A Common Schema for the Internet White Pages Service

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

Overview

The IETF Integrated Directory Services (IDS) Working Group proposes to establish a specification for a simple Internet white pages service. To facilitate this effort it would be helpful to have a common schema used by the various white page servers. This document is designed to specify the basic set of attributes to be used for a white page entry for a person. This schema does not describe how to represent other objects in the White page service. It does describe how new objects can be defined and registered. This schema is independent of implementations of the White Page service.

1.0 Introduction

The Internet community has stated that there is a need for the development and deployment of a White Page service. This service would be used to locate information about people in the Internet. To facilitate interoperability and a common user experience the Internet White Pages service needs to have a common set of information about each person.

This Document will focus only on common information modeling issues to which all IWPS providers must conform. To insure a consistent User experience of this service we need to define a common User object. This will allow a User to go between different implementations of the service and have a consistent expectation as to what information can be found about people on the Internet. Developers of this service need to have an unambiguous method of representing the Information
objects managed by the service. This will help facilitate interoperability and data management.

2.0 Scope

This document attempts to establish a simple set of information objects templates that should prove extensible and usable by developers of the IWPS. It will not attempt to be an exhaustive specification of all objects that will be stored in the IWPS. It will provide a specification of how objects will be defined and registered as part of the IWPS.

3.0 IWPS Schema Considerations

The information object description requirements for the IWPS consists of the following:

1. Syntax for definition/representation of Information Object Templates.
2. Registration procedures for information object Templates, etc.
3. Database structure or schema.

Items 1 and 2 will be covered in this Document. Database structure because, it will potentially restrict implementations (i.e. X.500 schema based Vs DNS schema based) will not be defined in this document. This area is a separate Research topic and will be covered in its own document.

3.1 Syntax for definition/representation of Information objects

A clear, precise and consistent method must be used when information object Templates and their attributes are discussed within the context of IWPS. There are two possible methods to do this. i.e.

1. BNF
2. ASN.1

The Working Group recommends the use of ASN.1. It provides us with a set of defined attributes and encoding syntax’s. Also, it is well documented and widely available.

The use of ASN.1 to specify the structure of the information objects does not imply the use of Basic Encoding Rules (BER) for any IWPS servers protocols. The use of Object inheritance is not used or specified by this document.

3.2 Registration of IWPS Information object Templates.
The Working Group recommends the registration and publication of all information object Templates used for the IWPS. We will use the IANA branch of the ISO OID tree for registration of the IWPS Object Templates. This branch was used by the Object Templates listed in Appendix A. To facilitate distribution of IWPS information object Templates they should be made available on the Internet information server (i.e. InterNIC). At a minimum it is recommended that any new information object Template that will be made available via the IWPS will be published in a RFC and its OID registered with IANA.

Individual organizations may define information object Templates that are only local in scope. This may be needed to meet local organizational needs. If these information object Templates are not registered with the IWPS, they may not be processable by the general IWPS UAs. All information that the organization wishes to be part of the IWPS must use an IWPS registered information object Template.

4.0 Security Certificates

Another feature that IWPS can provide us is the ability to store Security Certificates. This capability is needed by secure mail services such as PEM and PGP. To facilitate the storage and management of these Certificates a new element is defined for the iwpPerson object. This new element will allow multiple Certificates to be stored with the person record. It also allows for the deprecation of certificates through the use of a validity field. This field is used to state the beginning and end dates the certificate is valid. The element "certificates" is defined in Appendix A.

5.0 Data Integrity

The question of Data Integrity was first addressed in RFC1107 [KS89]. It basically states, that if the information is out of date it is useless and the service will not be used. Therefore, a clear requirement is that any production IWPS provider must insure that all data is reasonably correct and current.

To facilitate the User in determining the quality of the data that has been retrieved it is recommended that the optional Ancillary information attribute of the IWPperson Template be supported. This would require the IWPS UA to be able to retrieve and display this information. This may be done as a separate operation from the fetch of the information object. The Ancillary Information Attribute is defined in Appendix A. It is further recommended that any new information object Template include as a minimum the Ancillary information attribute as an optional attribute. It would then be left to the IWPS servers to optionally support the storage and retrieval of this data.
The Ancillary Information attribute has been designed to provide the following information about the information object with which it is associated:

1. The date and time of the last modification.
2. Who performed the last modification.
3. Who owns or is responsible for the data stored in the information object.
4. What is the official source of the data.
5. Which attributes in the information object have been changed.

As new information object Templates are defined for the IWPS a new changeRecord type will need to be defined for it and assigned to the changeRecord attribute.

This attribute is not a part of the White Page Name (WPN). Where WPN is an identifier for an instance of Information Object Template. The WPN is constructed from the attributes of the Object. The Ancillary Information attribute is not to be used as part of the Purported Name presented to the IWPS UA.

6.0 Unstructured Data

There are a number of existing directory based systems that are currently providing White Pages style of information. These systems respond to queries by returning information without regard to any structure of the data. There is nothing in their protocol specifications that identify individual fields or attributes in the response that would allow it to be machine processable.

To accommodate these systems and the way they return information, the element unstructureData has been added to the iwpPerson object. This element consists of a 1k block of data without any structure or content requirements. It can be used to represent/store any of the current sets of White Pages information.

It should be noted that this element is added for backward compatibility of the existing systems only. It should not be used for the development of any new white page service.

7.0 References

Appendix A Information Object Template Definitions

The Information Objects Template and attributes defined in this appendix are used to define the contents of Information Objects of the IWPS. In particular the Template defined below deals with the person Object. Any new Information Object must be registered with IANA.

-- The Information Object Template for the IWPS person --

iwpPerson OBJECT-CLASS
  SUBCLASS OF top
  MUST CONTAIN{
    commonName,
    wpi}
  MAY CONTAIN{
    surname,
    organizationalName,
    postalAddress,
    telephoneNumber,
    emailAddress,
    certificates,
    unstructuredData,
    ancillaryInformation}
::={iwpsObjectTemplate.1}

-- The WPI attribute to be use by Information Objects of the IWPS --

wpi ATTRIBUTE
  WITH ATTRIBUTE-SYNTAX
caseIgnoreStringSyntax
  ((SIZE(1..ub-iwps-wpi))
::={iwpsAttributeType 2}

-- The element for the storage of Email information --

emailAddress ATTRIBUTE
  WITH ATTRIBUTE-SYNTAX EmailAddress
::={iwpsAttributeType 1}

EmailAddress ::= SEQUENCE (SIZE(1..ub-email-boxes)) OF
  caseIgnoreString(SIZE(1..ub-email-addr))

-- The element to be used to store Security Certificates --

certificates ::= ATTRIBUTE WITH ATTRIBUTE-SYNTAX
  Keys{iwpsAttributeType 3}

Keys ::= SEQUENCE (SIZE(1..ub-keys)) OF keyInfo

keyInfo ::= SEQUENCE{
  validity    Valid,
  key         KeyType}

Valid ::= SEQUENCE{
  notBefore    UTCTime,
  notAfter     UTCTime}

KeyType ::= SEQUENCE{
  algorithm    OBJECT IDENTIFIER,
  subjectKey   caseIgnoreStringSyntax(SIZE(1..ub-keysize))}

-- The Unstructured Data element used to contain free form data --

unstructuredData ::= caseIgnoreStringSyntax(SIZE(1..ub-data))

-- The Ancillary Information attribute used for data integrity --

ancillaryInformation ::= SEQUENCE{
  LastModifiedDate
    UTCTime,
  LastModifiedBy,
    commonName,
  OwnerofData,
    commonName,
  OfficialSourceofData
dataBase,
  WhatWasChanged
    changeRecord}
database ::= caseIgnoreStringSyntax(SIZE(1..ub-database))

-- Change record subtypes are the MUST CONTAIN attributes --

changeRecord ::= iwpsPersonType (commonName | wpi)

iwpsPersonType ::= 
BIT STRING {
    commonName             (0),
    surname                (1),
    organizationalName     (2),
    postalAddress          (3),
    telephoneNumber        (4),
    emailAddress           (5),
    wpi                    (6)
}

-- Size limits used by the IWPS --

ub-database            INTEGER ::= 1024
ub-data                INTEGER ::= 1024
ub-email-boxes         INTEGER ::= 8
ub-email-addr          INTEGER ::= 1024
ub-keys                INTEGER ::= 6
ub-keysize             INTEGER ::= 512
ub-iwps-wpi            INTEGER ::= 256

-- Object Identifiers use by the IWPS --

Internet OBJECT IDENTIFIER ::= {ISO(1) org(3) DOD(6) 1}
iwps OBJECT IDENTIFIER ::= {Internet NN}
iwpsAttributeType OBJECT IDENTIFIER ::= {iwps 1}
iwpsObjectTemplate OBJECT IDENTIFIER ::= {iwps 2}