

CMED - Technical Design Document

Version	Date	Author(s)	Description of Change
1.0	Jan 23, 2012	Manuj Aggarwal	Created
1.1	Feb 9, 2012	Bob Walker	LMS and LOR first draft
1.2	Feb 15, 2012	Manuj Aggarwal	Updated after the first internal review
1.3	Feb 15, 2012	Bob Walker	LMS and LOR second draft

CONTENTS

Introduction....7
Objectives....7
Scope....7
Document Structure....7
References....7
System Overview....9
System Components....10
Core LMS....10
Security....10
Course Boundary....11
CMED Portal....11
Portal Modules....11
Personalization....11
Administration....11
Security....11
Roles....11
LMS....11
LMS Content Organization....11
Linking to LOR Content....12
Content Search....12
Administration....12
Security....12
Roles....12
LOR....12
LOR Content Organization....12
Metadata....12
Content Search....12
Administration....12
Security....12
Roles....12
Security....13
Authentication....13
Authorization....13

Table 1 Document Structure.....7
Table 2 List Of References.....8

Figure 1 Conceptual CMED System Structure.....7
Figure 2 System Overview.....9
Figure 3 UBC IT Shibboleth Infrastructure.....13

INTRODUCTION

The CMED eco-system will comprise of multiple applications sourced from multiple vendors working with each other and providing a seamless experience to the end user. There will be myriad of use cases and requirements which will be executed by different type of users. Most of the required functionality is already available out-of-box int the respective CMED applications. But some customization, integration and configuration will be required to make these components work as per specific requirements of the CMED project. This document provides detailed technical design specifications of such customization and configuration. All integrations will be documented in separate integration documents.

OBJECTIVES

The objectives of this document is list all the required technical changes required for each of the CMED component to satistfy the CMED specific requirements. These technical changes could be customization via custom development or configuration of the system components. This document provide detailed design specifications as to how these technical changes will be implemented. It also includes details around deployment and maintenance of these technical changes.

The target audiences of this document is achitects, designers, developers or any other technical group who is involved in development, maintenance or operation of CMED systems; OR wants to integrate with CMED systems.

SCOPE

The conceptual structure envisaged for CMED solution is as follows:

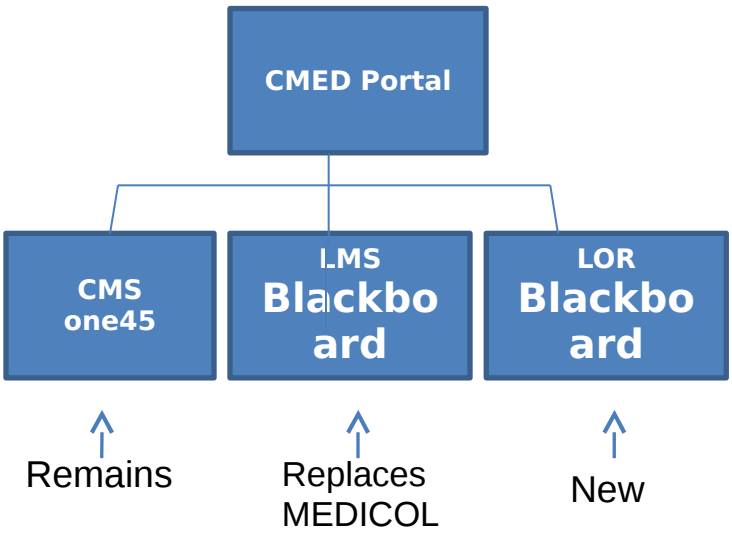


Figure 1 Conceptual CMED System Structure

DOCUMENT STRUCTURE

Section	Description

Table 1 Document Structure

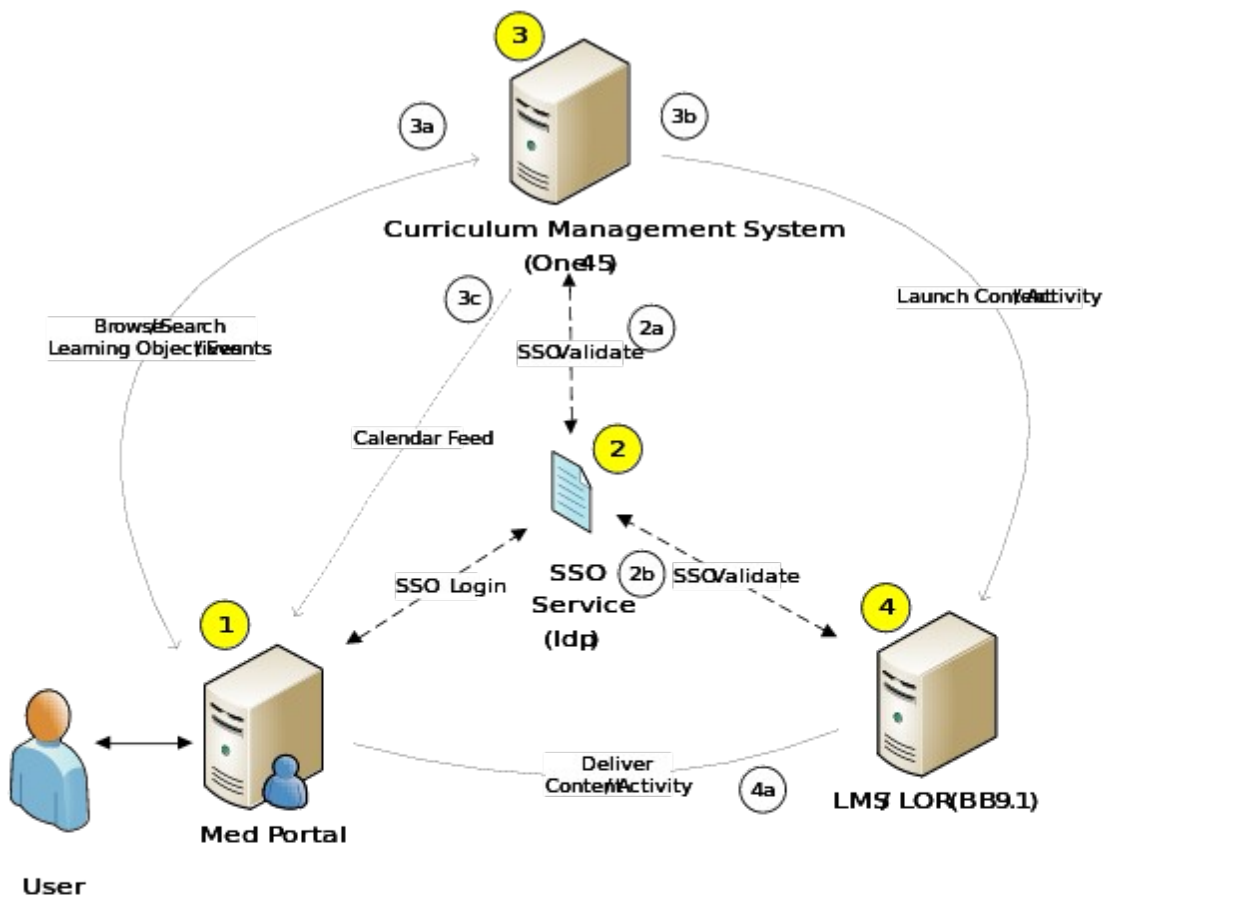
REFERENCES

Title	Description

Table 2 List Of References

SYSTEM OVERVIEW

This section describes the overall system and the internal components of the CMED application eco-system.



1. User goes to MEdPortal, a consolidated portal site for accessing teaching and learning resc
2. The portal login provides Single Sign On to various applications in the ecosystem (Shibboleth/SWI)
2a. SSO validation with One45
2b. SSO with LMS/LOR
3. User views the consolidated calendar in the portal (3a) and views the associated even details in Curriculum Management System (One45)
3a. The curriculum map can be browsed to view learning objectives and associated ev
3b. User selects a learning event and launches associated activity or content
4. The LMS delivers the learning activities and provides access to content within the LOR

Figure 2 System Overview

SYSTEM COMPONENTS

CORE LMS

SECURITY

ROLES

BlackBoard Learn provides various ways to configure role based security within the LMS system. Multiple types of roles are available depending on the type of user and security required.

These roles types are:

SYSTEM ROLES

System Roles permit administrative privileges.

System Roles are assigned in two ways:

- Attached to the user account at creation or through the Manage User page.
- Assigned to a user with a domain to create a domain administrator.

In both instances, multiple System Roles can be assigned to the user. Multiple System Roles grant the user the sum of their privileges. This makes it possible to create System Roles based on tasks and flexibly apply privileges.

INSTITUTION ROLES

Institution Roles control access to information and services. Portal features such as tabs, modules, and brands can be controlled through Institution Roles. Institution Roles are a part of the community engagement capabilities of Blackboard Learn that extend to features and functions in other sets of capabilities. The Virtual hard drive uses Institution Roles to determine file access for specific user groups. Institution Roles make Blackboard Learn a role-based system where tools and content are defined for distinct groups of one, few, or many users.

COURSE ROLES

Course Roles control access to the content and tools within a Course. Each user is assigned a role for each Course (or Organization) in which they participate. For example, a User with a role of Teaching Assistant in one Course can have a role of Student in another Course.

Instructors may use these roles to delegate some of the responsibility for maintaining the Course.

COURSE BOUNDARY

Most of the data maintained with BB Learn LMS is bound within course boundaries. There are some features like communities, portal framework etc. which can store and has access to global data for a user. But other than these feature – all content, user enrollments, grades etc. reside within a course boundary. For instance, a user enrolled in one course may not be able to send a message via BB messaging system to a user enrolled in another course.

This may have implication on the setup of course layout within FoM.

If we need a group of users to interact with other or collaborate on a piece of content – they may need to be enrolled in single BB course or alternatively should be enrolled in a common community.

CMED PORTAL

PORTAL MODULES

PERSONALIZATION

ADMINISTRATION

SECURITY

ROLES

LMS CONTENT ORGANIZATION

The Technical Design team has determined that the course configuration for the new MEDICOL in Blackboard 9 will be one LMS course per curricular year. This will be deployed as

an LMS course for each of Year 1 through Year 4 and optionally other courses to represent other curricular groups.

As well, a review of Selective/Adaptive release rules will take place to achieve administrative gains in managing groups within courses.

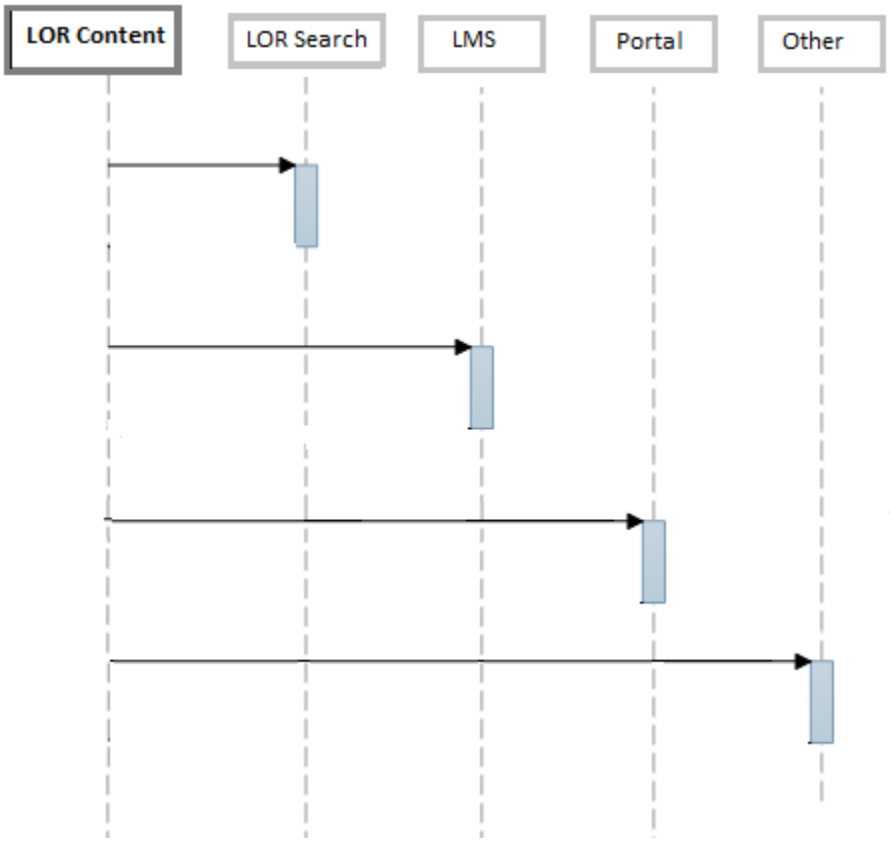
During the migration phase, existing MEDICOL content will be reviewed with the intent of moving informational or non-curricular material from LMS courses into the portal itself.

In choosing a course configuration for MEDICOL, three options were studied. The resulting decision was based on an anlaysis that took into account past history, CMED de-centralization priorities, and a balance between control, flexibility, and risk. See Appendix A for full details as to the analysis process.

LINKING TO LOR CONTENT

Much of the learning materials that are presented in the LMS are documents, such as html and pdf files. These documents will be stored in the Institution area of the LOR.

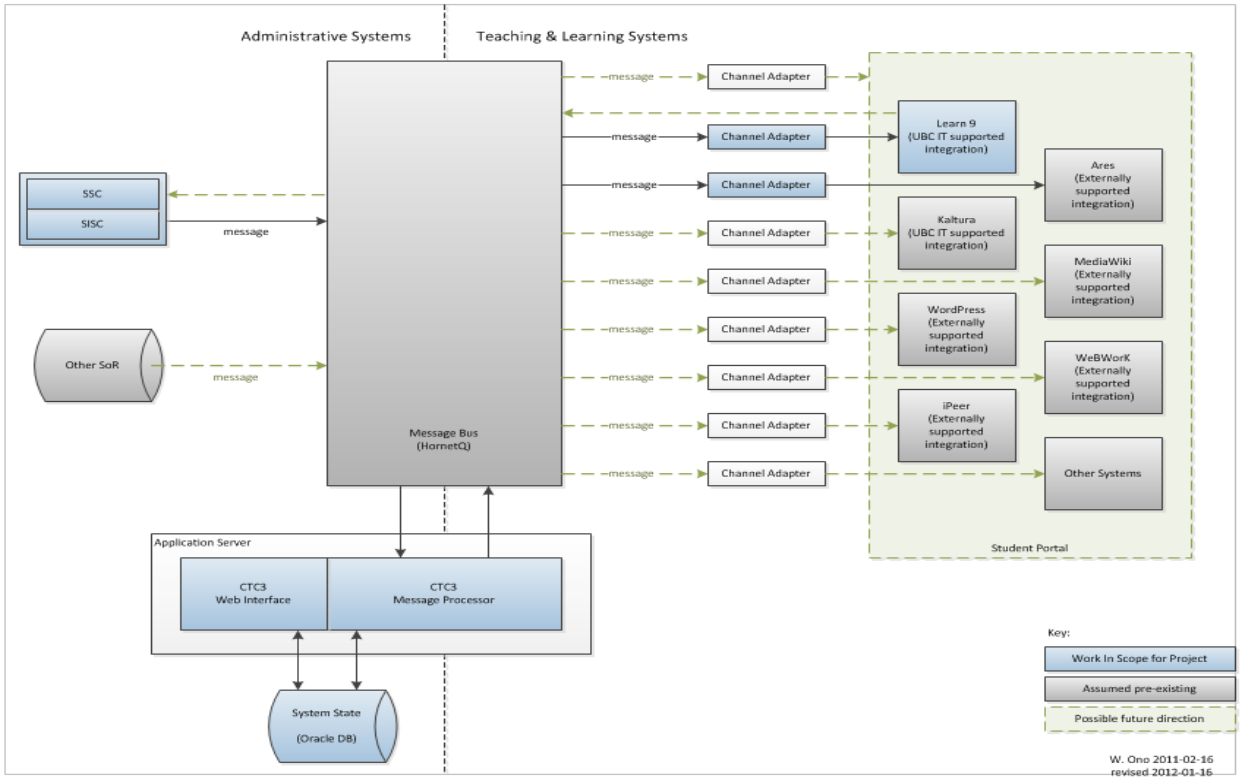
Learning Modules and other LMS objects will reference content in the LOR. Content from the LOR can also be referenced directly in the portal, through the LOR search tool, eventually externally.



CONTENT SEARCH

** Brandon **

ADMINISTRATION



Interface: CTC3 and Blackboard9. From UBC IT.

Administrative Management of users:
Blackboard LMS courses will be linked to CTC3 for student course enrollments. One connection per LMS course is required. SIS sections ORNT 400-01 and ORNT 400-02 (Undergraduate Medicine orientation courses) are re-linked every year for the current academic semester. This results in the addition of new MEDICOL 1st year students to the LMS courses.

Non-student users will be added to the Blackboard MEDICOL courses by hand using CTC3. Users will be added with course roles via CTC3 based on their assigned capabilities in that course. Users course roles can be different in different courses.

Course groups will be managed manually in all LMS courses. Course groups will need to be duplicated in all courses. Groups are used for protection of content rules.

Group Name	Membership

year1	Year 1 students
year2	Year 2 students
year3	Year 3 students
year4	Year 4 students
Alumni	Past students for one year only ??
Employees	Instructors, staff

Course Developers (course role: instructor) will not need to be a member of a course group.

Note that due to the Open Curriculum policy, all students have access to all courses. This means that Year 1 students will be members of the Year 4 course, however they will be indentified within that course in a group called Year 1. Thus each course: Year1 through Year4 will all have Year 1 through Year 4 course groups.

As part of the Summer Refresh process, students will be moved to the next year group, or into the alumni group, in all courses. This is a manual process. New students will be added to the courses by CTC3 and to the year1 group manually. Past students who are no longer in the program for N years will be removed from all courses.

Management of LMS Content:
Users in the *Instructor* course role will be the Course Designers who manage the content of the LMS courses.
Designated MedIT staff are Course Designers in all courses.

SECURITY

Each curriculum block has Course Designers to manage content within that block. Program Area administrators are responsible for assigning Course Designers for their area.

Designated program block Course Designers will be reviewed every summer as part of the Summer Refresh.

Program block Course Designers will have access to other blocks within their course. (Example prin manager will have access to fergu LMS content). Course designers are excpected to be responsible and manage their designated content only.

LMS Course	Block/Area	Course Designer
Year 1	prin, hdi, cv, pulm, fergu	Program Area admininstrators
Year 2	gi, bl, mlk, endo, bb, repro, ngd	Program Area admininstrators
Year 3	??	
Year 4	??	

Some course content is protected from certain groups of users or at certain times. See the Protection Of Content document for details of what content is protected.

Course Designers are responsible for maintaining the Protection of Content rules for the subject matter in their block.

ROLES

There are two types of roles or groupings in the LMS: course roles and course groups.

Course roles: assigned to a user when added to the course with CTC3.

Blackboard 9 course role	Capabilities
Student	Browse courses
Advisor	Browse courses with more access
Instructor	Manage LMS content
Teaching Assistant ?? not sure	Browse courses and manage grades

Course groups: are used to enforce Protection of Content rules within a course. See above under Administration(TODO: should we repeat the above table, move it here, or remove this section???)

INTEGRATIONS

FMIS

Videos that are part of the MEDICOL curriculum are located on a separate media server. These videos are invoked from an LMS course through a process that checks authenticity of the request, and records information about the user and video being viewed.

If the user has not logged into the special MEDICOL login, they will be presented with the standard CWL login dialogue.

Videos are created by the video creation team, and are uploaded to the FMIS video server. The video is entered into the MedIT video database and assigned a reference number. This reference number is used when creating a url to invoke the playing of the video.

Example URL: `http://www.medicol.med.ubc.ca/requestVidoeo.aspx?VideoID=NNN`

LOR

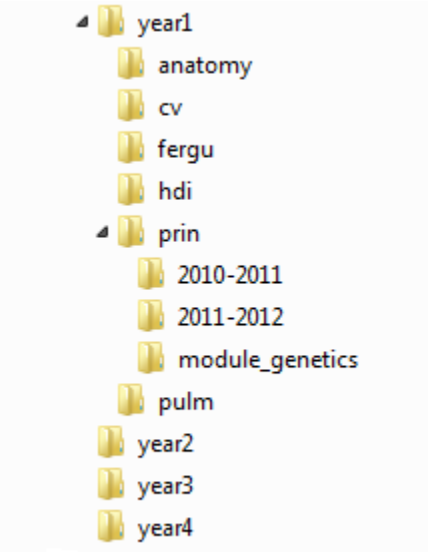
LOR CONTENT ORGANIZATION

The Learning Object Repository resides as part of the Blackboard application suite. It provides the FoM with a means of storing learning content that can be displayed in multiple ways.

All content for CMED will be stored in the Institution area of the LOR. The LOR will be primarily structured by year, then by curricular block using the MedIT naming convention acronym for the curricular block (see Appendix B) .

Within each program block folder, content that is sensitive to the academic year (example: weekly objectives) will be in folder named for that year. Stable, ongoing content, will be either directly under the program directory or in folders labled accordingly to topic or current practice on Vista.

Content that is global to CMED as a whole will be stored outside of the year structure in folders according to topic and current practice.



The documents can be any of the following: html, MS Office document, image, video, pdf.

METADATA

insert Marcelina's document

CONTENT SEARCH

The Blackboard LOR can be searched and browsed.

When browsed, the view is similar to what one would see in Windows Explorer or when viewing any other hierarchical system.

Content can be searched using the search tool provided by Blackboard as part of the LOR. Search can be done by filename, content, or metadata tags. Results of a search can be a folder, which then provides access to all docments in that folder. Results are returned in a listing that gives the whole path name.

ADMINISTRATION

Program area staff will manage content they are responsible for in their areas. This will include transforming, uploading, and storing originals. These procedures will be defined in a subsequent content management workflow document. See Appendix C.

SECURITY

As the Institution area of the LOR will be the sole repository of content, permissions will be explicity granted depending on requirements.

All users will be granted read access to all content in the LOR (with some exceptions. TODO: what are these exceptions? Eg. Year4 PMP).

Permission to update content will be controlled directly in the LOR using folder permissions. Program area users will be identified that are responsible for content by curriculum block, and create/update/delete access will be granted to these users. This may be done by user or by some yet to be determined role or grouping.

ROLES

.

SECURITY

AUTHENTICATION

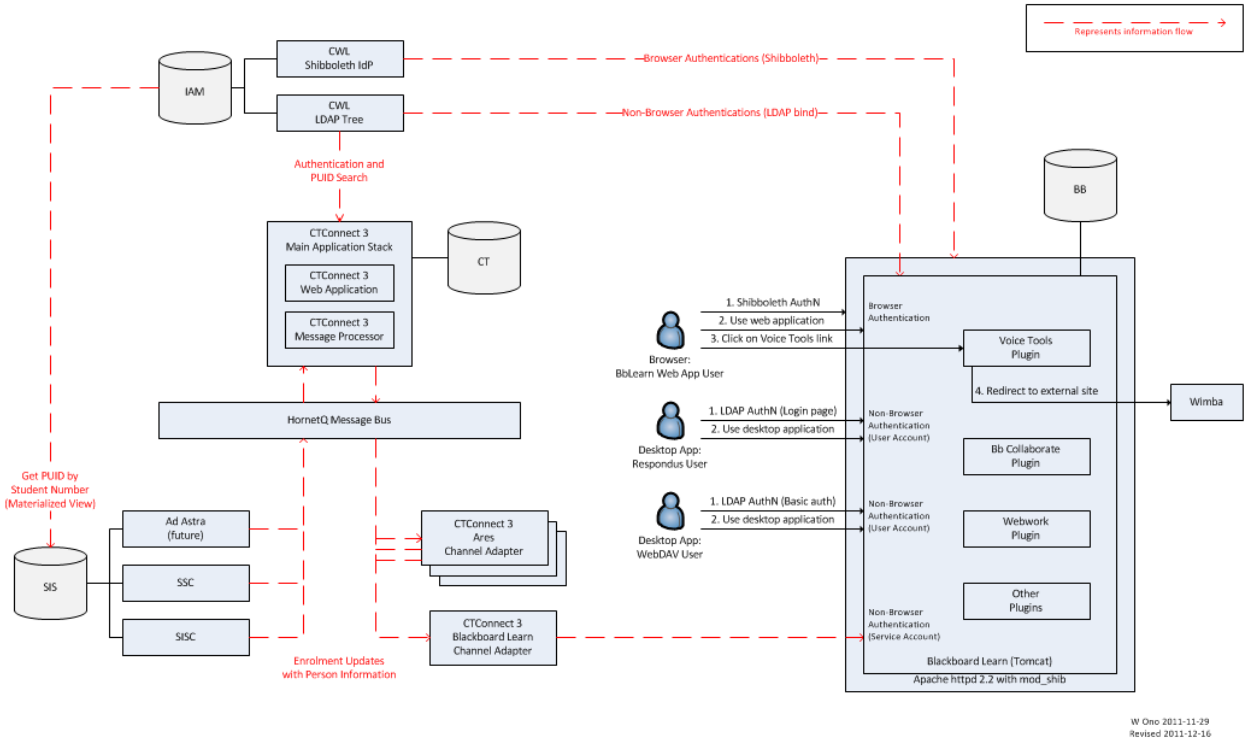


Figure 3 UBC IT Shibboleth Infrastructure

AUTHORIZATION

APPENDIX A: PROTECTION OF CONTENT - SELECTIVE/ADAPTIVE RELEASE

Selective Release in Vista, Adaptive Release in BB9.

Advisors and student year groups are constructed and maintained for the sole purpose of maintaining protection of content. This represents a significant overhead in course management and is an impediment to breaking MEDICOL up into smaller sections. It is one of the main reasons why MEDICOL in Vista is one course.

There are 4-6 items per week that are subject to protection. Typically these consist of:

- Case objectives (files stored in the LOR) - created on Wed or Thur. Installed with release time of 12 noon Friday.
- Assessments (stored in the LMS) - created any-time prior (usually about a week) and installed with release time of 12noon Friday.

A typical release criteria for a content piece consists of (example: Year 1 case objective):

- advisors, year2, year3, year4 can see the item immediately from the time it is created.
- year1 students cannot see the item until the appointed time.

This means usually there is a 1-5 day time frame where some groups can see an item and another group cannot.

Is it important that non-targeted users see this content for 1-5 days prior to when targeted students can see it? If not, protection rules could be applied globally and there is no need for student year groups and adaptive release by course groups.

Example:

- Is it important that advisors and Year 2,3,4 students see a Year 1 assessment for 3-5 days prior to Year 1 students (course designer would still be able to see it)?
- Is it important that advisors and Year 2,3,4 students see a Year 1 Case Objectives 1-2 days prior to Year 1 students (course designer would still be able to see it)?

Proposed solution:

- Remove all course year based groups.
- Assessments: This is an LMS item: create item prior to need and apply Adaptive Release globally.
- Case Objectives*: This is a LOR item: create item prior to need and make available by an operator at release time (just-in-time release).

* Also applies to other content that are files that are stored in the LOR. LOR content is not subject to BB LMS Adaptive Release rules. Students could see a content item through LOR browsing even though it is protected in the LMS. To prevent this, must either be: 1) protected in the LOR as well as the LMS, 2)stored in the LMS (and moved to LOR when released) or 3) as above, released just-in-time).

APPENDIX B: MEDICOL NAMING CONVENTION CHEAT SHEET.

Year 1: Principles of Human Biology	Prin
Year 1: Host Defenses & Infection	Hdi
Year 1: Cardiovascular	Cv
Year 1: Pulmonary	Pulm
Year 1: Fluid, Electrolytes, Renal & GU	Furgu
Year 2: Gastrointestinal	Gi
Year 2: Blood & Lymphatics	Bl
Year 2: Musculoskeletal & Locomotor	Msk
Year 2: Endocrine & Metabolism	Endo
Year 2: Integument	Integ
Year 2: Brain & Behaviour	Bb
Year 2: Reproduction	Repro
Year 2: Nutrition, Growth & Development	Ngd
Year 3: Rural FMPR Clerkship	Rural
Year 3: Anaesthesia	Anae
Year 3: Dermatology	Derm
Year 3: Emergency Medicine	Emer
Year 3: Medicine	Medi
Year 3: Obstetrics & Gynaecology	Obst
Year 3: Ophthalmology	Opth
Year 3: Orthopaedics	Orpa
Year 3: Paediatrics	Paed
Year 3: Psychiatry	Psyt
Year 3: Surgery	Surg
Year 3: Integrated Community Clerkships	Icc

APPENDIX C:

A review of the content management workflow will make sure that future de-centralized content management is in line with current practices. This will encompass discovering current practices, reviewing these practices, and developing a Content Management Workflow that is workable for program area staff.

Maintaining LOR Content:
Content typically consists of html documents, MS Office documents, and pdf documents. Content will need to be edited/created outside Blackboard and then uploaded. Upload methods are: Blackboard Content Collection upload, WebDav, BB-Drive, other ftp-like clients. BB-Drive is an included product from Blackboard that shows the LOR as a network drive on a client machine (similar to the network Drive S:). Data can be edited directly on the BB-Drive drive. LOR versioning is respected. However, LOR Metadata cannot be entered for new files using this method.

Relationship with Network S: drive:
Currently, *S:\Ed Tech\e-Learning Support\undergrad\MEDICOL_Vista* is (almost) and exact copy of the MEDICOL Vista File Manager area. Is this to continue?

Content Management Workflow:
This encompasses all the items mentioned above. There needs to be a consistent well-defined procedure for updating data in the LOR. Factors in this decision are:

- Allow for Program areas as well as MedIT to update LOR content .
- Where is the current authorized copy of a document stored? –Should the LOR be the location for the current authorized document? Currently S: drive is the default authority, but program area hard drives also have documents. Often the program area version is the authentic version.
- Versioning – Do we use the LOR versioning process for document management?
- How is the document to be updated in the LOR? Possible options:
    - LOR is authority:
        - Download using webdav, edit in client program (like Word). Upload using webdav.
        - Download using BB Content Collection tool, edit in client program. Upload using BB Content Collection upload.
        - Edit directly using BB Drive using client program. This is the option that Sauder has chosen.
    - S: drive or local hard drive is authority

- Edit on S: drive or locally with client program. Upload using webdav or Content Collection OR
- Edit on S: drive or locally with client program. Drag and drop to BB Drive

LOR content management challenges:

- Stability and maintenance of WebDav and BB Drive. There would be a wide distribution of these client applications and, if used, will be a critical part of the user workflow. Integration of applications with workstation template and help desk support would be needed.
- Operational procedure changes: working with HTML, converting MS Word to pdf and protecting, converting PowerPoint presentations.
- Management of MetaData must be done from within Blackboard. Management of content will probably be a two step process using different tools.

Recommendation: None at present. Needs more analysis.

LOR Related Business Analysis:

- LO uploading workflows
  - Determine the processes, workflows and permissions for uploading new learning objects
    - Determine permissions and controls for faculty who wish to upload own learning objects related to teaching events.
    - Determine approvals of newly uploaded learning objects (do staff need to verify LOs uploaded by staff?)
    - Determine workflows for students wishing to upload content, and the approvals and validation points required by staff and facutly.
- LO management
  - Determine workflows for reusing learning objects (when faculty wish to reuse the same presentation they used last year).
  - Determine version management (when the same faculty member or staff upload a PowerPoint with the same name (but slightly updated content).
  - Determine responsibilities for ongoing management of LO folders, workflows, folder changes, new user groups seeking access etc.
- LO tagging
  - Determine process of adding metadata

    - Align metadata with One45 mapping workflows
    - Metadata validation requirements (by whom, how rigorous)?
    - Determine tagging responsibilities
    - Determine acceptable tagging timelines (can an object be tagged 2 weeks after it is uploaded?)

- Determine the sequence of LOR functionality and workflows release cycle (work with Ranvir)
    - For example, we can start with limiting the uploading capability first to staff, and determine when it is appropriate to release this to faculty and/or students
    - We may not implement a ‘rating feature’ right away.
- Determine process of synchronizing selective release and group permissions in the LOR with other systems.