



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.350

(08/2003)

SERIE H: SISTEMAS AUDIOVISUALES Y
MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Sistemas y
equipos terminales para los servicios audiovisuales

**Arquitectura de servicios de directorio para
conferencia multimedios**

Recomendación UIT-T H.350

RECOMENDACIONES UIT-T DE LA SERIE H
SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
SISTEMAS Y EQUIPOS TERMINALES PARA LOS SERVICIOS AUDIOVISUALES	H.300–H.399
SERVICIOS SUPLEMENTARIOS PARA MULTIMEDIOS	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedia de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedia	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedia	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedia	H.540–H.549
Procedimientos de interfuncionamiento de la movilidad	H.550–H.559
Procedimientos de interfuncionamiento de colaboración en móviles multimedia	H.560–H.569
SERVICIOS DE BANDA ANCHA Y DE TRÍADA MULTIMEDIOS	
Servicios multimedia de banda ancha sobre VDSL	H.610–H.619

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

Recomendación UIT-T H.350

Arquitectura de servicios de directorio para conferencia multimedios

Resumen

En esta Recomendación se describe una arquitectura de servicios de directorio para conferencia multimedios utilizando LDAP. Los servicios de directorio normalizados soportan la asociación de personas con puntos extremos, las páginas blancas susceptibles de búsqueda y la marcación mediante clics. Los servicios de directorio también pueden ayudar a configurar puntos extremos y a autenticar usuarios en base a fuentes de datos autorizadas. En esta Recomendación se describe un esquema LDAP normalizado para representar puntos extremos en la red y asociar dichos puntos extremos a usuarios. Se analizan consideraciones de diseño e implementación para la interrelación de directorios de vídeo y de voz, directorios de empresa, servidores de llamada y puntos extremos.

Orígenes

La Recomendación UIT-T H.350 fue aprobada por la Comisión de Estudio 16 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8 el 6 de agosto de 2003.

Palabras clave

H.235, H.320, H.323, LDAP, servicios de directorio, SIP.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) 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.

© UIT 2004

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
1.1 Objetivos de diseño	2
1.2 Ampliación del esquema	3
2 Referencias	4
2.1 Referencias normativas	5
2.2 Referencias informativas	5
3 Definiciones.....	5
4 Abreviaturas.....	5
5 Convenios	6
6 Definición de commURIObject.....	6
6.1 commURIObject.....	6
6.2 commURI	6
7 Definición de CommObject.....	7
7.1 commObject	7
7.2 commUniqueId	7
7.3 commOwner	8
7.4 commPrivate.....	8
8 Ficheros LDIF CommObject	9
8.1 LDIF para commURIObject.....	9
8.2 LDIF para commObject.....	10
Anexo A – Perfil de indexación.....	12
Apéndice I – Consideraciones relativas a la implementación.....	12
I.1 Relaciones entre directorios de empresas y directorios commObject.....	12
Apéndice II – Flujos de llamada	14
II.1 Escenarios de flujos de llamada	14
Apéndice III – Ficheros electrónicos	17

Recomendación UIT-T H.350

Arquitectura de servicios de directorio para conferencia multimedios

1 Alcance

En esta Recomendación se describe una arquitectura de servicios de directorio para conferencia multimedios utilizando LDAP. Los servicios de directorio normalizados soportan la asociación de personas con puntos extremos, páginas blancas susceptibles de búsqueda y marcación mediante clics. Los servicios de directorio también pueden ayudar a configurar puntos extremos y autenticar usuarios en base a fuentes de datos autorizadas. En esta Recomendación se describe un esquema LDAP normalizado para representar puntos extremos de la red y asociar dichos puntos extremos a usuarios. Se analizan aspectos de diseño e implementación para la interrelación de directorios de vídeo y de voz, directorios de empresa, servidores de llamadas y puntos extremos.

La utilización de una fuente de datos autorizada y común para información del servidor de llamadas, punto extremo, usuario, autenticación y páginas blancas es un aspecto importante de los entornos de conferencia multimedios de gran tamaño. Sin una fuente de datos comunes, los proveedores de servicio deben crear procesos separados para gestionar cada una de dichas funciones. La normalización del esquema LDAP utilizado para representar los datos subyacentes, permite que los productos de distintos vendedores de sistemas puedan desplegarse conjuntamente para crear un entorno de aplicación global. Por ejemplo, una máquina de búsqueda para páginas blancas desarrollada por un proveedor puede ser utilizada para información de directorios de teléfonos IP elaborada por otro proveedor, utilizando un servidor de llamadas de un tercer proveedor para gestionar la señalización. Cada uno de estos sistemas diferenciados puede acceder a la misma fuente de datos subyacentes, reduciendo o eliminando la necesidad de coordinar la gestión independiente de cada sistema. Un beneficio significativo para el usuario es que la gestión de estos datos puede incorporarse en las herramientas de gestión de clientes existentes, permitiendo así un crecimiento o escalado flexible y rápido de las aplicaciones. Ciertamente, numerosos proveedores de tecnología ya han incorporado LDAP a sus productos, pero se han visto forzados a hacerlo sin beneficiarse de un esquema normalizado. Esta Recomendación constituye un esfuerzo para normalizar dichas representaciones a fin de mejorar la interoperabilidad y las prestaciones.

Si bien las URL ya están normalizadas para varios protocolos de conferencia, no ocurre lo mismo en lo que se refiere a su representación en un directorio. Esta Recomendación soporta una forma normalizada para la búsqueda y localización de las URL. Constituye un paso necesario para soportar la 'marcación mediante clics'.

La gestión de las configuraciones de puntos extremos puede mejorarse si el proveedor de servicio almacena los valores correctos en una ubicación accesible tanto para el proveedor de servicio como para el punto extremo. LDAP proporciona una ubicación de almacenamiento conveniente accesible para el servidor de llamadas y para el punto extremo; por lo tanto, es posible utilizar el directorio para la configuración del punto extremo, lo cual es importante en aras de una operación simplificada y para soportar la movilidad de los usuarios. Nótese que otras tecnologías también soportan la configuración de puntos extremos, notablemente el SNMP para la configuración completa y los registros SRV para obtener direcciones de servidores de registro. Por lo tanto, esta Recomendación H.350 no debería verse como una arquitectura autorizada para la configuración de puntos extremos, sino como una herramienta que puede ayudar a realizar dicha tarea. Nótese que la utilización de H.350 tiene una característica de configuración específica de puntos extremos, para la que es recomendable que cada punto extremo tenga una configuración específica.

Esta arquitectura utiliza una clase objeto genérica, denominada commObject, para representar atributos comunes a cualquier protocolo de vídeo o voz. Las clases auxiliares representan protocolos específicos tales como H.323, H.235 o H.320, tal como se describe en las

Recomendaciones de la serie H.350.x. Las distintas clases H.350.x pueden combinarse para representar puntos extremos que soporten más de un protocolo. Por ejemplo, los puntos extremos que soporten H.323, H.235 y H.320 incluyen H.350, H.350.1, H.350.2 y H.350.3 en sus representaciones LDAP. Además, cada entrada debe contener commObject que sirva como clase objeto estructural de la entrada.

Existen dos componentes básicas en la arquitectura. El objeto commURI es una clase cuyo único propósito es vincular una persona o un recurso a un commObject. Situando un 'puntero' commURI en la entrada correspondiente a un individuo del directorio, se asocia dicho individuo con el commObject objetivo. Igualmente, commObject contiene un puntero denominado commOwner que apunta al individuo o recurso asociado con commObject. De esta forma, personas o recursos pueden asociarse con puntos extremos. El único cambio que es necesario en el directorio de empresas es la adición de la clase de objeto simple commURI. Los datos commObject pueden incorporarse en el mismo directorio o en directorios completamente separados, permitiendo así una gran flexibilidad en la implementación.

1.1 Objetivos de diseño

Los despliegues a gran escala de servicios de vídeo y voz sobre IP han demostrado la necesidad de un elemento de intermediación complementario para los servicios de directorio. Los administradores de servicios necesitan servidores de llamadas que conozcan los directorios de empresa para evitar duplicación en los procesos de gestión de cuentas. Los usuarios necesitan las 'páginas blancas' para localizar a otros usuarios con los que deseen comunicarse. Todos estos procesos deberían recuperar la información que necesitan de fuentes de datos canónicas a fin de reducir procesos administrativos redundantes y asegurar la exactitud de la información. Para esta arquitectura, se han establecido los criterios de diseño siguientes. La arquitectura:

- 1) Permitirá asociar información de punto extremo con personas. Alternativamente, debe permitir que la información de punto extremo se asocie con recursos, tales como salas de conferencia o aulas.
- 2) Permitirá la existencia de "páginas blancas" sobre las que se puedan realizar búsquedas en línea y en las que la información de marcación (por ejemplo las direcciones de los puntos extremos) pueda encontrarse junto con otra información "tradicional" del usuario incluida en el directorio, tales como nombre, dirección, teléfono, correo electrónico, etc.
- 3) Permitirá que la información sobre punto extremo se almacene en una fuente de datos canónica (el directorio), en lugar de hacerlo en una local asociada al servidor de llamadas, de forma que los puntos extremos pueden ser gestionados accediendo a un directorio de empresa en lugar de hacerlo mediante un acceso directo al servidor de llamadas.
- 4) Soportará la creación de directorios distribuidos de gran tamaño. Éstos deben incluir "portales" de páginas blancas que permitan la búsqueda de usuarios a través de múltiples directorios institucionales. En esta aplicación, cada directorio de empresa se registra en un directorio de directorios (o bien éste detecta la presencia de aquél inadvertidamente) que puede realizar búsquedas en múltiples directorios LDAP.
- 5) Soportará múltiples ejemplares de puntos extremos por cada usuario o recurso.
- 6) Representará puntos extremos que soporten más de un protocolo, por ejemplo puntos extremos que sean tanto H.320 como H.323.
- 7) Almacenará suficiente información sobre la configuración de los puntos extremos de forma que los valores de configuración correcta se documenten en los usuarios finales para cada punto extremo, a modo de herramienta de soporte, o cargado automáticamente en el punto extremo.
- 8) Será ampliable, en la medida que sea necesario, para permitir la implementación de atributos específicos.

- 9) No invadirá el ámbito del directorio de empresa de forma que el soporte de la conferencia multimedia pueda realizarse en forma modular sin cambios significativos en el directorio de empresa.

El alcance de esta Recomendación no incluye la extensión de funcionalidades a protocolos tal como están definidas en dichos protocolos. No es el objetivo de esta Recomendación añadir prestaciones, sino sencillamente representar los atributos de protocolo existentes. Se produce una excepción cuando el propio directorio implica una funcionalidad, como por ejemplo, el atributo `commPrivate`.

1.2 Ampliación del esquema

Las clases de objeto H.350 pueden ampliarse en la medida que sea necesario para implementaciones específicas. Por ejemplo, una clase puede ampliarse para soportar códigos de referencia de facturación. Las ampliaciones del esquema no se consideran parte de la Recomendación y no traen consigo la obligación de cumplimiento.

En algunos casos puede ser necesario ampliar los esquemas H.350 a fin de representar información adicional a la soportada por las Recomendaciones. Esto puede ser importante para desarrolladores que implementen alguna funcionalidad de punto extremo no normalizada que deba ser representada mediante atributos en el directorio. También puede ser importante para aplicaciones de empresa. Por ejemplo 'modelNumber' y 'accountNumber' son ejemplos de atributos que no están definidos en la Recomendación pero que pueden ser útiles si se implementan. La adición de atributos a esta arquitectura debe hacerse manteniendo la compatibilidad con esta Recomendación.

Queda fuera del ámbito de esta Recomendación hacer un análisis completo del diseño y ampliación de esquemas. Para más información, véase RFC 2252 del IETF. Dos métodos básicos para la ampliación de esquemas que no infringen la compatibilidad con esta Recomendación son la ampliación mediante subclase y la ampliación mediante clases auxiliares.

1.2.1 Ampliación mediante subclases

Es posible crear subclases de una clase objeto predefinida existente a fin de añadirle nuevos atributos. Para crear una subclase, debe definirse un nuevo objeto clase que sea una subclase de otro existente, indicando en la definición de la nueva clase que la clase existente es su superior. Una vez que se ha creado la subclase, pueden definirse nuevos atributos de la misma.

El ejemplo siguiente muestra cómo la clase `commObject` puede ser ordenada en subclases a fin de añadir un atributo que represente una cuenta de facturación y un gestor de facturación.

```
objectclass ( BillingInfo-OID
NAME 'BillingInfo'
DESC 'Billing Reference Information'
SUP commObject STRUCTURAL
MAY ( BillingAccount $ BillingManager $ )
)
```

Nótese que `BillingInfo-OID` debe ser sustituida por un OID real. También debe señalarse que siempre que se amplíe una clase estructural, su subclase también debe ser estructural.

El ejemplo de entrada siguiente muestra los atributos recién creados. Este ejemplo también utiliza la Rec. UIT-T H.350.1 para `h323Identity`.

```
dn: commUniqueId=2000,ou=h323identity, dc=company, dc=com
objectclass: top
objectclass: commObject
objectclass: h323Identity
objectclass: BillingInfo
commUniqueId: 2000
BillingAccount: 0023456
BillingManager: John Smith
```

Nótese que este ejemplo y el método utilizado sólo supone la ampliación del objeto clase `commObject` general, y no ninguna de las clases H.350.x individuales. Si se desea ampliar una clase auxiliar H.350.x, ello debería hacerse mediante la definición de clases auxiliares adicionales que soporten los atributos deseados tal como se describe en 1.2.2.

1.2.2 Ampliación mediante clases auxiliares

Es posible añadir atributos a una entrada LDAP definiendo una clase auxiliar que contenga los nuevos atributos y aplicando dichos atributos a valores ejemplificados en el directorio. La clase auxiliar no debe ser clasificada en subclases a partir de un objeto clase existente. Nótese que su superior (SUP) debe ser la clase especial "top" (arriba). En el ejemplo siguiente se crean los mismos atributos de cuenta de facturación y gestor de facturación que en el ejemplo anterior, pero se hace definiéndolos en su propia clase auxiliar.

```
objectclass ( BillingInfo-OID
NAME 'BillingInfo'
DESC 'Billing Reference Information'
SUP top AUXILIARY
MAY ( BillingAccount $ BillingManager $ )
)
```

Nótese que se modificó el superior de `commObject` "top" (arriba), y la clase objeto pasó de ser estructural a auxiliar.

Se recomienda que todos los atributos de la clase auxiliar sean opcionales en lugar de obligatorios. De esta forma, la clase objeto auxiliar puede asociarse con una entrada con independencia de si algunos de los valores de sus atributos están presentes.

El ejemplo siguiente muestra un punto extremo que utiliza la nueva clase auxiliar y atributos. Este ejemplo también utiliza H.350.1 para `h323Identity`.

```
dn: commUniqueId=2000,ou=h323identity, dc=company, dc=com
objectclass: top
objectclass: commObject
objectclass: BillingInfo
commUniqueId: 2000
BillingAccount: 0023456
BillingManager: John Smith
```

1.2.3 Identificadores de objeto

El identificador de objeto (OID, *object identifier*) de un atributo es un identificador numérico exclusivo que normalmente se escribe como una secuencia de enteros separados por puntos. Por ejemplo, el OID de `commUniqueId` es 0.0.8.350.1.1.2.1.1. Todos los atributos deben tener un OID. Los OID pueden obtenerse de cualquiera que disponga de uno y esté dispuesto a delegar una parte o arco del mismo, manteniendo un registro de los arcos delegados a fin de evitar duplicaciones. Además, la autoridad de asignación de números Internet (IANA, *Internet assigned numbers authority*) entrega los OID que le solicite cualquier organización.

2 Referencias

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

2.1 Referencias normativas

- IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification*.

2.2 Referencias informativas

- Recomendación UIT-T H.225.0 (2003), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.
- Recomendación UIT-T H.235 (2003), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.
- Recomendación UIT-T H.320 (1999), *Sistemas y equipos terminales videotelefónicos de banda estrecha*.
- Recomendación UIT-T H.323 (2003), *Sistemas de comunicación multimedios basados en paquetes*.
- HOWES (Timothy A.), PhD, SMITH (Mark C.), GOOD (Gordon S.): *Understanding And Deploying LDAP Directory Services*, New Riders Publishing, 1999, ISBN: 1578700701.
- HOWES (Timothy A.), PhD, SMITH (Mark C.): *LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*, New Riders Publishing, 1997, ISBN: 1578700000.

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 servidor de llamadas: Máquina de señalización específica para cada protocolo que encamina llamadas de vídeo o de voz sobre la red. En la Rec. UIT-T H.323, esta entidad es un controlador de acceso. En SIP, esta entidad es un servidor apoderado y SIP. Nótese que no todos los protocolos de señalización utilizan un servidor de llamadas.

3.2 punto extremo: Dispositivo lógico que proporciona la codificación/decodificación de medios de vídeo y/o voz, así como funciones de señalización. Son ejemplos de ello:

- 1) un grupo de dispositivos de teleconferencia situados en una sala de conferencia;
- 2) un teléfono IP;
- 3) un programa que tome señales de vídeo y de voz de una cámara y un micrófono, las codifique y aplique señalización utilizando una computadora anfitriona.

3.3 directorio de empresa: Colección canónica de información sobre usuarios de una organización. Típicamente, esta información se recopila de las diversas unidades de la organización. Por ejemplo, Recursos Humanos puede proporcionar el nombre y la dirección, Telecomunicaciones puede proporcionar el número de teléfono, Tecnología de la Información puede proporcionar la dirección de correo electrónico, etc. A los efectos de esta arquitectura, se supone que un directorio de empresas es accesible a través de LDAP.

3.4 páginas blancas: Aplicación que permite a los usuarios finales buscar la dirección de otro usuario. Puede estar basada en web o utilizar algún otro tipo de interfaz.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas:

CN Nombre común (*common name*)

- DN Nombre distinguido (*distinguished name*)
- LDAP Protocolo ligero de acceso al directorio (tal como se define en RFC 1777) (*lightweight directory access protocol*)
- RDN Nombre distinguido relativo (*relative distinguished name*)

5 Convenios

En esta Recomendación se utilizan los convenios siguientes:

El tiempo futuro o la expresión "deberá" indican un requisito obligatorio.

El condicional "debería" indica una forma de proceder aconsejada pero no exigida.

"Puede" o "podrá" indica una forma de proceder opcional más que una recomendación de que algo tenga lugar.

Las referencias a cláusulas, subcláusulas, anexos y apéndices hacen referencia a dichos elementos de esta Recomendación, salvo que explícitamente se mencione otra especificación.

6 Definición de commURIObject

Clase objeto auxiliar que contiene el atributo commURI. Este atributo se añade a un objeto persona o recurso para asociar uno o más ejemplares de commObject a dicho objeto. Sus valores son URI de LDAP que apuntan a los commObjects asociados, por ejemplo a un equipo de conferencia H.323 de un usuario y a un teléfono IP SIP. Nótese que los múltiples ejemplares de commURI no necesitan apuntar al mismo directorio commObject. De hecho, cada ejemplar de commURI podría apuntar a un punto extremo gestionado por un proveedor de servicio diferente.

6.1 commURIObject

```
OID: 0.0.8.350.1.1.1.2.1
objectclasses: (0.0.8.350.1.1.1.2.1
NAME 'commURIObject'
DESC 'object that contains the URI attribute type'
SUP top AUXILIARY
MAY ( commURI )
)
```

6.2 commURI

```
OID: 0.0.8.350.1.1.1.1.1
attributetypes: ( 0.0.8.350.1.1.1.1.1
NAME 'commURI'
DESC 'Labeled URI format to point to the distinguished name of the commUniqueId'
EQUALITY caseExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Clase utilidad de aplicación

normalizada

Número de valores

múltiples

Definición

URI etiquetada que contiene una URL LDAP que identifica al directorio que incluye el ejemplar commObject referenciado. El filtro de búsqueda especificado por dicha URL LDAP especificará una búsqueda basada en la igualdad del atributo commUniqueId de la clase commObject.

Valores admisibles (si están controlados)

Notas

Utilizado para encontrar el punto extremo del usuario en cuestión. El campo etiqueta puede utilizarse para representar la función del punto extremo, como por ejemplo 'teléfono IP del hogar' o 'equipo de vídeo de escritorio' al objeto de representar la interfaz de usuario.

Nótese que la porción de la etiqueta del campo puede contener espacios, como ocurre en el ejemplo siguiente que muestra un 'equipo de vídeo de escritorio'.

Semánticas

Ejemplo de aplicaciones para las cuales este atributo sería útil

Ejemplo (fragmento LDIF)

```
commURI: ldap://directory.acme.com/dc=acme,dc=com??sub?(commUniqueId=bob)
desktop video
```

7 Definición de CommObject

Abstracción de vídeo o de voz sobre un dispositivo IP. La clase commObject permite representar un punto extremo (punto extremo H.323 o agente de usuario SIP u otro punto extremo de protocolo) y todos sus alias mediante una única entrada del directorio. Nótese que cada entrada del directorio debiera incluir commObject como la clase objeto estructural correspondiente a la entrada. Dicha entrada puede asimismo incluir clases auxiliares H.350.x.

7.1 commObject

```
OID: 0.0.8.350.1.1.2.2.1
objectclasses: (0.0.8.350.1.1.2.2.1
NAME 'commObject'
DESC 'object that contains the Communication attributes'
SUP top STRUCTURAL
MUST commUniqueId
MAY ( commOwner $ commPrivate )
)
```

7.2 commUniqueId

```
OID: 0.0.8.350.1.1.2.1.1
attributetypes: (0.0.8.350.1.1.2.1.1
NAME 'commUniqueId'
DESC 'To hold the endpoints unique Id'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Clase utilidad de aplicación

normalizada

Número de valores

múltiples

Definición

ID singular del punto extremo.

Valores admisibles (si están controlados)

Notas

Es el RDN de este objeto. En la práctica habrá siempre exclusivamente un `commUniqueId` para cada punto extremo. Este atributo identifica inequívocamente un punto extremo en el directorio `commObject`. Debe ser único en dicho directorio, pero no es necesario que sea único globalmente. Este atributo no tiene relación alguna con el directorio de empresa.

Semánticas

Ejemplo de aplicaciones para las cuales este atributo sería útil

Ejemplo (fragmento LDIF)

```
commUniqueId: bob
```

7.3 commOwner

```
OID: 0.0.8.350.1.1.2.1.2
attributetypes: 0.0.8.350.1.1.2.1.2
NAME 'commOwner'
DESC 'Labeled URI to point back to the original owner'
EQUALITY caseExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Clase utilidad de aplicación

normalizada

Número de valores

múltiples

Definición

Formato de URI etiquetado para apuntar al objeto persona o recurso asociado con esta entrada.

Valores admisibles (si están controlados)

Notas

Se utiliza como buscador inverso del propietario o propietarios. Este atributo puede apuntar a grupos. Nótese que este URI puede apuntar a un `cn`, pero en aplicaciones en las que se desea vincular información de autenticación de los directorios de empresa y `commObject`, puede ser conveniente que el `commOwner` apunte a un `dn` en lugar de a un `cn`, de forma que se identifique inequívocamente al propietario del `commObject`.

Semánticas

Ejemplo de aplicaciones para las cuales este atributo sería útil

Ejemplo (fragmento LDIF)

```
commOwner: ldap://directory.acme.com/dc=acme,dc=com??sub?(cn=bob%20smith)
commOwner: uid=bob,ou=people,dc=acme,dc=com
```

7.4 commPrivate

```
OID: 0.0.8.350.1.1.2.1.3
attributetypes: (0.0.8.350.1.1.2.1.3
NAME 'commPrivate'
DESC 'To decide whether the entry is visible to world or not'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Clase utilidad de aplicación

normalizada

Número de valores

múltiples

Definición

Para ser utilizado por el usuario e indicar las opciones de privacidad de un punto extremo, es decir un número no incluido en la lista.

Valores admisibles (si están controlados)

Notas

Este atributo se define como booleano. En versiones futuras de esta Recomendación se podrá desarrollar un vocabulario controlado para este atributo a fin de incluir múltiples tipos de privacidad.

Semánticas

Ejemplo de aplicaciones para las cuales este atributo sería útil

Ejemplo (fragmento LDIF)

```
commPrivate: true
```

8 Ficheros LDIF CommObject

En esta cláusula se incluye un fichero de configuración de esquema para commURIObject y commObject, que puede ser utilizado para configurar un servidor LDAP a fin de que soporte estas clases.

8.1 LDIF para commURIObject

```
# Esquema del objeto comunicación
#
# Esquema para representar objetos de comunicación en un directorio LDAP
#
# Resumen
#
# En esta Recomendación se define el esquema para representar objetos
# comunicación en un directorio LDAP [LDAPv3]. Define elementos del esquema
# para representar el URI de un objeto de comunicación [commURIObject].
#
#
#
#           .1 = Actividad relacionada con la comunicación
#           .1.1 = commURIObject
#           .1.1.1 = atributos
#           .1.1.2 = objectclass
#           .1.1.3 = syntax
#
# Definiciones de tipos de atributos
#
#   En esta Recomendación se definen los tipos de atributos siguientes:
#
#           commURI
dn: cn=schema
changetype: modify
#
# si es necesario modificar la definición de un atributo,
#           en primer lugar realícese la supresión y la nueva adición en un
#           solo paso
#
# si es la primera vez que añade la clase objeto commObject
# utilizando este fichero LDIF, se debe desactivar, con el
# correspondiente símbolo de comentario la modificación de supresión de
# attributetypes, ya que ésta fallará.
# Alternativamente, si el ldapmodify tiene un conmutador que permite continuar
# a pesar de los errores, utilícese dicho conmutador -- si se es cuidadoso
```

```

#
delete: attributetypes
attributetypes: (0.0.8.350.1.1.1.1.1 NAME 'commURI' )
-
#
# se vuelven a añadir los atributos -- en caso de que haya un cambio de
# definición
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.1.1.1
    NAME 'commURI'
    DESC 'Labeled URI format to point to the distinguished name of the
commUniqueId'
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
-
# Definiciones de clase de objeto
#
# En esta Recomendación se definen las siguientes clases de objeto:
#
# commURIObject
#
# commURIObject
#
# Esta clase de objeto auxiliar representa un tipo de atributo URI
#
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.1.2.1 NAME 'commURIObject' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.1.2.1
    NAME 'commURIObject'
    DESC 'object that contains the URI attribute type'
    SUP top AUXILIARY
    MAY ( commURI )
    )
-
#
# final del LDIF
#

```

8.2 LDIF para commObject

```

# Esquema del objeto comunicación
#
# Esquema para representar objetos comunicación en un directorio LDAP
#
# Resumen
#
# Esta Recomendación define el esquema para representar objetos comunicación
# en un directorio LDAP [LDAPv3]. Define elementos del esquema
# para representar un objeto comunicación [commObject].
#
#
# .1 = Actividad relacionada con la comunicación
# .1.2 = commObject
# .1.2.1 = atributos
# .1.2.2 = objectclass
# .1.2.3 = syntax
#
#
# Deficiones de tipos de atributo

```

```

#
#   En esta Recomendación se definen los siguientes tipos de atributo:
#
#       commUniqueId
#       commOwner
#       commPrivate
dn: cn=schema
changetype: modify
#
# si es necesario cambiar la definición de un atributo, en primer lugar
#       realícese la supresión y la nueva adición en un solo paso
#
# si es la primera vez que se añade la clase objeto commObject
# utilizando este fichero LDIF, debe desactivar, con el correspondiente
# símbolo de comentario, la modificación supresión de attributetypes
# ya que ésta falló. Alternativamente, si el ldapmodify tiene un
# conmutador que permite continuar a pesar de los errores, utilícese dicho
# conmutador -- si se es cuidadoso
#
delete: attributetypes
attributetypes: (0.0.8.350.1.1.2.1.1 NAME 'commUniqueId' )
attributetypes: (0.0.8.350.1.1.2.1.2 NAME 'commOwner' )
attributetypes: (0.0.8.350.1.1.2.1.3 NAME 'commPrivate' )
-
#
# se vuelven a añadir los atributos -- en caso en el que haya un cambio en la
# definición
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.2.1.1
    NAME 'commUniqueId'
    DESC 'To hold the endpoints unique Id'
    EQUALITY caseIgnoreIA5Match
    SUBSTR caseIgnoreIA5SubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.2.1.2
    NAME 'commOwner'
    DESC 'Labeled URI to point back to the original owner'
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.2.1.3
    NAME 'commPrivate'
    DESC 'To decide whether the entry is visible to world or not'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
-
# Deficiones de clases de objeto
#
#   En esta Recomendación se definen las siguientes clases objeto:
#
#       commObject
#
# commObject
#
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.2.2.1 NAME 'commObject' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.2.2.1
    NAME 'commObject'
    DESC 'object that contains the Communication attributes'
    SUP top STRUCTURAL
    MUST commUniqueId

```

```
MAY ( commOwner $ commPrivate )
)
-
#
# final del LDIF
#
```

Anexo A

Perfil de indexación

La indexación de atributos es una actividad propia de cada implementación y depende de la aplicación. Los atributos no indexados puede hacer que se produzcan tiempos de búsqueda suficientemente largos como para que determinadas aplicaciones queden inutilizables. En particular, la consulta de usuario y de alias debería ser rápida. En el anexo A, Perfil de indexación, se describe una configuración de indexación para directorios commObject que se optimizará para ser utilizada en aplicaciones de directorio de directorios. La utilización de este perfil es opcional.

commURI: no existe recomendación

commUniqueId: igualdad

commOwner: presencia

commPrivate: presencia

Apéndice I

Consideraciones relativas a la implementación

I.1 Relaciones entre directorios de empresas y directorios commObject

La información CommObject se ubica separadamente de la información de persona o de recurso. Puede situarse en un subárbol de un directorio de empresa de mayor tamaño o en un servidor lógico separado. El directorio de personas continuará acogiendo la información tradicional de personas o de recursos tales como nombre, teléfono, dirección, etc. Además tendrá un enlace commURI con el atributo commUniqueId de commObject. En lugar de ampliar la clase de objeto persona del directorio de empresa, el establecimiento de dicho enlace proporciona las ventajas siguientes:

- 1) Los cambios en el directorio de empresa deben realizarse cuidadosamente, no estando a menudo bajo el control administrativo del proveedor de servicio de vídeo/voz sobre IP.
- 2) Los elementos asociados con las comunicaciones de vídeo y de voz sobre IP son muy dinámicas. La propia tecnología de los sistemas de directorio de empresa cambia rápidamente. Por ejemplo, los cambios que se produzcan en un protocolo específico requerirían cambios en el directorio de la empresa si su representación se heredara de una clase de objeto persona del directorio de empresa y estuviera integrada en dicho directorio de empresa. La separación permite realizar cambios en la infraestructura LDAP commObject sin modificar el directorio de empresa.

- 3) Un servidor de llamadas puede necesitar acceder a los datos commObject de forma muy distinta a como otras aplicaciones acceden al directorio de empresa. Puede disponerse de un servidor diferenciado para que la política de calidad de funcionamiento y de acceso acomode dichos requisitos de implementación. Por ejemplo, un servidor de llamadas puede necesitar hacer consultas al servidor commObject para procesar llamadas en tiempo real, o puede leer y almacenar en caché muchos atributos commObject de una sola vez.

Cualquier usuario o recurso con capacidades de conferencia multimedios debería disponer de un ejemplar de commObject creado y enlazado con una entrada existente en el directorio de empresa con un commURI. Los servidores de llamadas pueden funcionar de dos modos alternativos. El método más sencillo es que el servidor de llamadas lea periódicamente ejemplares del commObject y los incorpore en su tabla interna de puntos extremos. El método preferido, y más escalable, es que el servidor de llamada consulte el servidor commObject cada vez que necesite información, por ejemplo cuando se registra un punto extremo o cuando se establece la comunicación.

I.1.1 Personas frente a recursos

Algunas implementaciones de conferencia multimedios están muy orientadas a los puntos extremos, mientras que otras están orientadas al usuario. Por ejemplo, es común encontrar un punto extremo de grupos de vídeo-teleconferencia en una sala de conferencias cuya identidad nunca cambie. A este punto extremo puede hacerse referencia como a la 'Sala de Conferencias 201'. Este punto extremo no está asociado con ninguna persona en particular, pero si lo está con la sala de conferencias 201 y está compartido con quien necesite utilizar dicha sala de conferencias.

Por otro lado, algunos puntos extremos son específicos del contexto del usuario, obteniendo sus identidades a partir de los usuarios vigentes. Por ejemplo, cuando alguien abre una sesión en una computadora identificándose como jdoe, se puede configurar un punto extremo de dicha computadora con la dirección de jdoe, tal como está almacenado en el perfil de usuario, y se registra en un servidor de llamadas. Otros usuarios que abran una sesión en la misma computadora pueden tener identidades distintas, por lo que sus mensajes de registro contendrán información de identidad diferente.

Esta dicotomía de usuarios frente a recursos hace que sea difícil realizar una asociación de puntos extremos con usuarios o recursos. Si bien es cierto que las clases de objeto persona están disponibles con facilidad, la clase de objeto recursos lo están menos. La vinculación de un commObject a una persona mediante un commURI, generaliza esta relación. Si un atributo commOwner apunta a una clase de objeto a persona, dicho commObject se asocia a dicha persona. Si un atributo commOwner apunta a una clase de objeto recurso, dicho commObject está asociado a dicho recurso. De otra forma, las personas o los recursos pueden tener punteros commURI que asocien puntos extremos con ellos. Los directorios de empresa que solamente soportan personas y no recursos pueden optar, simplemente, por tratar los recursos como personas.

I.1.2 Seguridad y autenticación

Casi todo lo relativo a la autenticación está orientado a personas. Por lo tanto, los recursos compartidos tales como salas de conferencia o sistemas de teleconferencia son a menudo menos seguros debido a que no tienen una identidad de autenticación asociada. Queda fuera del alcance de esta Recomendación analizar lo relativo a la autenticación, sin embargo se insta a que los implementadores analicen cuidadosamente los aspectos de seguridad de las distintas opciones arquitectónicas.

Las listas de control de acceso y otros mecanismos de seguridad asociados con el directorio quedan fuera del alcance de esta Recomendación. Se insta a que los implementadores consideren cuidadosamente los aspectos de privacidad y seguridad de los datos presentes en los directorios.

Apéndice II

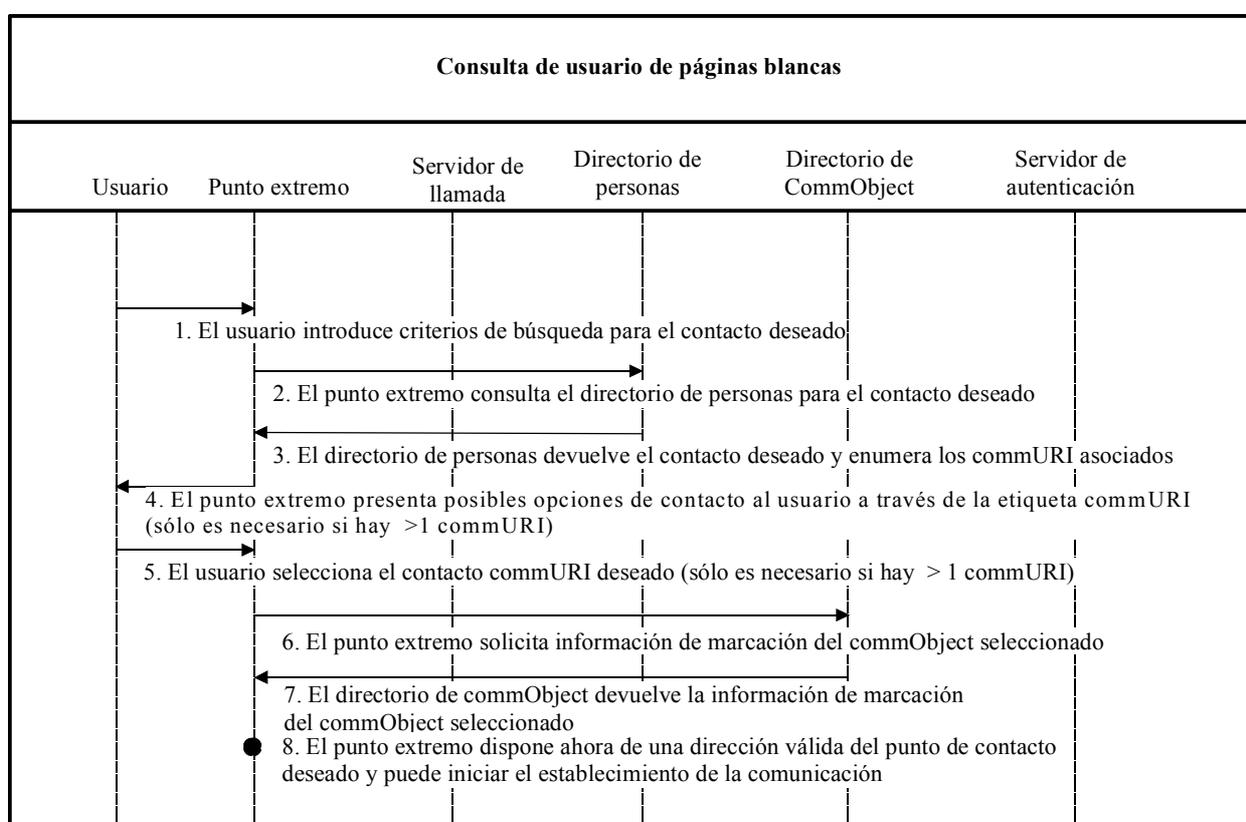
Flujos de llamada

II.1 Escenarios de flujos de llamada

Los siguientes flujos de llamada representan posibles escenarios de aplicación sobre cómo puede utilizarse H.350. Estos flujos de llamada son sólo ilustrativos y no normativos. Específicamente, H.350 define cómo se representan los elementos de datos en directorios LDAP, pero no cómo se utilizan dichos elementos de datos.

II.1.1 Consulta de usuario de páginas blancas

En la figura II.1 se muestra cómo un punto extremo habilitado para LDAP puede buscar un usuario en un directorio, obtener la información commObject del usuario y marcar el punto extremo del mismo. En este escenario, el punto extremo puede preconfigurarse para buscar en un directorio de empresa determinado, o puede ser configurado para buscar en un portal directorio que, a su vez, realiza la búsqueda en varios directorios. Este escenario muestra cómo un dispositivo puede realizar la búsqueda, presentando elecciones y resultados en la interfaz de usuario. Sin embargo, esta funcionalidad también puede implementarse mediante una página web, en la que los criterios de búsqueda se introducen en un formulario web y los resultados se devuelven y visualizan en una página web, permitiendo una marcación mediante clics. Nótese que, si bien este ejemplo ilustra cómo un punto extremo puede realizar una búsqueda consulta LDAP, también es posible que un servidor de llamadas pueda realizar consultas en nombre de puntos extremos y pasar la información al correspondiente punto extremo a través de un trayecto de comunicación alternativo, centralizando así algunos aspectos del acceso a páginas blancas.

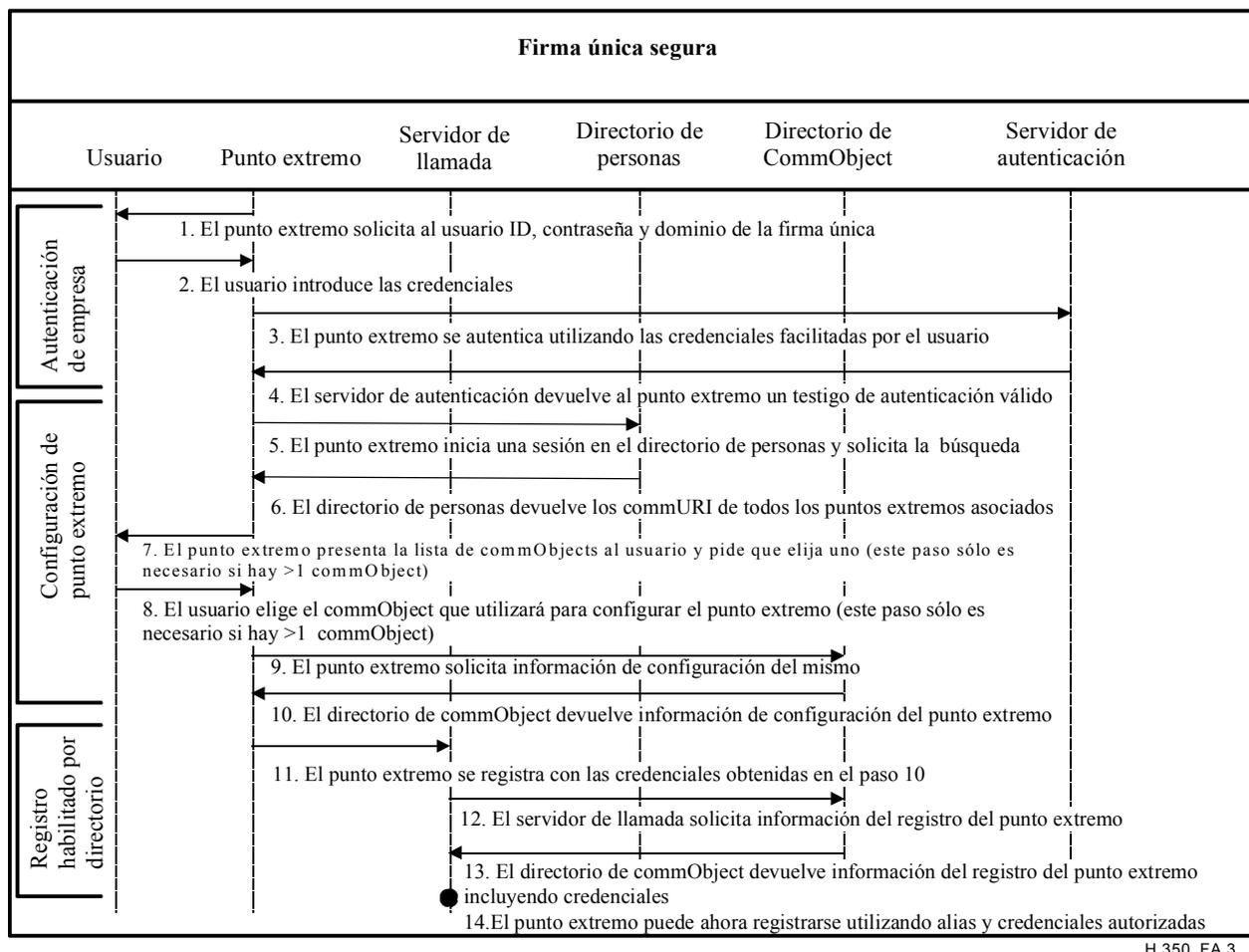


H.350_FA.1

Figura II.1/H.350 – Consulta de usuario de páginas blancas

II.1.3 Firma única segura

La figura II.3 ilustra cómo puede crearse un entorno en el que un usuario utilice una identidad de autenticación de empresa existente para acceder a diversas entidades de punto extremo. Este escenario tiene varias características fundamentales que son deseables para instalaciones de gran tamaño. El punto extremo se configura automáticamente utilizando información del directorio. Ello elimina los errores de usuario en el proceso de configuración y simplifica la instalación. En segundo lugar, el usuario sólo debe recordar sus credenciales de firma única, que típicamente están constituidas por el identificador de usuario de empresa y una contraseña. Los puntos extremos pueden tener (y a menudo deben tener) varias credenciales, pero el usuario no necesita conocerlas todas debido a que éstas se cargan directamente en el punto extremo desde el directorio. Debido a que las credenciales del punto extremo se cargan automáticamente, éstas pueden ser refrescadas con frecuencia. Por ejemplo, una herramienta de gestión podría generar credenciales aleatorias para cada punto extremo y almacenarlas en el directorio commObject cada noche. Ello crea un entorno muy seguro en el que las credenciales son asimismo seguras, e incluso, en caso de necesidad, éstas pueden ser suprimidas y sustituidas por otras en un periodo de tiempo muy breve. Este escenario soporta la utilización de ID/contraseñas o certificados basados en credenciales del punto extremo. Tradicionalmente, los certificados han sido difíciles de desplegar debido a las dificultades de gestión que presentan para los usuarios. Este escenario resuelve el problema de la gestión de certificados y abre la posibilidad de que éstos puedan ser gestionados por, o en nombre de, un sistema de gestión de certificado central, en lugar de hacerlo en nombre de los usuarios, desligando así a éstos de la complejidad de los sistemas PKI pero disfrutando de sus ventajas en términos de seguridad.



H.350_FA.3

Figura II.3/H.350 – Firma única segura

En este escenario, los pasos de autenticación de empresa representan a un usuario autenticándose ante un servidor de autenticación existente instalado para firma única y de propósito general (por ejemplo, correo electrónico, web, uso compartido de ficheros) en un sistema de autenticación. Una vez autenticado, el usuario puede conectarse directamente al servidor LDAP y recuperar la información de configuración que necesite del punto extremo seleccionado, incluyendo datos de configuración y credenciales de autenticación para el punto extremo. Finalmente, utilizando dichas credenciales, el punto extremo puede autenticarse ante el servidor de llamadas utilizando cualquier esquema de autenticación vigente (por ejemplo, los anexos D o E/H.235). Es conveniente utilizar la seguridad de la capa de transporte para asegurar la privacidad de estas transacciones.

Apéndice III

Ficheros electrónicos¹

El fichero anexo `commURI.ldif.txt` contiene una versión de sólo texto del fichero LDIF descrito en 8.1.



`commURI.ldif.txt`

El fichero anexo `commObject.ldif.txt` contiene una versión de sólo texto del fichero LDIF descrito en 8.2.



`commObject.ldif.txt`

¹ Para ayudar a los usuarios de la versión impresa, el contenido de este apéndice se puede obtener gratuitamente en el sitio web de publicaciones de la UIT:

<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.350>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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 multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
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 y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación