Good morning. My name is Christopher Watson and for my Level 4 Individual Project I designed and implemented a departmental resource server for the University of Glasgow's Department of Computing Science. Security was a key criteria for this service, meaning that the implementation had to be "cryptographically secure" and as such employed an attribute-based encryption system for storage of uploaded resources.

WHY DO WE NEED RESOURCE SERVERS? WHAT CAN THEY DO?

- Organisations are large & complex in structure
- DCS — 500+ members (staff & students)
- Different roles, teams, groups etc.
- Members often separated for security
- Staff & students need to share some resources
- Users need to upload & download resources
- Users can grant access to other users
- Access to resources must be granular
- Communication and resources must be secure

Organisations - large & complex
Organisation hierarchy => many roles/teams/groups
DCS alone is over 500 members incl. staff + students
    DCS staff split into research groups
        such as the (GIST) & (FATA) groups
    and within, split into themes
        such as the (IR), (IDI) & (MOG) themes.
    within these themes, staff are often split into smaller, focused teams as well
With organisation member roles so carefully defined
Members of Org are often digitally separated for security

In DCS, a clear separation lies between staff & students
Yet some resources are shared with staff & students
    for example lecture notes

A resource server needs to:
    Allow uploading of own resources & downloading resources of others
        assuming they have access
    Let users grant access to their uploads
    Access should be granular

HOW SECURE DOES A RESOURCE SERVER NEED TO BE?

- Depends on organisation e.g. financial
- Depends on information e.g. HR files
- Department resources can be confidential
- Must be protected against 3rd parties
- DCS resources may be private; not top secret
- Exam scripts example of confidential resource
- Resources encrypted during transmission
- HTTPS with SSL/TLS cert
- Resources must also be encrypted at-rest

…but just how secure does a resource server need to be?

Security of resource server depends on the organisation
    Financial institutes will probably have more stringent requirements (FCA accredited)
    than a private company
Also depends on the purpose of the server
    HR file storage should be confidential and restricted
    Department memos and newsletters could be public and unrestricted
Resources could be confidential to department and
Must be protected from unknown, 3rd party access

For the DCS, resources are unlikely to be top secret, mostly “Internal”
    Will be restricted from general access
Exam scripts & marking schemes are examples of confidential resources
    Must not be accessible to students

Resource must be encrypted for transmission
    HTTPS w/ SSL certificate
This is not enough for an organisation and so
Resources must also be encrypted at-rest [TRANSITION TO NEXT SLIDE]

AT-REST ENCRYPTION & ATTRIBUTE-BASED ENCRYPTION (ABE)

- Services often leave uploaded resources unencrypted
- Slack, Facebook, Instagram, Twitter etc.
- Leaves resources *vulnerable* if a breach occurs
- Organisations require at-rest encryption — AES 128-bit & above
- Google Drive, OneDrive etc. store symmetric AES keys themselves
- ABE encryption only requires a stored public key
- Embeds access policies into encrypted resources
- Only private user keys can decrypt; embedded attributes as proof

Most services don’t consider resources as private
    Store uploads unencrypted for simple sharing/processing
    Slack, Facebook, Instagram, Twitter keep resources public
Unencrypted resources are vulnerable to breaches
Not acceptable for business/organisation use - need at-rest encryption
    Encrypted files can be stolen by hackers without risk of information breach
    Google Drive, OneDrive etc. offer AES encryption (for business)
    But store AES *symmetric* keys themselves
        Stored separately - still vulnerable

ABE encryption avoids this risk since user keys are private
    Server only stores a public key (for distribution)
Instead embeds policies into encrypted resources
User keys then use embedded attributes to prove access
    Decryption is then a local process by users

Deployment of a resource server is extremely important [TRANSITION TO NEXT SLIDE]

DEPLOYMENT & USER ENROLMENT

- Deployed resource server is a ‘dumb’ service by design
- Unaware of contents of resources
- Distributes the master public key
- Allows upload & download of any resource
- Never performs encryption/decryption tasks

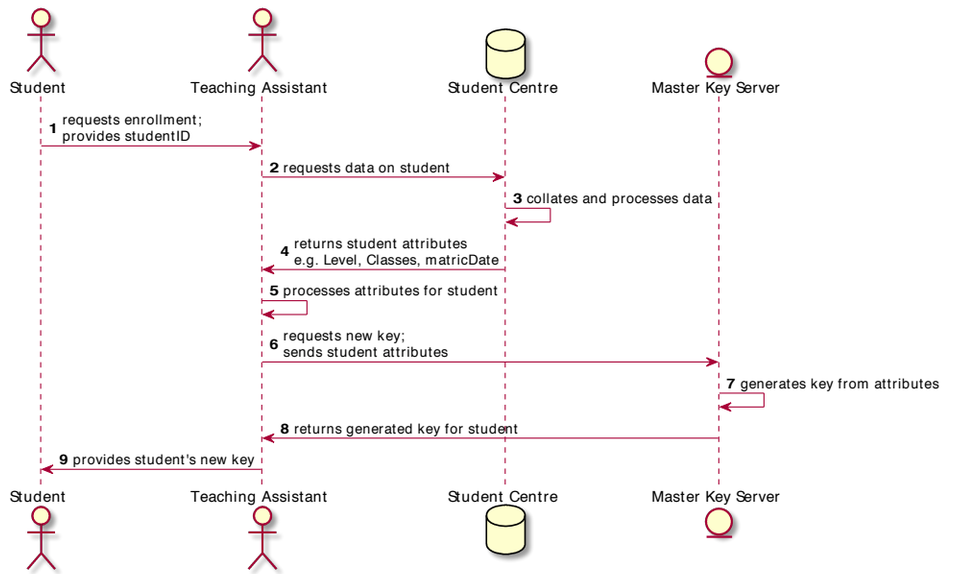
- Users need their private user key generated
- Enrolment requires DCS members visit Teaching Office
- Member of Admin then verifies identity; generates user key
- Embedding attributes extracted from MyCampus

…and in this case, the deployed resource server offers a ‘dumb’ service by design
Unaware of resource contents & unable to access information
Server also distributes the master public key
    on behalf of Master Key Server (offline system)
Server allows users to upload & download any resource
    safe as the resources are encrypted and cannot be interpreted
The server is incapable of encrypting or decrypting resources
    has no keys, no ABE library etc.

Users must enrol for the service, acquire their user key
    Has to be generated/signed by the offline Master Key Server
For DCS deployment, Master Key server would be in locked room
    Physical access only for Admin Staff
    DCS members must visit Teaching Office for key
Admin staff verify identity then generate key
Attributes for the key extracted from MyCampus system

Process diagram next slide [TRANSITION TO CONCLUSION SLIDE]

USER ENROLMENT PROCESS



Users must enrol for the service, acquire their user key

- Has to be generated/signed by the offline Master Key Server

For DCS deployment, Master Key server would be in locked room

- Physical access only for Admin Staff
- DCS members must visit Teaching Office for key

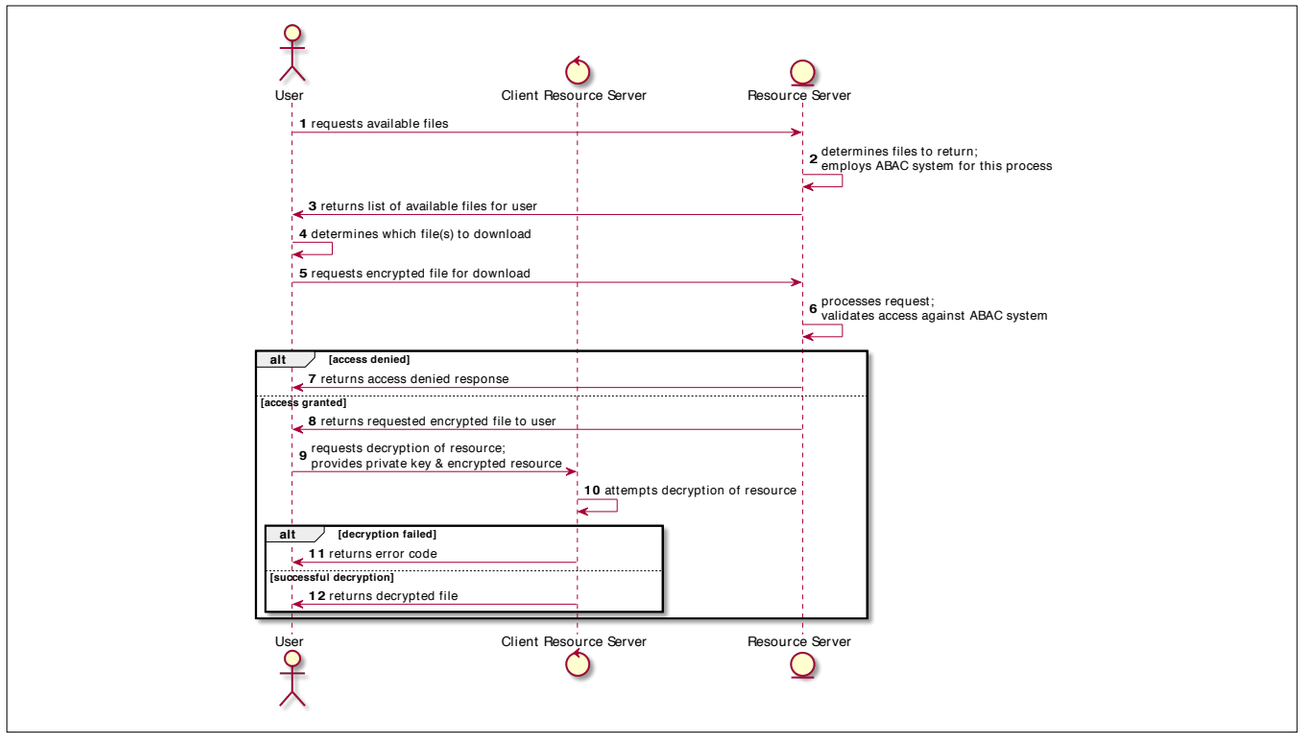
Admin staff verify identity then generate key

Attributes for the key extracted from MyCampus system

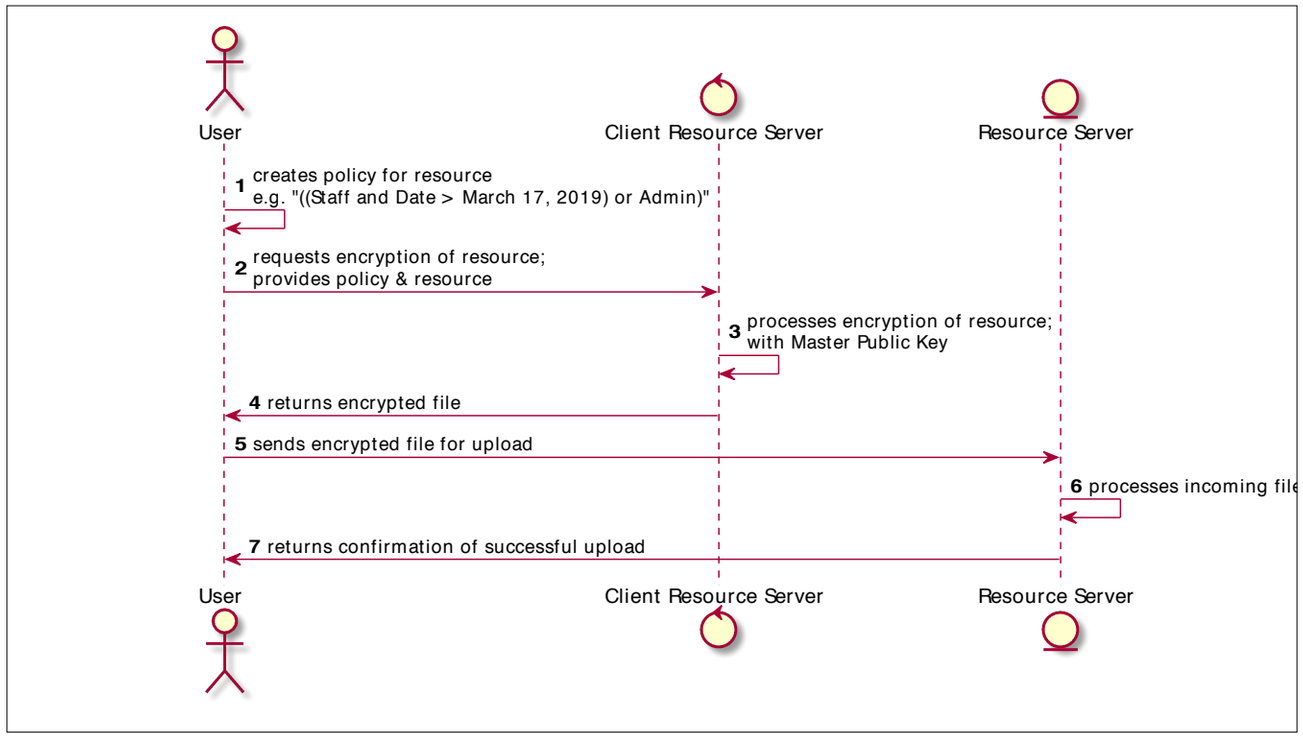
CONCLUSIONS

- Designed and created a resource server for the Department of Computing Science
- Analysed the structure of the DCS
- Implemented an Attribute-Based encryption system
- Created an infrastructure for deployment
- Developed a deployment process
- Including an enrolment process for users

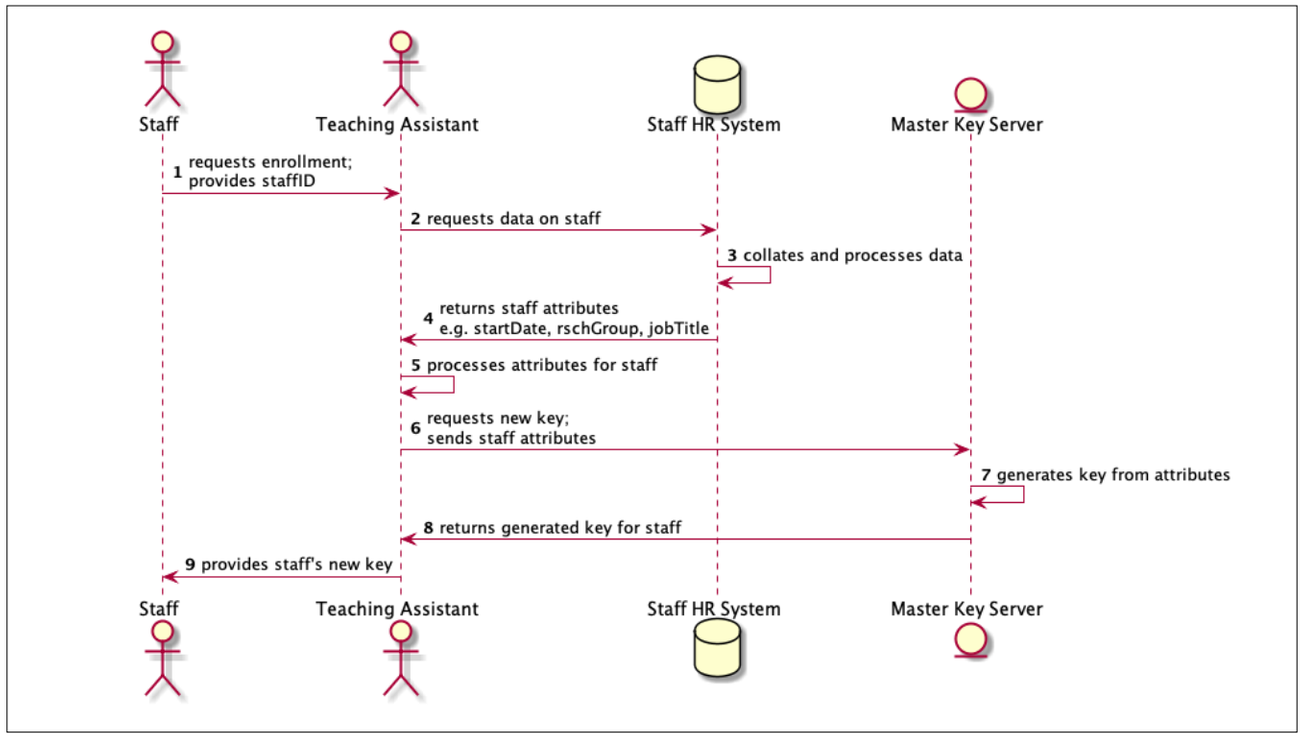
QUESTIONS?



Download & Decryption process



Encryption & Upload process



Staff Enrolment process

Deployment Diagram