

# Extensible Resource Identifiers and Descriptor Sequences, a key to what is becoming a standard within the internet digital identity layer:

Using XRI and XRDS together to create abstract structured identifiers.

XRI is the interface, or abstract identifier containing metadata to describe the resource. XRDS is the standard providing the discovery process derived from the the XRI interface. Together and separate these two standards have become key building blocks of the internet identity layer, and provided synergy with other Oasis specifications.

XRI is a new type of internet identifier, built upon the latest IRI standard and designed expressively to work with digital identity. XRI is an open standard for expressing and discovering Abstract Structured identifiers.

“XRI and XRDS have become essential elements of the Higgins Project. Without them, we couldn’t fully implement the abstract data model that is the heart of Higgins and the key to the user-controlled identity and data sharing.”

- Paul Trevithick  
**Higgins Project Lead**

## What is XRI

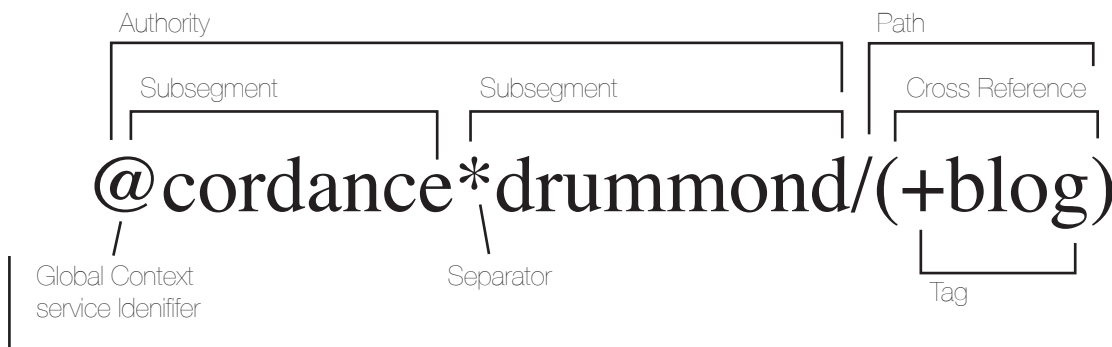


fig. 1

Abstract - Identifiers which are known to resolve to other identifiers, or multiple identifiers which are known to resolve to the same concrete identifier.

Structured - Identifiers which may contain self-describing data, using standard building blocks acting like “XML for identifiers”.

The specification allows for:

Persistence- Identifiers which are still abstract and discoverable, yet are not re-assignable throughout the life of object.

For example, XRI contains built in global context identifiers to resolve to organizations, individuals, tagged items and/or persistent items. Thus the same resolvable location can abstractly be described and discovered through two different global contexts.

Note: the “\$” is reserved for internal system use and is used as URNs.

=example | = 例子\*example | @example/(+contact) | @!B3A7.5537.9FEA.31EC!133 |  
+flower | \$xml

XRI's have applied for an URI schema space, however can be used with existing technologies. It is designed to run on top of existing protocols including HTTP (HXRI).

QXRI

xri://@example.com\*john.doe

HXRI

http://resolve.freexri.net/ns/=drummond

## What is XRDS

XRDS is the standard document which describes how an XRI will resolve to a given resource and provides discovery services for XRI identifiers. It is simple, extensible and XML based. It is a discovery format for any XRI or URL-identifiable resource. It is the logical equivalent of a DNS Zone record for XRI resolution. XRDS is a standard also being used within other standards such as OpenId 2.0, OAuth and Higgins.

XRDS through the discovery process can bind together various abstract identifiers and authenticate against a persistent identifier to provide a base level of identity authentication. It is the building block for other identity solutions.

```
<?xml version="1.0" encoding="UTF-8"?>
<XRDS>
  <XRD>
    <Query>*example</Query>
    <ProviderID>xri://=</ProviderID>
    <ProviderID>xri://!776A.F060.AACC.1F3D</ProviderID>
    <Service priority="10">
      <Type select="true">xri://$res*auth*($v*2.0)</Type>
      <URI>http://res.example.com/=!776A.F060.AACC.1F3D</URI>
    </Service>
    <Service priority="10" >
      <Type>http://openid.net/signon/1.1</Type>
      <Type>http://openid.net/signon/2.0</Type>
      <Path>+openid</Path>
      <URI>http://res.example.com/openid/</URI>
    </Service>
  </XRD>
</XRDS>
```

## How XRI and XRDS work together.

Generally an i-names registrar (www.inames.net) assigns two identifiers to a person. Which is logically broken into the categories i-number (persistent) and i-name (abstract)

The persistent and abstract identifier can both be used to resolve to a concrete identifier such as a telephone number, fax number or other “real-world” identifier or digital resource.

For example:

```
=!7edf.92ee.f2a5  
=drummond  
=drummond/phone/(+mobile)  
=drummond/phone/(+office)
```

note:

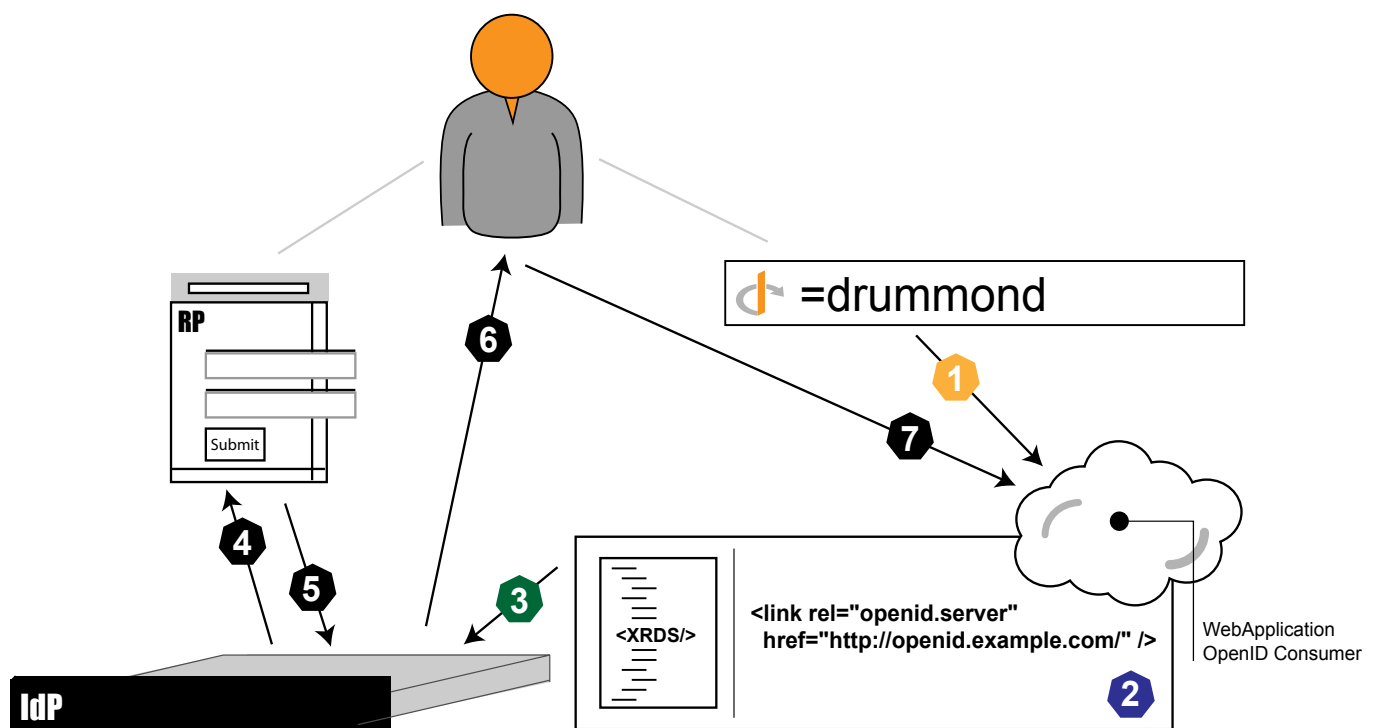
=durmmmond and (!7edf.92ee.f2a5) both resolve to the same XRDS document

Within the XRDS document, service end point resolution is performed for a mobile telephone number and an office phone number respectively.

The correct resolved number is returned within an XML response.

## How XRI helps solve some problems for OpenID 2.0

“Not only did XRI and XRDS become an integral part of OpenId 2.0, but the XRI technical community has become an integral part of the OpenID community” - Bill Washburn, Executive Director, OpenID Foundation



Steps:

1. User posts to login OpenID identifier
2. Extensible discovery process of the OpenID Provider (OP) initiated by the web application
3. The OP generates a shared secret
4. Resolution to the OP login
5. User logs in to the OpenID provider using a username and password
6. The OP redirects back to the user
7. Results of the OP login are posted to the web application

XRI and XRDS helped solve the following problems:

## 1. Post to login with re-assignable identifiers

Problem:

When the service provider controls username they control the binding of the user profile with the password. However with OpenId, the user controls binding of the credential. Therefore if a user loses control of the identifier they lose control of the credential.

Solution: ***Persistent synonyms***

With XRI a user can bind a recyclable OpenID identifier with a non-recyclable (persistent) identifier, such as an XRI i-number.

The authentication process will always use the persistent identifier and treat the recyclable OpenID identifier as a temporary handle for the persistent identifier. Therefore always protecting the user from losing control of an identifier.

## 2. Extensible discovery process

Problem:

Beginning with OpenID 2.0, there became a need to describe what versions of OpenID an identifier supported. Also what OpenID extensions a identifier supports such as SREG, AX, PAPE, etc. or what services may be available like OAuth, SAML or XDI. The discovery process needed to be redundant, and allow for prioritized OpenID provider endpoint URLs

Solution: ***XRDS documents***

XRDS documents are a simple, standards based discovery format, which can be hosted on any web server, Identity Management system, blog, etc. XRDS documents are easily extensible by using new URIs or XRIs to define service types or with elements from other XML namespaces.

### 3. Automatic secure resolution to the OpenID provider login

Problem:

When using a URL as an identifier, OpenID could not specify HTTPS resolution for **all** OpenID URLs for reasons such as; too many users do not have access to HTTPS certificates or server infrastructure to implement HTTPS. Therefore the default resolution process would require only HTTP, forcing those who wished to use secure resolution to enter the entire HTTPS URL including the HTTPS scheme to specify its use.

Solution: **XRI secure resolution**

As abstract identifiers XRIs always resolve to concrete identifiers. Through the XRI resolution process three trusted modes may be used; which are HTTPS, SAML or both. XRI identifiers used as OpenIDs can use HTTPS resolution as the default and users have no need to install or know anything about how they are being protected throughout the resolution process.

## XRI and XRDS are building blocks for other Identity solutions

XRI and XRDS are also used in the following solutions:

OAuth

XRDS discovery

Higgins Project

Context discovery and resolution

SAML and Information Cards

Privacy protected identifier claims

XDI.org

i-name/i-number registries and resolution

## Conclusion

XRI abstract identifiers offer three key features for the internet identity layer:

Simple, safe strong identifiers

Simple, extensible, secure service discovery

Interoperability between multiple identity protocols and frameworks

**XRI and XRDS are building blocks everyone can use**

# Glossary

---

Concrete identifier

An identifier which is linked to a hard resource

Abstract identifier:

An identifier which is linked to one or more concrete identifiers

Structured Identifier:

Persistent Identifier:

Discovery:

The process of finding service endpoints for service types, such as OpenId or (+contact) when using i-names.

i-name:

An XRI which is managed by XDI.org

i-number:

A persistent XRI which is managed by XDI.org

IRI:

A superset of URI which extends to international character sets

URI:

Uniform Resource Identifier, a string of characters used to identify a resource

URN:

Uniform Resource Name, a subset of URI which does not imply the availability of a resource These can be used in cross-references with XRIs

SAML:

SREG:

AX:

PAPE:

XDI:

OpenID: