Network Information System

Data Access Server: Auditing LTER Data Access

Project Plan (Version 1.0)

03 October 2012

Mark Servilla
servilla@LTERnet.edu

LTER Network Office
Department of Biology, MSC03 2020
1 University of New Mexico
Albuquerque, NM 87131-0001

Revision History

Date	Version	Description	Author
1 October 2008	1.0	First creation of document.	M. Servilla
17 October 2008	1.0	Incorporated edits from D. Costa.	D. Costa
20 October 2008	1.0	Additional edits in section 3 – General Timeline.	M. Servilla
12 November 2008	1.0	Rewrite of Section 2.2 following VTC discussion with Wade Sheldon	D. Costa
13 November 2008	1.0	Simplified Section 2.2 by collapsing options into Section 4.0 (Appendix – Registering Multiple urlHead Values).	M. Servilla
3 December 2008	1.0	Provided minor edits to Section 4. Added content for *data use statement* in Section 2.1 and *end user email notification* in Section 2.3. Added email templates as Sections 5 and 6 (Appendices).	M. Servilla
18 February 2009	1.0	Changed all references to 'das.lternet.edu' to 'metacat.lternet.edu'. Added generic email header to notifications in Sections 5 and 6. Added Section 7 – EML Dependencies to document.	M. Servilla
3 October 2012	1.0	Changed servlet context reference in URLs from “/knb” to “/das” where relevant.	M. Servilla

Table of Contents

Preface

The following document is the “Data Access Server” Project Plan. The Data Access Server (DAS) is a model for abstracting access to LTER generated data behind a proxy server that provides key services in support of the LTER Data Policy, including authentication, auditing, and notification. This document includes a description of the motivation behind DAS, a design specification, and use case scenarios, which describe the operation of the DAS. Parts of this document come from the original Request for Comments text (http://intranet.lternet.edu/archives/documents/Newsletters/DataBits/07fall/#fa3). This document should be considered a living document until the “Final” label appears next to the version number on the title page.

This document should be used in lieu of a second revision of the Request for Comments. Comments and or questions should be forwarded to Mark Servilla at the LTER Network Office (servilla@LTERnet.edu).

1 Introduction

The LTER Network has invested considerable time, effort, and funding into the collection of scientific data. Access and use of this data is formalized through the end user's acceptance of the LTER Network Data Access Policy, Data Access Requirements, and the General Data Use Agreement (http://www.lternet.edu/data/netpolicy.html), which were approved by the LTER Network Coordinating Committee on 6 April 2005. Motivation behind these policies and agreements is driven by the need to document the flow of data from the LTER Network out to the community to validate broader impacts of the LTER program. As such, the LTER Network has adopted a "standard" for data *access* and *use* that needs to be implemented into both local and network-wide computing infrastructure. This standard requires that the end user provide basic identifying information, including name, affiliation, email address, and contact information, in an electronic format that can be provided to the data owner. Further, acknowledgment and acceptance of either the General Public Use Agreement and or the Restricted Data Use Agreement applied to a data set, and a statement of the intended use of the LTER data, will be recorded prior to the release of any LTER data.

The following document outlines a plan, as part of the LTER Network Information System, to support sites in their compliance with LTER data policies. This plan will provide sites with the ability to replace “direct link” data URLs with proxy URLs, which will route all data requests through an authentication, auditing, and notification service called the Data Access Server (DAS). The DAS will support five primary objectives that have been defined through analysis of use case scenarios (refer to DAS-UseCase.odt):

1) end user registration and acceptance of the LTER data agreements, including authentication;
2) URL management;
3) notification of data access to the Data Set Contact;
4) auditing of all data access; and
5) reporting.

Each of these objectives are discussed in greater detail below in section 2.

The basic notion of the DAS is that sites may register a data URL expression into the DAS URL management interface and replace the data URL with a similar representation using a proxy URL. The goal of the DAS is to route end users (including non-interactive applications) through the DAS so that access to LTER data can be logged and the appropriate contact be notified about the access event. The DAS strives to use as much existing LTER cyberinfrastructure as reasonable, including:

1) the LTER Data Catalog servlet infrastructure to support the integration of DAS components;
2) Ecological Metadata Language documents in the LTER Data Catalog to identify appropriate contact information for notification and to ascertain data table entity names; and
3) the LTER LDAP for end user contact information and authentication (authentication will also use LDAP databases of our affiliate networks, such as NCEAS and PISCO).

A graphical representation of the DAS network topology is shown in Figure 1.

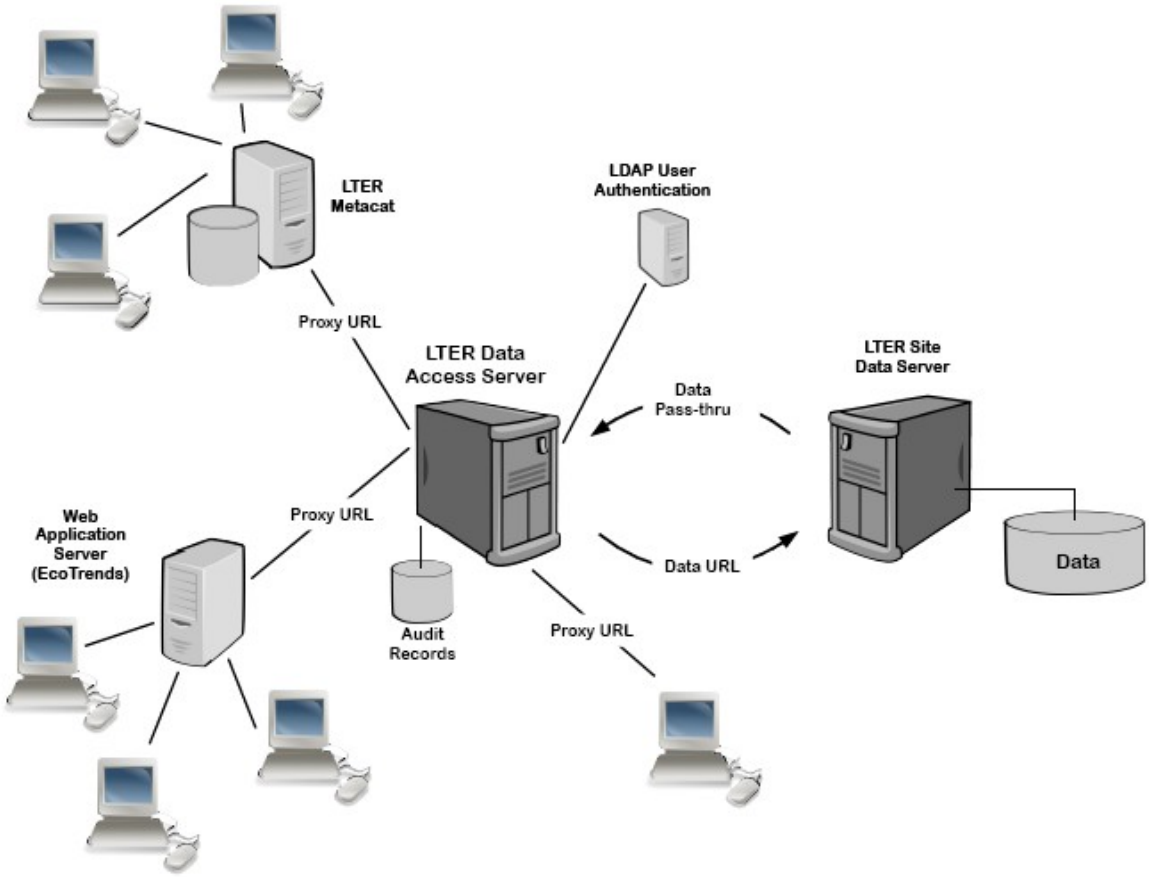

Figure 1: Hypothetical network topology of the Data Access Server.

The DAS project plan has shifted from the original DAS Request for Comments

(http://intranet.lternet.edu/archives/documents/Newsletters/DataBits/07fall/#fa3) in four significant areas:

1. The DAS is no longer focusing on Internet persistence of digital objects as a key objective. There are other initiatives that are addressing this issue, including Digital Object Identifiers (DOI), Life Science Identifiers (LSID), Persistent URLs (PURL), and Archive Resource Keys (ARK). More recent examination of the standard URI specification shows that it too can perform the role of a persistent identifier through carefully constructed URLs.
2. The proxy URL will no longer be represented by an obscure string (e.g., an MD5 hash value as described in the original RFC); in lieu of the MD5 hash value, the URL will be constructed of a proxy component (the part of the URL that directs data access through the DAS) and a site component (the part of the URL that uniquely identifies the requested data set). We believe that the DAS should allow sites to replace data URLs with a proxy that is closest to their original form, thereby limiting the mapping complexity between URLs and to allow URLs that point to dynamically generated data objects. The proxy URL will still obscure direct access to LTER data by replacing the domain name component (and any other non-varying path component) of the data URL with the proxy address. This will significantly reduce the number of entries in the DAS URL management database.
3. The DAS will require that all data referenced through its services must have a corresponding Ecological Metadata Language document in the LTER Data Catalog (more specifically, the LTER Metacat) for the following reasons:
   a) data access notification will rely on the appropriate contact information found in the corresponding EML document;
   b) where available, the file name used for identifying the data stream through the proxy pass-through will use the “object” name identified in the EML document; and
   c) the proxy URL will require the EML document id as part of the URL query string.
4. The DAS will be integrated with the LTER Data Catalog interface and will jointly use the LDAP authentication performed as part of the Metacat API, if applicable, otherwise a separate database will manage users external to the LTER Network.

We believe that this union of applications is both logical and intuitive for users of the LTER Data Catalog. This approach will not preclude the use of proxy URLs in venues outside of the LTER Data Catalog.

2 General Design

The DAS design is, in principle, identical to that described in the original RFC – end users attempting to access an LTER data set via a data URL will be routed through the Data Access Server by way of a proxy URL. As described briefly above, the DAS serves four primary objectives:

1) end user registration and authentication;

2) URL management;

3) data access notification;

4) data access auditing; and

5) reporting.

The DAS is designed to be an extension to the LTER Data Catalog, and is, therefore, written as a set of Java Server Pages and Servlets that interact with the LTER LDAP, the Metacat, and the audit database that is already integrated into the LTER Data Catalog (Figure 2). Additional database tables will be utilized to register non-LTER end

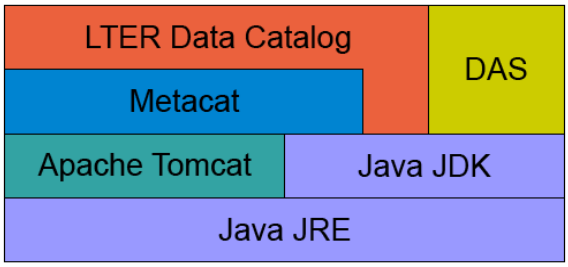

Figure 2: Relationship of the Data Access Server software with other components.

users and to record user acceptance to the LTER data agreements.

2.1 End User Registration and Authentication

According to the LTER Network Data Access Requirements statement, an end user must accept the General Public Use Agreement and/or the Restricted Data Use Agreement prior to obtaining access to any LTER Network data. Further, the end user must register specific information (e.g., Name, Affiliation, Email Address, and Full Contact Information) to be recorded for the purpose of tracking data usage, evaluate community impact of the data, and confirm the user's acceptance of the LTER data agreements (http:// www.lternet.edu/data/netpolicy.html). Finally, the end user must submit a statement of their intended use of the data. The DAS will comply with these requirements by confirming that an end user who is requesting access to DAS managed LTER data is registered as part of the LTER Data Catalog user base and has accepted the LTER data agreements. In addition, the DAS will attempt to make the registration and authentication process as seamless and transparent to the end user as possible.

The DAS recognizes two different classes of end users with respect to registration:

1) those directly associated with the LTER Network (i.e., those that have a record in the LTER LDAP); and

2) all others.

Registration/contact information will be maintained in either the LTER LDAP for LTER users or a separate table within the DAS relational database for all others. Maintaining contact information in the LTER LDAP, where possible, will eliminate the need for synchronization between two separate tables. It is unlikely, however, that the LTER LDAP will accommodate the intended data use statement. This statement will be recorded in a separate table of the DAS relational database for both LTER and non-

LTER users. Similarly, acceptance of the LTER data agreements for both LTER and non-LTER users will be recorded into a single table within the DAS relational database[1].

End user authentication is divided into three classes:

1) those in the LTER LDAP;
2) those in an affiliated network (e.g., NCEAS, PISCO, etc.) that is part of the ecoinformatics LDAP referral system; and
3) all others.

End users in classes 1 or 2 will be able to use their LDAP user name and password for authentication purposes (users in class 2, however, will be required to register their contact information). Users in class 3 will be required to create a user name and password during the registration process. The user name and password, along with the required user contact information, will be maintained in a registration table within the DAS relational database.

The following general use case scenario associated with end user registration and authentication is invoked at the point when a user attempts to access LTER Network data through a DAS proxy URL:

1. If the user is not authenticated, they are directed to the LTER Data Catalog user management page to login into the system.
   a) If the user is registered in the LTER LDAP or a network affiliate or as a DAS user, they may use their respective account information to login into the system.
   b) If the user is not registered in the LTER LDAP or a network affiliate or as a DAS user, they are directed to the DAS user registration page. The user is authenticated immediately after registration.
2. If the end user has not accepted the LTER data agreements they are directed to the General Public Use Agreement and or the Restricted Data Use Agreement references and are requested to accept or decline the agreements.
3. If the user is registered in the LTER LDAP, the system will confirm that the required user contact information is sufficient, otherwise the user will be requested to complete the contact information. Users of network affiliates or who have registered as a DAS user are required to enter the appropriate contact information. Once the agreements have been accepted and all contact information is confirmed, the data access process will proceed.

Authentication remains a complex issue that will be addressed by the DAS in multiple phases:

Phase 1 – The initial phase of the DAS will consider only human interactive authentication and data access through web-browser technology. The authentication process will support “cookie-based” tokens, which will afford an automatic login for end users whose web browsers support and allow cookies. Those users whose web browsers do not support or allow cookies will be

1 The LTER LDAP does not currently support an attribute for recording acceptance of the LTER data agreements .

required to authenticate for each web session.

Phase 2 – The initial requirement of human interactive authentication disenfranchises secondary applications that would be directed through the DAS during a request for LTER data (e.g., Kepler). For this reason, the DAS development team will immediately begin investigating methods of proxy authentication. Such authentication methods may include direct management of X.509 certificates or integration of service applications, like myProxy.

2.2 URL Management

The primary purpose of the DAS is to route Internet users attempting to access LTER data through an audit service by way of a proxy URL in lieu of direct access to data through a data URL. As such, the URL management functionality of the DAS serves two very important purposes:

1. it provides a mechanism for a site Information Manager to transform a site data URL to a DAS proxy URL; and
2. it provides a mechanism for the DAS service to translate a DAS proxy URL back to its original site data URL.

The DAS will provide and maintain a user interface designed to assist in the management of these functions.

Before explaining how the DAS will provide URL management and how a proxy URL will be translated back to a site data URL, it is crucial to understand how the DAS characterizes site data URLs.

2.2.1 Characterizing Site Data URLs

Analysis of site data URLs have shown that they are, in general, composed of two parts:

1. a leading “non-varying” component that directs end users to the site's web server and, possibly, a hierarchical path to the site's data store (referred to herein as the **urlHead**); and
2. a trailing or “varying” component that uniquely identifies the requested data object (referred to herein as the **urlTail**).

The following data URL demonstrates this concept :

```
http://ecosystems.mbl.edu/PIE/data/MAR/data/LTE-MP-NAC-biomassmeans.dat
```

In this example, the **urlHead** is:

```
http://ecosystems.mbl.edu/PIE/data/
```

and the **urlTail** is:

```
MAR/data/LTE-MP-NAC-biomassmeans.dat
```

In this case, the **urlHead** component includes a Fully Qualified Domain Name (FQDN) that points to a host server (**http://ecosystems.mbl.edu**) and a hierarchical path that consists of simple data directory (**/PIE/data/**). The **urlTail** component is of a path/file combination that varies based on the month of the year, in this case “MAR” for March,

and ends with a single data ".dat" file (**MAR/data/LTER-MP-NAC-biomassmeans.dat**).

This same two-part pattern is also evident in more complex data URLs as shown in the example below:

```
http://gce-lter.marsci.uga.edu/public/app/send_file.asp?
lnoproxy=yes&accession=PLT-GCET-0711&filename=PLT-GCET-0711_2_1.TXT
```

where, the **urlHead** is:

```
http://gce-lter.marsci.uga.edu/public/app/send_file.asp?lnoproxy=yes&
```

and the **urlTail** is:

```
accession=PLT-GCET-0711&filename=PLT-GCET-0711_2_1.TXT
```

In addition to the FQDN and hierarchical path (**http://gce-lter.marsci.uga.edu/public/app/**), this **urlHead** example includes a dynamically executed server-side script and a partial set of parameters (**send_file.asp?lnoproxy=yes&**). The **urlTail** consists of the remaining parameters for the server-side script (**accession=PLT-GCET-0711& filename=PLT-GCET-0711_2_1.TXT**).

From these two examples it should begin to be obvious that additional data objects can be accessed by appending a new **urlTail** to the same **urlHead**. This repetitive pattern is the guiding principle of the DAS proxy URL translation process – because the urlHead is constant, it now becomes a key field held within the DAS database when used by the proxy URL when looking for the actual data. Beware that this approach does not imply fixed rules for determining exactly where the **urlHead** component should be split off from the **urlTail** component for the data URLs at a given site. In fact, it is up to the site Information Manager to specify where data URLs should be split. The only requirements enforced by the DAS URL scheme are that:

1. the **urlHead** is the leading part of the data URL that is common to a collection of data objects at the site; and
2. concatenation of the **urlHead** and a given data object's **urlTail** will result in the complete URL to that data object.

2.2.2 Registering the urlHead

Now that the basic process of characterizing the data URL into the **urlHead** and **urlTail** is defined, the next step is to register the **urlHead** into the DAS database. The **urlHead** is used by the DAS when translating the proxy URL back into the site data URL. Most sites will have only a single **urlHead** entry in the DAS database (see Section 4 to register multiple **urlHeads**). This entry will correspond to the the site's three letter acronym, the **urlHeadID**, and the actual **urlHead** value. Using the PIE LTER site example in this section, the registered value would be:

Site	urlHeadID	urlHead
PIE	1	http://ecosystems.mbl.edu/PIE/data/

2.2.3 Composing the DAS Proxy URL

The DAS proxy URL is the URL expression that replaces the site data URL. It can replace the data URL in any document where a data set is exposed to an end user,

including the data distribution element within an EML document, on the site's public web site, or as a reference within a published manuscript. An example of a proxy URL follows below:

```
http://metacat.lternet.edu/das/dataAccessServlet?docid=knb-lter-pie.135.17&
                urlTail=MAR/data/LTE-MP-NAC-biomassmeans.dat
```

Similar to the data URL, the proxy URL is also defined by two parts:

1. a proxy component (the part of the URL that directs data access through the DAS); and
2. a site component (the part of the URL that specifies access to a particular data object at the site, including associated metadata).

The proxy component is simply the FQDN of the DAS network address and the server-side servlet that analyzes the site component of the proxy URL to perform the necessary proxy to host translation. The full proxy component is:

```
http://metacat.lternet.edu/das/dataAccessServlet?
```

The site component consists of two required URL request parameters that are passed to the server-side servlet[2]. These parameters are:

1. the EML document identifier as specified by "**docid=knb-lter-pie.135.17**"; and
2. the **urlTail** (see Section 2.2.1) as specified by "**urlTail=MAR/data/LTE-MP-NAC-biomassmeans.dat**".

The full site component is:

```
docid=knb-lter-pie.135.17&urlTail=MAR/data/LTE-MP-NAC-biomassmeans.dat
```

The document identifier parameter serves two purposes: First, it identifies which site the data should be accessed from and thus determines which **urlHead** component should be applied. In the above example, the site would be determined to be "PIE", and the **urlHead** component registered for the PIE site would be applied by the DAS when forming the original data URL.

Second, it specifies which EML document to look up in the LTER Data Catalog to obtain metadata about the specific data object being retrieved. The DAS will read the EML document to determine contact information (i.e. who should be emailed about this data access) and the entity name (i.e., what file name should be used when downloading the data to the end-user's desktop).

Note that the document identifier value may be specified with or without a revision number. If the document identifier is specified *with* a revision number, the particular revision of the EML document will be retrieved from the LTER Data Catalog (revision 17 in the above example). If it is specified *without* a revision number (e.g. **docid=knb-lter-pie.135**), the most current revision of the EML will be retrieved from the LTER Data Catalog. Information Managers should decide whether they want the data URL to be associated with a specific revision of the metadata or whether it makes more sense to use the most current revision of the metadata, and thus specify the revision number (or

2 There is an optional third parameter that is used for multiple **urlHeads** if necessary (see Section 4).

not) accordingly.

Finally, the **urlTail** parameter provides the specific information necessary to return the data object. This is the same information found in the “varying” component of the original site data URL described in section 2.2.1 and is exactly the same string value to be appended with the **urlHead** when forming the original data URL.

2.2.4 Translating a Proxy URL to a Site Data URL

The following procedure outlines the steps performed by the DAS service when an end-user selects a DAS proxy URL:

1. End user selects DAS proxy URL.
2. DAS service parses proxy URL to determine the site (and use it to look-up the **urlHead** component in the DAS registry), the EML document identifier, and the **urlTail** component. Using the above proxy URL example (see Section 2.2.3), the results are:

   Site - `PIE`
   urlHead component - `http://ecosystems.mbl.edu/PIE/data/`
   EML document identifier - `knb-lter-pie.135.17`
   urlTail component - `MAR/data/LTE-MP-NAC-biomassmeans.dat`

3. DAS service uses the EML document identifier to retrieve metadata such as contact info (for notification purposes) and entity name (for naming the data file).
4. The DAS service joins the non-varying (**urlHead**) and varying (**urlTail**) components of the data URL to form the original site data URL:

   `http://ecosystems.mbl.edu/PIE/data/MAR/data/LTE-MP-NAC-biomassmeans.dat`

5. The DAS service retrieves the data set identified by the original site data URL, including any detected mime-type, and returns it to the end user's web browser. If a data table entity name exists within the EML document associated with the data set, it too will be returned as part of the HTML header.

2.3 Data Access Notification

The DAS “data access notification” service provides email notifications to two parties when data are accessed through the DAS: 1) to the responsible party caring for the data set and 2) to the end user who accesses the data.

The first notification email (see Section 5 for a sample email) to the responsible party caring for the data set will contain the contact information of the end user who accessed the data set, the time and date of access, the EML document identifier associated with the data set, and the data URL and proxy URL used for the access. The “responsible party” is derived from all “responsible party” elements within the EML document that is associated with the data set. Specific responsible party elements that are required in each EML document include, at minimum, one data set “creator” and one data set “contact”. Optional elements include the data set “metadata provider” and or “publisher”. An email will be generated and sent to each responsible party if and only if the “email” field within the responsible party element is available. Through the DAS URL

management interface, the site information manager will be able to select zero or more responsible party element containers for which to receive the notification email per each “key-value” record (e.g., for key “knb-lter-pie”, “creator” and “contact” to receive notification, but not “metadata provider” or “publisher”).

The second notification email (see section 6 for a sample email) to the end user will contain information about the data set “creator” for the purpose of citation attribution, along with information for the data set “contact” if additional information about the data set is required. This email will also contain a URL to the associated EML document in the LTER Data Catalog and a URL to the LTER Network Data Access Policy.

2.4 Data Access Audits

The DAS “data access audit” service will record each data set access event into a DAS relational database table. The information recorded will include the user identifier of the end user, the time and date of access, the EML document identifier associated with the data set, and the data URL and proxy URL used for the access.

The DAS will provide an audit management interface for searching the audit table and for generating reports based on temporal, spatial (i.e., site), and EML document identifier criteria.

2.5 Reporting

The DAS reporting service will provide calendar-based reports that will be emailed to the site information manager, in addition to interactive and web-service based interfaces that will allow users to query for specific audit logs.

3 General Timeline

The DAS project timeline is separated into 4 major sections, including Design and Planning, Prototype and Development, Testing, and Release. The overall duration is calculated to be approximately 15 weeks (3.7 months). We assume that 4 weeks will be devoted to deployment and testing at between 2-3 early adopter LTER sites. During this period, the NIS development team will work on additional projects. Further, we plan to reuse packaged developed for the EcoTrends project, a close representation of specific packages within the DAS project. Design, development, and testing is estimated to being in early October 2008 and last through January 2009. A break down of general task follows.

3.1 Design and Planning

1. Use Case Scenario: 1 week
2. Project plan: 2 weeks

TOTAL: 3 weeks

3.2 Prototype & Development

1. End user registration and authentication: 2 weeks

2. URL management and interface: 1 week
3. Data access notification: 0.5 weeks
4. Data access auditing: 0.5 weeks
5. Auditing report interface: 1 week

TOTAL: 5 weeks

3.3 Testing

1. End user registration and authentication: 0.5 weeks
2. URL management and interface: 0.75 weeks
3. Data access notification: 0.25 weeks
4. Data access auditing: 0.25 weeks
5. Auditing report interface: 0.25 weeks
6. Site implementation (early adopter) and testing: 4 weeks

TOTAL: 6 weeks

3.4 Release

TOTAL: 1 week

4 Appendix – Registering Multiple urlHead Values

We expect that most sites will need to register only a single **urlHead** value, which will be applicable to all the data accessible at the site. However, the DAS URL scheme is designed to accommodate sites that store their data among multiple hosts and would therefore need to register multiple urlHead values (one per host). For example, site 'ABC' registers three **urlHead** values corresponding to three different hosts where the data resides at their site:

Site	urlHeadID	urlHead
ABC	1	http://host1.abc.edu/data/
ABC	2	http://host2.abc.edu/data/
ABC	3	http://host3.abc.edu/data/

The proxy URL (see Section 2.2.3) for such cases should include an optional request parameter called the **urlHeadID**:

> **urlHeadID** (e.g. `urlHeadID=1`) – The **urlHeadID** parameter is an optional parameter used only in cases where a site has registered more than one **urlHead** value with the DAS. The value of the **urlHeadID** parameter determines which of the **urlHead** values registered by the site should be applied when composing the data URL.

An example of a proxy URL that includes a **urlHeadID** request parameter is:

```
http://metacat.lternet.edu/das/dataAccessServlet?docid=knb-lter-
abc.100&urlHeadID=2&urlTail=dataset_100.dat
```

In this example, the DAS proxy service will look-up the **urlHead** value corresponding to a urlHeadID value of “2”:

```
http://host2.abc.edu/data/
```

After appending the **urlTail** value specified in the proxy URL, the full data URL will be:

```
http://host2.abc.edu/data/dataset_100.dat
```

It is expected that most sites will not need to register more than a single urlHead value, and thus can omit the **urlHeadID** parameter (defaulting to a value of “1”) when composing their proxy URLs .

5 Appendix – DAS Access Notification to Responsible Party

Sample email to the Responsible Party caring for data sets when the data are accessed by an end user.

```
You have received this automated email from the LTER Data Access Server
because an LTER data set that you are associated with was accessed by some
user. If you believe that you received this email in error, please send a
reply email to 'das@LTERnet.edu' that contains the original notification.
Thank you.

Data was accessed by the following user on 2008-11-20 08:28:32:
---------------------------------------------------------------
User ID:      dcosta
Given Name:   Duane
Surname:      Costa
Organization: University of New Mexico
Affiliation:  LTER
Email:        dcosta@LTERnet.edu
Phone:        505-269-9632

The following data object was accessed:
---------------------------------------
Docid:        knb-lter-gce.247.8
Entity Name:  MET-GCES-0508b_1_2.TXT
Proxy URL:    http://tropical.lternet.edu:8888/das/dataAccessServlet?
              docid=knb-lter-gce.247.8&urlTail=accession=MET-GCES-
              0508b&filename=MET-GCES-0508b_1_2.TXT
Data URL:     http://gce-lter.marsci.uga.edu/public/app/send_file.asp?
              lnoproxy=yes&accession=MET-GCES-0508b&filename=MET-GCES-
              0508b_1_2.TXT
Metadata URL: http://metacat.lternet.edu/knb/metacat?action=read&docid=knb-
lter-gce.247.8
```

6 Appendix – DAS Access Notification to End User

Sample email to the End User when accessed a data set.

```
You have received this automated email from the LTER Data Access Server
because you have accessed an LTER data set. If you believe that you received
this email in error, please send a reply email to 'das@LTERnet.edu' that
contains the original notification. Thank you.

The use of data from the LTER Network requires compliance with the LTER
Network Data Policy (http://www.lternet.edu/data/netpolicy.html).

The following data object was accessed on 2008-11-20 08:28:32:
---------------------------------------------------------------
Docid:        knb-lter-gce.247.8
Entity Name:  MET-GCES-0508b_1_2.TXT
Metadata URL: http://metacat.lternet.edu/knb/metacat?action=read&docid=kknb-
lter-gce.247.8

Citation credit should be given to:
-----------------------------------
Given Name:   Duane
Surname:      Costa
Organization: University of New Mexico
Affiliation:  LTER
Email:        dcosta@LTERnet.edu
Phone:        505-269-9632

For additional information about this data object, please contact:
------------------------------------------------------------------
Given Name:   Duane
Surname:      Costa
Organization: University of New Mexico
Affiliation:  LTER
Email:        dcosta@LTERnet.edu
Phone:        505-269-9632

-------------------------------------------------
Long-Term Ecological Research Network Mailing List
das@LTERnet.edu
```

7 Appendix – Ecological Metadata Language Dependencies

The Data Acces Server is dependent on rich content of the Ecological Metadata Language (EML) for providing optimal service when obtaining (1) the email address used to notify the data set owner and (2) the data object name used during the data transfer 'pass-through' from the site to the end user's client browser.

7.1 Email Address

The DAS parses the EML document that is associated with the data object to determine the proper information for creating and sending the notification email to the data set owner and the data set user. This information is contained within the 'responsibleParty' sub-tree of the EML document and can be one of three types of responsible parties: (1) creator, (2) metadataProvider, or (3) contact. In addition to the email address used for the “To” field in the data set owner email, general information about the responsible party is retrieved from the EML document to 'flesh out' the content that is sent to the data set user.

7.2 Entity Name

The DAS parses the EML document that is associated with the data object to set the name of the data object that is delivered to the data set user. This information is obtained first from the “objectName” field of the 'physical group' subtree and second from the “entityName” field of the 'entity group' subtree. If neither information is available, a random object name is generated.