The new (and improved!) CERN Single-Sign-On

Adeel Ahmad[1], *Asier* Aguado Corman[1], *Maria* Fava[1], *Maria V.* Georgiou[1], *Julien* Rische[1], *Ioan Cristian* Schuszter[1], *Hannah* Short[1,*], and *Paolo* Tedesco[1,**]

[1]European Organization for Nuclear Research (CERN)

Abstract. The new CERN Single-Sign-On (SSO), built around an open source stack, has been in production for over a year and many CERN users are already familiar with its approach to authentication, either as a developer or as an end user. What is visible upon logging in, however, is only the tip of the iceberg. Behind the scenes there has been a significant amount of work taking place to migrate accounts management and to decouple Kerberos [1] authentication from legacy Microsoft components. Along the way the team has been engaging with the community through multiple fora, to make sure that a solution is provided that not only replaces functionality but also improves the user experience for all CERN members. This paper will summarise key evolutions and clarify what is to come in the future.

1 Introduction

The Malt Authentication and Authorization Project (Malt Auth) was established to migrate CERN's Identity and Access Management system to a vendor-independent, open source, microservice architecture [2]. It is part of the wider Malt Project [3] and is one of the most complex areas in which CERN is seeking to re-assess the IT Provisioning Strategy for core services. A new version of CERN's SSO was released in 2019 and, as of February 2021, has over 3000 registered applications. This constitutes a significant proportion of the roughly 15000, applications that were configured on the old SSO but indicates that there is much work remaining to complete the migration. For the time being, CERN's authorization ecosystem is split between the old world (Microsoft based) and the new. The goal for the coming years is to complete the transition and to improve the service offering along the way.

2 Recent Progress

2.1 Single Sign On

The Single Sign On service has been consolidated to cope with the increasing amount of applications registered on it, and to provide a more mature set of features to users. One of the major improvements is the possibility for users to choose between One Time Passwords (OTP) and WebAuthN [4] hardware tokens (Yubikey) as second factor authentication (2FA) possibilities. The possibility to register guest accounts, simply based on a username and password, has been offered as well, to support users who do not want to use work or personal social accounts to access CERN services (for example for access to the CERN Marketplace).

*e-mail: hannah.short@cern.ch
**e-mail: paolo.tedesco@cern.ch

2.2 LDAP and Kerberos Migration

The LDAP server is at the heart of the authentication system. It stores usernames and passwords as well as acting as a registry for services. In the current system this component is Microsoft Active Directory [5] and will be migrated to FreeIPA [6]. Also included in FreeIPA is MIT's KDC (Key Distribution Center) managing Kerberos authentication [1], which is heavily used by both users and services for authentication at CERN. FreeIPA also provides a Certificate Authority, dogtag [7], which will be used to provision host certificates, removing a dependency on the existing Microsoft Certificate Authority.

Similarly to the rest of the system, there will be a significant period where both the old and new directory service systems will be available in parallel. The system is too complex and distributed to manage a "big bang" migration and the decision was taken to migrate clients and services slowly from Active Directory to FreeIPA. Consequently many of the infrastructure configuration tools must become made aware of the two distinct realms and be able to map users and services to one or the other. Figure 1 describes the LDAP (AD or IPA) configuration, DNS domains and kerberos realms before, during and after the transition. CERN's production environment is currently in the pre transition phase.

Work is currently ongoing to deploy a production-like environment based on FreeIPA, including both the FreeIPA server configuration and enhancement of the many clients that use Directory Services. Many of the configuration management tools (such as puppet and host certificate provisioning) are currently being adapted to allow them to support FreeIPA. A particular challenge is to migrate Kerberos authentication, it must be possible for a user to acquire a valid token for either the old Kerberos realm or the new and present the correct one to a target service.

A prototype service will be set up during the first half of 2021 to demonstrate Batch Grid job submission where the host and workers are authenticated using FreeIPA. Following that it is anticipated that the new Single-Sign-On will be one of the first adopters of FreeIPA.

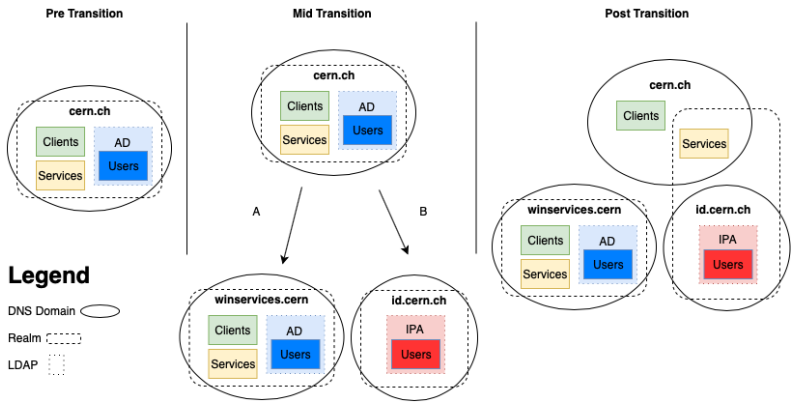

Figure 1. Schematic of proposed DNS Domains, Kerberos Realms and LDAP Instances. We are currently still in the pre transition phase. During the mid transition phase: A) a subset of users, services and clients that require Microsoft Active Directory will be synchronised to a new Active Directory, B) all Users will be synchronised to FreeIPA. Post transition legacy clients and services will be able to remain in the .cern.ch domain, and services will be added to the FreeIPA Realm. Trust Relationships will ensure that authentication continues to succeed smoothly.

2.3 Account Management Migration

Several of the user facing components of the authentication and authorization infrastructure have been deployed without the need to change the underlying primary source of account information, i.e. Active Directory. Migrating Account Management is an important step towards removing our dependency on this component. In the future, the master of account information will be the Authorization Service, a component developed in-house which choreographs the account life-cycle from creation in LDAP to eventual deletion. This change will take place during the first half of 2021 and requires porting much functionality from the legacy systems such as account creation requests and password management.

This is also an opportunity to improve password management in line with new best practices. In particular, users will be able to choose either a short-and-complex password or a longer passphrase. Hashed passwords will also be checked against a list of passwords that have been made public through data breaches at external sites and are used by hackers during brute force attacks. Users that have chosen these "compromised" passwords will be prompted to change their password to improve the security of their account. A 2FA service is provided to allow users with CERN accounts to configure an additional token - some applications base access constraints on whether or not a user has authenticated with 2FA.

2.4 Community Engagement

CERN's Single Sign On has been offered as a service for over 10 years, with users able to register sites easily and independently. To date there are over 15000 services registered that must be migrated to the new SSO. Contacting CERN users is notoriously difficult, e.g. many inboxes go unread, and so a change management process with a strong communication plan is critical. In addition, many of those who originally created the SSO registration have long left CERN, and the registrations have been passed to individuals who have no experience with SSO integration and may be unaware that the site has become their responsibility.

LDAP migration is an even greater challenge. Anonymous LDAP is offered at CERN, meaning that understanding which services are performing LDAP queries is not possible. Furthermore, it is difficult to understand which data is being used, as users often make queries for a larger set of data than they actually require (e.g. all attributes and groups associated with a user, when they only need to know a subset).

The Malt Active Directory Task Force was set up in late 2020 to engage directly with representatives from many of the technical sectors of CERN. Representatives from Departments and Groups were invited to join and describe the different use cases within their domain. Smaller focus meetings were held between the Malt Auth team and each Department or Group to fully understand potential hurdles and identify requirements. To date, discussions have focused on requirements for Kerberos authentication and key functionality for authorization groups and mailing lists.

The Malt Auth project has been presented in multiple fora, for the CERN community and beyond, including CHEP 2019 [2] and HEPiX.

3 Information for Service Managers

The following sections include useful information for those running services that interact with CERN's Identity Management infrastructure.

3.1 Authorization

Authorization information will be available in multiple ways, as depicted in Figure 2. An important change compared to the previous system is that only CERN accounts will be stored in CERN's LDAP (FreeIPA). Any service that requires authorization information for Guest Accounts, or for users from external Identity Providers (e.g. eduGAIN or Google) must either consume authorization information from SSO Tokens by configuring application specific roles that are linked to groups (see Service A in Figure 2) or make authenticated queries to the Authorization Service API (see Service B in Figure 2). Services that are only interested in authorization information for CERN accounts have the additional option of querying LDAP directly (see Service C in Figure 2). In rare cases, services of type A may request to receive a user's full list of groups; this requires manual validation due to the potential impact on a user's privacy.

The legacy authorization system, e-groups, was used for both authorization and for mailing lists. These use cases will be decoupled in the new system. Existing e-groups will be imported as both authorization groups and mailing lists.

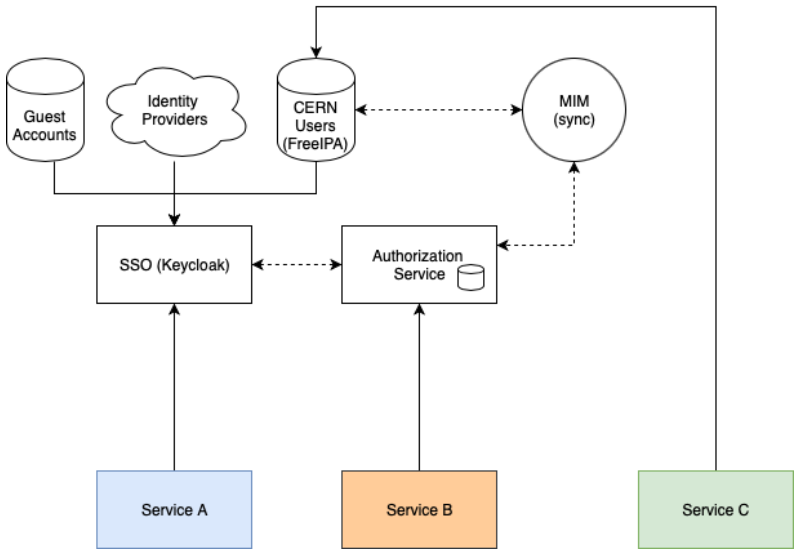

Figure 2. Services can access authorization information in 3 ways. Service A is connected to CERN SSO and receives roles and/or groups in authentication tokens. Service B queries groups in the Authorization Service API. Service C queries group information in LDAP (FreeIPA). Authorization information from the Authorization Service is synchronised to FreeIPA using a separate component called Microsoft Identity Manager (MIM)[8]. The Single-Sign-On (SSO) is implemented using the open source identity and access management tool, Keycloak [9].

3.2 Requests to the CERN Community

Although many changes will be transparent to users, there are several areas where application or resource owners must be involved in the migration process. Table 1 summarises actions required from resource owners. The migration of applications on central managed services (e.g. centrally managed web services) are anticipated to be migrated transparently for users.

I have a...	I should...	Timeline
Website on the old SSO	Migrate to the new SSO (no action required for centrally managed sites)	H1 2021
Application that uses LDAP for authentication (Active Directory)	Test the new LDAP Servers (FreeIPA)	H2 2021
Application that runs LDAP Queries for Users and Groups	Migrate to the new REST API or (if only require CERN Users) migrate queries to FreeIPA format	H2 2021
Windows PC	Analyse whether this should be centrally managed and kept in Active Directory (at a cost)	H1 2022

Table 1. Actions required from CERN Resource Owners

4 Conclusions & Next Steps

2021 will be an important year in the migration away from the legacy authentication and authorization infrastructure. Once account management has been migrated it will become feasible to duplicate users to FreeIPA and allow CERN's services and clients to begin their migration. In addition to this, Resources Management (i.e. the life-cycle management of assets such as websites) is estimated to begin in earnest this year. It is crucial that the Malt Auth team continue to engage with the CERN community and experiments, both by presenting plans and listening to concerns. Useful resources are included in Appendix A.

References

[1] B.C. Neuman, T. Ts'o, IEEE Communications magazine **32**, 33 (1994)

[2] Aguado Corman, Asier, Fernández Rodríguez, Daniel, Georgiou, Maria V., Rische, Julien, Schuszter, Ioan Cristian, Short, Hannah, Tedesco, Paolo, EPJ Web Conf. **245**, 03012 (2020)

[3] *The MALT Project*, `https://malt.web.cern.ch/malt/index.html`

[4] *Web Authentication: An API for accessing Public Key Credentials* (2019), `https://www.w3.org/TR/2019/REC-webauthn-1-20190304`

[5] *Active Directory Domain Services*, `https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services`

[6] *FreeIPA Open Source Identity Management Solution*, `https://www.freeipa.org`

[7] *Dogtag Public Key Infarstructure*, `https://www.dogtagpki.org`

[8] *Microsoft Identity Manager*, `https://docs.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016`

[9] *Keycloak, Open Source Identity and Access Management For Modern Applications and Services*, `https://www.keycloak.org/`

A Resources

- User Documentation for the CERN authorization Service: https://auth.docs.cern.ch
- User Documentation for FreeIPA: https://ds-docs.web.cern.ch
- Mattermost Support Channel: https://mattermost.web.cern.ch/it-dep/channels/Malt-authentication