CERN Computing Resources Lifecycle Management

Alexey Tselishchev, Paolo Tedesco, Emmanuel Ormancey, Christian Isnard

CERN IT/OIS
CERN, Route de Meyrin, CH-1211 Geneva 23, Switzerland
Email: Alexey.Tselishchev@cern.ch

Abstract. Computing environments in High Energy Physics are typically complex and heterogeneous, with a wide variety of hardware resources, operating systems and applications. The research activity in all its aspects is carried out by international collaborations constituted by a growing number of participants with a high manpower turnover. These factors can increase the administrative workload required to manage the computing infrastructure and to track resource usage and inheritance. It is therefore necessary to rationalize and formalize the computing resources management, while respecting the requirement of flexibility of scientific applications and services. This paper shows how during the last years the CERN computing infrastructure has been moving in this direction, establishing well-defined policies and lifecycles for resource management. Applications are being migrated towards proposed common identity, authentication and authorization models, reducing their complexity while increasing security and usability. Regular tasks like the creation of primary user accounts are being automated, and self-service facilities are being introduced for common operations, like creation of additional accounts, group subscriptions and password reset. This approach is leading to more efficient and manageable systems.

1. Introduction

Until now many computing service managers at CERN had to manage their users and their computing resources on their own. They had to create accounts when users arrived, grant permissions, remove rights from users and clean up their resources when they left by hand. For many reasons it was highly desirable to perform these actions consistently and automatically across the various systems and services at CERN, and so it was proposed to provide service managers and end-users with tools addressing general and common needs for account and resources management.

The strategy of the Computing resources lifecycle management project was to design a generic, maintainable solution for the whole community of system and service managers. The objectives were to simplify and standardise account management at CERN, better differentiate Identity, Authentication and Authorization, and manage the lifecycle of identities, accounts and associated computing resources.

As benefits for service managers and owners, access rights to resources can be automatically added and removed as a person progresses through his/her career, roles and eventual departure. This is increasingly important as management of the rights of individuals to access computing resources is essential to maintain security and prevents keeping unintentionally left open doors.
In addition the system empowers the end users by providing self-service functionalities in a dedicated Web portal and, by automating many of the procedures, reducing helpdesk tickets and dedicated system management actions drastically. The system ensures that account data is consistent and will dispose of obsolete computing resources making easier to manage it maintaining reliability and performance.

2. Identity, Authentication, Authorization Model

The general idea of the CERN Account Management is focused around Identity, Authentication and Authorization (IAA), defined as follows:

| Provided by | Answer the questions: | Attributes |
|-------------|-----------------------|------------|
| **Identity** | User | “Who are you?” | Public assertion |
| **Authentication** | User | “OK, how can you prove it?” | Secret response |
| **Authorization** | System | “What can I do?” | Token or ticket Access control |

Identity: A user (typically you) wants to access a system. Because the system doesn’t know you yet, you need to make a declaration of who you are. Your answer to the question “Who are you?” is the first thing you present to a system when you want to use it. Some common examples of identity are user IDs, digital certificates.

At CERN, Identities are managed by the personal information defined in Human Resources (HR) databases. On the base of this data, the Account Management system creates the accounts (username information) that represent these Identities in the CERN computing environment.

Authentication: Is the answer to the question “OK, how can you prove it?” When you present your identity to a system, the system wants you to prove that it is indeed you and not someone else. The system will challenge you, and you must respond in some way. Common authenticators include passwords, private keys, and PINs. Whereas identity is public, authentication is private: it is a secret known (presumably) only by you.

CERN authenticators include for example passwords and private keys with Digital Certificates through a variety of authentication systems like Kerberos, Single Sign-On or SSH. This is handled by Microsoft Active Directory through a set of standards (Kerberos, LDAP, SSO, etc.).

Authorization: Once you have successfully authenticated yourself to a system, the system controls which resources you are allowed to access. Typically this is done through the use of a token or ticket mechanism checked against an access control list maintained by the system administrators.

A wide range of CERN applications use E-Groups ([1]) to maintain the access control lists (each application should have a dedicated E-Group containing the list of authorized users): the token or ticket mechanism contains the list of the E-Groups the user is member of. The application simply compares the E-Group membership list with the access control list and the user is given access if a match is found.
3. Unified Authentication and Authorization model
The Identity, Authentication, Authorization model integration in CERN’s heterogeneous environment (see figure 1) has been implemented over several years (see [2]), implementing new applications and migrating existing applications.

Today CERN is able to use a single electronic identity representation for a person, with a single account and password (see [3]) clearly assigned to a valid human identity in the Human Resources database. The Account Management framework provides account lifecycle and automatic provisioning to applications and resources.

Authentication: The central Authentication is handled by Microsoft Active Directory which provides a set of standards for authentication systems (Kerberos, LDAP, SSO, etc.) and for account information publishing (LDAP, SSO, etc.), backed up by a set of custom systems (Oracle tables, SOAP methods) so that applications in multiple environments can interact with the central system.

Authorization: The unified Authorization source is based on the E-Group system that CERN has been running for several years. Its simplicity and popularity made it the perfect candidate. Each application
can rely on one or several E-Groups to grant access to a user based on the user’s E-Group membership. The E-Group data is published through the same tools as Authentication, using the Microsoft Active Directory based publishing mechanisms (Kerberos, LDAP, SSO, SOAP, Oracle, etc.).

4. Automate user account lifecycle

The primary goal of the new account management framework was automation. A newcomer should be able to use CERN resources as soon as he arrives, without having to wait for synchronizations, signatures or manual actions.

A complete policy on automation was defined and implemented, allowing the user accounts to be created on the fly based on Human Resources database information, including electronic mailbox provisioning. Now every CERN user gets his or her accounts created automatically on the first day at CERN and removed at the end of the affiliation. All specific accounts are automatically blocked or reassigned and this allows to avoid accumulating orphaned accounts. Users are also granted access to specific applications (storing their financial data and others) after their leave using automatically created external account connected to their private email address.

Automation has taken away the need of human intervention making the process more reliable as along with the automatic creation system allows to perform many checks and avoid invalid data (such as mistyped email addresses, birth dates etc) to be propagated further. Single authoritative data source for all user data and synchronization engine ensure that changes made are correctly reflected in all connected data sources and applications that are using new system.

![Account Management self-service interface.](image)

Figure 2: Account Management self-service interface.
5. Self-Service tools for the end-users

Empowering the end-users was an important part of the implementation, to ensure they are able to manage themselves at any time their resources. An Account Management Web Portal was implemented (see figure 2 and [4]), allowing the users to manage their account(s) but also to manage their applications and resources (see figure 3), from authorization request to specific settings. Previously many of these actions such as creating additional accounts or subscribing to specific services required manual work involving the helpdesk, service managers and computing group administrators.

6. Facilitate tasks for targeted CERN staff

Within the self-service portal for end-users, a specific web interface (see figure 4) was implemented for people with administrative rights. The Helpdesk team who solves problems or the supervisors who can help their supervisees use this interface to act on users account, applications and resources.

![Figure 3: Applications and Resources self-service interface.](image)

![Figure 4: Targeted staff administrative interface.](image)
7. **Perspective and conclusions**

In the nearest future it is planned to start managing other types of objects (computers, printers, smart devices, etc.) in the system, to introduce other automated features and to provide users with more self-service functionalities giving higher level of independence and flexibility.

Following well-defined models that were designed to fit CERN needs and policies that facilitate everyday workflows allows to increase overall security and at the same time to reduce workload and make everyday life easier for CERN staff and users.

**References**

[1] Grzywaczewski P 2009 E-groups takes over from SIMBA *CERN Computer Newsletter* Volume 44, Issue 1 – IOP Publishing 2009 [http://images.iop.org/objects/cern/cnl/6/1/1/jan-marpdf.pdf](http://images.iop.org/objects/cern/cnl/6/1/1/jan-marpdf.pdf)

[2] Pace A 2007 CERN:Identity Mangement *CHEP 2007 Plenary Session* [http://indico.cern.ch/contributionDisplay.py?contribId=54&confId=3580](http://indico.cern.ch/contributionDisplay.py?contribId=54&confId=3580)

[3] Ormancey E 2008 CERN single sign on solution *Journal of Physics: Conference Series*, Volume 119, Issue 8, pp. 082008 (2008)

[4] [http://www.cern.ch/account](http://www.cern.ch/account)