

## Recommendation H.350.2 Directory Services Architecture for H.235

### Summary

This Recommendation describes an LDAP schema to represent H.235 elements. It is an auxiliary class related to H.350 and derives much of its functionality from that architecture. Implementers should review H.350 in detail before proceeding with this Recommendation. Its attributes include H.235 identity, password and certificate elements. These elements can be downloaded to an endpoint for automatic configuration or accessed by a gatekeeper for call signalling and authentication.

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 H.235 protocol, but rather to represent the minimal set required to accomplish the design goals enumerated in H.350.

### Keywords

LDAP, Directory Services, H.323, H.320, H.235, SIP

---

<b>Contact:</b>	Tyler Miller Johnson University of North Carolina at Chapel Hill USA	Tel: +1.919.843.7004 Fax: +1.919.843.7008 Email: Tyler_Johnson@unc.edu
-----------------	--	--

**Attention:** This is not a publication made available to the public, but **an internal ITU-T Document** intended only for use by the Member States of the ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of the ITU-T.

## Table of Contents

1	Scope .....	3
1.1	Extending the Schema .....	3
2	References.....	3
2.1	Normative References .....	3
2.2	Non-Normative References .....	3
3	Definitions .....	4
4	Abbreviations.....	4
5	Conventions .....	4
6	Object Class Definitions .....	4
6.1	h235Identity.....	4
6.2	h235IdentityEndpointID.....	4
6.3	h235IdentityPassword .....	5
7	h235Identity LDIF Files .....	6
A	Annex A Indexing Profile.....	8
I	Electronic Attachment .....	9

## 1 Scope

This Recommendation describes an LDAP schema to represent H.235 elements. It is an auxiliary class related to H.350 and derives much of its functionality from that architecture. Implementers should review H.350 in detail before proceeding with this Recommendation. Its attributes include H.235 identity, password and certificate elements. These aliases can be downloaded to an endpoint for automatic configuration or accessed by a gatekeeper for call signalling and authentication.

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 H.235 protocol, but rather to represent the minimal set required to accomplish the design goals enumerated in H.350.

### 1.1 Extending the Schema

The `h235Identity` classes may be extended as necessary for specific implementations. See the base H.350 document 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

### 2.1 Normative References

- ITU-T Recommendation H.235 (2000), *Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals*.
- ITU-T Recommendation H.350 (2003), *Directory Services Architecture for Multimedia Conferencing*.
- ITU-T Recommendation H.323 (2000), *Packet-based multimedia communications systems*.
- ITU-T Recommendation H.225.0 (2000), *Call signalling protocols and media stream packetization for packet-based multimedia communications systems*.
- IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification*.

### 2.2 Non-Normative References

- Timothy A. Howes, PhD, Mark C. Smith, Gordon S. Good, New Riders Publishing (1999), ISBN: 1578700701, *Understanding And Deploying LDAP Directory Services*.
- Timothy A. Howes, PhD, Mark C. Smith, New Riders Publishing (1997), ISBN: 1578700000, *LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*.

### 3 Definitions

The following terms used throughout the document:

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

**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.

### 4 Abbreviations

**LDAP:** Lightweight Directory Access Protocol as defined in RFC 1777.

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

### 6 Object Class Definitions

The h235Identity object class defines two attributes, h235IdentityEndpointID and h235IdentityPassword, which are needed to be able to implement H.235 Annex D. The remaining attributes that are used, and which are already defined in LDAP, are needed to be able to implement H.235 Annex E. Those attributes are userCertificate, cACertificate, authorityRevocationList, certificateRevocationList, and crossCertificatePair. The definitions and purpose of each of those attributes are defined in IETF RFC2256.

#### 6.1 h235Identity

```
OID: 0.0.8.350.1.1.4.2.1
objectclasses: (0.0.8.350.1.1.4.2.1
NAME 'h235Identity'
DESC 'h235Identity object'
SUP top AUXILIARY
MAY ( h235IdentityEndpointID $ h235IdentityPassword $
userCertificate $ cACertificate $ authorityRevocationList $
certificateRevocationList $ crossCertificatePair )
)
```

#### 6.2 h235IdentityEndpointID

```
OID: 0.0.8.350.1.1.4.1.1
```

```
attributetypes: (0.0.8.350.1.1.4.1.1
NAME 'h235IdentityEndpointID'
DESC 'The Sender ID as defined in ITU-H235.'
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 endpoint's senderID as defined in ITU-H235. This is always identical to endpointID.

#### Permissible values (if controlled)

#### Notes

In practice, there will always be one and only one h235identityEndpointID attribute for every endpoint. For applications where the endpoint authenticates against an LDAP directory, this value may be equal to the commUniqueId value defined in the H.350 document.

#### Semantics

Example applications for which this attribute would be useful

#### Example (LDIF fragment)

```
h235IdentityEndpointID: bobsmith
```

### 6.3 h235IdentityPassword

```
OID: 0.0.8.350.1.1.4.1.2
attributetypes: (0.0.8.350.1.1.4.1.2
NAME 'h235IdentityPassword'
DESC 'The endpoint password as defined in ITU-H325.'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

#### Application utility class

Standard

#### Number of values

multi

#### Definition

The endpoint's H.323 password as defined in ITU-T H.235.

#### Permissible values (if controlled)

#### Notes

In practice, there will always be one and only one h235IdentityPassword attribute for every endpoint.

If the password is stored in LDAP in encrypted format, then the LDAP encryption algorithm should match the encryption algorithm for the gatekeeper and endpoint, i.e. the gatekeeper and endpoint should support the same encryption format as the LDAP server, even as systems are upgraded over time. This is so the endpoint and gatekeeper may derive

the unencrypted password in order to perform H.235 Annex D operations. Since this may not always be possible, the password may be stored in LDAP in an unencrypted fashion. In this case, whenever the password is read by a gatekeeper or endpoint, that communication should be transacted over a secure transport mechanism, e.g. TLS.

## Semantics

Example applications for which this attribute would be useful

### Example (LDIF fragment)

```
h235IdentityPassword: 36zxJmCIB18dM0FVAj
```

## 7 h235Identity LDIF Files

This section contains a schema configuration file for h235Identity that can be used to configure an LDAP server to support this class.

```
# h235Identity Object Schema
#
# Schema for representing h235Identity Object in an LDAP Directory
#
# Abstract
#
# This document defines the schema for representing h235Identity
# object in an LDAP directory [LDAPv3]. It defines schema elements
# to represent an h235Identity object [h235Identity].
#
#           .1 = Communication related work
#           .1.4 = h235Identity
#           .1.4.1 = attributes
#           .1.4.2 = objectclass
#           .1.4.3 = syntax
#
#
# Attribute Type Definitions
#
# The following attribute types are defined in this document:
#
#           h235IdentityEndpointID
#           h235IdentityPassword
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 h235Identity
# 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: (0.0.8.350.1.1.4.1.1 NAME 'h235IdentityEndpointID' )
attributetypes: (0.0.8.350.1.1.4.1.2 NAME 'h235IdentityPassword' )
-
#
# re-add the attributes -- in case there is a change of definition
#
```

```
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.4.1.1
  NAME 'h235IdentityEndpointID'
  DESC 'The Sender ID as defined in ITU-H235v2.'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: (0.0.8.350.1.1.4.1.2
  NAME 'h235IdentityPassword'
  DESC 'The endpoint H.323 password as defined in ITU-H235v2.'
  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:
#
#       h235Identity
#
# h235Identity
#
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.4.2.1 NAME 'h235Identity' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.4.2.1
  NAME 'h235Identity'
  DESC 'h235Identity object'
  SUP top AUXILIARY
  MAY ( h235IdentityEndpointID $ h235IdentityPassword $
    userCertificate $ cACertificate $
    authorityRevocationList $ certificateRevocationList $
    crossCertificatePair )
  )
-
#
# end of LDIF
#
```

## **Annex A: Indexing Profile**

### **A Annex A Indexing Profile**

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. The Annex A Indexing Profile describes an indexing configuration for h235Identity directories that will be optimized for use in directory of directories applications. Use of this profile is optional.

h235IdentityEndpointID: no recommendation

h235IdentityPassword: equality

## Appendix I Electronic Attachment

### I Electronic Attachment

The attached file `h235Identity.ldif.txt` contains a text only version of the LDIF file described in section 7.



`h235Identity.ldif.t`  
`xt`

---