LIGO Identity Management Practices
LIGO-T1200144-v3

March 22, 2012

1 Scope of this document

This document outlines the electronic identity management practices of the LIGO Collaboration. It details what personally identifiable information is collected and managed as part of issuing electronic identities to LIGO collaboration members and associated guests and how that information is stored and made available or not to third parties.

In cases where an electronic identity is not issued by LIGO but instead asserted by an external identity provider (federated identity) this document details how attributes about an individual asserted by the IdP are stored and used by the collaboration.

The scope does not include the identity management practices of the LIGO Laboratory where they differ or are separate from those of the LIGO Scientific Collaboration (LSC) and laboratory members should consult the LIGO Laboratory identity management practices and privacy policy documentation for details.

2 LIGO Laboratory, LSC, and "LIGO"

The Laser Interferometer Gravitational-Wave Observatory (LIGO) consists of two widely separated installations within the United States one in Hanford Washington and the other in Livingston, Louisiana operated in unison as a single observatory. LIGO is operated by the LIGO Laboratory, a consortium of the California Institute of Technology (Caltech) and the Massachusetts Institute of Technology (MIT), and funded by the United States National Science Foundation.

The LIGO Scientific Collaboration (LSC) is a group seeking to make the first direct detection of gravitational waves, use them to explore the fundamental physics of gravity, and develop the emerging field of gravitational wave science as a tool of astronomical discovery. The LSC carries out the science of the LIGO Observatories, located in Hanford, Washington and Livingston, Louisiana as well as that of the GEO600 detector in Hannover, Germany.

Institutions join the LSC after signing a MOU with LIGO Laboratory and the LSC.

Unless otherwise indicated the term "LIGO" represents the union of the LIGO Laboratory and the LSC.

3 LIGO Identity Management Project

The LIGO Computing Committee under the authority of the LIGO Directorate sponsors and manages the LIGO Identity Management (IdM) Project, often referred to within LIGO as the "Auth Project".

The LIGO IdM Project designs and architects identity management infrastructure and services to help LIGO accomplish its scientific mission. The project itself does not deploy or operate infrastructure and services but rather collaborates with staff throughout the collaboration for the deployment and operation of the infrastructure and the services and applications that integrate with the infrastructure. Most members of the IdM Project have some deployment and operational responsibilities.

4 LIGO electronic identity

4.1 Who is issued a LIGO identity

A LIGO electronic identity, sometimes referred to as an @LIGO.ORG or "albert.einstein" identity, account, or login is a digital identity issued to all LIGO collaboration members.

LIGO identities may also be issued to the following groups who are not members of the LSC or the LIGO Laboratory:

- Virgo collaborators
- NSF program managers
- Advisory panel and committee members
- Other authorized guests of LIGO

4.2 Properties of a LIGO identity

Notable properties for a LIGO identity include:

- Uniqueness: each identifier is unique; that is, each identifier is associated with a single person or other entity
- One Identifier: an individual may have no more than one active LIGO identity.
- Non-Reassignment: Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.

4.3 Collected personal information and attributes

During enrollment in LIGO and as part of the process of provisioning a LIGO identity the following information may be collected:

- Given or first name
- Middle name
- Family or last name
- Name suffix
- Name honorific
- Institutional email address
- Institutional address
- Institutional telephone numbers
- Affiliation with LIGO

After enrollment a collaboration member may choose to add and link the following information to their LIGO identity:

- Additional email addresses

As part of the collaboration the following information about each member is collected and managed and linked to a member's LIGO identity:

- Membership in LIGO MOU groups, working groups and committees

4.4 How personal information is stored

The information about and linked to a LIGO identity is stored as follows:

- Personal information including name, institutional address and telephone number, and email addresses are collected and managed using the MyLIGO (`https://my.ligo.org`) service. The service stores the information in a relational database. Authentication and authorization to the MyLIGO service is required to enter or edit the information. No other user tool or service accesses the data in the relational database other than the LIGO roster (see below). Other tools and infrastructure managed directly by the LIGO IdM Project for the purposes of supporting the infrastructure and providing reporting functions do have secure access to the relational database. All access to the relational database requires strong authentication and authorization.

- Personal information including name, institutional address and phone number, email addresses, and LIGO MOU group membership are also stored in the LIGO LDAP server. At this time the LIGO LDAP server and its replicas support anonymous binds. It is expected that anonymous binds will not be supported in the future.
- Membership in LIGO MOU groups, working groups, and committees is managed using the LIGO Grouper service. Access to the Grouper service requires authentication and authorization. Membership information is also reflected into the LIGO LDAP server and its replicas.
- The LIGO Document Control Center (DCC) inherits some group membership information from MyLIGO and stores its own copy of that information in both a relational database and group membership files needed to support operation of the DCC.

4.5 How personal information is published

Personal information linked to a LIGO identity is published in the following ways:

- the LIGO Roster (`https://roster.ligo.org`) or directory is a publicly available service that publishes the name, institutional affiliation, institutional address, institutional phone number, and email address for collaboration members. Also available is an individual's status as a principal investigator (PI) and a member of the LSC Council.
- the LIGO LDAP server, as noted above, makes certain information publicly available via anonymous binds. Anonymous binds may not be supported in the future.

4.6 Demographics

The LSC and LIGO Laboratory request that their members contribute personal demographic information. Providing this information is optional and members have the ability at any time in the future to change or remove provided information.

The information is requested primarily from individuals affiliated with US institutions that receive support from the National Science Foundation for reasons specified in NSF Form 1225:

> Demographic data allows NSF to gauge whether our programs and other opportunities in science and technology are fairly reaching and benefiting everyone regardless of demographic category; to ensure that those in under-represented groups have the same knowledge of and access to programs and other research and educational opportunities; and to assess involvement of international investigators in work supported by NSF.

Information provided is used to produce reports in aggregated form without reference to personal identities as follows:

- Large multiple-group statistical summaries (e.g., all NSF-funded LSC personnel, or all LIGO Laboratory personnel). Such reports may be made available to the NSF or other oversight bodies by the LIGO Directorate. In addition, reports on LSC demographics will be accessible to all LSC members.
- An individual institution's demographics will be accessible only by that group's principal investigator (PI); the PI may use this information in accord with his/her NSF grant stipulations.

Access to individual records is restricted only to (i) the individual entering the information and (ii) technical support staff who will access it only on an as-needed basis in order to provide user help support.

4.7 Suspension and revocation

Collaboration computing staff, acting under the authorization of the LIGO Directorate, the LSC Security Committee, the LIGO Laboratory Security Officer, or the Computing Committee may suspend or revoke access to and the use of a LIGO electronic identity without prior notice.

4.8 Sharing with third parties

4.8.1 Assertion to federated service providers

LIGO services may, in order to enable efficient use of by collaboration members of services and tools not operated or managed by LIGO, assert attributes about a collaboration member to the third party service.

Examples of such third party services or tools include:

- CILogon service
- Globus Online services
- Google Apps for education

The following personally identifiable attributes about a collaboration member may be asserted:

- Given or first name
- Surname or family or last name
- Email address

Note that only given name and surname are asserted to Google Apps for education.

4.8.2 Commercial organizations

No personally identifiable information about collaboration members is released to any commercial organization with the exception of Google Apps for education.

5 Federated identity management

Some LIGO services interoperate with IdPs managed by other organizations or institutions and are able to consume identity and attribute assertions by the external IdPs.

6 Expected attribute assertions by external IdPs

LIGO services consuming federated identities as asserted by external IdPs generally expect an IdP to assert the following attributes:

- mail
- givenName
- surName
- displayName
- eduPersonPrincipalName
- eduPersonTargetedID
- eduPersonScopedAffiliation

7 Uses of attribute assertions by external IdPs

The LIGO service providers that consume federated identity and attribute assertions use the asserted attribute values to enhance scientific and technical collaboration in support of the LIGO scientific mission. Attribute values may be stored, recorded, and logged in support of that goal. Examples include:

- Wikis used for collaboration may record the name, email, eduPersonPrincipalName, or eduPersonTargetedID to indicate which individuals edited or authored wiki content. The servers may record the same attribute values to log access to the service.
- The LIGO Grouper deployment may consume federated identity and record all asserted attributes in order to manage the membership of the user in LIGO groups.
- Collaboration management tools such as COmanage may consume federated identity and all asserted attributes and record them in order to enhance collaboration management activities for LIGO.

8 LIGO service providers consuming federated identity

At this time the following LIGO services consume federated identity and use or store the asserted attributes as indicated:

- Compact Binary Coalescence (CBC) wiki
  - eduPersonPrincipalName: used as the identifier for the Moin wiki program and stored as a record of who edited or authored wiki content. The web server hosting the wiki logs the eduPersonPrincipalName and IP address for each access to the wiki.

9 Logging

LIGO service providers consuming federated identity log and record at least one attribute asserted by the external IdP along with the IP address of the client accessing the service. Log files are only available to authorized LIGO system administrator and security personnel.