Multi Cloud

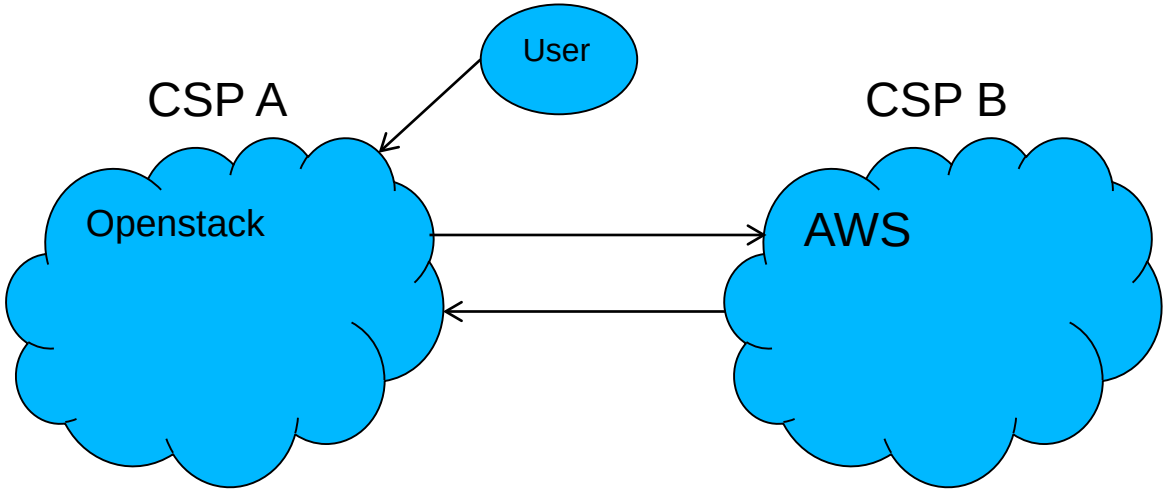
Navid Pustchi

April 25, 2014

navid.pustchi@utsa.edu

Motivation

- User seamlessly or by choice can use services from another cloud.
- The user belongs to one CSP.
- Each cloud has independent administration(different).



Background

- Federation
  - Deployment of multiple CSPs (heterogeneous or homogenous) to provide complex services.

- Based on deployment
  - Hybrid Cloud
  - Community Cloud

Hybrid Cloud

- Composition of two or more cloud deployment models that remain unique entities but are bound together by proprietary technology that enables data and application portability.

- One organization provides and manages the resources.

[NIST 2012, p18]

Community Cloud

- Provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.
- It may be owned, managed and operated by one or more of the organizations in the cloud.

[NIST 2012, p18]

Multi Cloud Restrictions

- Heterogeneity and tight coupling.
- Pre-established business agreements.
- Service Delivery Model.

Multi Cloud Architectures

- A central management system.
- Homogenous federation running the same management system on all infrastructures.
- Central front end.
- Common API on top of distinct independent management systems.

[VANDER 2012, p4]

Central management system

- Separate infrastructure replaces their management system with a common one.
- Easy to deploy and maintain.
- Potential compatibility issues and new software adoption.

[VANDER 2012, p5]

Homogenous Federation

- Each infrastructure manages its resources independent from a central point.
- Each management infrastructure should be replaced with tools capable of federation.

[VANDER 2012, p6]

Central front-end

- All facilities and associated tools remain unchanged and keep their own user registration, procedures, etc.
- The only commonality is a central location, hosting a list of all facilities and their tools.

[VANDER 2012, p5]

Common API

- Each facility keeps its current management software.
- Common interfaces on top of each management software are specified, standardized and made available within the federation.
- The need of a common protocol.

[VANDER 2012, p6]

Security Prospects Multi Cloud

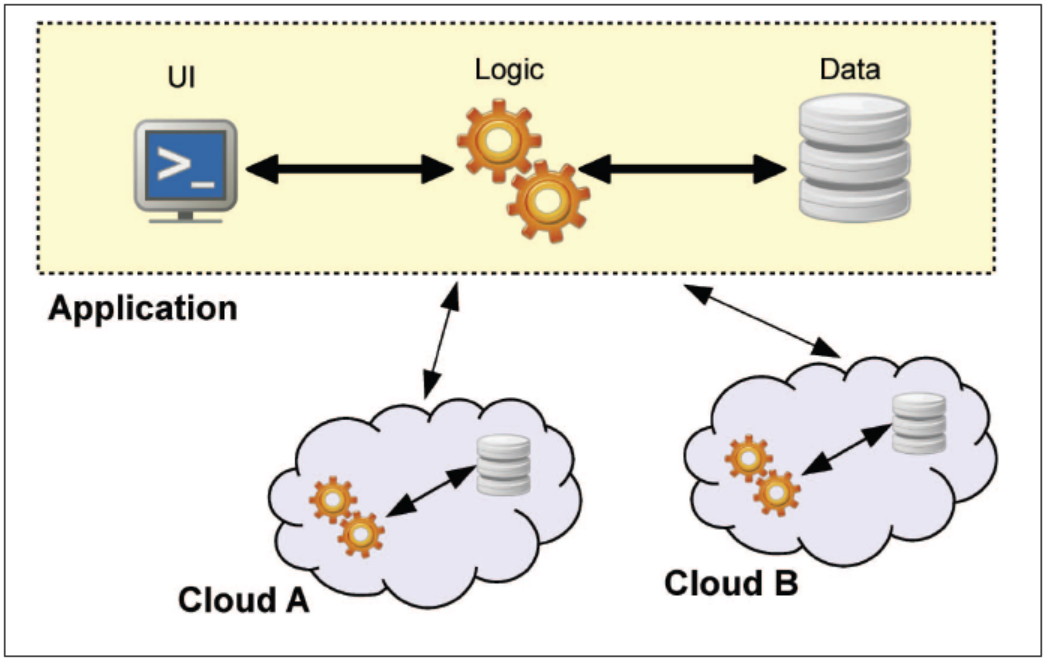
- Replication of application.
- Partition of application system into tiers.
- Partition of application logic into fragments.
- Partition of application data into fragments.

[BOHLI 2013, p3]

Replication of Application

- Allows to receive multiple results from one operation performed in distinct clouds and compare them.

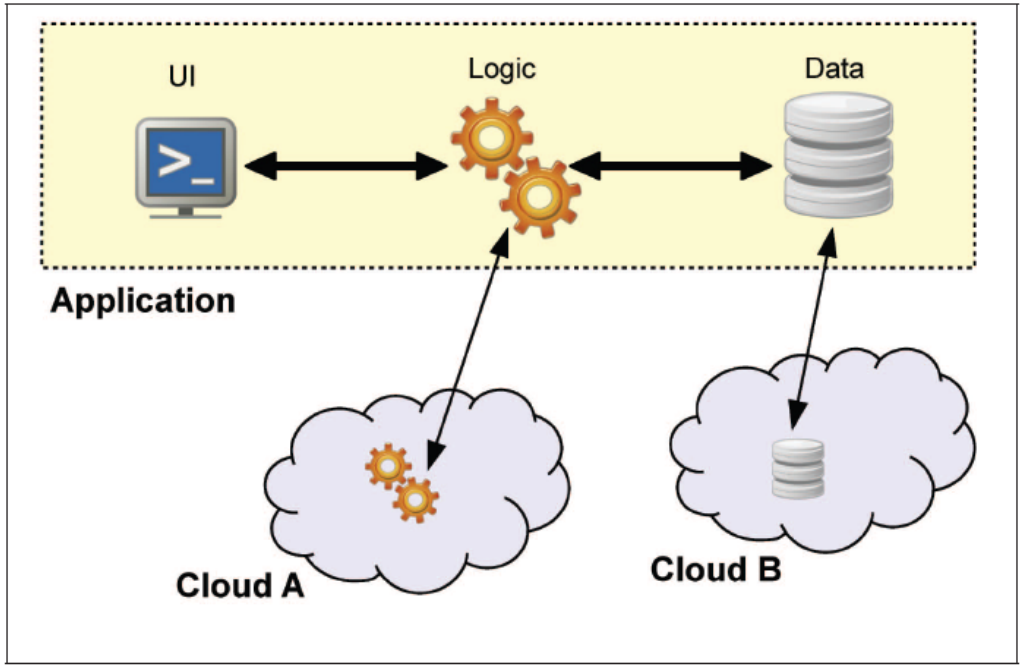
- Integrity of the result.



[BOHLI 2013, p3]

Partition into tiers

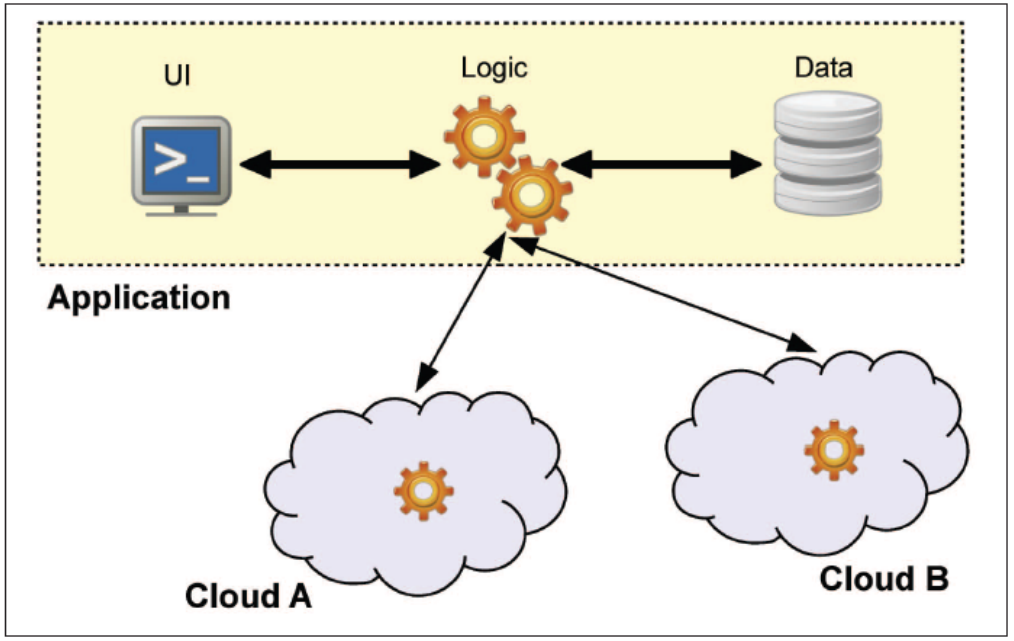
- Allows to separate the logic from the data.
- Additional protection against data leakage due to flaws in application logic.



[BOHLI 2013, p5]

Logic into Fragments

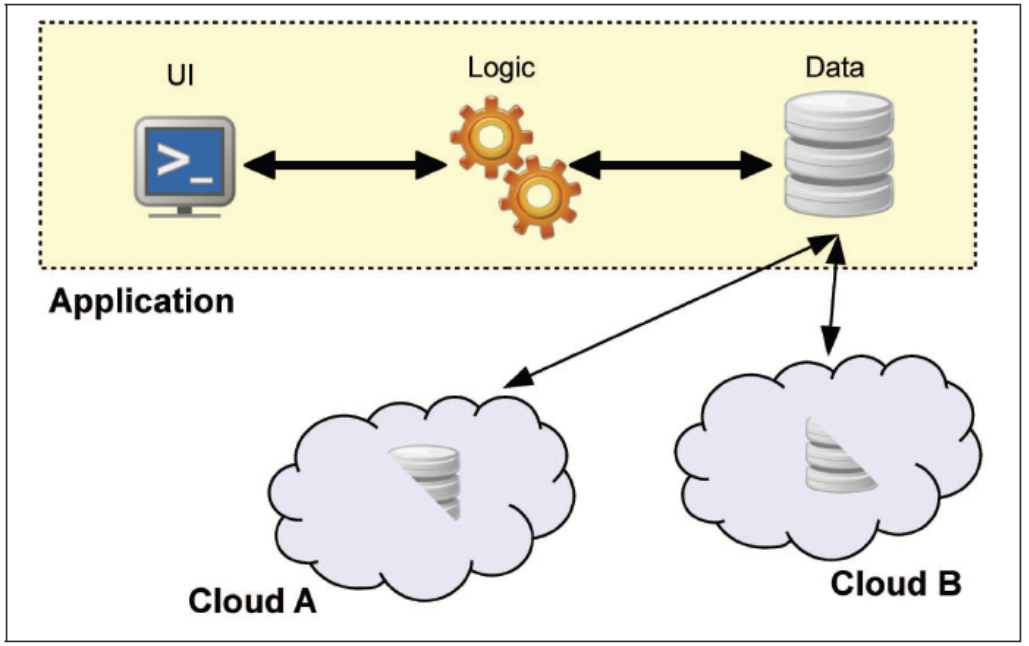
- Allows to distribute the application logic into distinct clouds.
- No cloud provider learns the complete application.
- No cloud provider learns the overall calculated result.



[BOHLI 2013, p5]

Data into Fragments

- Allows distributing fine-grained fragments of data to distinct clouds.
- None of the involved cloud providers gains access to all the data.



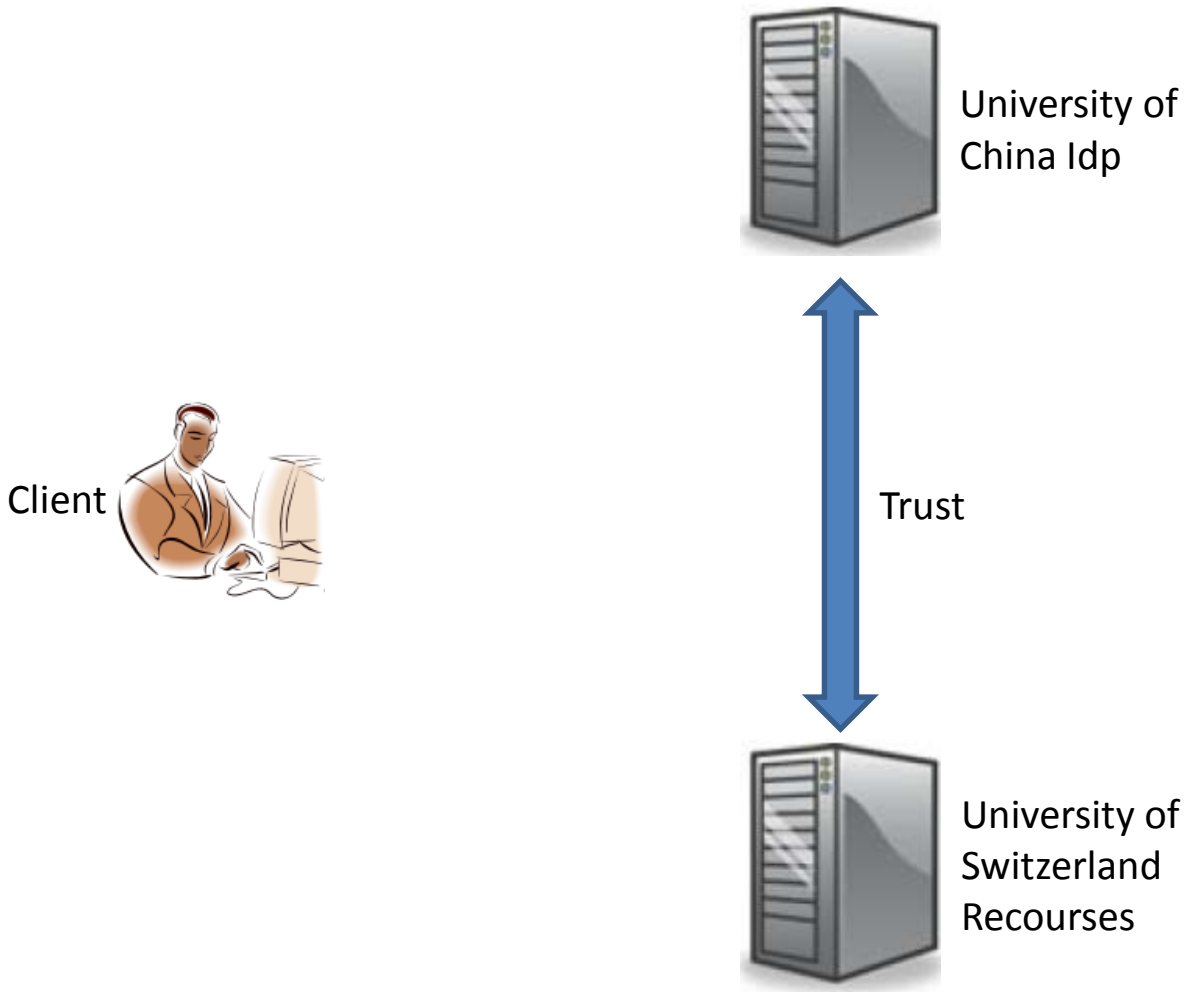
[BOHLI 2013, p7]

Federation

- We imagine a university Professor in physics at University of china that is a part of a multi institute scientific collaboration like CERN, who is collaborating on a new data set.

- He wants to start an analysis program, which dispatches his code to the remote location where data is stored at University of Switzerland. Hence it contacts his identity provider at university of china, in order to get access to University of Switzerland resources that can be used for his simulation.

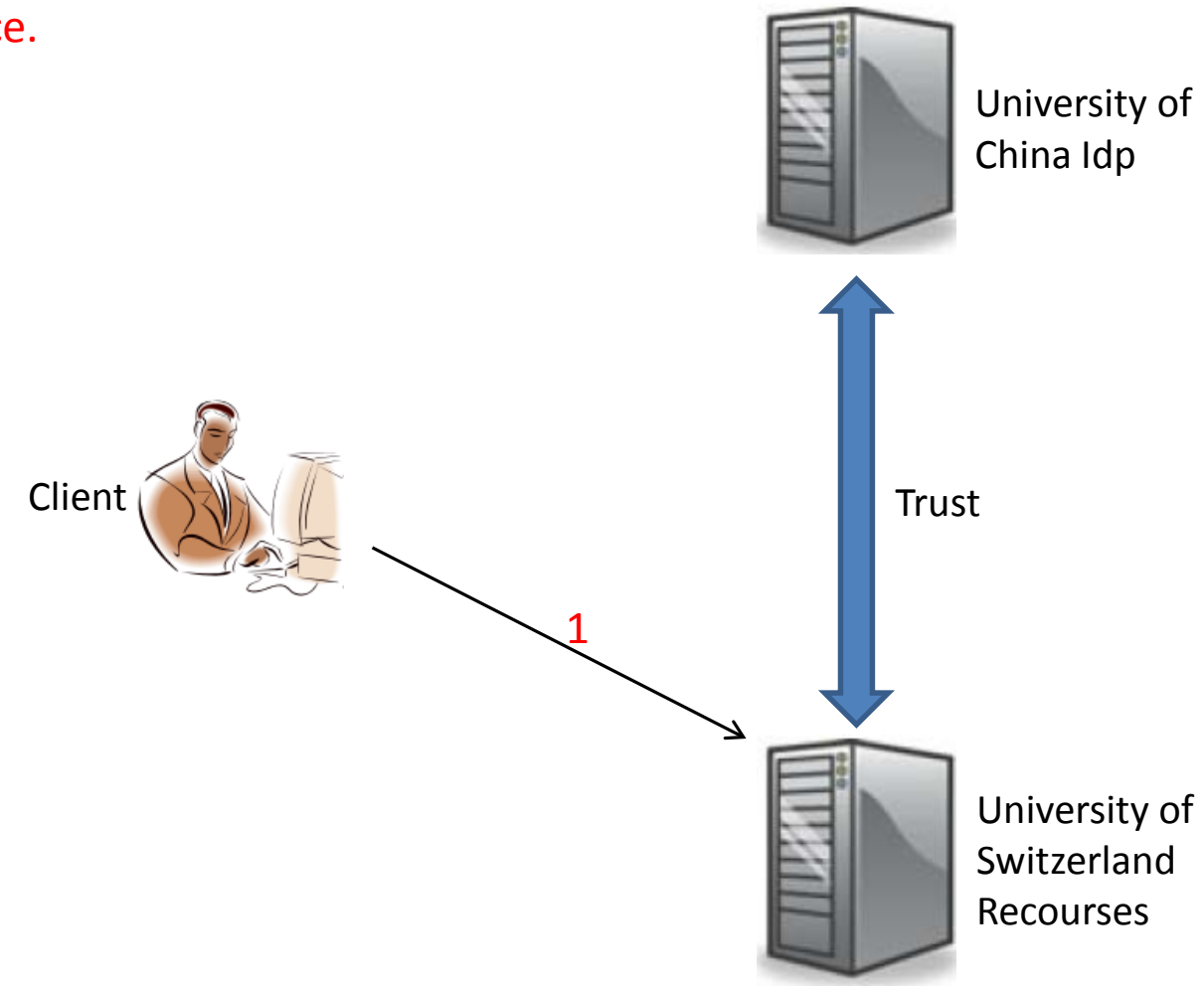
Federation



[CHADWK 2014]

Federation

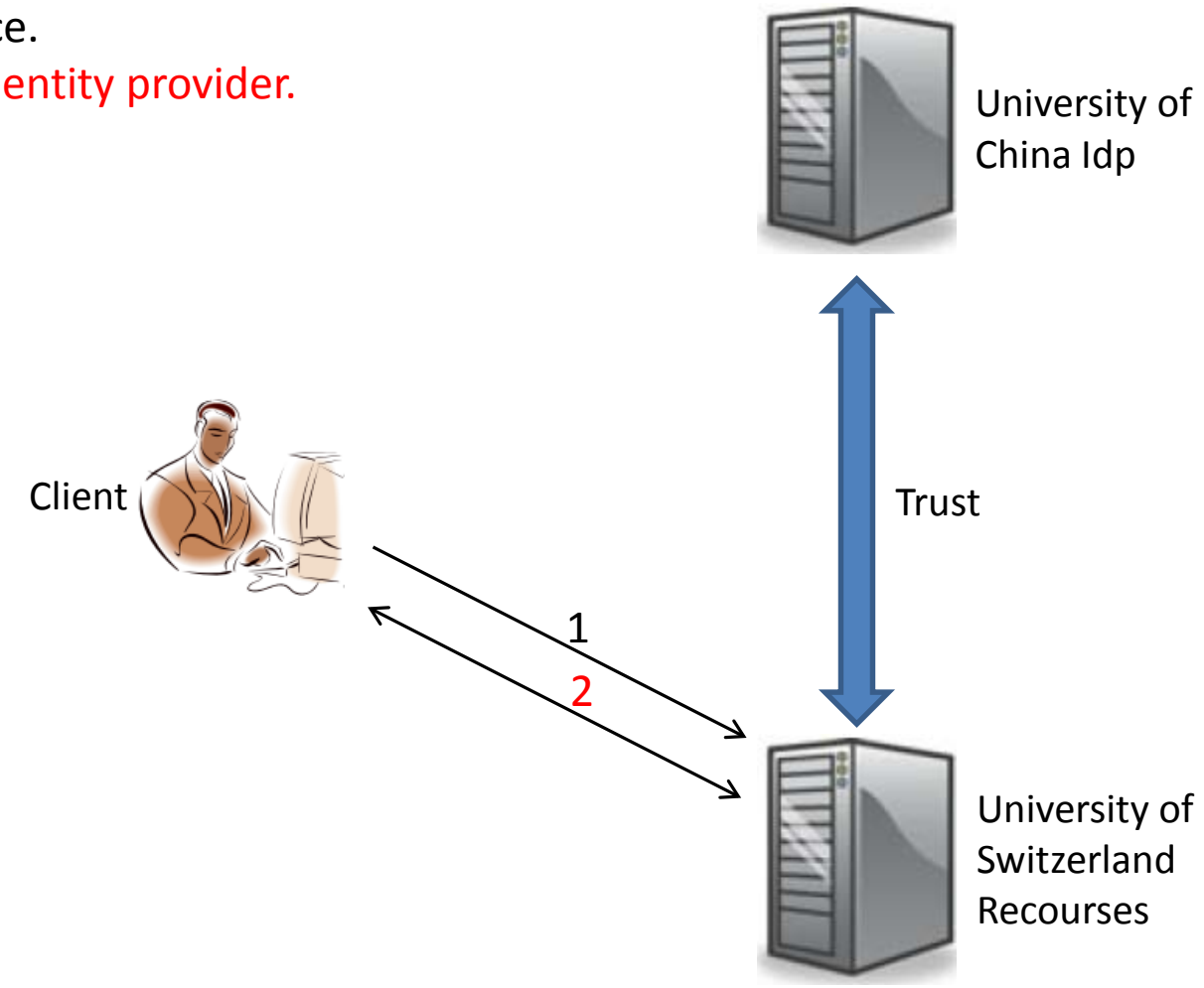
1. Request for a service.



[CHADWK 2014]

Federation

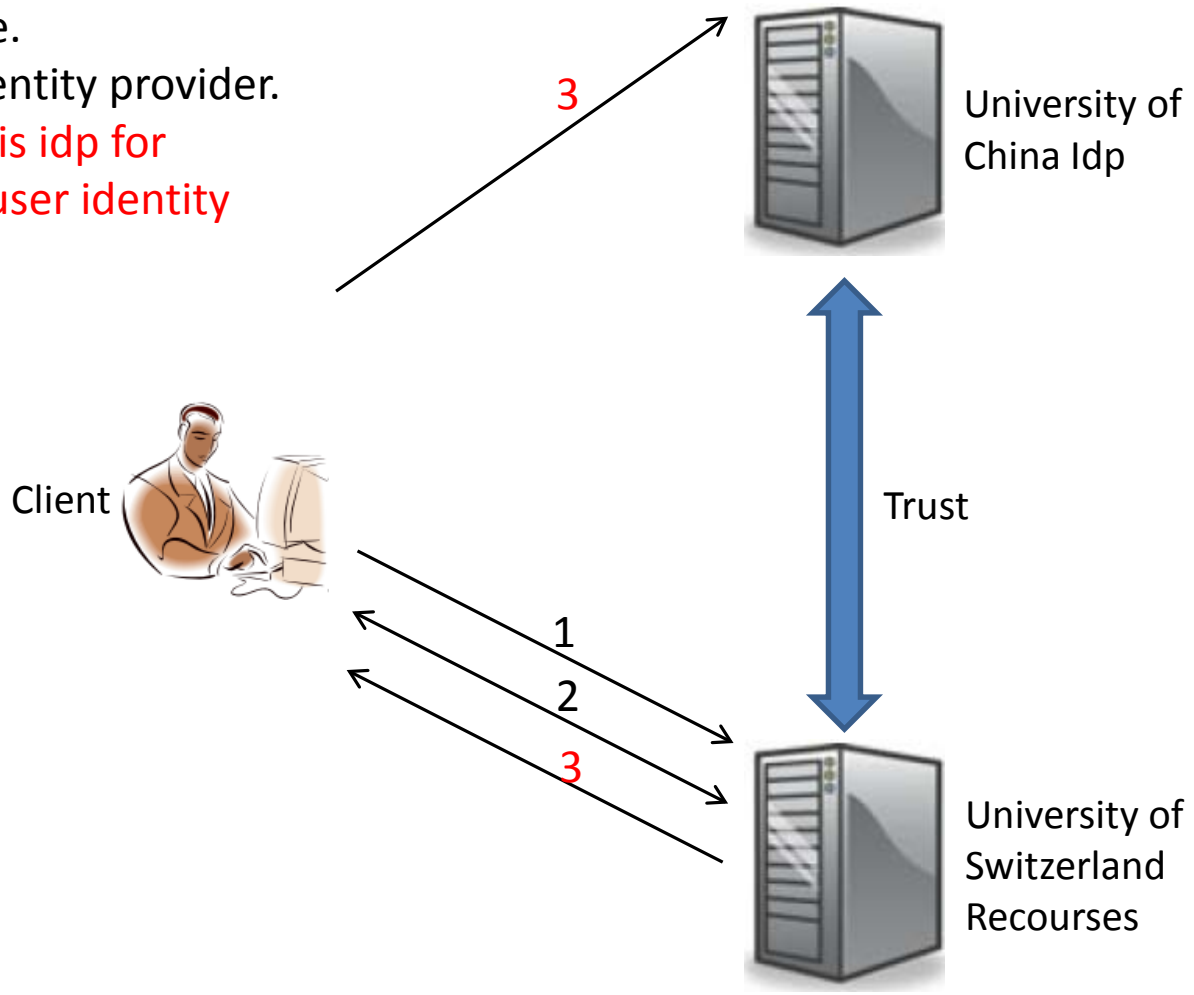
1. Request for a service.
2. Determine user's identity provider.



[CHADWK 2014]

Federation

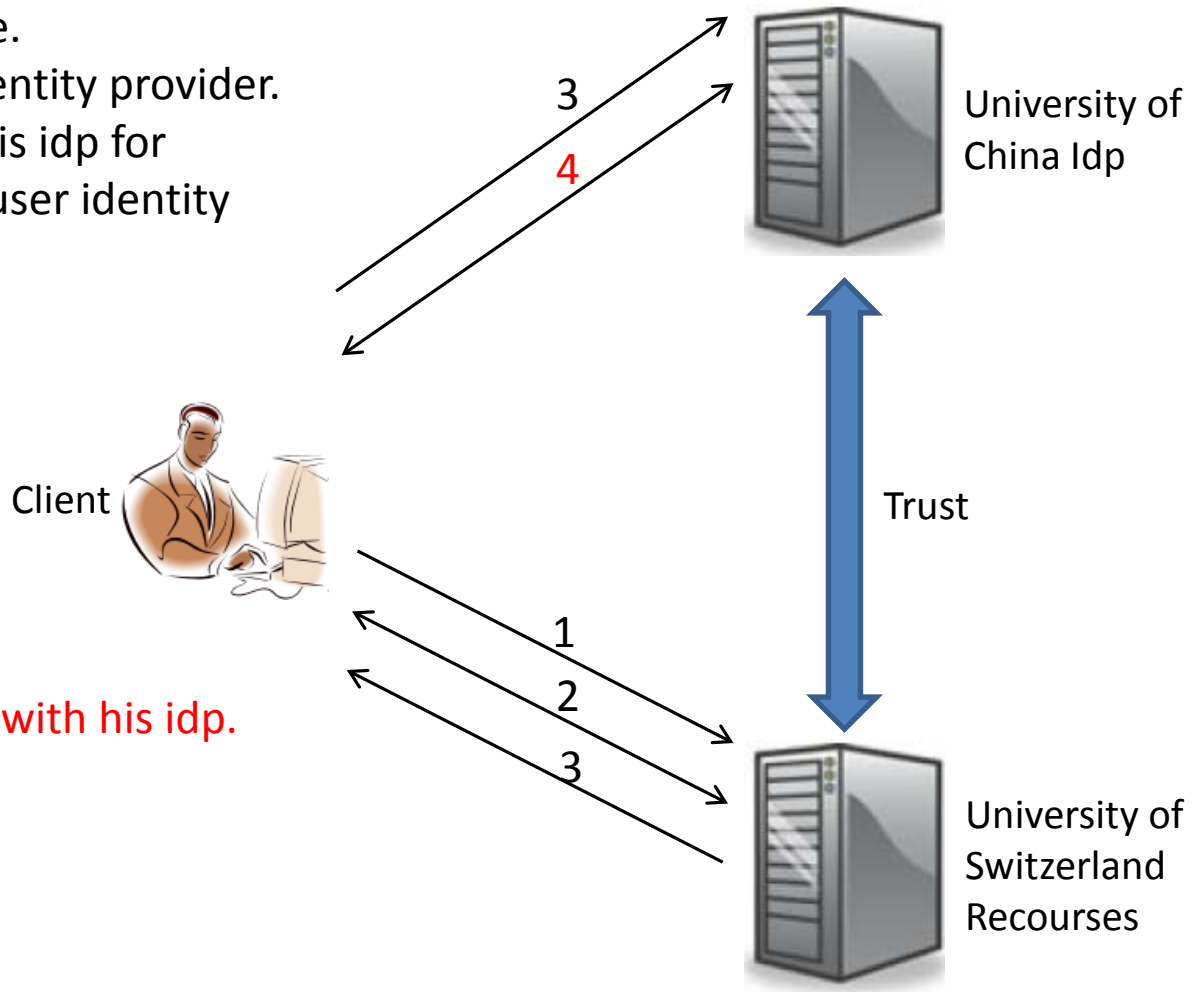
1. Request for a service.
2. Determine user's identity provider.
3. SP redirect user to his idp for authentication and user identity attributes.



[CHADWK 2014]

Federation

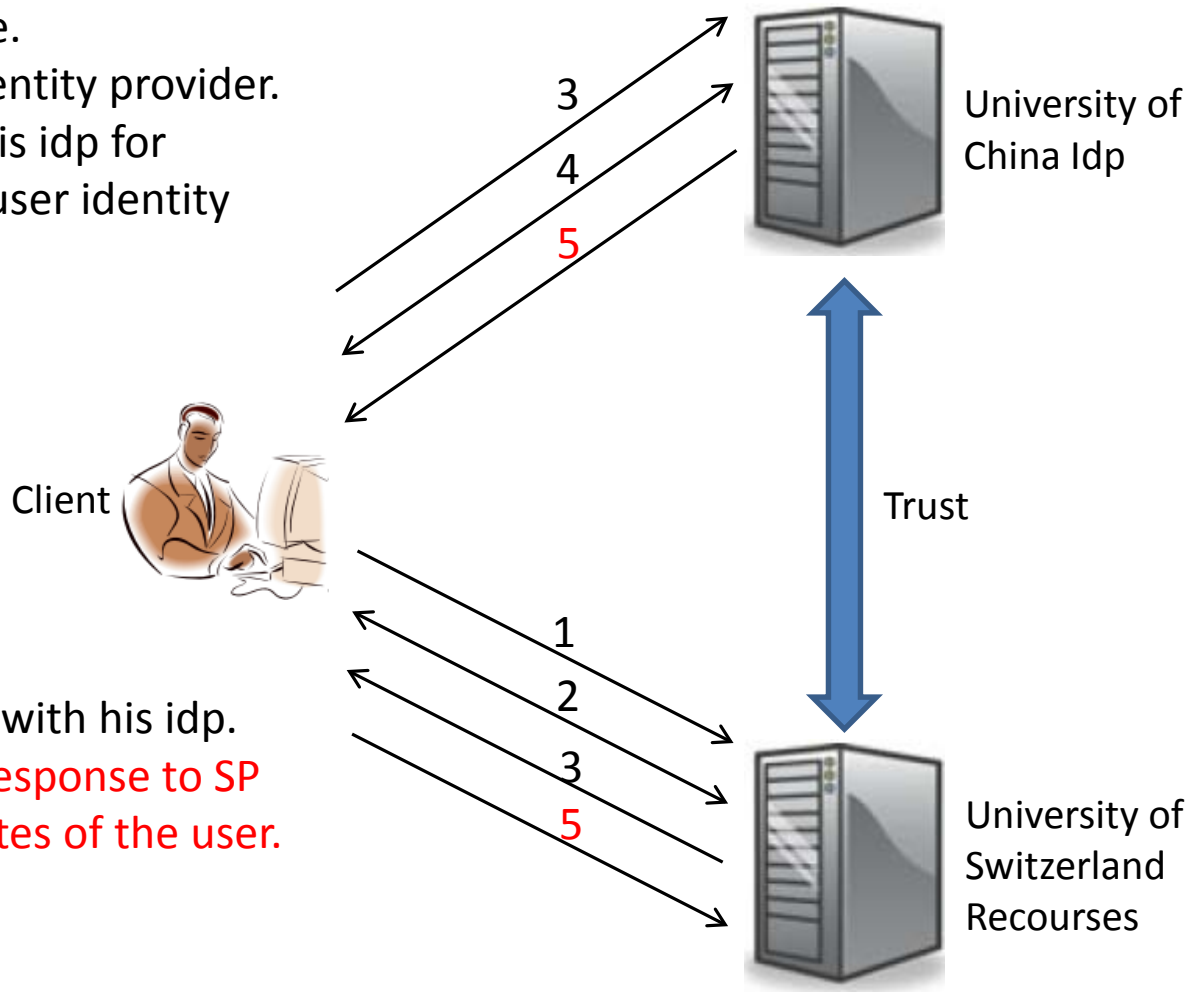
1. Request for a service.
2. Determine user's identity provider.
3. SP redirect user to his idp for authentication and user identity attributes.
4. User authentication with his idp.



[CHADWK 2014]

Federation

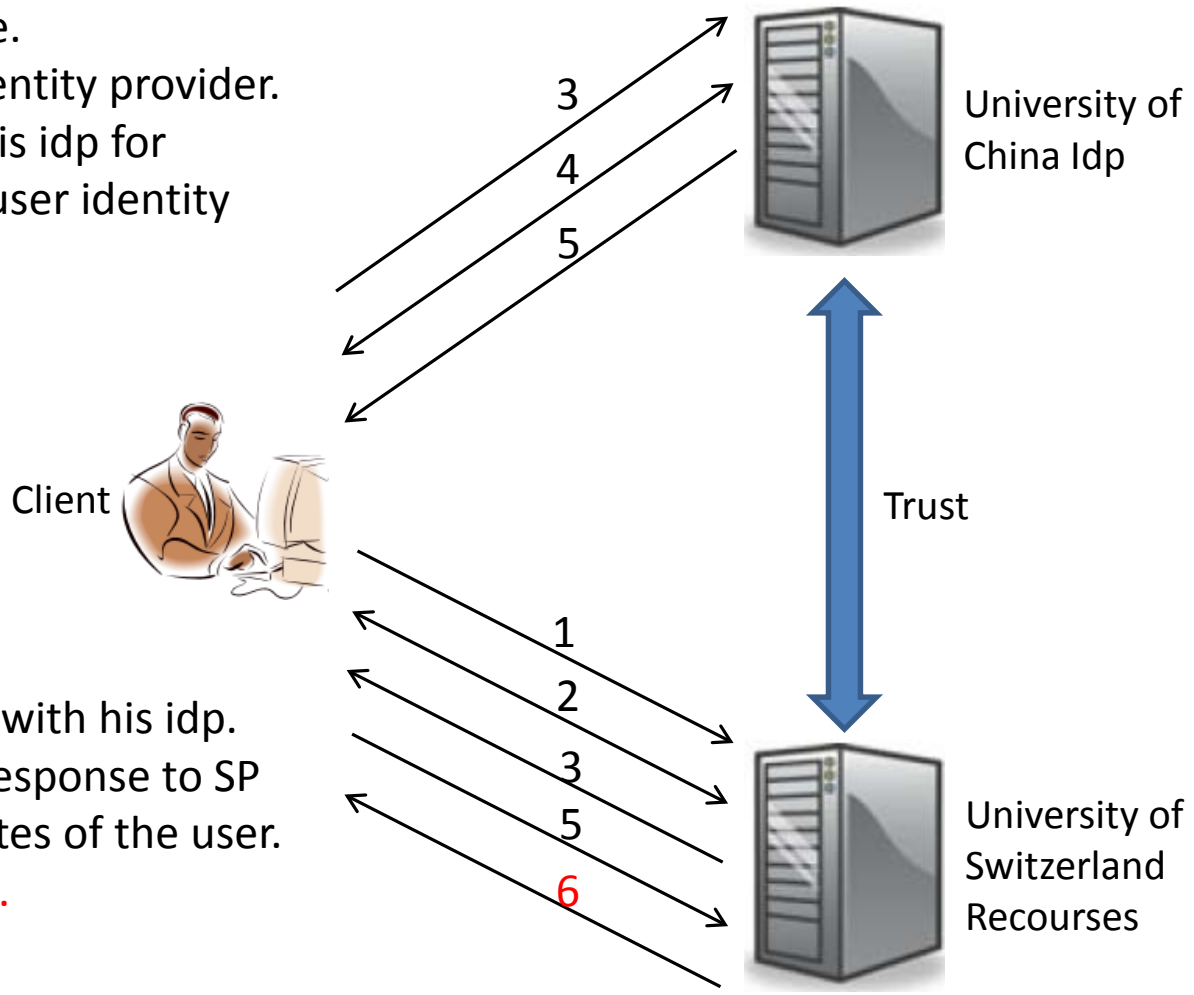
1. Request for a service.
2. Determine user's identity provider.
3. SP redirect user to his idp for authentication and user identity attributes.
4. User authentication with his idp.
5. Idp authentication response to SP with identity attributes of the user.



[CHADWK 2014]

Federation

1. Request for a service.
2. Determine user's identity provider.
3. SP redirect user to his idp for authentication and user identity attributes.

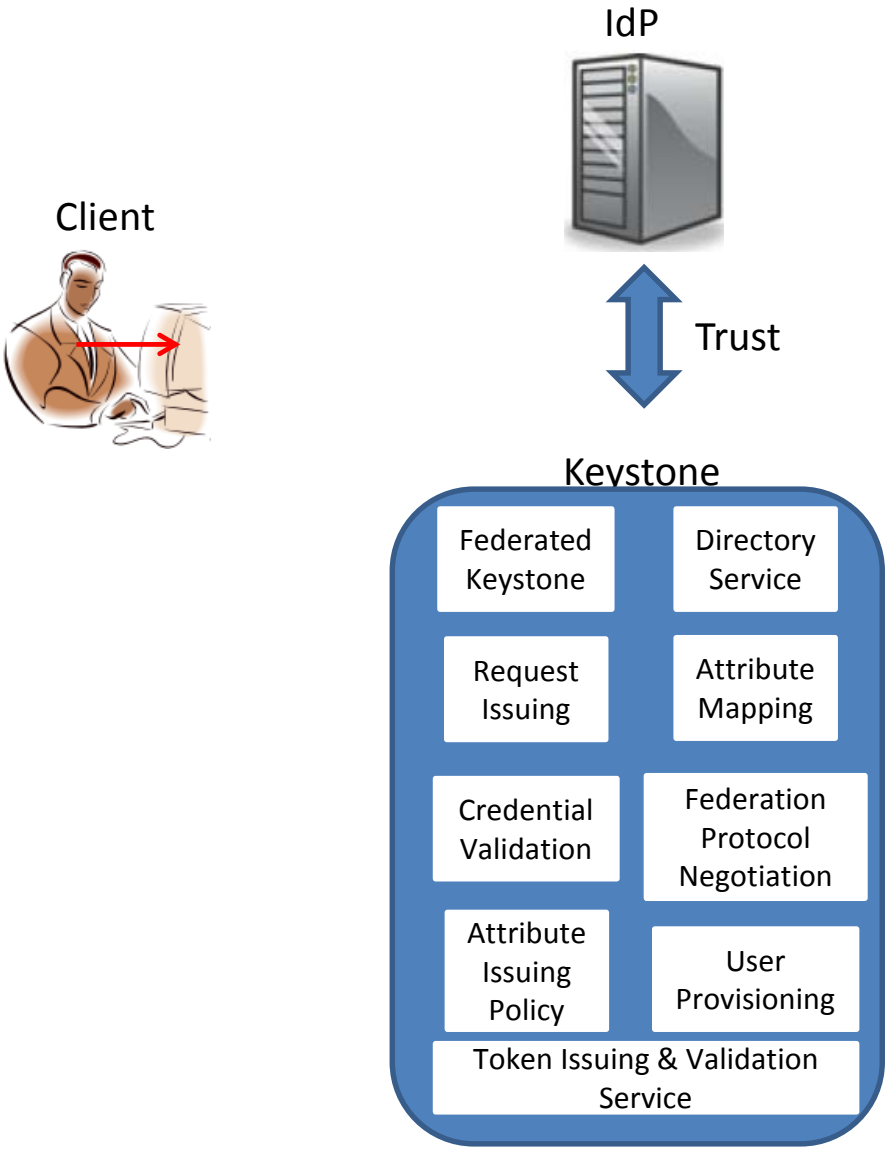


4. User authentication with his idp.
5. Idp authentication response to SP with identity attributes of the user.
6. Access the resource.

[CHADWK 2014]

Federation Protocol Sequence

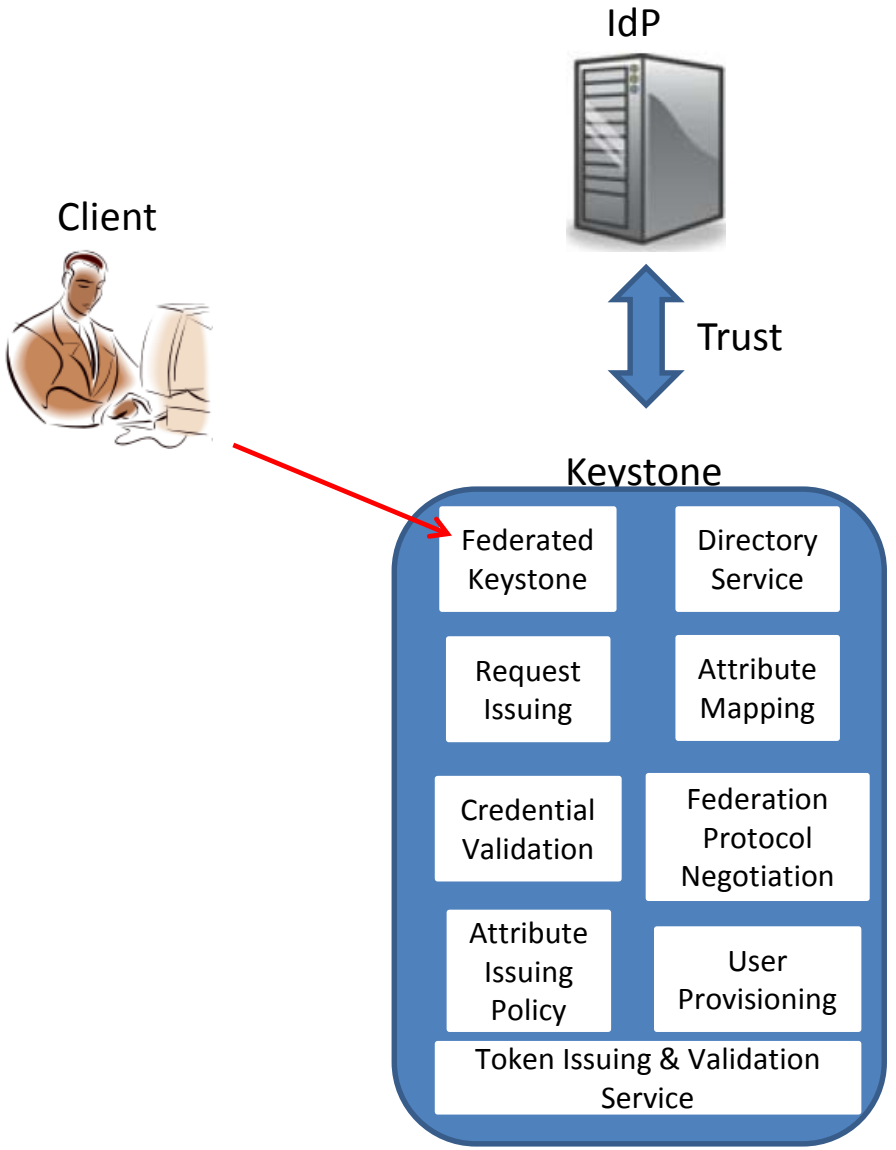
1. User calling the client for federated log in, giving it the address of the keystone service.



[CHADWK 2014]

Federation Protocol Sequence

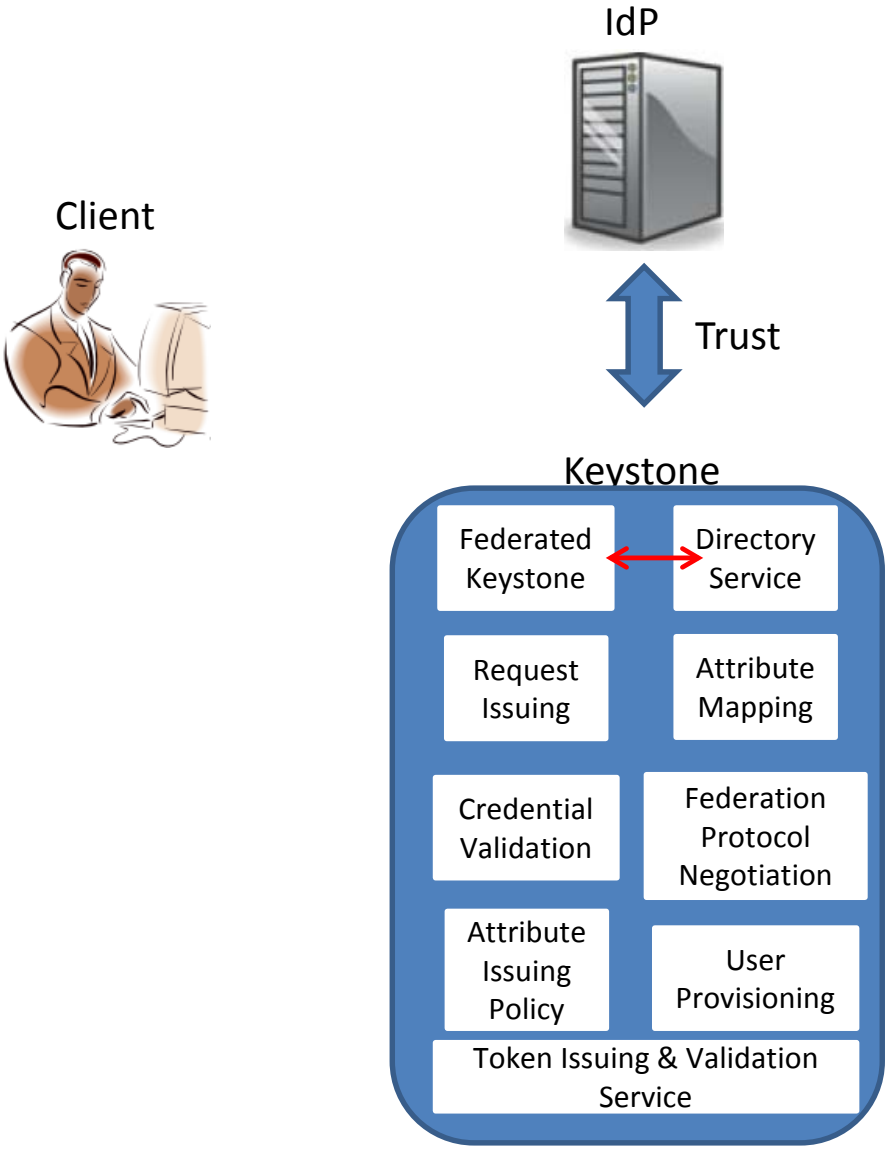
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.



[CHADWK 2014]

Federation Protocol Sequence

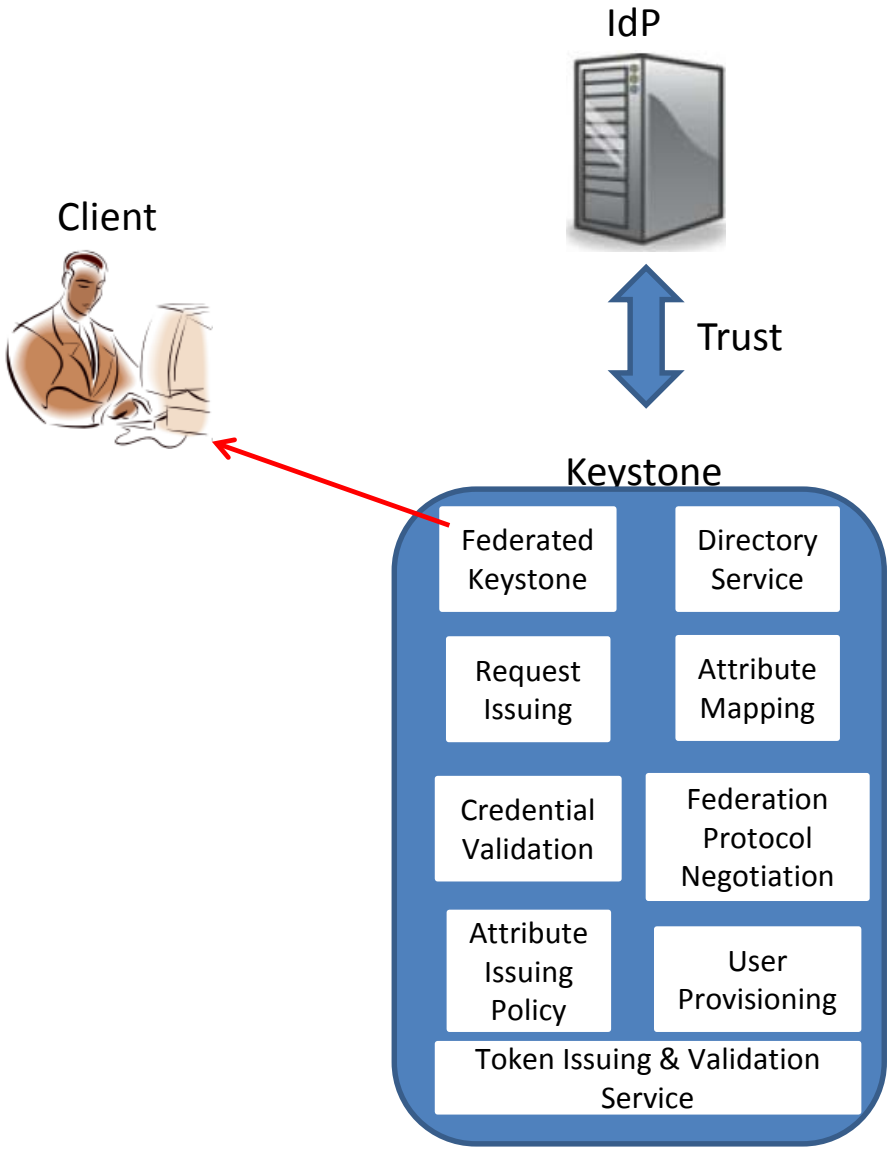
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.



[CHADWK 2014]

Federation Protocol Sequence

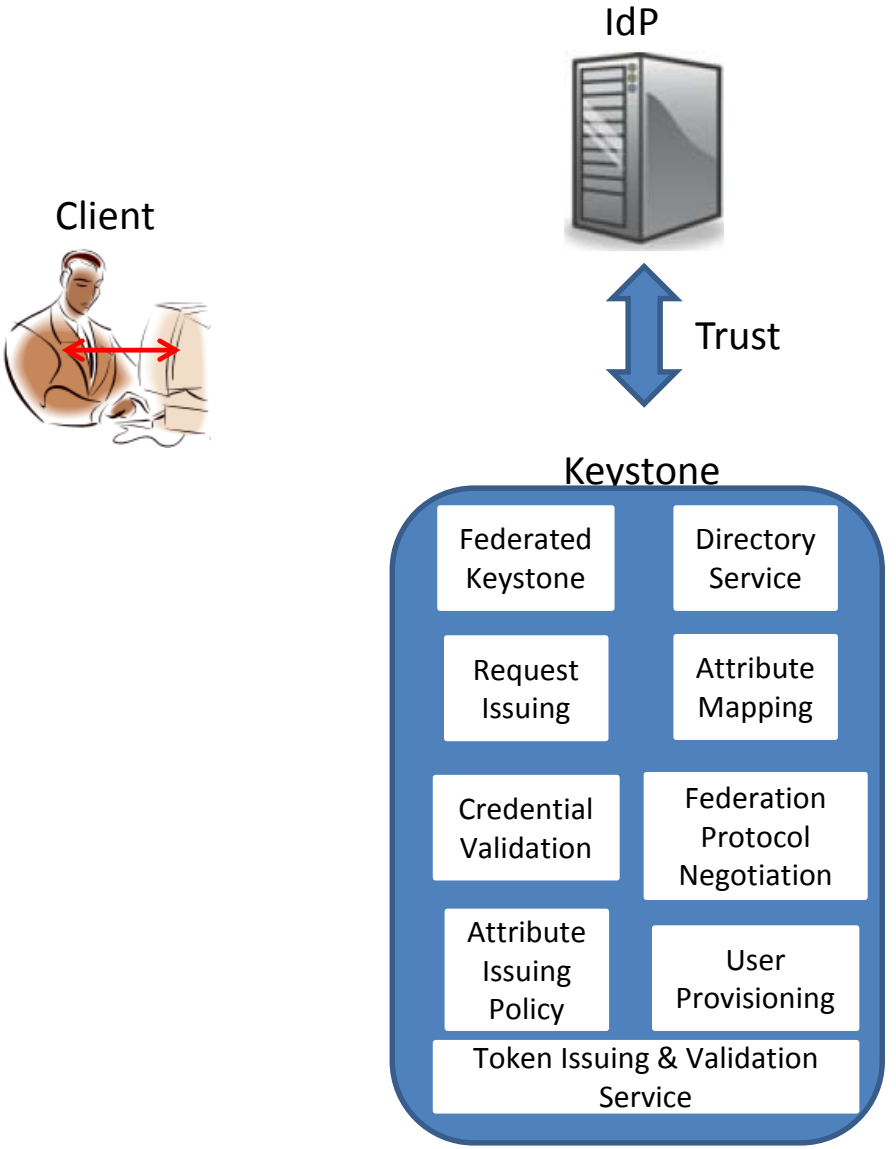
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.



[CHADWK 2014]

Federation Protocol Sequence

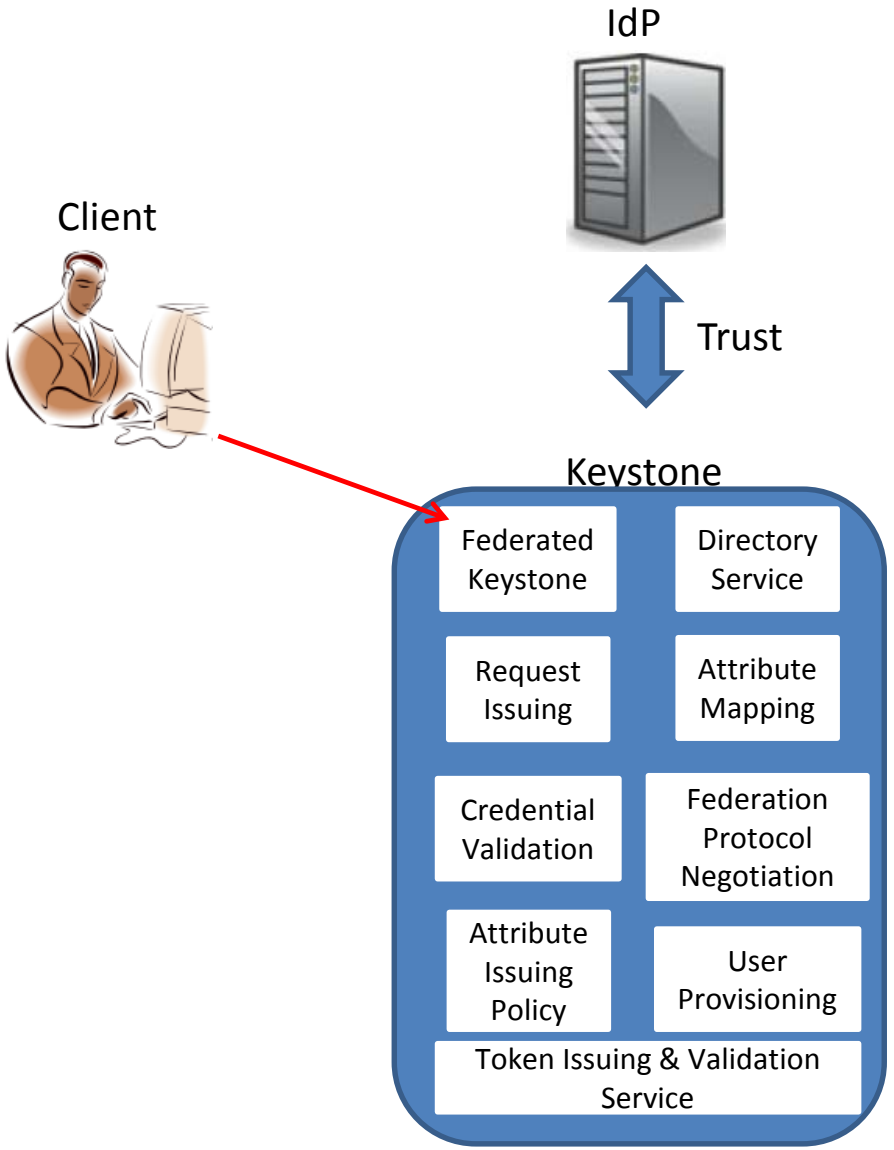
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.
5. User chooses the idp.



[CHADWK 2014]

Federation Protocol Sequence

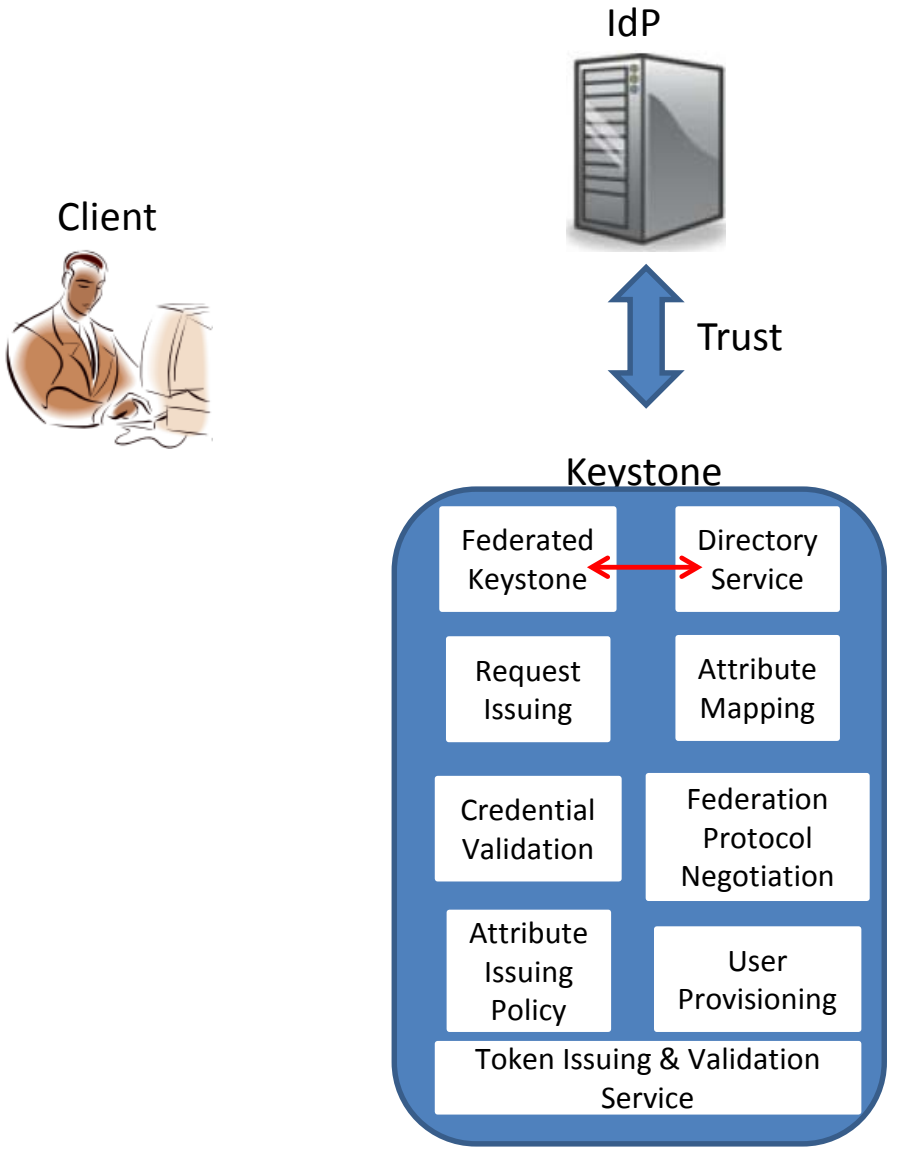
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.
5. User chooses the idp.
6. The client returns the chosen idp and asks an Idp request message.



[CHADWK 2014]

Federation Protocol Sequence

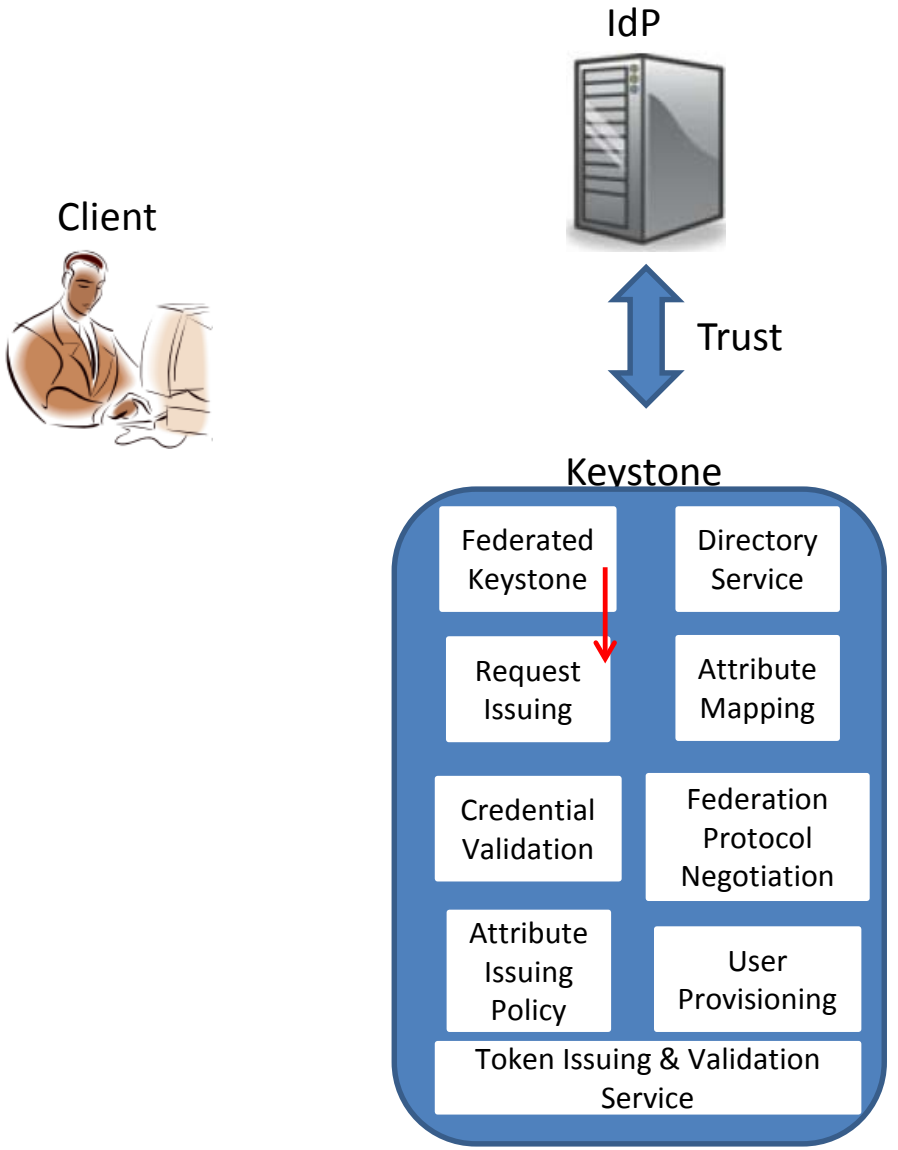
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.
5. User chooses the idp.
6. The client returns the chosen idp and asks an Idp request message.
7. Keystone look up the identity provider for its protocol.



[CHADWK 2014]

Federation Protocol Sequence

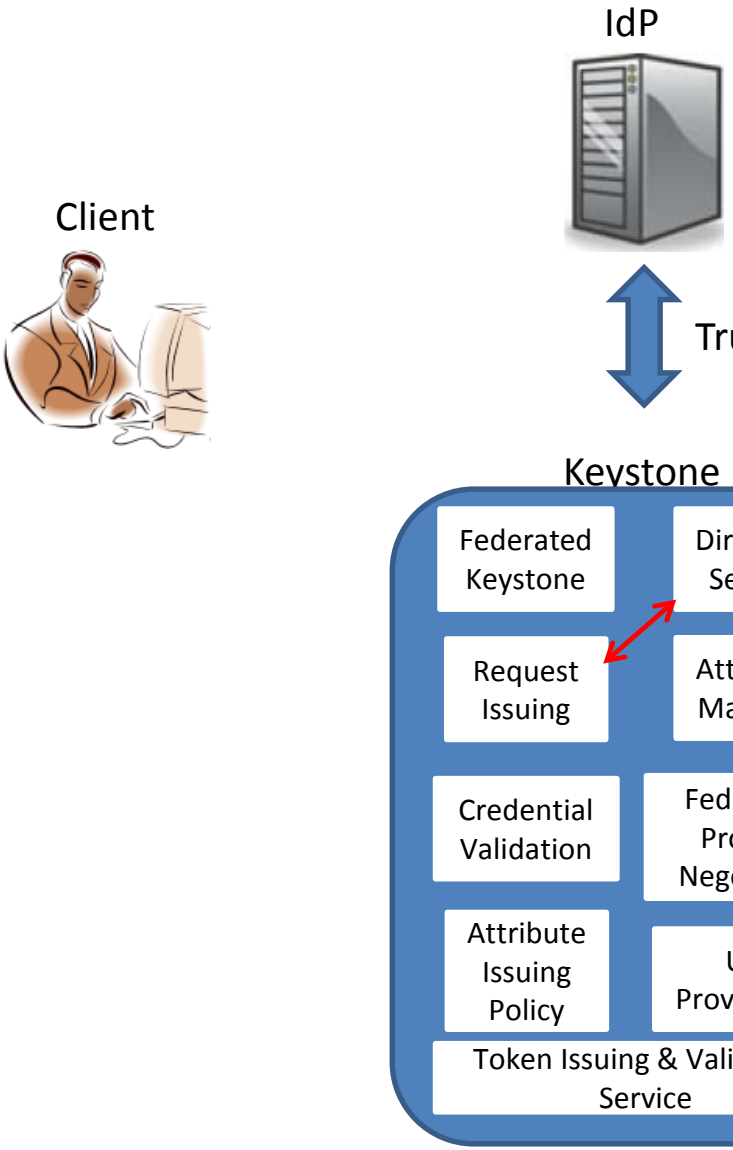
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.
5. User chooses the idp.
6. The client returns the chosen idp and asks an Idp request message.
7. Keystone look up the identity provider for its protocol.
8. Keystone asks RI for appropriate format of authentication and attribute request.



[CHADWK 2014]

Federation Protocol Sequence

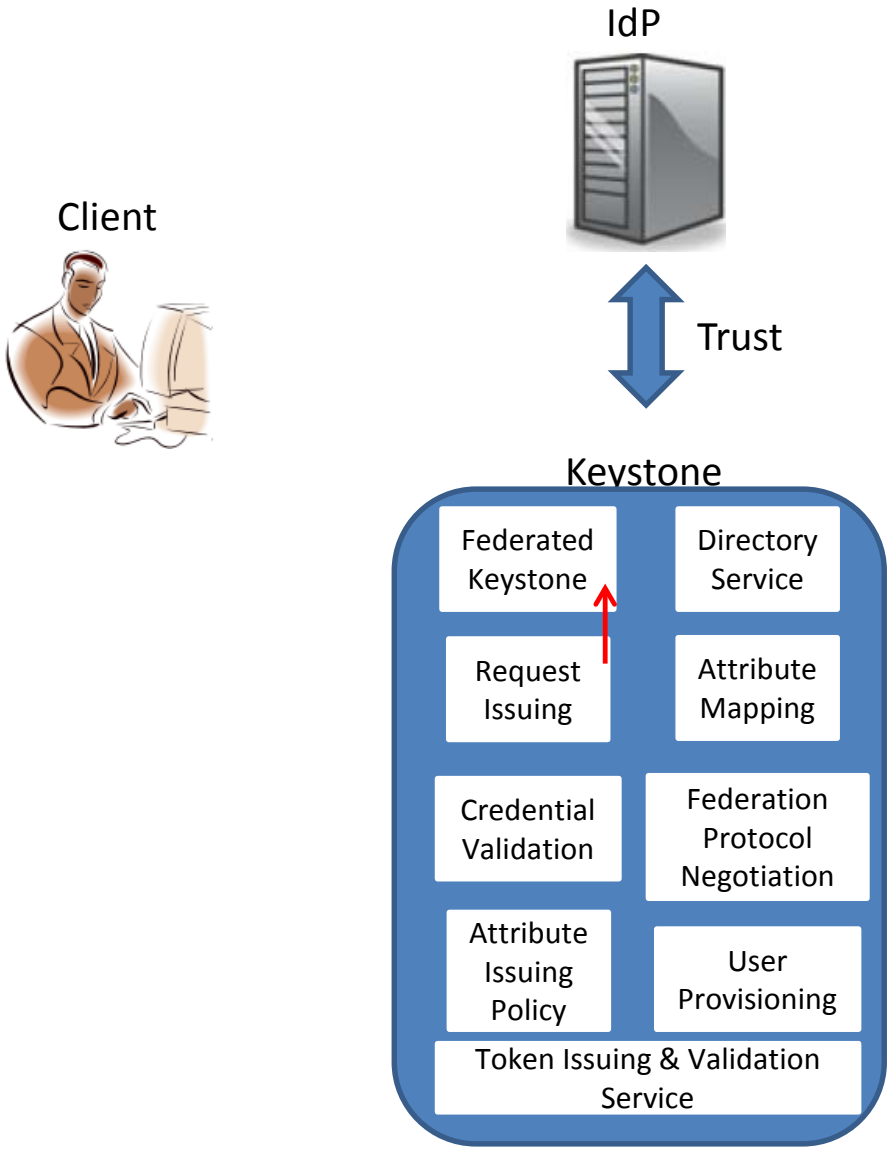
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.
5. User chooses the idp.
6. The client returns the chosen idp and asks an Idp request message.
7. Keystone look up the identity provider for its protocol.
8. Keystone asks RI for appropriate format of authentication and attribute request.
9. RI make request to Directory Service to obtain Idp metadata.



[CHADWK 2014]

Federation Protocol Sequence

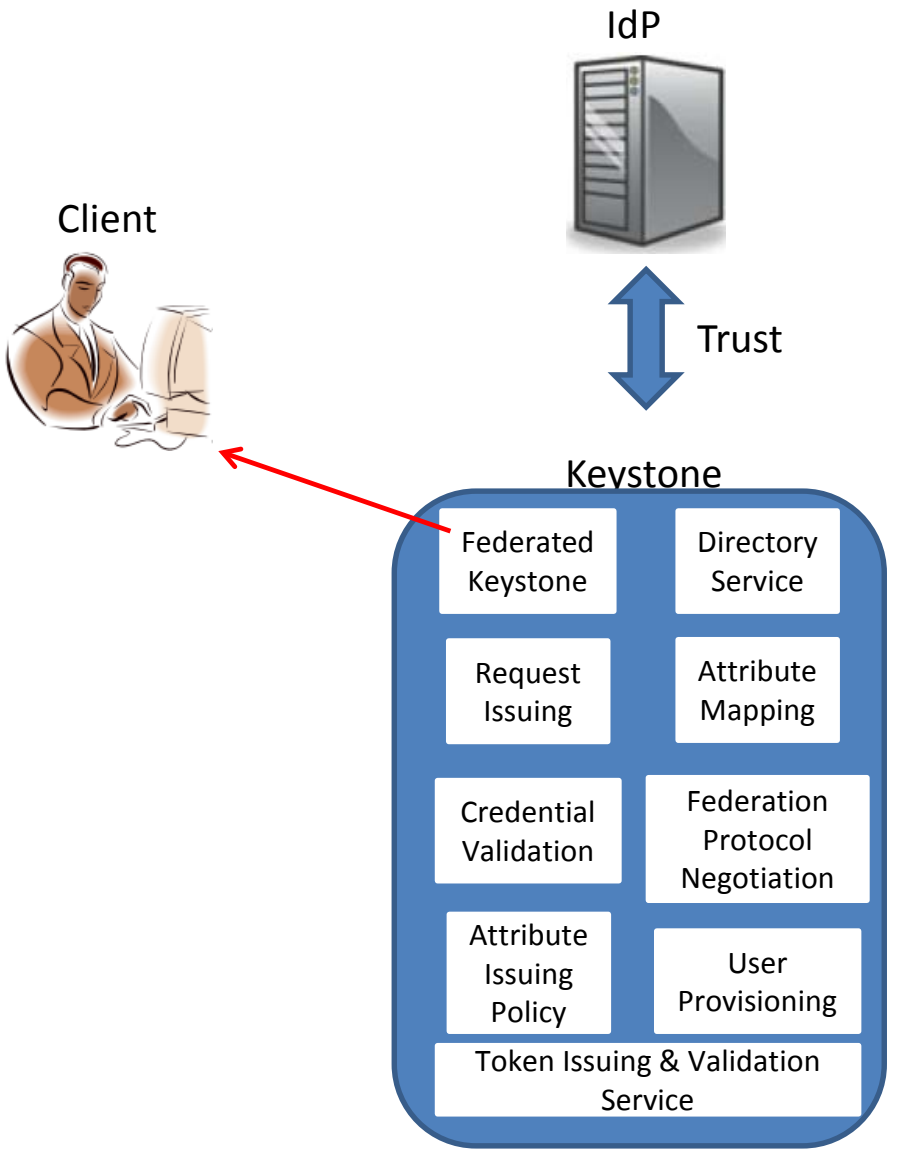
1. User calling the client for federated log in, giving it the address of the keystone service.
2. The client calls the federated keystone for the list of IdPs.
3. Keystone Calls Directory Service to obtain the list of federation IdPs.
4. Keystone sends the set of idps back to the client.
5. User chooses the idp.
6. The client returns the chosen idp and asks an Idp request message.
7. Keystone look up the identity provider for its protocol.
8. Keystone asks RI for appropriate format of authentication and attribute request.
9. RI make request to Directory Service to obtain Idp metadata.
10. RI returns Idp message to keystone.



[CHADWK 2014]

Federation Protocol Sequence

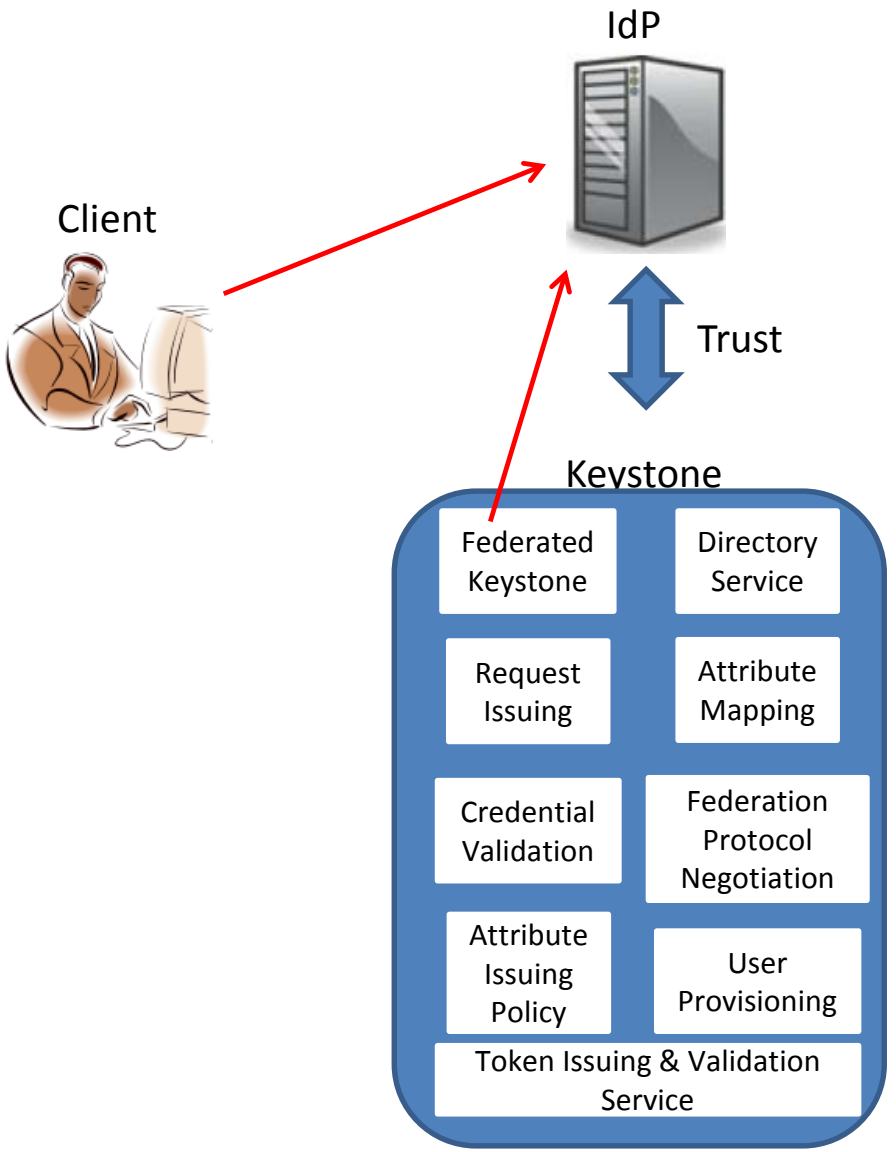
11. Keystone returns the request message to client.



[CHADWK 2014]

Federation Protocol Sequence

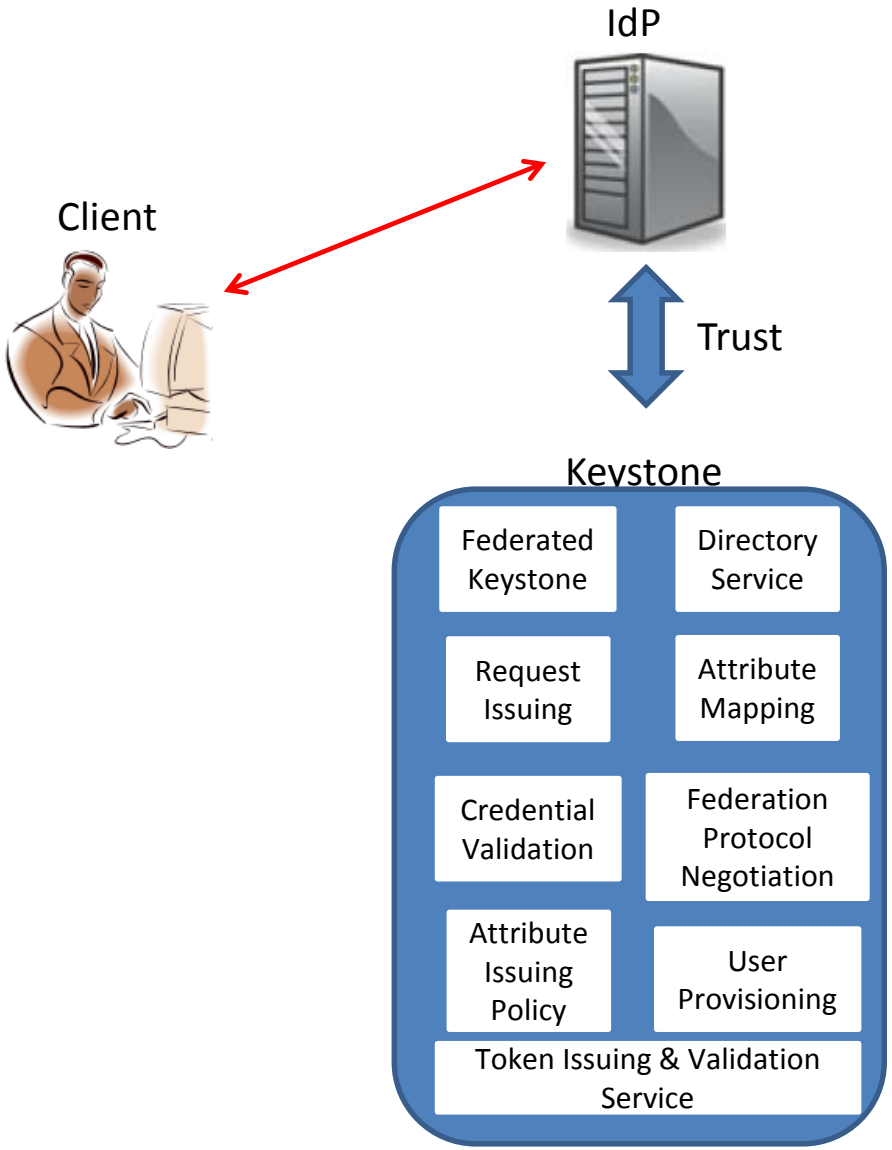
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.



[CHADWK 2014]

Federation Protocol Sequence

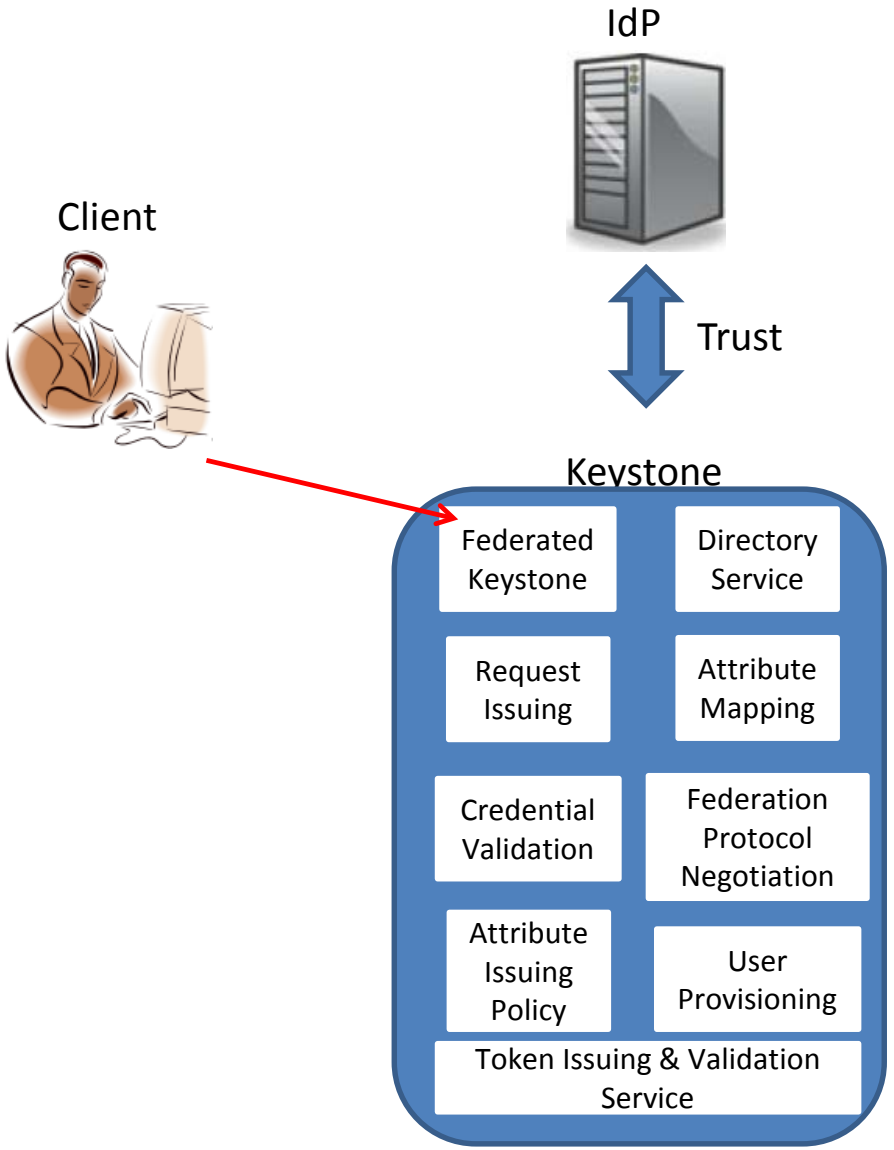
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.



[CHADWK 2014]

Federation Protocol Sequence

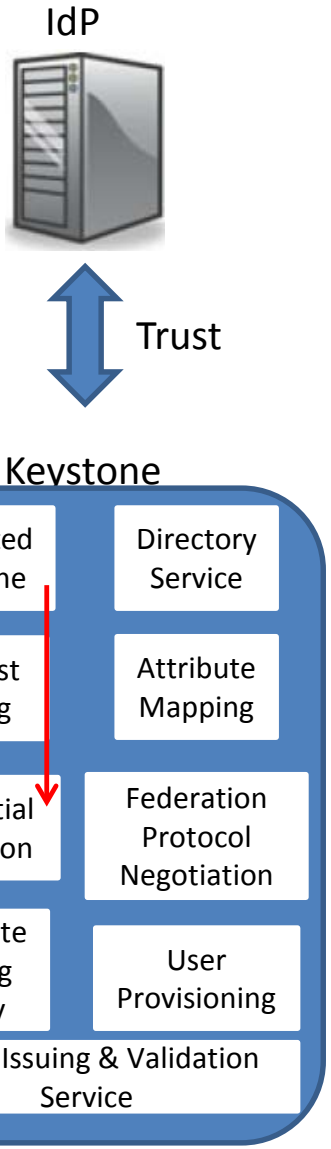
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.
14. Client passes the Idps response to keystone.



[CHADWK 2014]

Federation Protocol Sequence

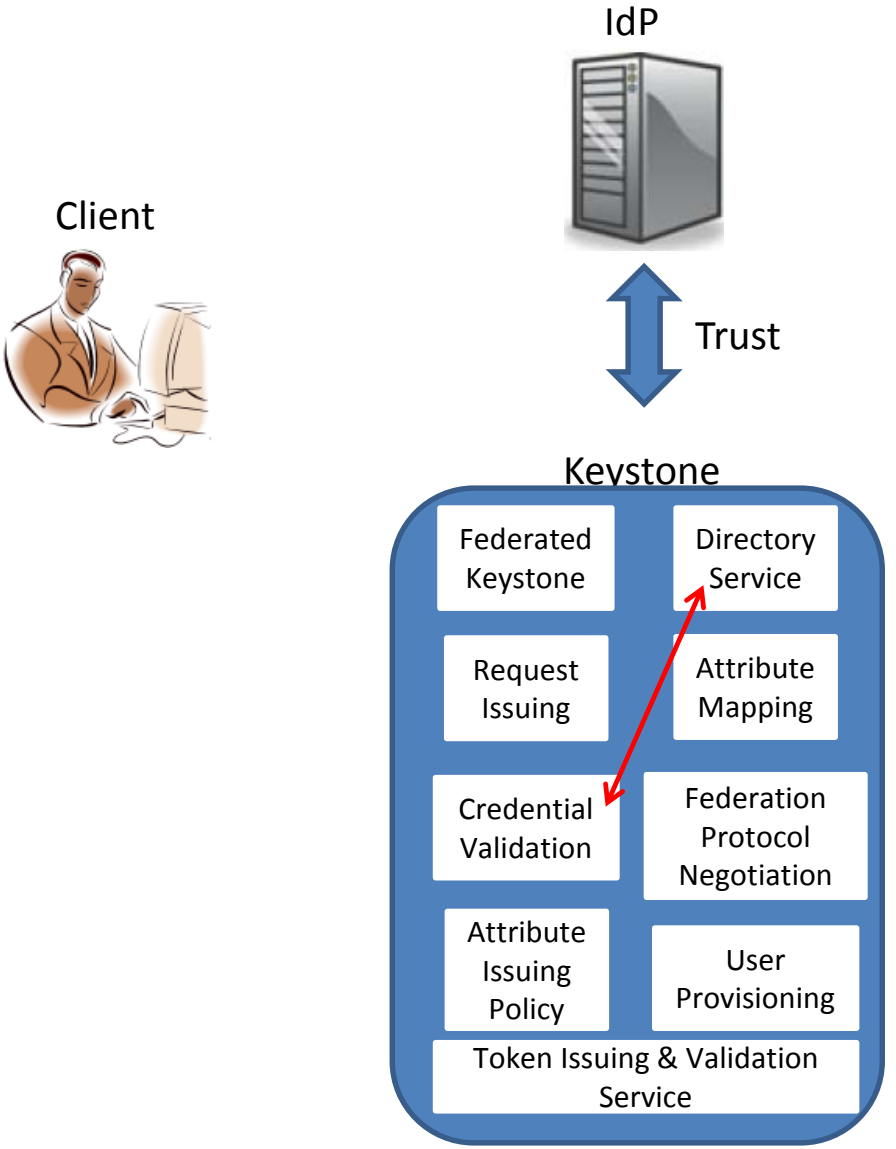
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.
14. Client passes the Idps response to keystone.
15. Keystone passes the response to the credential validation function.



[CHADWK 2014]

Federation Protocol Sequence

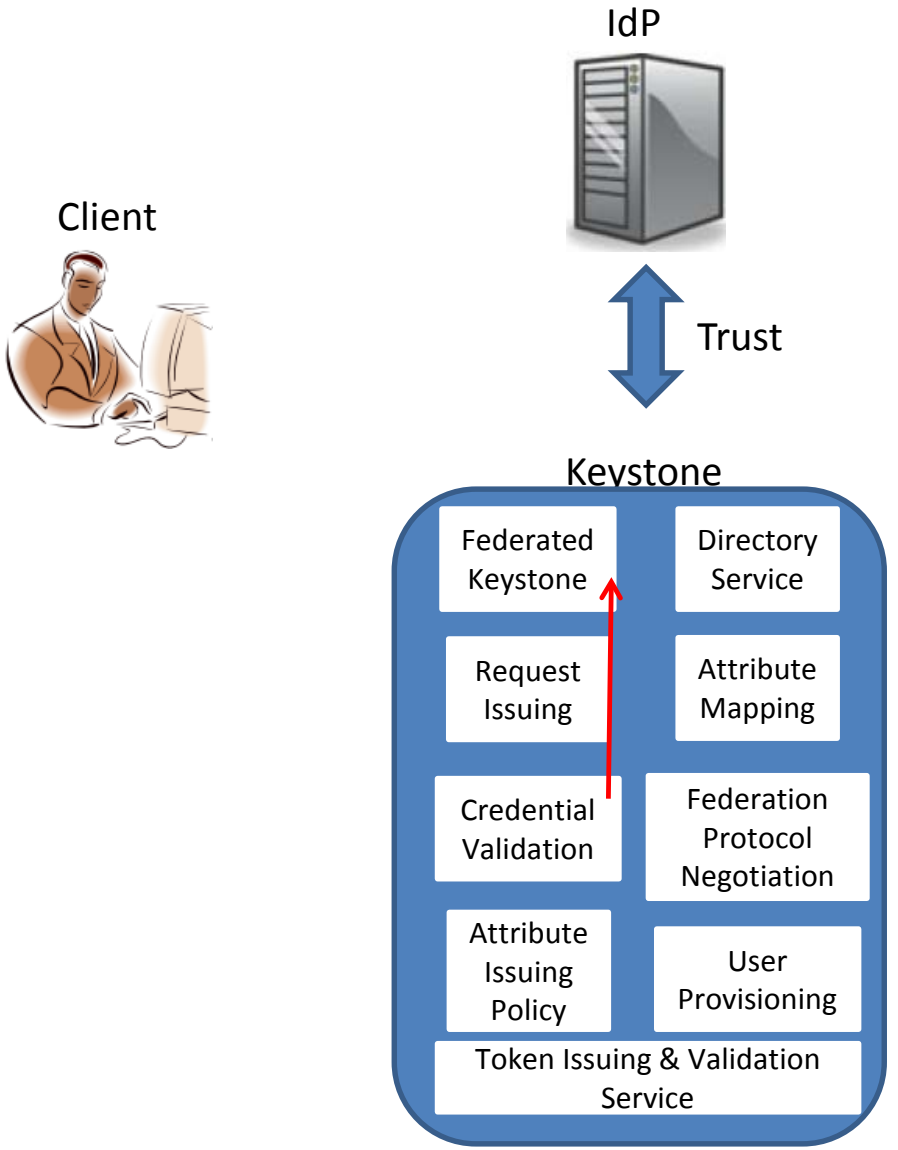
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.
14. Client passes the Idps response to keystone.
15. Keystone passes the response to the credential validation function.
16. Credential validation calls directory to obtain metadata to validate the response.



[CHADWK 2014]

Federation Protocol Sequence

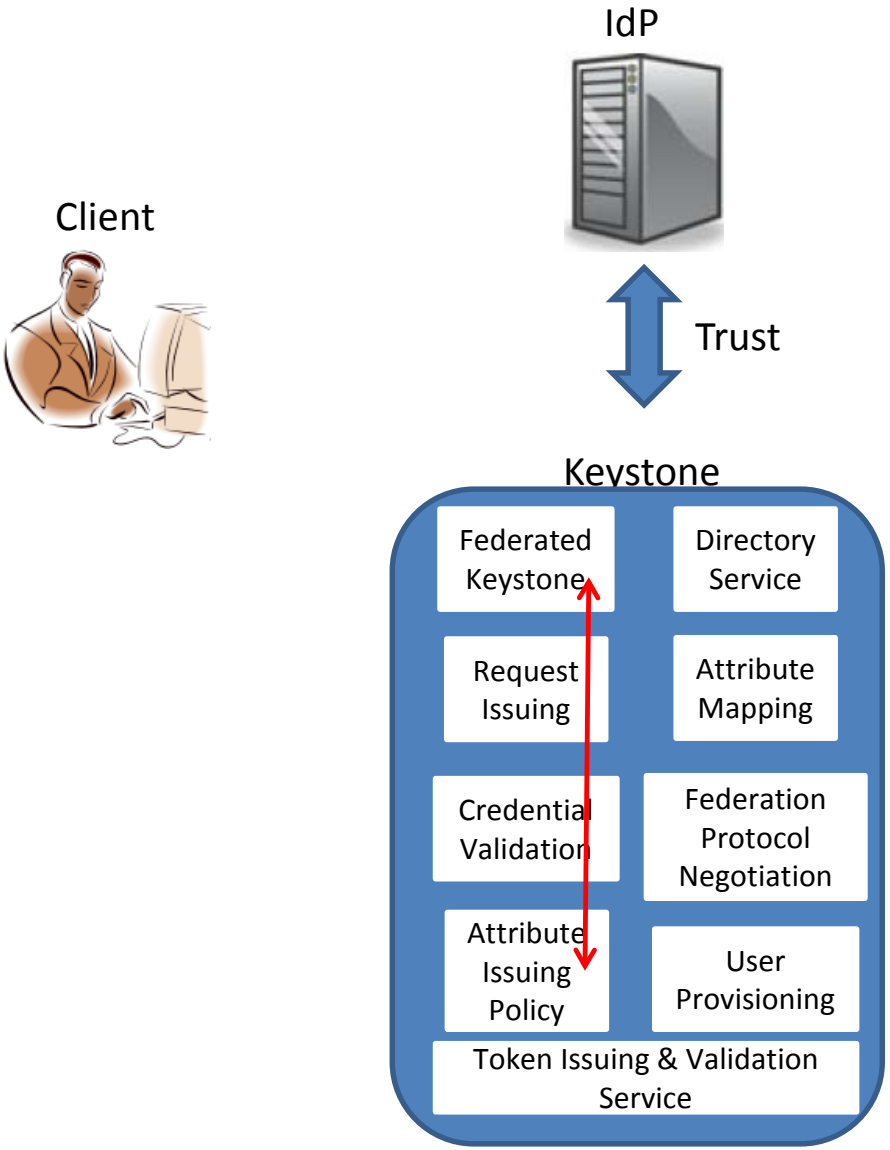
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.
14. Client passes the Idps response to keystone.
15. Keystone passes the response to the credential validation function.
16. Credential validation calls directory to obtain metadata to validate the response.
17. Credential validation returns the user's ID, set of identity attributes and idp to keystone.



[CHADWK 2014]

Federation Protocol Sequence

11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.
14. Client passes the Idps response to keystone.
15. Keystone passes the response to the credential validation function.
16. Credential validation calls directory to obtain metadata to validate the response.
17. Credential validation returns the user's ID, set of identity attributes and idp to keystone.
18. Keystone checks with Attribute Issuer Policy to ensure only allowed attributes asserted by Idp.

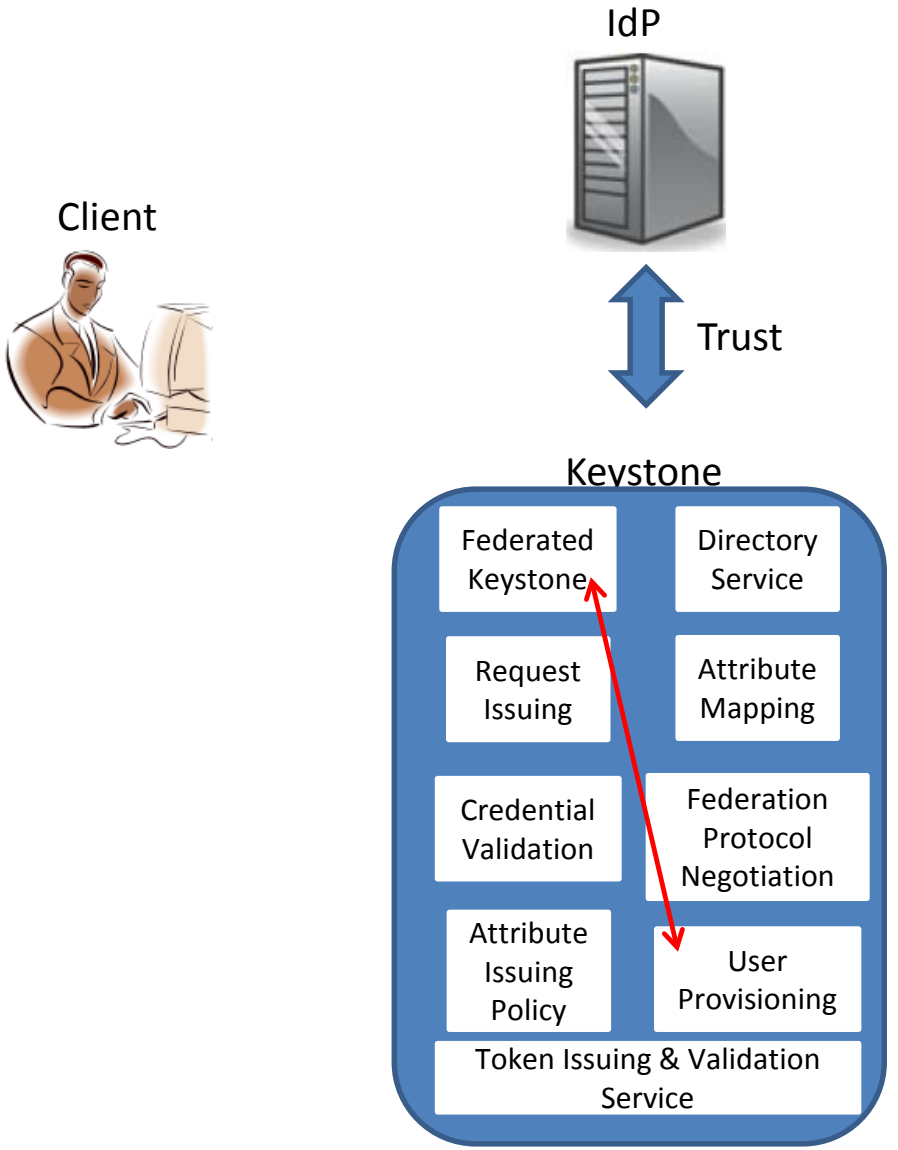


[CHADWK 2014]

Federation Protocol Sequence

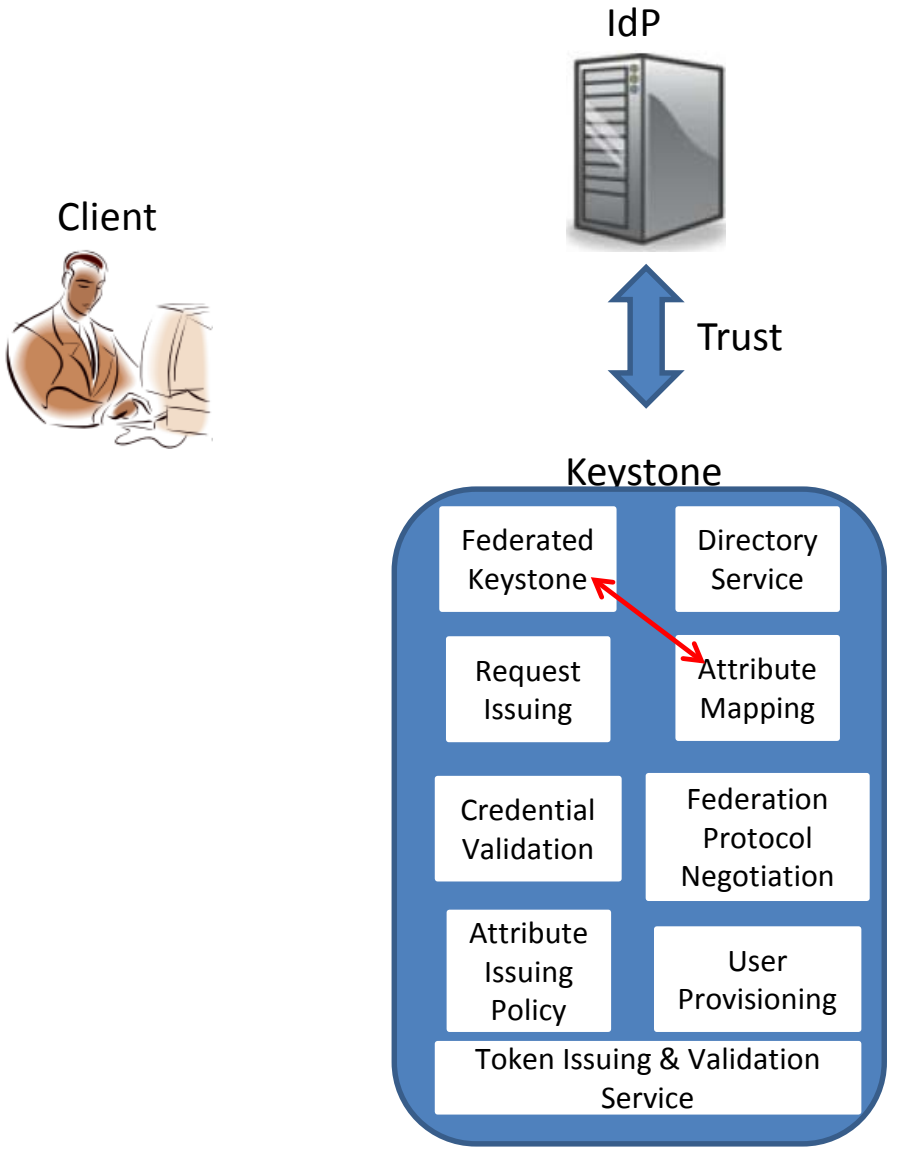
11. Keystone returns the request message to client.
12. Client or keystone passes request to Idp.
13. Idp asks user to authenticate.
14. Client passes the Idps response to keystone.
15. Keystone passes the response to the credential validation function.
16. Credential validation calls directory to obtain metadata to validate the response.
17. Credential validation returns the user's ID, set of identity attributes and idp to keystone.
18. Keystone checks with Attribute Issuer Policy to ensure only allowed attributes asserted by Idp.
19. Keystone calls User Provisioning module , deletes expired entries and create temporary entry for the user.

[CHADWK 2014]



Federation Protocol Sequence

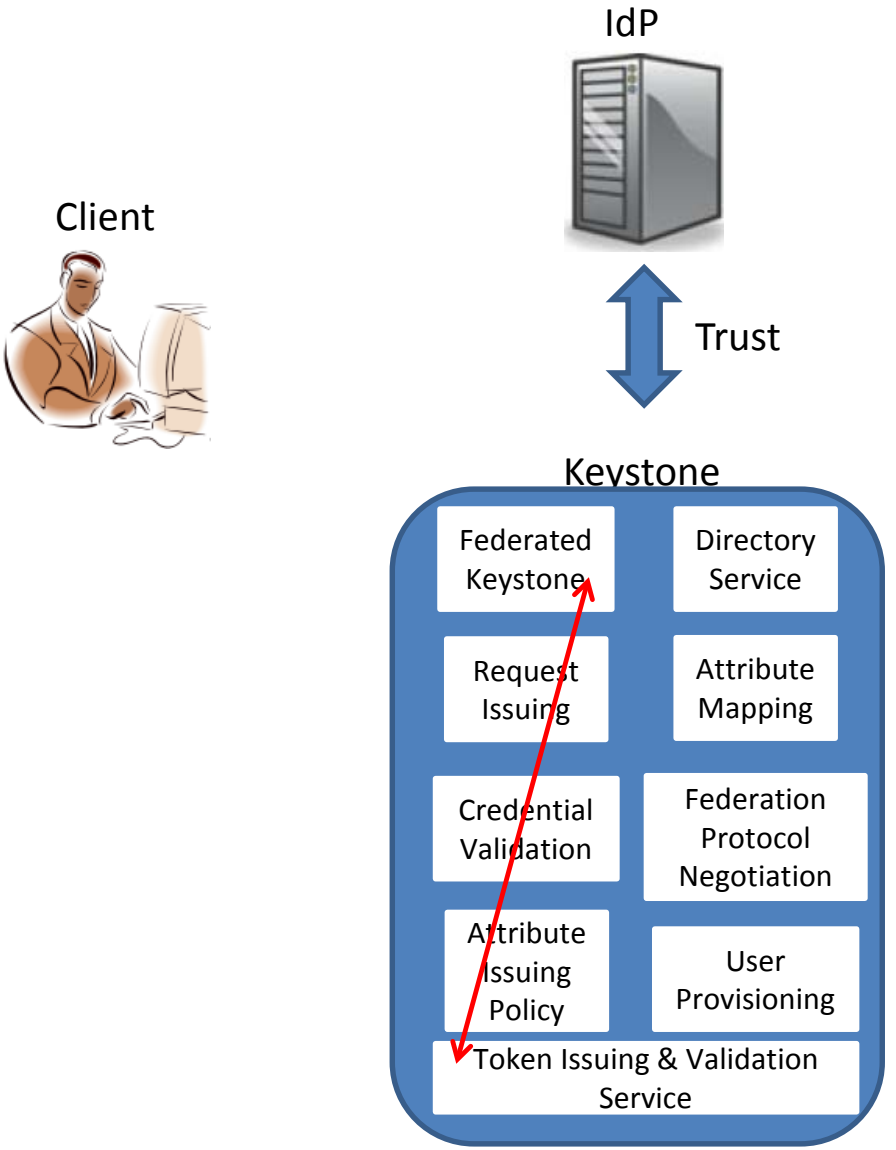
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.



[CHADWK 2014]

Federation Protocol Sequence

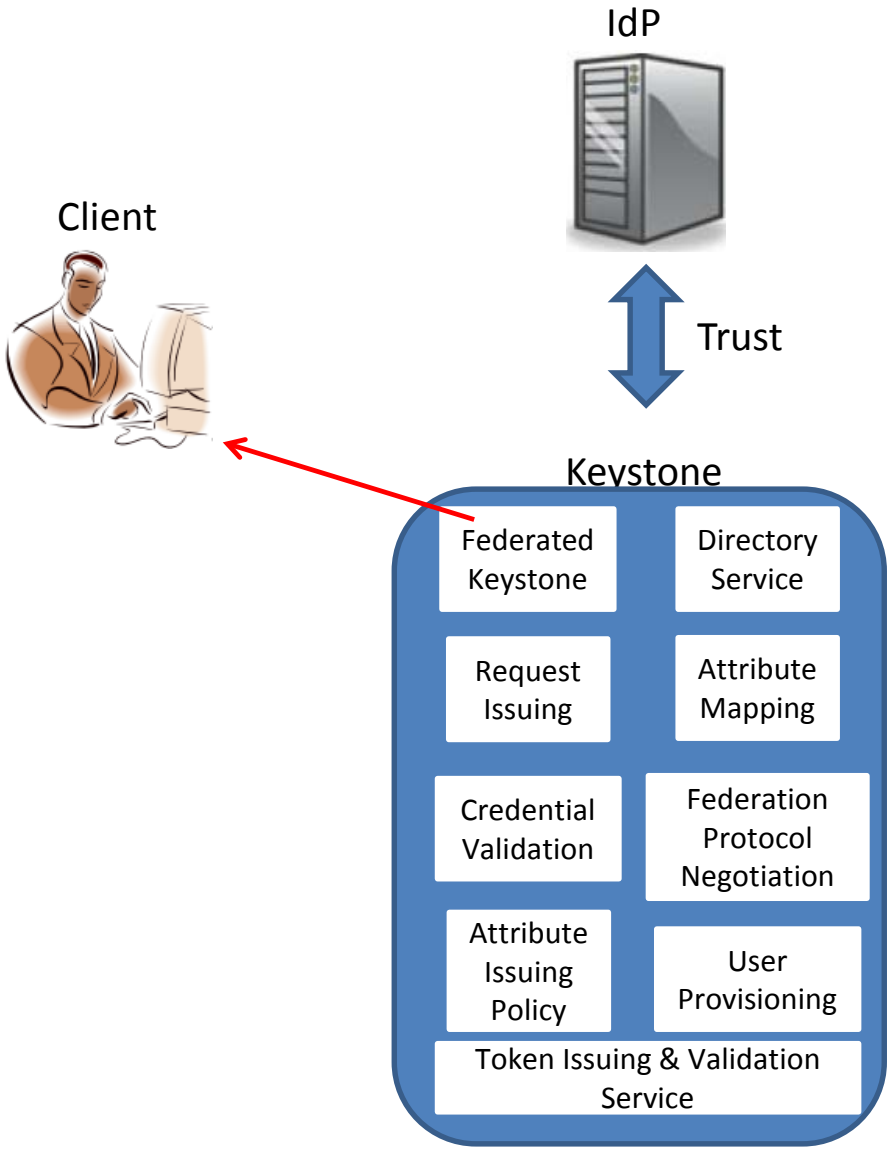
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.



[CHADWK 2014]

Federation Protocol Sequence

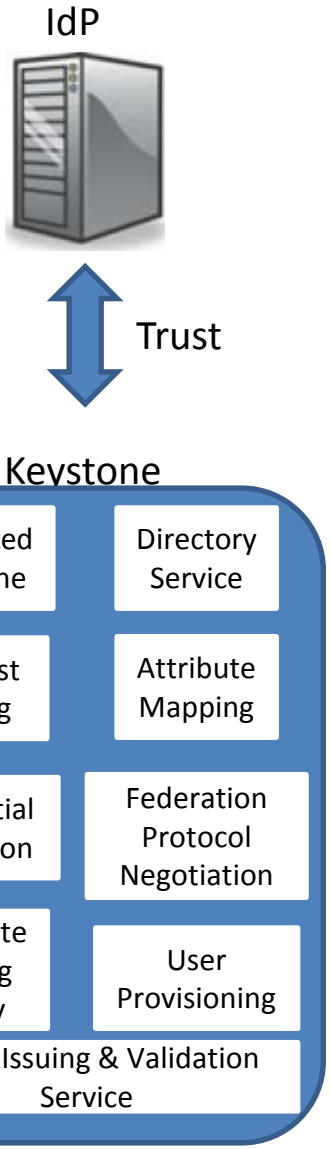
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.



[CHADWK 2014]

Federation Protocol Sequence

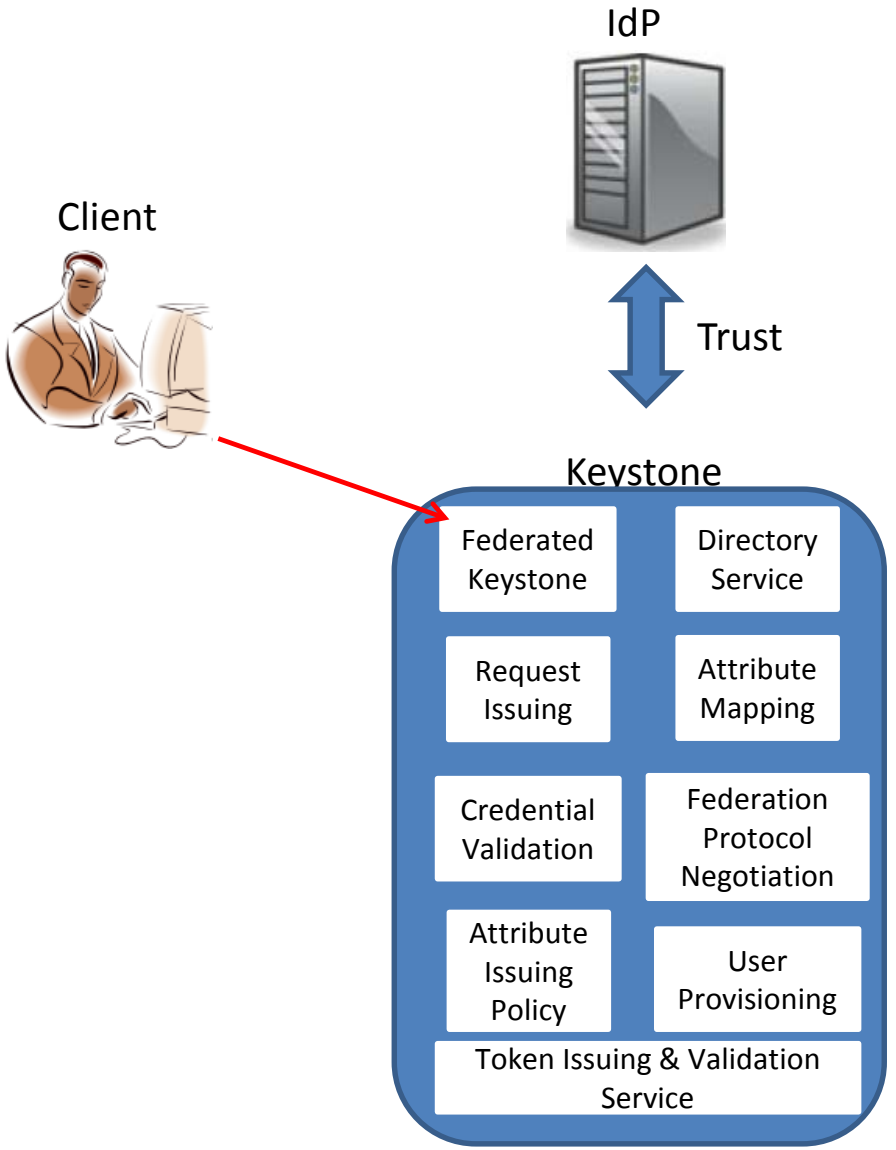
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.



[CHADWK 2014]

Federation Protocol Sequence

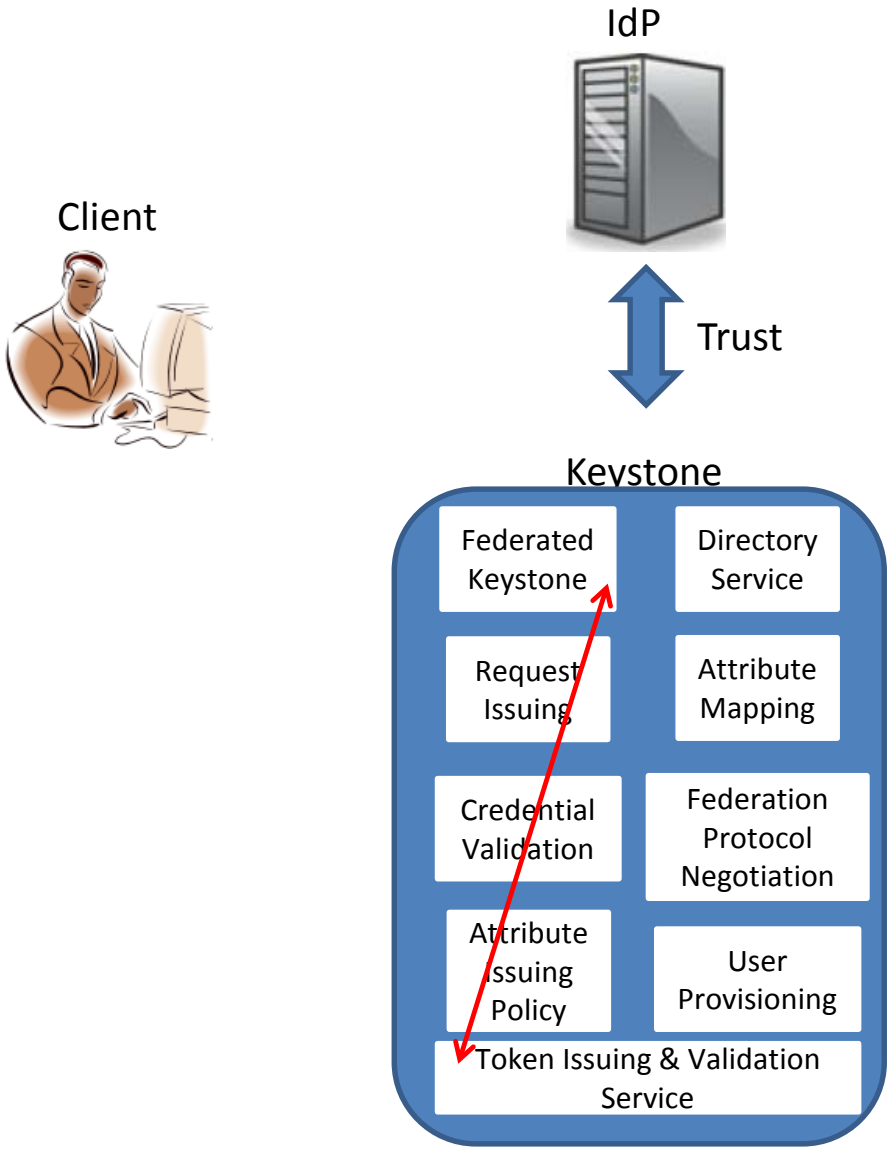
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.



[CHADWK 2014]

Federation Protocol Sequence

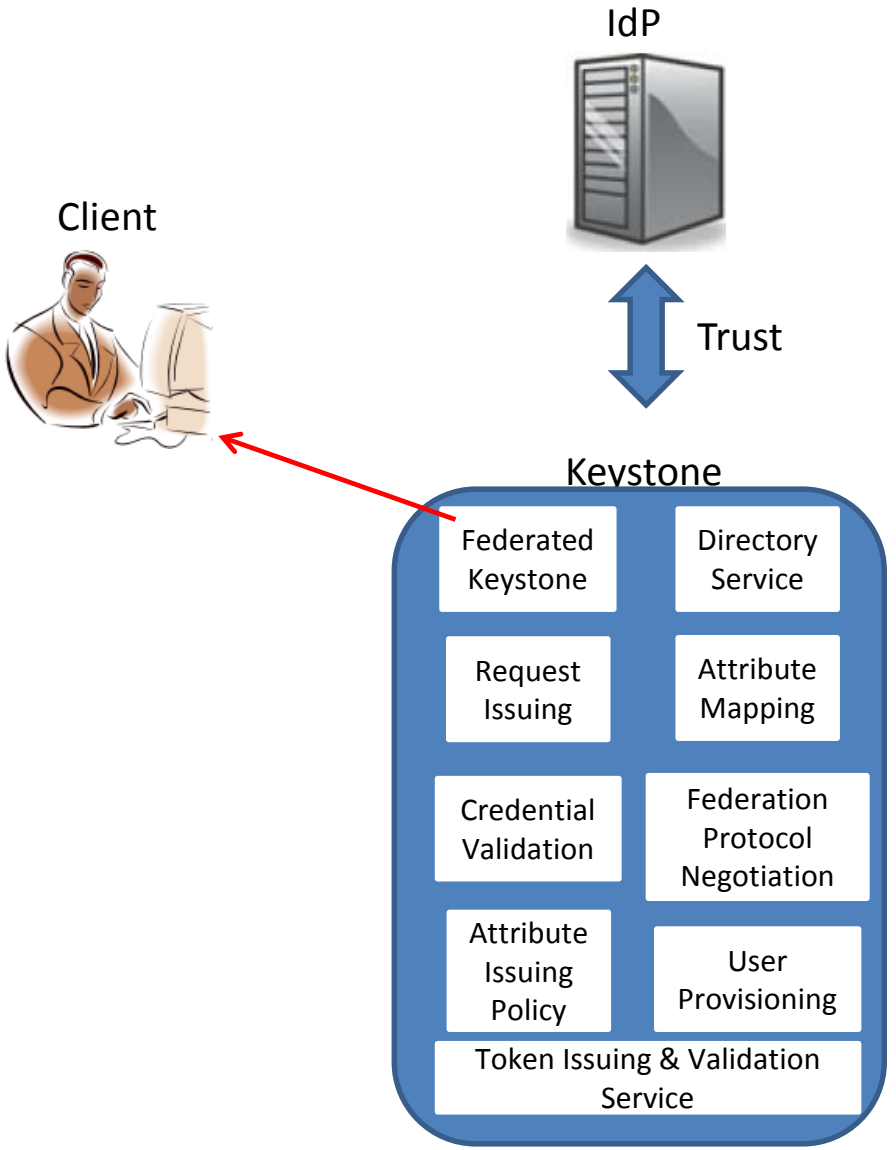
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.



[CHADWK 2014]

Federation Protocol Sequence

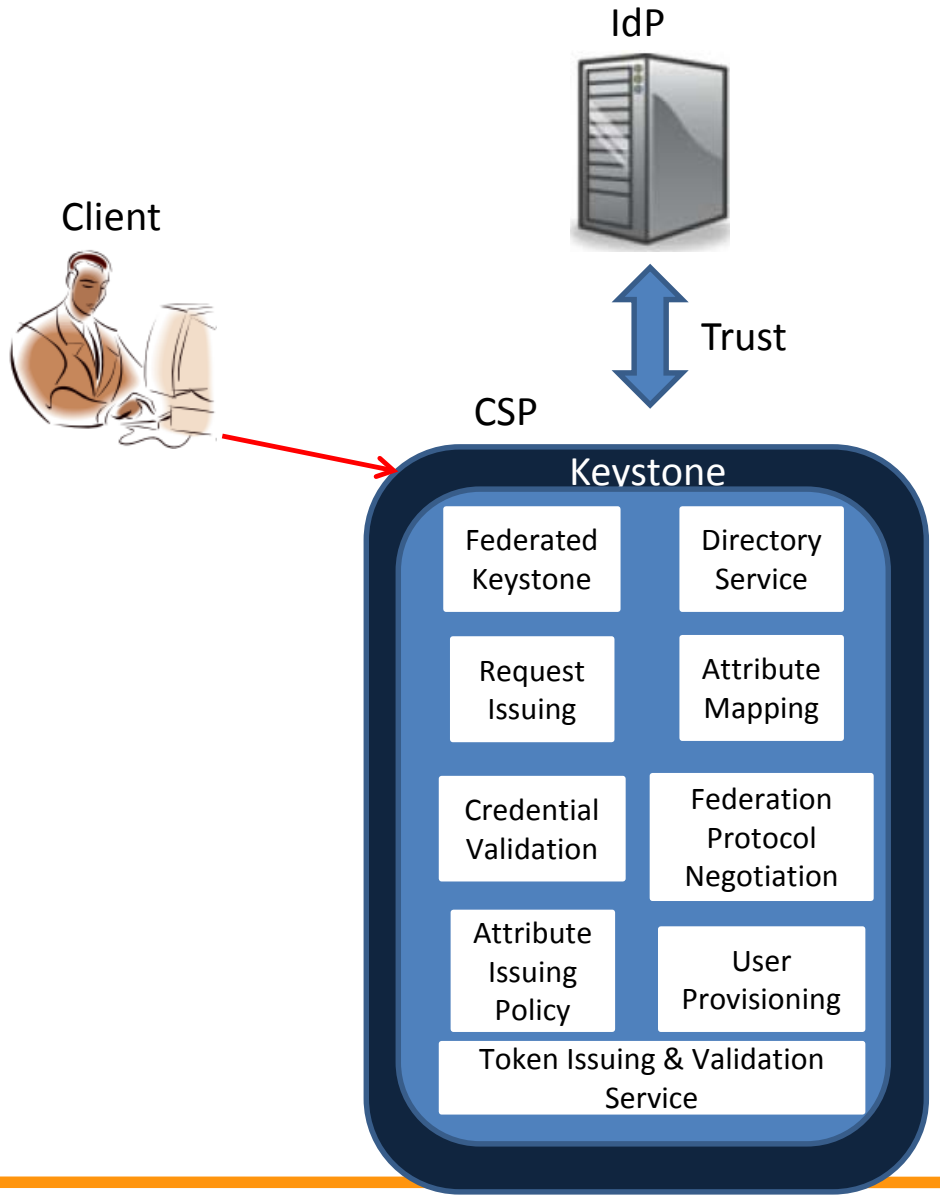
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.
26. Keystone returns to the client scoped token and list of services.



[CHADWK 2014]

Federation Protocol Sequence

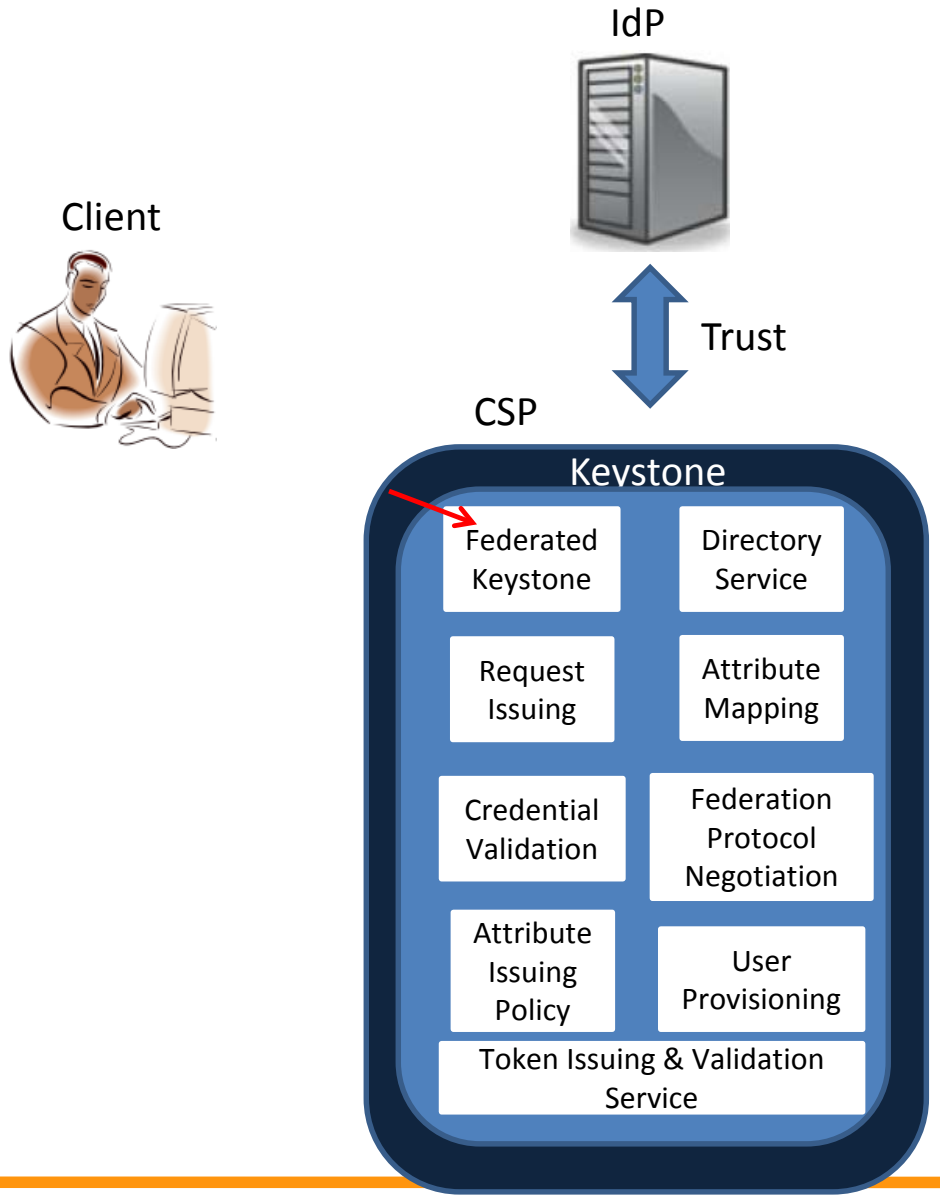
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.
26. Keystone returns to the client scoped token and list of services.
27. Client contact the service provider requesting service.



[CHADWK 2014]

Federation Protocol Sequence

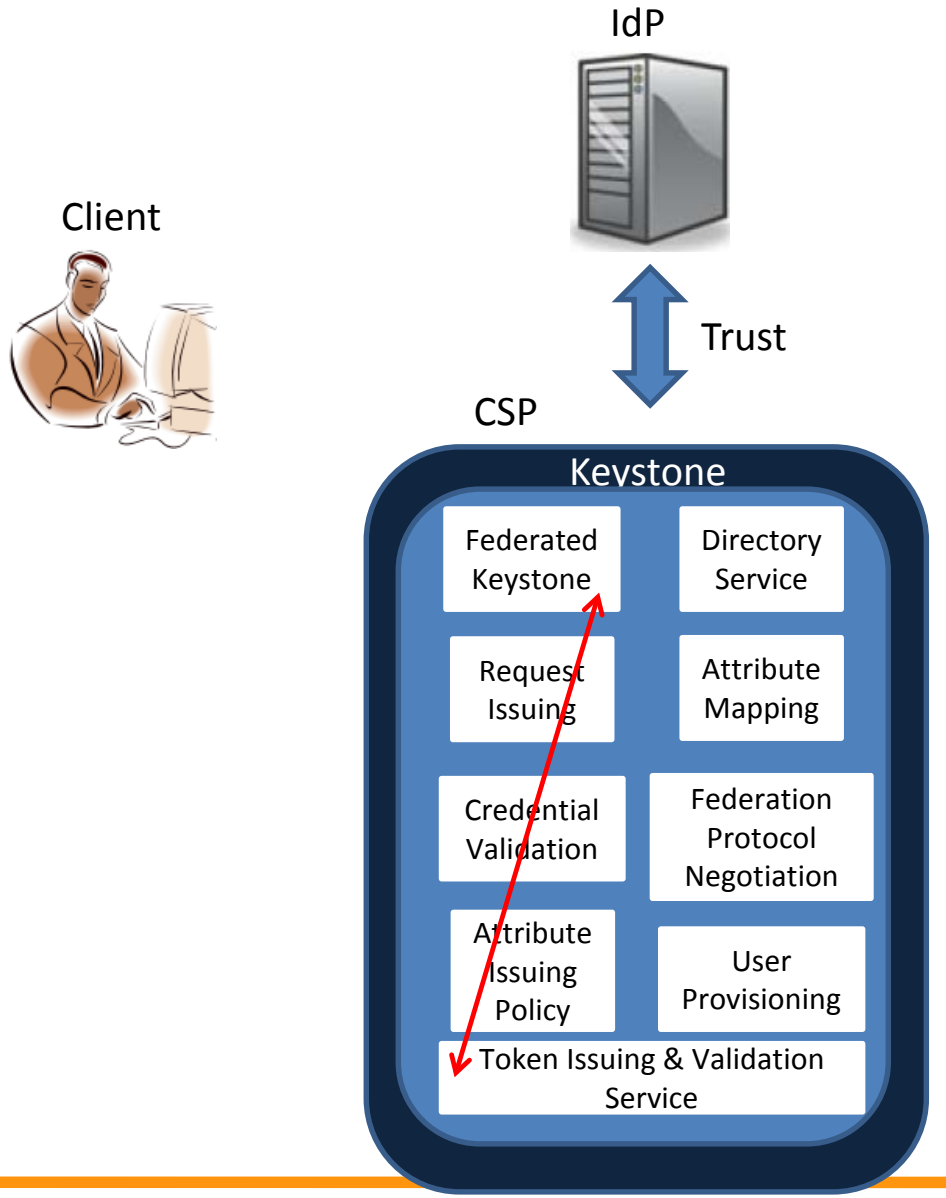
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.
26. Keystone returns to the client scoped token and list of services.
27. Client contact the service provider requesting service.
28. CSP passes the token to Keystone for validation.



[CHADWK 2014]

Federation Protocol Sequence

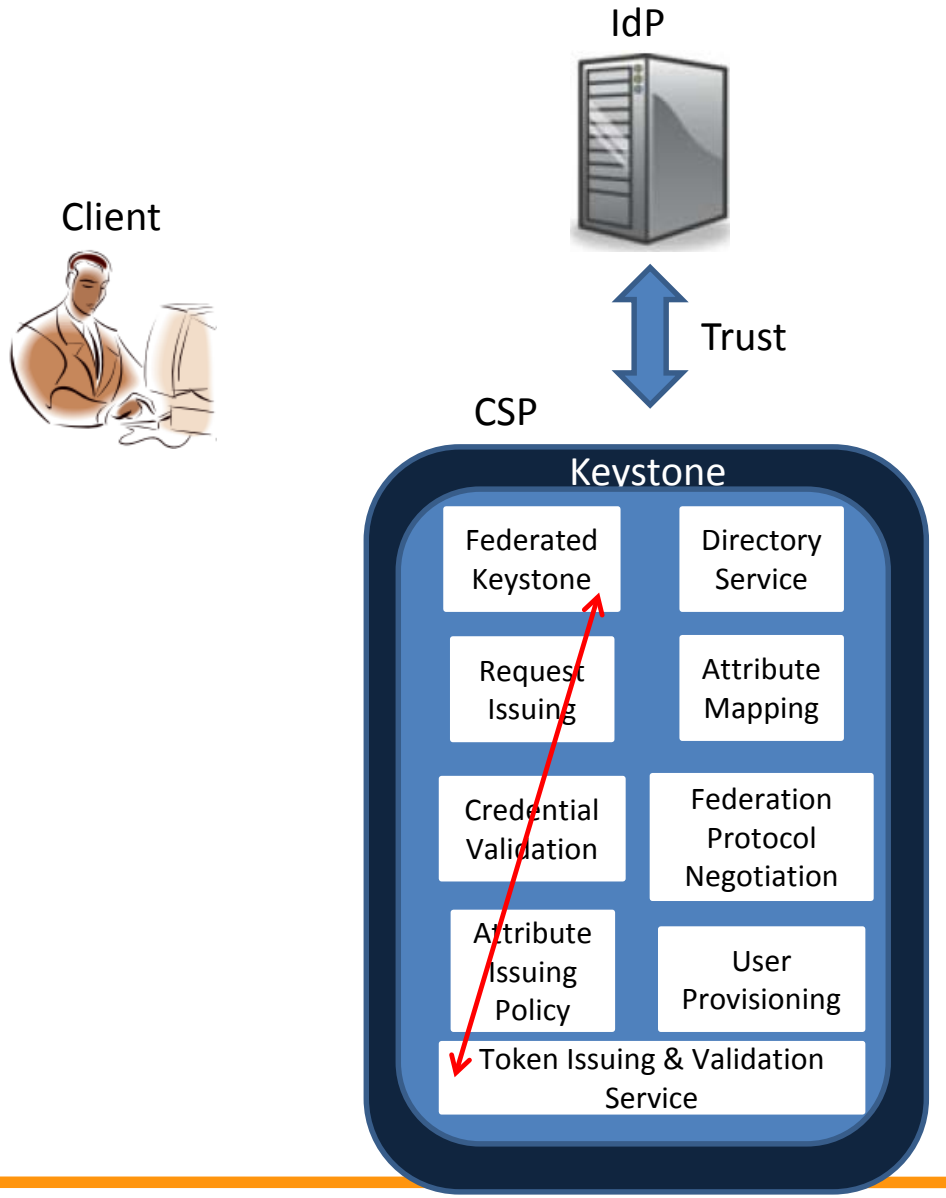
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.
26. Keystone returns to the client scoped token and list of services.
27. Client contact the service provider requesting service.
28. CSP passes the token to Keystone for validation.
29. Keystone contact TS.



[CHADWK 2014]

Federation Protocol Sequence

20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.
26. Keystone returns to the client scoped token and list of services.
27. Client contact the service provider requesting service.
28. CSP passes the token to Keystone for validation.
29. Keystone contact TS.

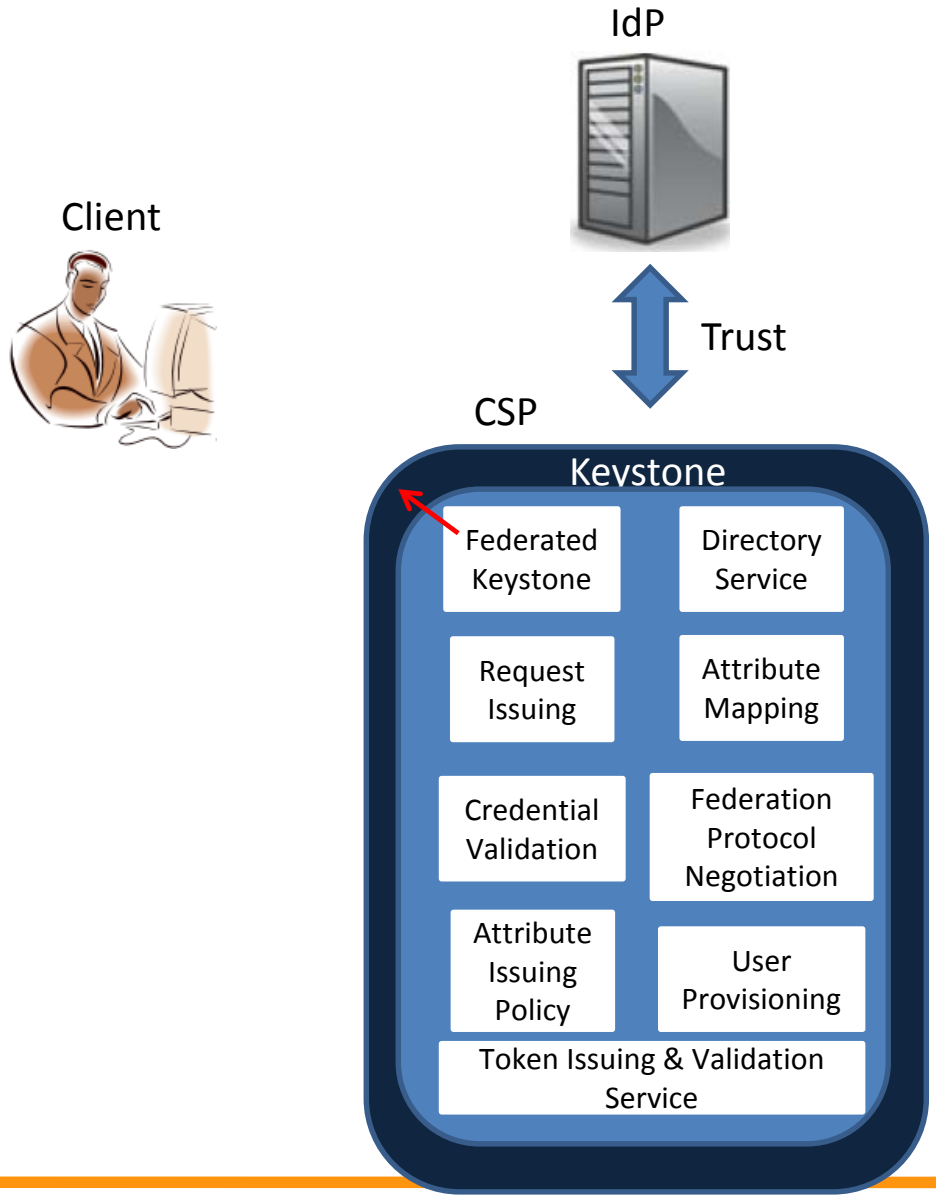


[CHADWK 2014]

Federation Protocol Sequence

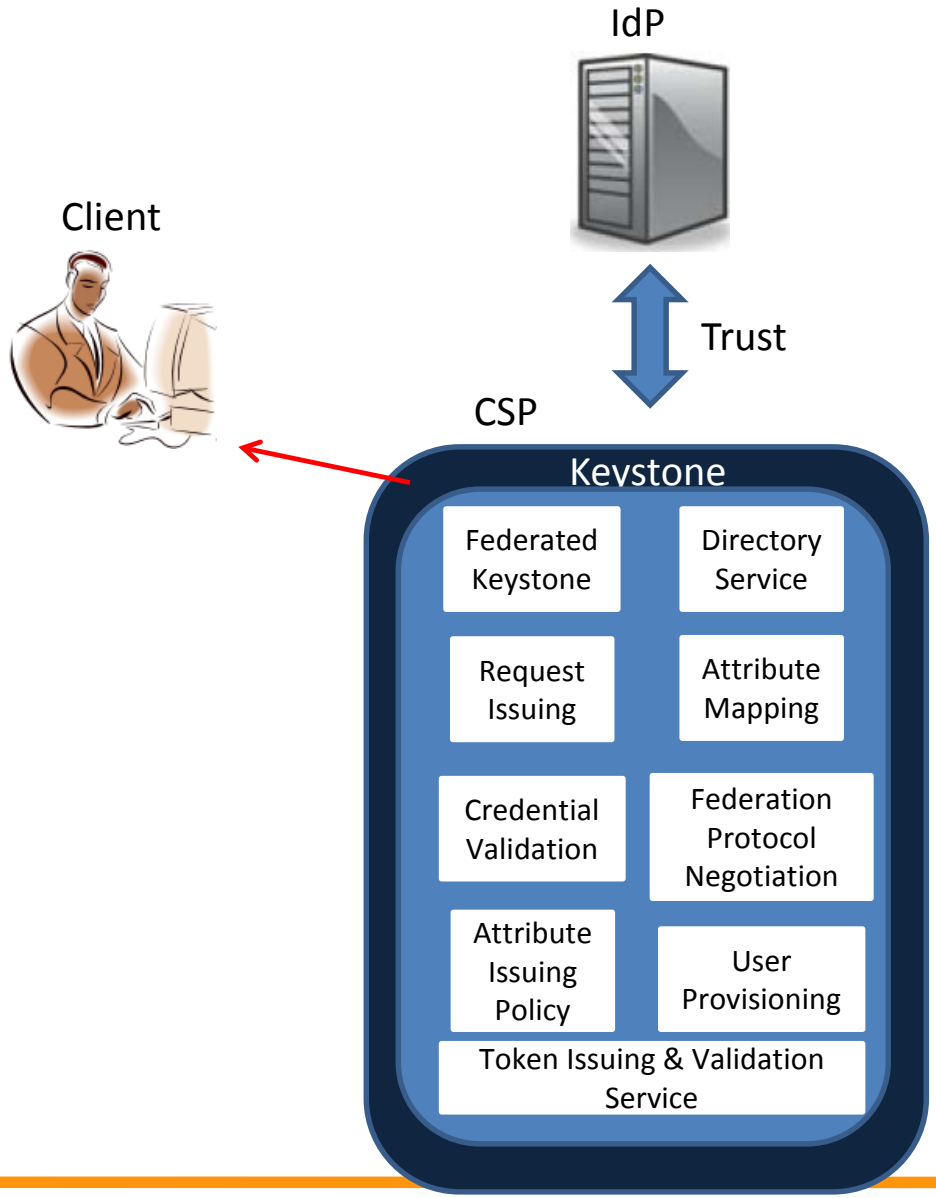
20. Keystone calls Attribute Mapper to obtain local set authorization attributes.
21. Keytone updates these attributes in the temporary user entry and calls the token service to obtain unscoped token.
22. Keystone returns the token and list endpoints available.
23. The user chooses the service.
24. The client passes the token and chosen domain and project to keystone.
25. Keystone calls TS to validate unscoped token and get scoped token.
26. Keystone returns to the client scoped token and list of services.
27. Client contact the service provider requesting service.
28. CSP passes the token to Keystone for validation.
29. Keystone contact TS.
30. Keystone sends the response to CSP.

[CHADWK 2014]



Federation Protocol Sequence

31. CSP checks PDP if authorized, reply is granted.



[CHADWK 2014]

References

- NIST. (2012). Cloud Computing Synopsis and Recommendations. Special Publication 800-146, May 2012
- VANDER. (2013). Architecture for the Heterogeneous Federation of Future Internet Experimentation Facilities. Future Network & MobileSummit, 2013
- BOHLI. (2013). Security and Privacy-Enhancing Multicloud Architectures. IEEE Transaction on Dependable and Secure Computing, 2013
- CASTILO. (2013). OpenStack Federation in Experimentation Multi-cloud Testbeds. UNICO, 2013
- CHADWK. (2014). Adding Federated Identity Management to OpenStack. Journal of Grid Computing, 2014