Group Management Service (GMS)

Brian Major, Patrick Dowler, Adrian Damian

Canadian Astronomy Data Centre

IVOA - October 2016

Authorization

Making the decision of whether to grant permission to a given resource

The decision can involve knowing an authenticated user's credentials

Resources

Resources are entities that may require authorization for access.

For example:

- Services (SIA, SODA, Processing, HR System)
- Data (archival data, VOSpace files, etc…)
- Metadata (TAP tables, TAP rows, VOSpace metadata, etc…)

Authorization: Two Distinct Aspects

1. The owner(s) of a resource may, at any time, change the rules by which a resource may be accessed. This is the granting and revoking of access.

2. When users try to access resources, the granting rules for that resource are evaluated at runtime. This is the authorization check.

Authorization Requirements

1) To allow for restricted access certain resources

Only a certain set of individuals may access certain resources

2) To allow certain individuals to set the access rules on resources

The owner(s) of the resources need to manage the access rules

Interoperable Authorization Requirements

3) To be able to re-use granting rules between resources

Projects must authorize access to a variety of proprietary resources

4) To be able manage granting rules at a single location

Projects should not have to update each resource on a change to a re-used grant

5) To be able to reference remote granting rules

Proprietary resources should not be confined to a single institution

Granting rules: groups

A single individual is too restrictive

Having a list of individuals is difficult to maintain

Grouping individuals and referencing them by a group identifier provides a necessary level of abstraction

Group Management Service (GMS)

A RESTful API for checking group membership.

Required:

```
isMember(Subject, Group)
```

For user controlled groups, an optional management API:

```
createGroup, addMember, etc..
```

GMS Group Identifiers

They are universal

ivo://authority/gms?groupName

To resolve the host GMS service, lookup the URL for serviceID ivo://authority/gms in Registry. This may result in (for example):

http://server.example.com/myGMS

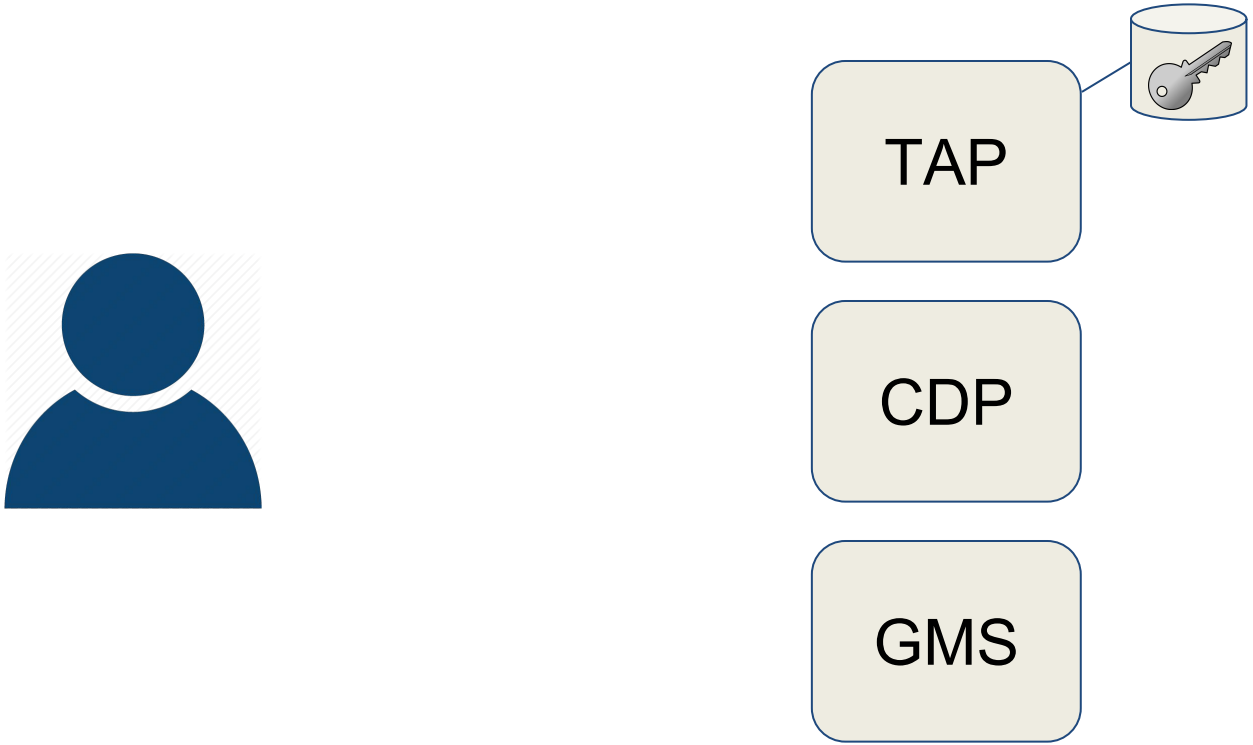
Credential Delegation Protocol (CDP) and GMS

Calls to GMS to check group membership must be done by the user.

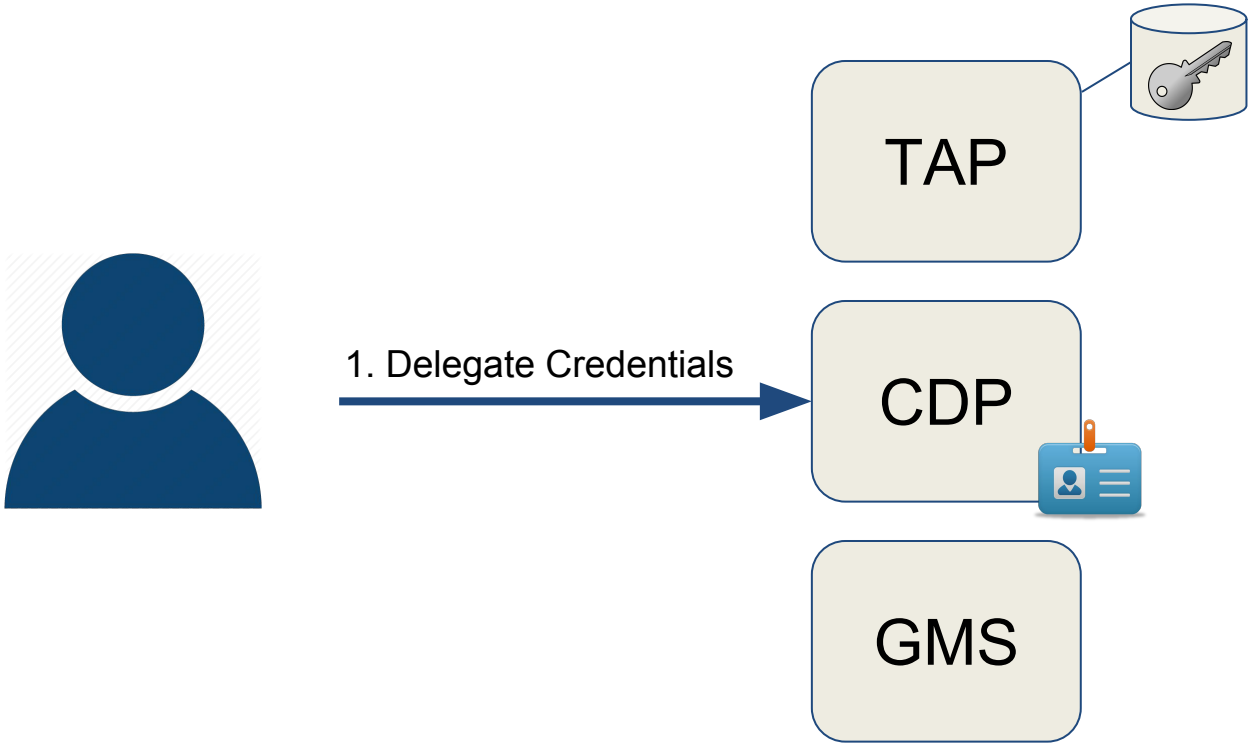
Group membership is private information.

CDP is used to get the user's credentials for inter-service calls.

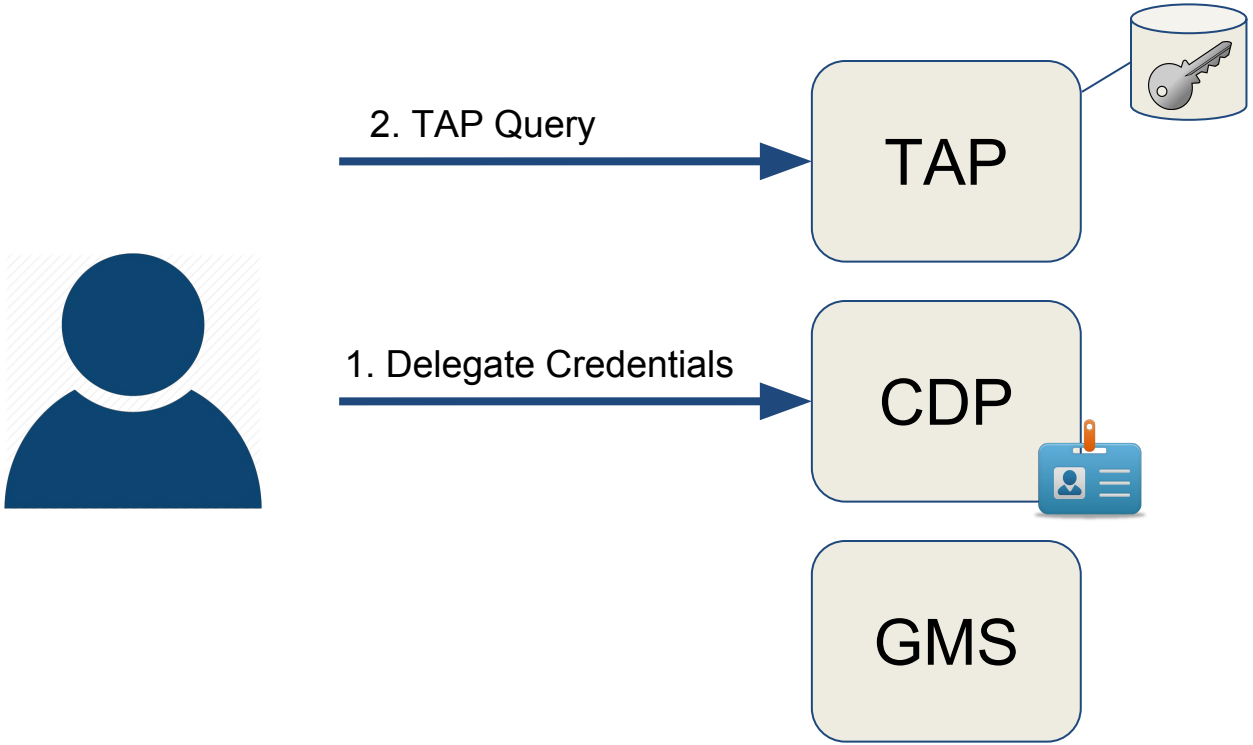
Use Case 1: Authorized TAP Query



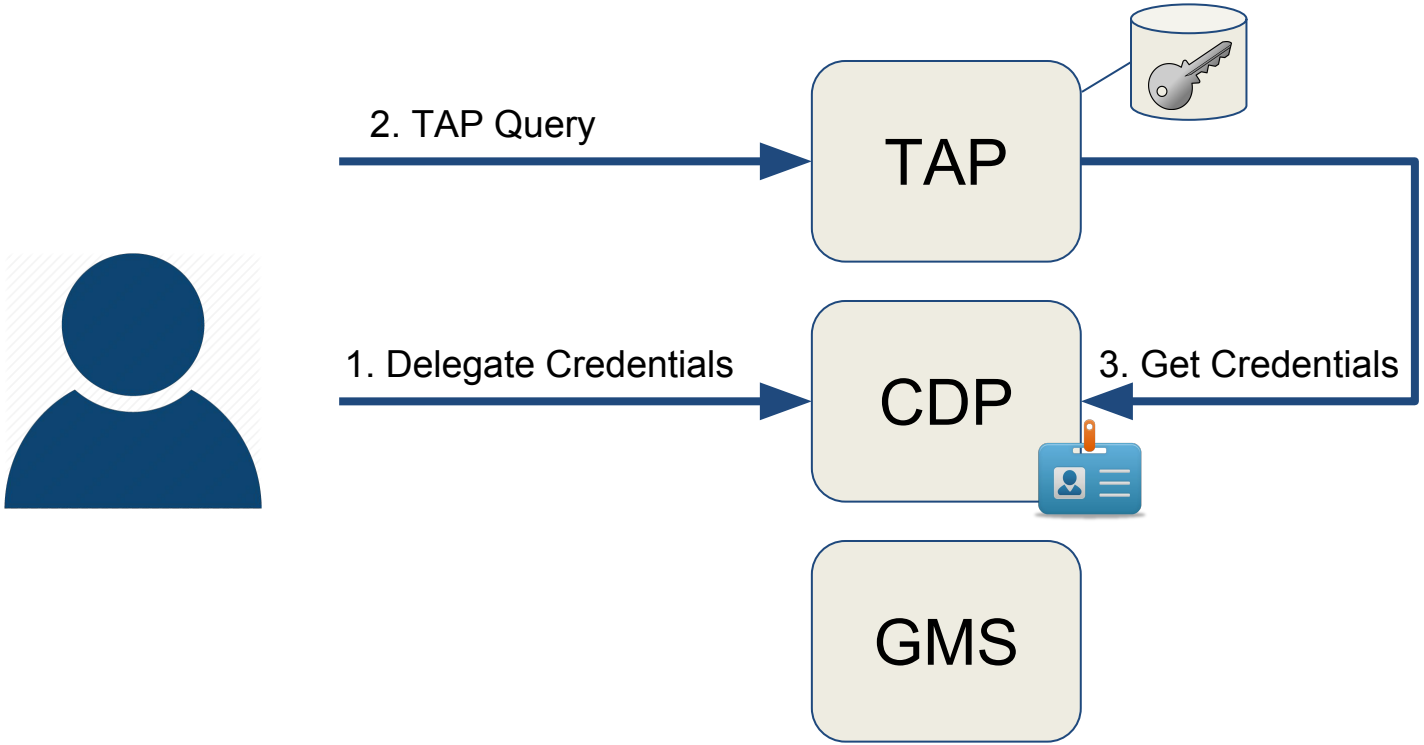
Use Case 1: Authorized TAP Query



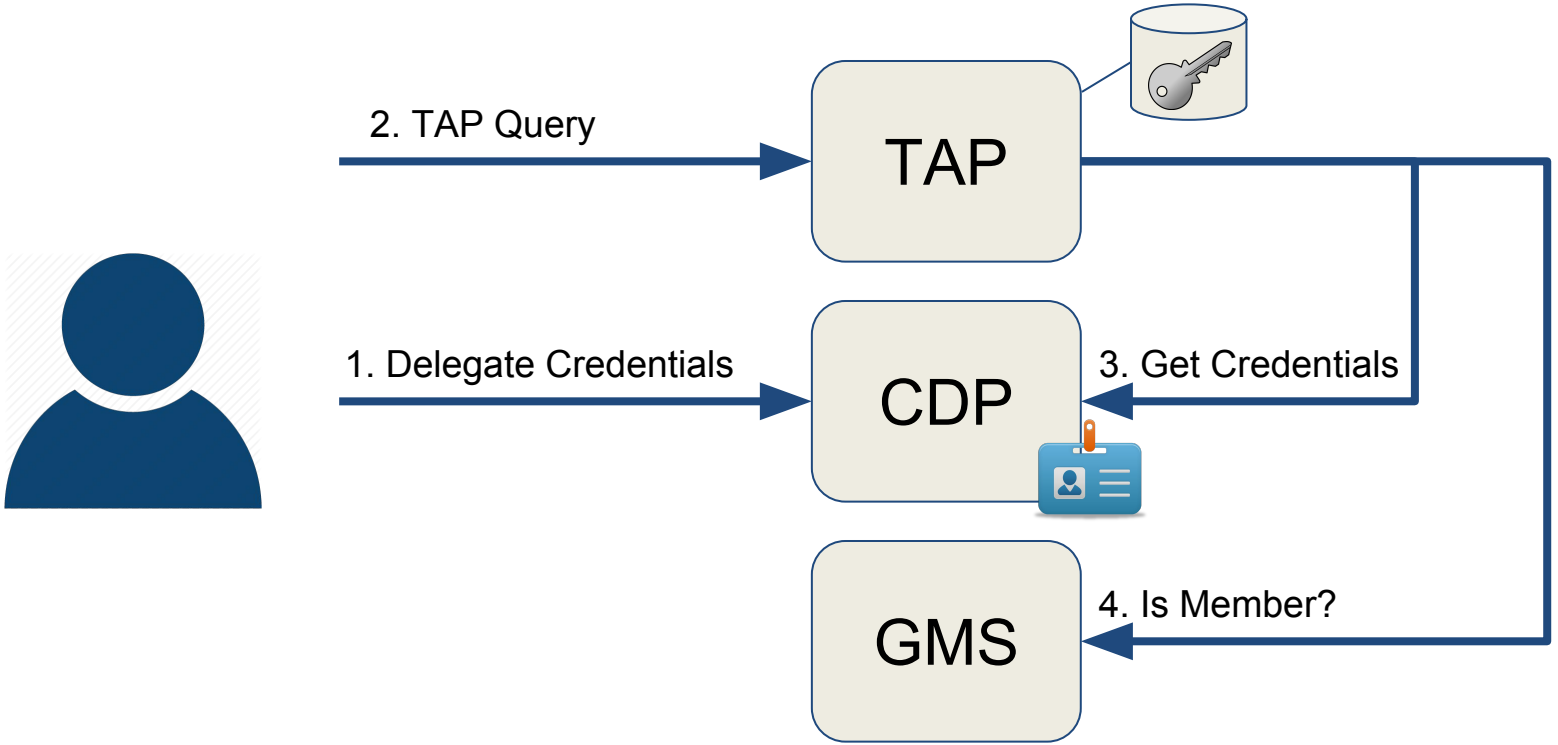
Use Case 1: Authorized TAP Query



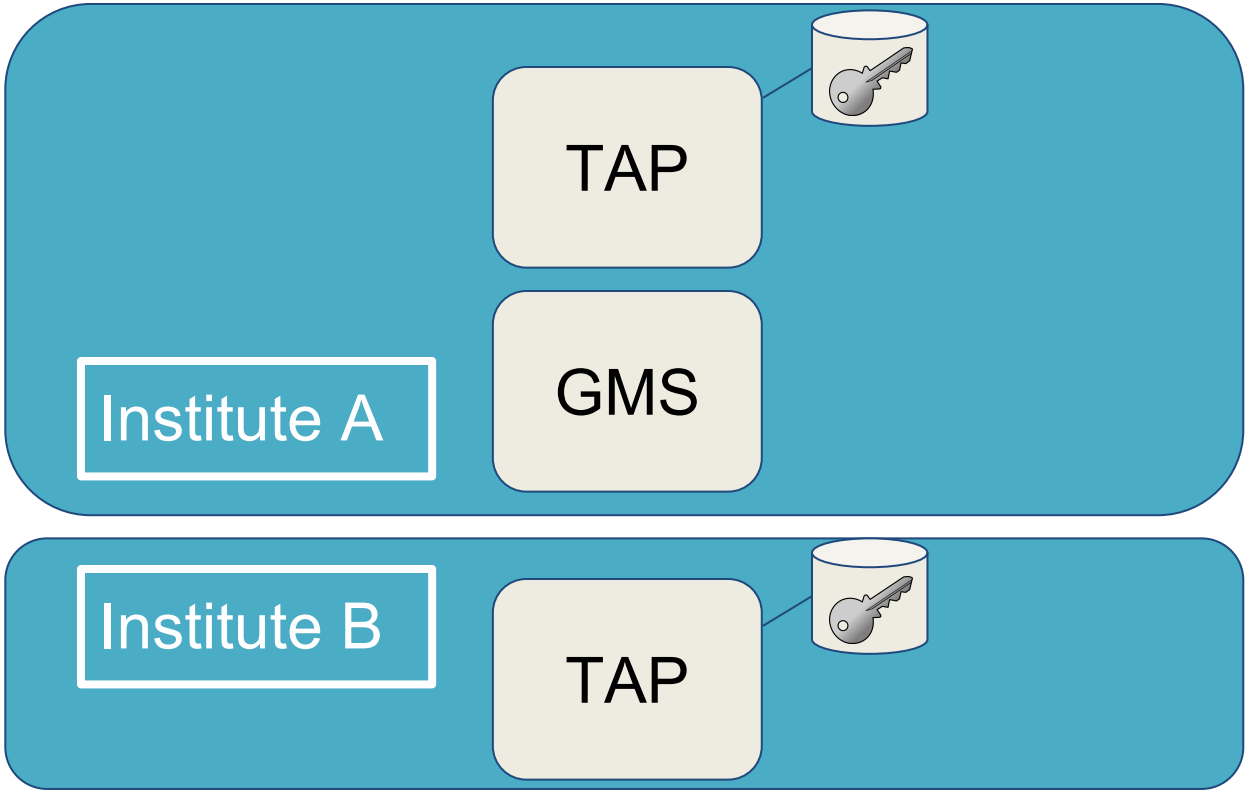
Use Case 1: Authorized TAP Query



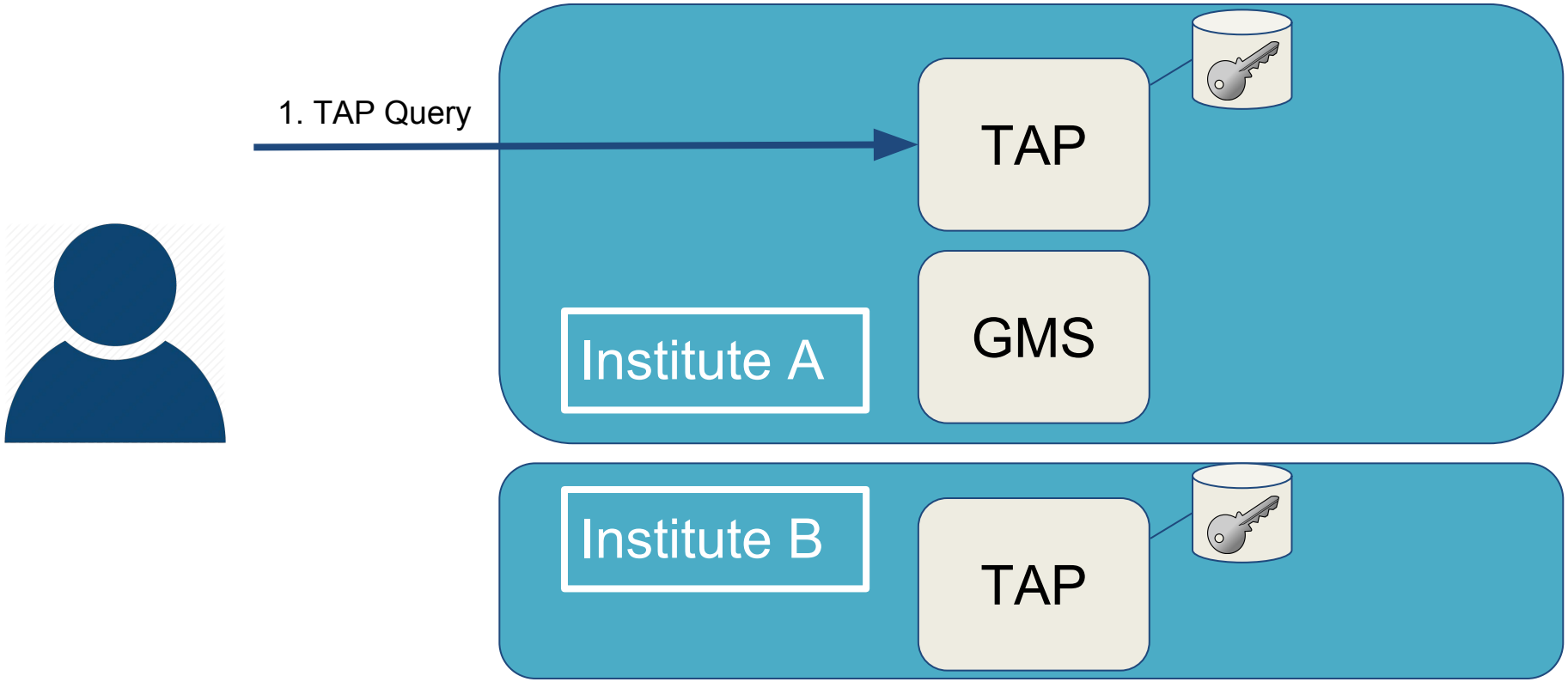
Use Case 1: Authorized TAP Query



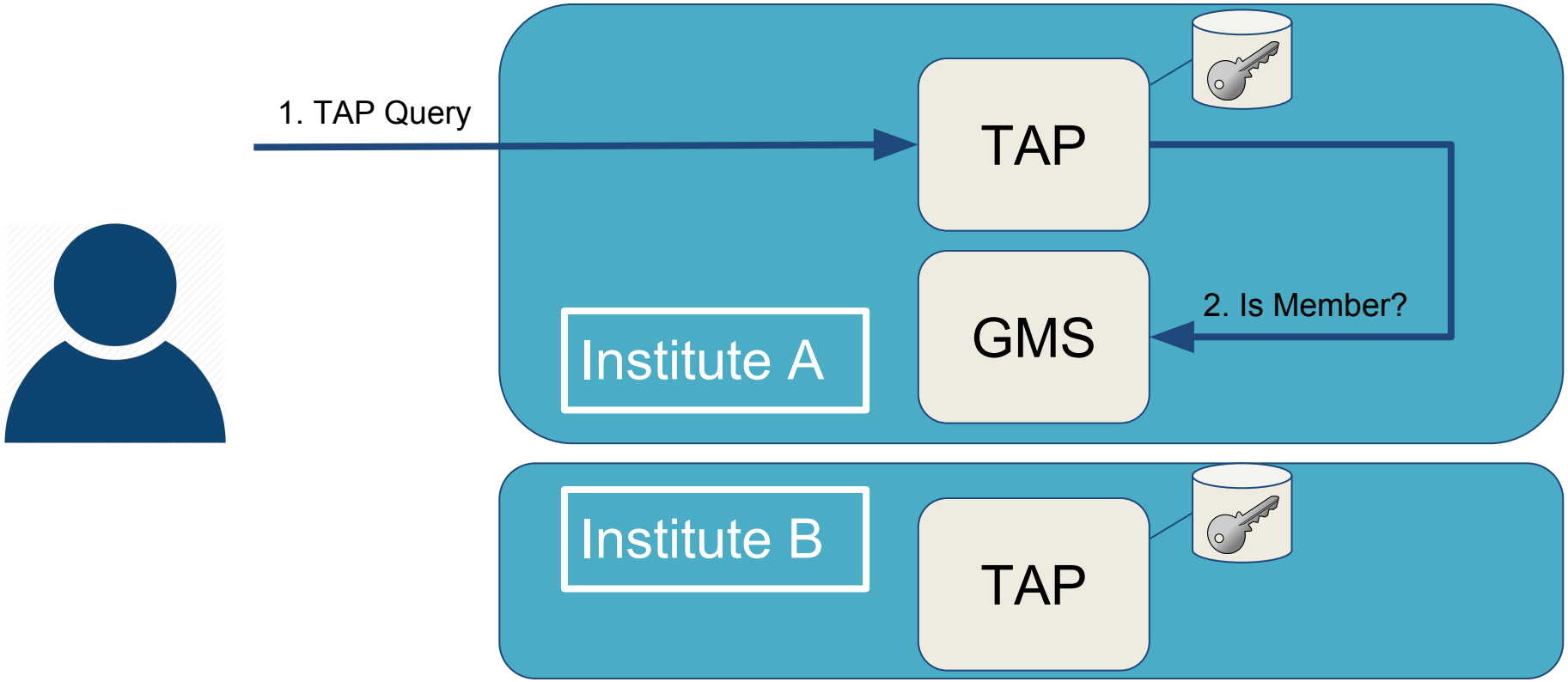
Use Case 2: Distributed TAP Query



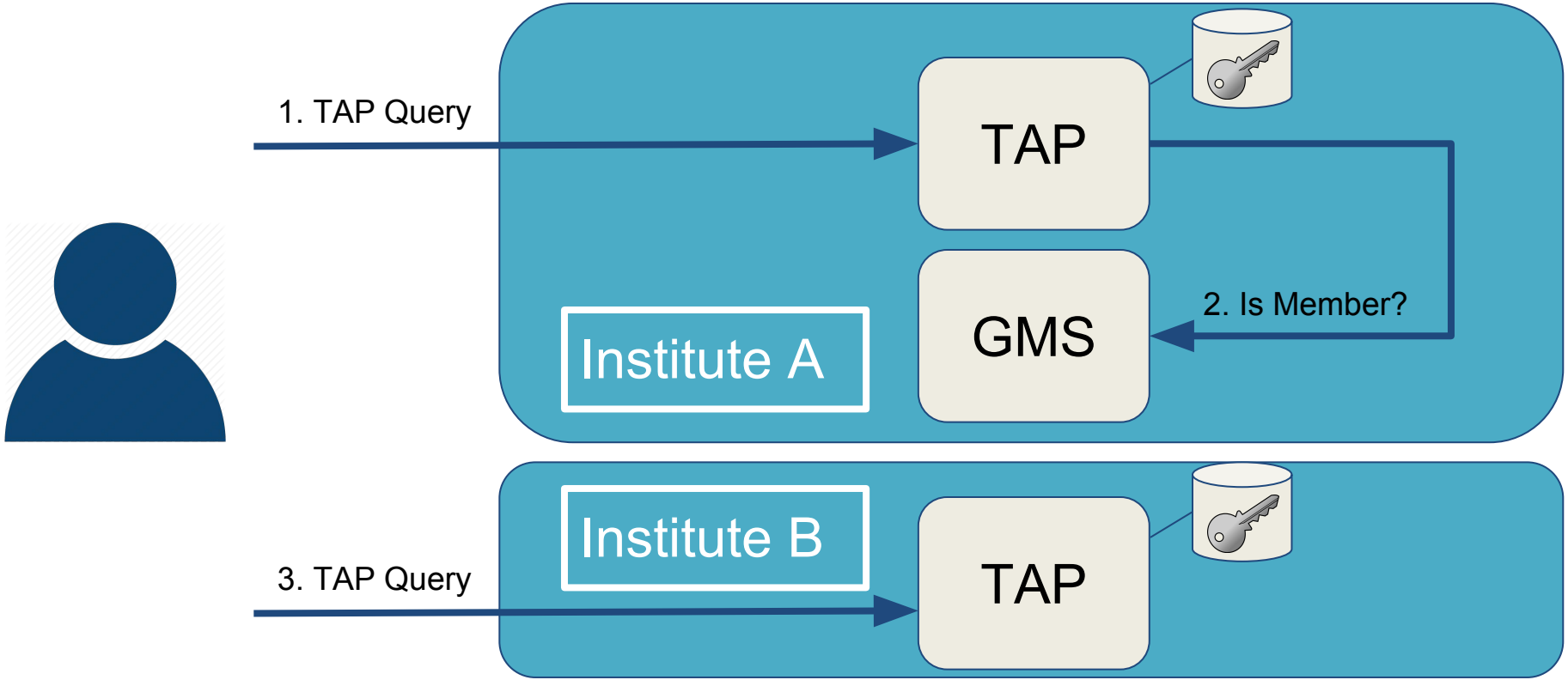
Use Case 2: Distributed TAP Query



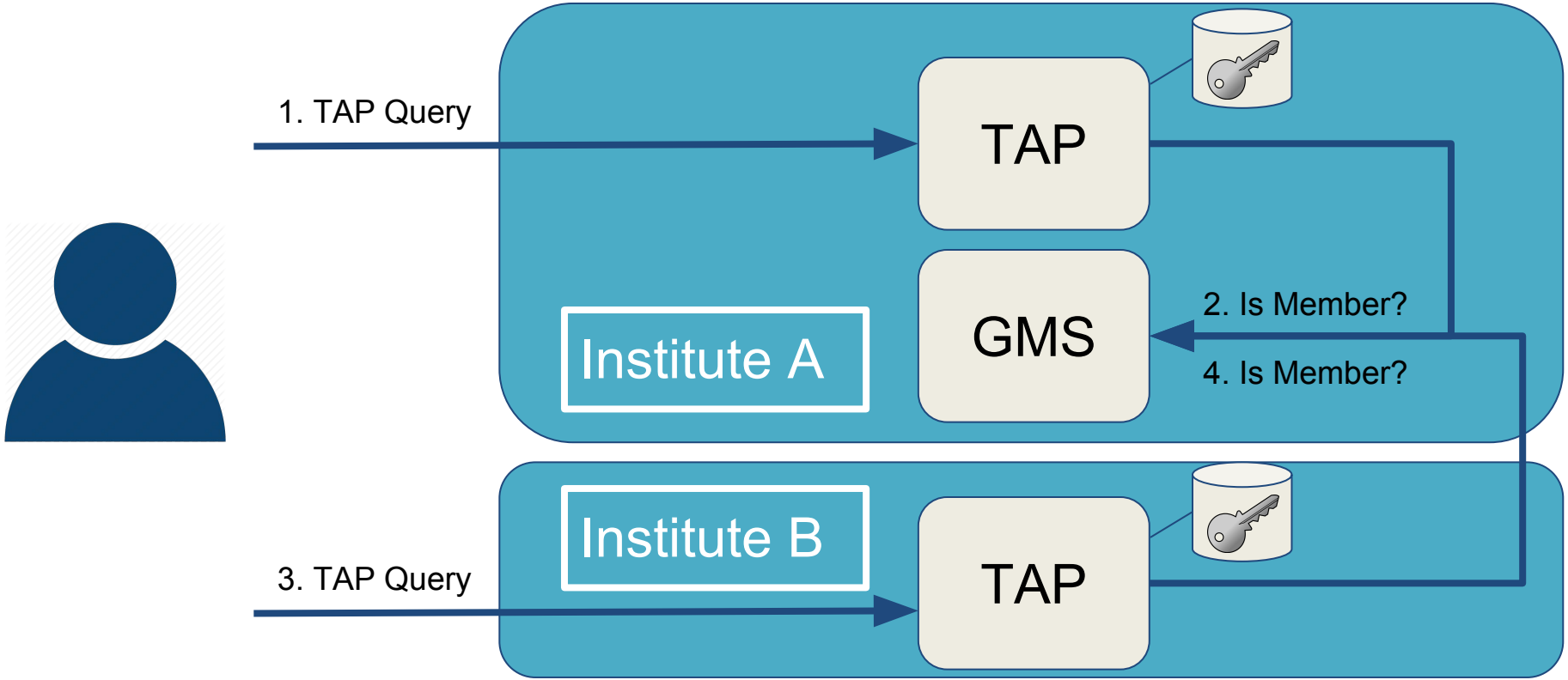
Use Case 2: Distributed TAP Query



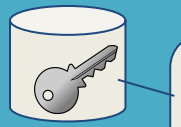
Use Case 2: Distributed TAP Query



Use Case 2: Distributed TAP Query



Use Case 3: Remote TAP Result Storage



TAP

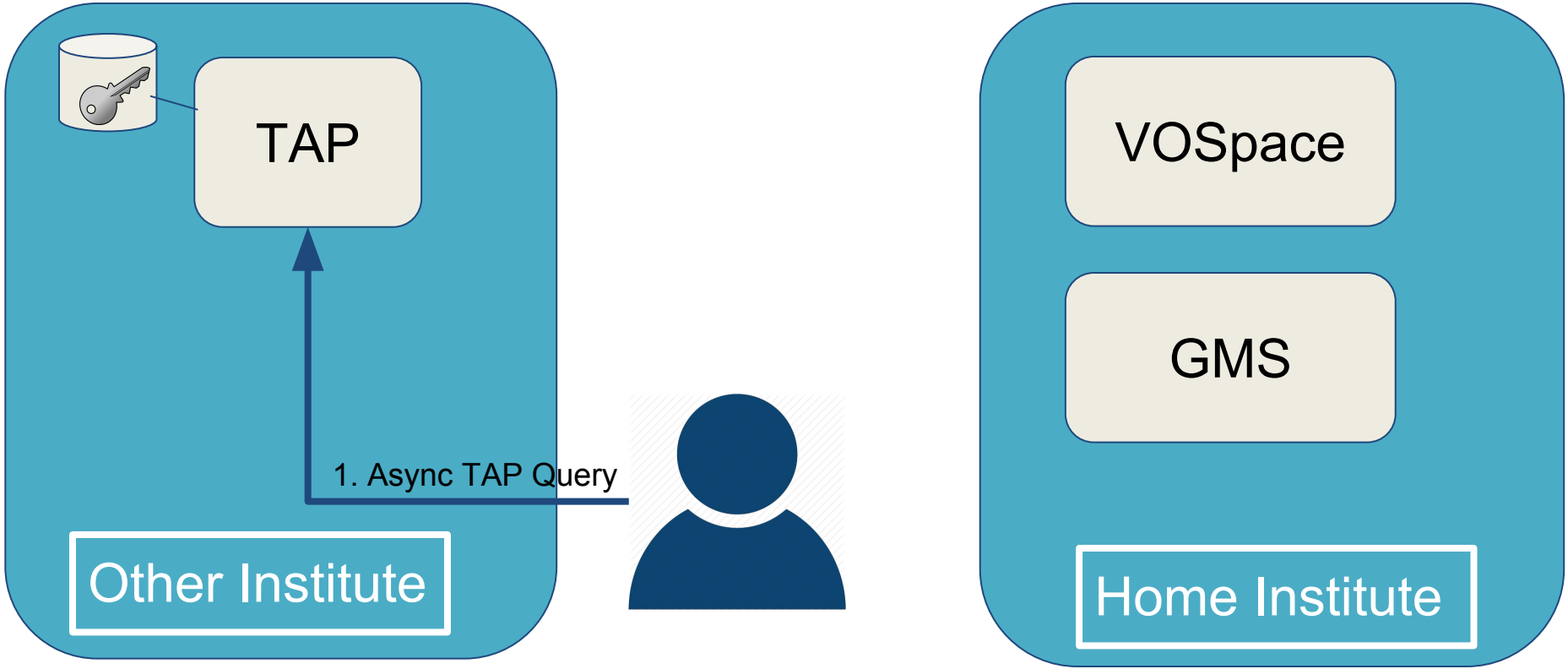
Other Institute

VOSpace

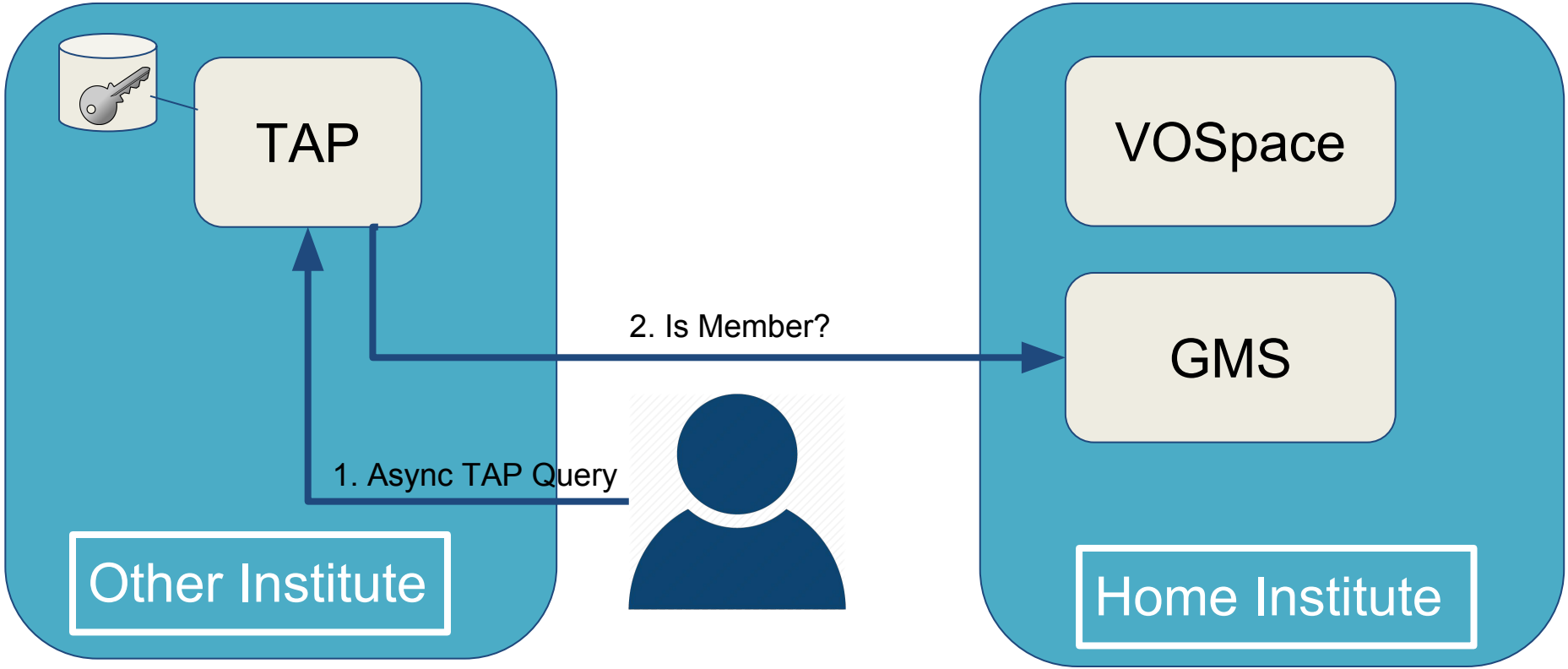
GMS

Home Institute

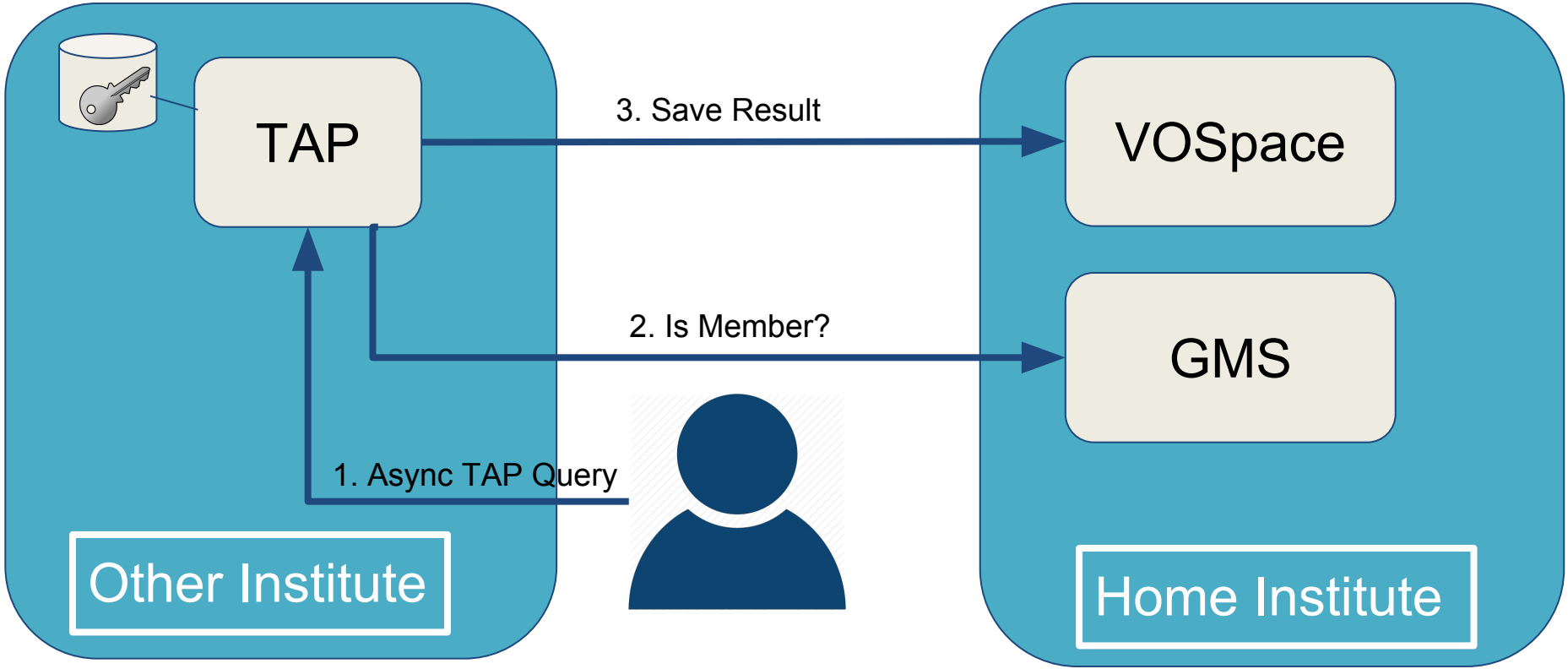
Use Case 3: Remote TAP Result Storage



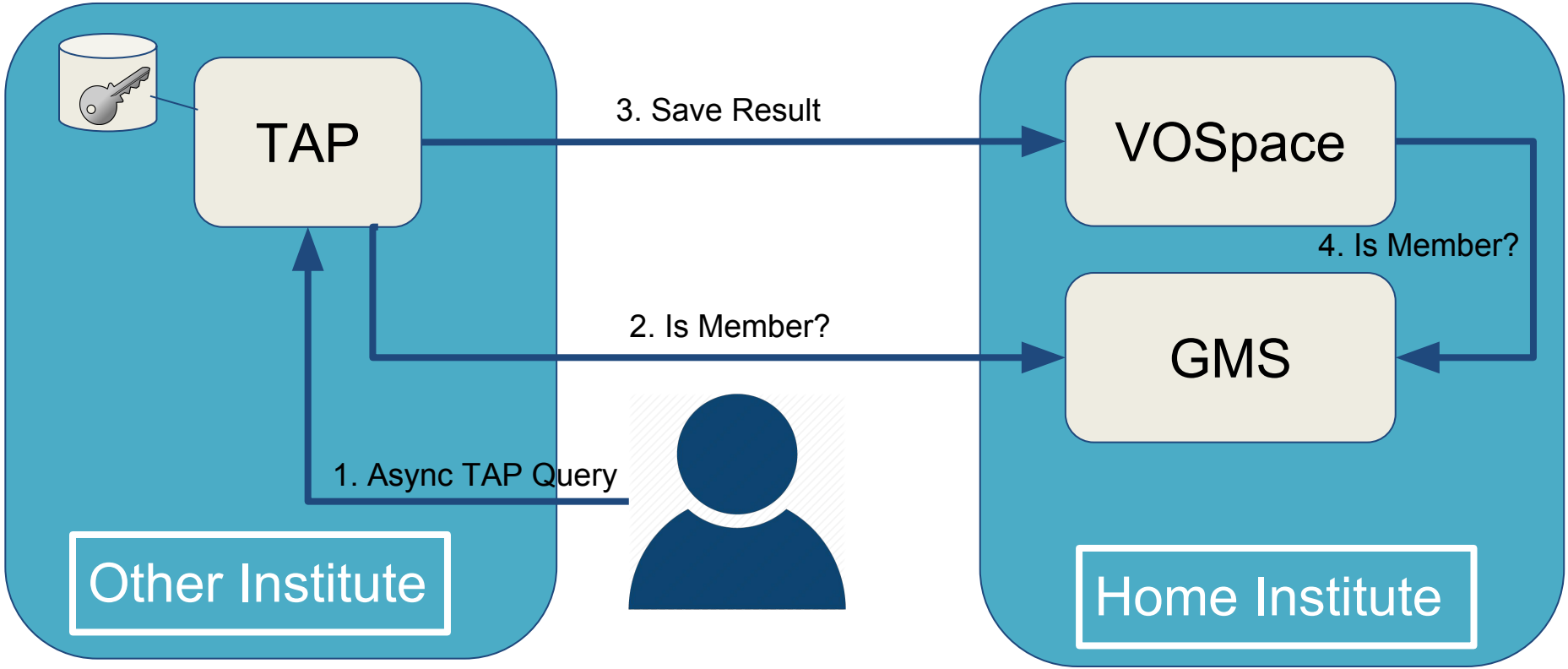
Use Case 3: Remote TAP Result Storage



Use Case 3: Remote TAP Result Storage



Use Case 3: Remote TAP Result Storage



Implementing the Group Management Service

Group management technologies:

- Grouper:

http://www.internet2.edu/products-services/trust-identity/grouper

- OpenCADC GMS:

https://github.com/opencadc/ac

Standardization

Standardization would allow for interoperable authorization (the last three requirements)

CADC and INAF have and interoperable prototype

Existing standard? - Voot - http://openvoot.org/protocol/

Questions?

Brian Major, Patrick Dowler, Adrian Damian

Canadian Astronomy Data Centre

IVOA - October 2016