables (por ejemplo, consentimiento expreso de los particulares, políticas del proveedor o normativa).

R-55 Los usuarios finales/abonados han de poder verificar la autenticidad de la entidad que solicita la IIP, antes de facilitar la información solicitada.

R-56 El PSId/NGN debe suprimir la IIP cuando se hayan cumplido los objetivos específicos para los que se recabaron y almacenaron los datos, de conformidad con los reglamentos, políticas y normas aplicables.

R-57 Los usuarios finales/abonados han de poder mantener su anonimato o emplear un pseudónimo, en función del contexto de aplicación y de conformidad con los reglamentos, políticas y normas aplicables.

8.7 Seguridad

La información y los datos de identidad son muy sensibles y objetivo de intrusos. Del mismo modo, dado que los servicios y capacidades de GId se utilizarán para controlar el acceso a las aplicaciones de interconexión de redes empresariales, estatales y sociales, los elementos y sistemas de red (por ejemplo, elementos y bases de datos de la red que soportan las funciones y capacidades de GId) serán objeto de ataques de seguridad e intrusiones. Por consiguiente, han de aplicarse medidas de seguridad apropiadas para asegurar y proteger los elementos y sistemas de la red donde residen las funciones, servicios y capacidades de GId.

8.7.1 Control de acceso a sistemas y datos

El control de acceso al sistema conlleva medidas de seguridad para impedir el acceso no autorizado a elementos y sistemas de la red y a sus correspondientes puntos de acceso. El acceso no autorizado a los elementos y sistemas de la red que soportan las funciones, capacidades y datos de GId puede representar varias amenazas. Por consiguiente, se han de implantar y aplicar las adecuadas medidas de control de acceso para evitar el acceso no autorizado.

R-58 El PSId/NGN debe soportar y aplicar medidas de control de acceso a sistemas para evitar el acceso no autorizado a los elementos y sistemas de la red que soportan las funciones y capacidades de GId. El PSId/NGN no permitirá a ninguna entidad acceder a los elementos y bases de datos de la red que soportan las funciones y capacidades de GId a menos que la entidad se haya identificado, autentificado y autorizado. Este requisito se aplica a todas las entidades (es decir, personas físicas, procesos y sistemas distantes).

El control de acceso a datos conlleva medidas de seguridad para impedir el acceso no autorizado a los datos almacenados o configurados y a los datos en tránsito. El acceso no autorizado a los datos de GId configurados o almacenados puede representar varias amenazas. Por consiguiente, se han de implantar y aplicar las adecuadas medidas de control de acceso para evitar el acceso no autorizado.

R-59 El PSId/NGN debe soportar y aplicar medidas de control de acceso para evitar el acceso no autorizado a los datos de GId, lo que comprende cualquier dato de identidad almacenado o configurado en las bases de datos de GId, los servidores de aplicación, los servidores de abonado residenciales (HSS), o cualquier otro elemento de la red. El PSId/NGN no permitirá a ninguna entidad acceder a los datos de GId a menos que la entidad se haya identificado, autentificado y autorizado. Este requisito se aplica a todas las entidades (es decir, personas físicas, procesos y sistemas distantes).

8.7.2 Integridad de sistemas y datos

Los elementos de red, los sistemas y las funciones que soportan los servicios y capacidades de GId han de contar con protección de la integridad, lo que incluye las bases de datos y servidores de aplicación de GId.

R-60 El PSId/NGN debe proteger la integridad de todos los elementos de red, sistemas y funciones que soportan los servicios y capacidades de GId.

La información y los datos de identidad almacenados han de contar con protección de la integridad a fin de evitar la corrupción o manipulación de los datos que pueda poner en peligro la integridad.

R-61 El PSId/NGN debe proteger la integridad de los datos configurados de GId.

R-62 El PSId/NGN debe proteger la integridad de la distribución, comunicación, actualización o modificación de los datos y de los datos fuera de línea asociados con la GId.

8.7.3 Confidencialidad de los datos

R-63 El PSId/NGN debe soportar y aplicar medidas de protección de los datos de GId configurados contra su observación por parte de entidades no autorizadas (por ejemplo, elementos internos no autorizados).

R-64 El PSId/NGN debe soportar y aplicar medidas de protección de la distribución, comunicación actualización o modificación de los datos de GId y de los datos fuera de línea de GId contra su observación por parte de entidades no autorizadas (por ejemplo, elementos internos no autorizados).

8.7.4 Protección de seguridad de las comunicaciones de GId

Las comunicaciones de GId (señalización y medios) han de estar protegidas contra el acceso no autorizado, la corrupción, la manipulación y la intercepción (por ejemplo, escuchas ilegales).

R-65 El PSId/NGN debe proteger la integridad y la confidencialidad de las comunicaciones de GId dentro de la red y entre redes. Todo el tráfico de señalización y medios relacionado con la GId que atraviese una interfaz red-red (NNI), una interfaz aplicación-red (ANI) o una interfaz servidor-red (SNI) entre dominios de red deberá contar con protección de la integridad.

8.7.5 Seguridad de gestión

Se ha de asegurar y proteger el acceso de gestión a los elementos de red NGN y a los datos configurados contra el acceso y los controles no autorizados.

R-66 El PSId/NGN debe impedir el acceso no autorizado a las interfaces y controles de gestión de los elementos de red y las entidades funcionales que soportan la GId.

El tráfico de gestión ha de estar asegurado y protegido contra la corrupción, la manipulación y la observación no autorizada.

R-67 El PSId/NGN debe proteger la integridad y la confidencialidad del tráfico de gestión asociado con el soporte de la GId.

8.7.6 Registros de seguridad y auditoría

Es necesario contar con registros de seguridad y de auditoría a fin de registrar los eventos que puedan servir para una investigación *a posteriori* de determinadas actividades.

R-68 El PSId/NGN debe generar registros de seguridad a fin de registrar eventos que puedan servir para una investigación *a posteriori* de determinadas actividades (por ejemplo, inscripciones, modificación de datos y recursos de sistema críticos, acceso de gestión a parámetros y recursos NGN configurados) relacionadas con el soporte de la GId.

8.7.7 Protección contra los ataques de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)

Los servicios y capacidades de GId han de tener una gran disponibilidad, por lo que han de estar protegidos contra las amenazas DoS y DDoS, que pueden afectar a su disponibilidad.

R-69 El PSId/NGN debe dar protección contra los ataques DoS, DDoS y de otro tipo que pueden afectar a la disponibilidad de los servicios y capacidades de GId, lo que incluye el soporte y utilización de las capacidades y herramientas adecuadas para detectar, aislar y paliar los ataques DoS y DDoS y de otro tipo.

8.7.8 Supervisión y detección de intrusión

R-70 El PSId/NGN debe soportar y utilizar herramientas de supervisión de seguridad y detección de intrusión, según proceda, a fin de detectar el fraude, abuso e intrusión en los elementos de red y sistemas de GId.

Apéndice I

Casos generales de utilización de la GId

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

I.1 Introducción

En este apéndice se presentan los casos generales de utilización de la GId por parte de los gobiernos, las empresas privadas y los usuarios finales/abonados.

I.2 Gobiernos

Los gobiernos pueden utilizar las capacidades de GId para mejorar y soportar aplicaciones y transacciones entre las empresas públicas y los ciudadanos, entre distintas organizaciones y agencias estatales (servicios públicos federados), y entre distintos gobiernos (por ejemplo, servicios federados entre gobiernos). Como ejemplo de los casos de utilización por parte de los gobiernos se pueden citar:

- Garantía de identificación de ciudadanos: el gobierno puede utilizar la GId para validar la identidad de los ciudadanos que van a recibir servicios estatales electrónicos, al tiempo que se mejora la protección de la IIP. La asistencia sanitaria puede ser ejemplo de ello, pues la sensibilidad de la información relacionada con la salud subraya la importancia de minimizar los datos y, más generalmente, la necesidad de seguridad y privacidad de la información de identidad.
- Garantía de identificación de funcionarios estatales para los servicios estatales federados: las empresas públicas pueden utilizar capacidades de GId para hallar soluciones comunes de identificación segura y fiable de los funcionarios a fin de mejorar la seguridad y la eficiencia, reducir los fraudes de identidad y proteger la privacidad personal.
- Mejora y soporte de servicios federados entre distintos gobiernos: la GId se puede utilizar para mejorar y soportar los servicios federados entre distintos gobiernos. Por ejemplo, los gobiernos pueden colaborar para hallar soluciones de GId mejoradas que comprendan la seguridad, la privacidad y la experiencia de usuario aplicables a los ciudadanos que viajen de un país a otro.

I.3 Empresas privadas

La GId se puede utilizar para ayudar a las empresas a mejorar y soportar nuevos negocios, así como los ya existentes, al tiempo que se mejora la seguridad, la privacidad y la protección de la IIP. Como ejemplo de los casos de utilización por parte de las empresas privadas se pueden citar:

- Servicios de identidad federados: se puede utilizar la GId para soportar servicios de inicio y término de sesión únicos para múltiples socios comerciales (incluidos los proveedores NGN, de servicios web, de contenido y terceros).
- Servicios de comunicación: los proveedores NGN pueden utilizar la GId para que los usuarios/abonados puedan disfrutar de servicios de aplicación en diferentes plataformas (por ejemplo, redes IP gestionadas, Internet y plataformas móviles) y permitir a los usuarios acceder a las aplicaciones que escojan a través de múltiples plataformas por medios que se ajustan a sus preferencias.
- Aplicaciones y transacciones financieras electrónicas: se puede utilizar la GId para mejorar y soportar aplicaciones de pago electrónico para las transacciones de comercio electrónico.

I.4 Usuarios extremos/abonados

Los usuarios finales/abonados pueden utilizar la GId para mejorar la experiencia y control de la IIP. Como ejemplo de los casos de utilización por parte de los usuarios finales/abonados se pueden citar:

- Control de la IIP por parte del usuario: se puede utilizar la GId para mejorar la experiencia de usuario y permitir el control de la IIP. Los particulares pueden utilizar múltiples pseudónimos para participar en diferentes actividades como los canales de noticias, la publicación de blogs, la gestión de las redes sociales y el intercambio de fotografías o música. La GId puede ofrecer a los particulares más opciones de participación en distintas comunidades y de determinar en qué grado quieren vincular aspectos de sus diferentes identidades (es decir control de su IIP).
- Redes sociales: se puede utilizar la GId para mejorar y soportar aplicaciones de redes sociales ofreciendo las herramientas necesarias para que el usuario controle efectivamente la IIP y asuma su responsabilidad al respecto.

Apéndice II

Casos de utilización de GId para las aplicaciones NGN

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

II.1 Introducción

En este apéndice se presentan ejemplos de casos de utilización de la gestión de identidad (GId) en las NGN. Estos ejemplos se pueden utilizar como base para elaborar los requisitos de GId en las NGN.

II.2 Caso de utilización básico

En la figura II.1 se muestra un ejemplo de caso de utilización básico en el que participan tres elementos. Aparte de este ejemplo básico, existen otros casos posibles de utilización, como los que figuran en el apéndice V (por ejemplo, casos centrados en el usuario).

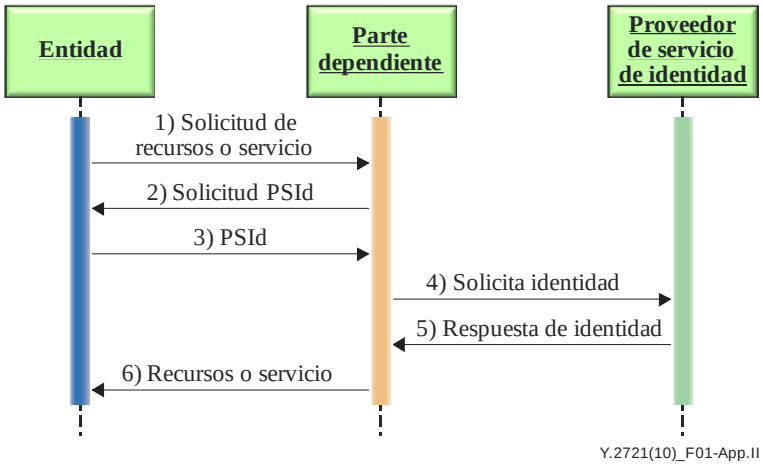


Figura II.1 – Caso de utilización básico

Los tres elementos son una entidad (una parte aseverante o principal) que desea obtener servicios de una parte dependiente (que puede ser una red o una aplicación) y que obtiene una aseveración de identidad, incluidas las aseveraciones anónimas o pseudónimas, de un proveedor de servicio de identidad (PSId) de acuerdo con la política de confianza y de seguridad.

En la figura II.1, se muestran los siguientes flujos de información de GId de alto nivel.

1) La entidad presenta la identidad declarada a la parte dependiente (el proveedor de recursos o servicios) y solicita un recurso o un servicio a esa parte dependiente.
2) La parte dependiente (la red o la aplicación) necesita autentificar la identidad declarada de la entidad antes de facilitar los recursos o servicios solicitados. Para la autentificación, la parte dependiente necesita información procedente del PSId adecuado, que ha de determinarse y con el que hay que entrar en contacto. La parte dependiente devuelve una "solicitud de información de PSId" a la entidad, pidiéndole que facilite el nombre del PSId correspondiente.
3) La entidad responde a esta "Solicitud de información de PSId" identificando al PSId correspondiente ante la parte dependiente. La entidad puede identificar a múltiples PSId.
4) La parte dependiente, a su vez, pide al PSId que valide la identidad declarada de la entidad con un nivel de confianza suficiente (nivel de garantía), según las necesidades.

5) El PSId confirma la identidad declarada de la entidad. Las funciones de PSId pueden comprender la delegación (lo que supone que el PSId puede delegar todos o algunos aspectos del proceso de autentificación en otros PSId transmitiéndoles la aseveración de identidad). La parte dependiente puede presentar al PSId más solicitudes en caso de necesitar un mayor nivel de garantía de autentificación u otras capacidades específicas.

6) La parte dependiente, una vez recibida del PSId la validación de la identidad declarada de la entidad, facilita el recurso o servicio solicitado.

Es posible combinar estos tres elementos (entidad, parte dependiente y PSId) los medios subyacentes no son relevantes. El único requisito es que estos mecanismos de comunicación estén "bien estructurados" con sintaxis y perfiles conocidos o que las partes involucradas puedan obtener, si disponen de los necesarios permisos para utilizar los mecanismos. Cuando proceda, se utilizarán mecanismos normalizados para lograr una compatibilidad global fiable.

Además, puede haber otros flujos de información de GId de alto nivel. Por ejemplo:

1) Una parte dependiente puede solicitar directamente a la entidad las credenciales de autentificación.

2) La entidad puede facilitar sus credenciales de autentificación a un PSId fiable.

3) El PSId puede validar las credenciales obtenidas de la entidad y, a continuación, generar nuevas credenciales para la entidad a fin de satisfacer la solicitud de autentificación de la parte dependiente.

4) La entidad (o su delegado) puede obtener del PSId las credenciales generadas y entregárselas a la parte dependiente.

5) Las credenciales generadas que la entidad envía a la parte dependiente pueden contener 1) una copia de las declaraciones de identidad generadas por el PSId, o 2) una referencia a las mismas.

Por otra parte, la entidad puede optar por no facilitar a la parte dependiente las credenciales de autentificación generadas por el PSId.

También es posible que haya una jerarquía de proveedores de servicios de identidad o una jerarquía de partes dependientes, así como que una entidad tenga más de un delegado.

II.3 Utilización de un sistema de GId común para el soporte de múltiples servicios de aplicación (por ejemplo, voz, datos, TVIP) en una red de proveedor de servicio

II.3.1 Aspectos generales

Los proveedores de red/servicio (por ejemplo, los proveedores NGN) soportarán y serán anfitriones de múltiples aplicaciones y servicios. Por su naturaleza distribuida, el entorno NGN permite que haya distintos servicios de aplicación en diferentes elementos de red y plataformas específicas del fabricante (por ejemplo, VoIP, datos y TVIP). Cada servicio dispondrá de sus propios medios, tecnológicos o definidos por el fabricante, para controlar el acceso y éstos no tienen por qué ser compatibles entre ellos, por lo que deberán configurarse, gestionarse y utilizarse por separado.

Pueden lograrse mayores beneficios en términos de eficacia comercial y de costes si se adopta un método de infraestructura de GId común que permita utilizar múltiples aplicaciones/servicios. Este método también permitiría a los creadores de aplicaciones utilizar habilitadores comunes para la GId, en lugar de que cada aplicación/servicio soporte funciones de GId específicas (por ejemplo, capacidades y mecanismos de control de acceso del fabricante), y seguir un proceso eficaz para el diseño, la aplicación y la oferta de servicios de aplicación. Además, este método común puede ayudar a gestionar los riesgos de seguridad de cada servicio de aplicación y de la infraestructura de red en su conjunto.

El método de GId para las NGN comprenderá soluciones para dentro de la red (es decir, soluciones en el dominio de proveedor NGN) y soluciones entre redes (es decir, entre diferentes proveedores NGN, incluidos los proveedores terceros). En el caso dentro de la red, esto puede comprender métodos que permitan la interacción entre diferentes elementos o componentes de red dentro de un dominio de proveedor NGN para la GId (por ejemplo, declarantes, sistemas dependientes y sistemas de identidad). Las soluciones entre redes pueden incluir la especificación de métodos que permitan la interacción entre entidades elementos de red en diferentes dominios NGN para la GId (por ejemplo, declarantes, partes dependientes y PSId).

NOTA – Un proveedor NGN también puede actuar de PSId.

II.3.2 Descripción del caso de utilización

En este ejemplo se muestra cómo múltiples servicios de aplicación (por ejemplo, VoIP, datos y TVIP) utilizan una infraestructura de gestión de identidad común para el control de acceso y la protección de seguridad del servicio de aplicación. En este caso interactúan las siguientes entidades:

- Usuarios extremos (es decir, usuario final y/o dispositivo de usuario final).
- Sistema dependiente (es decir, servicio de aplicación o sistema de red).
- Sistema de GId (es decir, sistema de red que ofrece servicios de GId, como el registro, la autentificación y la autorización, la información de perfil de abono).

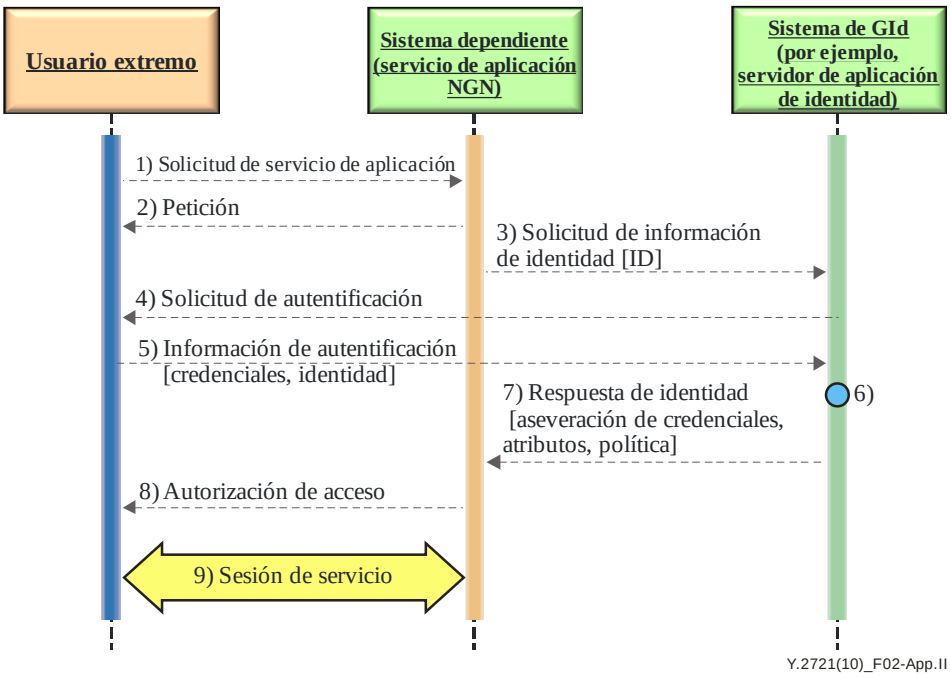


Figura II.2 – Caso de utilización básico

En la figura II.2 se muestra un caso básico en que un servicio de aplicación utiliza los servicios de un sistema de GId externo o independiente del servicio de aplicación para controlar el acceso y gestionar los privilegios. Los flujos de llamada de este ejemplo son:

1) Solicitud de servicio de aplicación: Este flujo de información representa la solicitud del usuario final para invocar el servicio de aplicación.
2) Petición: El servicio de aplicación envía una respuesta impidiendo el acceso de usuario.
3) Solicitud de información de identidad [ID de usuario]: El servicio de aplicación envía al sistema de GId una solicitud para que asevere la identidad de usuario y facilite los atributos asociados con el ID de usuario. Puede incluirse aquí información como el perfil de servicio,

los privilegios, las preferencias y la información de política, por ejemplo, cualquier política o restricción asociada con la identidad.

4) Solicitud de autentificación: El sistema de GId envía al usuario una solicitud de autentificación.

5) Información de autentificación [credenciales]: El usuario facilita información para la autentificación (por ejemplo, ID de usuario y contraseña o número de identificación personal).

6) Autentificación: El sistema de GId realiza la autentificación y obtiene otra información necesaria, lo que puede conllevar la obtención de información procedente de otros sistemas de la red (por ejemplo, HSS).

7) Respuesta de información de identidad [aseveración de credenciales, atributos, política]: El sistema de GId facilita información aseverando las credenciales. Pueden también incluirse los atributos asociados con el ID de usuario (por ejemplo, privilegios y preferencias) y la política asociada a la información de identidad (por ejemplo, cualquier restricción impuesta a la utilización, visualización y divulgación).

8) Autorización de acceso: El servicio de aplicación indica al usuario que se le concede acceso al servicio.

9) Sesión de servicio de aplicación: Este flujo de información representa el satisfactorio establecimiento de una sesión del servicio de aplicación para el usuario.

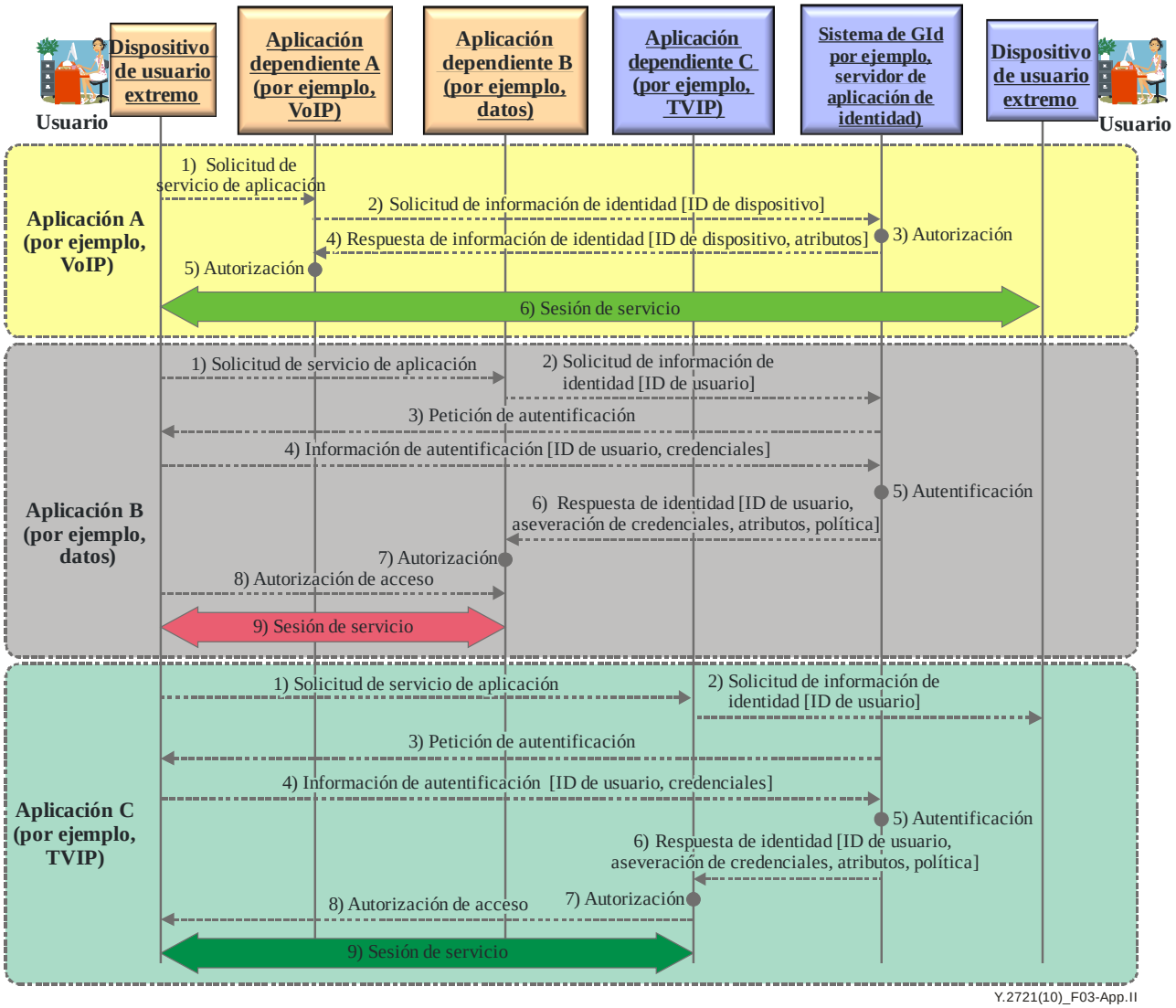


Figura II.3 – Utilización de una infraestructura de GId común para múltiples servicios de aplicación

En la figura II.3 se muestra un ejemplo de utilización cuando múltiples servicios de aplicación (por ejemplo, VoIP, datos y TVIP) utilizan un sistema de GId común externo e independiente de los servicios de aplicación. En este ejemplo se asume que el dispositivo de usuario final está registrado y se comunica con el proveedor de servicio utilizando los procedimientos corrientes.

En el ejemplo, los flujos de información de la aplicación A (VoIP) son los siguientes:

1) Solicitud de servicio de aplicación: Este flujo de información representa el inicio de llamada por parte del usuario final.

2) Solicitud de información de identidad [ID de dispositivo]: El servicio de aplicación envía al sistema de GId una solicitud para que verifique si el dispositivo de usuario final está autorizado para el servicio VoIP. En este ejemplo se asume que el servicio VoIP se basa en el perfil de abono del dispositivo de usuario o de la línea (por ejemplo, abono xDSL).

3) Autorización: El sistema de GId determina si el usuario final está autorizado para el servicio VoIP.

NOTA 1 – Se asume que para ello se extrae la información de perfil de abono del dispositivo de usuario final o la línea (por ejemplo, xDSL). También se asume para el servicio VoIP no es necesario autentificar al usuario final.

4) Respuesta de información de identidad [ID de dispositivo, atributos]: El sistema de GId facilita los atributos asociados con el ID de dispositivo (es decir, si el dispositivo está autorizado para el servicio VoIP), lo que puede incluir la información pertinente obtenida del perfil de abono (por ejemplo, privilegios y preferencias).

5) Autorización de acceso: El servicio de aplicación indica al usuario que puede acceder al servicio.

6) Sesión de servicio de aplicación: Este flujo de información representa la sesión de llamada del usuario.

En el ejemplo, los flujos de información de la aplicación B (datos) son los siguientes:

1) Solicitud de servicio de aplicación: Este flujo de información representa la solicitud del usuario final para invocar el servicio de aplicación.

2) Solicitud de información de identidad [ID de usuario]: El servicio de aplicación envía al sistema de GId una solicitud para que asevere la identidad del usuario y facilite los atributos asociados con el ID de usuario, lo que puede incluir información como el perfil del servicio, los privilegios, las preferencias y la política, por ejemplo, cualquier política o restricción asociada con la identidad.

3) Petición de autentificación: El sistema de GId envía al usuario una solicitud de autentificación.

4) Información de autentificación [credenciales]: El usuario facilita información para la autentificación (por ejemplo ID de usuario y contraseña o número de identificación personal).

5) Autentificación: El sistema de GId realiza la autentificación y obtiene otra información necesaria, que puede suponer la obtención de información procedente de otros sistemas de la red (por ejemplo, HSS u otras bases de datos de abono).

6) Respuesta de información de identidad [aseveración de credenciales, atributos, política]: El sistema de GId facilita información aseverando las credenciales. Se pueden incluir además los atributos asociados con el ID de usuario (por ejemplo privilegios y preferencias) y la política asociada con la información de identidad (por ejemplo, restricciones relativas a la utilización, la visualización y la divulgación).

7) Autorización: El servicio de aplicación procesa la información y determina que el usuario está autorizado para el servicio.

8) Autorización de acceso: El servicio de aplicación indica al usuario que puede acceder al servicio.

9) Sesión de servicio de aplicación: Este flujo de información representa el satisfactorio establecimiento de una sesión del servicio de aplicación para el usuario.

En el ejemplo, los flujos de llamada de la aplicación C (TVIP) son los siguientes:

1) Solicitud de servicio de aplicación: Este flujo de información representa la solicitud del usuario final para invocar el servicio de aplicación.

2) Solicitud de información de identidad [ID de usuario]: El servicio de aplicación envía al sistema de GId una solicitud para que asevere la identidad de usuario y facilite los atributos asociados con el ID de usuario, lo que puede incluir información como el perfil del servicio, los privilegios, las preferencias y la política. Por ejemplo, toda política o restricción asociada con la identidad.

3) Petición de autentificación: El sistema de GId envía al usuario una solicitud de autentificación.

4) Información de autentificación [credenciales]: El usuario facilita información para la autentificación (por ejemplo, ID de usuario y contraseña o número de identificación personal).

5) Autentificación: El sistema de GId realiza la autentificación y obtiene otra información necesaria, lo que puede suponer la obtención de información procedente de otros sistemas de la red (por ejemplo, HSS u otras bases de datos de abono).

6) Respuesta de información de identidad [aseveración de credenciales, atributos, política]: El sistema de GId facilita información aseverando las credenciales. Pueden incluirse también los atributos asociados con el ID de usuario (por ejemplo privilegios y preferencias) y la política asociada con la información de identidad (por ejemplo, restricciones relativas a la utilización, la visualización y la divulgación).

7) Autorización: El servicio de aplicación procesa la información y determina que el usuario está autorizado para el servicio.

8) Autorización de acceso: El servicio de aplicación indica al usuario que puede acceder al servicio.

9) Sesión de servicio de aplicación: Este flujo de información representa el satisfactorio establecimiento de una sesión del servicio de aplicación para el usuario.

NOTA 2 – Para poder efectuar la autentificación mutua (es decir, autentificar al proveedor de servicio o aplicación), se requerirán funcionalidades y flujos adicionales, que no se muestran en la figura II.3.

II.3.3 Requisitos implícitos

En este ejemplo están implícitos los siguientes requisitos:

- Las NGN soportarán una infraestructura de GId común que utilizarán múltiples aplicaciones y servicios independientemente de cuál sea la plataforma de aplicación o la opción del fabricante.
- No deberán utilizarse funciones GId comunes, si éstas contravienen los principios de limitación de la recopilación de datos, minimización de datos, separación de datos, especificación de la finalidad y uso limitado.
- Las NGN soportarán la utilización de un método normalizado y estructurado que permita a los servicios de aplicación descubrir los sistemas de GId e intercambiar datos de manera segura.

II.4 Inicio/término de sesión único para múltiples servicios de aplicación (por ejemplo, voz, datos y TVIP) en una red de proveedor de servicio

II.4.1 Aspectos generales

Los usuarios normalmente han de iniciar una sesión en múltiples sistemas anfitriones de servicios de aplicación (por ejemplo, VoIP, datos y TVIP), lo que conlleva un número equivalente de diálogos de inicio de sesión en cada uno de los cuales se pueden utilizar diferentes nombres de usuario e información de autentificación. Los administradores de sistema se encuentran que tienen que gestionar las cuentas de usuario en cada uno de los múltiples sistemas a que se quiere acceder de manera coordinada a fin de mantener la integridad de la política de seguridad.

Los abonados usuarios finales piden características de fácil utilización, como el "inicio/término de sesión único". El principio del "inicio de sesión único" es que un usuario final, un dispositivo o una combinación de usuario final y dispositivo puedan iniciar sólo una sesión (es decir, presentando la información de credenciales para la autentificación y la autorización) con un servicio en una red de la próxima generación (NGN) y, como resultado, queden autentificados para uno o más servicios adicionales de la misma NGN (es decir, el usuario final no tiene que realizar la autentificación para cada servicio). En este contexto, "inicio de sesión" equivale a "inscripción" o "registro", en los casos en que el usuario final/dispositivo "se registra en" o "se inscribe en" un servicio. Del mismo

modo, el "término de sesión único" permite no tener que terminar las sesiones de los servicios de aplicación una por una.

Beneficios que reportan los servicios de inicio/terminación de sesión únicos:

- Reducción del tiempo que invierten los usuarios en iniciar una sesión en cada dominio, y reducción de la posibilidad de fallo de esas operaciones.
- Mejora de la seguridad al reducirse la necesidad de que el usuario maneje y recuerde diversas informaciones de autentificación.
- Reducción del tiempo que invierten los administradores de sistema en añadir y eliminar usuarios del sistema o en modificar sus derechos de acceso, por lo que se mejora su capacidad de respuesta.
- Mejora de la seguridad al tener los administradores de sistema mayor capacidad de mantenimiento de la integridad de la configuración de la cuenta del usuario, incluida la capacidad de bloquear o eliminar el acceso de un único usuario a todos los recursos del sistema de manera coordinada y coherente.

II.4.2 Descripción del caso de utilización

En este ejemplo se muestra cómo se utiliza un sistema de GId para soportar el "inicio/término de sesión único" para múltiples servicios de aplicación (por ejemplo, VoIP, datos y TVIP) en un dominio de proveedor NGN. En este caso interactúan las siguientes entidades:

- Usuario extremo (es decir, usuario final y/o dispositivo de usuario final).
- Sistema dependiente (es decir, servicio de aplicación o sistema de red).
- Sistema de GId (es decir, sistema de red que ofrece servicios de GId como el registro, la autentificación y la autorización y la información de perfil de abono).

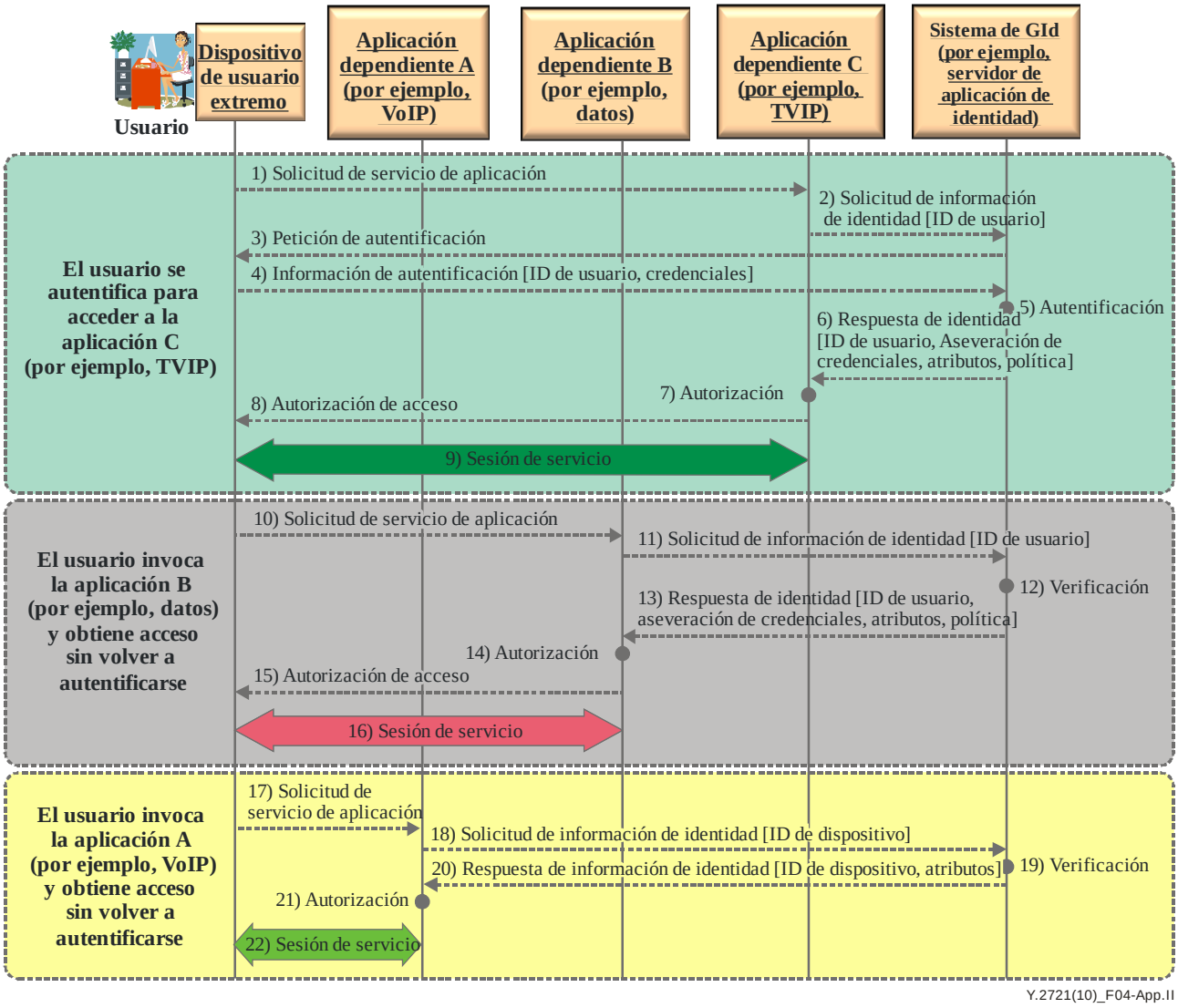


Figura II.4 – Inicio de sesión único

En la figura II.4 se muestra un ejemplo de abonado usuario final que utiliza el servicio de inicio de sesión único para acceder a múltiples servicios de aplicación (por ejemplo, VoIP, datos y TVIP). En este ejemplo se asume que el dispositivo de usuario final está registrado y se conecta al NGN utilizando los procedimientos corrientes.

En este ejemplo, los flujos de llamada son los siguientes:

1) Solicitud de servicio de aplicación: Este flujo de información representa la solicitud del usuario final para invocar el servicio de aplicación C (TVIP).

2) Solicitud de información de identidad [ID de usuario]: El servicio de aplicación C (TVIP) envía al sistema de GId una solicitud para que asevere la identidad de usuario y facilite los atributos asociados con el ID de usuario, lo que puede incluir información como el perfil de servicio, los privilegios, las preferencias y la política. Por ejemplo, las políticas o restricciones asociadas con la identidad.

3) Petición de autentificación: El sistema de GId pide al usuario que se autentifique.

4) Información de autentificación [credenciales]: El usuario facilita información para la autentificación (por ejemplo, ID de usuario y contraseña o número de identificación personal).

5) Autentificación: El sistema de GId realiza la autentificación y obtiene otra información necesaria, lo que puede suponer la obtención de información procedente de otros sistemas de la red (por ejemplo, HSS u otras bases de datos de abono).

6) Respuesta de información de identidad [aseveración de credenciales, atributos, política]: El sistema de GId facilita información aseverando las credenciales. Se pueden incluir también los atributos asociados con el ID de usuario (por ejemplo privilegios y preferencias) y la política asociada con la información de identidad (por ejemplo, restricciones relativas a la utilización, la visualización y la divulgación).

7) Autorización: El servicio de aplicación C (TVIP) procesa la información y determina que el usuario está autorizado para el servicio.

8) Autorización de acceso: El servicio de aplicación C (TVIP) indica al usuario que puede acceder al servicio.

9) Sesión de servicio de aplicación: Este flujo de información representa el satisfactorio establecimiento de una sesión del servicio de aplicación C (TVIP) para el usuario.

10) Solicitud de servicio de aplicación: Este flujo de información representa la solicitud del usuario para invocar el servicio de aplicación B (datos).

11) Solicitud de información de identidad [ID de usuario]: El servicio de aplicación B (datos) envía al sistema de GId una solicitud para que asevere la identidad de usuario y facilite los atributos asociados con el ID de usuario, lo que puede incluir información como el perfil de servicio, los privilegios, las preferencias y la política. Por ejemplo, las políticas o restricciones asociadas con la identidad.

12) Verificación: El sistema de GId procesa la solicitud, determina que el inicio de sesión único es aplicable y verifica que la autentificación del usuario sigue siendo válida.

13) Respuesta de información de identidad [aseveración de credenciales, atributos, política]: El sistema de GId facilita información aseverando las credenciales. Se pueden incluir también los atributos asociados con el ID de usuario (por ejemplo privilegios y preferencias) y la política asociada con la información de identidad (por ejemplo, restricciones relativas a la utilización, la visualización y la divulgación).

14) Autorización: El servicio de aplicación B (datos) procesa la información y determina que el usuario está autorizado para el servicio.

15) Autorización de acceso: El servicio de aplicación B (datos) indica al usuario que puede acceder al servicio.

16) Sesión de servicio de aplicación: Este flujo de información representa el satisfactorio establecimiento de una sesión del servicio de aplicación B (datos) para el usuario.

17) Solicitud de servicio de aplicación: Este flujo de información representa la solicitud del usuario para invocar el servicio de aplicación A (VoIP).

18) Solicitud de información de identidad [ID de dispositivo]: El servicio de aplicación A (VoIP) envía al sistema de GId una solicitud para que asevere la identidad del usuario y facilite los atributos asociados con el ID de dispositivo.

19) Verificación: El sistema de GId procesa la solicitud, determina que el inicio de sesión único es aplicable y verifica que la autentificación del usuario sigue siendo válida.

20) Respuesta de información de identidad [aseveración de credenciales, atributos, política]: El sistema de GId facilita información aseverando las credenciales. Se pueden incluir también los atributos asociados con el ID de dispositivo (por ejemplo, privilegios y preferencias) y la política asociada con la información de identidad (por ejemplo, restricciones relativas a la utilización, la visualización y la divulgación).

21) Autorización: El servicio de aplicación A (VoIP) procesa la información y determina que el usuario está autorizado para el servicio.

22) Sesión de servicio de aplicación: Este flujo de información representa el satisfactorio establecimiento de una sesión del servicio de aplicación A (VoIP) para el usuario.

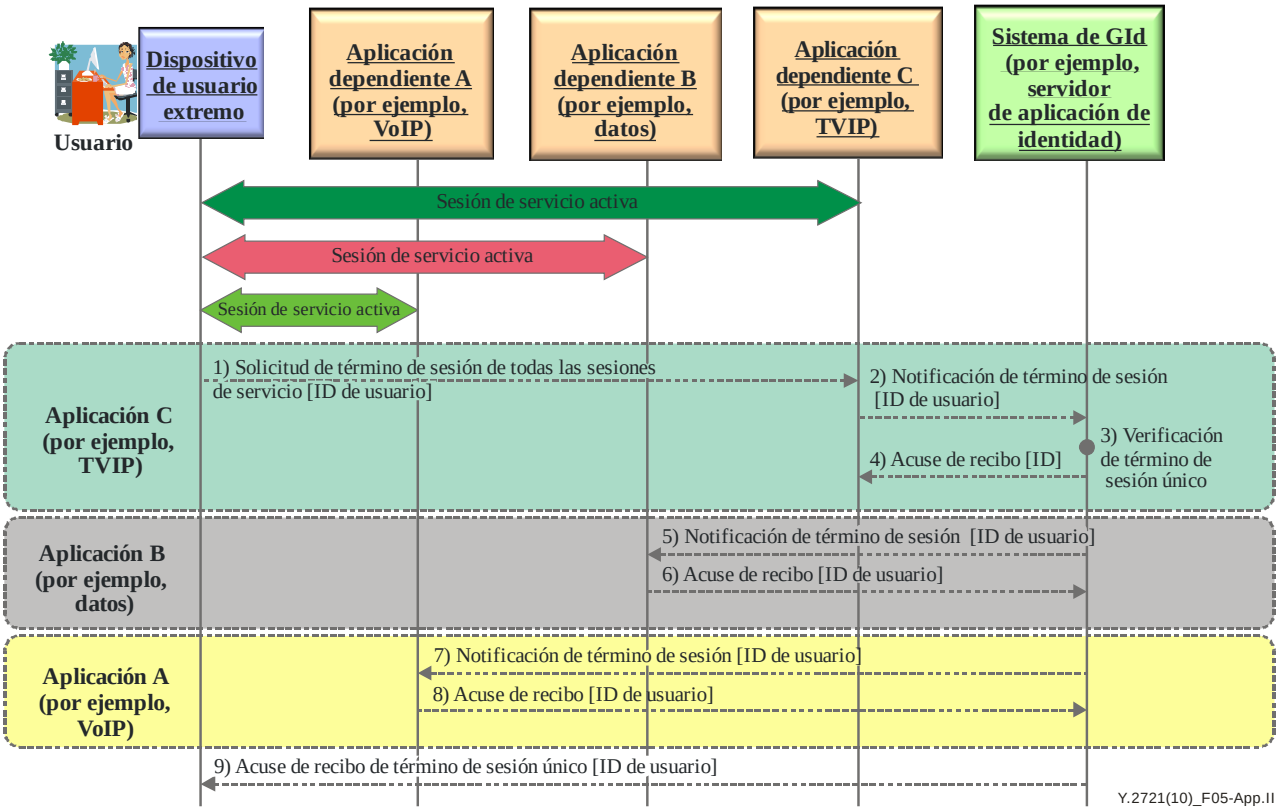


Figura II.5 – Término de sesión único

En la figura II.5 se muestra un ejemplo del servicio de "término de sesión único" que permite al usuario terminar automáticamente las sesiones de múltiples servicios de aplicación (VoIP, datos y TVIP) sin tener que cerrarlas una por una. En este ejemplo se asume que el usuario mantiene una sesión de servicio activa con los servicios de aplicación A (VoIP), B (datos) y C (TVIP).

Los flujos de llamada son los siguientes:

1) Término de sesión de servicio [ID de usuario]: Este flujo de llamada representa la solicitud del usuario para terminar todas las sesiones de servicio.

2) Notificación de término de sesión [ID de usuario]: El servicio de aplicación C (TVIP) notifica al sistema de GId la solicitud de término de sesión del usuario.

3) Verificación de término de sesión único: El sistema de GId determina que el término de sesión único es aplicable y verifica los servicios de aplicación activos.

4) Acuse de recibo [ID de usuario]: El sistema de GId envía al servicio de aplicación C (TVIP) un acuse de recibo relativo al término de la sesión de servicio.

5) Notificación de término de sesión [ID de usuario]: El sistema de GId notifica al servicio de aplicación B (datos) el término de sesión.

6) Acuse de recibo [ID de usuario]: El servicio de aplicación B (datos) acusa recibo del término de sesión.

7) Notificación de término de sesión [ID de dispositivo]: El sistema de GId notifica al servicio de aplicación A (VoIP) el término de sesión.

8) Acuse de recibo [ID de dispositivo]: El servicio de aplicación A (VoIP) acusa recibo del término de sesión.

9) Acuse de recibo de término de sesión único [ID de usuario]: El sistema de GId envía al usuario un acuse de recibo confirmando el término de todas las sesiones de los servicios de aplicación activos.

II.5 Correlación de la información de identidad distribuida para la garantía de autentificación multifactor

II.5.1 Aspectos generales

En este ejemplo se muestra la utilización de la GId para correlacionar y vincular múltiples elementos de información de identidad (por ejemplo, identificadores, credenciales y atributos) a fin de garantizar la identidad de un usuario final/abonado. Por ejemplo, la información de identidad asociada con el abonado (por ejemplo, ID de usuario), el dispositivo de abonado (por ejemplo, ID de dispositivo) y la información de ubicación pueden correlacionarse para dar un nivel más alto de garantía del abonado.

II.5.2 Ejemplo de caso de utilización

En la figura II.6 se muestra un ejemplo de vinculación de la identidad del usuario con la identidad del dispositivo y de su correlación con la información de presencia y ubicación a fin de dar un nivel más alto de garantía de la identidad y las declaraciones asociadas con ella.

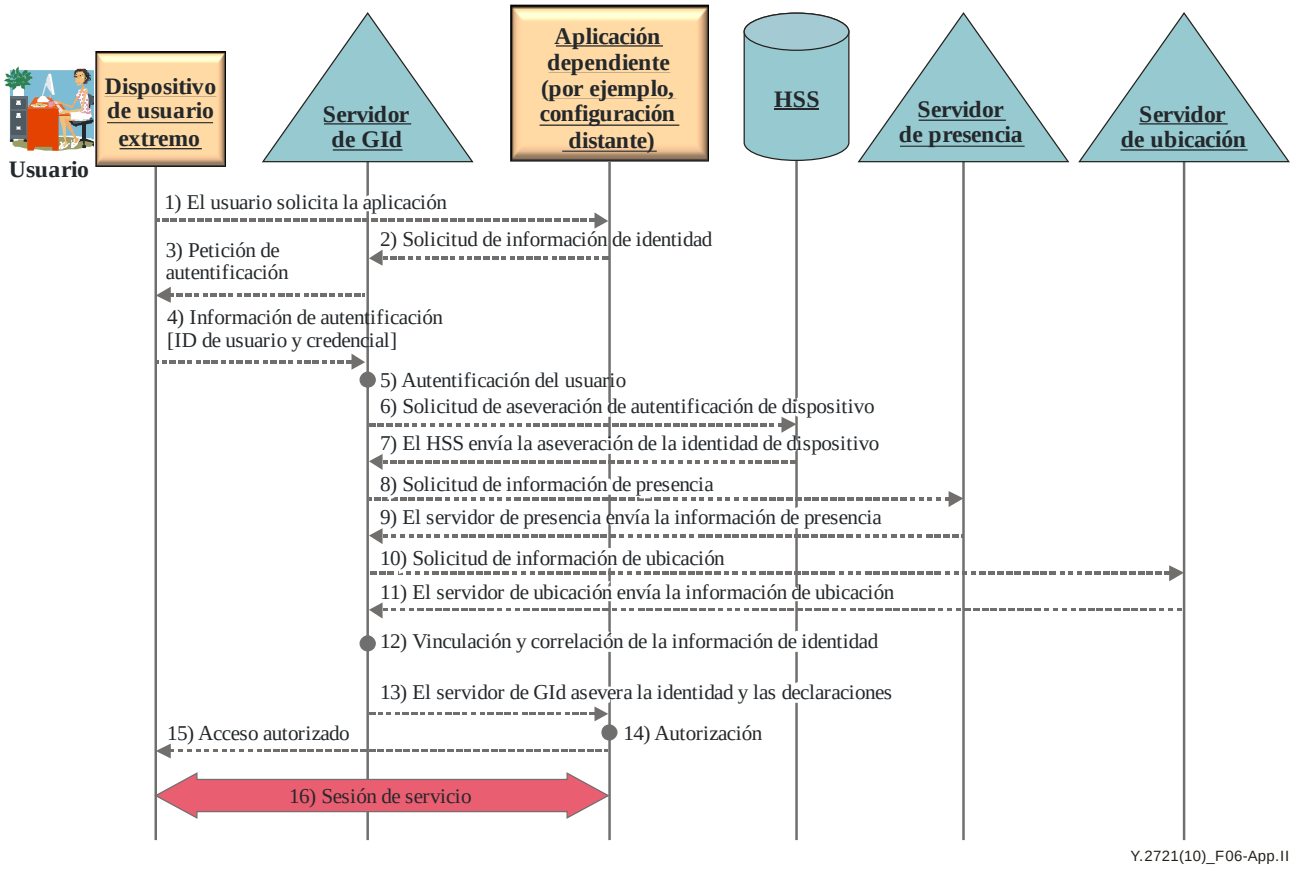


Figura II.6 – Correlación de la información de identidad

En este ejemplo, el usuario final/abonado intenta acceder a una aplicación que necesita un alto nivel de garantía de la identidad del usuario y de los privilegios asociados con ella, porque los riesgos de seguridad asociados con el acceso no autorizado a la aplicación o el recurso pueden ser costosos.

En este ejemplo, los flujos de llamada son los siguientes:

1) El usuario solicita el acceso a la aplicación.
2) La aplicación envía al servidor de GId una solicitud de aseveración de la identidad de usuario y de las declaraciones asociadas con ella.
3) El servidor de GId envía una petición de autentificación al usuario.
4) El usuario facilita la información de autentificación (por ejemplo, ID de usuario y credenciales) al servidor de GId.
5) El servidor de GId autentifica al usuario.
6) El servidor de GId envía al HSS una solicitud de aseveración de la identidad del dispositivo de usuario (Nota: Se supone que el dispositivo de usuario está registrado y se autentifica en la red utilizando los procedimientos corrientes).
7) El HSS envía una aseveración de la identidad del dispositivo de usuario.
8) El servidor de GId envía al servidor de presencia una solicitud de información de presencia.
9) El servidor de presencia facilita la información de presencia al servidor GId.
10) El servidor de GId envía al servidor de ubicación una solicitud de información de ubicación.
11) El servidor de ubicación facilita la información de ubicación al servidor de GId.
12) El servidor de GId vincula la identidad de usuario y la identidad de dispositivo de usuario. Esta identidad combinada se correlaciona con la información de presencia y ubicación para verificar las declaraciones (por ejemplo, privilegios) asociadas con la identidad.
13) El servidor de GId facilita a la aplicación las aseveraciones de la identidad de usuario y de las declaraciones asociadas con ella.
14) La aplicación determina si el usuario está autorizado para el acceso.
15) El usuario puede acceder a la aplicación.
16) Se establece una sesión de servicio.

II.6 Aplicación del control de usuario de la información de identificación personal (por ejemplo, preferencias) entre redes pares/dominios de proveedor de servicio

II.6.1 Aspectos generales

La protección de la IIP es capital para los usuarios finales/abonados. Una importante característica de la GId es que permite a los usuarios finales/abonados facilitar a los proveedores de servicio y PSId información sobre las condiciones, restricciones, consentimientos y autorizaciones relativas a la creación, recopilación, utilización y diseminación de su información de identidad.

II.6.2 Descripción del caso de utilización

En este ejemplo se observa la aplicación de las políticas pertinentes, como las relativas a la información de identidad anónima o pseudónima.

En la figura II.7 se muestra un ejemplo en que el usuario solicita el anonimato.

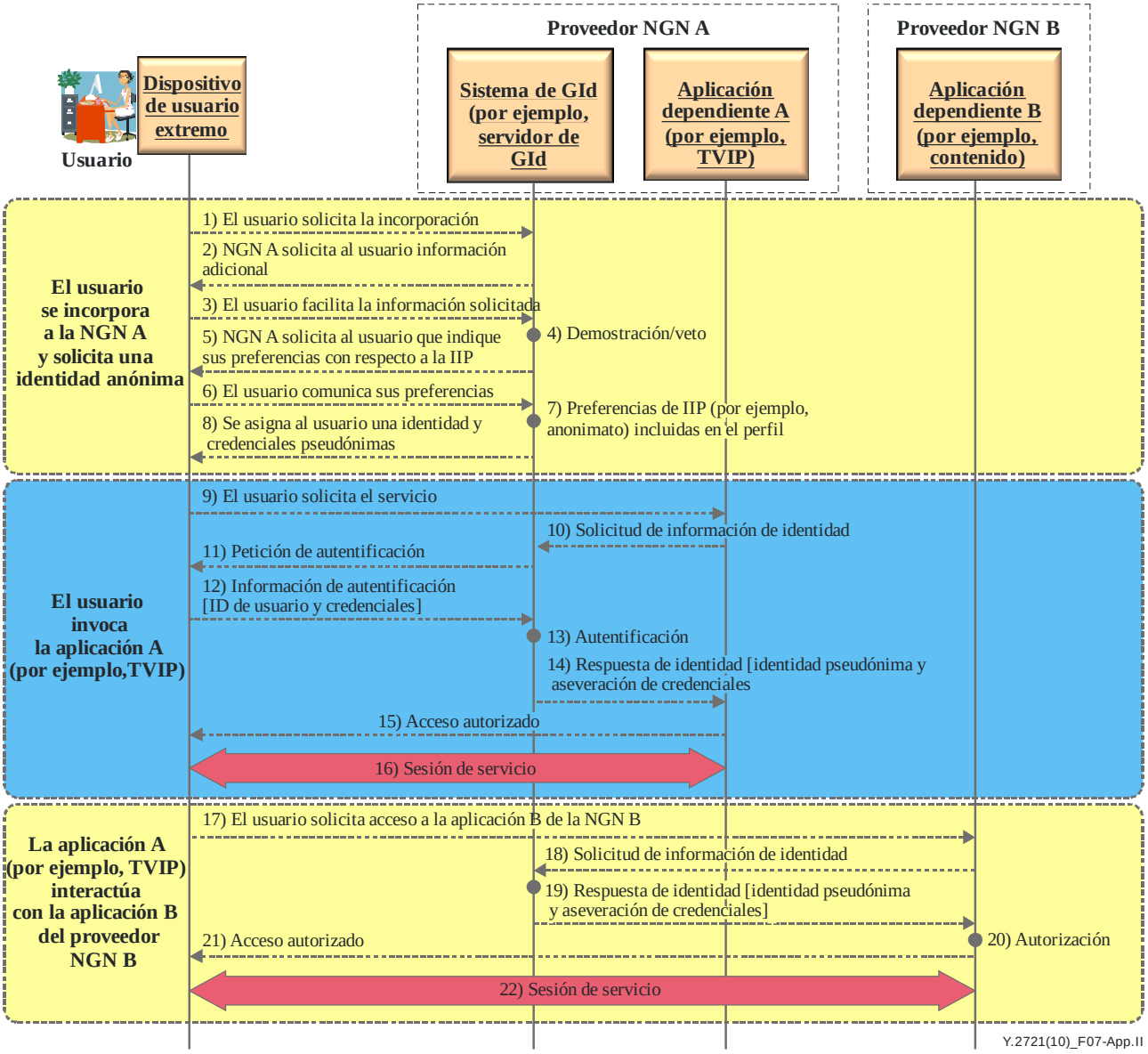


Figura II.7 – Identidad de usuario anónima

NOTA – El término "sistema de GId" se utiliza como término genérico que representa cualquier elemento de la red que puede realizar funciones de GId y permite la realización/aplicación de diversas posibilidades.

En este ejemplo se muestra un proveedor NGN (proveedor NGN A) que asigna una identidad utilizando pseudónimos en respuesta a una solicitud de anonimato del usuario final/abonado. La identidad pseudónima se utiliza para interactuar con el proveedor NGN B a fin de proteger la información de identificación personal del abonado usuario final.

En este ejemplo, los flujos de llamada son los siguientes:

1) El usuario solicita su incorporación al proveedor NGN A.
2) El proveedor NGN A pide al usuario información adicional.
3) El usuario facilita al proveedor NGN A la información solicitada.
4) El proveedor NGN A investiga y demuestra la información.
5) El proveedor NGN A pide al usuario información sobre sus preferencias con respecto a la información de identificación personal (IIP).
6) El usuario indica su preferencia por el anonimato.

7) El proveedor NGN A incluye la preferencia de anonimato en la información de perfil de usuario.

8) Se asigna al usuario una identidad pseudónima y credenciales vinculadas a la identidad.

9) El usuario invoca la aplicación A (por ejemplo, TVIP) del proveedor NGN A.

10) La aplicación dependiente A solicita al sistema de GId (por ejemplo, servidor de GId) información de identidad del usuario.

11) El sistema de GId envía una petición de autentificación al usuario.

12) El usuario facilita la información de autentificación al sistema de GId (por ejemplo, ID de usuario y credencial).

13) El sistema de GId autentifica al usuario.

14) El sistema de GId envía a la aplicación dependiente A aseveraciones de la identidad de usuario y las credenciales

NOTA – Para mantener el anonimato sólo se facilita información de identidad pseudónima.

15) Se autoriza el acceso del usuario a la aplicación A.

16) Sesión de servicio.

17) El usuario solicita acceso a la aplicación B de la NGN B.

18) La aplicación B envía al sistema de GId una solicitud de aseveración de la identidad de usuario y las declaraciones asociadas.

19) El sistema de GId asevera la identidad de usuario y las declaraciones asociadas. Para atenerse a la política de anonimato sólo se facilita información de identidad pseudónima.

20) La aplicación B verifica la información para la autorización.

21) Se da al usuario autorización de acceso.

22) Se establece una sesión de servicio.

II.7 Vinculación/correspondencia entre sistemas de GId heterogéneos

II.7.1 Aspectos generales

Para que un usuario pueda recibir múltiples servicios ofrecidos por los diversos componentes de las NGN, éstas han de disponer de mecanismos de vinculación de los diferentes sistemas de GId. Este requisito se ejemplifica en el caso de utilización que se describe a continuación.

II.7.2 Descripción del caso de utilización

En este ejemplo se muestra un abonado de una NGN que accede a un recurso (por ejemplo, servidor de directorio) ubicado en una red de empresa por medio de su dispositivo de bolsillo. Dado que la NGN y la red de empresa emplean mecanismos de GId diferentes, es necesario vincular los sistemas de GId de esas redes.

En este ejemplo participan las siguientes entidades:

- El sistema de GId de la NGN. Este sistema está modificado de manera que, además de soportar la autentificación AKA mutua del dispositivo de bolsillo del usuario, puede facilitarle credenciales para la autentificación ante el sistema de GId de la red de empresa.
- El sistema de GId de la red de empresa (por ejemplo, centro de distribución de claves).
- El servidor de directorio de empresa (SDE) ubicado en la red de empresa.
- El dispositivo de bolsillo del usuario.
- Estas entidades interactúan de la siguiente manera:
  - El dispositivo de bolsillo del usuario y la red móvil se autentifican mutuamente por el método AKA.

– El usuario, utilizando el dispositivo de bolsillo, envía una solicitud al servidor de directorio de empresa (SDE) ubicado en la red de empresa.
– El SDE responde solicitando la autentificación.
– El usuario obtiene del sistema de GId de la NGN las credenciales de autentificación (por ejemplo, un tique Kerberos), basadas en los resultados de la autentificación AKA, válidas para la autentificación ante el sistema de GId de empresa.

Por ejemplo, el dispositivo de bolsillo del usuario obtiene un tique para el centro de distribución de claves (CDC) de la red de empresa. Específicamente, el tique permite al usuario autentificarse ante el servidor de concesión de tique (SCT), que forma parte del CDC.

- El usuario solicita al SCT un tique para autentificarse ante el SDE.
- El SCT valida las credenciales presentadas y responde al usuario con un tique para el SDE.
- El usuario final responde a la solicitud de autentificación del SDE con el tique recibido del SCT.
- El SDE autentifica al usuario y responde con sus propias credenciales para autentificar al usuario y con una confirmación para el servicio solicitado. Una vez validadas las credenciales del SDE, el usuario puede acceder al SDE.

II.7.3 Requisitos implícitos

- El sistema de GId de la NGN ha de soportar el mecanismo de autentificación AKA y el mecanismo de autentificación (por ejemplo, Kerberos) de la red de empresa.
- El sistema de GId de la NGN ha de ser capaz de expedir credenciales de autentificación (por ejemplo, un tique Kerberos) al dispositivo de usuario final para autentificar al usuario ante el sistema de GId de empresa.
- El sistema de GId de la NGN ha de gestionar la identidad de usuario y las credenciales.
- El sistema de GId de empresa ha de gestionar la identidad de servidor y las credenciales.

NOTA – a) No se exige a las redes 3G ninguna capacidad nueva (por lo que pueden servir de ejemplo); b) Estos requisitos se aplican específicamente al soporte del ejemplo expuesto.

II.8 Soporte de servicios convergentes (por ejemplo, acceso fijo y móvil) en una red de proveedor de servicio

II.8.1 Aspectos generales

Las redes de la próxima generación prometen soportar una multitud de servicios convergentes a través de las redes de acceso fijo y móvil. Por tanto, el usuario tendrá la flexibilidad de invocar un servicio utilizando el dispositivo de acceso y la red que le sean convenientes en cada momento. (A su vez, el proveedor de servicio podrá ampliar su base de clientes e incrementar sus ingresos.) Dado que los mecanismos de seguridad subyacentes en los entornos fijo y móvil son generalmente distintos, resultará muy importante disponer de un sistema de GId convergente, que pueda hacerse cargo de las diferencias. La GId convergente gestionará las identidades y credenciales de los usuarios finales y los servidores de red, independientemente de la tecnología de acceso utilizada.

II.8.2 Descripción del caso de utilización

En este ejemplo se muestra un abonado a una red 3G que accede a un recurso (por ejemplo, servidor de vídeo a la carta) ubicado en una red fija utilizando su dispositivo de bolsillo. En este ejemplo, la red 3G y el recurso de la red fija soportan distintos mecanismos de GId. En este ejemplo participan las siguientes entidades:

- El sistema de GId de la red 3G. Este sistema está modificado de manera que, además de soportar la autentificación AKA mutua con el dispositivo de bolsillo del usuario, puede facilitarle credenciales para la autentificación ante el servidor de vídeo a la carta (VoD).

- El servidor VoD ubicado en la red fija.
- El dispositivo de bolsillo 3G del usuario.
- Estas entidades interactúan de la siguiente manera:
  - El dispositivo de bolsillo del usuario y la red móvil se autentifican mutuamente con el método AKA.
  - El usuario, utilizando su dispositivo de bolsillo, envía una solicitud al servidor VoD.
  - El servidor VoD responde al usuario con una solicitud de autentificación.
  - El usuario obtiene las credenciales de autentificación (por ejemplo, tique Kerberos) del sistema de GId de la red 3G, que genera esas credenciales basándose en los resultados de la autentificación AKA.
  - El usuario responde al servidor VoD con las credenciales de autentificación (un tique).
  - El servidor VoD autentifica al usuario y responde con una confirmación para el servicio solicitado.

II.8.3 Requisitos implícitos

- El sistema de GId de la red 3G ha de soportar el mecanismo de autentificación AKA y el mecanismo de autentificación (por ejemplo, Kerberos) del servidor VoD.
- El sistema de GId debe ser capaz de expedir credenciales de autentificación (por ejemplo, tique) al dispositivo de usuario para la autentificación del usuario ante el servidor VoD.
- El sistema de GId de la red 3G ha de gestionar la identidad de usuario y las credenciales.
- El sistema de GId de la red 3G debe gestionar la identidad del servidor VoD y las credenciales.

NOTA – Estos requisitos se aplican específicamente al soporte del ejemplo presentado.

II.9 Ejemplo de caso de utilización – Autentificación del usuario y autorización del proveedor NGN (autentificación y autorización mutuas)

En la figura II.8 se muestra un ejemplo donde se utiliza la autentificación de usuario de un proveedor NGN. En este ejemplo se asume la existencia de un entorno de servicio abierto, donde los proveedores NGN pueden hacer publicidad de los servicios para los usuarios. En este ejemplo se destacan las lagunas o carencias en la capacidad del usuario para autentificar y autorizar a los proveedores NGN (o autentificación mutua) en un entorno multiproveedor de servicio abierto.

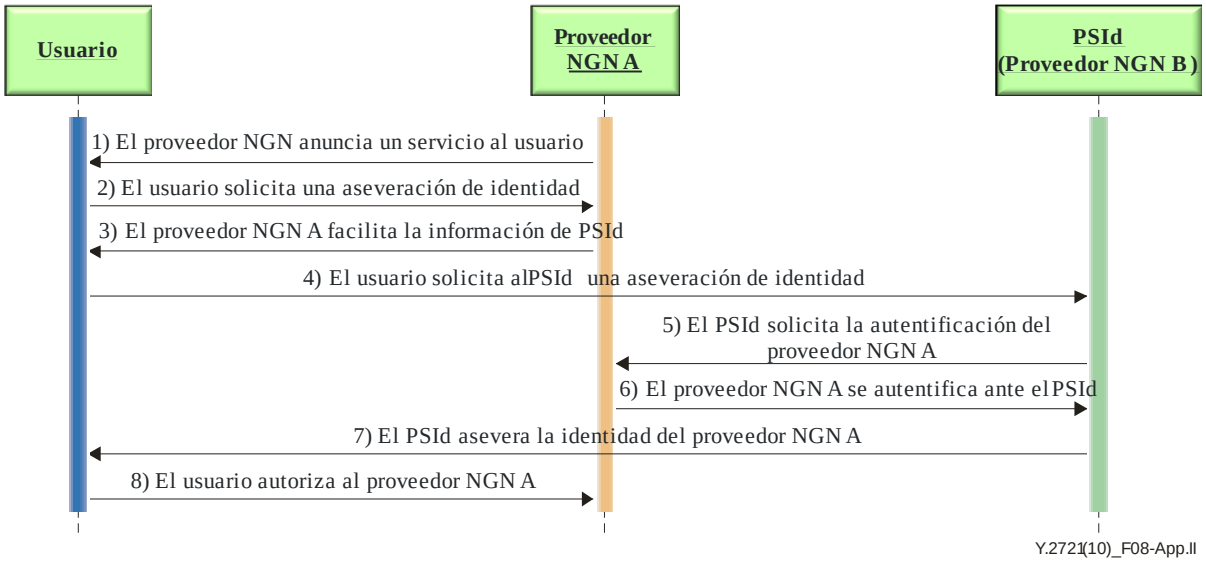


Figura II.8 – Ejemplo de caso de utilización: autentificación y autorización de usuario del proveedor NGN

En este ejemplo, los flujos de llamada son los siguientes:

1) El proveedor NGN anuncia servicios al usuario.
2) El usuario solicita la aseveración de la identidad del proveedor NGN A.
3) El proveedor NGN facilita al usuario la dirección de un PSId.
4) El usuario envía al PSId una solicitud de aseveración de la identidad del proveedor NGN A.
5) El PSId solicita al proveedor NGN A que se autentifique.
6) El proveedor NGN A facilita la información de autentificación.
7) El PSId envía al usuario información aseverando la identidad del proveedor NGN A.
8) El usuario autoriza al proveedor NGN A a prestar servicios.

NOTA – En este ejemplo no se muestran los flujos relacionados con la autentificación y autorización del proveedor NGN o el usuario.

II.10 Ejemplo de caso de utilización – Aseveración de usuarios pares (transacciones no pecuniarias)

En la actualidad no se dispone todavía de capacidades de GId para las NGN que permitan a los usuarios autentificar el origen de las comunicaciones o las fuentes de datos. En general, los métodos de GId que se están definiendo se centran principalmente en la GId para las transacciones pecuniarias y el comercio electrónico. Las NGN deberán soportar capacidades de GId para una amplia gama de transacciones y comunicaciones, pues es especialmente importante para algunos servicios de emergencias que deberán soportar las NGN. En la figura II.9 se muestra un ejemplo que ilustra por qué es necesario que las capacidades GId de las NGN permitan a los usuarios aseverar mutuamente su identidad en las comunicaciones pares y las transacciones no pecuniarias. Por ejemplo, es posible que un usuario tenga que autentificar la fuente de un mensaje recibido (por ejemplo, correo electrónico o mensaje instantáneo), una solicitud de comunicación (por ejemplo, comunicación de voz, vídeo o datos) o de datos recibidos. No existe hoy en día una especificación NGN que soporte tales capacidades de GId.

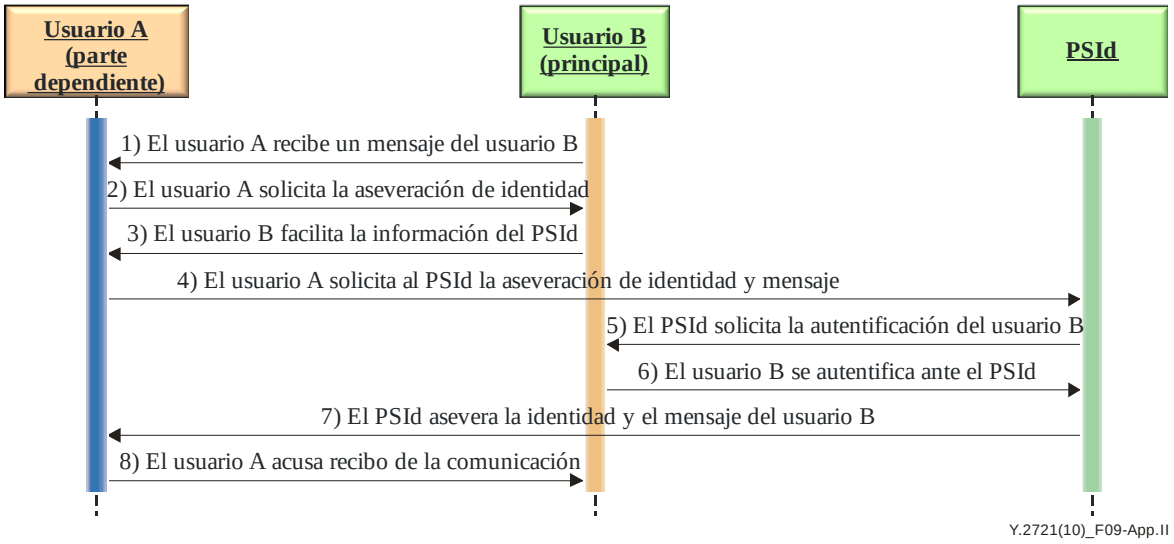


Figura II.9 – Ejemplo de caso de utilización: aseveración de usuarios pares (transacciones no pecuniarias)

En el ejemplo de la figura II.9 se asume que el usuario A recibe un mensaje o una solicitud de comunicación del usuario B y querría aseverar la identidad del usuario B y de los datos recibidos. En este ejemplo, los flujos de llamada son los siguientes:

1) El usuario A recibe un mensaje o una solicitud de comunicación del usuario B.
2) El usuario A solicita la aseveración de la identidad del usuario B y la autentificación de la información recibida del usuario B.
3) El usuario B facilita al usuario A la información de dirección del proveedor de servicio de identidad (PSId).
4) El usuario A envía al PSId una solicitud de aseveración de la identidad del usuario B y la autentificación de la información recibida.
5) El PSId envía al usuario B una solicitud de autentificación.
6) El usuario B responde y se autentifica ante el PSId.
7) El PSId responde al usuario A aseverando la identidad del usuario B y la información recibida.
8) El usuario A acusa recibo de la comunicación al usuario B.

II.11 Caso de utilización de GId – Garantía de la identidad e integridad del dispositivo de usuario final

Las NGN soportarán diversos dispositivos de usuario (por ejemplo, teléfonos fijos, teléfonos inalámbricos, computadores personales, agendas digitales, descodificadores de TVIP). Los componentes de hardware y software de los dispositivos conectados a la NGN abarcan toda la gama de complejidad y, de ser robados o manipulados, pueden ser utilizados para orquestar diversos tipos de ataques.

Deberían diseñarse y utilizarse capacidades de seguridad especiales en el componente de hardware resistente a los ataques de los dispositivos de usuario final a fin de conservar encriptados los datos de gestión de identidad y soportar capacidades de seguridad especializadas para validar la identidad e integridad de los dispositivos de usuario final. En esta cláusula se presenta un ejemplo en que podría diseñarse y aplicarse un componente de hardware de seguridad especializado para los dispositivos de usuario extreme, que se utilizaría para soportar los servicios de gestión de identidad para:

1) Garantizar la identidad de un dispositivo de usuario final.

2) Garantizar la integridad de un dispositivo de usuario final (es decir, verificar que el software y el hardware configurados no se han manipulado).

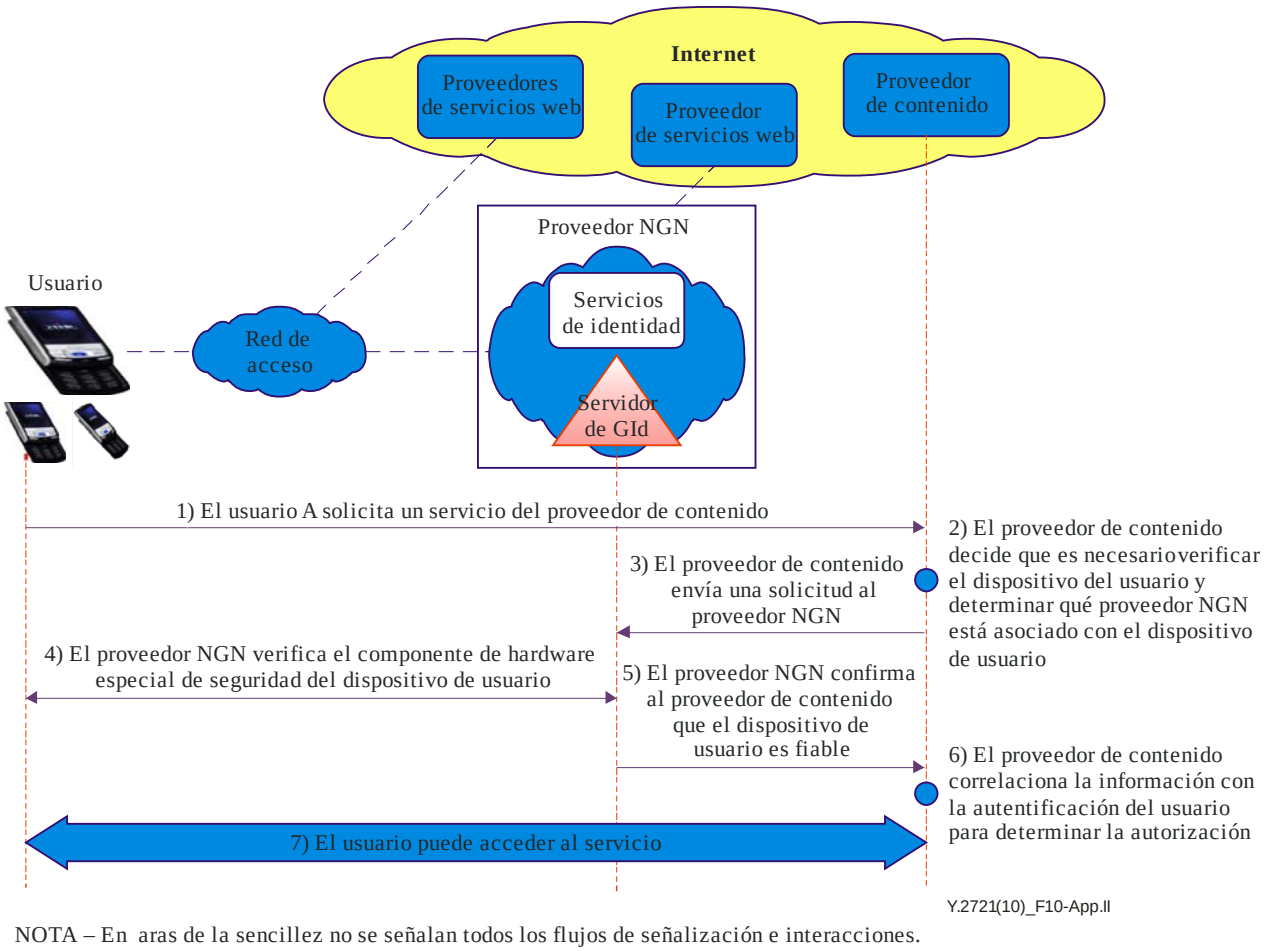
3) Permitir a los usuarios encriptar y proteger la IIP y otros datos sensibles en los dispositivos de usuario final.

II.11.1 Ejemplo de caso de utilización – Garantía de autentificación de usuario y dispositivo

En este caso, es necesario que se soporte el componente de hardware especializado resistente a los ataques en el dispositivo de usuario final para la identificación unívoca del dispositivo. Por ejemplo, las contraseñas, claves digitales y certificados pueden almacenarse en el componente de hardware especializado resistente a los ataques del dispositivo a fin de identificar unívocamente al dispositivo. El componente de hardware especializado podría soportar las interfaces de programación de aplicaciones (API) normalizadas para soportar los servicios de aplicación de seguridad dependientes del componente de hardware especializado para confiar en el dispositivo.

La identificación y autentificación unívocas del componente de hardware resistente a los ataques podrían correlacionarse con la identificación y autentificación del usuario a fin de lograr un mayor grado de garantía para el control de acceso en un entorno de proveedor multiservicio.

En la figura II.10 se muestra un ejemplo en que se ha diseñado y aplicado un componente de hardware especializado resistente a los ataques en el dispositivo de usuario final para la identificación unívoca del dispositivo. En este ejemplo, se supone que el componente de hardware especializado resistente a los ataques está controlado por un proveedor NGN en virtud de un acuerdo contractual con el abonado. Previo consentimiento del usuario cualificado, el PSId/NGN puede prestar servicios de identidad a otros proveedores (por ejemplo, proveedores de contenido, proveedores de servicios web, y proveedores terceros) y asociados garantizando la identidad y la autentificación del dispositivo de usuario final. De este modo, los proveedores de servicio tendrían confianza en la identidad y la autentificación del dispositivo de usuario final. La información relativa a la identidad y la autentificación del dispositivo de usuario puede correlacionarse con la autentificación del usuario para lograr un mayor grado de garantía y confianza.



NOTA – En aras de la sencillez no se señalan todos los flujos de señalización e interacciones.

Figura II.10 – Correlación de la autentificación de usuario y dispositivo para la garantía

En este ejemplo, los flujos de llamada son los siguientes:

1) El usuario solicita un servicio del proveedor de contenido.

2) El proveedor de contenido decide que es necesario verificar el dispositivo de usuario para permitir el acceso al servicio y determina que el proveedor NGN está asociado con el dispositivo de usuario.

3) El proveedor de contenido envía al proveedor NGN una solicitud de aseveración de la identidad y la autentificación del dispositivo de usuario.

4) El proveedor NGN identifica y autentifica el componente de hardware especial de seguridad del dispositivo de usuario (por ejemplo, verificando los certificados almacenados en el componente de hardware de seguridad resistente a los ataques del dispositivo).

5) El proveedor NGN envía una respuesta al proveedor de contenido validando la identidad y la autentificación del dispositivo de usuario.

6) El proveedor de contenido correlaciona la información del proveedor NGN con la información de autentificación del usuario y determina la autorización para el servicio.

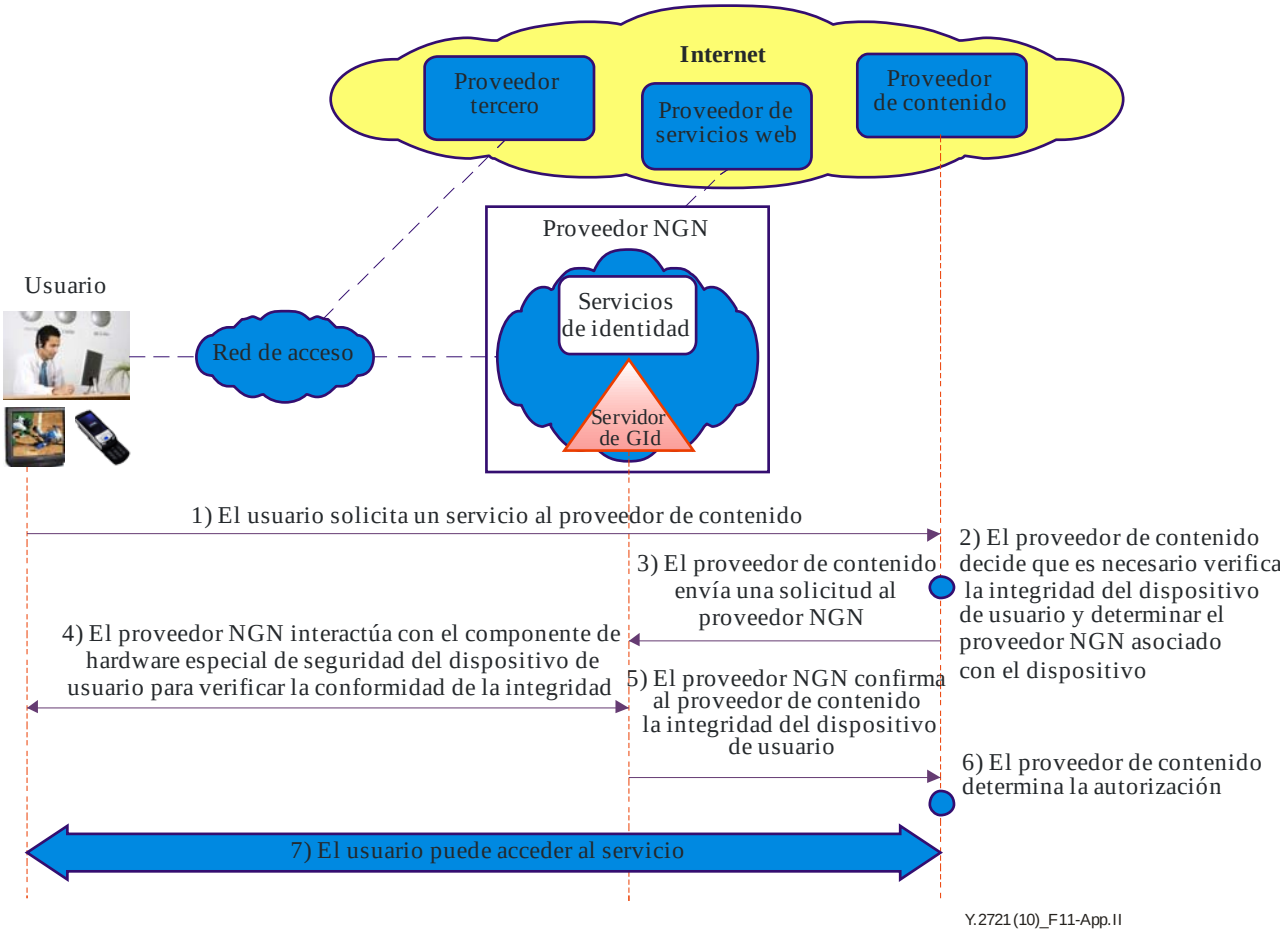
7) El usuario puede acceder al servicio (por ejemplo, contenido).

II.11.2 Ejemplo de caso de utilización – Garantía de la integridad del dispositivo de usuario

En el entorno de seguridad actual, los abonados se conectan a la red utilizando diversos dispositivos (por ejemplo, teléfonos fijos, teléfonos inalámbricos, computadores personales, agendas digitales, descodificadores de TVIP). La integridad de los dispositivos de usuario final (por ejemplo, el hardware y el software configurados) puede fácilmente ponerse en peligro sin que el usuario/abonado lo sepa. Las aplicaciones Internet populares, como los navegadores web y el correo electrónico, y otras aplicaciones que se ejecutan en los dispositivos de abonado para que éstos puedan interactuar con los servicios y las características de dispositivo locales, pueden poner en peligro la integridad del dispositivo debilitándolo. Por ejemplo, estas aplicaciones pueden tener fallos de seguridad inherentes o soportar características, como las descargas de ficheros, los applets de software, los plug-ins de navegación y los enlaces incorporados, que pueden utilizarse para ese fin. Las descargas de software y de ficheros, sobre todo cuando proceden de una fuente no fiable, hacen que los dispositivos de abonado san vulnerables a códigos malignos, gusanos, virus y caballos de Troya. Los registradores de claves que registran todas las entradas de claves, incluidos los nombres de usuario y las contraseñas, y transmiten la información a atacantes que pueden utilizarlas para obtener acceso sin autorización) son un tipo de código maligno muy corriente. Entre los códigos malignos se cuentan también el spyware (programas que rastrean la actividad del abonado) y el adware (programas que envían publicidad no deseada, normalmente en respuesta a información obtenida controlando al abonado). Algunos de estos programas literalmente piratean los dispositivos de usuario y ocultan su presencia incrustándose en el sistema operativo.

Este ejemplo muestra la utilización del componente de hardware especializado resistente a los ataques en los dispositivos de usuario para realizar verificaciones de integridad y confirmar a las aplicaciones y servicios la integridad del dispositivo. Por ejemplo, el componente de hardware especializado resistente a los ataques puede contener algoritmos y funciones propios del fabricante para verificar los problemas de integridad. El componente de hardware especial puede incluir un modelo de referencia con un conjunto de valores de integridad correctos conocidos para identificar específicamente el código correcto y servir de valor de referencia para el dispositivo. Los valores de integridad correctos conocidos se utilizarán para efectuar una comparación con los valores reales de la configuración y determinar si la unidad mantiene su integridad.

En la figura II.11 se muestra un ejemplo en que se diseña y aplica un componente de hardware especializado resistente a los ataques en el dispositivo de usuario final para verificar la integridad del dispositivo. En este ejemplo, se supone que el componente de hardware especializado resistente a los ataques está controlado por el proveedor NGN mediante acuerdo contractual con el abonado. Previo consentimiento del usuario cualificado, el PSId/NGN puede prestar servicios de identidad a otros proveedores (por ejemplo, proveedores de contenido, proveedores de servicios web y proveedores terceros) y asociados validando la integridad y la conformidad del dispositivo de usuario final.



NOTA – En aras de la sencillez no se muestran todos los flujos de señalización e interacciones.

Figura II.11 – Garantía de integridad de dispositivo

En el ejemplo, los flujos de llamada son los siguientes:

1) El usuario solicita un servicio al proveedor de contenido.

2) El proveedor de contenido determina que es necesario verificar la integridad del dispositivo de usuario y determinar el proveedor NGN asociado con el dispositivo de usuario.

3) El proveedor de contenido envía al proveedor NGN una solicitud de confirmación de la integridad del dispositivo de usuario.

4) El proveedor NGN interactúa con el componente de hardware especial de seguridad del dispositivo de usuario para verificar la conformidad de la integridad.

5) El proveedor NGN confirma al proveedor de contenido la integridad del dispositivo de usuario.

6) El proveedor de contenido determina la autorización.

7) El usuario puede acceder al servicio (por ejemplo, contenido).

II.11.3 Ejemplo de caso de utilización – Encriptación de la IIP y de los ficheros/datos sensibles

La pérdida o el robo de un dispositivo con IIP y otro tipo de datos sensible puede tener serias consecuencias para los particulares y las empresas públicas y privadas. El componente de hardware especializado diseñado para identificar unívocamente y confirmar la integridad de los dispositivos fiables también podría soportar capacidades de encriptación y protección de la IIP y otro tipo de datos sensibles en los dispositivos de usuario final. Al estar encriptados los datos confidenciales, las partes no autorizadas no pueden acceder a esos datos en los computadores, teléfonos celulares o dispositivos de almacenamiento sin manipularlos, lo que conlleva un gasto.

Apéndice III

Casos de utilización de la GId en el servicio de telecomunicaciones de emergencia (STE)

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

III.1 Introducción

En el presente apéndice se facilitan ejemplos de utilización de la gestión de identidad (GId) en el STE. Éste es un servicio que requiere trato prioritario. Véase la cláusula 8.4.7.

III.2 Garantía de autentificación utilizando una combinación de dispositivo y usuario

La autentificación de usuarios autorizados del STE es necesaria para proteger la disponibilidad e integridad del STE y de las redes asociadas. Actualmente se utilizan dos métodos básicos de autentificación para las aplicaciones STE tradicionales, a saber:

1) método basado en PIN; y

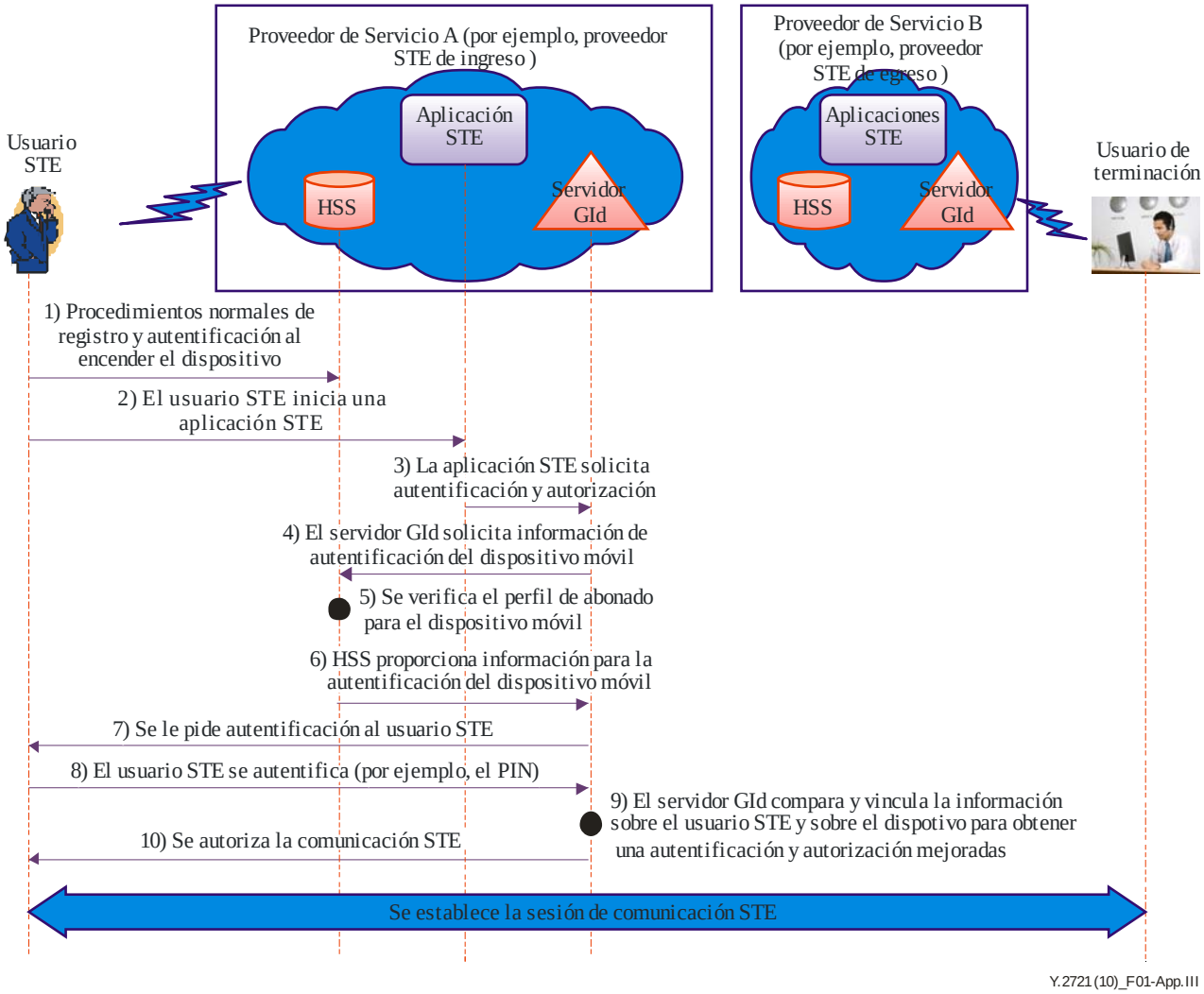
2) método basado en la suscripción.

El primer método consiste en recurrir a números de identificación personal (PIN) para efectuar la autentificación y autorización. El usuario queda autentificado tras verificarse el PIN, autorizándolo así a utilizar el STE. Mediante este método se identifica el usuario pero no el dispositivo del usuario. Por consiguiente, este método se suele utilizar en casos en los que el usuario puede emplear el STE desde cualquier dispositivo.

El segundo método consiste en la autentificación y autorización basada en la información del perfil del abonado asociado con un determinado terminal o dispositivo de usuario. La identidad del dispositivo o terminal de usuario se autentifica siguiendo los procedimientos habituales de registro y autorización del proveedor NGN (es decir, el proveedor del STE), por lo que para autorizar las llamadas/sesiones del STE se verifica el perfil del abonado al servicio (es decir, si la suscripción al servicio permite efectuar llamadas/sesiones del STE a partir de dicho dispositivo). Este método consiste en autentificar el dispositivo del usuario (es decir, el terminal inalámbrico) y no el usuario.

La utilización de estos métodos sencillos basados en el PIN y en la suscripción resultan adecuados para las aplicaciones del STE tradicionales, pero no así para todos los tipos de aplicaciones STE en el entorno NGN. Concretamente, en aplicaciones tales como los servicios prioritarios multimedios (por ejemplo, servicios de datos y vídeo) se requerirán un mayor grado de garantía o confianza en cuanto a la identidad del usuario del STE y al nivel de autorización para acceder a la aplicación STE y los correspondientes recursos. Por consiguiente, además de poder utilizar los métodos de autentificación basados en el PIN y en la suscripción, las NGN tendrán también que disponer de mecanismos avanzados para autentificar y autorizar a usuarios y dispositivos del STE.

Una posibilidad a la hora de examinar la transición del STE (es decir, servicios vocales prioritarios) hacia el entorno de las NGN es recurrir a la GId para correlacionar y vincular la autentificación del usuario y la identificación y autentificación del dispositivo de usuario. De este modo se obtiene mayor garantía (es decir, confianza) de la identidad y la autorización del usuario para acceder al STE. Este concepto se describe en el ejemplo de utilización general que figura a continuación.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.1 – Autentificación combinada de usuario y dispositivo

En la figura III.1 se muestra un ejemplo en el que se utilizan las funciones GId para combinar la autentificación de usuario y de dispositivo con el fin de obtener mayor garantía en la autorización de usuarios STE.

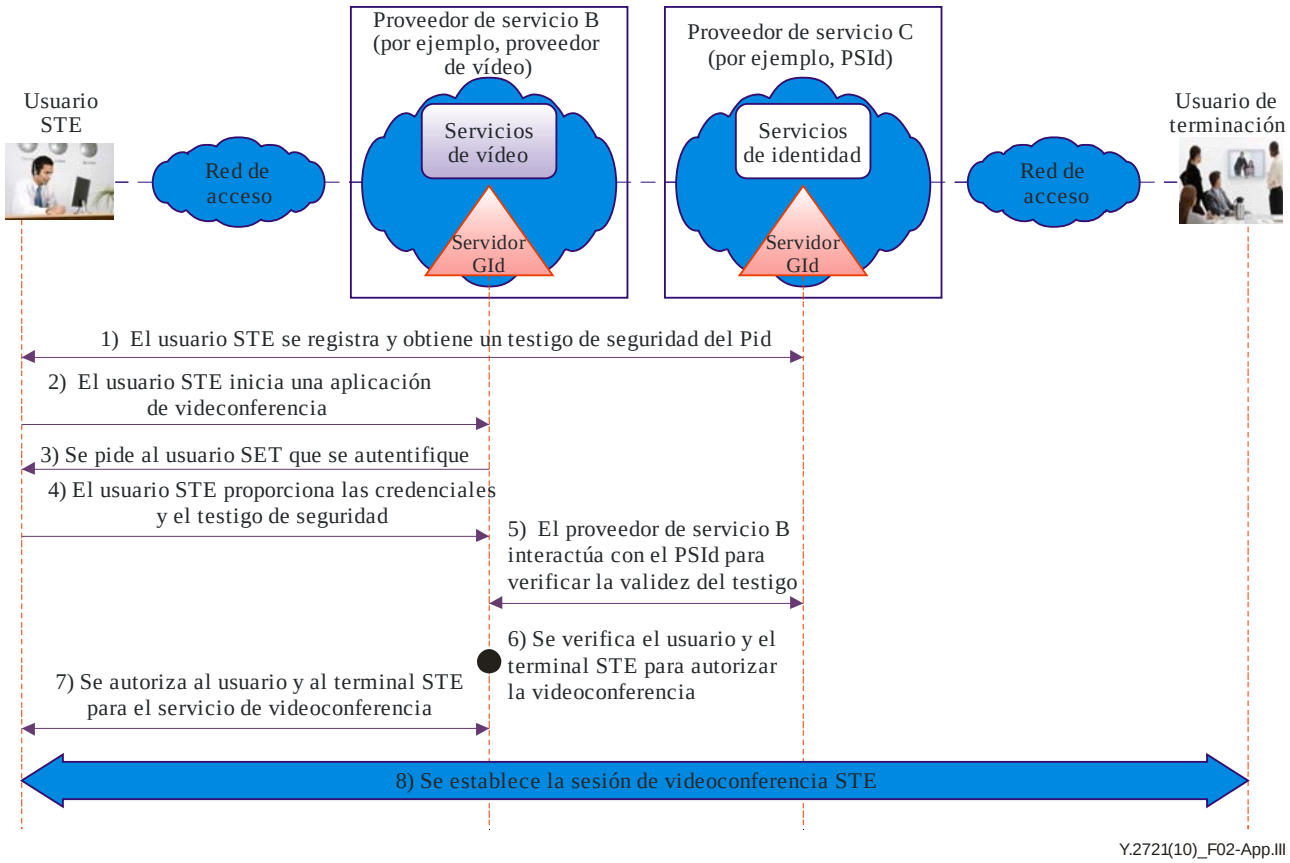
El flujo de la llamada de este ejemplo puede resumirse así:

1) El dispositivo móvil del usuario se registra y autentifica utilizando los procedimientos habituales tras ponerlo en funcionamiento.
2) El usuario STE inicia una aplicación STE.
3) La aplicación STE solicita autentificación y autorización al servidor GId.
4) El servidor GId solicita información de autentificación del dispositivo móvil.
5) El HSS verifica el perfil de abonado para el dispositivo móvil.
6) HSS proporciona al servidor GId la información de autentificación del dispositivo móvil.
7) Se le pide autentificación al usuario SET.
8) El usuario STE se autentifica (por ejemplo, el PIN).
9) El servidor GId compara y vincula la información sobre el usuario STE y sobre el dispositivo móvil para obtener una autentificación y autorización mejoradas.
10) Se autoriza la comunicación STE.

Siguiendo este flujo de ejemplo se obtiene una mayor garantía de la identidad del usuario STE y de la autorización para utilizar el servicio. Para combinar la autentificación del dispositivo con el usuario se requerirán interacciones adicionales con el usuario STE a los efectos de su autentificación, lo que podría considerarse excesivo. Aunque no es necesario recurrir a este procedimiento para todas las sesiones STE, podría considerarse la posibilidad de recurrir al mismo para sesiones STE que requieran mayores niveles de garantía.

III.3 Autentificación mejorada de usuarios STE para servicios prioritarios de la próxima generación (servicios multimedios prioritarios)

A medida que el entorno de las comunicaciones evolucione hacia el entorno de las NGN/IMS, los usuarios STE tendrán que mantenerse al corriente de los cambios tecnológicos y de las nuevas tendencias en el sector. Por ejemplo, para llevar a cabo su cometido los usuarios STE son cada vez más dependientes de otros tipos de comunicaciones aparte de las vocales, tales como la mensajería instantánea, la mensajería de texto y el correo electrónico. En general, existen varias iniciativas en fase de planificación y desarrollo para permitir a los usuarios del STE obtener acceso prioritario a servicios multimedios tales como servicios de voz, datos y vídeo. Ahora bien, los mecanismos basados en suscripción y PIN utilizados para el STE en el entorno de la RTPC no resultan adecuados para servicios multimedios en el entorno NGN/IMS. Concretamente, aplicaciones tales como los servicios prioritarios multimedios (por ejemplo, servicios de datos y vídeo) requerirán un mayor grado de garantía o confianza en cuanto a la identidad del usuario del STE y al nivel de autorización para poder acceder a la aplicación STE y los correspondientes recursos, debido a que los riesgos y las posibles amenazas a la seguridad en el entorno NGN son en general mayores. Por otra parte, a diferencia del STE actual que funciona en la RTPC, cabe esperar que la nueva generación de servicios multimedios prioritarios se autorizarán únicamente para una determinada población de usuarios del STE. Además, como el objetivo general de los usuarios STE es disponer de acceso amplio y fácil de utilizar desde cualquier lugar, en cualquier momento y a través de cualquier dispositivo, es importante que se considere la posibilidad de recurrir a mecanismos GId más avanzados y versátiles, según proceda. Para proteger la integridad y disponibilidad de los servicios y recursos multimedios del STE y de la infraestructura NGN/IMS en general en situaciones de emergencia y en caso de catástrofe es fundamental tener una mayor garantía de la identidad del usuario STE. Las aplicaciones de datos y vídeo multimedios (por ejemplo, información por la web o descargada de vídeos) consumen más anchura de banda y recursos que las aplicaciones vocales. Si no se dispone de mecanismos de control adecuados, el acceso no autorizado a aplicaciones de datos y vídeos del STE podría afectar negativamente a las aplicaciones STE propiamente dichas y a la infraestructura de comunicaciones en general. Por ejemplo, el acceso no autorizado a una aplicación STE que consume muchos recursos podría emplearse para congestionar la red o efectuar ataques de denegación de servicio. Por consiguiente, es preciso recurrir a métodos más sofisticados basados en testigos de seguridad, certificados digitales, reconocimiento de la voz o funciones biomédicas para autentificar y autorizar a los usuarios del STE y/o a los terminales.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.2 – Autentificación mejorada para servicios prioritarios de la próxima generación

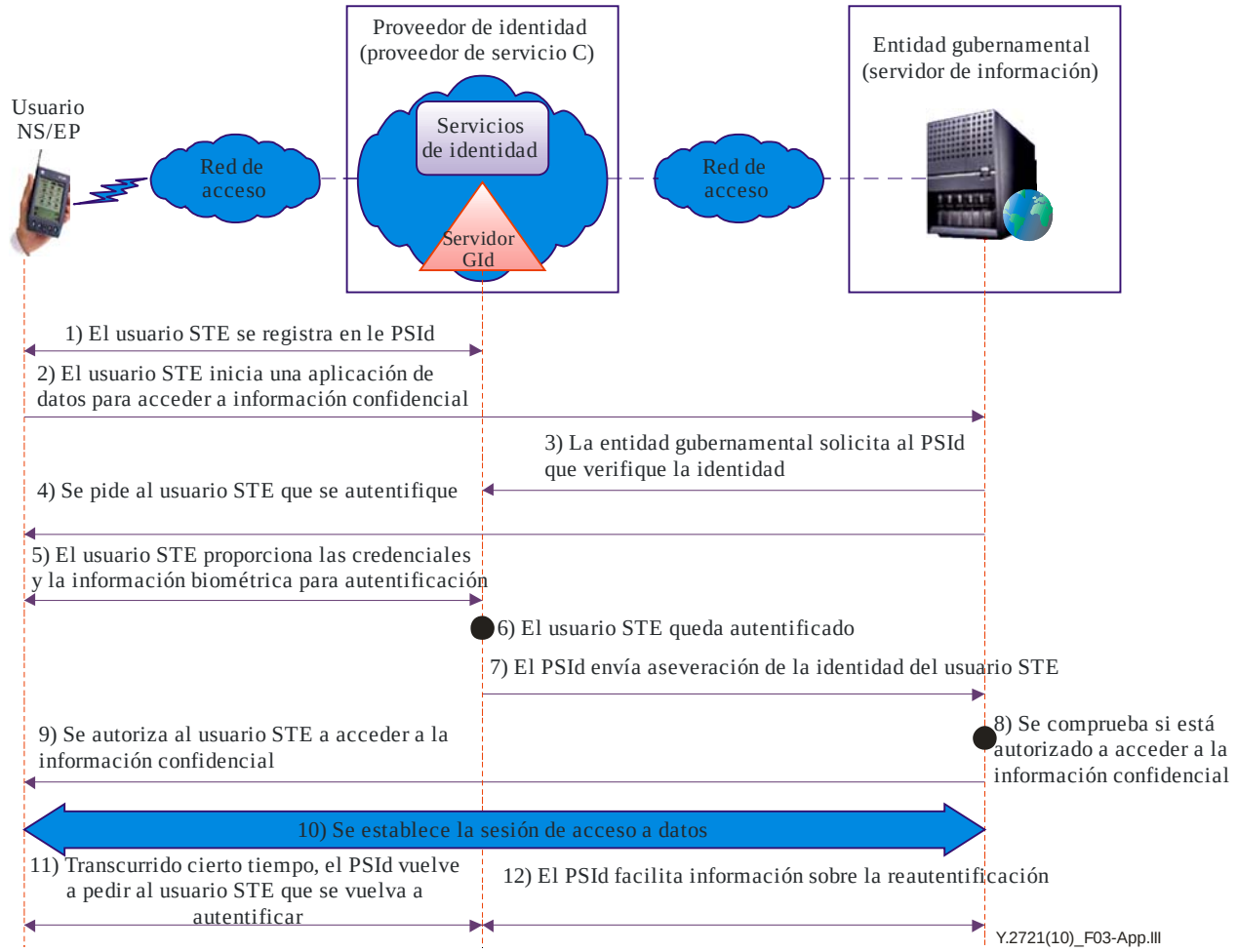
En la figura III.2 se muestra un ejemplo en el que se recurre a la autentificación avanzada de usuarios autorizados para servicios multimedios prioritarios de la próxima generación (por ejemplo, videoconferencia). En este ejemplo se parte del supuesto de que la credencial de identidad (es decir, el testigo de seguridad o el certificado digital) la facilita un PSId distinto del proveedor del servicio multimedios (aunque es posible que los dos sean el mismo). Si el PSId y el proveedor de servicios son entidades distintas, será necesario concertar de antemano los necesarios acuerdos comerciales y de confianza. También será preciso efectuar la autentificación mutua entre el PSId y el proveedor de servicios.

El flujo de la llamada de este ejemplo puede resumirse así:

1) El usuario STE se registra y obtiene una credencial (testigo de seguridad o certificado digital) que lo identifica y define sus privilegios para servicios multimedios.
2) El usuario STE inicia una aplicación de videoconferencia.
3) Se pide al usuario del SET que se autentifique.
4) El usuario STE proporciona las credenciales (testigo de seguridad o certificado digital) para la autentificación.
5) El proveedor de servicio B interactúa con el PSId para verificar la validez de las credenciales (testigo de seguridad o certificado digital).
6) El proveedor de servicio B procesa y verifica la información para determinar si el usuario del STE y el terminal están autorizados a utilizar servicios multimedios prioritarios.
7) Una vez autentificado, se autoriza al usuario del STE y al terminal a iniciar el servicio multimedios prioritario (por ejemplo, videoconferencia).

8) Se crea y establece la sesión multimedios.

Es posible que en el caso de ciertas comunicaciones multimedios de la próxima generación se haya de recurrir a información biométrica para autentificar a los usuarios del STE autorizados. Por ejemplo, el carácter confidencial de cierta información podría exigir que sólo un determinado conjunto de usuarios del STE autorizados tengan acceso a la misma. En tales casos es indispensable obtener un mayor grado de confianza al verificar la identidad del usuario del STE, por lo que cabría considerar la posibilidad de recurrir a mecanismos biométricos como posible solución tecnológica para efectuar dicha verificación.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.3 – Ejemplo de utilización de tecnología biométrica

En la figura III.3 se muestra un ejemplo en el que se recurre a funciones biométricas. En este ejemplo se parte de la hipótesis de que el dispositivo del usuario dispone de una función adecuada para leer información biométrica. También se supone que el usuario del STE se registró previamente en el PSId y que éste ha obtenido y tiene almacenada la información biométrica necesaria. Obsérvese que también puede darse el caso de que la entidad gubernamental disponga y proporcione servicios de identidad (por ejemplo, registra y almacena la identidad del usuario del STE y su información biométrica), en lugar de recurrir a los servicios de un tercero. A continuación se resume el flujo de llamada:

1) El usuario STE se registra en el PSId para activar el servicio de autentificación biométrica. Se supone que ya se ha completado el procedimiento para recabar y verificar la información biométrica y de identidad (por ejemplo, al registrarse en persona).

2) El usuario STE inicia la comunicación para acceder a distancia a la base de datos de la entidad gubernamental que alberga el servicio de información.

3) La política de seguridad que aplica la entidad gubernamental exige que se requiera un mayor nivel de garantía para permitir el acceso, e inicia un procedimiento de redirección al PSId.

4) Se solicita al usuario SET que se autentifique y se le remite al PSId.

5) El usuario STE procede a la autentificación, por ejemplo el usuario STE escanea su pulgar con el chip biométrico especial integrado en su dispositivo móvil inalámbrico.

6) El PSId utiliza la información suministrada por el usuario del STE para autentificarlo.

7) El PSId envía información a la entidad gubernamental en la que asevera la identidad del usuario del STE.

8) La entidad gubernamental comprueba si dicho usuario está autorizado a acceder al servidor de información que contiene datos confidenciales.

9) Se autoriza al usuario STE a acceder a la información confidencial.

10) Se establece la sesión de acceso a datos.

11) Transcurrido cierto tiempo, el PSId vuelve a pedir al usuario STE que se vuelva a autentificar, conforme a la política de seguridad que aplica el servidor de información de la entidad gubernamental.

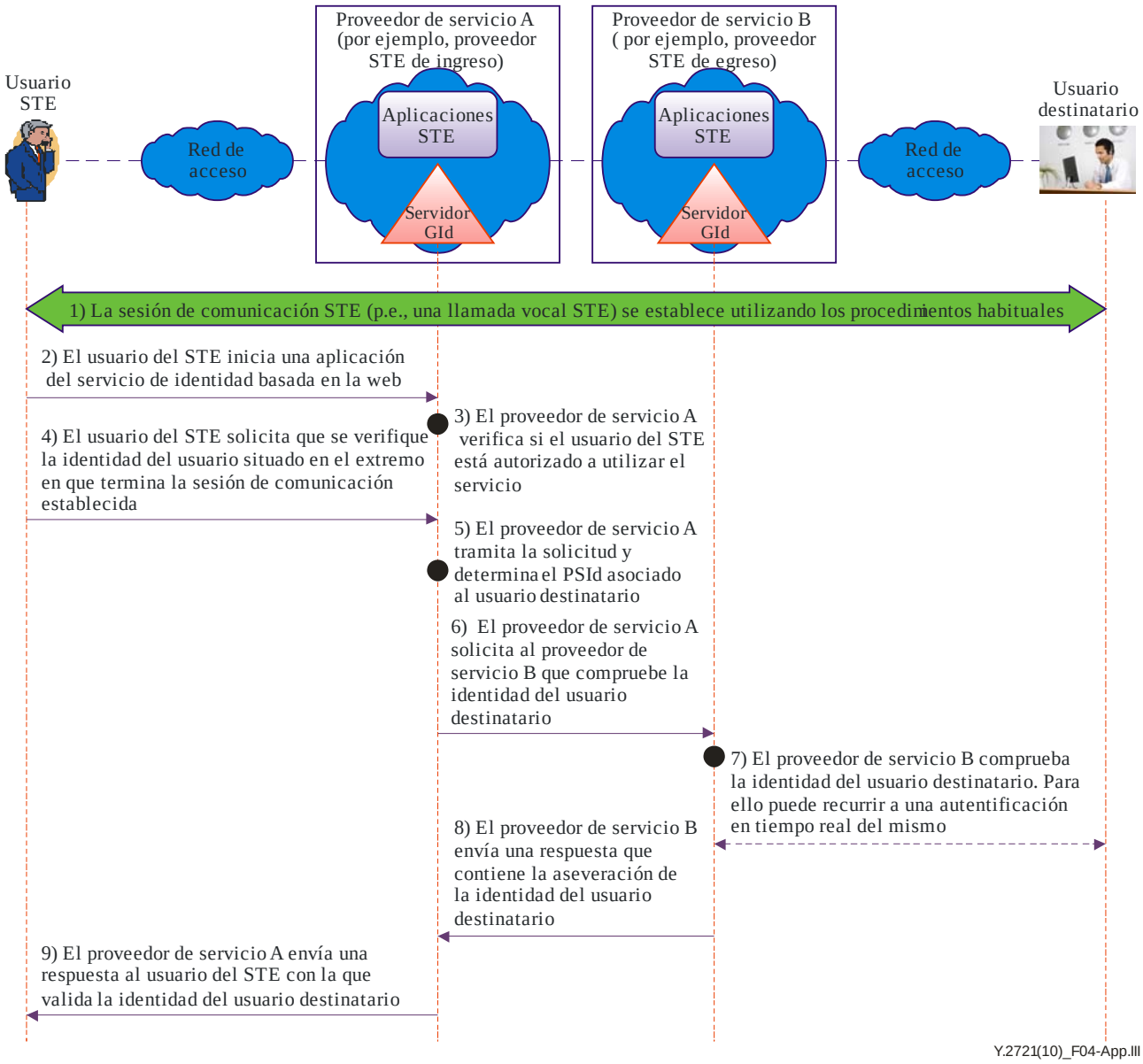
12) El PSId facilita a la entidad gubernamental información sobre la reautentificación del usuario del STE.

III.4 Autentificación de la parte llamada y del origen de la comunicación de datos

Actualmente las aplicaciones del STE no disponen de un mecanismo específico para autentificar la parte llamada de la sesión de comunicación (es decir, el lado en que termina la llamada del STE). En el entorno cerrado de la RTPC, ello no suponía problema alguno. Sin embargo, con la transición al entorno NGN/IMS con transporte por IP se abre la posibilidad de falsificar el número de parte llamada y la información de encaminamiento, lo que permite maquillar las amenazas.

En el futuro quizá sea posible mejorar los servicios de gestión de identidad ofrecidos por los proveedores de servicios de comunicaciones (PSC) y los proveedores de servicio terceros para autentificar la parte llamada o el lado en que terminan las sesiones de comunicaciones en el STE. Concretamente, el proveedor de servicio STE podría disponer de funciones GId para ofrecer servicios de identidad destinados a autentificar usuarios y aseverar la identidad de los mismos. Para garantizar la identidad del usuario podría recurrirse, por ejemplo, a verificar cierta información como el nombre del llamante y de la línea, o bien a mecanismos de autentificación más potentes tales como los testigos de seguridad, las tarjetas inteligentes o los certificados digitales.

En la figura III.4 se ilustra un ejemplo en el que se verifica el usuario destinatario de una sesión de comunicación del STE (por ejemplo una llamada vocal del STE). Concretamente, en este ejemplo se parte del supuesto de que el usuario STE se ha registrado previamente en el proveedor de servicio STE para servicios de identidad por la web. Tras establecer una comunicación STE (por ejemplo una llamada vocal del STE) hacia un usuario de la red pública, el usuario STE inicia el servicio de identidad a través del portal web con el fin de verificar la identidad del usuario destinatario de la llamada en el otro extremo de la comunicación del STE. En este ejemplo, el establecimiento de la sesión de comunicación del STE es independiente del servicio de identidad utilizado para comprobar la identidad del usuario destinatario.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.4 – Verificación de la identidad del usuario destinatario

A continuación se resume el flujo de llamada y las interacciones:

1) El usuario del STE inicia una sesión de comunicación STE (por ejemplo, una llamada vocal STE). La sesión se establece utilizando los procedimientos habituales.

2) El usuario del STE inicia un servicio de identidad basado en la web (por ejemplo a través del portal web del proveedor de servicio A, el proveedor STE de ingreso) para validar el usuario situado en el extremo en que termina la sesión de comunicación STE establecida.

3) El proveedor de servicio A verifica si el usuario del STE está autorizado a utilizar el servicio.

4) El usuario del STE solicita que se verifique la identidad del usuario situado en el extremo en que termina la sesión de comunicación establecida.

5) El proveedor de servicio A tramita la solicitud y determina el PSId asociado al usuario destinatario (es decir, el proveedor del STE de egreso).

6) El proveedor de servicio A envía una solicitud al proveedor del servicio B para que verifique la identidad del usuario de terminación.

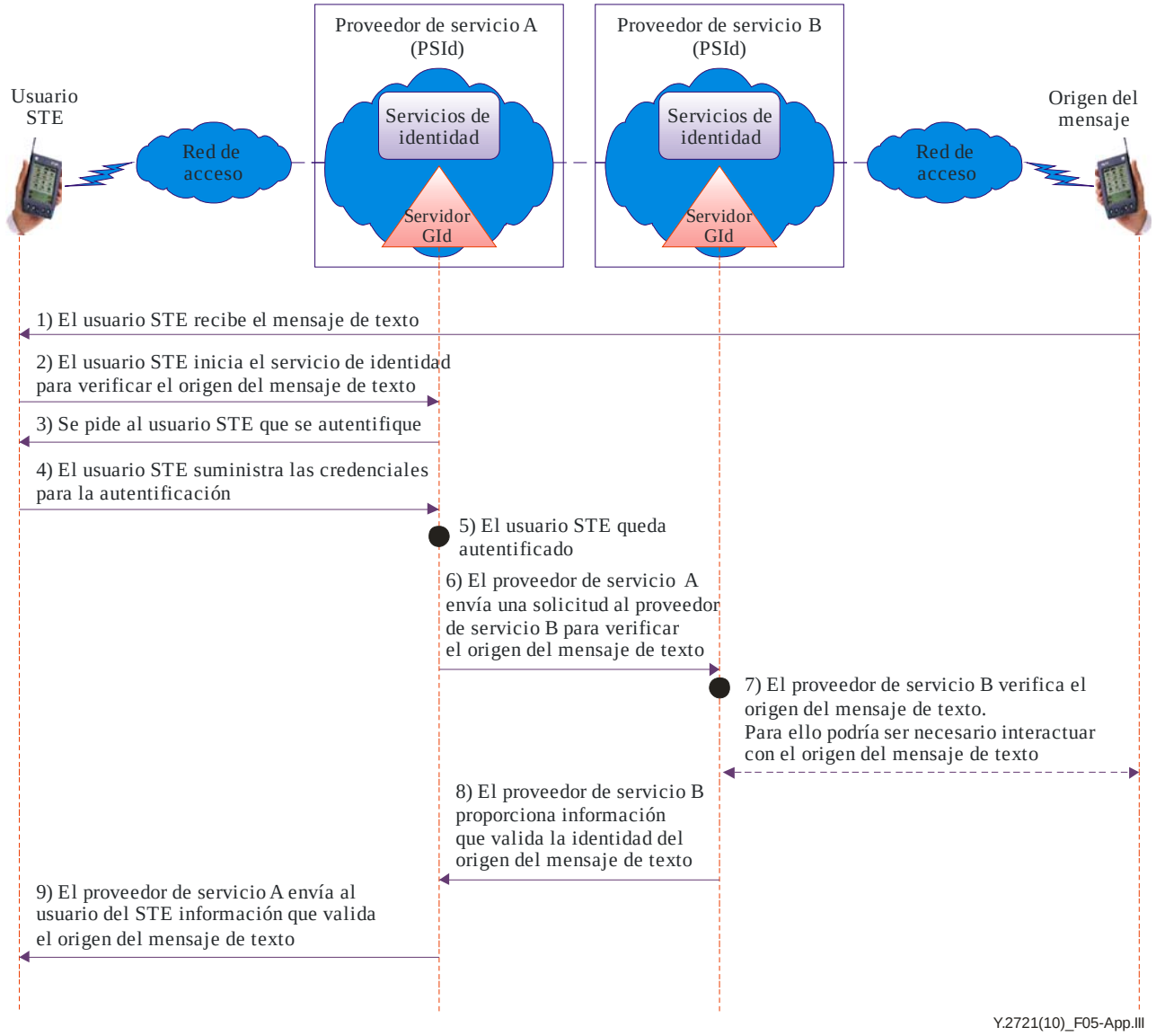
7) El proveedor de servicio B comprueba la identidad del usuario destinatario. Para ello puede recurrir a un autentificación en tiempo real del usuario destinatario.

8) El proveedor de servicio B envía una respuesta que contiene la aseveración de la identidad del usuario destinatario.

9) El proveedor de servicio A envía una respuesta al usuario del STE (por ejemplo un mensaje visual por la web) con el que valida la identidad del usuario de terminación de la sesión de comunicaciones del STE.

Por otra parte, los usuarios del STE dependen cada vez más de la utilización de servicios de datos, tales como el correo electrónico, la mensajería instantánea y la mensajería de texto. En determinadas situaciones puede ser necesario autentificar o validar el origen de tales servicios de datos. Dada la abundancia de correo basura, la capacidad de distinguir y validar mensajes auténticos en caso de catástrofe es fundamental para los usuarios del STE.

En la figura III.5 se muestra un ejemplo de verificación del origen de un mensaje de texto. En este ejemplo, se parte de la hipótesis de que el usuario del STE recibe un mensaje de texto procedente de una fuente que puede ser o no otro usuario del STE. Para asegurarse del origen del mensaje de texto, se recurre a los servicios de identidad de un proveedor de servicios. El servicio identidad que permite verificar el origen de mensaje de texto puede formar parte o no del propio servicio de mensajes de texto.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.5 – Verificación del origen del mensaje de texto

A continuación se resumen las interacciones:

1) El usuario del STE recibe el mensaje de texto.

2) El usuario del STE desea verificar la autenticidad del origen del mensaje de texto e inicia los servicios de identidad del proveedor de servicio A.

3) Se pide al usuario del STE que se autentifique.

4) El usuario del STE suministra las credenciales para la autentificación.

5) El proveedor de servicio A autentifica el usuario del STE y verifica si está autorizado para utilizar el servicio de identidad.

6) El proveedor de servicio A envía una solicitud al proveedor de servicio B para verificar el origen del mensaje de texto.

7) El proveedor de servicio B tramita la solicitud y verifica el origen del mensaje de texto. Para ello podría ser necesario interactuar con el origen del mensaje de texto.

8) El proveedor de servicio B envía una respuesta al proveedor de servicio A en la que asevera la identidad del origen del mensaje de texto.

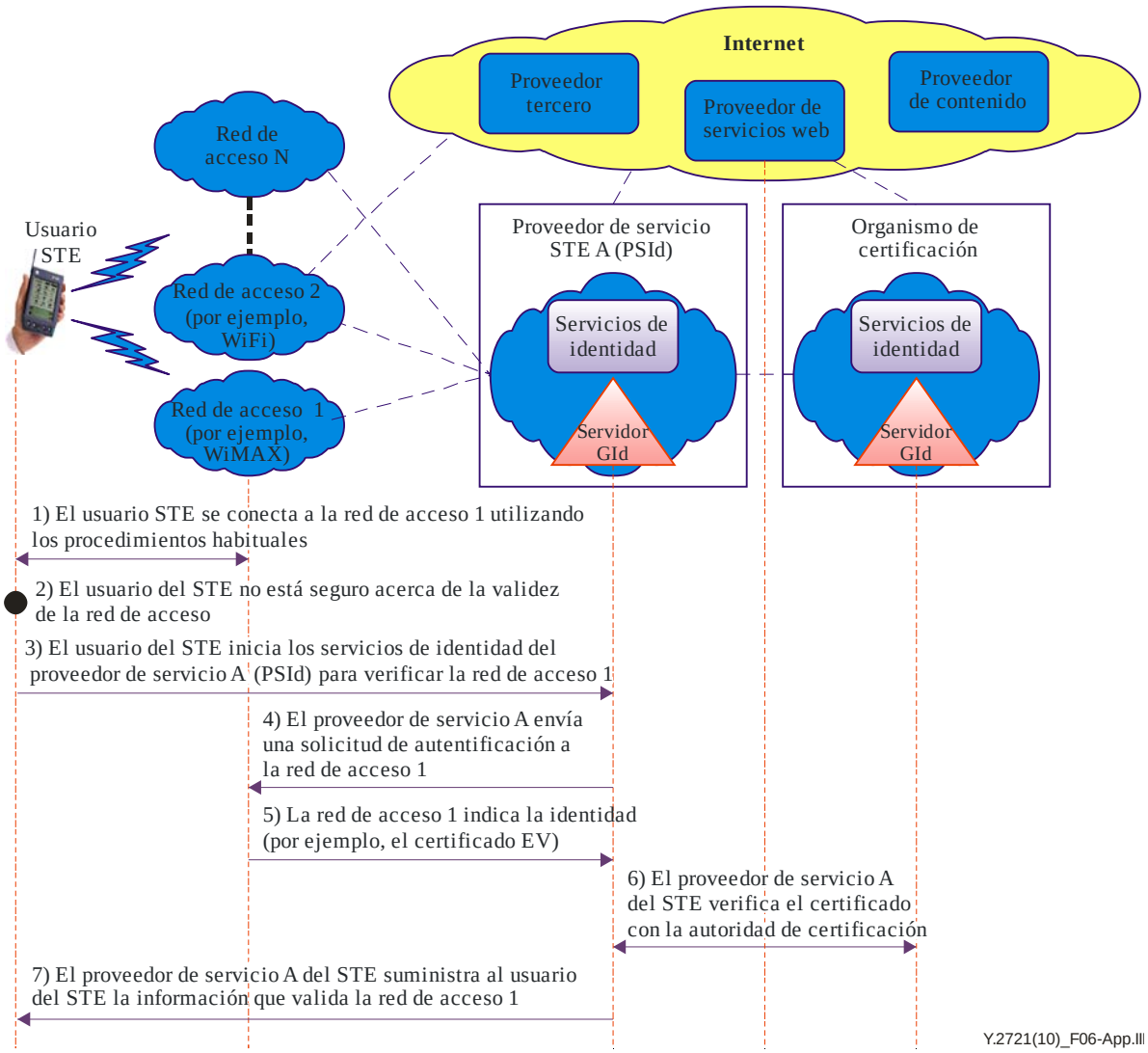
9) El proveedor de servicio A envía al usuario del STE información que valida el origen del mensaje de texto.

III.5 Identificación y autentificación fiables de proveedores de servicio en un entorno multiproveedor

La infraestructura de comunicaciones de hoy en día ha evolucionado hacia un entorno multiproveedor, formado por proveedores de acceso fijo y móvil que utilizan distintas tecnologías (por ejemplo, xDSL, cable, FTTX, WiFi, WiMAX, EV-DO, LTE), proveedores de servicios de comunicaciones que utilizarán "redes IP medulares gestionadas", proveedores de servicios web, proveedores de contenido y proveedores que actúan de terceros. En este entorno multiproveedor ya no es posible confiar de manera tácita en la identidad del proveedor de servicio como sucedía en el entorno cerrado de la RTPC.

Así pues, en el entorno abierto multiproveedor no existen funciones que permitan identificar, autentificar y autorizar de manera fiable a los proveedores de servicio, lo que abre la puerta al maquillaje ilegítimo de entidades, la falsificación y la suplantación de proveedores de servicios legítimos. Por consiguiente, las funciones GId para identificar y validar proveedores de servicio son esenciales para proteger la infraestructura. Además, cuando los proveedores de servicio ofrecen servicios STE, dichas funciones son indispensables para garantizar la seguridad nacional.

En la figura III.6 se muestra un ejemplo en el que el usuario del STE trata de obtener acceso a la red en un entorno multiproveedor. Concretamente, el usuario del STE se desplaza con un dispositivo móvil de bolsillo con el que puede conectarse a uno de los tantos proveedores de red de acceso que dan servicio en la zona en que se encuentra (no todos los proveedores de servicio están autorizados para ofrecer servicios STE). En este ejemplo, se parte del supuesto de que el usuario del STE se conecta preferentemente a la red de acceso 1. Una vez conectado a la red 1, el usuario del STE desea verificar la red antes de entablar comunicaciones STE importantes. Existen varias opciones y variantes para verificar el proveedor de la red de acceso, en particular la autentificación directa por parte del usuario del STE. En este ejemplo se supone que el usuario del STE recurre a los servicios de identidad que ofrece el proveedor de servicio A del STE para verificar la red de acceso. Además, el usuario del STE de este ejemplo confía en el proveedor de servicio A y acepta la información de validación que le envía dicho proveedor A en relación con la red de acceso 1.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.6 – Validación del proveedor del servicio de acceso

A continuación se resumen las interacciones:

1) El usuario del STE se desplaza con un dispositivo móvil de bolsillo que es capaz de conectarse a diferentes tipos de redes de acceso (por ejemplo, WiFi, WiMAX, LTE o EV-DO). El dispositivo móvil de bolsillo del usuario del STE se conecta a la red 1 (es decir, la opción preferente basada en factores tales como los proveedores de STE conocidos y la intensidad de la señal).

2) El usuario del STE desea verificar la red 1 antes de autorizar los servicios.

3) El usuario del STE inicia los servicios de identidad del proveedor de servicio A del STE para verificar la red de acceso 1.

4) El proveedor de servicio A envía una solicitud de autentificación a la red de acceso 1.

5) La red de acceso 1 proporciona información sobre identidad para la autentificación (por ejemplo, el certificado de validación ampliada de la UIT-T X.509).

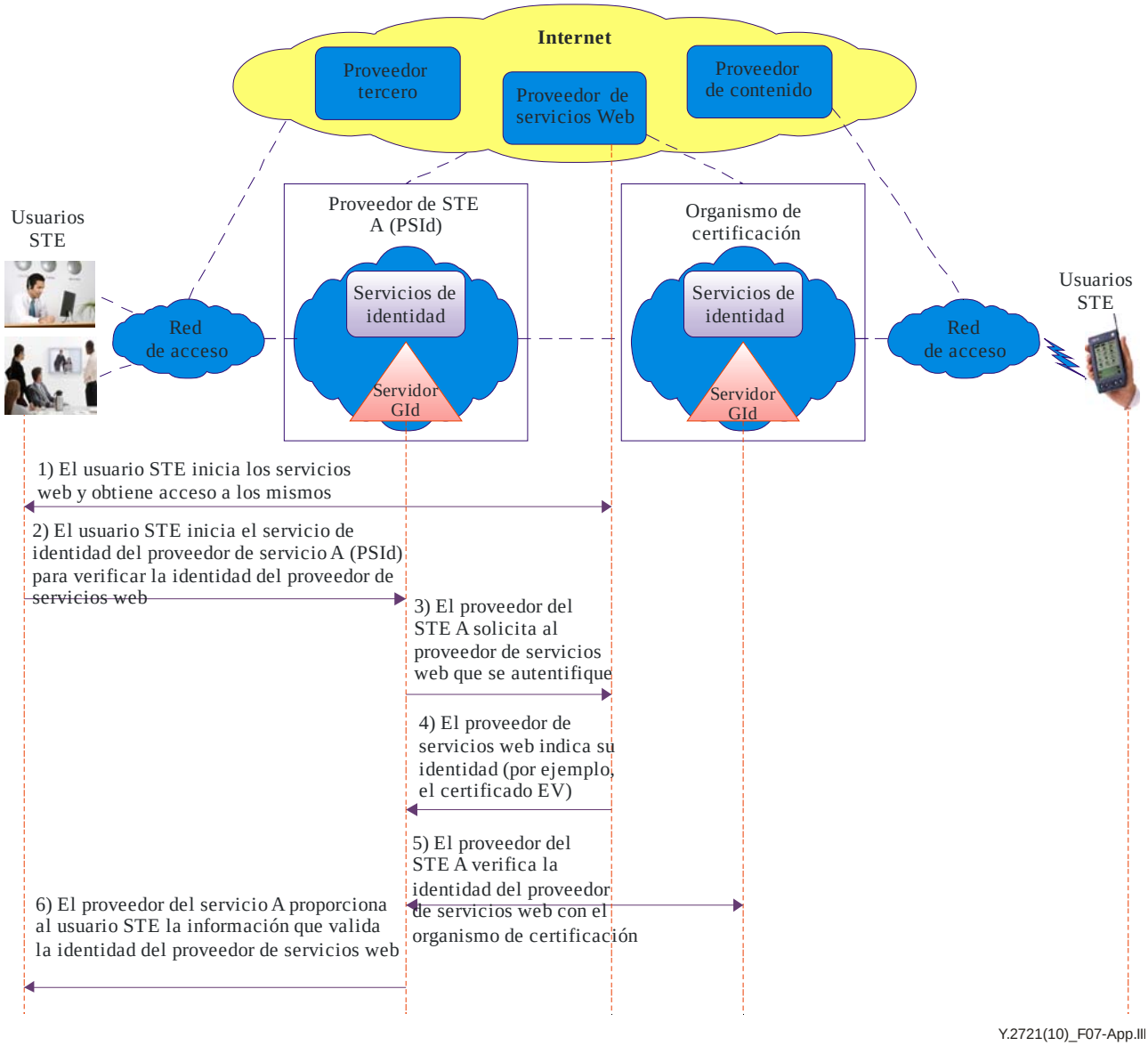
6) El proveedor de servicio A del STE verifica el certificado de la red 1 con la autoridad de certificación.

7) El proveedor de servicio A del STE suministra al usuario del STE la información que valida la red de acceso 1.

Este procedimiento permite al usuario del STE confiar en que su dispositivo móvil de bolsillo se ha conectado a una red de acceso autorizada.

Tras obtener la red de acceso, el usuario del STE podría utilizar los servicios de diversos proveedores de servicios en la infraestructura. Por ejemplo, puede darse el caso de que el usuario STE necesite utilizar los servicios de proveedores de servicios web (por ejemplo proveedores de datos/mapas de la Tierra o de otro tipo), o proveedores de contenido (por ejemplo, proveedores de servicios que ofrezcan transmisión en tiempo real de cámaras de vigilancia, informes meteorológicos o vídeo). También es posible que el usuario del STE pueda acceder a servicios web y a proveedores de contenido directamente a través del acceso a Internet o de manera indirecta a través de servicios de proveedores de NGN. En cualquiera de estos casos, el usuario del STE puede necesitar validar el proveedor de un determinado servicio.

En la figura III.7 se muestra un ejemplo en el que el usuario del STE necesita validar la identidad de un proveedor de servicios web. Al igual que en el ejemplo anterior, cabe considerar muchas opciones y variantes para validar el proveedor de servicios web, en particular la autentificación directa por parte del usuario del STE. En este ejemplo se parte del supuesto de que el usuario del STE utiliza los servicios de identidad del proveedor de servicio A del STE para validar el proveedor de servicio web. Al igual que el ejemplo anterior, el usuario del STE confía en el proveedor de servicios A y aceptará la información de validación que éste le proporcione acerca del proveedor de servicios web.



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.7 – Variación de un proveedor de servicio web o de contenido

A continuación se resumen las interacciones:

1) El usuario del STE inicia y accede a los servicios web. Ahora bien, el usuario del STE desea validar el proveedor de servicios web para confiar en los datos que éste le suministra.

2) El usuario del STE inicia el servicio de identidad del proveedor A del STE para validar la identidad del proveedor de servicios web.

3) El proveedor de servicio A del STE solicita al proveedor de servicios web que se autentifique.

4) El proveedor de servicios web proporciona información para autentificarse (por ejemplo, el certificado EV[1]).

[1] El certificado de validación ampliada (EV) es un tipo especial de certificado UIT-T X.509 que exige al organismo de certificación una amplia investigación de la entidad solicitante antes de su expedición.

5) El proveedor de servicio A del STE verifica la información con el organismo de certificación.

6) El proveedor de servicio A del STE proporciona al usuario STE la información que valida la identidad del proveedor de servicios web.

La validación del proveedor de servicios web permite al usuario del STE confiar en la identidad del proveedor de servicios web y, por ende, aumenta su confianza en la información que obtiene del mismo.

III.6 Inicio y cierre de sesión únicos

Por regla general, los usuarios tienen que realizar el inicio de sesión en múltiples sistemas que contienen los servicios de aplicación (por ejemplo, VoIP, datos y vídeo), para lo cual han de rellenar un número equivalente de cuadros de diálogo de inicio de sesión, cada uno de los cuales requiere distintos nombres de usuarios y de información de autentificación. Así pues los administradores de sistema tienen que gestionar las cuentas de usuario para cada uno de estos múltiples sistemas y coordinarlos de manera que se apliquen las políticas de seguridad.

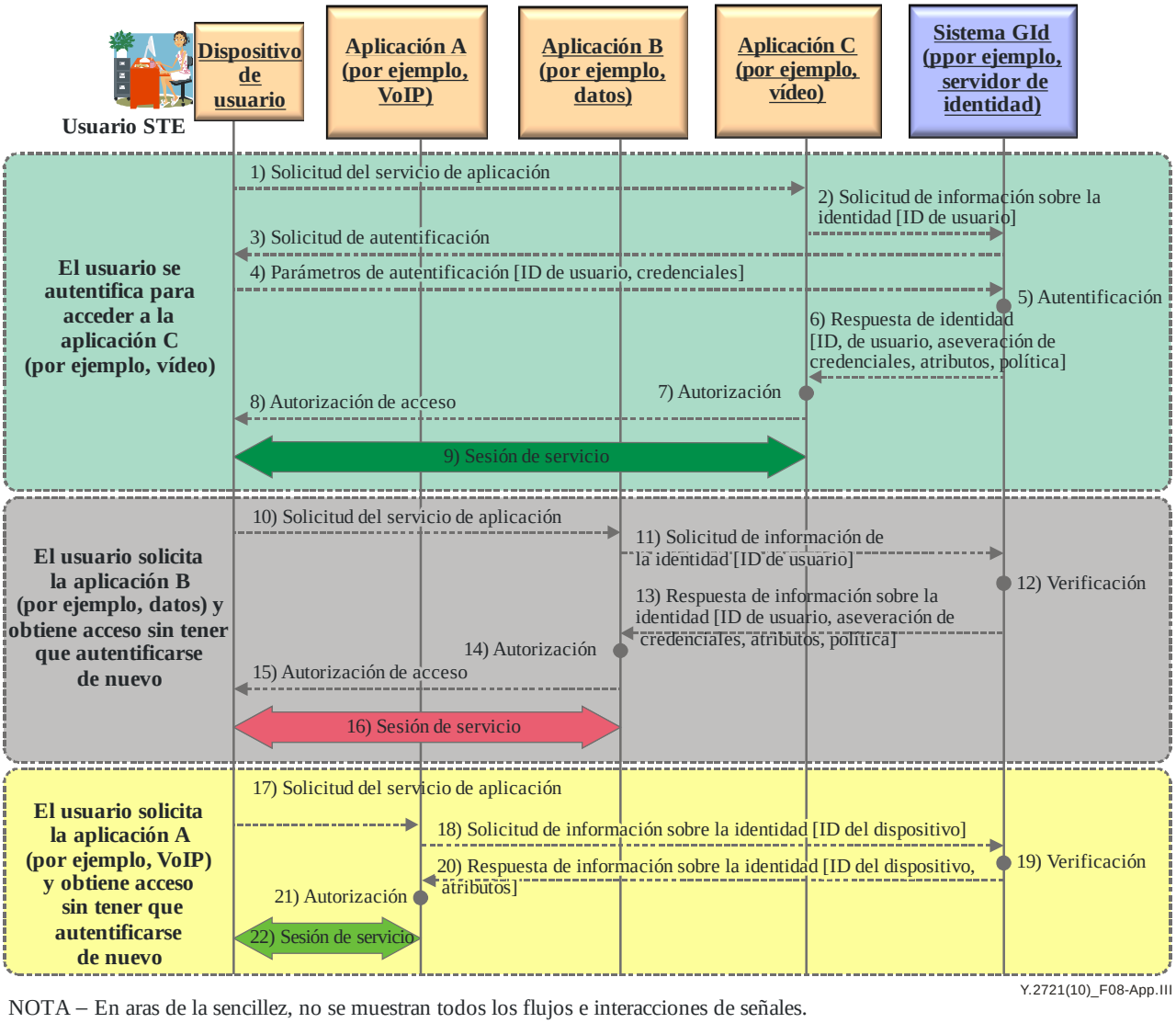
Los usuarios del STE quizá necesiten potenciar las funciones de GId tales como el "inicio/cierre de sesión único". El inicio de sesión único consiste en que un determinado usuario, dispositivo o una combinación de usuario y dispositivo pueden iniciar una sesión para un servicio (es decir, proporcionar las credenciales para la autentificación y la autorización) y quedar así autentificado para uno o varios servicios adicionales en el mismo dominio NGN, o en el caso de servicios federados, a través de varios dominios NGN. La ventaja del inicio de sesión único es que el usuario no tiene la ardua tarea de tener que autentificarse para cada servicio. Por "inicio de sesión" en este contexto se entiende lo mismo que el procedimiento de "registrarse" o "entrar" en el sistema con el que el usuario o dispositivo accede a un servicio. Análogamente, el "cierre de sesión único" permite efectuar de una vez el "cierre de sesión" de varios servicios de aplicaciones en una determinada sesión.

Entre las ventajas que supone para el usuario del STE las funciones de inicio/cierre de sesión único cabe citar las siguientes:

- Reducción del tiempo necesario para iniciar una sesión en cada uno de los dominios, y por tanto la reducción del número de errores de inicio de sesión. También se aumenta la seguridad gracias a que el usuario ya no tiene que gestionar y recordar varios pares de información de autentificación.
- Reducción del tiempo que tarda el administrador del sistema en añadir o eliminar usuarios del sistema o modificar sus derechos de acceso.
- Aumento de la seguridad, ya que resulta más fácil al administrador del sistema mantener la integridad de la configuración de las cuentas de usuario, en particular para impedir o suprimir el acceso por un determinado usuario a todos los recursos del sistema de una manera coherente y consistente.

En la figura III.8 se ilustra un ejemplo en el que se recurre a un sistema GId para el "inicio/cierre de sesión único" de varios servicios de aplicación (por ejemplo, VoIP, datos y vídeo), dentro del dominio de un proveedor NGN. En este caso es necesaria la interacción entre las siguientes entidades:

- Usuarios (es decir, el usuario y/o su dispositivo).
- Sistema de retransmisión (esto es, el servicio de aplicación o el sistema de red).
- El sistema GId (es decir, el sistema de red que ofrece los servicios de GId tales como registro, autentificación y autorización, así como la información sobre el perfil del abonado).



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales.

Figura III.8 – Inicio de sesión único

En este ejemplo se parte del supuesto de que el dispositivo de usuario se ha registrado y conectado a la NGN siguiendo los procedimientos habituales.

Los flujos de llamada son los siguientes:

1) Solicitud del servicio de aplicación: Este flujo de información representa la solicitud procedente del usuario del STE para invocar el servicio de aplicación C (vídeo).

2) Solicitud de información sobre la identidad [ID de usuario]: El servicio de aplicación C (vídeo) envía una solicitud al sistema GId para aseverar la identidad del usuario y proporcionar los atributos asociados al ID del usuario. Podría tratarse de información como el perfil de servicio, los privilegios, las preferencias y la política, por ejemplo, toda política o restricción aplicable a dicha identidad.

3) Solicitud de autentificación: El sistema GId solicita al usuario que se autentifique.

4) Parámetros de autentificación [credenciales]: El usuario facilita información para autentificarse (por ejemplo, el ID de usuario y la contraseña o su número de identificación personal).

5) Autentificación: El sistema GId realiza la autentificación y obtiene otra información necesaria. Para ello quizá hay de obtener información de otros sistemas de red (por ejemplo, HSS u otra base de datos de suscripciones).

6) Respuesta de identidad [aseveración de credenciales, atributos, política]: El sistema GId facilita la información para aseverar las credenciales. Podría incluir otra información, como por ejemplo atributos asociados al ID de usuario (tales como privilegios y preferencias) y política aplicable a dicha identidad (restricciones de utilización, de visualización o de divulgación).

7) Autorización: El servicio de aplicación C (vídeo) procesa la información y determina si el usuario está autorizado a utilizar el servicio.

8) Autorización de acceso: El servicio de aplicación C (vídeo) informa al usuario de que se le ha concedido acceso al servicio.

9) Sesión de servicio: Se establece la sesión del usuario con el servicio de aplicación C (vídeo).

10) Solicitud del servicio de aplicación: El usuario solicita acceder al servicio de aplicación B (datos).

11) Solicitud de información de la identidad [ID de usuario]: El servicio de aplicación B (datos) solicita al sistema GId que verifique la identidad del usuario y proporcione los atributos asociados al mismo. Podría tratarse de información como el perfil de servicio, los privilegios, las preferencias y la política, por ejemplo, toda política o restricción aplicable a dicha identidad.

12) Verificación: El sistema GId procesa la solicitud, determina si el inicio de sesión único es aplicable y verifica que la autentificación del usuario sigue siendo válida.

13) Respuesta de información sobre la identidad [aseveración de credenciales, atributos, política]: El sistema GId facilita la información para aseverar las credenciales. Podría incluir otra información, como por ejemplo atributos asociados al ID de usuario (tales como privilegios y preferencias) y política aplicable a dicha identidad (restricciones de utilización, de visualización o de divulgación).

14) Autorización: El servicio de aplicación B (datos) procesa la información y determina si el usuario está autorizado a utilizar el servicio.

15) Autorización de acceso: El servicio de aplicación B (datos) informa al usuario de que se le ha concedido acceso al servicio.

16) Sesión de servicio: Se inicia la sesión del usuario con el servicio de aplicación B (datos).

17) Solicitud del servicio de aplicación: El usuario solicita acceder al servicio de aplicación A (VoIP).

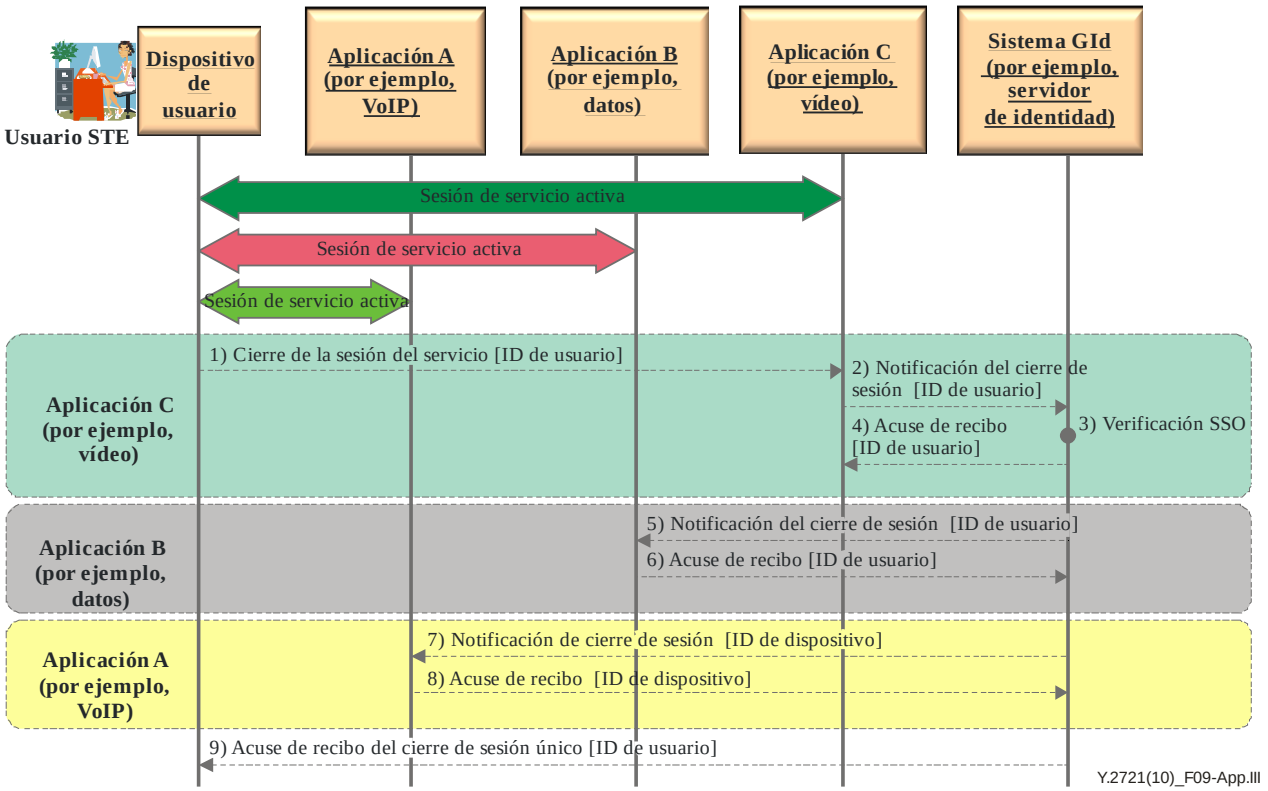
18) Solicitud de información sobre la identidad [ID del dispositivo]: El servicio de aplicación A (VoIP) solicita al sistema GId que verifique la identidad del usuario y proporcione los atributos asociados al ID del dispositivo.

19) Verificación: El sistema GId procesa la solicitud, determina si el inicio de sesión único es aplicable y verifica que la autentificación del usuario sigue siendo válida.

20) Respuesta de información sobre la identidad [aseveración de credenciales, atributos, política]: El sistema GId facilita la información para aseverar las credenciales. Podría incluir otra información, como por ejemplo atributos asociados al ID del dispositivo (tales como privilegios y preferencias) y política aplicable a dicha identidad (restricciones de utilización, de visualización o de divulgación).

21) Autorización: El servicio de aplicación A (VoIP) procesa la información y determina si el usuario está autorizado a utilizar el servicio.

22) Sesión de servicio de aplicación: Se inicia la sesión del usuario con el servicio de aplicación A (VoIP).



NOTA – En aras de la sencillez, no se muestran todos los flujos e interacciones de señales

Figura III.9 – Cierre de sesión único

La figura III.9 muestra un servicio de "inicio de sesión único" que permite al usuario iniciar automáticamente la sesión de varios servicios de aplicación (VoIP, datos y vídeo) sin tener que cerrar la sesión de cada servicio de aplicación abierto. En este ejemplo se parte de la hipótesis de que el usuario tiene abierta una sesión de servicio con los servicios de aplicación activos A (VoIP), B (datos) y C (vídeo).

Los flujos de llamada son los siguientes:

1) Cierre de la sesión del servicio [ID de usuario]: El usuario del STE solicita terminar la sesión del servicio.

2) Notificación del cierre de sesión [ID de usuario]: El servicio de aplicación C (vídeo) notifica al sistema GId que el usuario ha solicitado el cierre de la sesión.

3) Verificación SSO: El sistema GId determina si el cierre de sesión único es aplicable y verifica los servicios de aplicación activos.

4) Acuse de recibo [ID de usuario]: El sistema GId acusa recibo al servicio de aplicación C (vídeo) para cerrar la sesión de servicio.

5) Notificación del cierre de sesión [ID de usuario]: El sistema GId notifica al servicio de aplicación B (datos) del cierre de la sesión.

6) Acuse de recibo [ID de usuario]: El servicio de aplicación B (datos) acusa recibo del cierre de sesión.

7) Notificación del cierre de sesión [ID de dispositivo]: El sistema GId notifica al servicio de aplicación A (VoIP) del cierre de la sesión.

8) Acuse de recibo [ID de dispositivo]: El servicio de aplicación A (VoIP) acusa recibo del cierre de sesión.

9) Acuse de recibo del cierre de sesión único [ID de usuario]: El sistema GId acusa recibo al usuario confirmándole que se han cerrado todos los servicios de aplicación activos en la sesión.

Apéndice IV

Casos de utilización en el entorno móvil

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

IV.1 Introducción

En esta sección se dan ejemplos de utilización de la GId en el contexto móvil. Los ejemplos se basan en casos de utilización descritos en el documento blanco de 3G Américas, *Identity Management: Overview of Standards and Technologies for Mobile and Fixed Internet* [b-3G Americas White Paper].

IV.2 Ejemplos de utilización

IV.2.1 Usuario móvil con un dispositivo 3G dotado de UICC accede al portal de un ORM (tienda por la web) para comprar una melodía para su teléfono.

Actores:

- Usuario móvil.
- ORM (operador de red móvil).
- PS (proveedor de servicio), que es el ORM.

Ventajas para el usuario:

- Inicio de sesión único con acceso a distintos servicios del ORM.

Principales restricciones:

- El PS y el ORM están en el mismo círculo de confianza (conforme a Liberty Alliance).

IV.2.2 El usuario móvil con un dispositivo 3G dotado de UICC accede al portal de la tienda web del ORM; recorre el catálogo digital de productos hasta dar con una oferta especial (por ejemplo un videojuego, para el que el ORM dispone de un contrato de distribución de contenido exclusivo) y efectúa una compra; luego selecciona efectuar el pago con cargo a su factura de teléfono móvil; el usuario puede descargar el videojuego desde un enlace seguro remitido desde el ORM hasta el proveedor de contenido.

Actores:

- Usuario móvil.
- ORM.
- PS-a, que es el ORM; PS-b, que es el proveedor de contenido externo (en este caso, el videojuego).

Ventajas para el usuario:

- Inicio de sesión único para el portal del ORM y del vendedor externo.
- Posibilidad de utilizar sus credenciales con el ORM para efectuar la transacción con el proveedor de contenido externo.

Principales restricciones:

- El PS-a (ORM) y el PS-b (proveedor de contenido del videojuego) están en el mismo círculo de confianza.

IV.2.3 El usuario móvil utiliza su teléfono inteligente 3G dotado de UICC desde otro país; al navegar por la red se inscribe a una revista extranjera de automóviles y lo paga con su tarjeta de crédito (los atributos de su perfil de usuario que mantiene su ORM se revelan selectivamente para completar el procedimiento de inscripción a la revista); la empresa de tarjeta de crédito autoriza el pago al portal de la revista en nombre del usuario móvil.

Actores:

- Usuario móvil.
- ORM.
- PS-a que es el proveedor de contenido (revista de automóvil); PS-b, que es la empresa de tarjetas de crédito.

Ventajas para el usuario:

- Inicio de sesión único para su ORM y la empresa de tarjetas de crédito.
- Posibilidad de utilizar sus credenciales con el ORM para autorizar el pago a la empresa de tarjetas de crédito y completar así la transacción con el proveedor de contenido externo.
- Posibilidad de reutilizar los atributos personales de su perfil de abonado al ORM para inscribirse a un servicio externo, por lo que ha de introducir mucha menos información.

Principales restricciones:

- El ORM y el PS-b (empresa de tarjetas de crédito) están en el mismo círculo de confianza.
- El PS-a (proveedor de la revista de automóviles extranjero) no forma parte del círculo de confianza.

IV.2.4 El usuario móvil utiliza su computador portátil 3G dotado de UICC desde otro país y, mientras espera en el aeropuerto se inscribe al servicio WiFi del aeropuerto durante varias horas; el operador WLAN tiene un acuerdo con el ORM del usuario en virtud del cual acepta que el coste de la conexión WiFi se cargue en su factura de teléfono móvil; además, una vez conectado al servicio WiFi el usuario accede a diversos portales web que consulta frecuentemente, en particular un banco, una agencia de viajes y una empresa de inversiones financieras; el usuario desea utilizar los servicios que ofrecen estas empresas sin tener que volver a iniciar la sesión y poder intercambiar información personal de manera segura.

Actores:

- Usuario móvil.
- Operador de WLAN.
- ORM.
- PS-a (el ORM); PS-b (el banco), PS-c (la agencia de viajes) y PS-d (la empresa de inversiones financieras).

Ventajas para el usuario:

- Inicio de sesión único para su ORM y el operador WiFi.
- Posibilidad de utilizar sus credenciales con el ORM para autorizar el pago por el servicio WiFi.
- Posibilidad de acceder a varios proveedores de servicios web que no están asociados con el ORG a través de procedimientos de inscripción simplificados y transferencia segura de información privada.

Principales restricciones:

- El ORM y el operador WLAN pertenecen al mismo círculo de confianza.
- El PS-a (banco), el PS-b (agencia de viajes) y el PS-c (empresa de inversiones financieras) no pertenecen al mismo círculo de confianza.

IV.2.5 El usuario móvil utiliza su computador portátil 3G dotado de UICC desde su casa, navega por Internet a través de su servicio DSL residencial de banda ancha mediante el cual accede al portal de su ORM; paga su factura por el servicio móvil (utilizando su tarjeta de crédito, cuya autorización previa está almacenada) y añade una nueva función a su inscripción móvil; a continuación se conecta a un sitio de alquiler de películas y se baja una con cargo a su tarjeta de crédito (no autorizado previamente).

Actores:

- Usuario móvil.
- Operador de red fija DSL.
- ORM.
- PS-a (ORM); PS-b (portal de alquiler de películas); PS-c (empresa de tarjetas de crédito).

Ventajas para el usuario:

- Inicio de sesión único para su operador de red fija y el ORM.
- Posibilidad de utilizar sus credenciales con el operador de red fija para autentificar su cuenta de servicio móvil y solicitar servicios adicionales del ORM.
- Posibilidad de autorizar que se cargue a su tarjeta de crédito las compras de contenido a un proveedor de servicio externo (por ejemplo, alquiler de películas).

Principales restricciones:

- El ORM, el operador de red fija y el PS-b (empresa de tarjetas de crédito) pertenecen al mismo círculo de confianza.
- El PS-c (portal de alquiler de películas) no pertenece al mismo círculo de confianza.

IV.2.6 El usuario móvil desea utilizar su dispositivo 3G dotado de UICC para acceder a recursos (por ejemplo, un servicio de directorio de empresas) situado en la red de una empresa.

Actores:

- Usuario móvil.
- ORM.
- Sistema GId de la empresa.
- Servicio de servicios de directorio de la empresa (servidor SDE).

A continuación se describen las interacciones a alto nivel entre estos actores.

- El usuario móvil solicita el servicio del servidor SDE.
- El servidor SDE pide al usuario que se autentifique.
- El usuario, que ya ha sido autentificado por el sistema del ORM, obtiene las credenciales de autentificación de éste para autentificarse ante el sistema GId de la empresa.
- El usuario presenta las credenciales al sistema GId de la empresa y, una vez autentificado correctamente, obtiene de éste las credenciales para autentificarse ante el servidor SDE.
- El usuario responde a la solicitud del servidor SDE con las credenciales recibidas del sistema GId de la empresa.
- El usuario obtiene acceso al servicio solicitado del servidor SDE.

Ventajas para el usuario:

- El usuario móvil puede acceder a los recursos disponibles en su red empresarial (por ejemplo, el servicio de directorio de la empresa) de manera rentable y cumpliendo los requisitos de seguridad estrictos que suelen aplicarse en los sistemas de tecnología de la información de las empresas.

Principales restricciones:

- El Sistema de GId de la empresa puede exigir la autentificación basada en dos factores (por ejemplo ID del usuario/contraseña/PIN), además de las credenciales de usuario facilitadas por el ORM.
- Los sistemas de GId del ORM y de la empresa pertenecen al mismo círculo de confianza.

Apéndice V

Ejemplos de modelos de transacciones GId

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

V.1 Introducción

En el presente apéndice se dan ejemplos de modelos de transacción para GId. Los modelos que se indican en este apéndice se describen en [b-UIT-T X.1250]. También son posibles otros modelos distintos a los que se mencionan en este apéndice.

V.2 Ejemplos de posibles modelos de transacción para la gestión de identidades

Una de las transacciones básicas en la gestión de identidad es el proceso de autentificación que se indica en la figura V.1. La forma más básica de autentificación consiste en que las dos partes utilizan un protocolo y un modelo de información convenido de antemano.

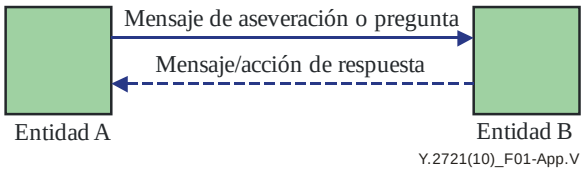


Figura V.1 – Proceso de intercambio de información básico basado en pregunta/respuesta

En el proceso de autentificación pueden participar todo tipo de entidades, ya sea personas físicas, animales, personas jurídicas, organizaciones, componentes activos o pasivos, dispositivos, aplicaciones software, servicios, etc., o un conjunto de éstos. En el contexto de las telecomunicaciones, las entidades pueden ser puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones software, servicios y dispositivos, interfaces, etc. Puede tratarse de cualquier objeto físico o virtual, por ejemplo equipo de red, software, dispositivos de terminal, sensores, objetos físicos etiquetados activamente (por ejemplo, mediante RFID o códigos ópticos), objetos etiquetados pasivamente. Así por ejemplo, los dispositivos de red pueden considerarse entidades sujetas a registros especiales de GId en nombre de usuarios, proveedores o autoridades públicas. En el contexto de la gestión de derechos digitales, la entidad considerada puede ser un material protegido por propiedad intelectual o derecho de autor, por ejemplo, contenido multimedios o TVIP. Un tipo especial de entidad es el que representa el grupo. La identidad de un grupo es la intersección del conjunto de identidades (atributos comunes) de cada miembro del grupo.

En la mayoría de los casos en que se recurre a la gestión de identidad interviene un proceso complejo, según el cual la parte que recibe originalmente la declaración no es el proveedor de servicio de identidad. Como puede verse en la figuras V.2 y V.3, la función que corresponde a un proveedor de entidad en cuanto tal está separada y es distinta de la parte dependiente. La función principal de la parte dependiente consiste en interpretar la respuesta del proveedor de servicio de identidad y decidir si la confianza en la legitimidad de la identidad alegada alcanza un nivel suficiente. La función principal del proveedor de servicio de identidad es gestionar la creación, actualización, verificación, suspensión y supresión de la información sobre la identidad.

Existen muchos modelos posibles para el intercambio de información sobre identidad. Uno bastante utilizado es el modelo tripartito de respuesta a una pregunta que se muestra en la figura V.2. Algunos de los nuevos protocolos GId abiertos se basan en este modelo.

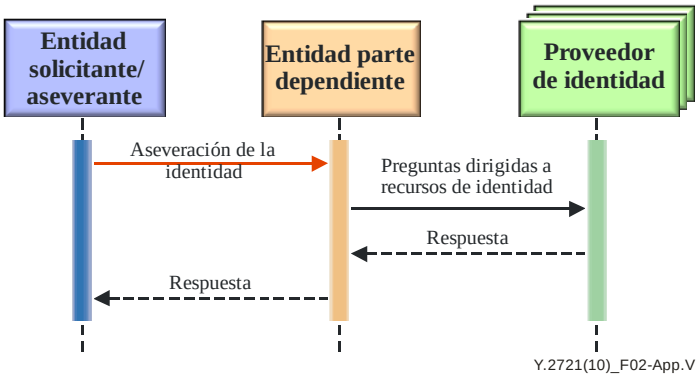


Figura V.2 – Ejemplo de modelo de gestión de identidad tripartito

En la figura V.3 se muestra otro modelo de gestión de identidad que proporciona a la parte solicitante mayor control de las relaciones de identidad.

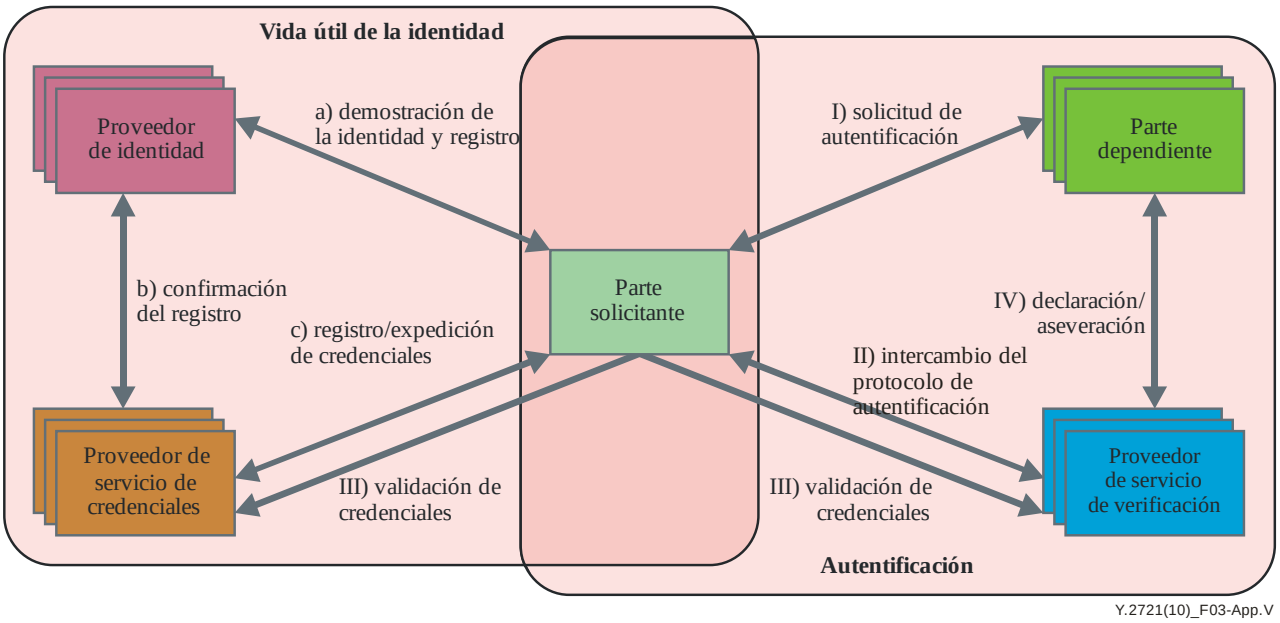


Figura V.3 – Ejemplo de modelo de gestión de la identidad pentapartito centrado en el usuario

Los modelos "centrados en el usuario" (es decir, que requieren la activación del control total de la parte solicitante sobre la utilización de sus identidades) están recibiendo considerable atención y en algunas jurisdicciones nacionales o regionales pueden incluso ser obligatorios. En la figura V.3 se muestra un ejemplo en el que distintos proveedores de servicios ofrecen funciones y capacidades especializadas para la gestión de identidades. Todas las preguntas/respuestas se dirigen a la parte solicitante. A los efectos de estos tipos de modelo, se definen las siguientes entidades:

- Proveedor de servicio de identidad: Una entidad que mantiene, gestiona y puede crear información sobre identidad fiable de otras entidades (por ejemplo, usuarios, organizaciones y dispositivos) y que ofrece servicios basados en la identidad. Esta entidad responsable de asignar y expedir atributos (relacionados con la identidad (por ejemplo, para un abonado a un proveedor de credenciales) en un contexto específico) -también denominado inscripción- se encarga de la gestión de la identidad a lo largo de toda la vida útil, en particular la demostración, inscripción y mantenimiento de la identidad, así como su revocación.

- Proveedor de servicio de credenciales: La entidad que ejerce funciones relativas a la expedición de credenciales y testigos (por ejemplo, credenciales que vinculan testigos con identificadores y atributos verificables).
- Proveedor del servicio de verificación: La entidad que ofrece capacidades para evaluar la información sobre identidad (por ejemplo, declaraciones y credenciales) y que clasifica su validez.
- Parte dependiente [UIT-T Y.2720]: Entidad que depende de una representación o declaración de identidad de una entidad solicitante/acertante en un determinado contexto.

Apéndice VI

Ejemplo ilustrativo de implantación de GId en las NGN

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

VI.1 Introducción

En este apéndice se describe un ejemplo de implantación de GId en las NGN.

VI.2 Arquitectura de instalación del GId

Las NGN pueden instalar infraestructura GId con funciones para servicios basados en identidad a sus usuarios, lo que mejora las capacidades y especificaciones de los servicios web definidos por el proyecto Liberty Alliance y OpenID, por ejemplo, las capacidades de GId que permiten a sus usuarios acceder a servicios y aplicaciones de distintos proveedores, incluidos los servicios de aplicación federados. Además, las NGN pueden recurrir a capacidades GId para ofrecer servicios de proveedor de servicio de identidad (PSId) a otros proveedores de servicios y aplicaciones (por ejemplo, aseveración de la identidad del usuario y autentificación, localización y otra información relacionada con la identidad).

Para facilitar capacidades de GId que permitan ofrecer servicios PSId y/o colaborar con otros proveedores de servicios o aplicaciones que utilizan diferentes tipos de sistemas de GId basados en semánticas, esquemas, tecnologías y mecanismos distintos, será necesario disponer de funciones de adaptación y de compatibilidad. Por ejemplo, para poder emplear las capacidades y el servicio GId con otros proveedores de servicios y aplicaciones (por ejemplo, proveedores de contenido y de servicios web), las NGN podrían disponer de capacidades para lo siguiente:

- Interfuncionamiento 3GPP GBA con el marco de Liberty Alliance.
- Interfuncionamiento 3GPP GBA con OpenID.
- Otros mecanismos de interfuncionamiento con OpenID y el marco Liberty Alliance.

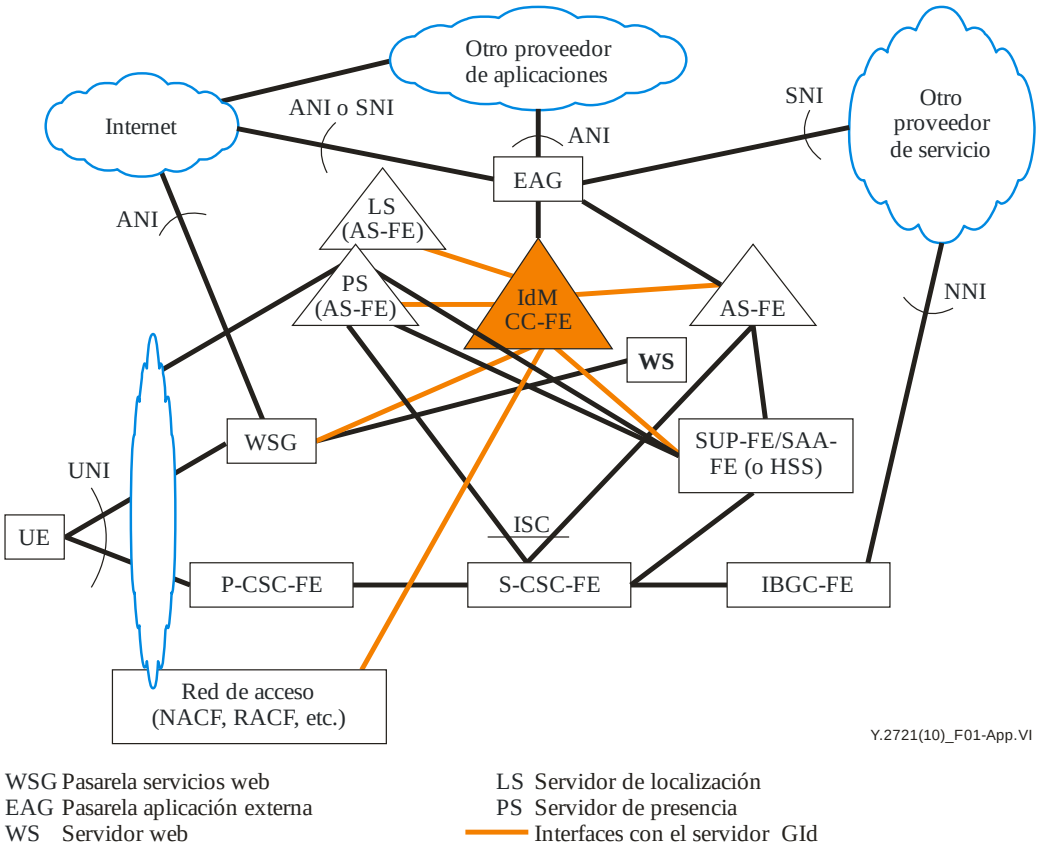


Figura VI.1 – Ejemplo de despliegue de GId en las NGN

En la figura VI.1 se muestra un ejemplo de implantación de la GId para las NGN. En este ejemplo se muestra la utilización de un servido GId que puede consistir en un sistema autónomo o un conjunto de funciones distribuidas, y/o estar situado en el HSS. El servicio GId actúa de interfaz e interactúa con los elementos de red que ejercen de entidades funcionales para las NGN. Por ejemplo, el servidor GId puede actuar de interfaz con:

- Los servidores de aplicación que facilitan el servicio, tales como un servidor de localización o un servidor de presencia, u otras aplicaciones con el fin de proporcionar un elevado nivel de garantía de autentificación y ofrecer servicios de aplicación basados en la identidad.
- Servidores de control, política y conexión para garantizar la autentificación y la gestión de políticas.

NOTA – En determinados reglamentos nacionales, lo anterior se traduce en crear funciones GId separadas en los diferentes estratos de las NGN.

Para ofrecer ciertos servicios de GId a los usuarios/abonados y prestar servicios PSId o de colaboración en materia de GId a otros proveedores de servicios y aplicaciones, las NGN tendrán que disponer de capacidades específicas que les permitan controlar el acceso y el intercambio de GId con otros proveedores de servicios y aplicaciones (por ejemplo, servicios web y proveedores de contenido). En este ejemplo ilustrativo se muestra cómo utilizar una pasarela de servicios web (WSG) y una pasarela de aplicaciones externas (EAG) para ofrecer servicios de GId que mejoran o colaboran con otros proveedores de servicios y aplicaciones. Concretamente, la figura VI.1 muestra el servidor GId que actúa de interfaz con el usuario a través de la pasarela de servicios web (WSG) que autentifica al usuario y le ofrece una interfaz para gestionar su perfil de identidad. En caso necesario, también se puede emplear la autentificación mutua entre el usuario y el proveedor de servicio. El servidor GId también actúa de interfaz con una pasarela de aplicación externa (EAG) que permite al usuario acceder a los servicios web de la NGN o de otros proveedores de servicios y aplicaciones.

Bibliografía

[b-UIT-T X.1141] Recomendación UIT-T X.1141 (2006), *Lenguaje de etiquetas de asertos de seguridad (SAML 2.0)*.

[b-UIT-T X.1250] Recomendación UIT-T X.1250 (2009), *Capacidades básicas para una confiabilidad y una interoperabilidad mejoradas de la gestión de identidad global*.

[b-UIT-T X.1251] Recomendación UIT-T X.1251 (2009), *Marco para el control por el usuario de la identidad digital*.

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

[b-NIST SP 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.

[b-NIST SP 800-94] NIST Special Publication 800-94 (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-CA/Browser Forum] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*.

[b-3G Americas White Paper] 3G Americas White Paper (2009), Identity Management: *Overview of Standards and Technologies for Mobile and Fixed Internet*.

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, 2012