Identity and Access Management for a Hospital Information System

Walter SWOBODA, Simon LEUTNER, Peter KLUTKE

Hospital of the University of Munich

Abstract. Because we are using several identity databases for clinical purposes (as many other hospitals), we were looking for a general role-based access system. A central identity management system (IAM) was implemented, which provides a very comfortable solution for physicians and nurses. We found a great deal of all uncovered errors and problems is associated with the HIS belong to roles, identity and identity management. So IAM systems are an important part of modern hospital information systems.

Keywords. Identity, Access, Role-based.

Introduction

At the Hospital of the University of Munich many different systems are used for sampling, storing, and processing data for clinical and administrative purposes. Hence several identity databases are existing, i.e. an SAP HR database for personnel management, Microsoft AD for user-registration on clients, a special SAP database for eprocurement, and some others. To decrease costs and complexity, we were looking for a central role-based access system to manage these different access databases.

1. Requirements

Now a new area-wide hospital information system (HIS, Siemens i.s.h.med) makes particular demands, because it handles with medical data which are directly used for treatment of patients. Therefore the HIS, its devices, and its network can be seen as a combined medical-engineering device with very high requirements on data security and data privacy by law (see DIN EN 80001).

As a specific challenge the HIS handles not only with the identity of the actual user, but also with the identity of a “responsible person”, normally a high qualified physician who can order x-rays and invasive examinations. In many cases the “responsible person” is identical to the user, but not on cases like preparing clinical orders by medical assistants (i.e. order for x-ray examination). Because of limited personal resources in clinical daily routine users will not accept frequent re-registering: single-sign-on is highly recommended. We need one single system for authorization on many systems with very high safety requirements.

1 Corresponding Author.
2. Method

We set up a “Who's Who” identity database of our employees based on Siemens' identity and access management (IAM) X.500/LDAP product DirX, which is filled with data of the MS AD database. To verify the authorization, the system searches in the personnel managers' SAP HR database for equality of name, first name, date of birth, job title, ward, and other items. Little differences can be balanced via a defined “matrix of tolerance”. Only after authorization in MS AD and SAP HR the user is able to log in an access application by name and password. Driven by special attributes of MS AD and SAP HR databases, the user's clinical role and the correct “responsible person” are chosen and transmitted to the HIS.

The access application is a very comfortable solution for our physicians and nurses, because it offers access not only to the HIS, but also to other applications of clinical interest, e.g. laboratory information system, radiology information system (RIS), picture information and communication system (PACS), applications for presentation of diagnostic findings, and others.

Table 1 shows the distribution of our roles.

<table>
<thead>
<tr>
<th>Physicians</th>
<th>Care</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,340</td>
<td>3,230</td>
<td>2,360</td>
</tr>
</tbody>
</table>

Total: 7930 roles for 5120 associates (updated 1/2011)

3. Lessons learned

The IAM system is still under construction, but integration tests (DirX, I.s.h.med, SAP, and MS AD) were successful performed. Approximately 20 percent of all uncovered errors and problems associated with the HIS belong to roles, identity and identity management (i.e. not to be able to do a specific clinical transaction like documentation of a diagnosis). Therefore IAM is an extremely important part of every HIS [1]

References