SELIS Towards a Shared European Logistics Intelligent Information Space

National Technical University of Athens

CSLab

Authentication and Authorization towards Federated Logistics Communities

Ioannis Konstantinou, CSLab, ICCS

Nikodimos Provatas, CSLab, ICCS

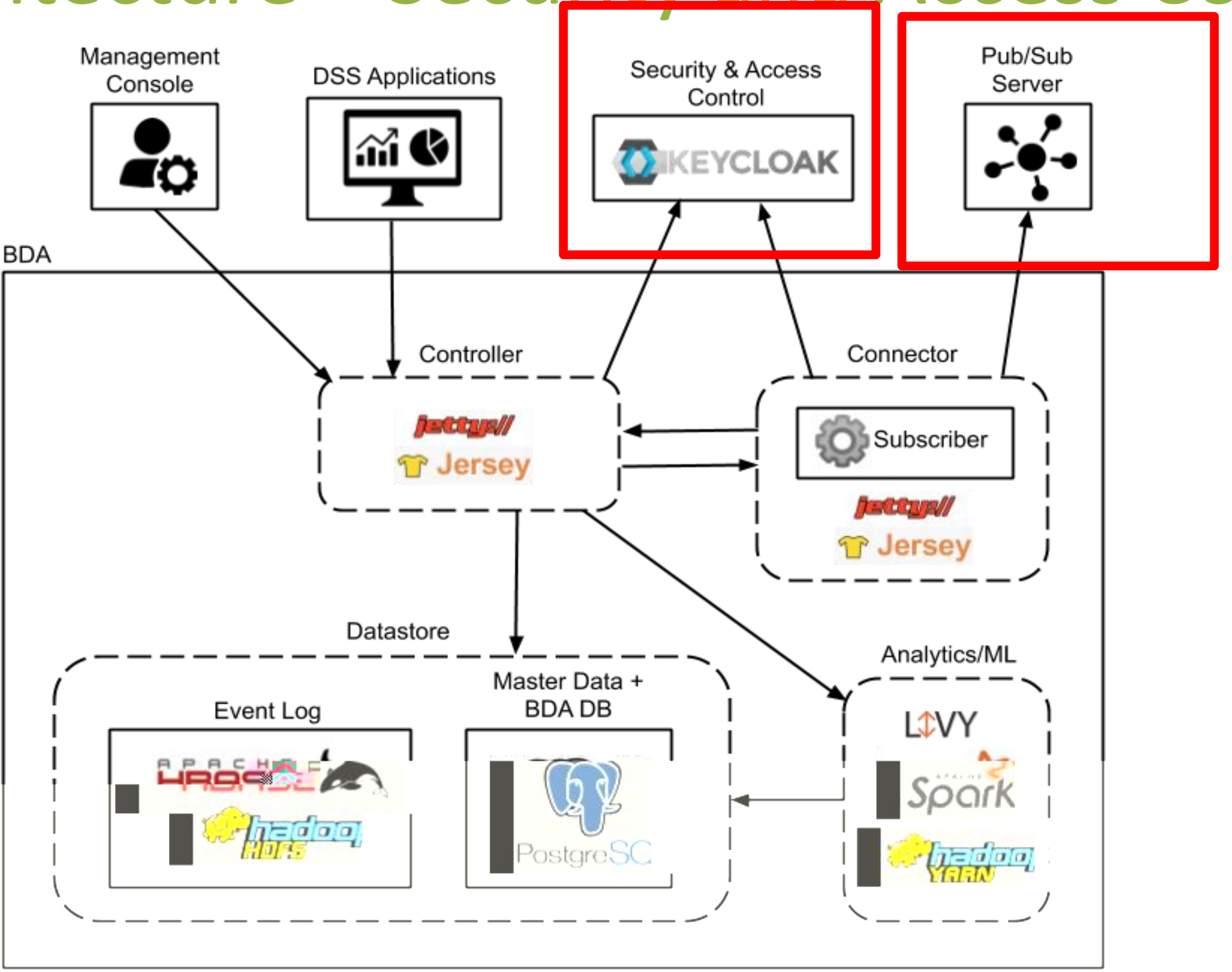
Evdokia Kassela, CSLab, ICCS

Tasos Bakogiannis, CSLab, ICCS

IPIC 2019

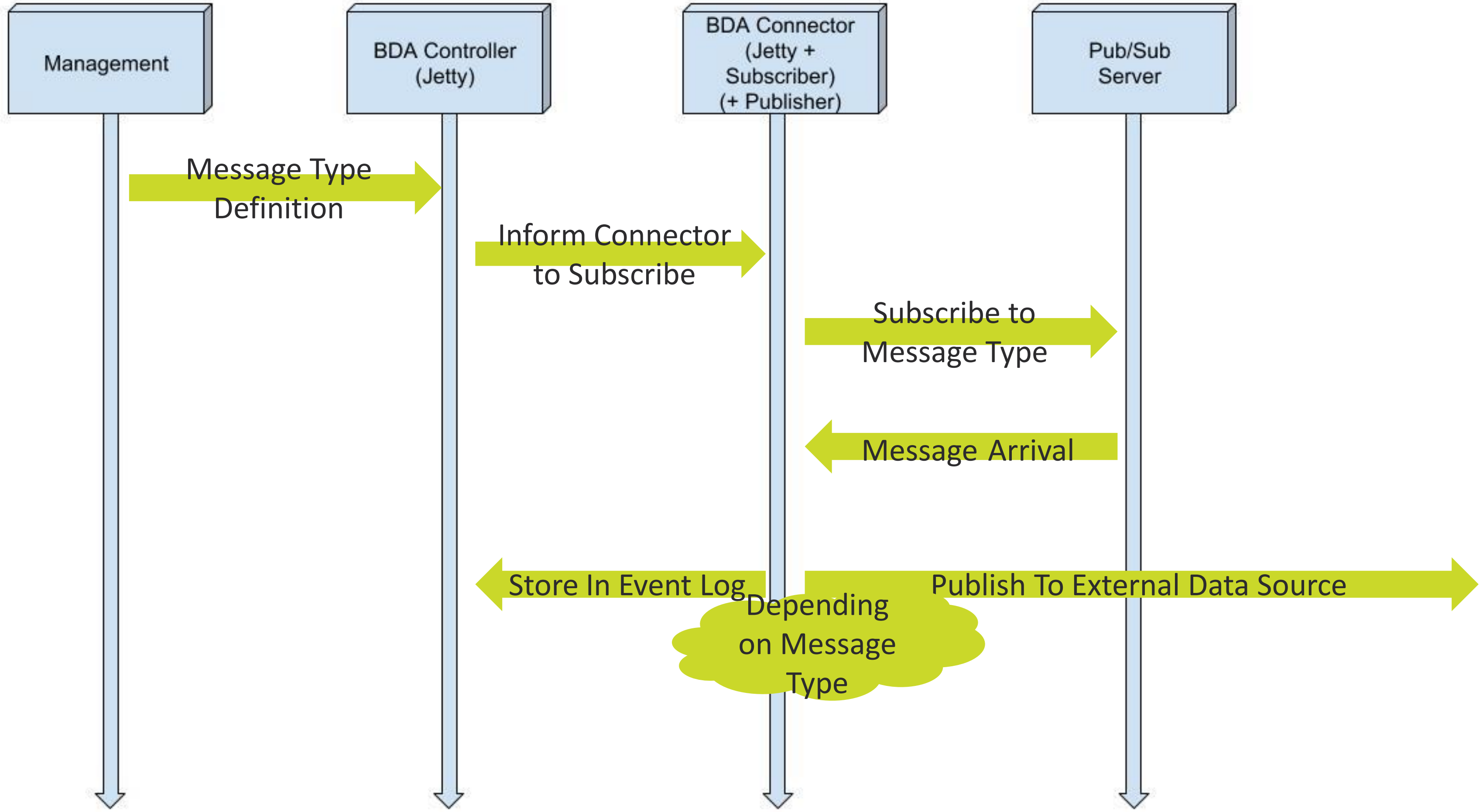
10th July 2019, London, UK

SCN Architecture – Security and Access Control



Data Exchange

- Subscribing/Publishing to Data Source (e.g. Pub/Sub)

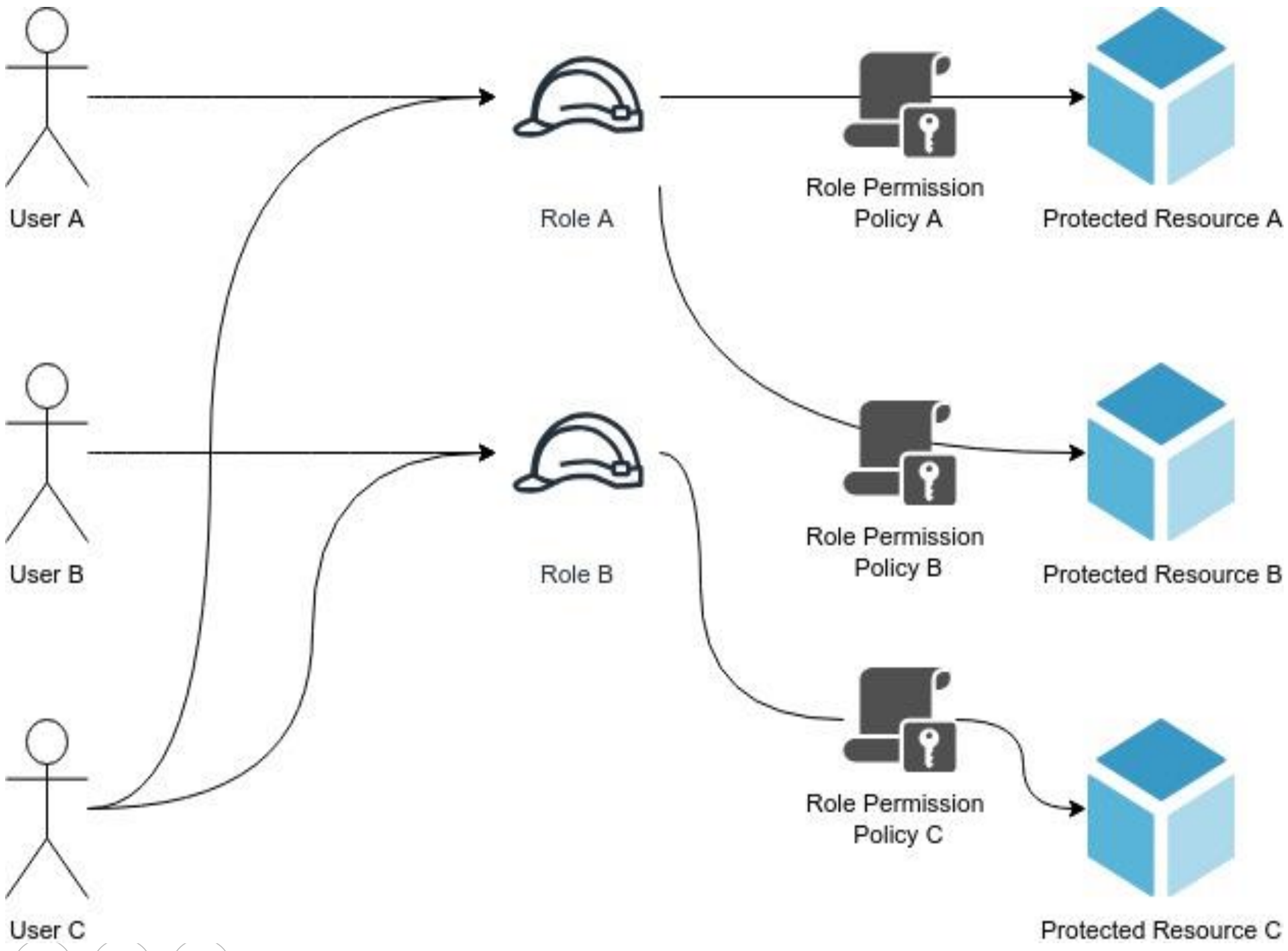


Management
BDA Controller (Jetty)
BDA Connector (Jetty + Subscriber) (+ Publisher)
Pub/Sub Server
Message Type Definition
Inform Connector to Subscribe
Subscribe to Message Type
Message Arrival
Store In Event Log
Publish To External Data Source
Depending on Message Type

Security Aspects - Semantics (I)

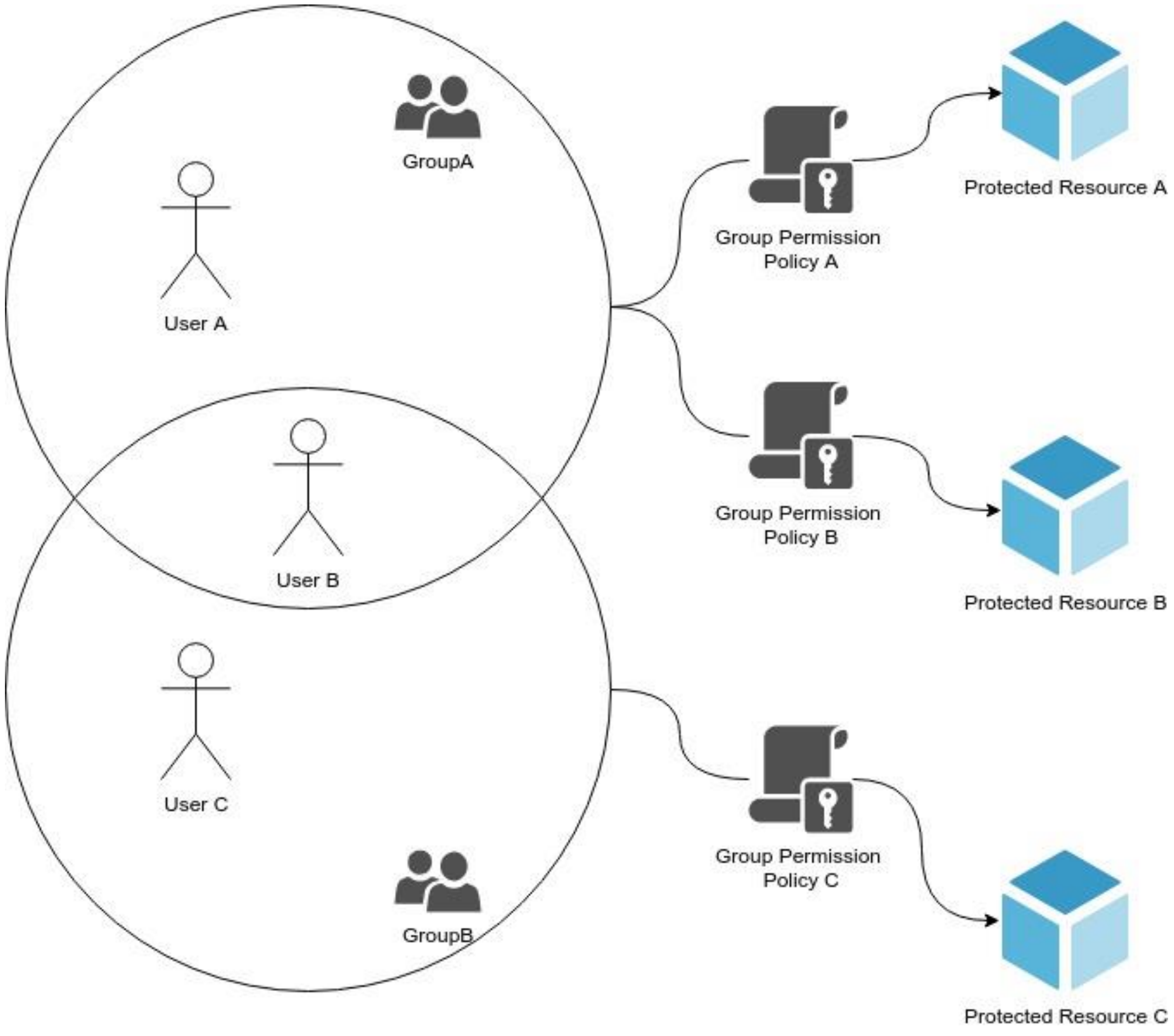
- Authorization / Authentication Performed by KEYCLOAK
- Semantics:
  - Resources : Anything that needs protection (REST API, PostgreSql Tables, HBase Namespaces, etc.)
  - Resource Scopes : Different aspects of resource protection – e.g. C(reate)R(ead)U(pdate)D(elete)
  - Clients / Resource Servers : Entities that protect some resources and authenticate users to access them
  - Users: Entities that demand access on a protect resource.
  - Permission: A user having a permission can access the corresponding scope / resource
  - Group : Define a group of users that have some permissions

Permissions/Policies Example using **Roles**



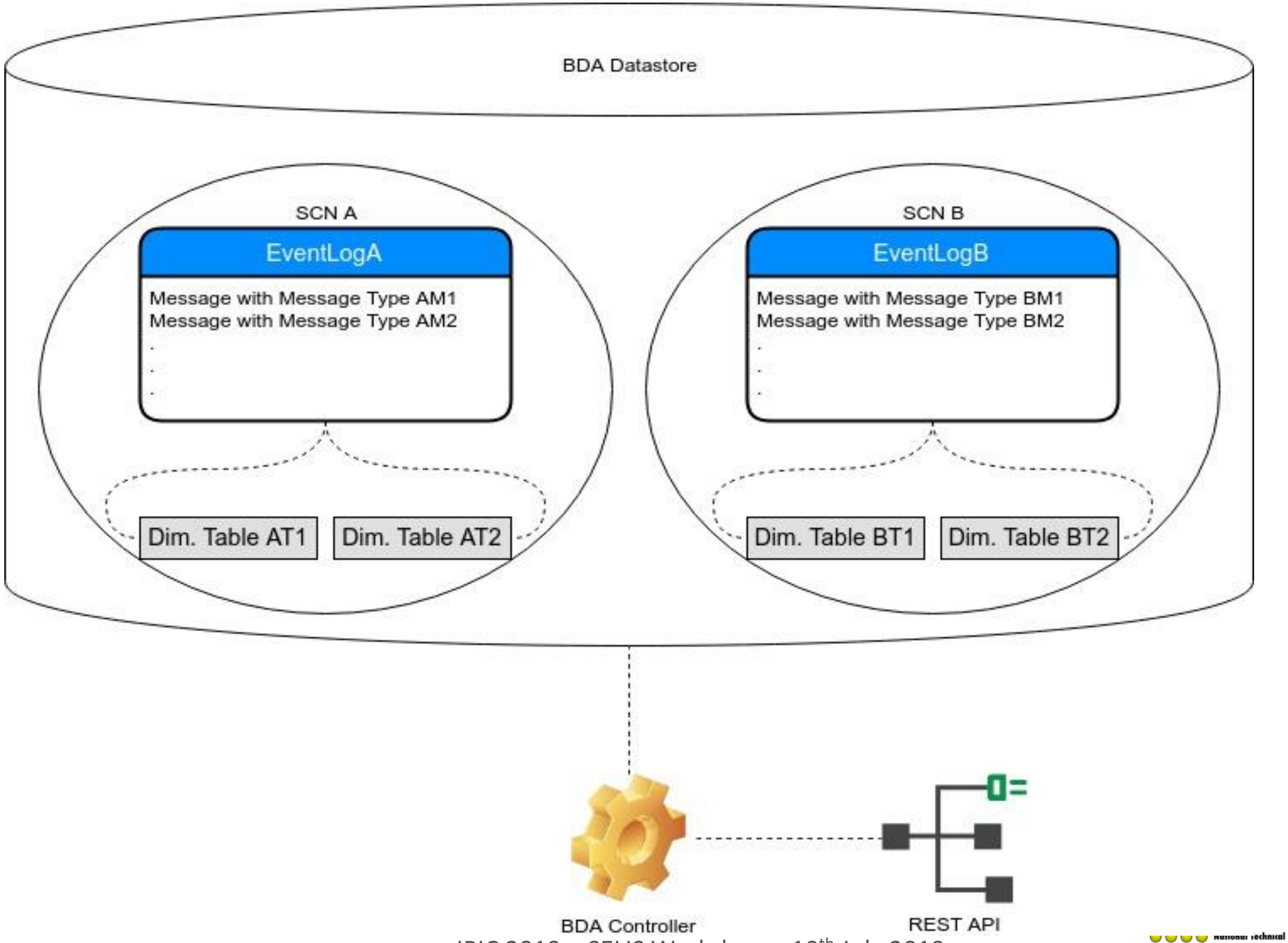
- User A: can access Resource A, B through Role A
- User B: Can access Resource B through Role B
- User C can access Resources A, B, C through Roles A, B

Permissions/Policies Example using **Groups**

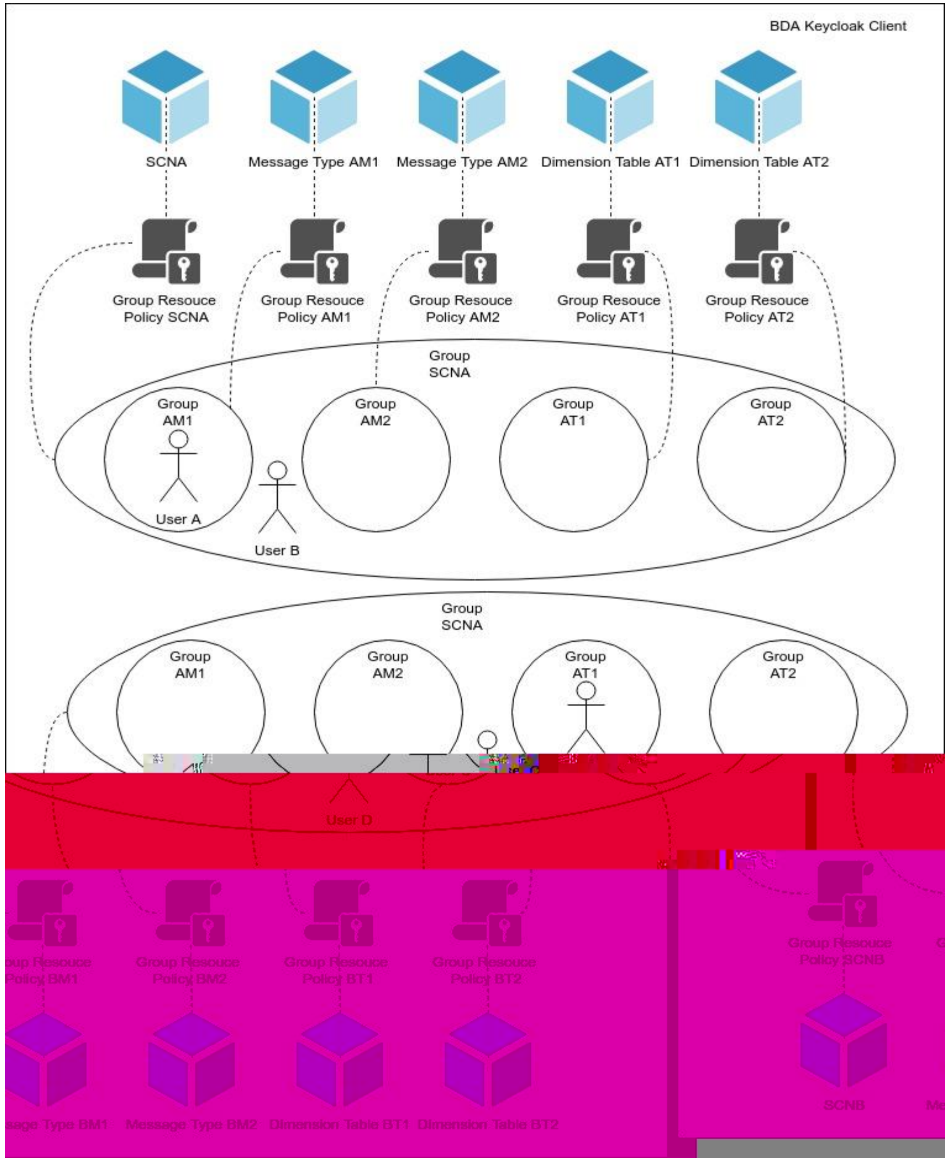


- Group A has two Group Permission Policies A and B that provide access to the Protected Resources A and B respectively.
- Group B can interact with Protected Resource C as it is defined by the Group Permission Policy C.
- User A can interact with Resources A and B since it belongs to Group A,
- User C has only access to the Protected Resource C through Group B.
- User B can interact with all the three stated resources, since she belong to both groups

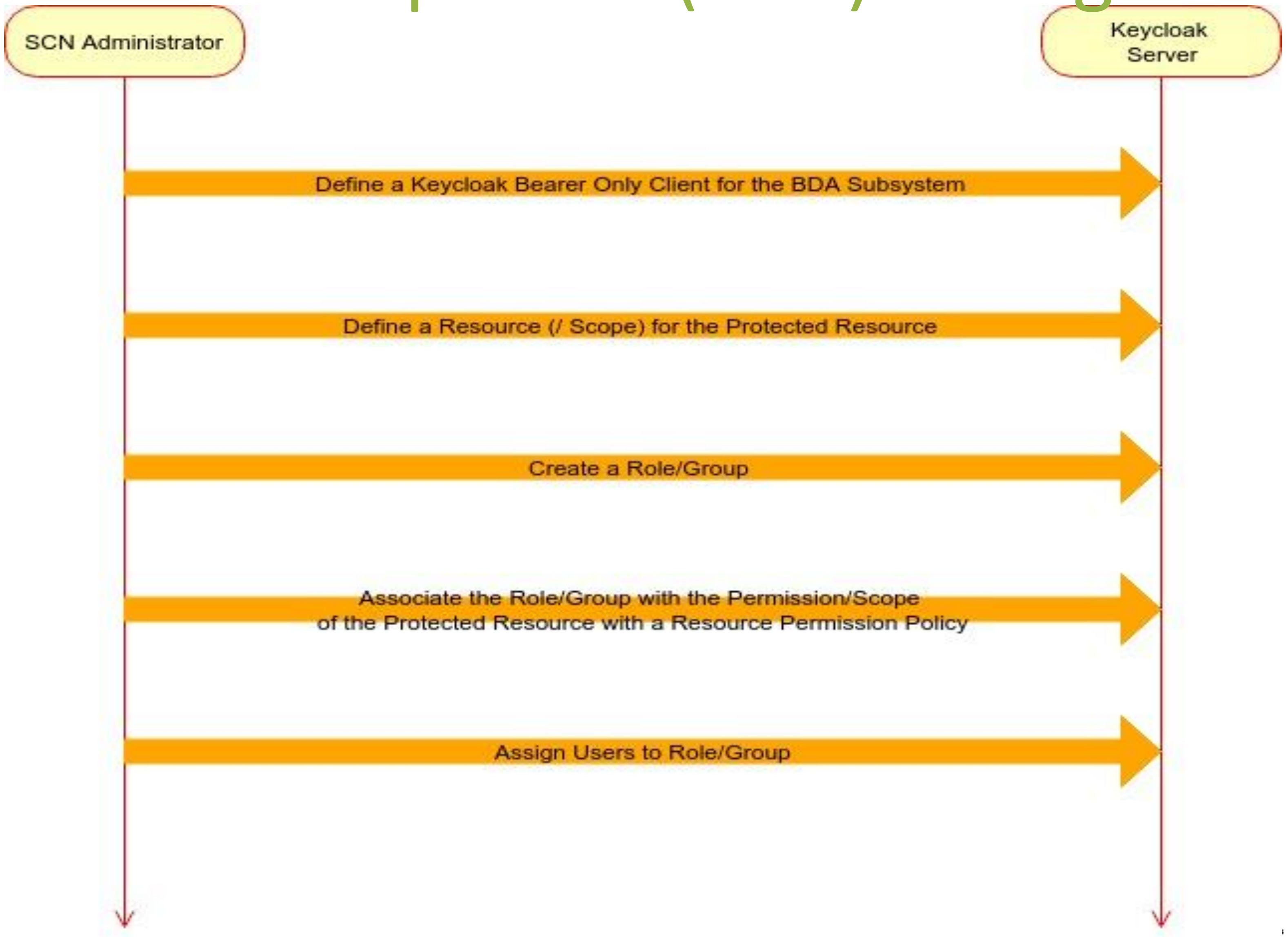
Putting it all together: Securing SELIS data communications



Putting it all together: Securing SELIS data communications

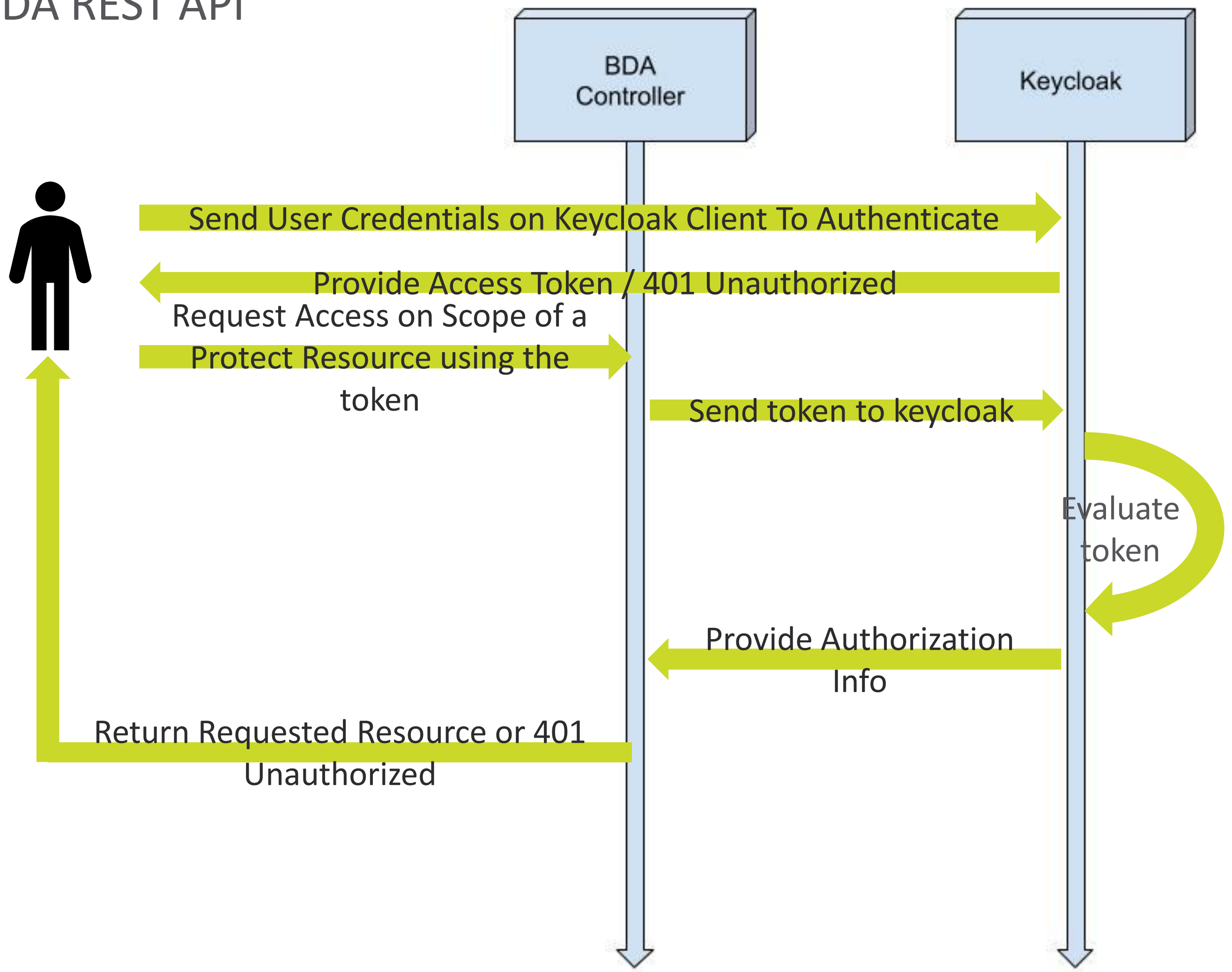


Securing an SCN component (BDA) during bootstrapping


SCN Administrator
Keycloak Server
Define a Keycloak Bearer Only Client for the BDA Subsystem
Define a Resource (/ Scope) for the Protected Resource
Create a Role/Group
Associate the Role/Group with the Permission/Scope of the Protected Resource with a Resource Permission Policy
Assign Users to Role/Group

Security Aspects – Data at Rest (III)

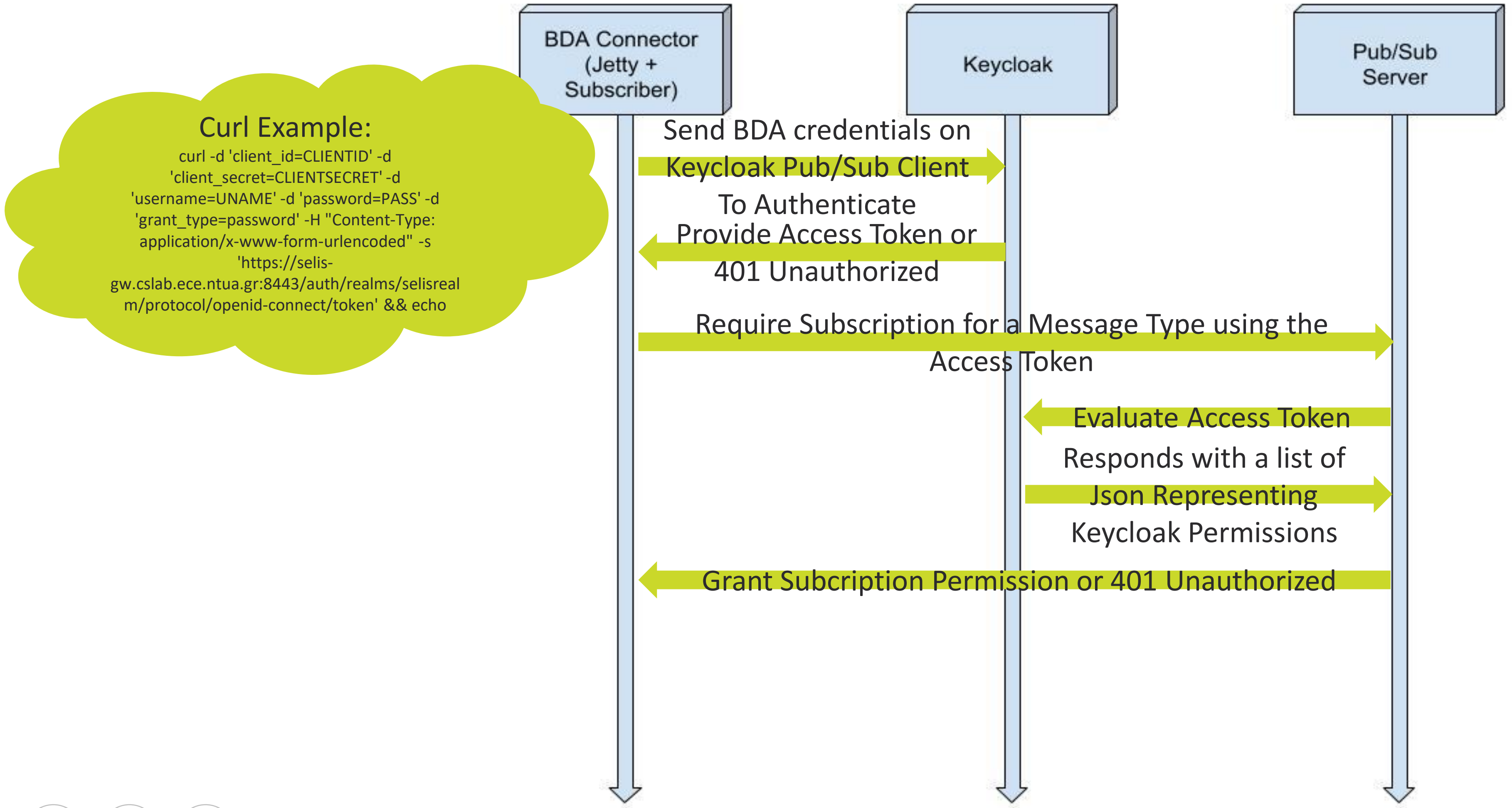
- Secured BDA REST API



BDA Controller
Keycloak
Send User Credentials on Keycloak Client To Authenticate
Provide Access Token / 401 Unauthorized
Request Access on Scope of a Protect Resource using the token
Send token to keycloak
Evaluate token
Provide Authorization Info
Return Requested Resource or 401 Unauthorized

Security Aspects - Data at Motion (II)

- Secured BDA subscription on Pub/Sub



Curl Example:

```
curl -d 'client_id=CLIENTID' -d
'client_secret=CLIENTSECRET' -d
'username=UNAME' -d 'password=PASS' -d
'grant_type=password' -H "Content-Type:
application/x-www-form-urlencoded" -s
'https://selis-
gw.cslab.ece.ntua.gr:8443/auth/realms/selisreal
m/protocol/openid-connect/token' && echo
```

Send BDA credentials on Keycloak Pub/Sub Client To Authenticate

Provide Access Token or 401 Unauthorized

Require Subscription for a Message Type using the Access Token

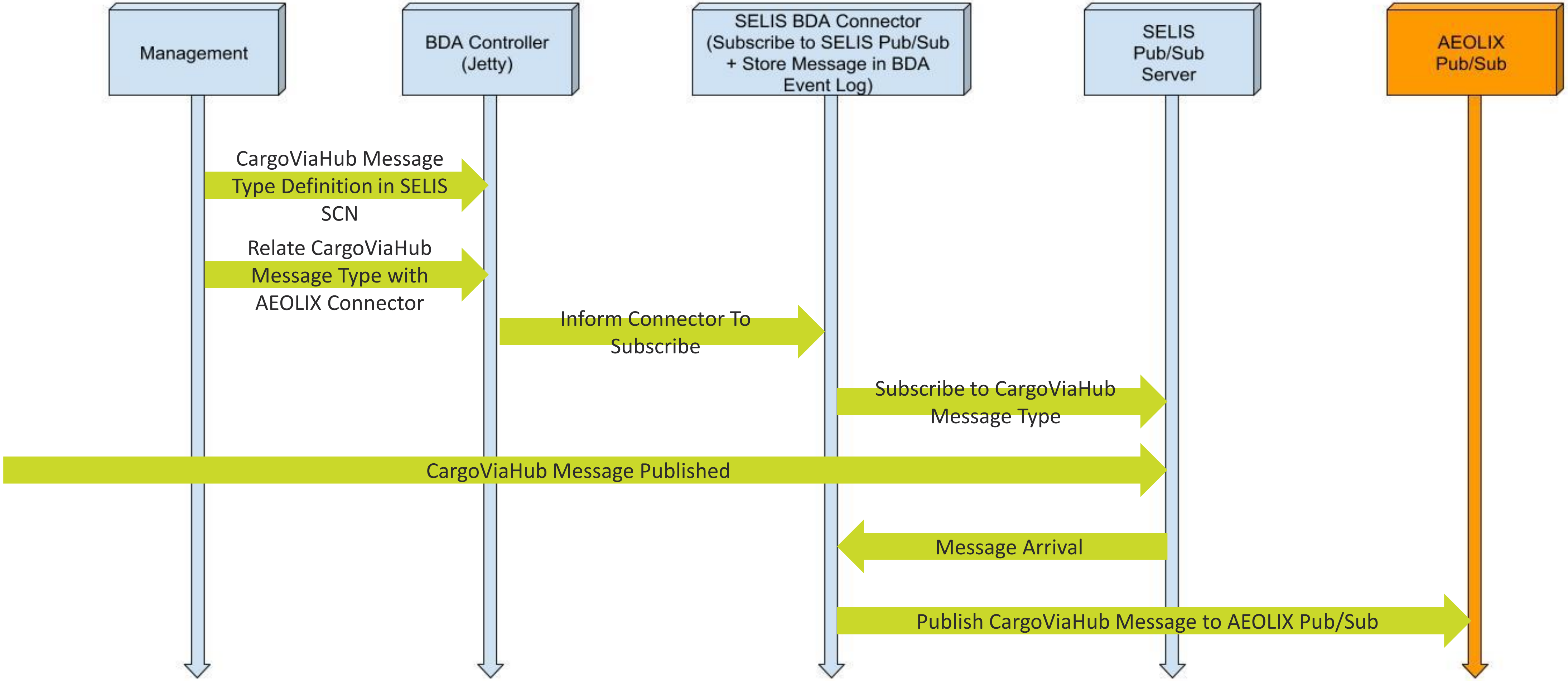
Evaluate Access Token

Responds with a list of Json Representing Keycloak Permissions

Grant Subcription Permission or 401 Unauthorized

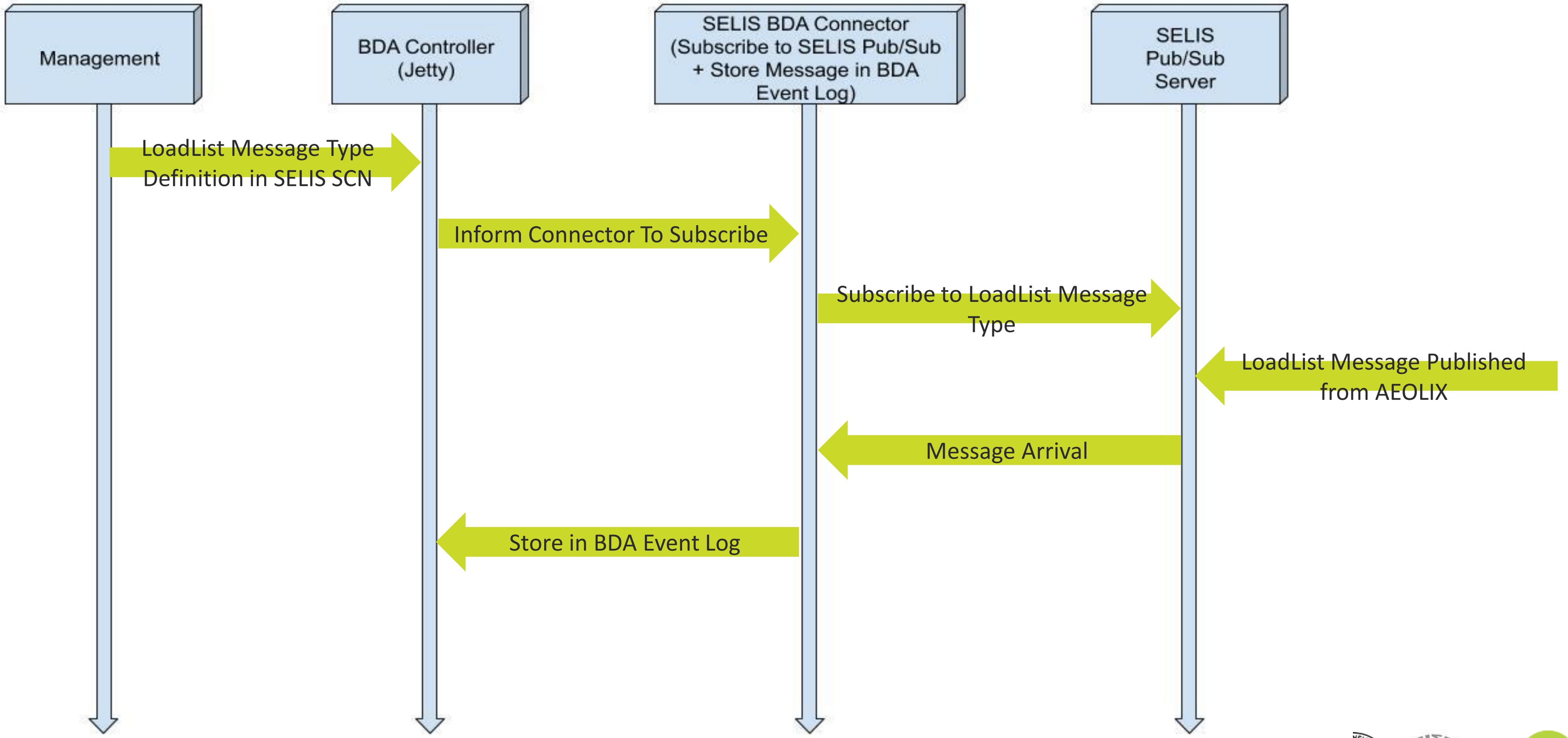
Data Exchange (AEOLIX Case) (I)

- Sending Data to AEOLIX


Management
BDA Controller (Jetty)
SELIS BDA Connector (Subscribe to SELIS Pub/Sub + Store Message in BDA Event Log)
SELIS Pub/Sub Server
AEOLIX Pub/Sub
CargoViaHub Message Type Definition in SELIS SCN
Relate CargoViaHub Message Type with AEOLIX Connector
Inform Connector To Subscribe
Subscribe to CargoViaHub Message Type
CargoViaHub Message Published
Message Arrival
Publish CargoViaHub Message to AEOLIX Pub/Sub

Data Exchange (AEOLIX Case) (II)

- Getting Data from AEOLIX


Management
BDA Controller (Jetty)
SELIS BDA Connector (Subscribe to SELIS Pub/Sub + Store Message in BDA Event Log)
SELIS Pub/Sub Server
LoadList Message Type Definition in SELIS SCN
Inform Connector To Subscribe
Subscribe to LoadList Message Type
LoadList Message Published from AEOLIX
Message Arrival
Store in BDA Event Log

Q&A

Contact Details

ICCS

Ioannis Konstantinou

ikons@cslab.ece.ntua.gr