

Use Cases

Breakdown of Use Cases for ABE Resource Server

📅 16 October 2018

Student - Level 2 - CompSci/Maths

Attempting to download JOOSE2 coursework.

Student wants to login to service and browse/search for resources of their JOOSE2 course. They may even be searching for the JOOSE2 coursework file directly. This file should show to the student if (and only if) they have certain attributes (listed below as considerations) such as enrollment in the JOOSE2 course. The metadata of the resource is compared to the student's account for this show/hide service. If they find the resource then the student would like to download the file and decrypt the contents using their Key.

Considerations:

- coursework may be uploaded in advance of handout deadline
- owner/lecturer may have the file set to staff only
- student must be enrolled in the course
- student must be in level 2
- although a level 4+ student may be a demonstrator
- ✓ - student must have an active account
- student should be in the university network (???)
- coursework solution should **not** be accessible, just handout/cover sheet

Student - Level 4 - CompSci

Attempting to upload WebSci coursework submission.

Student wants to upload an encrypted resource to the server. The resource should be encrypted with a set of attributes allowing themselves, the lecturer and any required external markers to decrypt the submission for marking. No other students or unnecessary staff should have the correct attributes to access. The student should set these attributes either manually through the CLI tool or automatically with an attributes file provided for the coursework submission (parsed by the CLI tool). After encryption they should be able to login to the resource server and upload their encrypted file in binary format.

Considerations:

- student should be able to decrypt their own submission

- staff/markers must be able to decrypt submission for marking
- only the encrypted file should be uploaded
- during encryption metadata should be generated from the attributes and attached to the binary file
- upload should not be possible without an active account
- student should be enrolled in WebSci before uploading submission

Student - Level 3 - CompSci [Class Rep]

Attempting to browse and then download minutes from a class rep meeting.

Student attended (or missed - we don't care) the class rep meeting but would like to find and download the official minutes from the meeting. There may be many minutes for class rep meetings available, and the student isn't necessarily sure if the latest meeting's minutes are uploaded yet. As such they need to browse all available minutes to find the latest uploaded. Only current class reps should have access to the minutes and other students should not even be able to see the minutes on the server. After finding the latest minutes available, the student's Key should be used with a CLI tool to decrypt the minutes for the student to view them.

Considerations:

- student must have an active account
- only class reps and staff should be able to download/decrypt the minutes
- there may be multiple versions of the minutes (classified/public)
- being a past class rep is not valid, only current
- minutes should only be available for class reps that were "in office" during a period where said minutes were created or dated

Student - Level 4 - CompSci [Demonstrator - 1P]

Attempting to browse and then download solution & lab for 1P course.

Student is a Demonstrator and thus also a Staff member. Normally they would not have access to a Level 1 course anymore, but would like to browse available 1P labs and solutions. On finding correct files for the week, the student would like to download both files before using their Key to decrypt the lab sheet & solutions with a CLI tool.

Considerations:

- student must have an active account
- only staff (incl. Demonstrator) should have access to solutions
- only staff and students enrolled in 1P should have access to the lab
- but a student that is a Demonstrator must be a 1P Demonstrator not 1CT
- must be a current Demonstrator not future or past

- solutions & lab only available if current or previous week

Lecturer - IDA - IR - Joemon Jose

Attempting to upload lecture slides for Web Science lecture.

Lecturer wants to upload lecture slides in advance of lecture - inline with University policy. The slides should only be available to students from 24 hours before the lecture and onwards. The lecturer needs to be able to encrypt the file with their Key locally using a CLI tool and a set of attributes. They may either set the attributes manually through the CLI or perhaps from an imported attributes file. After encryption the lecturer would upload the binary file to the server. They may upload the file at any point before the lecture, however the file should be locked to staff (perhaps IDA staff) only until 24 hours prior to lecture.

Considerations:

- lecturer must be an active lecturer of websci course
- must have lecturer role not just title
- staff should be able to access from moment of upload
- may be limited to staff section
- a student should only have access if <24 hours before lecture
- a student must be enrolled in the course
- only the encrypted file should be uploaded
- during encryption metadata should be generated from the attributes and attached to the binary file

Lecturer - GLASS - SE - Tim Storer

Attempting to upload Level 3 project proposals.

Lecturer/Projects Coordinator wants to upload the latest list of project proposals. This is in advance of the release of the proposals and as such should not be available to students, but rather staff-only with some external access (scope???) for proposal contacts to check their proposals are correct. After proposal release, all Level 3 students should have access to all proposals to aide in selecting their preferred project. The files should all be encrypted locally with the lecturer's Key using a CLI tool that embeds relevant metadata into the binary files.

Considerations:

- lecturer must be the head lecturer (project coordinator) of TP3
- must have lecturer role not just title
- staff should be able to access from moment of upload
- may also need external access for the 'customer' to review
- a student should only have access proposals have been released

- a student must be enrolled in Level 3
- only the encrypted files should be uploaded
- during encryption metadata should be generated from the attributes and attached to each binary files

Staff - Head of School - Chris Johnson

Attempting to upload minutes from Senior Staff meeting.

After Senior Staff meetings the minutes are written up and then uploaded by the Head of School. Minutes should only be available to Senior Staff members such as Readers and above. An alternative School Update could be prepared and distributed to ALL staff members, but would not contain the same contents as the Senior Staff meeting minutes. The Head of School would encrypt the minutes with their own Key and define certain attributes using the CLI tool - perhaps by importing an attributes file. The CLI tool would assign these attributes as metadata to the binary file as well before uploading to the server.

Considerations:

- staff must be an active staff member
- staff must be the Head of School
- senior staff should be able to access the file after upload
- senior staff would be Readers and up
- no students would be able to see or decrypt the file
- only the encrypted files should be uploaded
- during encryption metadata should be generated from the attributes and attached to each binary files

Staff - Technical - Systems Team Manager

Attempting to upload a system architecture diagram.

Periodically the Systems architecture diagram needs updating to ensure an up-to-date copy is available to the Systems team. As such the file needs to be accessible by the full Systems staff team, as well as all Senior staff. The Systems Team Manager is responsible for updating the file and as such would like to encrypt the file with their Key whilst embedding the necessary attributes and metadata to the file. The encryption process would be carried out using a CLI tool with an imported attribute list or with manual setting of each attribute, again through the CLI.

Considerations:

- only the encrypted file should be uploaded
- on uploading the new encrypted file, it should replace the previous version
- or at least make it clear which is the current version

- no students should be able to see or access
- most staff will not have access
- a staff member must either be:
 - in the Systems team (or at least the Technical group)
 - a Senior member of staff (Reader and above)
- during encryption metadata should be generated from the attributes and attached to each binary files

Staff - Technical - Cybersecurity Network Integrator [SCOPE - May have to avoid external]

Attempting to find and download an externally-uploaded penetration testing report.

In order to enhance security of the DCS network, external 3rd-party companies are hired to carry out penetration testing in order to uncover and report vulnerabilities. After the testing is complete the external party upload the results to the server with a Key and ensure the results can only be downloaded and decrypted by the Cybersecurity Network Integrator, the Systems Team Manager and the Head of School. All other staff should not have access or visibility as this is a Highly Confidential file that could reveal flaws in the DCS network. The Cybersecurity Network Integrator would like to browse the server for the latest penetration testing report and download it. The report may be spread over multiple files and older reports may still be present on the server. After finding the file(s) the Cybersecurity Network Integrator would like to download and then decrypt the file(s) using their Key with the CLI tool.

Considerations:

- uploaded by an external party
- external upload is one-way, so they can not access the file again
- students can not see or access
- most staff can not see or access
- must be Cybersecurity Network Integrator or Systems Team Manager or the Head of School
- previous reports may also be present
- may be spread over multiple files (lumped into zip though?)

Staff - Admin - Teaching Administrator

Attempting to upload a newsletter for Honours students.

Teaching Administrator wants to upload a newsletter intended for all Honours students, but first needs to check that the Teaching Administrator Assistant hasn't already uploaded the same newsletter. Teaching Administrator needs to be able to check what newsletters are already available/uploaded before they upload it themselves. Hence the newsletters should be accessible to staff as well as current Honours students (Levels 3 & 4). After confirming that the newsletter has not yet been uploaded, the Teaching Administrator wants to encrypt it with their Key and in the process assign the correct attributes and metadata to the file using the CLI tool. After encryption, the new binary file (with embedded metadata) can be uploaded by the Teaching Administrator to the server.

Considerations:

- only students in Levels 3 or 4 should see or have access
- students Level M+ could also have access??
- all staff should have access
- not a confidential file, just irrelevant for Levels 1 & 2
- newsletters must be viewable to staff so they can check previous newsletters for redundancy
- only the encrypted files should be uploaded
- during encryption metadata should be generated from the attributes and attached to each binary files