

Access Control in the CLICKS PPM Solution

Glenn Engstrand, Dynamical Software, Inc.

August 2008

1 Introduction

Access control comprises of the rules and logic by which it is determined whether or not a particular user can access a specific object or resource. This is extremely important for this collaborative software development project life cycle management tool because business software provides competitive advantage. You wouldn't want your competitors to be able to gain insight into your internal business practices.

This paper discusses the access control model for the CLICKS PPM solution. The key to writing successful software is to get really clear and focused on the goals that the funding organization wants the software to achieve. The problem is that those goals can get really elaborate and complex and decision makers get tired having to think about all that. So, they get overwhelmed, burn out, and just let those with less oversight take over the decision making process. That is when the project is in the most jeopardy. The CLICKS PPM solution is designed to keep the team focused without getting overwhelmed. You can learn more about CLICKS PPM by downloading the white paper at <http://www.dynamicalsoftware.com/clicksppm.pdf> with particular interest in section 5 on page 7. The last column of this feature matrix gives insight as to the access control restrictions of various objects.

Dynamical Software is committed to producing software that is powerful and remains so by evolving over time to market conditions in order to stay relevant. Its founder has demonstrated over 20 years of participation in the field of business application software development in the engineer, architect, and director roles. Dynamical Software possesses a large body of knowledge and expertise over what works and what doesn't when it comes to writing successful software. Go to <http://www.dynamicalsoftware.com> to learn more about Dynamical Software.

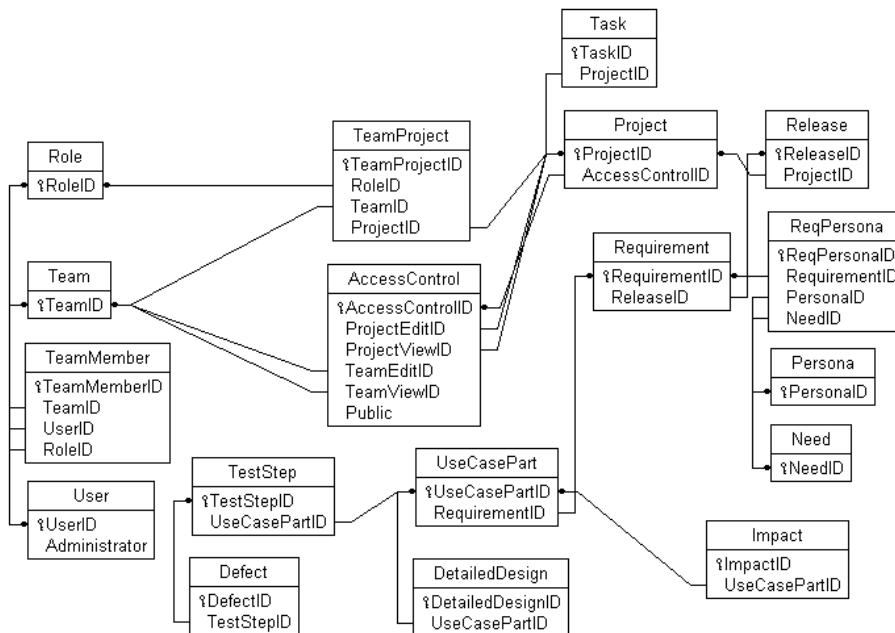
This access control model is specific to the CLICKS PPM solution. It is not based on a general model of access control such as the USDOD's 'Orange Book' specification. General approaches tend to be very complex which makes it harder for the user to make sensible choices with regards to controlling access.

2 Data Model

The portion of the data model for the CLICKS PPM solution that is relevant to access control is excerpted and presented here. Notice that many tables and fields are missing. That is because this paper is only about access control and the parts that are missing are not relevant to access control.

2.1 Project Oriented

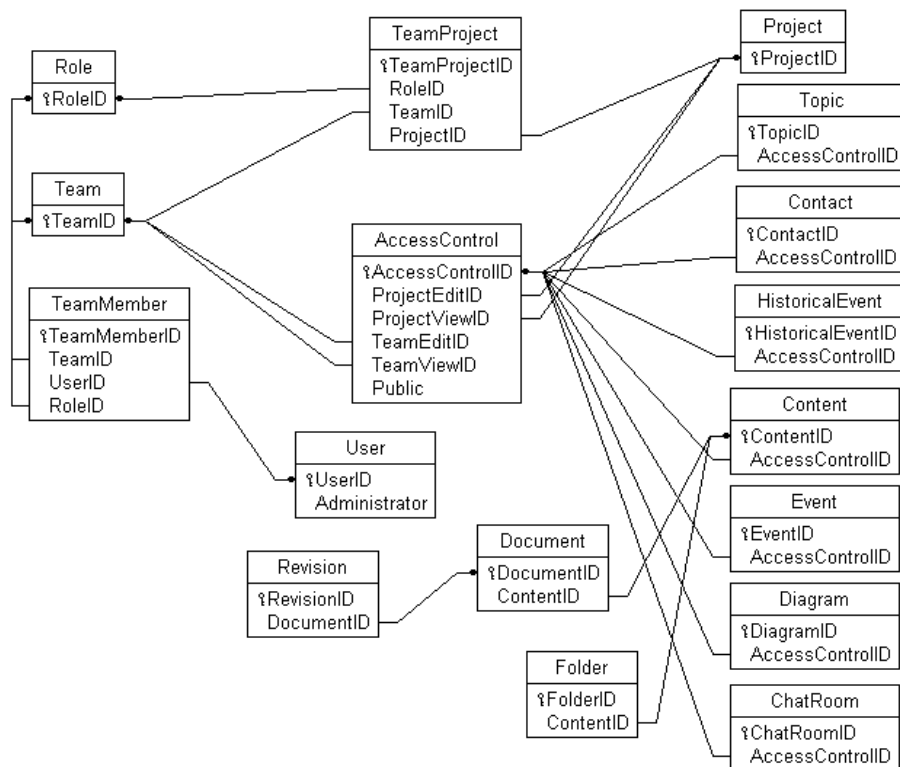
Each project comes in releases. Each release has a group of requirements, the the needs they serve, and design personas. Each use-case is an analysis of some set of requirements. Both designs and test plans are built to satisfy the use-cases. Defects are created where actual test results differ from expected results in the test plans. Tasks are also related to projects. The access control for all of these objects is determined by the access control of the parent project.



ERD for Project Oriented Access Control

2.2 Collaboration Oriented

Not everything is related to a project, however. Topics, attachments, events, diagrams, and chat are not necessarily tied to any one project so they must have their own access control. Although a user's profile is public, the contact information within that profile has its own access control. That also includes work and school history.



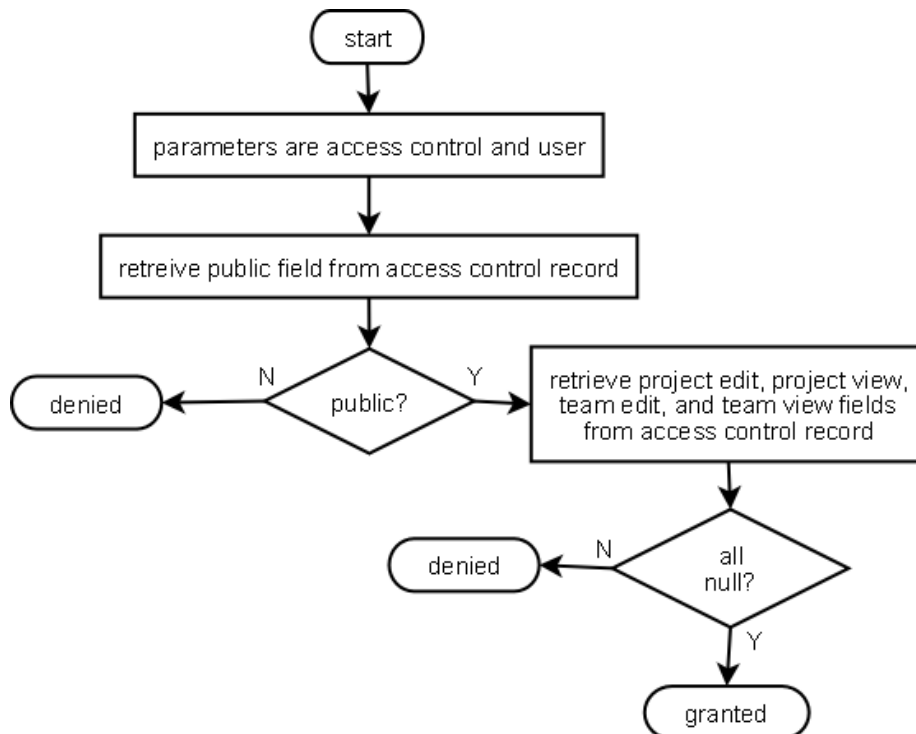
ERD for non-Project Oriented Access Control

3 Control Flow

What is presented here are flowcharts that detail the logic of access control. The administrator always has unrestricted access.

3.1 Checking for Public Access

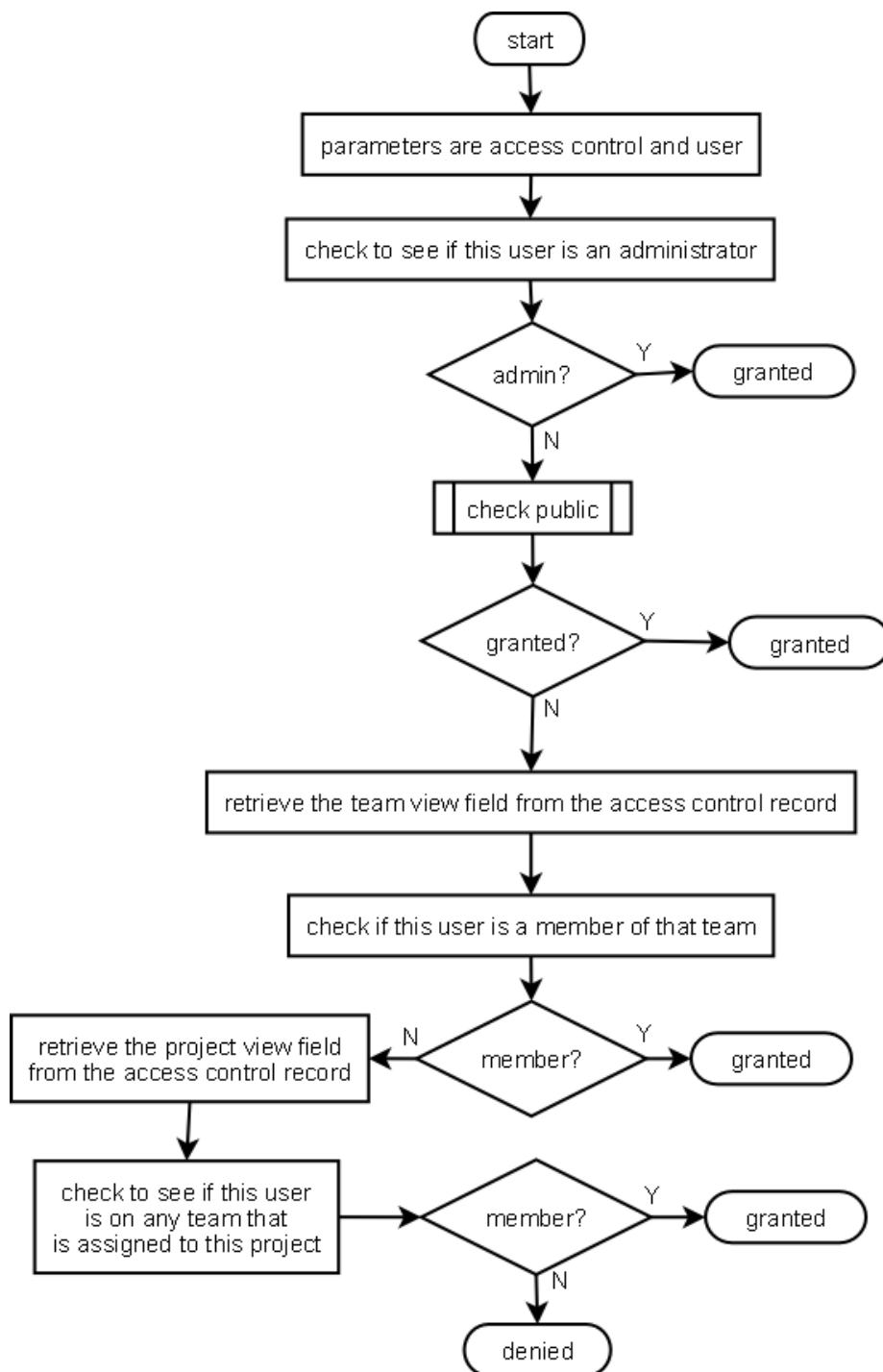
If the associated access control record is marked as public and has no associated teams or projects with edit or view privileges, then access is unrestricted.



Flowchart for Checking if Access Control is Unrestricted

3.2 Checking for View Access

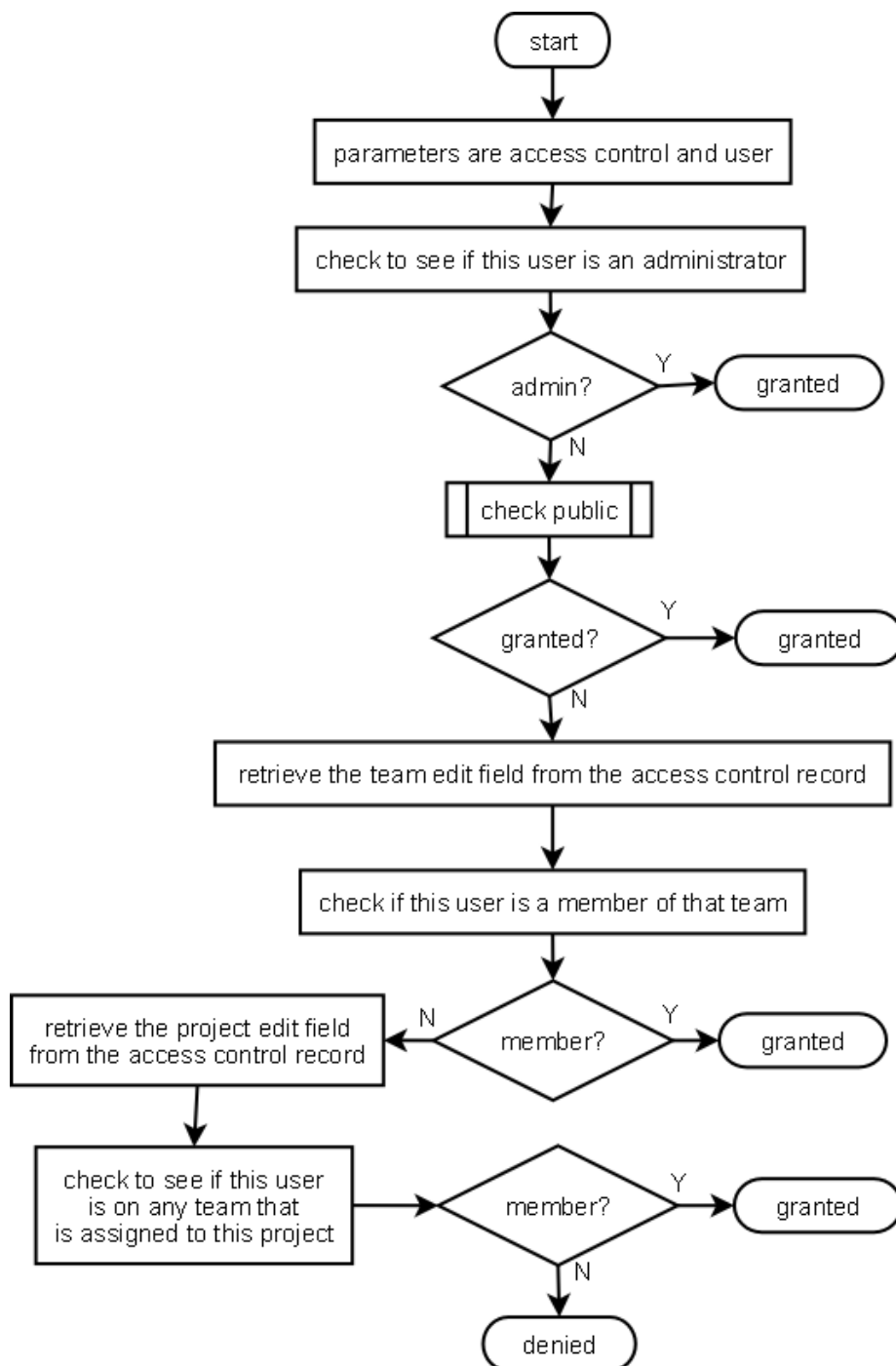
The requesting user can view the information if that user is a member of the team with view privileges or if that user is a member of any team assigned to the project with view privileges.



Flowchart for Checking View Permission

3.3 Checking for Edit Access

The requesting user can edit the information if that user is a member of the team with edit privileges or if that user is a member of any team assigned to the project with edit privileges. See the next page for the flowchart which describes this logic.



Flowchart for Checking Edit Permission

3.4 Checking for Create Access

It is the role that the user plays on a team or on a project that determines whether or not the requesting user can create an object of the desired type. See the next page for the flowchart which describes this logic.

