



Remote Authentication and Single Sign-on Support in Tk20



**Your complete assessment
and reporting solution**

Table of content

Introduction:.....	3
Architecture.....	3
Single Sign-on.....	5
Remote Authentication	6
Request for Information.....	8
Testing Procedure	10
Test Suite	11
Project Plan.....	12
Production Rollout procedure.....	13
Known Issues in production environment	14
Emergency Handling Procedure in Campustools Highered	15

Single Sign on & Remote Authentication Services

Introduction:

Most of the universities use Single Sign on as method of access control that enables a user to authenticate once and gain access to the resources of multiple software systems. There is also a need to maintain a single source of authentication information for all users on Campus and that multiple clients validate this information against this common repository.

Tk20 Campustools HigherEd is designed to meet these needs. The architecture lends itself to be flexible for integration with external web portal. Campustools is designed to support authentication against different authentication sources. Additionally it can also be configured to authenticate different types of users against different authentication sources on a single deployment.

Architecture:

The Tk20 Campustools HigherEd system uses an n-tier, Java 2 Enterprise Edition

Architecture, built using proven, open-source operating system and software components.

It is written in Java, and comprises of three tiers, a web tier, a middle tier, and a database

tier. All tiers function independently, and have their own interfaces for communication.

They can be physically located in the same server, or have multiple servers allocated to

each one, depending upon load and configuration.

One of the component that gets deployed as part of Tk20 installation in the application server (JBOSS) is the **Pluggable Authentication Module (PAM)**.

Pluggable Authentication module is the heart and soul of this architecture.

Different types of users exist in university environment like Student, Faculty, Co-operating teachers, program coordinators etc. In Campustools HigherEd each user is assigned a role. Additionally it is possible that some or all of such users have campus account and are required to access campus services via a web portal or that the campus maintains only one source of authentication information and all the clients that need access to authentication information need to access the central repository. It is also possible that there is a set of users that need to access Tk20 system, but their authentication information is not centrally managed by Campus.

Campustools HigherEd is designed to meet all of the above needs through configuration management. In Campustools HigherEd it is possible to specify the authentication source for each type of user. For example, it is possible to specify

that for authentication Student and faculty an external LDAP server needs to be communicated to and that all Co-operating teachers need to be authenticated against Tk20 local database. Depending upon the configuration data, PAM instantiates the implementation class and carries out remote authentication against any authentication source.

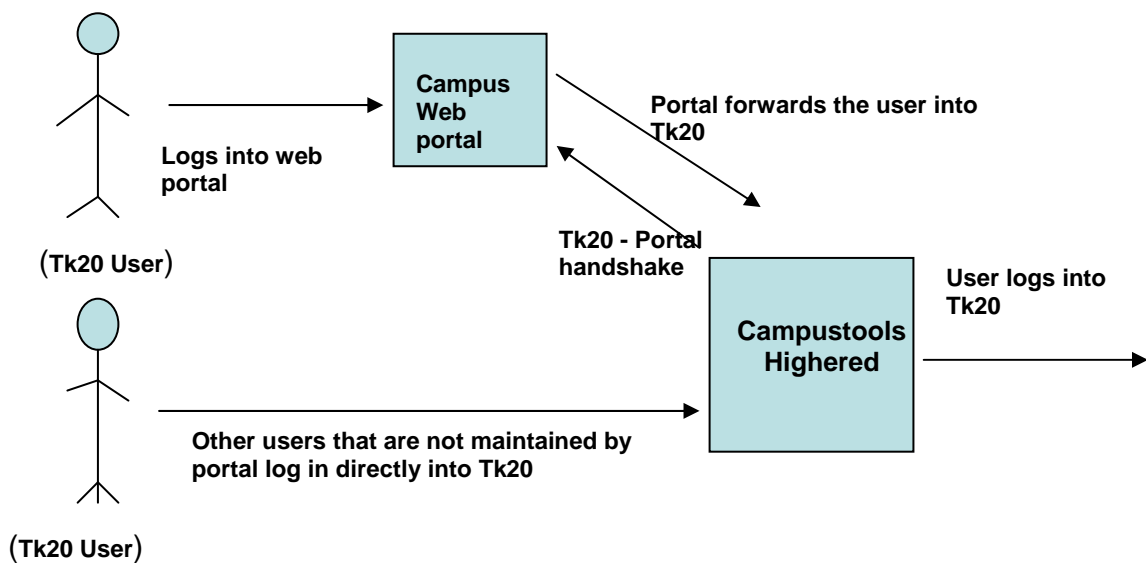
Single Sign-on

Single Sign On provides users with access to multiple environments with a single secure password. Most of the universities maintain their web portals and have the users on the campus use single authentication information to log into the portal. Once they log into the portal they can access various websites or other services such as Tk20.

In such scenario, typically once the user gets authenticated via portal, a request is forwarded to Campustools Highered. Once the software receives such request coming in from the web portal, a secure handshake with the web portal ensures that the request coming in is a legitimate request. Once the request is validated, information pertaining to the user trying to access Tk20 is also exchanged. Software ensures that the user trying to access Campustools highered is a valid Tk20 user. Once these checks are passed, user is directly brought to the home page of the Campustools Highered application. In this case, user does not see the Tk20 login page as the authentication takes place only once when the user logs into the web portal on the campus. Campustools Highered merely integrates with the web portal, ensures the proper authorization and allows the user into Campustools Highered.

Campustools highered is designed to allow access to such users that do not have access to campus portal, but do need access to Tk20. In such cases, the authentication information of such users is maintained in Tk20 database locally.

The sequence of events during this process is depicted below

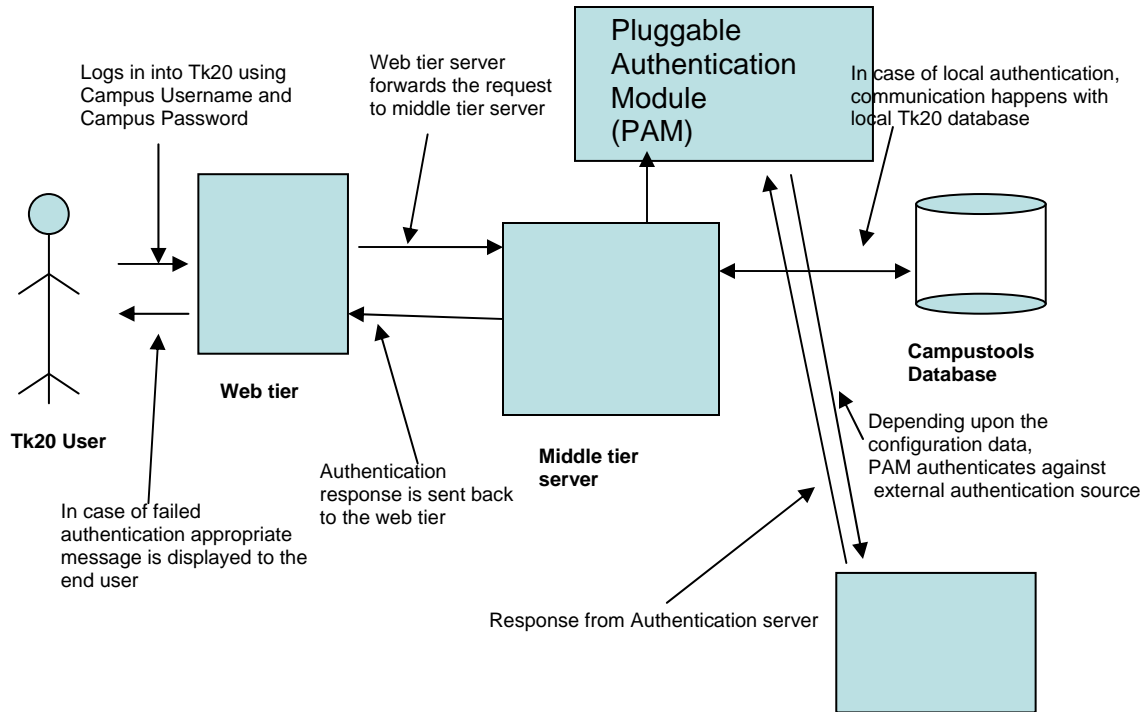


Remote Authentication

For universities that maintain the central repository of authentication information and need the clients to access this repository, Campustools highered is designed to be able to communicate with external authentication sources to look up the authentication information. A few examples of external authentication sources that Campustools Highered currently authenticates the users against include LDAP (Lightweight Directory Access Protocol) servers, Radius Server, Central Authentication Services (CAS) and Banner Authentication. The architecture is flexible to enhance this ability against any other authentication source.

During remote authentication, all the Tk20 user access the system by going to Tk20 URL and logging into Tk20. Depending upon the type of user that is trying to access the system and the configuration data, the pluggable authentication module (PAM) makes the decision about which authentication source to connect to, in order to authenticate the user. Depending upon the response from the external authentication source, in case of failed authentication appropriate message is conveyed back to the user. In case of successful authentication, system runs the authorization checks on the users before granting access to the system. This is depicted in the diagram below

Remote Authentication Architecture Diagram



Request for Information

In order for Tk20 to authenticate the users against external authentication source we will need the following information

If the external authentication source is something other than LDAP please complete the following information:

A. Information about External Authentication Source

1. Are there any ports that need to be opened on your firewall to accept incoming traffic from the client machines?
2. Do you need to know the IP addresses of the client machine that attempt the connection to the authentication source?
3. Are there any security certificates/files that need to be installed/imported on the client machine?

If the external authentication source at your institution is LDAP/AD, please provide the following

1. LDAP server:
2. Port of communication:
3. Search/User Base:
4. Bind Account dn:
5. Bind Account pwd: - Please provide the number to call in case it can't be distributed via document
6. User Attribute for searching (Filter will be created based on this attribute):
7. Attributes we can request to be returned after initial bind (we will use these to get the DN for the user):

If the external authentication source is something other than LDAP server, please provide the following

1. What is the external authentication source?
2. How does the client connect to the external authentication source?
3. What is the recommended communication protocol?
4. Is there any service account that the client needs to use for connecting to the external authentication source?
5. Is there any user Attribute information that we need to know to be able to create search filters during authentication?
6. In implementation/testing phase will we be connecting to the same authentication source that will be used in production or is there a test server setup that we will be accessing during this phase?
7. Is there any other configuration that needs to be done on the client machine?

8. Does the external authentication source need to be down for maintenance or patches etc? In that case what is the process of notifying the clients?

B. Information about technical implementation

- a. Are there any public APIs that are used to connect to the external authentication source?
- b. Please provide any documentation and sample client code regarding connecting and authenticating users against external authentication source.
- c. How the external authentication source respond back to the client. Please specify in detail the response during
 - i. Successful authentication
 - ii. Unsuccessful authentication – Please specify the error codes and their meanings if any
- d. What are the types of users that are supposed to get authenticated against this external authentication source? (For example, all faculty, students, deans etc.)
- e. Please provide the name and the contact information of the personnel that we can call on in case we need assistance during implementation?
- f. What are the contact hours and recommended mode of communication (Phone, email etc?)
- g. Can you provide any client utility or any other resources in order for us to test the connection to authentication source?

C. Information about testing the implementation

- a. Can you setup 3 different test accounts for us to use during the testing phase so that we can try to mimic the normal system usage?
- b. Can you ensure that the passwords of these accounts are alive and valid until the implementation is rolled out into production

D. Emergency escalation

- a. In case of an event where external authentication source does not respond or stops functioning due to error condition how do we escalate this issue?

Testing Procedure

Once we receive all the information requested and implementation of the authentication module is complete, following steps are taken as part of test procedure

1. A test release with this authentication module is created
2. Test release is deployed on a test server

Configuration:

Once the test release is deployed following configuration items are carried out before starting the testing:

1. Different properties pertaining to external authentication source and connection parameters are configured
2. Roles that need to be externally authenticated are configured to be authenticated externally in testing dataset.
3. Test user accounts are created; so that the usernames for those users in Tk20 match the usernames provided by university.
4. Some of the test accounts are marked inactive in Tk20
5. Some of the test accounts are marked not paid in Tk20
6. Some of the test accounts are assigned a role that need to be externally authenticated
7. Some of the test accounts are assigned a role that needs to be locally authenticated.
8. For these test accounts, password change flags are set so that they don't get directed to password change page the first time they log in.
9. Forgot username/password link on the login page of Tk20 is removed.
10. Messages to be displayed to the end user are configured.
11. If necessary a default test suite is enhanced to take in account additional scenarios.

Test Suite:

A. Remote Authentication

1. User with inactive Tk20 account logs in with correct credentials in Tk20
2. User with not paid Tk20 account logs in with correct credentials in Tk20
3. User with expired Tk20 accounts logs in with correct credentials in Tk20
4. User logs in with correct credential but does not exist in Tk20 system
5. User logs in with incorrect username
6. User logs in with correct username and incorrect password
7. User logs in with correct login credentials and has active/paid account in Tk20
8. User with active/paid account logs into Tk20 and gets authenticated against external authentication source.
9. User with active/paid account logs into Tk20 and gets authenticated locally against Tk20 database.
10. User that gets authenticated locally logs into Tk20 for the first time

B. Single Sign on (portal integration)

1. User logs in successfully in the portal and has sufficient privileges to access Tk20 account.
2. User logs in with incorrect credentials in the portal
3. User with inactive Tk20 account logs in with correct credentials in the portal
4. User with not paid Tk20 account logs in with correct credentials in portal
5. User with expired Tk20 accounts logs in with correct credentials in portal
6. User that exists in portal logs in with correct credential but does not exist in Tk20 system

Project Plan

No	Item	Responsible Party	Timeline
1	Initial conference call to gather general requirements and distribute the documentation	Tk20	
2	University to provide the requested information in section titled "Request for Information"		
3	Seek clarification about the information and make sure that all the information necessary for technical implementation is obtained		
4	Technical implementation of remote authentication/single sign on		2 ½ weeks
5	Create the test release		1 ½ weeks
6	Deployment of test release on a test server		
7	Load necessary dataset on a test server		
8	Create necessary configuration for test suites		
9	Execute the test suite to ensure that the test case passes		
10	Start planning Production rollout as per section titled "Production rollout procedure"		

Production Rollout procedure

Once the technical implementation is complete and the full test suite is successfully run, only then the software becomes a candidate for deployment in production environment. At this time the system would be in-use by various administrators, faculty and other users. Since this upgrade needs to be happen on a live server, following needs to happen before an upgrade can happen on live server

Coordination:

Unit Administrators need to be notified about the impending system upgrade. Careful coordination between Tk20 product designee and Tk20 Unit Administrator will indicate the time when system can be upgraded. Once such time is decided, it will be notified to all the members of supporting staff from your university.

System Downtime:

A message indicating system downtime is configured to let the Tk20 users know about the impending upgrade. Typically the downtime for an upgrade will be about 4 hours.

Configuration:

Once the production release is rolled out, following configuration items need to be completed before the system can work with remote authentication or single sign on

1. Different properties pertaining to external authentication source and connection parameters are configured
2. Roles that need to be externally authenticated are configured to be authenticated externally in live dataset.
3. Usernames in live dataset need to match the ones in external authentication source.
4. Password change flags are set so that those users don't get directed to password change page the first time they log in.
5. Forgot username/password link on the login page of Tk20 is removed.
6. Messages to be displayed to the end user are configured.

Known Issues in production environment

Once the system is deployed in production environment following issues may arise through the use of system

1. If any users that are to be authenticated externally are created manually using administration section of the system
 - a. They may not have their username same as the one in external authentication source
 - b. If the usernames are identical, they will be directed to the password change screen the first time they log in
2. If a new role is created in the system and the users with that role need to be externally authenticated, then this needs to be marked manually in the database by engineering. Failure to do so will result in invalid password error when those users try to login into Campustools HigherEd.
3. If password of the user that gets externally authenticated is reset via administrative functions, the next time user logs in he will be directed to change password page.
4. If external emails pertaining to survey are sent out, the email usually contains the encrypted authentication information so that clicking on the link authenticates the user in Tk20 and user doesn't have to login into Tk20. However, in case of remote authentication since we do not have complete authentication information clicking on a survey email link will redirect the page to Campustools HigherEd login page since such user can not be validated via Tk20.
5. For remote authentication to work through Campustools HigherEd usernames in Tk20 need to match the usernames in external authentication source. This needs to be ensured anytime users are entered in the system via data loads. Data load files should contain usernames information so that usernames can be updated to match the ones in external authentication source.

Emergency Handling Procedure in Campustools Highered

In case of an event where the external authentication source does not respond or stop functioning due to error condition please provide the contact information of the personnel that can be reached during such emergency.