AMS-AC (AUTHORIZATION MANAGEMENT SYSTEM) AND DATABASES FOR ACCESS CONTROL

U. Epting
Division ST - Monitoring and Communication Group (ST/MC)
CERN, Geneva, Switzerland

Abstract
The concept for AMS-AC (Authorization Management System for Access Control) was developed in 1996/1997 with the participation of the Divisions AS, DSU, PE, PPE, ST and TIS. It covers the entrance rules to CERN, the types of CERN cards, and the access authorizations to controlled areas. The former paper-based procedure to obtain an access authorization has been transferred to a database driven system with electronic signatures. All necessary information are stored in the human resource database (HR). From there, the data is distributed to all card readers at CERN. A UNIX server controls the updating of the authorization data and performs automatic data transfers.
Additionally, several procedures have been developed:
1) HTML-based on-line database checks for immediate data control;
2) Database verification procedures;
3) Automatic information distribution.

1. INTRODUCTION

In 1996, the Director General asked for a global and effective access control policy for CERN. This was the reason for initiating the AMS-AC (Authorization Management System for Access Control) project. It resulted in three major improvements:

- Identification of every person on the CERN domain,
- Reduction of paper-based demands and replacement by electronic signatures,
- Stable databases and faster data transfer to CERN access points.

The concept was developed until Spring 1997 with the participation of the Divisions AS, DSU, PE, PPE, ST and TIS. The realization is progressing and is mainly done by the Divisions AS and ST. Additional software tools have been developed to facilitate the daily work of the persons concerned.

One of the results of the AMS-AC concept was the update of the Operational Circular No. 2, which defines the access rules to the CERN domain and all installations.

2. IDENTIFICATION OF PERSONS

The identification of persons on the CERN domain will be made by plastic cards. Everyone who has a working relationship with CERN or is member of the CERN Pension Fund should be in possession of a *CERN CARD*. These persons are registered in the CERN human resource database, called Oracle*HR (or shorter, HR).

All other persons will have a temporary access card, called *TEMPO CARD*. These persons are mainly visitors or persons staying at CERN for a short period (i.e. for some installation work) and are not registered in the HR database.

Six production points have been installed to ensure a proper distribution of the *CERN CARD*s and *TEMPO CARD*s. These production points are:

- Reception Desk in Building 33 (*CERN CARD*s and *TEMPO CARDs*),
- Registration Service in Building 55 (*CERN CARD*s and *TEMPO CARDs*),
- Users Office in Building 61 (*CERN CARD*s),
- Meyrin Entrance B in Building 120 (*TEMPO CARDs*);
- Prevessin Entrance in Building 880 (*TEMPO CARDs*)

Each plastic card has a unique identification number and shows the name of the card holder. Either a *CERN CARD* or a *TEMPO CARD* is issued to everybody before entering on the CERN site. This allows to identify every person traveling inside CERN.

The existing non-nominative visitor cards will be suppressed and replaced by the *TEMPO CARDs!*

3. REDUCTION OF PAPER-BASED DEMANDS AND ACTIONS

The *CERN CARD* or *TEMPO CARD* allows automatically the access to the CERN site. Access to specific areas, e.g. the LEP tunnel, is given upon demand and after the safety instructions into force have been followed.

The demands for access authorization to specific areas are presently done with a document which has to be signed by the responsible persons. The paper is usually transmitted by internal mail and it can take up to two weeks before it arrives at the Registration Service and that the requested authorization be entered in the database. This means that a person who asks for the access authorization for the LEP tunnel has to wait 2 weeks before he/she can access the required area.

According to the AMS-AC concept, the demand and the authorization of access will be done electronically. The demand will be filled in by the divisional secretariat, the Users Office, or any other responsible service. The demand will be transmitted electronically to the responsible persons who also “sign” electronically. After the necessary “signatures” have been given, the authorization is transferred immediately into the HR database and no further action is necessary. To speed up urgent demands, the responsible person for a specific area can enter the authorization directly into the HR database.

Safety courses to be followed or film badges issued will also be entered directly into the database and no lists will be sent to inform persons of the actions taken. This means that every service enters its data into the database instead of letting somebody else to take care of it.

4. STABLE DATA BASES AND FASTER DATA TRANSFER

All data has its source in the HR database. This ensures data integrity, safety, regular backups, and recovery in case of database failures. The data concerning access control consist of information about the *CERN CARD*, contractual data, and all access authorizations.

The connection to the HR database is done via a UNIX server, where all necessary programs are installed. Each night, several database checks are performed to ensure database integrity. Data records which are not following specific rules are sent via e-mail to the person responsible in order to rectify the situation.

For all types of access authorizations the data is transferred once per night to the appropriate card readers. Additionally “online transfers” are performed after data has been changed in the HR database during the day, to enable immediate access if necessary. These “online transfers” are presently done every hour.

5. CONTROL PROCEDURES AND FACILITIES

Several procedures and facilities have been realized in addition to the above-mentioned main tasks.

Internet based programs (but password protected) allow a fast access to all access control relevant data:

- checking data in the HR database,
- checking the actual status of the card readers,
- authorize persons temporarily at specific access points,
- gather data from the card production points for punctual maintenance.

Background processes allow to automatically inform persons in advance about any changes in their access conditions, e.g. all users receive, six weeks before the expiration of their access cards, an electronic mail which gives them their actual status and the necessary actions to take.

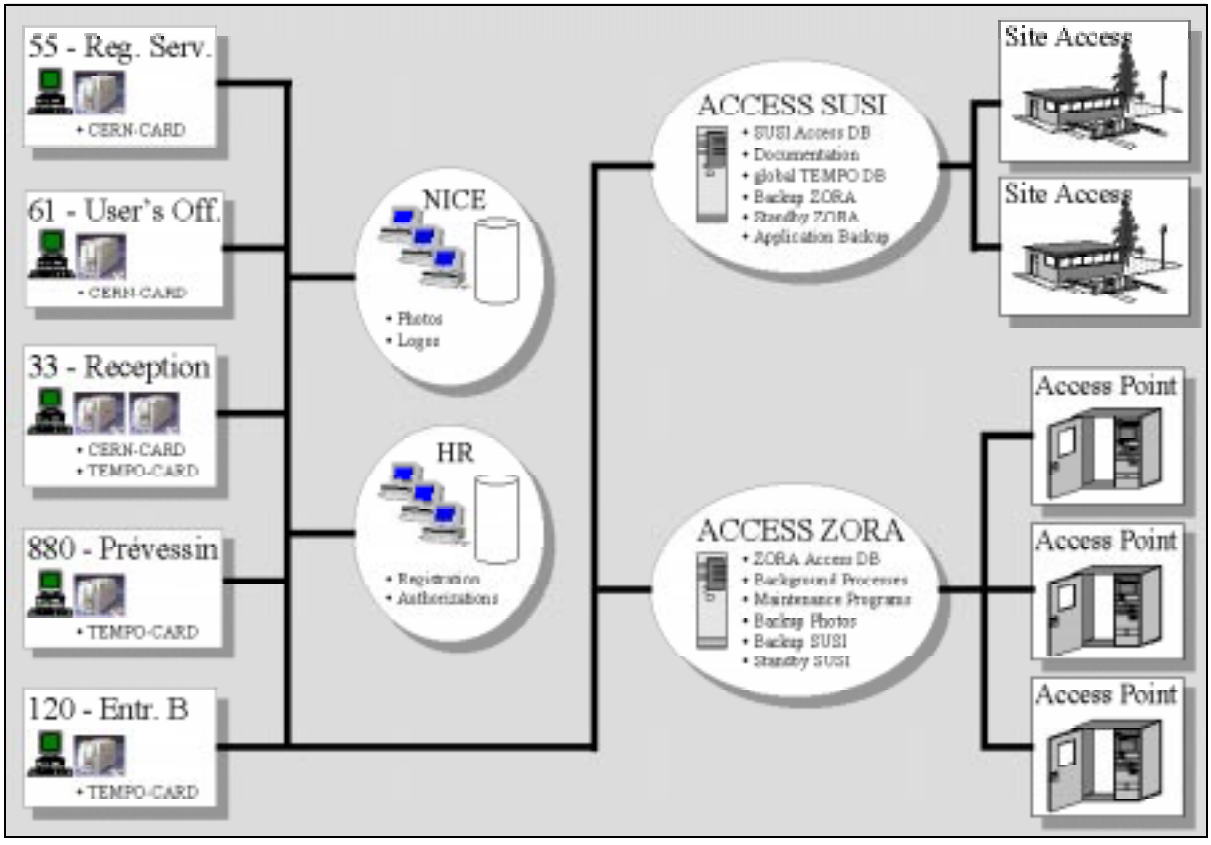

Fig. 1: System architecture.

REFERENCE

AMS-AC Proposal for the Future Concept - ST/MC/54/UE (February 1997).