

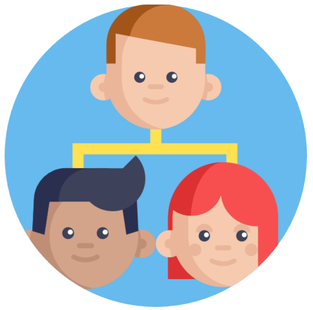
A CRYPTOGRAPHICALLY SECURE DEPARTMENTAL RESOURCE SERVER

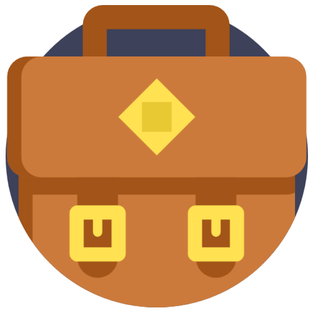
"Designing and constructing a departmental resource server for the Department of Computing Science, with implementation of attribute-based encryption to provide a cryptographically secure service"

Chris Watson (2190594w)

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





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

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

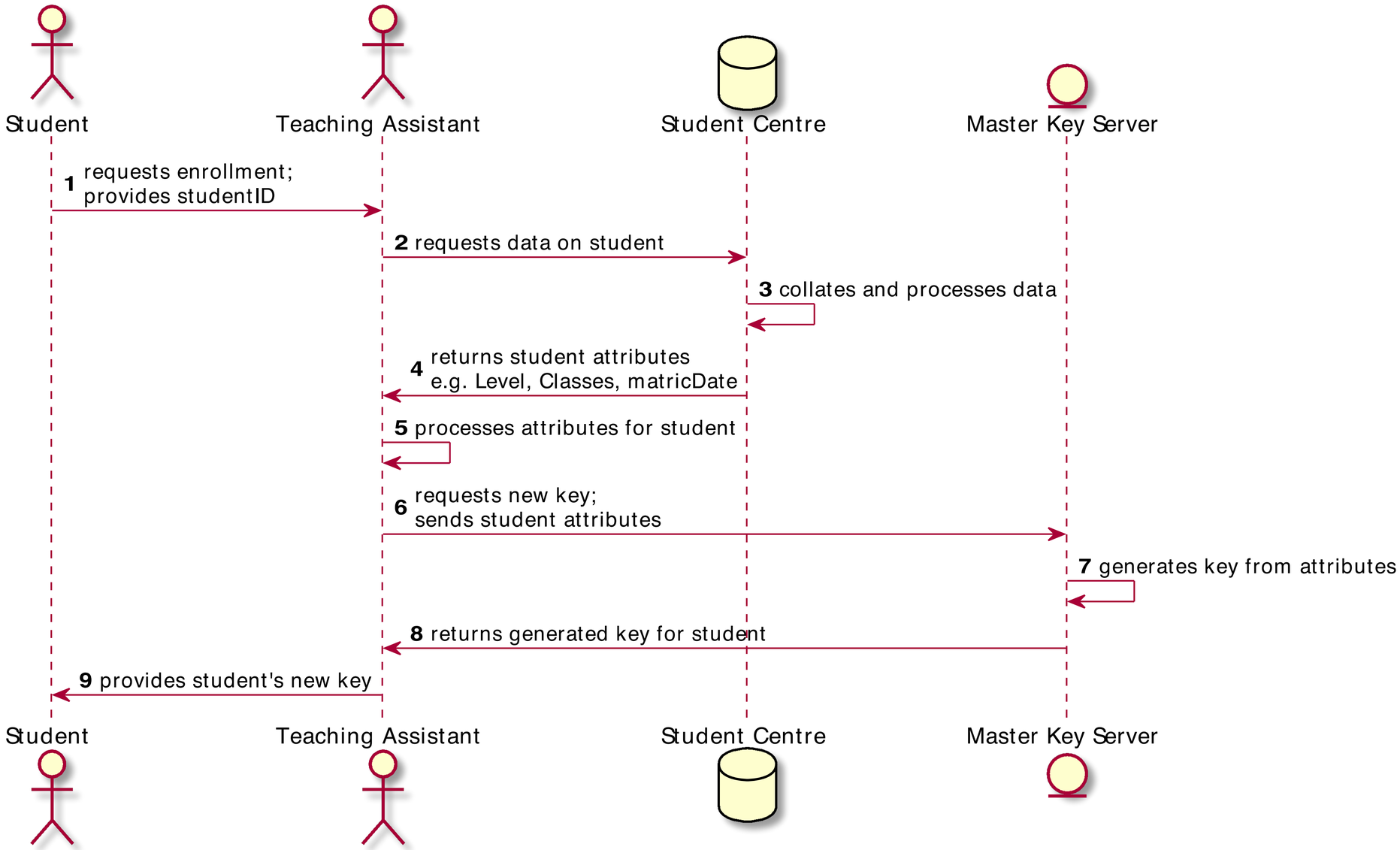
- Services often leave uploaded resources unencrypted
- Slack, Facebook, Instagram, Twitter etc.
- Leaves resources *vulnerable* if a breach occurs
- Organisations require at-rest encryption — AES 128-bit & above
- Google Drive, OneDrive etc. store symmetric AES keys themselves
- ABE encryption only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

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

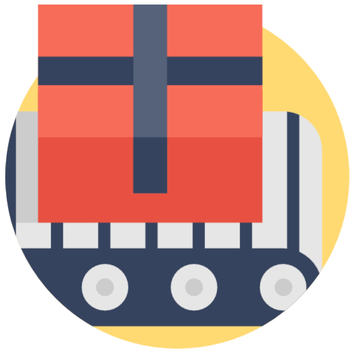
- Users need their private user key generated
- Enrolment requires DCS members visit Teaching Office
- Member of Admin then verifies identity; generates user key
- Embedding attributes extracted from MyCampus

USER ENROLMENT PROCESS



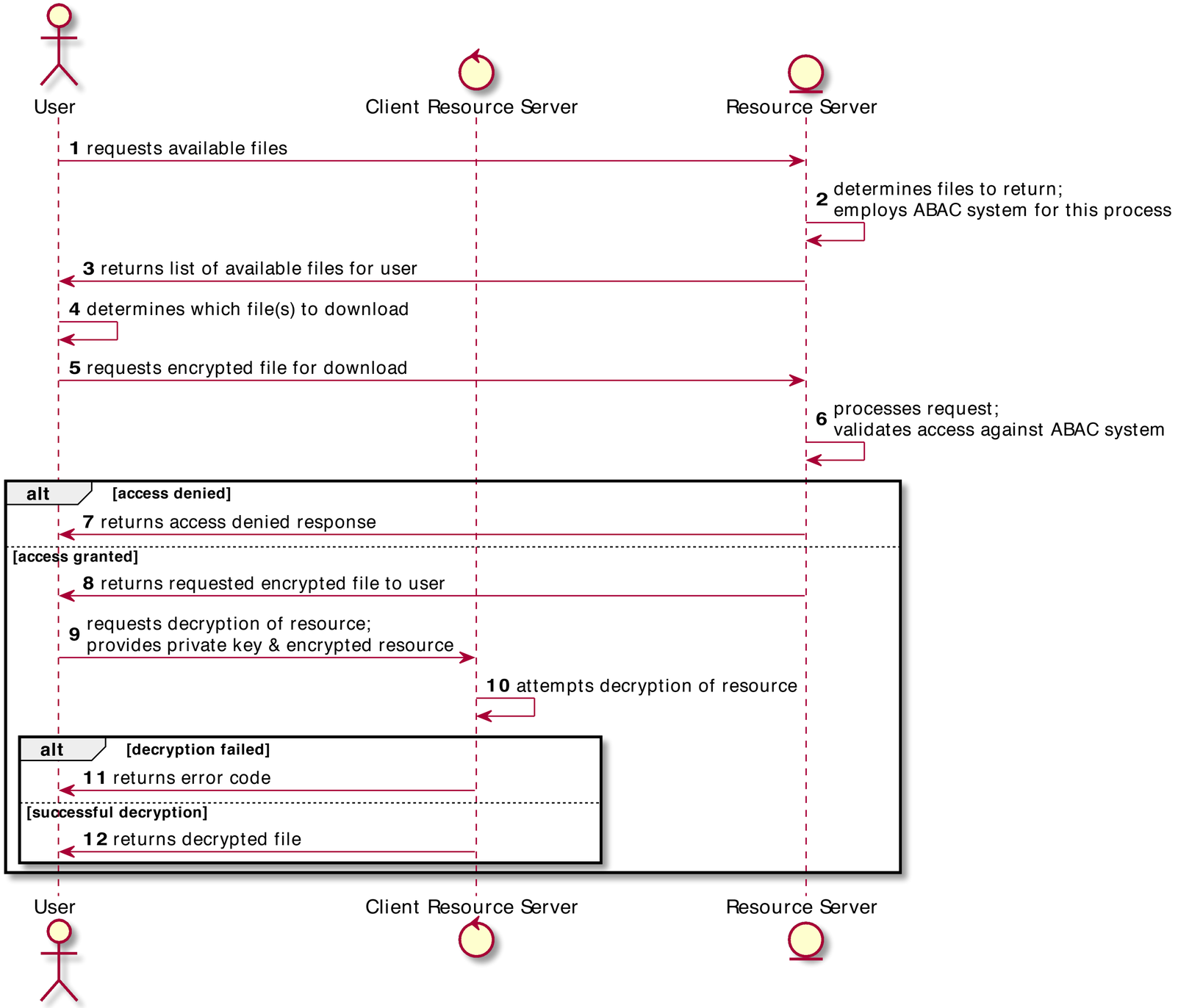
CONCLUSIONS

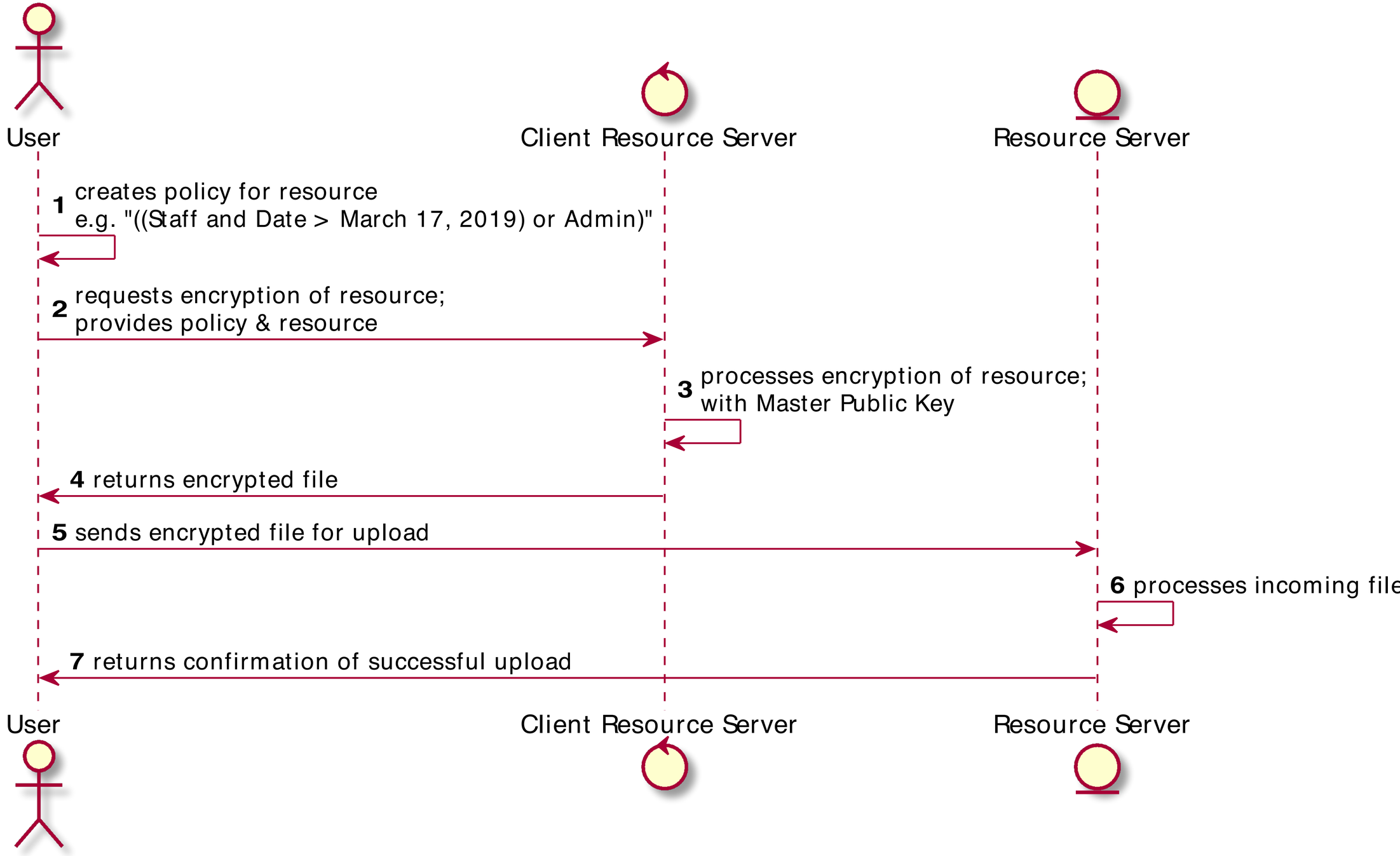
- Designed and created a resource server for the Department of Computing Science
- Resource server was cryptographically secure in implementation
- Analysed the structure of the DCS
- Implemented an Attribute-Based encryption system
- Created an infrastructure for deployment
- Developed a deployment process
- Including an enrolment process for users
- Producing a complete & secure product for future use

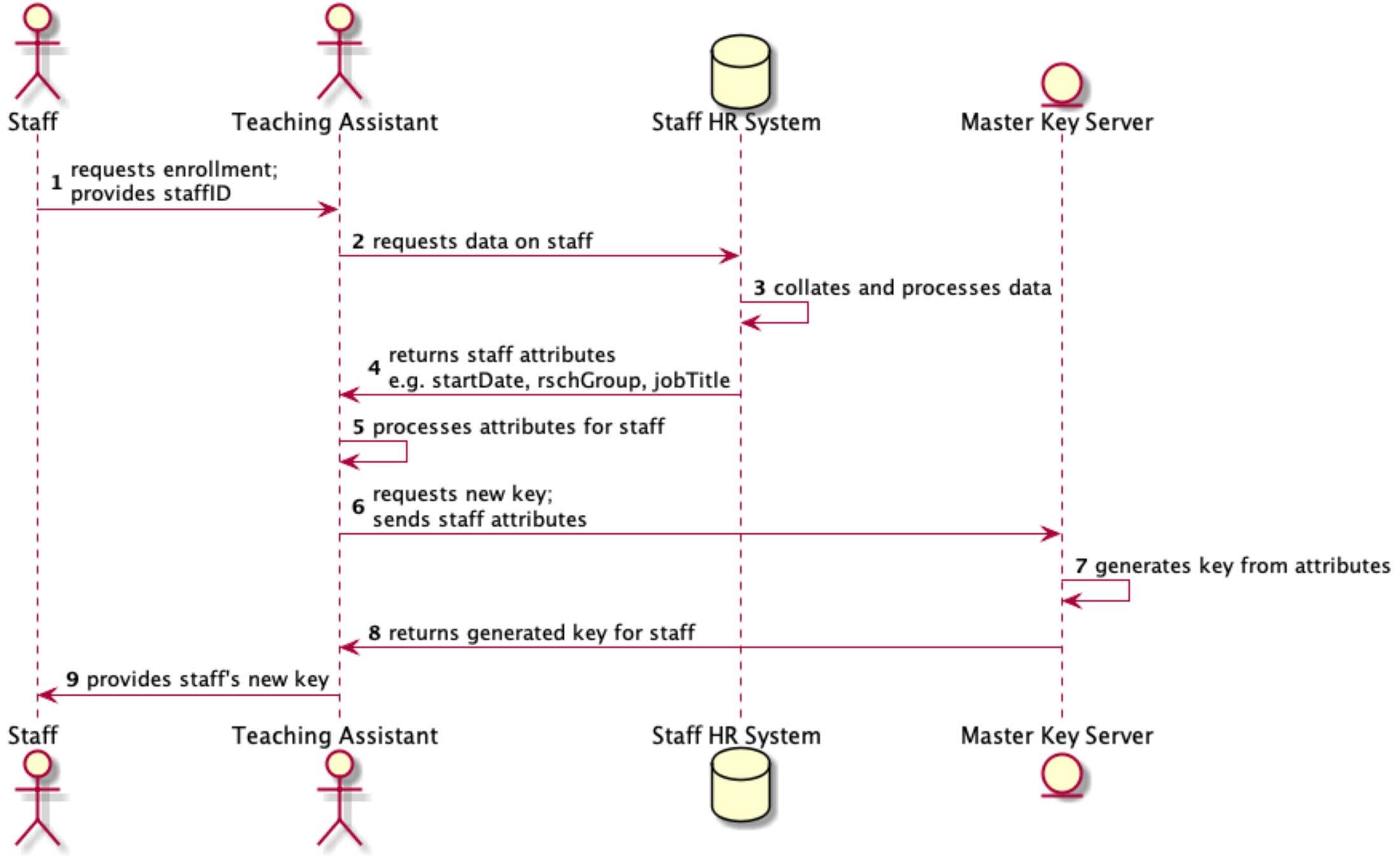


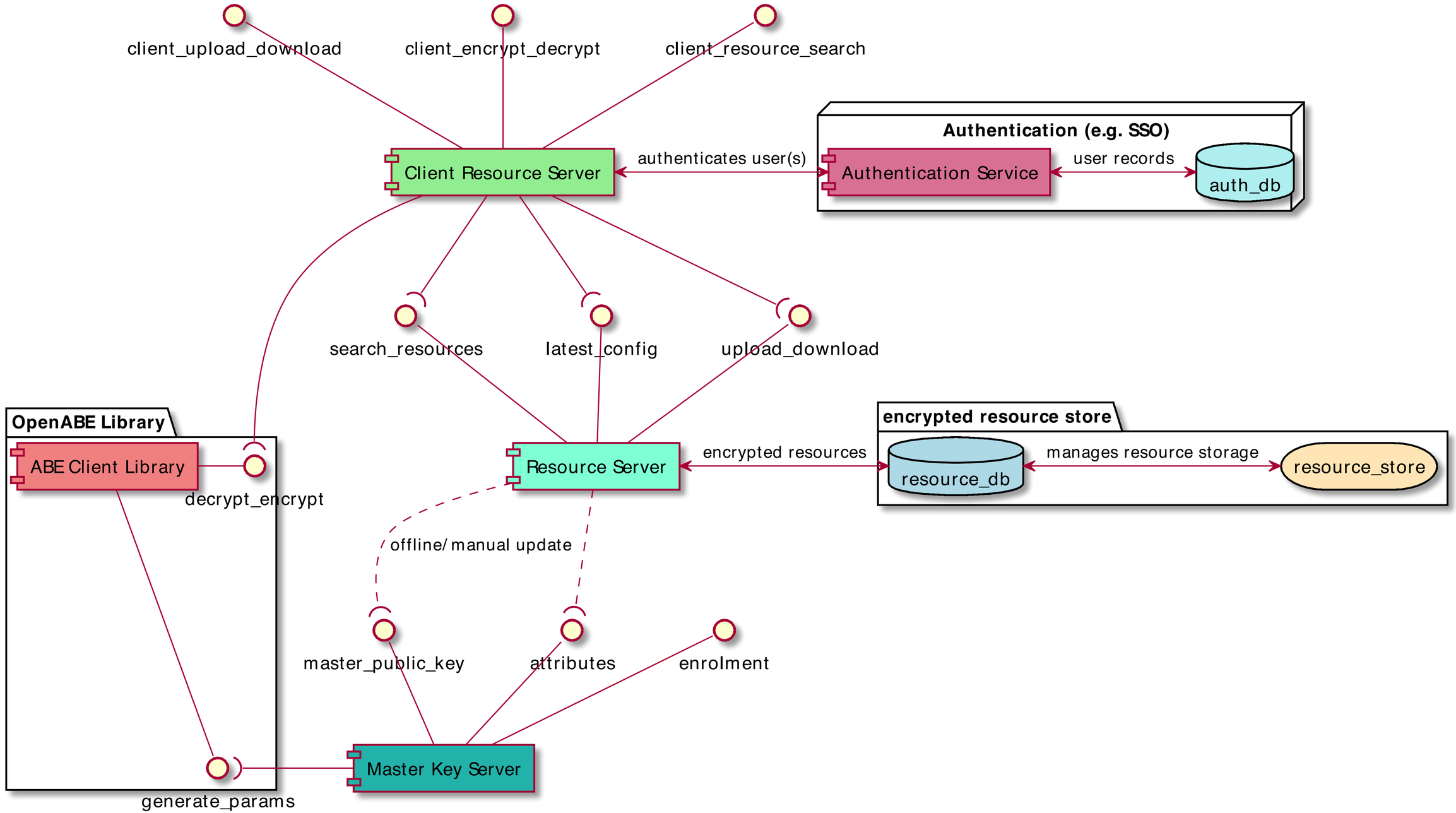


QUESTIONS?


User
Client Resource Server
Resource Server
1 requests available files
2 determines files to return;
employs ABAC system for this process
3 returns list of available files for user
4 determines which file(s) to download
5 requests encrypted file for download
6 processes request;
validates access against ABAC system
alt
[access denied]
7 returns access denied response
[access granted]
8 returns requested encrypted file to user
9 requests decryption of resource;
provides private key & encrypted resource
10 attempts decryption of resource
alt
[decryption failed]
11 returns error code
[successful decryption]
12 returns decrypted file
User
Client Resource Server
Resource Server


User
Client Resource Server
Resource Server
1 creates policy for resource
e.g. "((Staff and Date > March 17, 2019) or Admin)"
2 requests encryption of resource;
provides policy & resource
3 processes encryption of resource;
with Master Public Key
4 returns encrypted file
5 sends encrypted file for upload
6 processes incoming file
7 returns confirmation of successful upload
User
Client Resource Server
Resource Server


Staff
Teaching Assistant
Staff HR System
Master Key Server
1 requests enrollment;
provides staffID
2 requests data on staff
3 collates and processes data
4 returns staff attributes
e.g. startDate, rschGroup, jobTitle
5 processes attributes for staff
6 requests new key;
sends staff attributes
7 generates key from attributes
8 returns generated key for staff
9 provides staff's new key
Staff
Teaching Assistant
Staff HR System
Master Key Server


client_upload_download
client_encrypt_decrypt
client_resource_search
Client Resource Server
authenticates user(s)
Authentication (e.g. SSO)
Authentication Service
user records
auth_db
search_resources
latest_config
upload_download
OpenABE Library
ABE Client Library
decrypt_encrypt
Resource Server
encrypted resources
encrypted resource store
resource_db
manages resource storage
resource_store
offline/ manual update
master_public_key
attributes
enrolment
Master Key Server
generate_params