caBIG® Clinical Trials Suite 2.2 Centralized Suite Security Technical Architecture Guide

caBIG® Clinical Trials Suite 2.2 Centralized Suite Security Technical Architecture Guide

This document includes the following topics.

Executive Summary

Overview

The caBIG® Clinical Trials Suite (the Suite) is an enterprise clinical trials system that has been developed and continues to be enhanced primarily for use in trial sites. The Suite is comprised of following interoperable applications:

- caBIG® Central Clinical Participant Registry (C3PR)
- caBIG® Patient Study Calendar (PSC)
- caBIG® Adverse Event Reporting System (caAERS)
- caBIG® Lab Viewer (formerly CTODS Lab Viewer)
- caBIG® Clinical Connector (formerly C3D Connector)
- caBIG® Integration Hub (formerly caXchange)

These applications store and share patient's information which requires access control. Most of these applications have two interfaces, a web front end interface via which the user interacts with them or a back end grid service interface. A proper security mechanism needs to be enforced at both these interfaces in order to enforce a singular access control on either of these interfaces.

Secondly, since all these Suite applications have to work in tandem, a Suite level user should be granted same level of access control across all the applications. These access privilege and rights must be granted at the Suite level versus having to configure them individually in each application.

As a result of these requirements, the Suite has adopted centralized security architecture. A first step towards this was centralizing Authentication for all the Suite applications. This was achieved by integration of caGrid's Web Single Sign On (WebSSO) into each of the application. WebSSO allows users to sign in once using their common Suite-level credentials and then access all the applications as well as services in the Suite without requiring re-login.

As part of its 2.2 release, Suite is adopting a centralized authorization architecture which allows user's Authorization policy to be provisioned singly within a central CSM store. All the applications in the Suite and their grid services will now look up against this central Common Security Module (CSM) to obtain a user's access privilege.

Scope of the Document

The intent of this document is to describe how centralized authorization architecture is achieved in the Suite using CSM. It highlights the current authorization mechanism employed by each application. It also depicts the changes that the applications will have to make in order to access the centralized CSM store. It also provides a future view as to how the Suite can leverage an Enterprise Level Authorization Service in future which can map to the centralized CSM store.

> **Note**
> This document does not cover the business architecture details of role harmonization across the Suite applications, nor does it discuss the usage of these common roles within each application. See the caBIG® Clinical Trials Suite 2.2 Administration Guide for more information.

Business Requirements

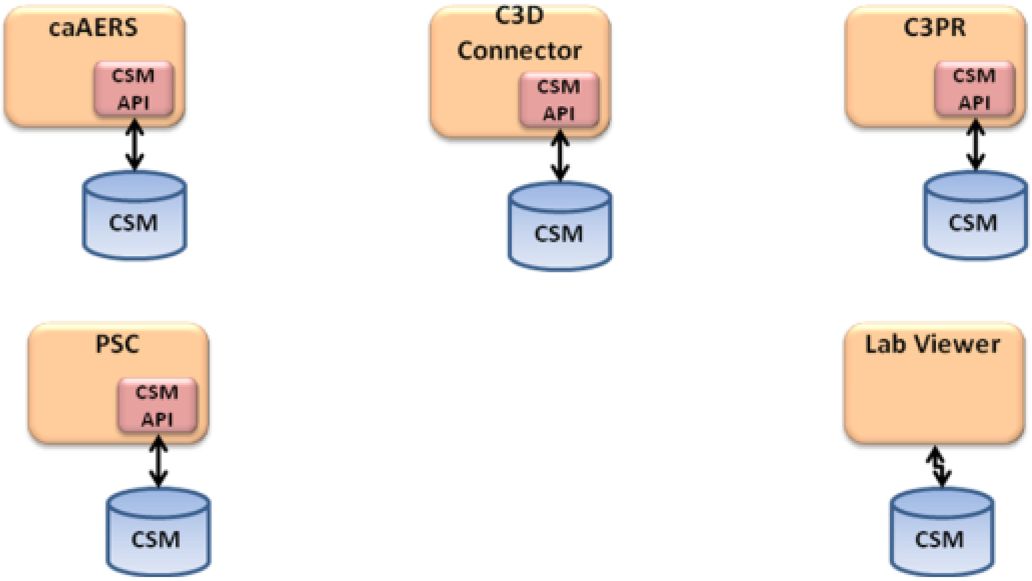
Most of the components within the Suite work in a cohesive manner to provide a single user experience. Similarly provisioning and enforcement of access privileges should also be performed in more cohesive way within the Suite. Following are some of the high-level business requirements, which such central authorization architecture must satisfy:

1. Single Authorization Source:
    a. User must be provisioned only once within the Suite for authorization purpose
    b. All the application must be able to leverage this single authorization policy provisioned at the Suite level
    c. Both the grid service interface and web front-end of the given application must enforce similar access controls
    d. In case of interoperability scenarios between applications, both the transmitting application and the receiving application must enforce similar access controls
2. Single Authorization Scheme:
    a. A unified authorization scheme with consistent user's role names across various applications within the Suite
    b. User's role must be harmonized across applications so as to ensure that a role has similar access privileges across the applications. This harmonization should be done at two levels:
        i. Privilege level: To ensure that the roles have similar privileges across all the applications
        ii. Scope level: To ensure that these privileges are applied at similar scope (study, site etc) across all the applications

Previous caBIG® Clinical Trials Suite Authorization Architecture

The following sections describe the authorization architecture which was employed by the Suite until version 2.1.

Application Level Authorization

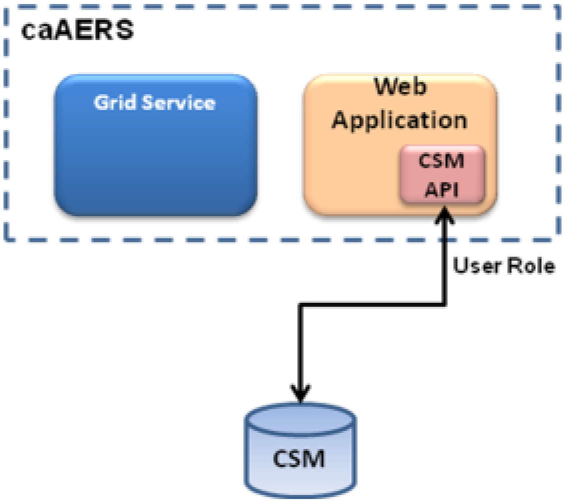


As shown in the diagram above, each application within the Suite employed local CSM for the purpose of authorization. Each application has a local CSM schema which is used to house local authorization policy. This CSM schema is access via the CSM APIs.

A single UPT instance (at the Suite level) was used to access these separate CSM schemas for the purpose of user's access control provisioning. This means that for a single Suite-level user, you will need to provision their authorization policy by logging into each application separately. This means that the user needs to be provisioned five times within the Suite in order to set their authorization policy across all the applications within the Suite.

Since all applications used their own logical authorization schemes to provision access control to the user, there was no harmonized way in which users were granted common access privileges across all applications. For example, there was no harmonization ensuring that a Study Registrar would have the same set of privileges in C3PR and caAERS.
In addition, Lab Viewer didn't access CSM using the standard CSM APIs. It had written direct SQL statements to access the CSM authorization schema. This meant that any changes to the CSM schema (as a result of a Suite-level CSM version upgrade) would require code as well as logic modifications within the Lab Viewer application.

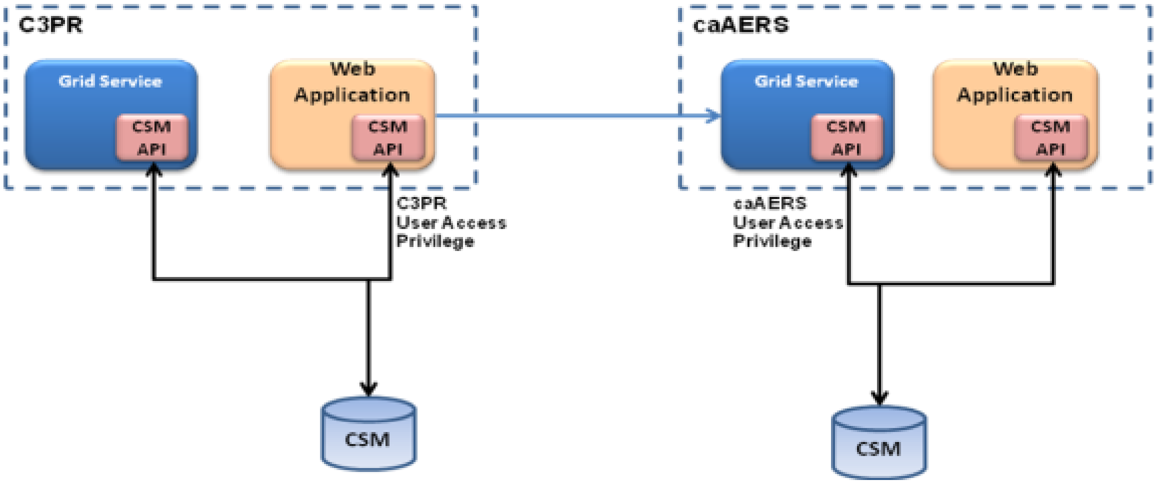
Grid Service Level Authorization



Most applications in the Suite also provide grid service interfaces for interoperability with the other applications. These grid service interfaces are used to accept messages from other application; for example, C3PR sends Registration Message to PSC, caAERS, and C3D.

caAERS (for e.g.) by itself has a registration capability in its front end UI that allows users to create and register a subject within a study. It enforces access control to allow only valid users to be able to register subjects to a study. However such enforcement is not always at the grid service level within the Suite.

This is would allow a user who does not have appropriate access privileges within the application to transmit messages and cause data modifications.



Also, in cases where the back end grid services enforced authorization, there was a harmonization issues. Since there was no centralized user's access policy between the transmitting application and the receiving application, the user has to be provisioned into both the application with same access privileges.

Cons of the Previous Authorization Architecture

The following are the cons for the authorization architecture employed by Suite v2.1 and earlier:

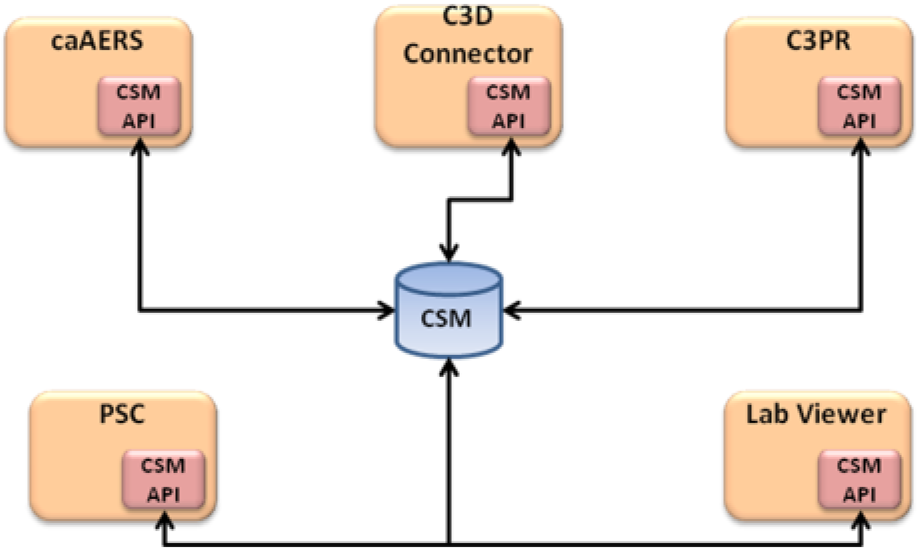
1. Multiple Authorization Policies stored locally within the application required the user to be provisioned into each of them separately.
2. Multiple Authorization Policies can lead to un-harmonized access privileges for a user across applications. E.g. A registrar can register subjects in C3PR but cannot do the same in caAERS

3. The back end grid interface to the application didn't enforce same access check as the front end web application
4. For interoperability scenarios, there was no harmonized checking of access privilege to ensure that the user transmitting the message has rights to cause that business operation on both the transmitting and receiving application.

caBIG® Clinical Trials Suite Centralized Authorization Architecture

The following sections provide the details about the new centralized authorization architecture employed using central CSM at the Suite level. For the Suite v2.2 release, CSM v4.2 has been used for the purpose of provisioning and enforcing centralized authorization scheme.

Single Authorization Source

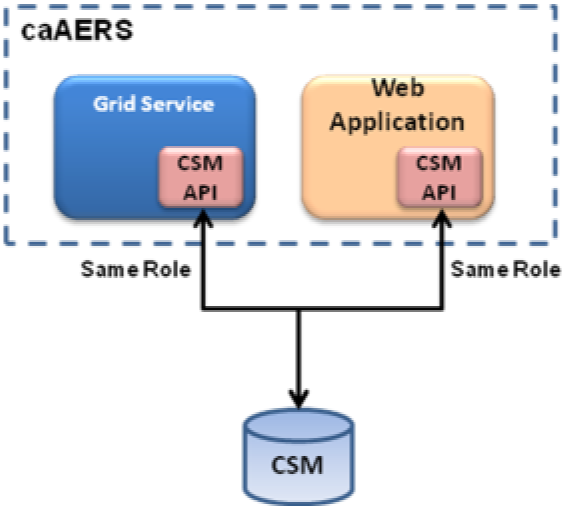


As part of new Suite v2.2 centralized authorization architecture, each application within the Suite will no longer employ local CSM for the purpose of authorization. There is a single CSM schema located centrally which is used to house authorization policies at the Suite level. Each of the Suite applications will access this central CSM schema via the same CSM APIs. The APIs are now configured to point to the central CSM schema instead of local CSM schema.
CSM also has the concept of an "application," which scopes user access, groups, protection elements, etc. Since we want all the applications to authorize users via the same roles, we will use a single CSM "application" for the Suite.

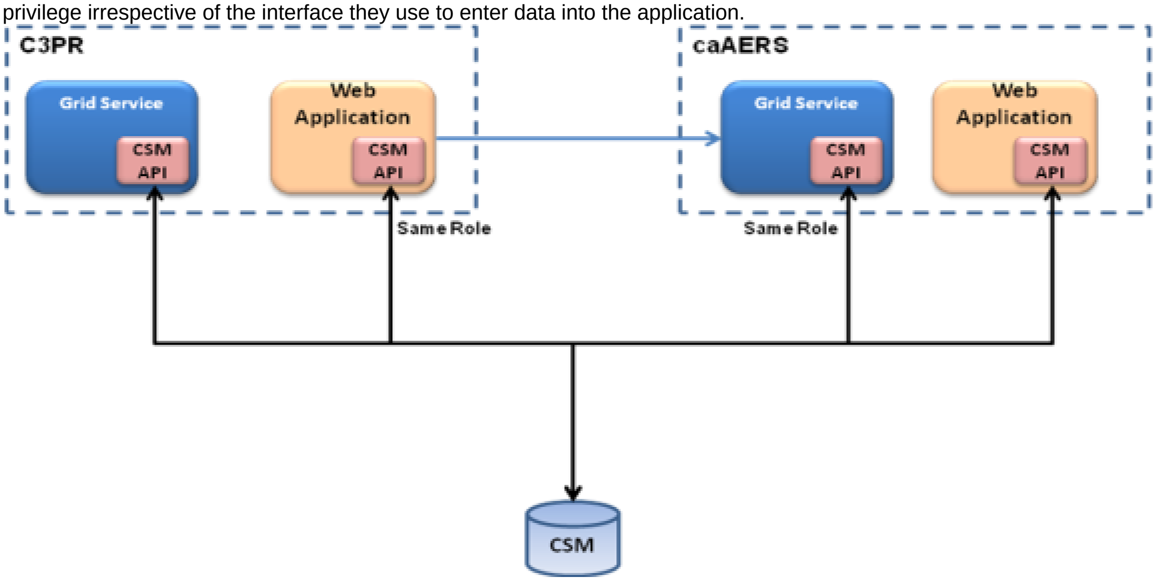
A single UPT instance (at the Suite level) will still be used to access the central CSM schemas for the purpose of user's access control provisioning. As there is only a single Suite level policy for the user, you will need to provision their authorization policy by logging into the central Suite-level application only. This means that the user doesn't need to be provisioned five separate times within the Suite in order to set their authorization policy across all the applications within the Suite.

As part of the new architecture, Lab Viewer application is modified to leverage the same CSM APIs as all other applications to access the common central CSM schema. This will decouple Lab Viewer from internal CSM schema changes, if any, in the future.

Grid Service Level Authorization



Grid service interfaces has been upgraded to leverage the central CSM authorization schema which is utilized by the front end UI as well. These grid service interfaces now enforce the same access control as the front end application. This ensures that users are granted same access privilege irrespective of the interface they use to enter data into the application.



Now since the roles have been harmonization across the applications, both the transmitting and the receiving application checks if the user has the same role. This ensures that same access privileges are enforced for transmission of messages across applications for interoperability scenarios.

Single Authorization Scheme

Role based security is used to provide a single authorization scheme across all the applications within the Suite. Business analysts did an initial analysis of the applications in the Suite and proposed a set of common roles. The Suite development team then used these roles to come up with the final list of unified roles across the applications.

Unified Roles

Based on the roles provided by the business analysts, the Suite teams have constituted a common set of harmonized roles that can be provisioned to the user at the Suite level. Each of the Suite application honors a subset of these roles thereby allowing the user appropriate access privileges within themselves. Since roles are provisioned centrally at the Suite level to the user, he obtains same set of privileges across all the applications. For example, if the user is granted common roles such as Study Registrar, he will have same set of privileges between Suite applications, namely C3PR and caAERS.

Also since the roles are provisioned centrally, the onus of ensuring what each of these roles can do lies with individual applications within the Suite. This way each application still controls the granular access control for each of the roles.

This approach required the following steps:

- Aligning the roles for the applications into a single unified set - This set is a superset of all the individual application's roles harmonized and merged
- Mapping the applications' current behaviors into this set of roles – Since the roles are harmonized, they need mapped back to individual functionality within the application

- Updating the applications to use a shared store for authorization information – Applications are modified to utilize this role information by accessing the single authorization source
- Updating the applications' authorization decisions to use the new roles – each application will have the onus of mapping the roles to the actual functions on which the user has access privileges.

Users are granted these roles in context of a particular study or at a site level. Based on these, these roles are scoped as follows:

- **Site Scoped**: These roles provide access privileges to particular sites only. Users with these roles can access the related site level functions for the granted sites only.
- **Study Scoped**: These roles provide access privileges to particular studies only. Users with these roles can access the related study level functions for the granted studies only.
- **All Sites Scoped**: These roles provide access privileges to all the sites. Users with these roles can access the related site level functions for all the sites.
- **All Studies Scoped**: These roles provide access privileges to all the studies. Users with these roles can access the related study level functions for all the studies.

These harmonized roles and their access privileges within each applications is defined on the following wiki page:
https://wiki.nci.nih.gov/display/Suite/Unified+Security+-+Roles

Provisioning of the Single Authorization Scheme

The Centralized CSM Schema is used for the purpose of housing the central authorization scheme across the Suite as shown below

1. A single Suite-level application "CTMS_SUITE" is created that houses the entire authorization scheme for the Suite. All individual Suite applications will access this common CSM application for the purpose of authorization
2. Harmonized roles are provisioned as Protection Group within this application. Since the list of roles is pre-defined and set, they are added to the CSM Schema as part of the installation seed data
3. A default CSM Role is created as part of the seed data. This Roles as a single associated privilege (This is just a placeholder entry as it is not really used in enforcing the Role based Scheme)
4. Studies and Sites on which the roles will have access to are stored as Protection Elements
    a. By default, Protection Elements for All Sites and All Studies are created
    b. At runtime, as new sites and studies are created, they are added to the CSM Schema as Protection Elements and associated with the appropriate roles. This is performed by C3PR as it is source of truth for such information.
5. As new users are added to the system at run time, they are granted access to the Protection Group and thereby the Roles. (Default Role is also assigned to satisfy CSM's Schema requirements)

Enforcement of Single Authorization Scheme

The Suite Common Library has been enhanced to provide wrapper on top of CSM APIs to aid Suite applications in incorporating and enforcing the single authorization scheme. The Suite Common Library now provides the following authorization features:

1. Improves performance for accessing the underlying CSM Schema to retrieve user's protection groups and roles by eliminating recursive self reference to the CSM's Protection Group table (it was not being used by the Suite and causing performance issues)
2. Provides an enumerated list of all the harmonized roles which the applications can use for the roles of their interests. This ensured consistency and accuracy between various application as to how these roles are named and accessed
3. Provides Helper Classes to be able to access the central authorization scheme stored at the central CSM installation
4. Provides functionality to check is the user has been assigned any of the harmonized roles or not. It also aids in determining the scope for these roles (All Sites, All Studies, Site, and Study).
5. If the Role is Site or Study Scoped it provides capabilities to determine if the user has access over that particular site or study by checking them within the list of provisioned sites or studies for that particular role

Following is a sample code snippet that shows how the Suite Common Library can be used to enforce a Single Authorization Scheme.

```
Map<SuiteRole, SuiteRoleMembership> userRoleMemberships =
getAuthorizationHelper().getUserRoleMemberships(username);
SuiteRole labLoaderRole = SuiteRole.LAB_DATA_USER;
if (userRoleMemberships.containsKey(labLoaderRole))
{
 if (labLoaderRole.isScoped())
 {
  SuiteRoleMembership userRoleMembership = userRoleMemberships.get(labLoaderRole);

  if (labLoaderRole.isStudyScoped())
  {
   HL7v3CtLabUnMarshaller unMarshaller = new HL7v3CtLabUnMarshaller();
   String studyId = unMarshaller.getStudyId(xml);
   if (studyId == null)
   {
    throw new SuiteAuthorizationAccessException("Role %s is study scoped - study identifier is null",
labLoaderRole.getDisplayName());
   }

   // if the user has permission to access specific studies (not all studies), then verify the study
if (!userRoleMembership.isAllStudies() && !userRoleMembership.getStudyIdentifiers().contains(studyId))
   {
    throw new SuiteAuthorizationAccessException("Username %s is not authorized for study %s",
username, studyId);
   }
  }

  if (labLoaderRole.isSiteScoped())
  {
   HL7v3CtLabUnMarshaller unMarshaller = new HL7v3CtLabUnMarshaller();
   String siteNciInstituteCode = unMarshaller.getSiteNciInstituteCode(xml);
   if (siteNciInstituteCode == null)
   {
    throw new SuiteAuthorizationAccessException("Role %s is site scoped - site NCI institute code is
null", labLoaderRole.getDisplayName());
   }

   // if the user has permission to access specific sites (not all sites), then verify the sites
if (!userRoleMembership.isAllSites() &&
!userRoleMembership.getSiteIdentifiers().contains(siteNciInstituteCode))
   {
    throw new SuiteAuthorizationAccessException("Username %s is not authorized for site %s", username,
siteNciInstituteCode);
   }
  }
 }
}
```

Pros of the Centralized Authorization Architecture

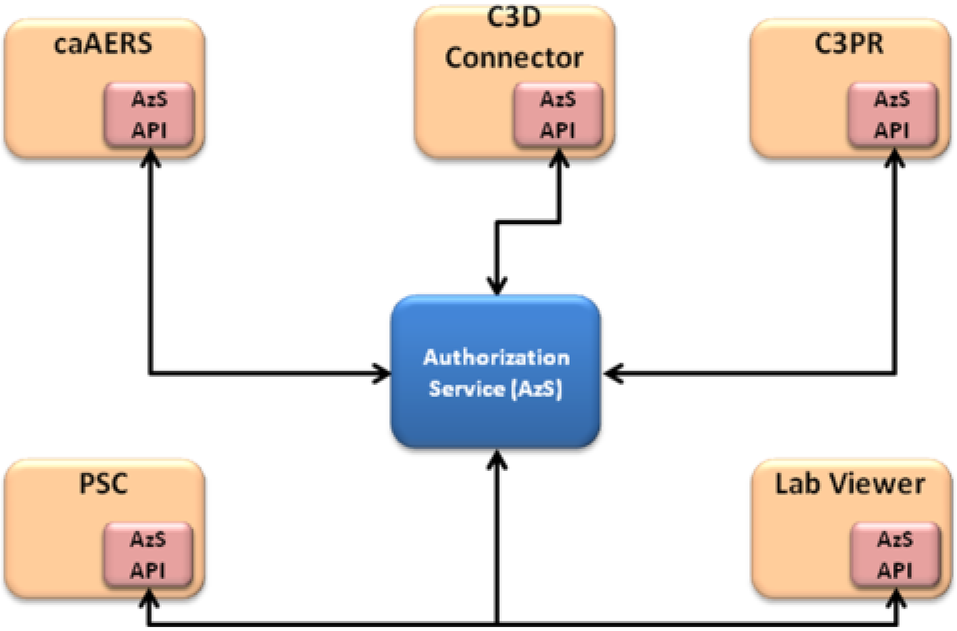
Following are the cons for the Old Authorization Architecture employed by the Suite v2.1 and earlier:

1. Single Suite-level Authorization Policy requires the user to be provisioned only once.
2. Due to provision of harmonized roles at the Suite level, access privilege for a user across applications is consistent. For example, a registrar can register subjects in C3PR as well as caAERS.
3. The back end grid interface to the application are modified to enforce the same access check as the front end web application.
4. For interoperability scenarios, harmonized checking of access privilege ensures that the user transmitting the message has rights to cause that business operation on both the transmitting and receiving application.

Future caBIG® Clinical Trials Suite Authorization Architecture

The following section highlights how the current centralized Suite authorization architecture can be enhance in future to leverage NCI's Authorization Service.

Leveraging NCI's Enterprise Authorization Service



As part of Suite v2.2, centralized security is already implemented using CSM. This paves the path forward for easy migration to a NCI's Enterprise Authorization Service when developed in the future. CSM implementation of the Authorization Service can be used to encompass the existing central CSM schema and expose it as an Enterprise Authorization Service. Individual applications within the Suite will be enhanced to use the Authorization Service APIs instead of the regular CSM APIs in order to interact with the Authorization Service. This architecture is Enterprise Compliance and Conformance Framework (ECCF) compliant.