UDC: 65.012:61
Preliminary communication

INTRODUCTION OF CENTRAL USER MANAGEMENT IN A LARGE UNIVERSITY HOSPITAL - A CASE STUDY

Peter Jürgen Klutke
University of Munich,
Faculty of Medicine, Munich, Germany
pklutke@med.uni-muenchen.de

Tobias Mertens
Microsoft GmbH, Unterschleissheim, Germany
tobiasm@microsoft.com

Abstract: *The department "organization and information technology" (OIT) of the Faculty of Medicine of the "Ludwig-Maximilians-Universität München" introduced a system to centrally manage user accounts and security during the last two years. The initial state was that we had several user directories for different services, resulting in high operating expense. We describe the aims, the concepts, the techniques, the realization and the difficulties we had introducing a central user directory. The new central user directory covers not only authentication, but also authorization in the connected subsystems. The following subsystems are connected: Windows logon, Email and Calendaring, various intranet services like medical documentation system, diagnostic findings of clinical chemistry or radiology, remote access to Email and Calendaring via a firewall, RADIUS and last but not least logging on to SAP, which is our ERP (enterprise resource planning system).*

Keywords: *central user management, user directory consolidation, Active Directory, LDAP, user authentication, user authorization.*

1. INTRODUCTION

The "**Ludwig-Maximilians-Universität München**" (LMU) is with about 44000 students and 19 faculties among the largest universities of Germany.

The **Faculty of Medicine**, which consists of the University Hospital located in Großhadern and the City Center of Munich, the clinical-theoretical and the theoretical facilities, is the largest medical training establishment in the south of Germany. The University hospital consists of 33 clinics, 9 institutes and 11 departments. It has 2560 beds, 480000 treatments per year (outpatient and stationary) and more than 9000 employees.

From an academic and clinical point of view as well the faculty enjoys an international reputation and an international standard, measured by the amount of outside funding, by the number of collaborative research centres of the Deutsche Forschungsgemeinschaft (a

German research association), of postgraduate courses, of research teams and of national and international cooperative projects.

The faculty's clinical focal points are many and varied. In particular, it is pre-eminent, both clinically and academically, in heart and circulatory diseases, the neurosciences, oncology, and transplant technology, and it is developing new diagnostic techniques with the help of imaging processes and the application of laser technology. With the Munich Model (Munich-Harvard Alliance) the Faculty of Medicine is establishing new forms of teaching and learning for studying human medicine.

The **department "Organisation und Informationstechnik"** (organization and information technology, OIT) of the Faculty of Medicine is a service organization for the clinical centre and of the theoretical institutes of the faculty in matters of **central electronic data processing** (EDP) including the organizational tasks in this field.

Among its tasks are in particular:

- Planning, operating and administration of the central communication network
- Coordination, support and advice regarding planning, purchase and start-up of data processing equipment and software
- Realization of data processing projects
- Development, coding, testing documentation of programs
- User support service including a central hotline
- Specification of central standards in reconciliation with the users

The department OIT has 70 employees, of them 26 in the subdivision operative information technology, 20 in EDP for business management and 11 in medical EDP.

The various departments belonging to the clinical centre (surgery, neurology, anaesthesia, ...) are rather independent concerning their department-specific EDP services (hardware and software). Using central EDP services, the departments have to collaborate with the OIT. To facilitate this, each department has a **commissioner for EDP**, who is the contact person for these concerns, especially the reconciliation of the department's EDP issues with the OIT. For example, he applies for new user accounts for central EDP services.

Because they are repeatedly needed, we would like to define the terms "authentication" and "authorization". "Authentication" is the way that you can confirm that you are who you say you are, when you need access to computer information that is restricted or confidential. Most of the time, a unique username and password pair is used to identify each person who uses a computer system. A person who knows username and password of a user is supposed to actually be this person. "Authorization" defines a (authenticated) user's access rights to resources, which could be files, printers, Emails or entire subsystems. For example, by joining a user to the administrators group, he is authorized to have full control of all files of a file system.

2. INITIAL STATE AND PROBLEMS

Two years ago, the services for personal computers were based on a **MS Windows NT 4.0 Domain**, a NT 4.0 fileserver in this domain and about 3000 NT 4.0 workstations, serving as workplace for doctors, nursing staff and administrative staff (see Figure1). The domain stores its user accounts its own proprietary user directory (SAM).

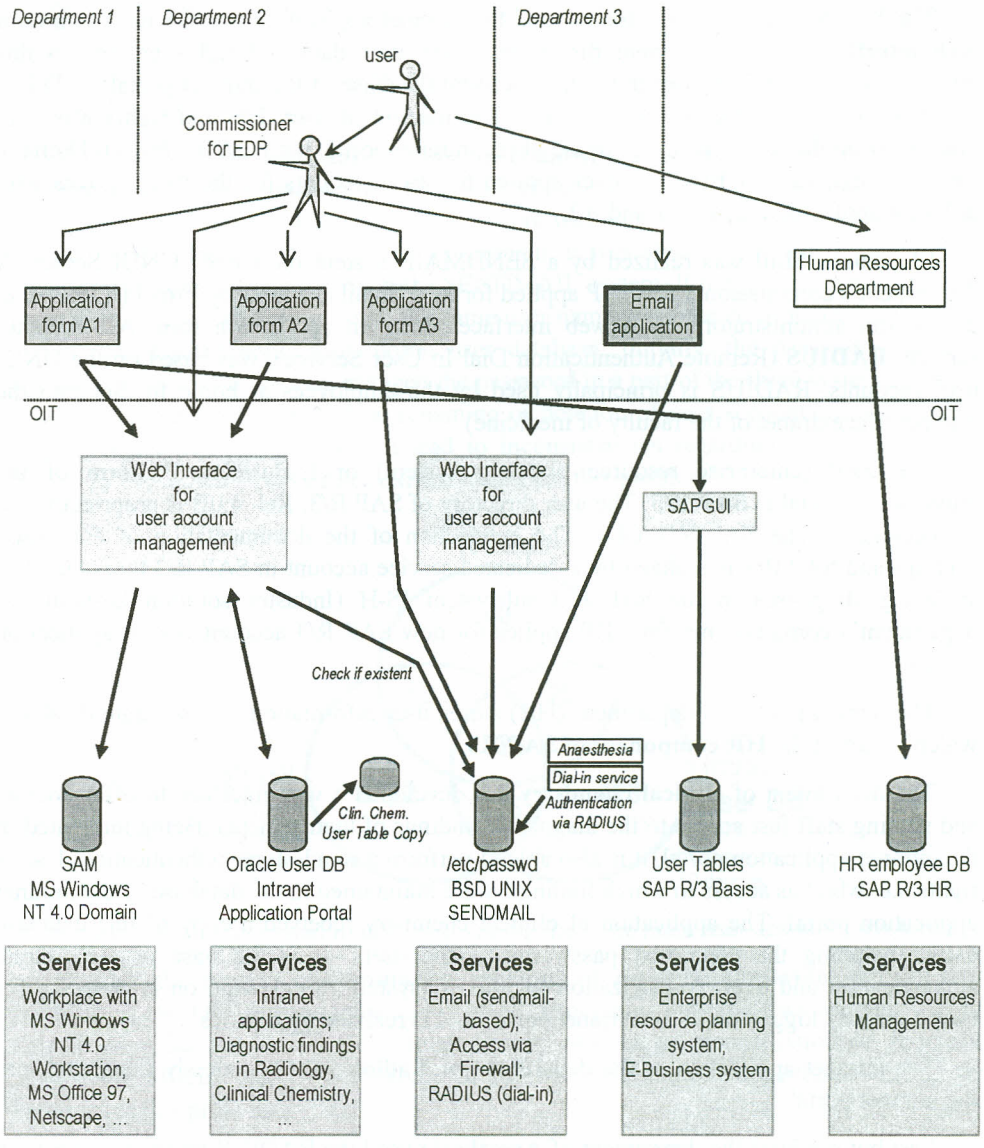

Figure 1: Initial state of user account management

In addition, the faculty has an **intranet application portal** ("Infothek") offering various intranet services. Among them are retrieval of findings concerning radiology including images, clinical chemistry, recordation of diagnoses and medical services, a reporting system of medical findings and more. The user directory for this intranet application portal was an Oracle Database, where user accounts, roles ant their relationship are stored.

The MS Windows NT 4.0 domain and the intranet application portal have a **common web interface** to their different directories. New user data and rights entered in this interface resulted in a new set in the user account database of the intranet portal AND in a new user account in the NT 4.0 Domain. The readout of user data and rights was only possible from the user account database of the intranet portal, not from the NT 4.0 Domain. The commissioner for EDP however applied for user accounts for the two services with different application forms A1 and A2.

Electronic Mail was realized by a SENDMAIL system on a BSD UNIX Server. A department's commissioner for EDP applied for new Email accounts by Email (if known to the system administrator), by a web interface or by an application form A3. Another service, **RADIUS** (Remote Authentication Dial In User Service), was based on the UNIX user accounts. RADIUS is principally used by the employees at home to dial into the internet (the extranet of the faculty of medicine).

The ERP (enterprise resource planning system) or E-Business Platform of the university hospital is **SAP R/3**. The user directory of SAP R/3, Rel. 4.0B is proprietary and is accessed by the SAP R/3 GUI. The connection of the documentation of diagnostic findings and SAP R/3 is realized by a dedicated service account in SAP R/3 that is used to store e.g. diagnoses in the SAP R/3 subsystem IS-H (Industry solution hospital). A department's commissioner for EDP applies for new SAP R/3 accounts by an application form A1.

The human resources department (HR) stores user information in a separate database, which is part of the **HR component of SAP/R3**.

The department of **clinical chemistry** has developed a web interface to offer doctors and nursing staff fast access to the diagnostic findings of their patients. Being integrated in the intranet application portal, it is also able to perform a stand-alone authentication. User's rights, i.e. who has access to which findings, were maintained in the database of the intranet application portal. The application of clinical chemistry received a copy of this database daily, including the clear text passwords of the users. It is the base of stand-alone authentication and every authorization for this subsystem. Single-sign on is possible if a user is already logged on to the intranet portal, and is realized by cookies.

The intranet application of the department of **Radiology** is seamlessly integrated into the intranet portal.

Last but not least the department of **Anesthesia** used the RADIUS protocol against the SENDMAIL server for authentication concerning the department's application.

The initial state implicated the following **disadvantages and problems**.

The **different and not transparent ways of application** for the various services made it difficult for the commissioner for EDP to order the services in the designated way. There was also a high administration effort.

User maintenance, apart from creation of users, was **hardly possible** and rarely done. Only the database of the intranet application portal allowed the commissioner for EDP to read user data of his department. The other systems did not have this completion confirmation. Especially when applying for services by an application form, a completion information would have been desirable but was not implemented. Furthermore, the application form was transported by interoffice mail, which is of course not the fastest way and not always reliable.

Another issue is that **hardly any mechanisms existed to keep the different directories in a synchronous state**. The SAP systems have a different naming convention and were not kept synchronous at all. When there was an application for an account for the intranet application portal or the NT 4.0 domain, it was always checked if there already existed an account for that person in the SENDMAIL system. If not, an account was created there at first. Then an account with the same user name was created in the NT 4.0 domain and in the intranet application portal user database. Initially, the passwords were set identical. However, if the user changed the password in a part of the three systems, it would result in different passwords. Also renaming or deletion of user accounts in a part of the three systems was possible, which lead to inconsistencies regarding user accounts (see Figure 2). No administrative rules existed to resolve this problem.

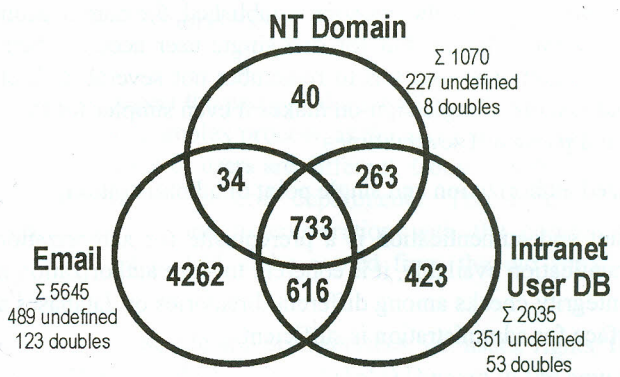

Figure 2: Differences and intersection among the three main user account directories

Besides, the process of **eliminating accounts of resigned employees** did not work properly. If the OIT got the information at all, it occurred that the user account was not deleted from all directories. No regular cleanup process or reconciliation of directories against the official employee database of the human resources department existed that could solve this problem.

What is more, *data security* concerning the intranet application portal was very weak. On the one hand, passwords were stored in clear text in the database and this database was copied to other departments, on the other hand, the password entered in the user interface was transported in clear text to the server performing the authentication. This evidence showed that the software architecture was not state of the art. On the other hand user

accounts commonly used by a department or even a whole clinic existed, making entry and change control impossible.

Finally, the **introduction of Windows 2000 and Exchange 2000** was pending. Consequently, a further user directory (MS Active Directory) had to be introduced and to be integrated in the existing structures. Leaving the existing structures unchanged would have lead to an even more complex structure. Maintenance of active directory user accounts by the existing web interface would not have been possible, especially as enhanced functionality of active directory is concerned.

3. OBJECTIVES

Consolidation of existing user directories to reduce complexity and administration effort:

Each directory needs maintenance effort by itself for hardware (server, hard disks), software (directory software, database), directory contents (objects, their properties, schema), interfaces (application forms, web interface, rights of administering users) and so on. So the reduction of the number of directories reduces the administration effort. What is more, the effort for manual synchronization of user accounts, passwords and attributes among the directories disappears.

- Simplified authentication by the same username/password for various applications or even single-sign-on for selected applications (Outlook 2000, SAP):

A central user directory for authentication established, the commissioners for EDP have to apply not for several different, but for one single user account, being the same with maintenance and deletion. The user has to remember not several different account names and passwords, but just one. Single-sign-on makes it even simpler for the user not having to reenter his name and password several times.

- Centralized authorization and single point of administration:

A user account and authentication is a prerequisite for authorization. A central user directory for authentication available, it is coherent to store authorization information in the same directory. Integrity checks among different directories or databases are not necessary, and a single interface for administration is sufficient.

- Introduction of validity checks for user accounts:

Security issues (among others) make it necessary to identify accounts of resigned employees, normally to eliminate them. Using the information of the official human resources database (SAP HR) can help to realize this.

- Simplification and acceleration of user account application:

When a new employee starts to work in the hospital, he immediately needs access to EDP-systems. As a result, a fast user account application including changes of user roles, rights and permissions is necessary.

- Seamless integration of the new back office, Email and client environment based on Windows 2000 Server and Workstation and Exchange 2000 / Outlook 2000:

The pending introduction and availability of the new directory "Active Directory" required for Windows 2000 should harmonize with the objectives mentioned above.

4. PROCEDURE

In this section, we first describe the principal way to achieve the objectives listed before. After that, specific realization details are highlighted.

4.1. PRINCIPAL WAY

For several reasons discussed in the next section, we chose Active Directory to realize our new central user directory.

To achieve the **consolidation of the user directories** in general, we had to export the user data (all stored attributes) of the existing user directories, check their validity and import them into Active Directory.

As a *first step*, we imported the database of the intranet application portal. A check for duplicate user names was not necessary because the former database used the user name as primary key and the Active Directory was initially empty. Simultaneously the authentication and authorization procedures of the intranet application portal system had to be modified so that they work against Active Directory using LDAP requests. In this state, the only function of Active Directory was to realize authentication and authorization for this system.

The *second step* was to import the users of the UNIX SENDMAIL system into Active Directory. This is a much more complex process, as the user names in the two systems need not be identical as well as the set of users are different. Consequently we divided this step into the import of users of the several departments. The validity checks and the consolidation of accounts was done in cooperation with the commissioner of EDP. Simultaneously, the user's Email had to be copied from the old Email system to the Exchange 2000 databases.

The *last step* was to move the file and print services, i.e. users, rights, files, directories and other and resources, from the old Windows NT 4.0 Domain to the new Windows 2000 Domain providing Active Directory. This step was also divided according to departments and done in cooperation with the commissioner of EDP. Subsequently, the whole PC based workplace of the users was migrated to the new domain. For users working with anonymous group accounts user accounts have been created.

With the new user directory being established, the subsystems of **Clinical Chemistry** and **Anaesthesiology** changed the Authentication procedure in their subsystems to LDAP requests against Active Directory, which could be achieved easily.

The next step, which is already in progress, realizes the authentication and authorization for inward and outward access via the **firewall** using Active Directory. Tests have shown this process to work properly.

Afterwards we will establish authentication and authorization of our **E-Business Platform** (SAP R/3) against Active Directory. Authentication will be realized using Single-Sign-On using the Kerberos protocol [5]. Other companies already use this procedure. For authorization, however, a user directory within the SAP system will persist. It will be synchronized with Active Directory regularly using procedures provided by SAP.

Finally, the following services will be available with the key "user name / password" of the new central user directory: Windows 2000 file and print services, Exchange 2000 office communication, various intranet applications, the subsystems of Clinical Chemistry and Anaesthesiology, firewall access and the E-Business platform. Authentication and Authorization of all mentioned subsystems can be centrally managed (see Figure 3).

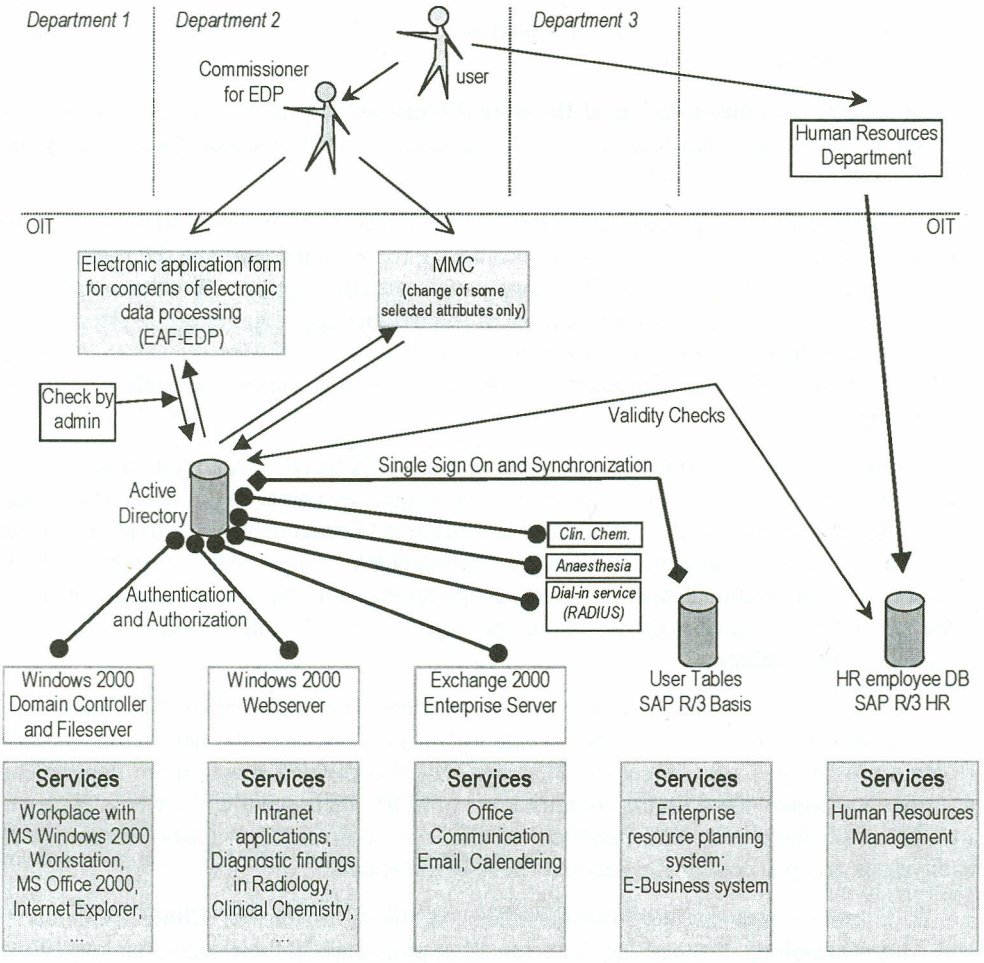

Figure 3: Nominal condition of user account management

Another objective was to simplify and accelerate user account application. To achieve this aim, we developed the **"electronic application form for concerns of electronic data processing"** (EAF-EDP). It is a web interface for the commissioner of EDP to "access" Active Directory. He can view all user accounts of his department and he can apply for new user accounts as well as for changes and for deletion of existing user accounts. The

workflow is as follows: The user informs his department's commissioner for EDP of his needs (e.g. new account, enhanced rights). The commissioner for EDP checks if the user is allowed to get his needs fulfilled. If so, he applies for these needs by filling out the web application form (EAF-EDP). Once completed, the form appears on the screen of an administrator. He inspects the application and checks for permission, plausibility and naming conventions. If successfully checked, the application form can be executed by the administrator, resulting in the related changes in Active Directory and other subsystems, e.g. the fileserver or the Exchange Server. An application may also be relegated to the commissioner of EDP. The EAF-EDP allows an administrator to work as a further instance of control which would not be possible if the commissioner used the Microsoft Management Console (MMC) directly. For user attributes that have no effect on rights and where changes are not critical (e.g. a user's description), the commissioner of EDP has direct access on the attribute by the MMC (see Figure 3).

Introduction of **validity checks for user accounts** is realized by two procedures using the employee asset database of our human resources department. When a new user account is to be created or an existing account is to be modified, its given name, surname and department are checked against the HR database. If the user exists in the database, its employee-ID from the HR database is stored in an attribute of the user in Active Directory. If the user cannot be found in the HR database, the account is marked as "external account", it has a maximum validity of six months and the HR department is automatically informed by Email. This first validity check is integrated in the EAF-EDP. The second check is a quarterly control run of a program that searches for each user account of AD (given name, surname, department, employee-ID) in the HR database. A report per department grouping the users of different levels of matching and the "external accounts" is generated. The commissioner of EDP has to confirm the correctness and has to apply for changes in AD where applicable (see Figure 3).

4.2. DETAILS

It is worth to have a closer look on how information regarding authentication and authorization of users is stored in and can be retrieved from Active Directory.

Authentication of a user is done by checking if the user account exists and is valid and whether the password for the user account is correct. User accounts are stored in active directory as well as their attributes, one of which is the user's password. The authentication when a user logs in to a Windows 2000 Workstation is integrated in the operating system. If you have developed an application of your own, the simplest method to authenticate a user is to try an LDAP BIND with its credentials (username/password) [7]. If it fails, authentication is not possible, if it succeeds, the user is authenticated. For example, the login procedure of the intranet application portal asks the user for username and password and tries an LDAP BIND against Active Directory. If it succeeds, the user is forwarded to a continuative web page. If it fails, however, an error message is displayed.

Authorization information can be stored in various ways in a directory, but it may also be stored outside of it. Three examples shall illustrate this.

1. In Active Directory, a user may be disabled and of course enabled again. If the user is enabled or not, is stored in a special attribute of the user. In this case the authorization

information is stored inside Active Directory. Another example would be the allowed logon time (e.g. on weekends only), which is also stored inside Active Directory.

2. A user may be given certain access rights on a file or on a directory. This information can be stored in the file system directly. For example, if a user "scott" has read and write access on a directory "surgery_studies", its SID (security identifier) together with the right "read and write" is stored in the ACL (access control list) of the directory "surgery_studies". This access control list is stored in the file system. In this case the authorization information is stored outside Active Directory.

3. The third method is a combination of the first and the second. In our example, it requires a group "surgery_studies-rw" (or similar) in Active Directory. The members of the group "surgery_studies-rw" are given read and write access on the related directory "surgery_studies" by a corresponding entry in the ACL list of the file system. The user "scott" is then made a member of the group "surgery_studies-rw". This group membership is stored in Active Directory. By adding or removing a user from the group, you can define if he has read and write access. Defining appropriate groups, the whole management of file access rights may be managed within Active Directory by group memberships. This is a recommended method (see Figure 4).

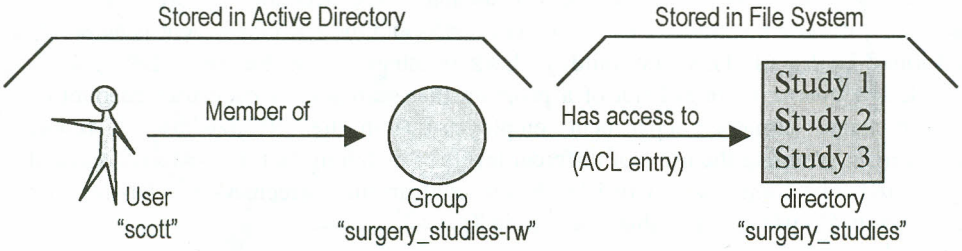

Figure 4: Defining file access rights using group memberships

To **store authorization information** of other applications or subsystems **in Active Directory**, we mostly use this third method. For example to store the authorization information of the subsystem "recordation of diagnoses and medical services", we defined two sets of groups. The first set of groups consists of one group for each medical unit. The second set of groups consists of one group for each role a doctor may have (e.g. "basics", "documentation officer", "controller", "medical administrator", "billing officer", etc.). By adding a user object to one or more groups of each set you can assign specific rights, for example the role "controller" for medical unit "Surg_1" and "Surg_3" (see Figure 5; the term "Surg" abbreviates "surgery").

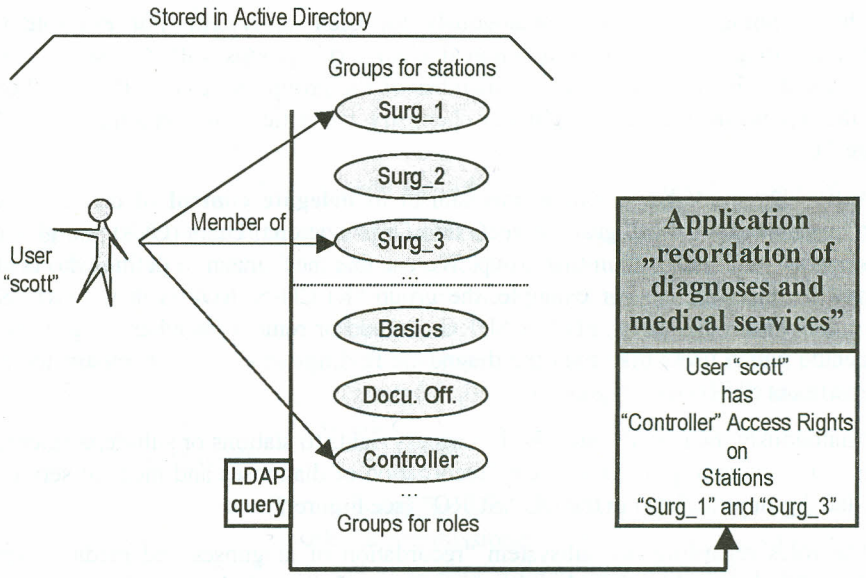

Figure 5: Defining application authorization using group memberships

Authorization information stored in this way may be retrieved by an LDAP query for the user's attribute "member of", which contains all group memberships of this user. For example, when an authenticated user chooses the subsystem "recordation of diagnoses and medical services" from the intranet application portal, his attribute "member of " is queried. Memberships relevant for "recordation of diagnoses and medical services" are recognized by naming conventions for the groups (prefix, suffix) or a group attribute. The rights for this user are set according to the relevant group memberships and stored in a ticket (see Figure 6).

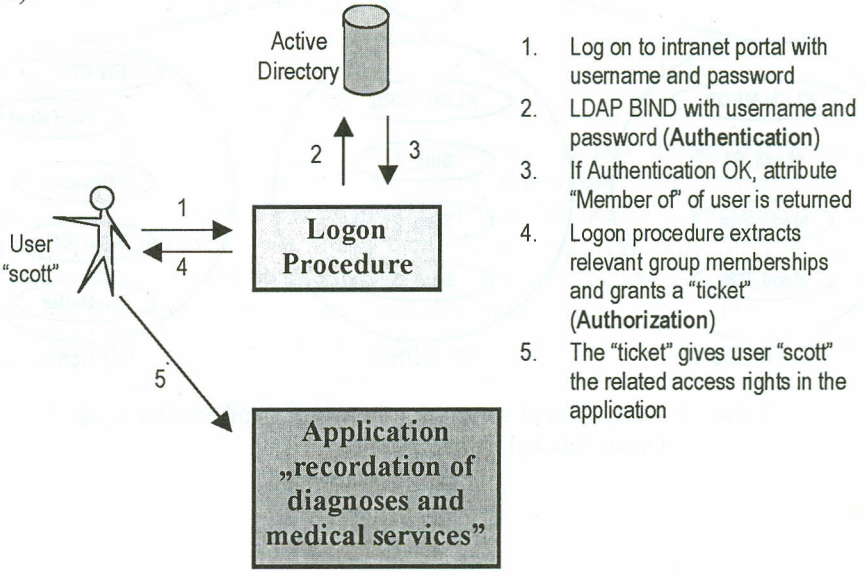

Figure 6: Workflow of Authentication and Authorization against Active Directory

This technique is repeated analogously for each subsystem. For example for the subsystem "diagnostic findings of clinical chemistry" groups with the syntax "KLCH-<department>" have been created. A member of the group "KLCH-SURG" is allowed to read the diagnostic findings of clinical chemistry for patients of department SURG (see Figure 7).

Active Directory has a simple mechanism to **delegate control** of certain objects to determined users. You can group objects into Organizational Units (OUs) and give certain users control of the objects in this group. We use this mechanism to define who is allowed to grant or reject rights. For example, the group "KLCH-SURG" is in the OU "SURG" where the commissioner for EDP of SURG can add or remove members of groups. So he can decide which users may read the diagnostic findings of clinical chemistry for patients of department SURG (see Figure 7).

Analogously, he may decide who has access rights to stations or sub-departments of his department concerning the subsystem "recordation of diagnoses and medical services". So the related groups are also in the OU "SURG" (see Figure 7).

The roles regarding the subsystem "recordation of diagnoses and medical services", however, are assigned by the administrators group. Consequently, the related groups are in the OU "Admin" (see Figure 7).

The integration of further subsystems into the management of authorization information is easily possible. Just a new set of groups has to be created and users have to be made member of them. For example, the groups "FW-TELNET" or "FW-FTP" may grant its members the right to use the related services across the firewall (see Figure 7).

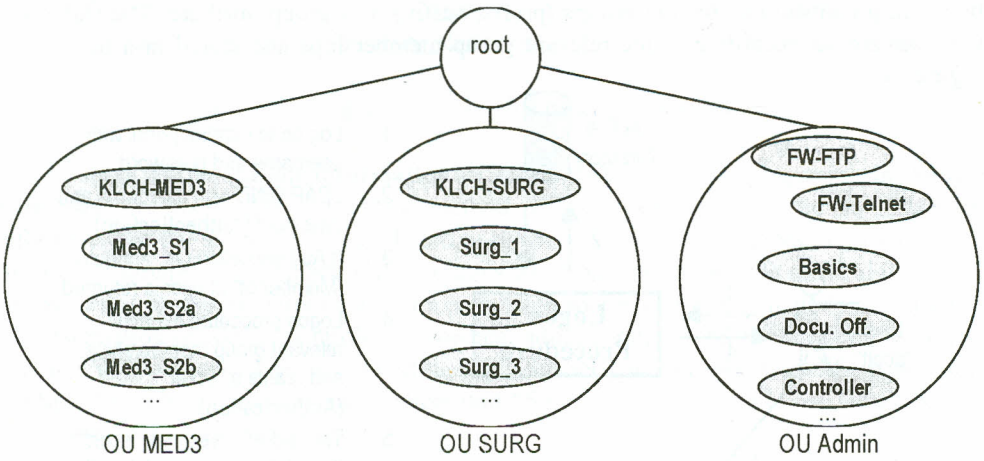

Figure 7: Delegation of control for the group memberships using Organizational Units (OUs)

5. RESULTS AND DISCUSSION

In this section we want to summarize the results and discuss them along with the method.

About 75% of the departments are moved to central user management. The connection of the E-Business platform and the firewall are tested and will be realized in the year 2002.

The objectives mentioned before were fulfilled. The account application time could be reduced from days to minutes. The administration of departments participating in central user management has become a lot simpler. Servers of old user databases have become needless. The concept of central management of authentication and authorization is successful and extensible. Validity checks against the HR database help to keep the directory clean. Anonymous group accounts have been replaced by personal user accounts as far as possible. Finally, the new Windows 2000 domain and the Exchange 2000 system could be integrated seamlessly.

The main difficulties occurred concern the cleanup of the user directories for each department. The communication with the commissioner for EDP was not always effective. Users have moved from one department to another without informing their commissioners for EDP or the OIT.

The consolidation of user directories could be achieved by introducing a metadirectory, like "Microsoft Metadirectory Services (MMS)" or "Siemens Metadirectory" [6]. However, this introduces extra costs. So we tried to achieve all objectives using MS Active Directory, which is part of the Windows 2000 Server family that we intended to introduce anyway. What is more, Active Directory already contains a complete security subsystem, which is used by all other Microsoft subsystems (file and print services, office communication system Exchange 2000) and a huge amount of further system providers.

The use of a database for integrated user management could also have been an alternative [4]. This procedure, however, could be implemented in Active Directory, too. Maintaining authorization information in an LDAP server has already been used for a web-based clinical information system [1].

We are convinced that a lot of the experiences gained during our project are transferable to other scenarios. Using Group membership to store authorization information of subsystems is a very flexible and extensible solution. The use of existing attributes or the application of schema extensions is less fault tolerant and more difficult. The access to authentication and authorization information by LDAP queries is simple and has proven to be robust. Moreover, it has already been used in similar frameworks [2]. The reconciliation to the HR database, i.e. the check while generating or modifying user accounts and the quarterly generation of reports is both simple and efficient. However, also automated synchronization may be useful here [3].

REFERENCES

[1] Hripcsak, G.; Cimino, J.J.; Sengupta, S. (1999): *WebCIS: large scale deployment of a Web-based clinical information system*, Proceedings-AMIA-Annual-Symposium.-AMIA-Symposium. 1999; 804-8

[2] Hughes, D. (2000): *User-centric account management and heterogeneous password changing*, Proceedings of the Fourteenth Systems Administration Conference (LISA XIV). USENIX Assoc, Berkeley, CA, USA; 2000; vii+378 pp. p.67-76.

[3] Jackson-Higgins, K. (2002): *Energizing the enterprise directory*, Network-Computing. vol.13, no.3; 4 Feb. 2002; p.55-7.

[4] LaMeyer, A.; Ganesan, S.; Johansson, JM. (2000): *On designing a database for integrated user management: pitfalls and possibilities*, Proceedings of the 3rd Large Installation System Administration of Windows NT/2000 Conference. USENIX Assoc, Berkeley, CA, USA; 2000; 69 pp. p.19-27

[5] Marks, H. (2000): *Using Win2000's foolproof encryption*, Network-Computing, vol. 11, no. 21, p.156-158

[6] Mester, A. (2000): *"Meta-directories" and federated information systems: can their communities learn from each other?*, Engineering Federated Information Systems. Proceedings of the 3rd Workshop EFIS 2000. Akademische Verlagsgesellschaft Aka, Berlin, Germany; 2000; v+114 pp. p.114.

[7] Morana, M. (2000): *Browser-based directory access through LDAP and COM*, C/C++-Users-Journal. vol.18, no.7; July 2000; p.34, 36, 38-40, 42-4, 46, 48-9

Received: 9 January 2003
Accepted: 9 October 2003