International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.350.7

(01/2007)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

Directory services architecture for XMPP

ITU-T Recommendation H.350.7

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 AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619

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

ITU-T Recommendation H.350.7

Directory services architecture for XMPP

Summary

The Extensible Messaging and Presence Protocol (XMPP) is an IETF standard protocol for exchanging information between network endpoints using Extensible Markup Language (XML). It is used to enable instant messaging and presence applications and is growing in popularity. This Recommendation includes XMPP in the suite of protocols that is supported in [ITU-T H.350], so that an organization can directory-enable and manage XMPP resources in the same way that other multimedia protocols (e.g., H.320, H.323, SIP) are managed in [ITU-T H.350].

Source

ITU-T Recommendation H.350.7 was approved on 13 January 2007 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Directory services, instant messaging, LDAP, presence, XMPP.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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 2007

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

CONTENTS

ITU-T Recommendation H.350.7

Directory services architecture for XMPP

1 Scope

The Extensible Messaging and Presence Protocol (XMPP) is an IETF standard protocol for exchanging information between network endpoints using Extensible Markup Language (XML). It is used to enable instant messaging and presence applications and is growing in popularity. This Recommendation includes XMPP in the suite of protocols that is supported in [ITU-T H.350], so that an organization can directory-enable and manage XMPP resources in the same way that other multimedia protocols (e.g., H.320, H.323, SIP) are managed in [ITU-T H.350]. The schema provides a method for representing XMPP URIs and user information in the directory. Note that this Recommendation defines representation of URIs and not IRIs, as described in [IETF RFC 4622].

The scope of this Recommendation does not include normative methods for the use of the LDAP directory itself or the data it contains.

1.1 Extending the schema

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

1.2 Typical use cases

Many applications external to an XMPP network may need to identify XMPP entities as full URIs; in this case an LDAP directory that needs to store XMPP addresses and non-native user agents (e.g., web browsers, calendaring applications and enterprise white pages) that provide interface to XMPP services. The simplest case is to have a white page lookup where a user is using a web browser to search for other users that are using an XMPP-based client.

Another use case would be for an XMPP server to use XMPP account credentials (xmppUserId and xmppPassword attributes) stored in an H.350 directory for authenticating requests from XMPP clients. This is useful for environments where there is no backend authentication mechanism available.

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.

[ITU-T H.350] ITU-T Recommendation H.350 (2003), *Directory services architecture for multimedia conferencing*.

[ITU-T H.350.1] ITU-T Recommendation H.350.1 (2003), *Directory services architecture for H.323*.

[ITU-T H.350.2] ITU-T Recommendation H.350.2 (2003), *Directory services architecture for H.235*.

[ITU-T H.350.3] ITU-T Recommendation H.350.3 (2003), *Directory services architecture for H.320*.

[ITU-T H.350.4] ITU-T Recommendation H.350.4 (2003), *Directory services architecture for SIP*.

[ITU-T H.350.5] ITU-T Recommendation H.350.5 (2003), *Directory services architecture for non-standard protocols*.

[IETF RFC 3920] IETF RFC 3920 (2004), *Extensible Messaging and Presence Protocol (XMPP): Core*.

[IETF RFC 4622] IETF RFC 4622 (2006), *Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifiers (URIs) for the Extensible Messaging and Presence Protocol (XMPP)*.

3 Definitions

This Recommendation uses the following terms defined elsewhere:

3.1 Uniform Resource Identifier (URI): See [IETF RFC 4622] for a discussion of URIs and IRIs in XMPP.

3.2 Internationalized Resource Identifier (IRI): See [IETF RFC 4622] for a discussion of URIs and IRIs in XMPP.

4 Abbreviations

This Recommendation uses the following abbreviations:

LDAP Lightweight Directory Access Protocol (as defined in [IETF RFC 1777]).

SASL Simple Authentication and Security Layer (as defined in [b-IETF RFC 4422]).

XMPP Extensible Messaging and Presence Protocol (an IETF standard protocol for exchanging information between network endpoints using Extensible Markup Language (XML). It is commonly used for instant messaging, presence and voice over IP applications.)

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 take 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 xmppURIObject represents an XMPP URI; that is, the address of an entity that is capable of communicating using the XMPP protocol. Because it is its own unique object class, the directory can be searched for the presence of this attribute.

Note that XMPP uses Simple Authentication and Security Layer (SASL) for authentication, enabling each deployment to make use of its own backend authentication mechanism such as Kerberos. Because of this, many applications will not need to use the username and password attributes. However, these attributes are included for those implementations which do not use backend authentication, or for implementations which do, but need a small number of static

identities such as might be associated with server accounts for which there is associated central identity management system in the enterprise.

6.1 xmppURIObject Object Class

```
OID: 0.0.8.350.1.1.9.2.1
objectclasses: (0.0.8.350.1.1.9.2.1
NAME 'xmppURIObject'
DESC 'XmppURI  object'
SUP top AUXILIARY
MAY ( xmppIdentityURI $ xmppUserId $ xmppPassword )
)
```

6.2 xmppIdentityURI attribute

```
OID: 0.0.8.350.1.1.9.1.1
attributetypes: (0.0.8.350.1.1.9.1.1
NAME 'xmppIdentityURI'
DESC 'Labeled URI format to represent an XMPP URI'
EQUALITY caseIgnoreMatch
EQUALITY caseIgnoreSubstringsMatch
SYNTAX 1 1.3.6.1.4.1.1466.115.121.1.15)
```

Application utility class

standard

Number of values

multi

Definition

Specifies an XMPP URI.

Permissible values (if controlled)

Notes

Implementers should review [IETF RFC 4622] for rules about escaping characters to ensure full international character set compatibility.

Semantics

Example applications for which this attribute would be useful

Example (LDIF fragment)

6.3 xmppUserId attribute

```
OID: 0.0.8.350.1.1.9.1.2
attributetypes: (0.0.8.350.1.1.9.1.2
NAME 'xmppUserId'
DESC 'Xmpp Userid'
EQUALITY caseIgnoreMatch
EQUALITY caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15)
```

Application utility class

standard

Number of values

multi

Definition

Holds the user ID of an XMPP user for authentication purposes.

Permissible values (if controlled)

Notes

Implementers should be aware that if a single H.350 directory serves multiple XMPP domains, it will not be possible to determine to which domain a particular user ID belongs. Care may be taken in the structure of the directory or in controlled access to the directory to ensure that this is deterministic.

This attribute is not necessary if backend authentication is used.

Semantics

Example applications for which this attribute would be useful

XMPP User ID and Password are useful if backend authentication is not used, or if implementation requires that users have multiple XMPP accounts.

Example (LDIF fragment)

6.4 xmppPassword attribute

```
OID: 0.0.8.350.1.1.9.1.3
attributetypes: (0.0.8.350.1.1.9.1.3
NAME 'xmppPassword'
DESC 'Xmpp password'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40)
```

Application utility class

standard

Number of values

multi

Definition

Holds the password of an XMPP user for authentication purposes.

Permissible values (if controlled)

Notes

Not necessary if backend authentication is used.

Semantics

Example applications for which this attribute would be useful

XMPP User ID and Password are useful if backend authentication is not used, or if implementation requires that users have multiple XMPP accounts.

Example (LDIF fragment)

7 xmppURIObject LDIF Files

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

```
# XmppURIObject Object Schema
#
# Schema for representing a XmppURIObject Object in an LDAP Directory
```

```
#
# Abstract
#
# This document defines the schema for representing XmppURIObject
# object in an LDAP directory [LDAPv3].  It defines schema elements
# to represent an xmppURIObject object [xmppURIObject].
#
#                      .1 = Communication related work
#                      .1.9 = xmppURIObject
#                      .1.9.1 = attributes
#                      .1.9.2 = objectclass
#                      .1.9.3 = syntax
#
#
#
# Attribute Type Definitions
#
#    The following attribute types are defined in this document:
#
#     xmppIdentityURI
#     xmppUserId
#     xmppPassword
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 genericIdentity
# 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're careful
#
delete: attributetypes
attributetypes:(0.0.8.350.1.1.9.1.1 NAME 'xmppIdentityURI' )
attributetypes:(0.0.8.350.1.1.9.1.2 NAME 'xmppUserId' )
attributetypes:(0.0.8.350.1.1.9.1.3 NAME 'xmppPassword' )
-
#
# re-add the attributes -- in case there is a change of definition
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.9.1.1
     NAME 'xmppIdentityURI'
     DESC 'Labeled URI format to represent an XMPP URI'
     EQUALITY caseIgnoreMatch
     EQUALITY caseIgnoreSubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.9.1.2
     NAME 'xmppUserId'
     DESC 'Xmpp Userid'
     EQUALITY caseIgnoreMatch
     EQUALITY caseIgnoreSubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.9.1.3
     NAME 'xmppPassword'
     DESC 'Xmpp password'
     EQUALITY octetStringMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
-
# Object Class Definitions
#
```

```
#    The following object class is defined in this document:
#
#        xmppURIObject
#
# xmppURIObject
#
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.9.2.1 NAME 'xmppURIObject' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.9.2.1
        NAME 'xmppURIObject'
        DESC 'XmppURI  object'
        SUP top AUXILIARY
        MAY ( xmppIdentityURI $ xmppUserId $ xmppPassword )
        )
-
#
# end of LDIF
#
```

8 ASN.1 representation

H.350.7 elements may be used in an X.500 directory architecture by using the ASN.1 representation of the object classes defined here.

```
XmppURIObject{ itu-t(0)  recommendation(0) h(8) 350 1 cr(1) xmpp(9) module(4) }
DEFINITIONS ::=
BEGIN

-- xmppURIObject Object Schema

-- Schema for representing a xmppURIObject Object in an LDAP Directory

-- Abstract

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

--                      .1 = Communication related work
--                      .1.9 = xmppURIObject
--                      .1.9.1 = attributes
--                      .1.9.2 = objectclass
--                      .1.9.3 = syntax

IMPORTS

-- from ITU-T Rec. H.350

h350-cr, caseIgnoreIA5Match, caseIgnoreIA5SubstringsMatch
     FROM CommURI { itu-t(0)  recommendation(0) h(8) 350 1 cr(1) commURI(1)
module(4) }

-- from ITU-T Rec. X.501 | ISO/IEC 9594-2

ATTRIBUTE, OBJECT-CLASS, top
     FROM InformationFramework {joint-iso-itu-t ds(5) module(1)
informationFramework(1) 4}

-- from ITU-T Rec. X.520 | ISO/IEC 9594-6
```

```
DirectoryString {}, caseExactMatch, caseExactSubstringsMatch, caseIgnoreMatch,
caseIgnoreSubstringsMatch, octetStringMatch
     FROM SelectedAttributeTypes {joint-iso-itu-t ds(5) module(1)
selectedAttributeTypes(5) 4} ;

-- Attribute Type Definitions

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

--     xmppIdentityURI
--     xmppUserId
--     xmppPassword

xmppIdentityURI ATTRIBUTE ::= {
     WITH SYNTAX DirectoryString {32768}
     EQUALITY MATCHING RULE caseIgnoreMatch
     SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
     ID { at 1 } }

xmppUserId ATTRIBUTE ::= {
     WITH SYNTAX DirectoryString {32768}
     EQUALITY MATCHING RULE caseIgnoreMatch
     SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
     ID { at 2 } }

xmppPassword ATTRIBUTE ::= {
     WITH SYNTAX OCTET STRING
     EQUALITY MATCHING RULE octetStringMatch
     ID { at 3 } }

-- Object Class Definitions

--    The following object class is defined in this document:
--
--        xmppURIObject

-- xmppURIObject

xmppURIObject OBJECT-CLASS ::= {
     SUBCLASS OF { top }
     MAY CONTAIN { xmppIdentityURI |
                   xmppUserId |
                   xmppPassword }
     ID { oc 1 } }

call-Id       OBJECT IDENTIFIER  ::=  { h350-cr call-Id(9) }
at        OBJECT IDENTIFIER  ::=  { call-Id at(1) }
oc        OBJECT IDENTIFIER  ::=  { call-Id oc(2) }

END -- end of ASN.1
```

9 DSML representation

H.350.7 elements may be described using the Directory Services Markup Language. That description is as follows.

```
<dsml:dsml xmlns:dsml='http://www.dsml.org/DSML'>
<dsml:directory-schema>


<dsml:attribute-type user-modification='false' id='#xmppIdentityURI'>
 <dsml:name>xmppIdentityURI</dsml:name>
```

```
 <dsml:description>Labeled URI format to represent an XMPP
URI</dsml:description>
 <dsml:object-identifier>0.0.8.350.1.1.9.1.1</dsml:object-identifier>
 <dsml:equality>caseIgnoreMatch</dsml:equality>
 <dsml:substr>caseIgnoreSubstringsMatch</dsml:substr>
 <dsml:syntax>1.3.6.1.4.1.1466.115.121.1.15</dsml:syntax>
</dsml:attribute-type>

<dsml:attribute-type user-modification='false' id='#xmppUserId'>
 <dsml:name>xmppUserId</dsml:name>
 <dsml:description>Xmpp Userid</dsml:description>
 <dsml:object-identifier>0.0.8.350.1.1.9.1.2</dsml:object-identifier>
 <dsml:equality>caseIgnoreMatch</dsml:equality>
 <dsml:substr>caseIgnoreSubstringsMatch</dsml:substr>
 <dsml:syntax>1.3.6.1.4.1.1466.115.121.1.15</dsml:syntax>
</dsml:attribute-type>

<dsml:attribute-type user-modification='false' id='#xmppPassword'>
 <dsml:name>xmppPassword</dsml:name>
 <dsml:description>Xmpp Password</dsml:description>
 <dsml:object-identifier>0.0.8.350.1.1.9.1.3</dsml:object-identifier>
 <dsml:equality>octetStringMatch</dsml:equality>
 <dsml:syntax>1.3.6.1.4.1.1466.115.121.1.40</dsml:syntax>
</dsml:attribute-type>

<dsml:class id='#xmppURIObject' superior='#top' type='auxiliary'>
 <dsml:name>xmppURIObject</dsml:name>
 <dsml:description>XmppURI object</dsml:description>
 <dsml:object-identifier>0.0.8.350.1.1.9.2.1</dsml:object-identifier>
 <dsml:attribute required='false' ref='xmppIdentityURI' />
 <dsml:attribute required='false' ref='xmppUserId' />
 <dsml:attribute required='false' ref='xmppPassword' />
</dsml:class>

</dsml:directory-schema>
</dsml:dsml>
```

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. This Annex A indexing profile describes an indexing configuration for xmppIdentityURI attributes that will be optimized for efficient call server lookup. Use of this profile is optional.

xmppIdentityURI: equality

xmppUserId: equality

Appendix I

Electronic versions of formal definitions

The formal definitions contained in this Recommendation are freely available in electronic format from ITU formal descriptions database http://www.itu.int/ITU-T/formal-language/index.html/ at the following addresses:

LDIF definition:

xmppIdentity.ldif: http://www.itu.int/ITU-T/formal-language/ldif/database/itu-t/h/h350.7/2007/index.html

ASN.1 definition:

xmppIdentity.asn: http://www.itu.int/ITU-T/asn1/database/itu-t/h/h350.7/2007/index.html

DSML definition:

xmppIdentityDSML: http://www.itu.int/ITU-T/formal-language/xml/database/itu-t/h/h350.7/2007/index.html

Bibliography

[b-LDAP 1] HOWES (T.A.), SMITH (M.C.), GOOD (G.S.): Understanding and Deploying LDAP Directory Services, *New Riders Publishing*, 1999, ISBN: 1578700701.

[b-LDAP 2] HOWES (T.A.), SMITH (M.C.): LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol, *New Riders Publishing*, 1997, ISBN: 1578700000.

[b-IETF RFC 3921] IETF RFC 3921 (2004), *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*.

[b-IETF RFC 3986] IETF RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Syntax*.

[b-IETF RFC 3987] IETF RFC 3987 (2005), *Internationalized Resource Identifiers (IRIs)*.

[b-IETF RFC 4422] IETF RFC 4422 (2006), *Simple Authentication and Security Layer (SASL)*.

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	Telephone transmission quality, telephone installations, local line networks
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

Printed in Switzerland
Geneva, 2007