



ARCHIVER Project

Technical Summary

PIC DATA DISTRIBUTION

Problem Definition:

We want to substitute the current in-house tape library storage, Hierarchical Storage Manager, disk storage and data distribution. Each instance of the service to be purchased is the 5-year safe-keeping and data distribution of a yearly dataset and its derived datasets from at most two sources according to the specifications below.

Lifecycle - Workflow Characteristics:

The Lifecycle - Workflow of “**PIC MIXED FILE REMOTE STORAGE**” and in addition:

- Additional metadata is maintained in the remote service using an extensible schema
- Some metadata instances are produced and linked as file attributes by the workflows at PIC or ORM that upload data.
- Other metadata instances are produced and linked as file attributes *a posteriori* using direct or scripted CLI commands or through API calls or via Web interfaces.
- Authenticated, authorized users anywhere in the world interact with the archive
 - Users issue metadata queries in order to generate “views” of the archive (define subsets of the files). The user should be able to save these “views” for later reuse.
 - Users access the subset of data defined in a given “view” by any of the following methods:
 - Download the selected files to their own computer using a Command Line Interface, a bash or python script, or a Web interface.
 - Perform remote file access from their computers directly to the archive, either directly, through a cache or using sync-and-share capabilities.
 - Good reliability and performance need only be guaranteed if the user’s computer is connected to a National Research and Education Network and through it to Géant.
- Typical access patterns are:
 - Recall asks for files of the same Filetype
 - Recall asks for files from the same Observation number or Observation date
 - Recall frequency is inversely proportional to the file size

- A given user will repeatedly access the same files during a period of weeks or months
- The prior notice for access to the “raw” data (the highest data volume component) could be maintained, but this would require additional software to enable user requests for unlocking access.

Authentication and Management Functions:

Authentication and Management of [PIC MIXED FILE REMOTE STORAGE] should be provided and will be used to maintain the metadata. In addition:

- Data consumers should be authenticated against PIC’s existing LDAP identity provider (IdP) and another existing AD Azure-hosted IdP.
- These IdPs also provide Authorization attributes which will be used to control access to different instances of the service. For example, a given user or a given group of users may only be allowed to read data from a given range of Observation dates or of given file types.

Data and Metadata Characteristics:

The Data and Metadata from [PIC MIXED FILE REMOTE STORAGE] and in addition:

- “Origin and type metadata” is a small number of 256-character strings which can be used to define groups of files. Metadata instances are produced and linked as file attributes by the workflows at PIC or ORM that upload data. Examples:
 - Metadata=Observation number: Groups all “raw” and “derived” files with the given observation number.
 - Metadata=Observation Date: Groups all “raw” and “derived” files where the raw data was produced on a given date.
 - Metadata=Filetype: Groups files of a given type
 - Combining Observation Date with Filetype: Groups all files of a given type derived from raw data produced on a given date
- “Scientific annotation metadata” is additional, evolving metadata defined according to the scientific needs arising. Attributes are expressed as 256-character strings or 64-bit integer or floating point numbers. Files are linked to instances of the metadata by scripts which select groups of files via queries on already linked metadata.

Interface Characteristics:

The Data and Metadata from [PIC MIXED FILE REMOTE STORAGE] and in addition:

- Interfaces that allow authenticated and authorized users to:
 - select groups of files and
 - use these files on their own premises by:
 - downloading them using a Web interface, a Command Line Interface (CLI), or a REST API.
 - accessing them using industry-standard protocols with access control (such as https or smb), ad-hoc TCP/IP based protocols (such as xrootd) or selective Sync-and-Share capabilities.

- Interfaces that allow a user to request unlocking of files with restricted access (for example raw data which requires a priori notice). This should give the ability to track the users who requested these unlocks.

Reliability Requirements:

Reliability Requirements from [PIC MIXED FILE REMOTE STORAGE] and in addition:

- Better than 99.7% availability for user access.
- Better than 99.9% success rate for downloads of randomly chosen files.

Compliance and Verification:

- Scrubbing: Supplier must provide evidence that every stored file has been read and its checksum freshly calculated at least once per year, without any intervention by the buyer. An alarm should be raised if the freshly calculated checksum does not match the original.
- Random 1% buyer’s monthly check of “raw” data: Each month, the buyer will give a one week notification simulating a recall of the “raw” data component of a yearly dataset. The buyer will then ask to recall a randomly chosen 1% subset of the “raw” data component of the dataset, which must be accomplished within 24 hours.
- Random buyer’s check of “derived” data: The buyer will randomly download, using the end-user interface, “derived” data files and verify their checksum, at a rate of 1% of the files per month.

Cost Requirements:

The total cost of an instance of the service must be less than 60k € total for the nominal data volume of 300 TB stored for 5 years (only one version of derived data stored) plus 10k € flat fee per additional version of derived data (up to 50 TB) stored, with 100 active users. A desired cost structure would consist of a fixed fee plus a variable fee proportional to the volume of data actually stored.

Initial Data Management Plan:

DMP Topic	What needs to be addressed
Data description and collection or re-use of existing data	Raw, calibration and derived datasets will be handled in the ARCHIVER project. These data will be from scientific projects in which IFAE participates and which have explicitly given their consent. Initially, data will be from the MAGIC Telescopes https://magic.mpp.mpg.de/ . Data will be re-used in the context of multi-instrument gamma-ray astrophysics.

Documentation and data quality	Data documentation will be done by adapting the internal Data Management and Preservation Plans (DMPP) of the scientific projects who own the data. MAGIC has already given permission to use their DMPP plan. Data quality is measured continuously by the scientific instruments and data quality tags will be available as metadata.
Storage and backup during the research process	Today, PIC is using its dCache/Enstore based service to archive 'cold data' in a HSM like (disk + automated tape) service. That layer is going to be replaced/extended with ARCHIVER services using an additional copy of the data. (cleanup at the end of the project requires no further data movement).
Legal and ethical requirements, codes of conduct	Citation should be given when data is used by permission.
Data sharing and long-term preservation	Easy to use data sharing, both amongst access-controlled groups as well as Open Data, is a major objective of placing the data in the ARCHIVER-developed platforms. Long-term preservation will be tested by simulating in an accelerated manner the Data Management and Preservation cycle.
Data management responsibilities and resources	High-level data management will remain the responsibility of IFAE, while low-level data management and resources will be provided by the vendors.