OpenEyes - Authentication

Editors: G W Aylward
Version: 0.9:
Date issued: 8 June 2010

Target Audience

General Interest	
Healthcare managers	
Ophthalmologists	✔
Developers	✔

Amendment Record

Issue	Description	Author	Date
0.9	First issue	G W Aylward	8 June 2010

Table of Contents

Introduction

Authentication is the act of confirming that a user is genuine, and then allowing access to the components of OpenEyes permitted for that user. A range of information will be held by the system about the user, and this document gives detailed information about where that information is held, and how much is editable either by the user, or the system administrator. Once the login process has finished, OpenEyes will know all relevant information about the user, not only for security reasons, but also to assist intelligently the user when performing data entry or retrieval.

User Information

Information about the user is held in several tables within OpenEyes, as well as in external systems which, in large installations, OpenEyes will interrogate. A large organisation such as a hospital will already have an established system for authentication. It is desirable for OpenEyes to make use of this, in order to avoid the duplication of effort and user confusion that might arise with a separate system for usernames and passwords. However, the Role Based Access Control system (RBAC) used by OpenEyes requires a level of detail that may not be present in a simple authentication system. Finally, detailed information used, for example, for correspondence required a level of detail unlikely to be found in either the authentication or the RBAC system.

Figure 1 shows how user information is distributed between components of a large system, recognising that for small scale user installations, these entities might well be compressed into one, or at least be running on a single machine. Table 1 shows the suggested configurations for a range of possible installations based on scale. In a single user system, a much simpler scheme using a simple user and password table, with no need for RBAC would be appropriate.

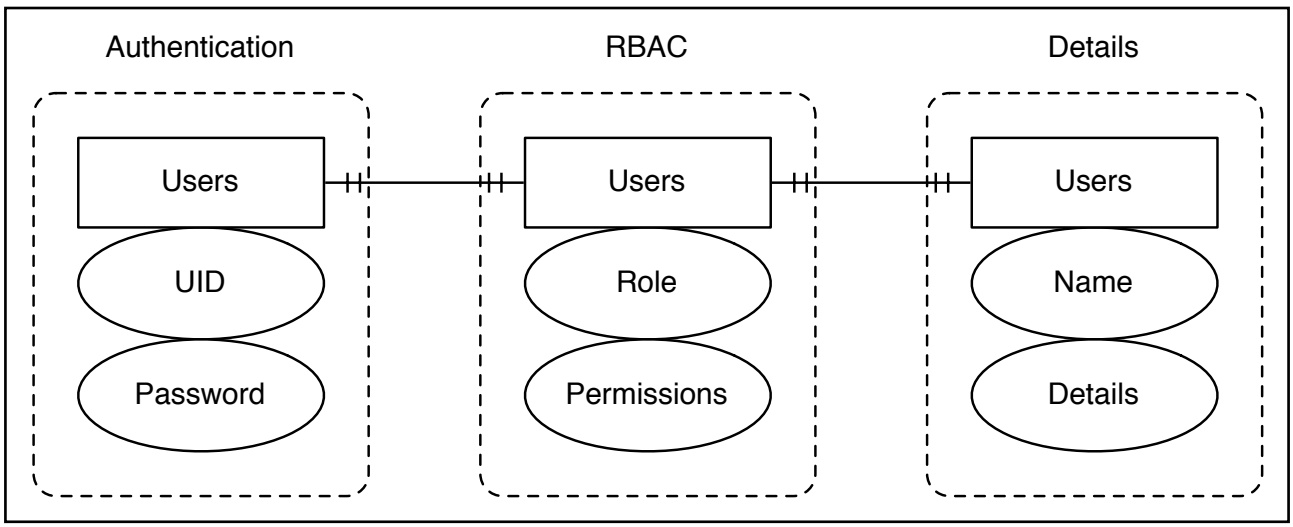


Figure 1. Entity diagram showing the distribution of user information throughout systems in a typical large organisation.

Table 1. Example configurations for OpenEyes installations of different scales

Setting	Individual practise	Small department	Large department	NHS Hospital
Users	1 - 2	10 - 20	50 - 100	200 +
Authentication	OpenEyes	OpenEyes	LDAP server	Active Directory
RBAC	None	OpenEyes	OpenEyes/LDAP server	OpenEyes/LDAP server
Details	OpenEyes	OpenEyes	OpenEyes	OpenEyes

Logging On

This section describes the login process in detail, and how user information for OpenEyes is distributed throughout a large department or NHS hospital. A flow chart summarising the process is shown in Figure 2.

1. Login screen

The login process takes two pieces of information, a unique user identifier (UID) and password. The UID is a string with no constraints on its format or content, other than being unique (i.e. a user may call themselves almost anything they like)

2. Authentication

After the user has submitted the UID and password, the system interrogates the system server to check credentials. This can be done either within OpenEyes, within RBAC, or from an external system, such as active directory. If successful, it will then retrieve the consultant firms that the user is associated with (firms are stored as roles within RBAC). There is a complex relationship between consultant firms, clinical services, and specialties which is the subject of another document.[1] These are then offered to the user to choose before proceeding. Once the choice of firm has been made, the time and date of the login are stored.

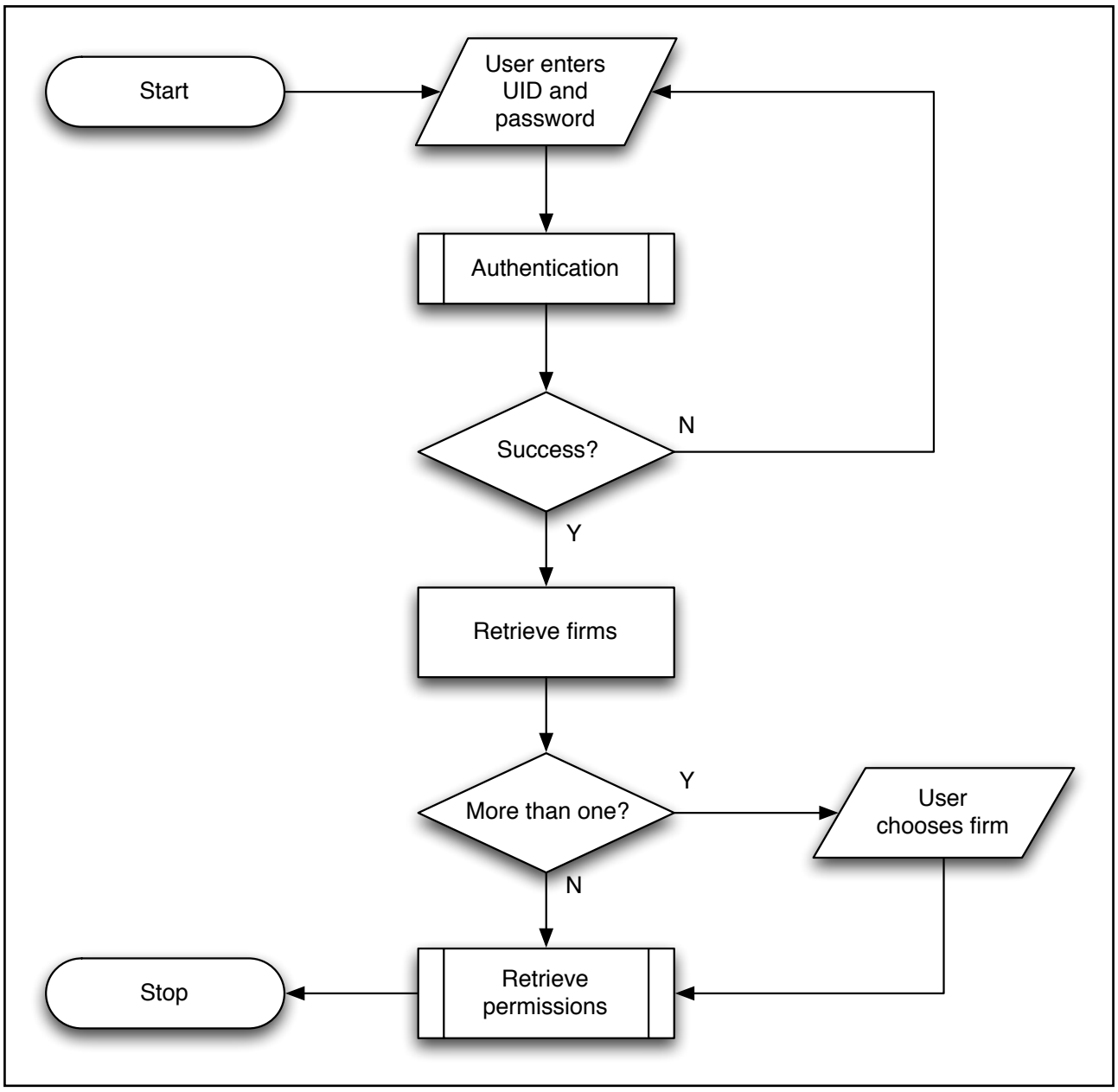
3. Permissions

The RBAC system is then interrogated to retrieve all permissions associated with the user (according to their role). Permissions are stored as an array in a session variable, so are accessible for the duration of the logged in period. The clinical service, and specialty are also retrieved and stored as session variables, so that system choices are appropriately tailored to the user.

4. Retrieve additional user information

More detailed user information (such as description, title, address, email and telephone numbers) are then retrieved from the OpenEyes database. Much detail (for example addresses, telephone numbers, and email are identical to external contacts, so are appropriately stored in the contacts table. All user related data within OpenEyes is linked by the numeric user_id field.

Figure 2. Logging on flowchart



User Information

Very few assumptions are made about how an organisation stores information about users, so OpenEyes only expects a minimum set of information to be retrieved following the authentication component of the login process (Table 2)

Table 2. Minimum information set retrieved from a hospital wide system, such as active directory

Item	Description
user_id	Unique integer primary key
uid	User name as entered by user at logon
forename	First name of user
surname	Last name of user

Additional information about roles, in particular firms, services and specialties is obtained from the RBAC service, which also supplies a full list of permissions based on the user's role and what permissions have been assigned to that role.[2]

Table Definitions

User information within OpenEyes is stored in the following tables, linked on user_id;

Users Table:

Field	Type	Comments
user_id	INT UNSIGNED NOT NULL AUTO_INCREMENT	Primary Key, 4 billion
uid	VARCHAR(40) NOT NULL	uid in the external authentication database (eg LDAP)
display_name	VARCHAR(40) NOT NULL	Full name used for display in output screens, and pick lists
contact_id	INT UNSIGNED	Foreign key referencing contacts

Contacts table:

Field	Type	Comments
contact_id	INT UNSIGNED NOT NULL AUTO_INCREMENT	Primary Key, 4 billion
paskey	VARCHAR(12)	uid in the external authentication database (eg LDAP)
title	VARCHAR(8)	
first_name	VARCHAR(20) NOT NULL	
last_name	VARCHAR(40) NOT NULL	
degrees	VARCHAR(20)	
nick_name	VARCHAR(20)	
description	VARCHAR(40)	e.g. 'Vitreoretinal Fellow'

Field	Type	Comments
company	VARCHAR(40)	Will vary according to type, but could be a Hospital name or an optometry premises
address1	VARCHAR(40)	
address2	VARCHAR(40)	
city	VARCHAR(24)	
postcode	VARCHAR(8)	
country	VARCHAR(16)	
telephone	VARCHAR(24)	
fax	VARCHAR(24)	
email	VARCHAR(60)	
type	ENUM("Consultant", "GP", "Optometrist", "Specialist", "Solicitor", "Other", "Social Worker", "Health Visitor", "Other")	

References

1. OpenEyes Organisational Structure
2. OpenEyes Access Control