

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.350.4

(05/2011)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Directory services
architecture for audiovisual and multimedia services

Directory services architecture for SIP

Recommendation ITU-T H.350.4



ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.350.4

Directory services architecture for SIP

Summary

Recommendation ITU-T H.350.4 describes a lightweight directory access protocol (LDAP) directory services architecture for multimedia conferencing using a session initiation protocol (SIP). In particular, it defines an LDAP schema to represent SIP user agents (UAs) on the network and associate those endpoints with users.

This Recommendation is intended to supplement the CommObject directory architecture as discussed in Recommendation ITU-T H.350, and not intended to be used as a stand-alone architecture. The implementation of this LDAP schema, together with the use of the ITU-T H.350 CommObject architecture, facilitates the integration of SIP user agents and conferencing devices into the existing enterprise directories; thus allowing the user to perform white page lookups and access clickable dialling supported by SIP devices. The primary reasons for implementing this schema are identical to those listed in Recommendation ITU-T H.350 (the CommObject class definition) as they apply specifically to the use of SIP UAs.

This revised version of Recommendation ITU-T H.350.4 introduces several enhancements and clarifications to the previous version, primarily the addition of ITU-T X.500 directories support.

This Recommendation includes an electronic attachment containing a schema configuration file for SIPIdentity.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.350.4	2003-08-06	16
1.0	ITU-T H.350.4 attachment	2003-08-06	16
2.0	ITU-T H.350.4	2011-05-14	16

Keywords

Directory services, ITU-T H.235.0, ITU-T H.320, ITU-T H.323, LDAP, SIP, ITU-T X.500.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
1.1 Extending the schema.....	1
2 References.....	1
3 Definitions	2
4 Abbreviations.....	3
5 Conventions	3
6 Object class definitions.....	4
6.1 SIPIIdentity	4
6.2 SIPIIdentitySIPURI	4
6.3 SIPIIdentityRegistrarAddress	4
6.4 SIPIIdentityProxyAddress	5
6.5 SIPIIdentityAddress.....	6
6.6 SIPIIdentityPassword.....	6
6.7 SIPIIdentityUserName.....	7
6.8 SIPIIdentityServiceLevel.....	7
7 SIPIIdentity LDIF files	8
8 Using ITU-T H.350 With ITU-T X.500 directories	10
8.1 IMPORTS of ITU-T X.500 ASN.1	10
8.2 sipIdentityASN1.asn.....	10
Annex A – Indexing profile	13
Appendix I – Electronic attachment.....	14
Bibliography.....	15

Electronic attachment: Schema configuration file for SIPIIdentity

Recommendation ITU-T H.350.4

Directory services architecture for SIP

1 Scope

This Recommendation¹ describes a lightweight directory access protocol (LDAP) directory services architecture for multimedia conferencing using a session initiation protocol (SIP). In particular, it defines an LDAP schema to represent SIP user agents (UAs) on the network and associate those endpoints with users.

This Recommendation is intended to supplement the CommObject directory architecture as discussed in [ITU-T H.350], and is not intended to be used as a stand-alone architecture. The implementation of this LDAP schema, together with the use of the ITU-T H.350 CommObject architecture, facilitates the integration of SIP user agents and conferencing devices into the existing enterprise directories; thus allowing the user to perform white page lookups and access clickable dialling supported by SIP devices. The primary reasons for implementing this schema include those listed in [ITU-T H.350] (the CommObject class definition) as they apply specifically to the use of SIP UAs, and to facilitate vendors making SIP services more readily available to their users.

The scope of this Recommendation includes recommendations for the architecture to integrate endpoint information for endpoints using SIP into the existing enterprise directories and white pages.

The scope of this Recommendation does not include normative methods for the use of the LDAP directory itself or the data it contains. The purpose of the schema is not to represent all possible data elements in the SIP protocol, but rather to represent the minimal set required to accomplish the design goals enumerated in [ITU-T H.350].

Note that SIP provides well-defined methods for discovering registrar addresses and locating users on the network. Some of the attributes defined here are intended for more trivial or manual implementations and may not be needed for all applications. For example, SIPIdentityRegistrarAddress and SIPIdentityAddress may not be needed for many applications, but are included here for completeness. Thus, SIPIdentitySIPURI is the primary attribute of interest that will be served out, especially for white page directory applications.

1.1 Extending the schema

The SIPIdentity classes may be extended as necessary for specific implementations. See the base [ITU-T H.350] for a discussion on schema extension.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

¹ This Recommendation includes an electronic attachment containing a text file with a schema configuration for SIPIdentity.

- [ITU-T H.350] Recommendation ITU-T H.350 (2011), *Directory services architecture for multimedia conferencing*.
- [ITU-T X.500] Recommendation ITU-T X.500 (2008) | ISO/IEC 9594-1:2008, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.
- [ITU-T X.501] Recommendation ITU-T X.501 (2008) | ISO/IEC 9594-2:2008, *Information technology – Open Systems Interconnection – The Directory: Models*.
- [ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.511] Recommendation ITU-T X.511 (2008) | ISO/IEC 9594-3:2008, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.
- [ITU-T X.518] Recommendation ITU-T X.518 (2008) | ISO/IEC 9594-4:2008, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.
- [ITU-T X.519] Recommendation ITU-T X.519 (2008) | ISO/IEC 9594-5:2008, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.
- [ITU-T X.520] Recommendation ITU-T X.520 (2008) | ISO/IEC 9594-6:2008, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- [ITU-T X.525] Recommendation ITU-T X.525 (2008) | ISO/IEC 9594-9:2008, *Information technology – Open Systems Interconnection – The Directory: Replication*.
- [IETF RFC 2069] IETF RFC 2069 (1997), *An Extension to HTTP: Digest Access Authentication*.
- [IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.
- [IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.
- [IETF RFC 4510] IETF RFC 4510 (2006), *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.
- [IETF RFC 4511] IETF RFC 4511 (2006), *Lightweight Directory Access Protocol (LDAP): The Protocol*.

3 Definitions

This Recommendation defines the following terms:

3.1 client: A SIP client is a network device that initiates SIP requests and receives SIP responses on a network.

3.2 commObject: An LDAP object class defined in [ITU-T H.350] that represents generic multimedia conferencing endpoints.

3.3 endpoint: A logical device that provides video and/or voice media encoding/decoding, and signalling functions. Examples include:

- 1) a group teleconferencing appliance that is located in a conference room;
- 2) an IP telephone;

- 3) a software program that takes video and voice from a camera and microphone and encodes it and applies signalling using a host computer.

Note that from the perspective of most signalling protocols, gateways and MCUs are special cases of endpoints.

3.4 enterprise directory: A canonical collection of information about users in an organization. Typically this information is collected from a variety of organizational units to create a whole. For example, Human Resources may provide name and address, Telecommunications may provide the telephone number, Information Technology may provide the e-mail address, etc. For the purposes of this architecture, it is assumed that an enterprise directory is accessible via LDAP.

3.5 gateway: A device that translates from one protocol to another. Often gateways translate between the IP network and the public switched voice network to allow integration of the two.

3.6 multipoint control unit (MCU): A device capable of mixing audio/video from multiple endpoints to create a virtual meeting space.

3.7 proxy server, SIP proxy: A server that acts as both a client and a server to make requests on behalf of another user agent (UA). The primary role of a proxy server is to ensure that a request generated by a UA is passed to another entity that is closer to the destination user.

3.8 registrar: A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.

3.9 SIP URI: A type of uniform resource identifier (URI) that identifies a communication resource in the session initiation protocol (SIP). A SIP URI usually contains a user name and a host name and is similar in format to an e-mail address.

3.10 user agent (UA): A device that can function as both a user agent client and server.

3.11 white pages: An application that allows end users to look up the address of another user.

4 Abbreviations

This Recommendation uses the following abbreviations:

LDAP	Lightweight Directory Access Protocol (as defined in [IETF RFC 4510])
LDIF	LDAP Data Interchange Format
MCU	Multipoint Control Unit
SIP	Session Initiation Protocol
UA	User Agent

5 Conventions

In this Recommendation, the following conventions are used:

"Shall" indicates a mandatory requirement.

"Should" indicates a suggested but optional course of action.

"May" indicates an optional course of action rather than a recommendation that something takes place.

References to clauses, subclauses, annexes and appendices refer to those items within this Recommendation, unless another specification is explicitly listed.

6 Object class definitions

The SIPIdentity object class represents SIP user agents (UAs). It is an auxiliary class and is derived from the commObject class, which is defined in [ITU-T H.350].

6.1 SIPIdentity

```
OID: 0.0.8.350.1.1.6.2.1
objectclasses: (0.0.8.350.1.1.6.2.1
NAME 'SIPIdentity'
DESC 'SIPIdentity object'
SUP top AUXILIARY
MAY ( SIPIdentitySIPURI $ SIPIdentityRegistrarAddress $
      SIPIdentityProxyAddress $ SIPIdentityUserName $
      SIPIdentityPassword $ SIPIdentityServiceLevel $
      userSMIMECertificate )
)
```

6.2 SIPIdentitySIPURI

```
OID: 0.0.8.350.1.1.6.1.1
attributetypes: (0.0.8.350.1.1.6.1.1
NAME 'SIPIdentitySIPURI'
DESC 'Universal Resource Indicator of the SIP UA'
EQUALITY caseExactMatch
SUBSTR caseExactSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Application utility class

standard

Number of values

multi

Definition

Uniform resource identifier that identifies a communication resource in SIP; it usually contains a user name and a host name and is often similar in format to an e-mail address.

Permissible values (if controlled)

Notes

This URI may institute SIP or SIPS (secure). In the event that SIPS is instituted, the URI must reflect that it is using SIPS as opposed to SIP. See examples below.

Semantics

Example applications for which this attribute would be useful

Online representation of most current listing of a user's SIP(S) UA.

Example

```
SIPIdentitySIPURI: sip:alice@foo.com // SIP example
SIPIdentitySIPURI: sip:alice@152.2.158.212 // SIP example
SIPIdentitySIPURI: sips:bob@birmingham.edu // SIPS example
```

6.3 SIPIdentityRegistrarAddress

```
OID: 0.0.8.350.1.1.6.1.2
attributetypes: (0.0.8.350.1.1.6.1.2
NAME 'SIPIdentityRegistrarAddress'
DESC 'specifies the location of the registrar'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Application utility class

Standard

Number of values

multi

Definition

Address for the domain to which the server that handles REGISTER requests and forwarding to the location server for a particular domain belongs.

Permissible values (if controlled)

Notes

Note that [IETF RFC 3261] states that user agents can discover their registrar address by configuration, using the address-of-record, or by multicast. The first scenario, by configuration, is noted as out of scope for [IETF RFC 3261]. This attribute may be used for the first scenario. It can be accomplished manually, (e.g., a web page that displays a user's correct registrar address) or automatically with an ITU-T H.350.4 aware user agent.

Semantics

Example applications for which this attribute would be useful

white pages, a web page that displays a user's correct configuration information.

Example (LDIF fragment)

```
SIPIdentityRegistrarAddress: 152.2.15.22 //IP address example
SIPIdentityRegistrarAddress: sipregistrar.unc.edu //FQDN example
```

6.4 SIPIdentityProxyAddress

```
OID: 0.0.8.350.1.1.6.1.3
attributetypes: (0.0.8.350.1.1.6.1.3
NAME 'SIPIdentityProxyAddress'
DESC 'Specifies the location of the SIP Proxy'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Application utility class

Standard

Number of values

multi

Definition

Address which specifies the domain location of a SIP proxy within a domain. [IETF RFC 3261] defines the role of the SIP proxy.

Permissible values (if controlled)

Notes

SIP user agents are not required to use a proxy, but will in many cases.

Semantics

Example applications for which this attribute would be useful

white pages, a web page that displays a user's correct configuration information.

Example (LDIF fragment)

```
SIPIdentityProxyAddress: 172.2.13.234 //IP address example
SIPIdentityProxyAddress: sipproxy.unc.edu //FQDN example
```

6.5 SIPIdentityAddress

```
OID: 0.0.8.350.1.1.6.1.4
attributetypes: (0.0.8.350.1.1.6.1.4
NAME 'SIPIdentityAddress'
DESC 'IP address or FQDN of the UA'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Application utility class

standard

Number of values

multi

Definition

Specifies the IP address or fully qualified domain name of the UA.

Permissible values (if controlled)

Notes

This attribute may be useful for applications in which UA-to-UA communication is direct, not involving a proxy or registrar.

Example applications for which this attribute would be useful

A web page that displays a user's proper user agent configuration information.

Example (LDIF fragment)

```
SIPIdentityAddress: 152.2.121.36 // IP address example
SIPIdentityAddress: ipPhone.foo.org // FQDN example
```

6.6 SIPIdentityPassword

```
OID: 0.0.8.350.1.1.6.1.5
attributetypes: (0.0.8.350.1.1.6.1.5
NAME 'SIPIdentityPassword'
DESC 'The user agent SIP password '
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

Application utility class

Standard

Number of values

multi

Definition

The SIP user agent's password, used for the HTTP digest authentication scheme as defined in [IETF RFC 2617].

Permissible values (if controlled)

Notes

Because [IETF RFC 2069], which was made obsolete by [IETF RFC 2617], was used as the basis for HTTP Digest in [IETF RFC 3261], any SIP servers supporting [IETF RFC 2617] must ensure backward compatibility with [IETF RFC 2069].

This SIPIdentityUserName, together with the SIPIdentityPassword, are reserved for the purpose of use with digest access authentication, and not intended for use with basic authentication methods.

LDAP provides one method to store user passwords for reference. If passwords are stored in LDAP, it makes the LDAP server a particularly valuable target for attack. Implementers are encouraged to exercise caution and implement appropriate security procedures such as encryption, access control, and transport layer security for access to this attribute.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

```
SIPIdentityPassword: 36zxJmCIB18dM0FVAj
```

6.7 SIPIdentityUserName

```
OID: 0.0.8.350.1.1.6.1.6
attributetypes: (0.0.8.350.1.1.6.1.6
NAME 'SIPIdentityUserName'
DESC 'The user agent user name.'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Application utility class

Standard

Number of values

multi

Definition

The SIP user agent's user name, used for the HTTP digest authentication scheme as defined in [IETF RFC 2617].

Permissible values (if controlled)

Notes

Because [IETF RFC 2069], which was made obsolete by [IETF RFC 2617], was used as the basis for HTTP digest authentication in [IETF RFC 3261], any SIP servers supporting HTTP digest authentication as defined in [IETF RFC 2617] must ensure backward compatibility with [IETF RFC 2069].

This SIPIdentityUserName, together with the SIPIdentityPassword, are reserved for the purpose of use with digest access authentication, and not intended for use with basic authentication methods.

Note that in many cases, the user name will be parsed from the user@proxy.domain portion of the SIP URI. In that case, it may not be necessary to populate this attribute.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

```
SIPIdentityUserName: nelkhour
```

6.8 SIPIdentityServiceLevel

```
OID: 0.0.8.350.1.1.6.1.7
attributetypes: (0.0.8.350.1.1.6.1.7
NAME 'SIPIdentityServiceLevel'
DESC 'To define services that a user can belong to.'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26)

Application utility class

Standard

Number of values

multi

Definition

This describes the level of services a user can belong to.

Permissible values (if controlled)

Notes

This attribute does not represent a data element found in SIP. SIP itself does not support distinctions in service levels. Instead, this attribute provides a mechanism for the storage of service level information directly in LDAP. This mapping allows service providers to adapt to an existing LDAP directory without changing the values of the SIPIdentityServiceLevel instances in the directory.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

```
SIPIdentityServiceLevel: premium
```

7 SIPIdentity LDIF files

This clause contains a schema configuration file for SIPIdentity that can be used to configure an LDAP server to support this class.

```
# SIPIdentity Object Schema
#
# Schema for representing SIPIdentity Object in an LDAP Directory
#
# Abstract
#
# This Recommendation defines the schema for representing SIPIdentity
# object in an LDAP directory [LDAPv3]. It defines schema elements
# to represent an SIPIdentity object [SIPIdentity].
#
#           .1 = Communication related work
#           .1.6 = SIPIdentity
#           .1.6.1 = attributes
#           .1.6.2 = objectclass
#           .1.6.3 = syntax
#
#
# Attribute Type Definitions
#
#   The following attribute types are defined in this Recommendation:
#
#   SIPIdentitySIPURI
#   SIPIdentityRegistrarAddress
#   SIPIdentityProxyAddress
#   SIPIdentityAddress
#   SIPIdentityPassword
#   SIPIdentityUserName
#   SIPIdentityServiceLevel
dn: cn=schema
changetype: modify
#
```

```

# if you need to change the definition of an attribute,
#         then first delete and re-add in one step
#
# if this is the first time you are adding the SIPIdentity
# objectclass using this LDIF file, then you should comment
# out the delete attributetypes modification since this will
# fail. Alternatively, if your ldapmodify has a switch to continue
# on errors, then just use that switch -- if you are careful
#
delete: attributetypes
attributetypes: (0.0.8.350.1.1.6.1.1 NAME 'SIPIdentitySIPURI' )
attributetypes: (0.0.8.350.1.1.6.1.2 NAME 'SIPIdentityRegistrarAddress' )
attributetypes: (0.0.8.350.1.1.6.1.3 NAME 'SIPIdentityProxyAddress' )
attributetypes: (0.0.8.350.1.1.6.1.4 NAME 'SIPIdentityAddress' )
attributetypes: (0.0.8.350.1.1.6.1.5 NAME 'SIPIdentityPassword' )
attributetypes: (0.0.8.350.1.1.6.1.6 NAME 'SIPIdentityUserName' )
attributetypes: (0.0.8.350.1.1.6.1.7 NAME 'SIPIdentityServiceLevel' )
-
#
# re-add the attributes -- in case there is a change of definition
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.6.1.1
  NAME 'SIPIdentitySIPURI'
  DESC 'Universal Resource Indicator of the SIP UA'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.6.1.2
  NAME 'SIPIdentityRegistrarAddress'
  DESC 'specifies the location of the registrar'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.6.1.3
  NAME 'SIPIdentityProxyAddress'
  DESC 'Specifies the location of the SIP Proxy'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.6.1.4
  NAME 'SIPIdentityAddress'
  DESC 'IP address of the UA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.6.1.5
  NAME 'SIPIdentityPassword'
  DESC 'The user agent SIP password '
  EQUALITY octetStringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
attributetypes: (0.0.8.350.1.1.6.1.6
  NAME 'SIPIdentityUserName'
  DESC 'The user agent user name.'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.6.1.7
  NAME 'SIPIdentityServiceLevel'
  DESC 'To define services that a user can belong to.'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
-
# Object Class Definitions
#
#   The following object class is defined in this Recommendation:
#
#       SIPIdentity
#
# SIPIdentity
#
#

```

```

delete: objectclasses
objectclasses: (0.0.8.350.1.1.6.2.1 NAME 'SIPIdentity' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.6.2.1
  NAME 'SIPIdentity'
  DESC 'SIPIdentity object'
  SUP top AUXILIARY
  MAY ( SIPIdentitySIPURI $ SIPIdentityRegistrarAddress $
        SIPIdentityProxyAddress $ SIPIdentityAddress $
        SIPIdentityPassword $ SIPIdentityUserName $
        SIPIdentityServiceLevel $ userSMIMECertificate )
)
-
#
# end of LDIF
#

```

8 Using ITU-T H.350 With ITU-T X.500 directories

8.1 IMPORTS of ITU-T X.500 ASN.1

To satisfy all the IMPORTS clauses, the following modules are needed:

- BasicAccessControl ([ITU-T X.501])
- DSAOperationalAttributeTypes ([ITU-T X.501])
- EnhancedSecurity ([ITU-T X.501])
- InformationFramework ([ITU-T X.501])
- OperationalBindingManagement ([ITU-T X.501])
- ServiceAdministration ([ITU-T X.501])
- UsefulDefinitions ([ITU-T X.501])
- AttributeCertificateDefinitions ([ITU-T X.509])
- AuthenticationFramework ([ITU-T X.509])
- CertificateExtensions ([ITU-T X.509])
- MTSAbstractService ([ITU-T X.509])
- PKIX1Implicit93 ([ITU-T X.509])
- DirectoryAbstractService ([ITU-T X.511])
- SpkmGssTokens ([ITU-T X.511])
- DistributedOperations ([ITU-T X.518])
- HierarchicalOperationalBindings ([ITU-T X.518])
- CommonProtocolSpecification ([ITU-T X.519])
- DirectoryOSIProtocols ([ITU-T X.519])
- DirectoryOperationalBindingTypes ([ITU-T X.519])
- OSIProtocolSpecification ([ITU-T X.519])
- SelectedAttributeTypes ([ITU-T X.520])
- DirectoryShadowAbstractService ([ITU-T X.525])
- ldap ([IETF RFC 4511])

It is noted that these modules can be downloaded from the [ITU-T ASN.1 module database](#).

8.2 sipIdentityASN1.asn

```
SipIdentity { itu-t(0) recommendation(0) h(8) 350 1 cr(1) sipIdentity(6) module(4) }
```

```

DEFINITIONS ::=
BEGIN

-- SIPIdentity Object Schema

-- Schema for representing SIPIdentity Object in an LDAP Directory

-- Abstract

-- This Recommendation defines the schema for representing SIPIdentity
-- object in an LDAP directory [LDAPv3]. It defines schema elements
-- to represent an SIPIdentity object [SIPIdentity].

--          .1 = Communication related work
--          .1.6 = SIPIdentity
--          .1.6.1 = attributes
--          .1.6.2 = objectclass
--          .1.6.3 = syntax

IMPORTS

-- from Rec. ITU-T H.350
h350-cr, caseIgnoreIA5Match, caseIgnoreIA5SubstringsMatch, userSMIMECertificate
    FROM CommURI { itu-t(0) recommendation(0) h(8) 350 1 cr(1) commURI(1) module(4) }

-- from Rec. ITU-T X.501 | ISO/IEC 9594-2
ATTRIBUTE, OBJECT-CLASS, top
    FROM InformationFramework {joint-iso-itu-t ds(5) module(1) informationFramework(1)
6}

-- from Rec. ITU-T X.520 | ISO/IEC 9594-6
UnboundedDirectoryString, caseExactMatch, caseExactSubstringsMatch, caseIgnoreMatch,
caseIgnoreSubstringsMatch, octetStringMatch
    FROM SelectedAttributeTypes {joint-iso-itu-t ds(5) module(1)
selectedAttributeTypes(5) 6} ;

-- Attribute Type Definitions

-- The following attribute types are defined in this Recommendation:

--     SIPIdentitySIPURI
--     SIPIdentityRegistrarAddress
--     SIPIdentityProxyAddress
--     SIPIdentityAddress
--     SIPIdentityPassword
--     SIPIdentityUserName
--     SIPIdentityServiceLevel

SIPIdentitySIPURI ATTRIBUTE ::= {
    WITH SYNTAX UnboundedDirectoryString
    EQUALITY MATCHING RULE caseExactMatch
    SUBSTRINGS MATCHING RULE caseExactSubstringsMatch
    ID { at 1 } }

SIPIdentityRegistrarAddress ATTRIBUTE ::= {
    WITH SYNTAX IA5String
    EQUALITY MATCHING RULE caseIgnoreIA5Match
    ID { at 2 } }

SIPIdentityProxyAddress ATTRIBUTE ::= {
    WITH SYNTAX IA5String
    EQUALITY MATCHING RULE caseIgnoreIA5Match
    ID { at 3 } }

SIPIdentityAddress ATTRIBUTE ::= {
    WITH SYNTAX IA5String
    EQUALITY MATCHING RULE caseIgnoreIA5Match

```

```

ID { at 4 } }

sIPIdentityPassword ATTRIBUTE ::= {
    WITH SYNTAX OCTET STRING
    EQUALITY MATCHING RULE octetStringMatch
    ID { at 5 } }

sIPIdentityUserName ATTRIBUTE ::= {
    WITH SYNTAX UnboundedDirectoryString
    EQUALITY MATCHING RULE caseIgnoreMatch
    SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
    ID { at 6 } }

sIPIdentityServiceLevel ATTRIBUTE ::= {
    WITH SYNTAX IA5String
    EQUALITY MATCHING RULE caseIgnoreIA5Match
    SUBSTRINGS MATCHING RULE caseIgnoreIA5SubstringsMatch
    ID { at 7 } }

-- Object Class Definitions

-- The following object class is defined in this Recommendation:

-- SIPIdentity

-- SIPIdentity

sIPIdentity OBJECT-CLASS ::= {
    SUBCLASS OF { top }
    MAY CONTAIN { sIPIdentitySIPURI |
        sIPIdentityRegistrarAddress |
        sIPIdentityProxyAddress |
        sIPIdentityAddress |
        sIPIdentityPassword |
        sIPIdentityUserName |
        sIPIdentityServiceLevel |
        userSMIMECertificate }
    ID { oc 1 } }

sip-Id OBJECT IDENTIFIER ::= { h350-cr sip-Id(6) }
at OBJECT IDENTIFIER ::= { sip-Id at(1) }
oc OBJECT IDENTIFIER ::= { sip-Id oc(2) }

END -- end of ASN.1

```

Annex A

Indexing profile

(This annex forms an integral part of this Recommendation.)

Indexing of attributes is an implementation-specific activity and depends upon the desired application. Non-indexed attributes can result in search times sufficiently long to render some applications unusable. Notably, user and alias lookup should be fast. This annex Indexing Profile describes an indexing configuration for SIPIdentity directories that will be optimized for use in the directory of directories applications. Use of this profile is optional.

SIPIdentitySIPURI: equality

SIPIdentityRegistrarAddress: no recommendation

SIPIdentityProxyAddress: no recommendation

SIPIdentityAddress: equality

SIPIdentityUserName: equality

SIPIdentityPassword: no recommendation

SIPIdentityServiceLevel: equality

Appendix I

Electronic attachment

(This appendix does not form an integral part of this Recommendation.)

The associated ZIP file for Recommendation ITU-T H.350.4 contains file `sipIdentity.ldif.txt` with a text-only version of the LDIF file described in clause 7.

The ZIP file is available for free download at <http://www.itu.int/rec/T-REC-H.350.4> .

Bibliography

- [b-IETF RFC 3263] IETF RFC 3263 (2002), *Session Initiation Protocol (SIP): Locating SIP Servers*.
- [b-Howes-1] Howes, T.A., PhD, Smith, M.C., and Good, G.S. (1998), *Understanding and Deploying LDAP Directory Services*, New Riders Publishing, ISBN: 1578700701.
- [b-Howes-2] Howes, T.A., PhD, and Smith, M.C. (1997), *LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*, New Riders Publishing, ISBN: 1578700000.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems