ADaMS 3: AN ENHANCED ACCESS CONTROL SYSTEM FOR CERN

P. Martel, C. Delamare, G. Godineau, R. Nunes
CERN, Geneva, Switzerland

Abstract

ADaMS is CERN's Access Distribution and Management System. It evaluates access authorisations to more than 400 zones and for more than 35000 persons. Although accesses are granted based on a combination of training courses, administrative authorisations and the radio-protection situation of an individual, the policies and technicalities are constantly evolving along with the laboratory's activities; the current version of ADaMS is based on a 7 year old design, and is starting to show its limits. A version 3 of ADaMS will allow improved synchronization with CERN's scheduling and planning tools (used heavily during technical shutdowns, for instance), will allow CERN's training catalogue to change without impacting access management and will simplify and reduce the administrative workload of granting access. The new version will provide enhanced self-services to end users by focusing on access points (the physical barriers) instead of safety zones. ADaMS 3 will be able to cope better with changing and new requirements, as well as the multiplication of access points. The project requires the cooperation of a dozen services at CERN, and should take 18 months to develop.

INTRODUCTION

ADaMS is a system that centralises and standardises access policies throughout CERN; it is a central management system generating access authorisations for a multitude of different physical access systems. ADaMS has existed since 2007, and was designed for the 30 access zones existing at the time and that were exclusively related to safety, each with a relatively small area and with their access points geographically close to each other.

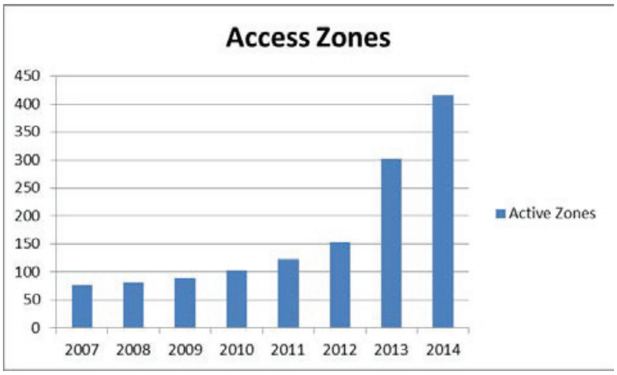

Figure 1: Evolution of the number of zones managed by ADaMS.

Today, the system is managing more than 400 zones (Fig. 1), not all related to safety, and with some of them concerning non-contiguous areas with access points very far from each other. At the same time, the business logic has changed dramatically both in quantity and quality; where originally only 5 criteria existed to grant or deny access (CERN access card, contractual situation of the person, dosimeter, followed courses and access request), new and more complex criteria have been added following new business requirements; IMPACT – a tool to coordinate the interventions on the accelerator premises during technical stops – now determines if access is granted or not, on top of the original criteria, for dozens of zones, and for around 200000 access authorizations (Fig. 2).

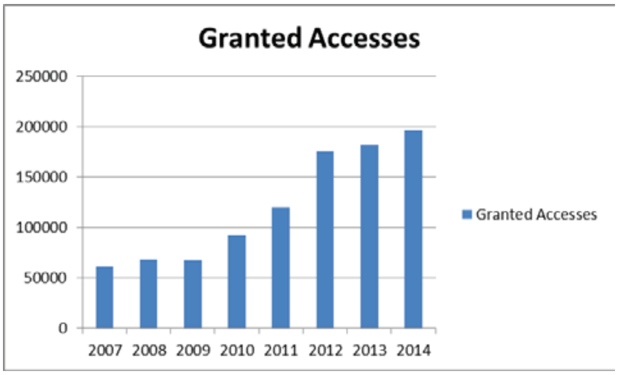

Figure 2: Evolution of the number of granted accesses by ADaMS per cycle.

With time, the changes and improvements to meet new requirements have been implemented on top of the original architecture; this means that even if for the past 8 years all new requirements were met with more or less complex adaptations of the original system, in some circumstances the system is no longer able to automatically justify the granting or revoking of an access right, as by design it does not collect and hold enough data for it. For these reasons, we have decided to build a new version from scratch.

MAJOR CHANGES FROM VERSION 2

Zones and Resources

One of the requirements that ADaMS 3 will have to fulfil is to be able to control access to entities other than "zones". Access to resources such as key cabinets, rooms

ISBN 978-3-95450-148-9

and cars are to be managed by ADaMS, using similar business logic to that of zones – namely criteria required to have access, notifications on access revoking, etc.

Access Points vs. Access Zones

Where in the past (with a small number of safety zones) it was easy to remember or deduce the equivalence between "safety zone" and "access point", currently (with more than 400 zones) this equivalence is difficult to remember or deduce. ADaMS 3 will focus on "access points", which is a concept closer to the end user, with a known identifier, and keep the "safety zones" concept as hidden from the end user as possible.

Access Profiles

ADaMS 3 will allow the definition of access profiles, a mechanism allowing to request a pre-defined set of access rights for a person, with a single operation. For those cases where each person arriving in a new service (e.g. CERN's Fire Brigade) is granted access to the same set of zones, the concept of an access profile will greatly simplify the acquisition of all required administrative authorisations as well as training requirements.

Identifiers Associated to Access Points

ADaMS 3 will make a clear distinction between the right to pass by an access point and the ability to do so with the needed identifier. This means that ADaMS will be able to inform the user that even if the authorisation to enter a certain area or take hold of a certain resource is granted, in practical terms, access cannot be done as the person concerned lacks the required device and/or biometric identifier.

Delegation /Simplification of Administrative Authorisations

ADaMS 3 will allow the administrative authorisation criteria for a zone or resource to be fulfilled without the circulation of an electronic document. The usage of an "egroups/roles" tool will allow to administratively allow the access to a resource without any administrative overhead. For instance, automatically authorising the shared access to a key or a room to those persons in a certain administrative unit at CERN, etc. This delegation (on the management of an egroup or role) of the administrative authorisations, even though not applicable to safety zones (where an explicit, personal signature will allow each person to gain access to it) is expected to greatly reduce the circulation of electronic documents concerning access authorisations at CERN.

Training "Ranks" (or levels)

In the beginning, ADaMS only took 3 safety courses into account; when those courses were replaced by other ones, some tweaking was done in the business logic in order to handle it (e.g. the waiving of a course A if course B had been followed, etc.). With the dozens of courses currently taken into account, and the constant changes to CERN's training catalogue, this way of working (hard-coding the business logic) can no longer be used, if an explanation on an access refusal is to be automatically deduced and a trace of changes in ranks/courses requirements is to exist. ADaMS 3 will interface with CERN's new LMS (Learning Management System), and delegate to it the management of "ranks" (or "levels") and courses. The system works with "ranks", independently of the course or certificate that grants it.

Better Anticipation of Changes

ADaMS will allow the definition of start and end dates for the criteria required (e.g. a new required rank) for a certain zone or resource, and will allow the evaluation of the impact of that change beforehand, namely in accesses granted or lost. It will also allow notification to those persons affected by the change before the change occurs.

More Systems Managed and Interfaced

ADaMS 3 will have more systems managed/interfaced and will work with more data about each of those systems; ADaMS was created to handle 1 access system for CERN's infrastructure and one accelerator access system. It was later enlarged and it now interfaces with multiple accelerator access systems (LHC/SPS/PS), 2 generic non-accelerator access systems, as well as SALTO for door locks, TRAKA for key cabinets, Altaïr for car barriers, and RFID reading systems for "kiosk IT". The interface between ADaMS and these systems is for the time being unidirectional, as all of them fetch data from ADaMS, but supply none, as ADaMS 2 does not work with any data from any physical system. ADaMS 3 will fetch data about the access systems, and will hold data about which systems are used, where, when and with which identifier. By scaling up the new architecture, it will be able to accommodate any new access control systems that may be added (e.g. Indico for room reservation and the SPS Access renovation project).

NEW INTERFACES

ADaMS 3 new graphical user interface will answer to the growing usage of the system by end users (Fig. 3); it will be leaner and more intuitive for the users, proposing more ways to find out if access to a certain location is granted or not; access checks will be proposed by access point name, location code or geographical location (in a map). It will be focused on access points, and not on access zones, and will be able to explain with a simple text, why access has been granted or revoked. It will also allow to easily identify the missing criteria in order to obtain access to a zone or resource.

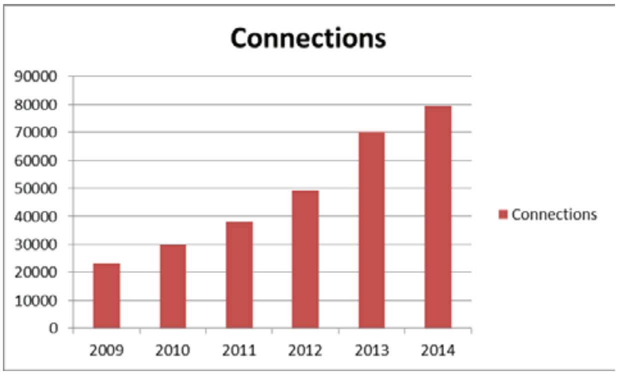

Figure 3: Evolution of the number logins to ADaMS GUI.

ISBN 978-3-95450-148-9

The new system will have functionality providing an overview of all access conditions and situations for the persons in an egroup or organisational unit; this will allow managing the accesses of a series of related persons, in an easy way.

ADaMS 3 will make data available to other systems via the conventional mechanism of database table or view; it will also expose data via RESTful Web Services.

ADaMS will propose simple, visually clear pages to be displayed at access points, with the reasons for an access refusal, at real time.

PERFORMANCE

The new system will perform a full evaluation of all accesses in less than 5 minutes (Fig. 4). This way, we can ensure a high degree of reactivity to any change in the source data used by ADaMS, This period of a refresh cycle will allow any modification to accesses to be propagated to any access point in less than 30 minutes, if desired.

ADaMS 3 will keep a full log of all changes in the source data; this new feature will allow to justify why an access has been lost or granted due to a change in the original system where data is fetched from, without the need to access that system's log mechanism (for those cases where there is one).

Unlike in the past, where for most criteria only the "date" was considered, ADaMS 3 will use the "hours and minutes" for start and end dates; this will allow to have finer access control, and better adapt to other systems such as IMPACT, that use the hours and minutes as well.

ADaMS will have a mechanism that will be able to asynchronously evaluate and make available one person's situation; this feature will be required if ADaMS is to be used as an individual protection equipment validator for access control in the future.

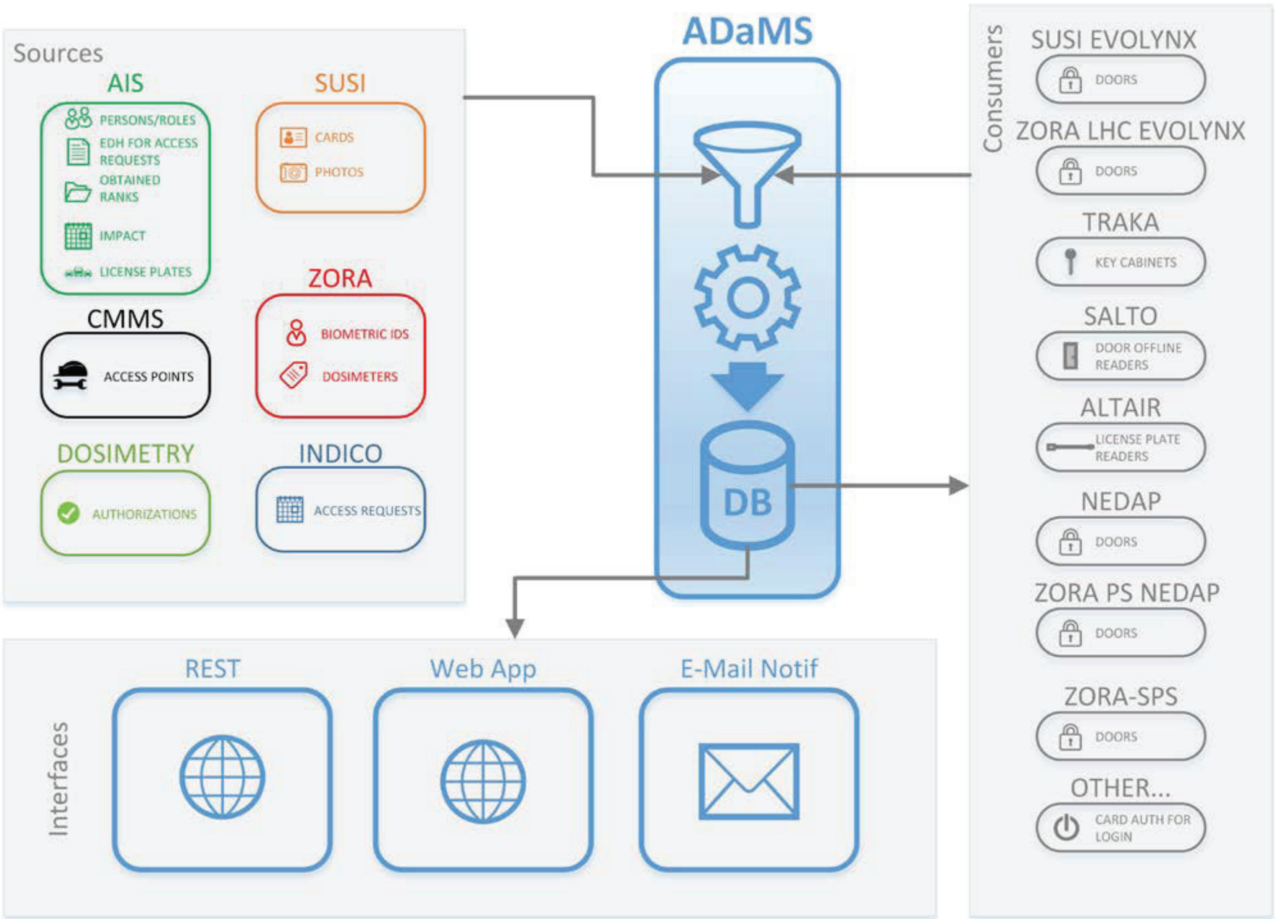

Figure 4: ADaMS 3 refresh mechanism, with its data sources and consumers.

ROLE BASED ACCESS CONTROL

ADaMS 3's interfaces (both GUI and programmable) will have a Role Based Access Control (RBAC) mechanism that will allow (or deny) a certain functionality to be applied to a particular data set; for instance, access to all access data concerning a contract's personnel will be granted to the person defined as the contract's manager.

ISBN 978-3-95450-148-9

RBAC will be implemented using CERN's AIS (Advanced Information Services) roles/egroups application, with role types and targets; the logged user is able to perform a certain function on data belonging to a certain person, if he/she is assigned to a role type that may perform the function on a target containing that person.

CONCLUSIONS

Physical access control for an organisation such as CERN is an evolving domain, with new and more complex constraints and devices being introduced constantly. ADaMS has been delivering access data to these systems, in accordance with changing policies since 2007; its original architecture has been stretched to the limit and it is now time to refresh its architecture.

ADaMS will help analyse and allow the modification of our access policies following the observations of the Long Shutdown 1 (LS1) access patterns and problems. It will also facilitate the access process and user experience for accelerator zones, providing new functionalities and interfaces.

ADaMS is also a key element in any access renovation project, as it needs to adapt to new constraints and requirements (e.g. the SPS access renovation project).

ADaMS 3 will allow CERN to continue having a single, centralised system for access management and distribution, adaptable to new requirements and scalable to the new domains where access control is required, while being at the same time, an important link in the safety chain of CERN's accelerators.

ISBN 978-3-95450-148-9