

Federations and interfederation plus/minus 3 years



David Simonsen
Rome, 30th of March 2009
www.wayf.dk

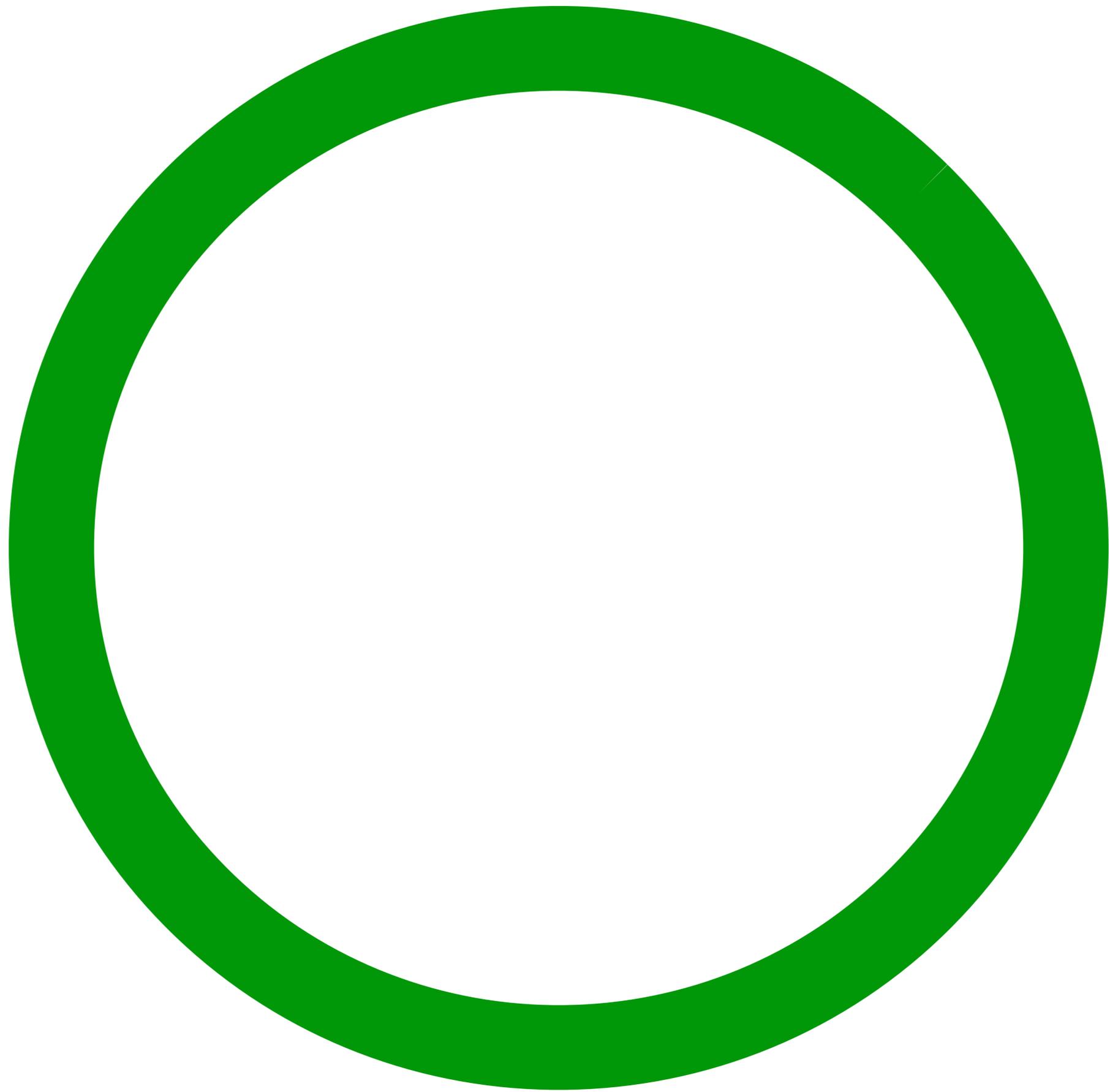
**What is ID federation
and
role based
access control?**

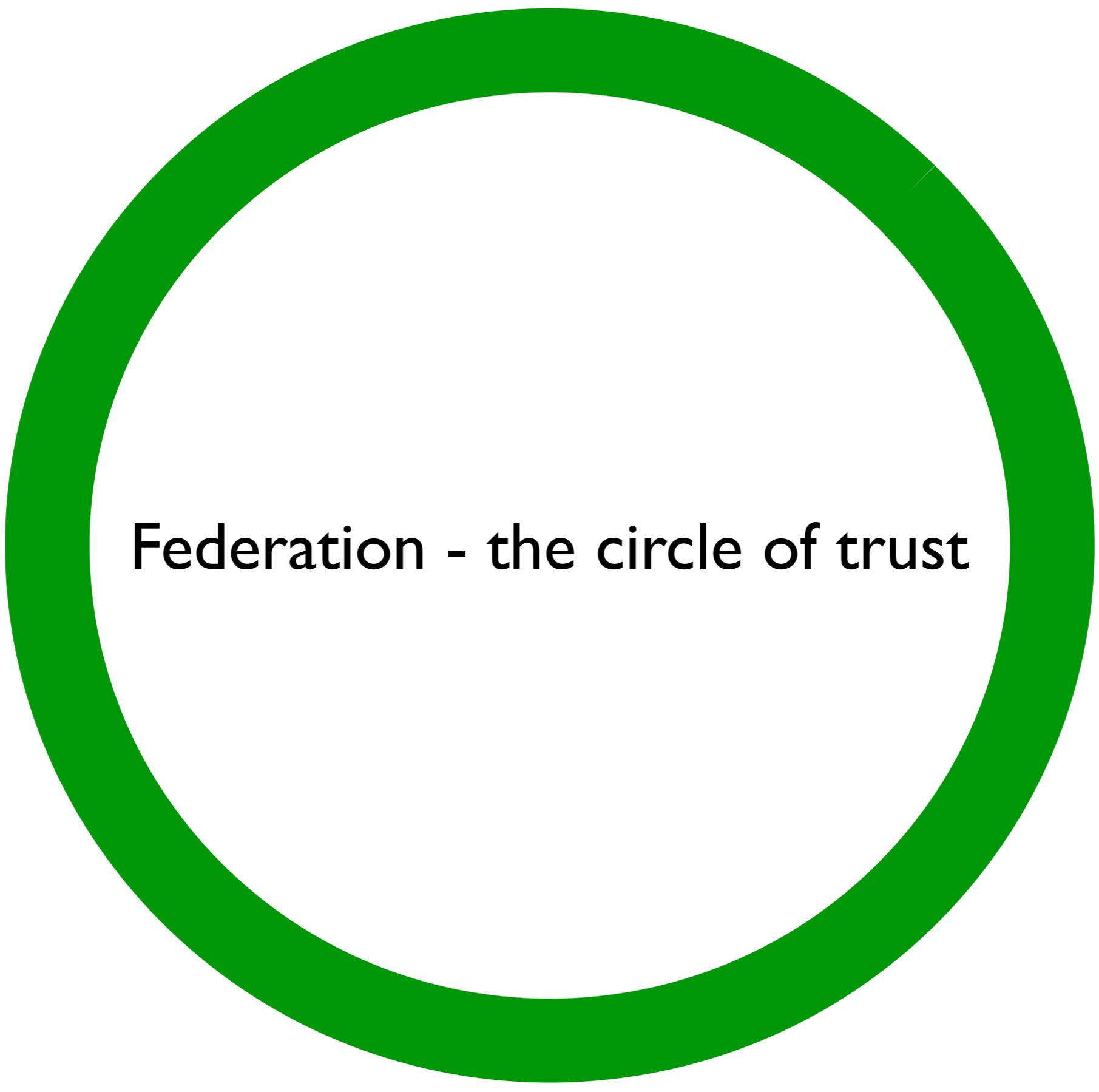


"On the Internet, nobody knows you're a dog."

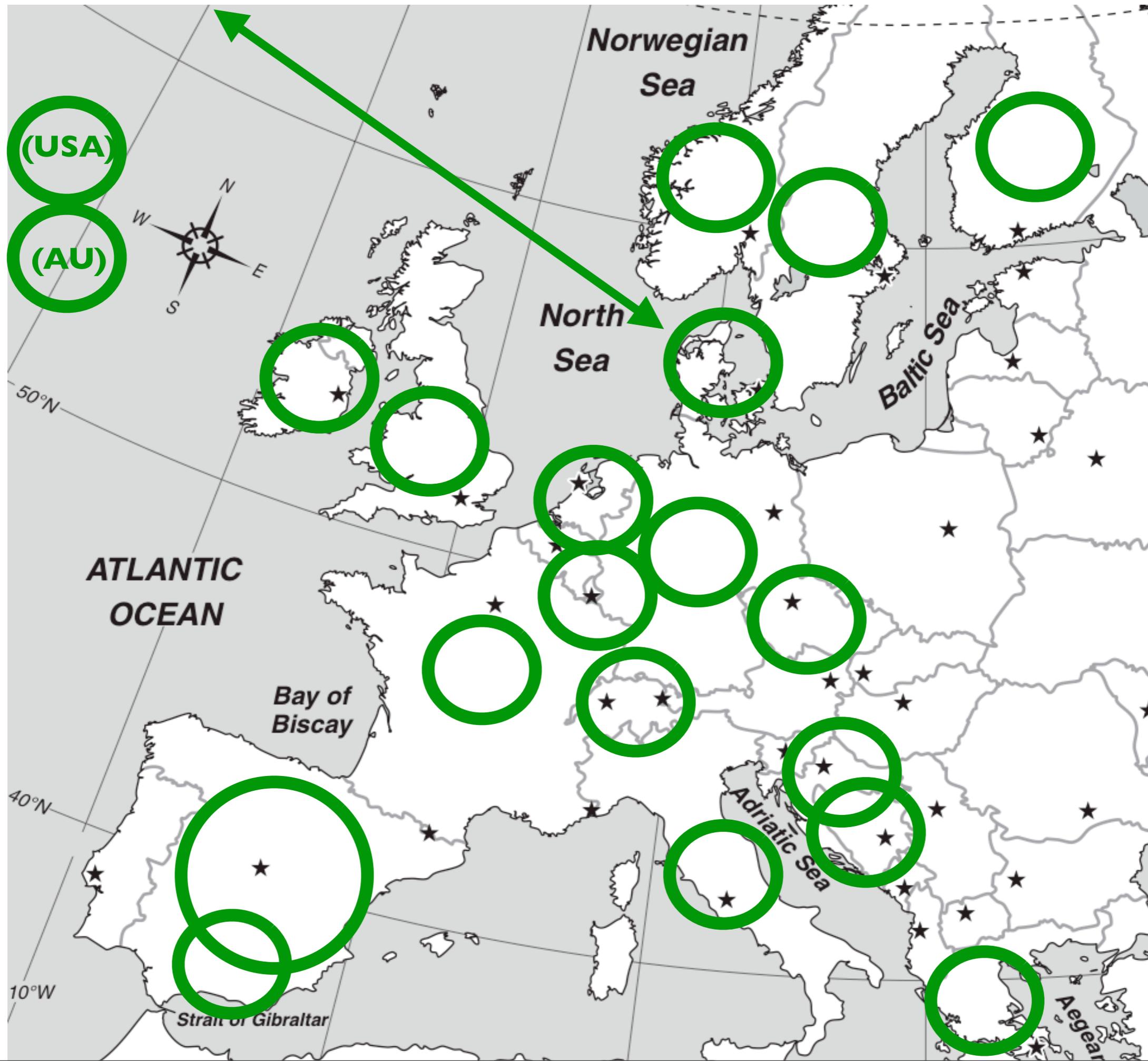


"On the Internet, nobody knows you're a dog."





Federation - the circle of trust



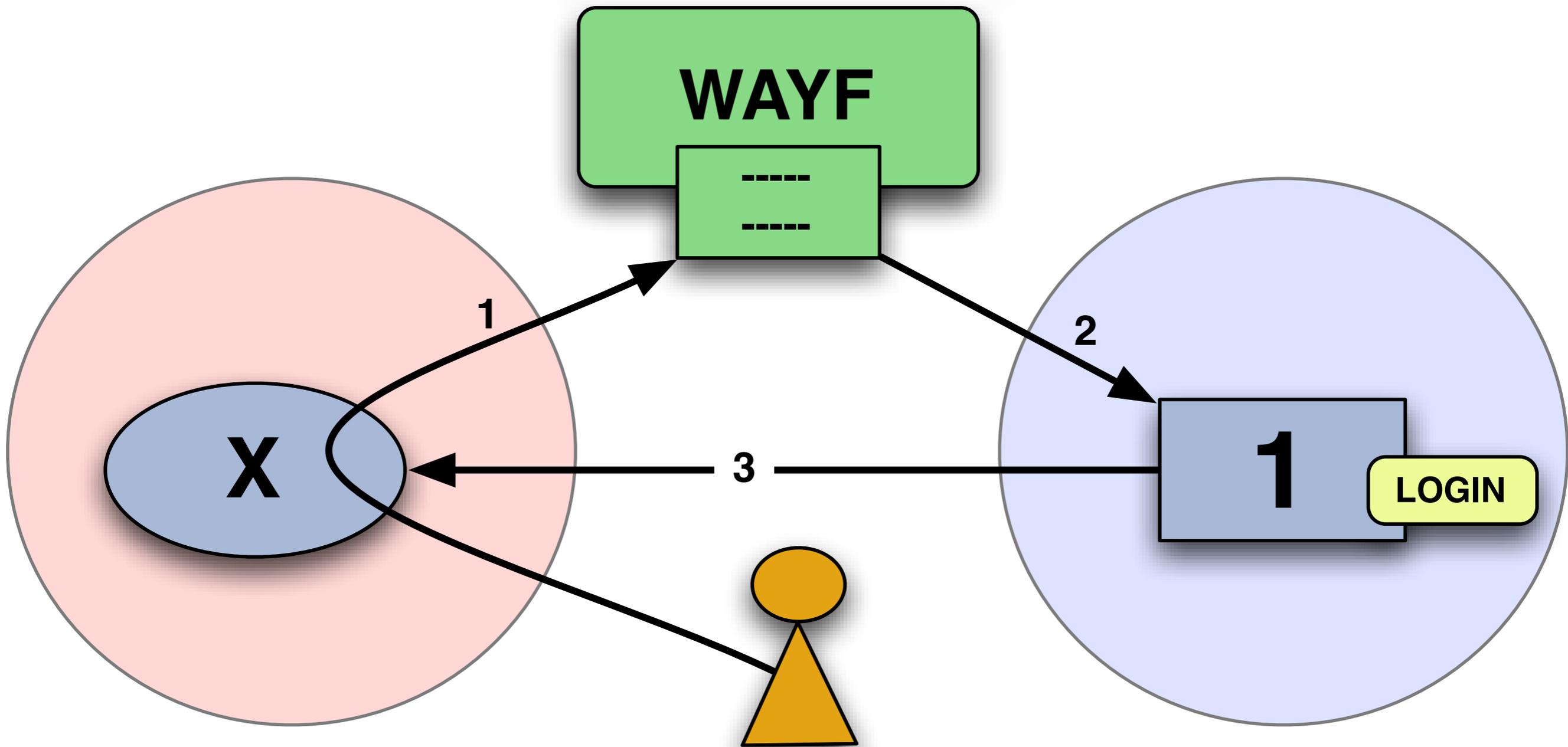
(USA)

(AU)

Basic concept

Service

Institution

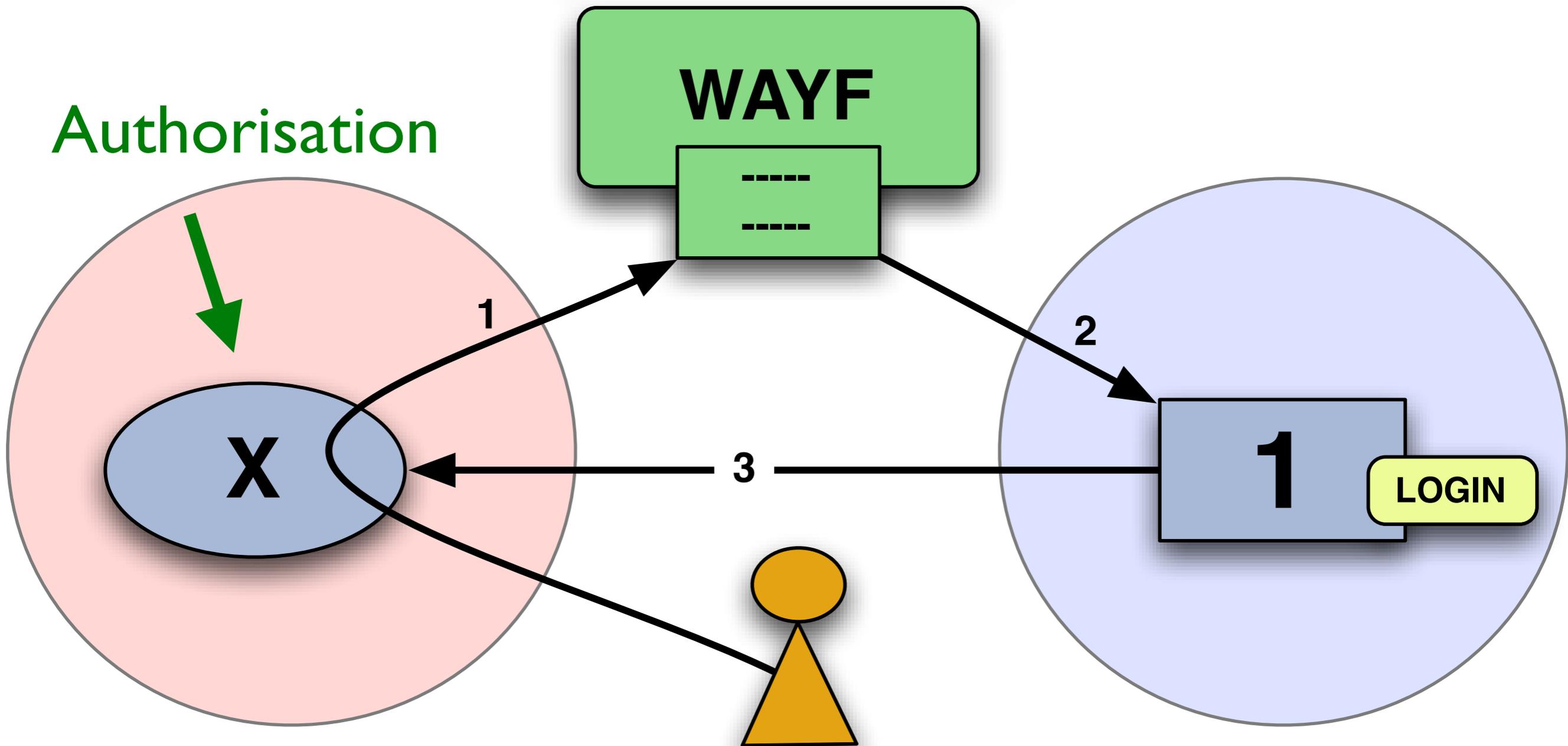


Basic concept

Service

Institution

Authorisation



Why federate?

Why federate?

- To provide more services to the users

Why federate?

- To provide more services to the users
- To get more users to the services

Why federate?

- To provide more services to the users
- To get more users to the services
- To have fewer user names + passwords

Why federate?

- To provide more services to the users
- To get more users to the services
- To have fewer user names + passwords
- To introduce role based access management

Why federate?

- To provide more services to the users
- To get more users to the services
- To have fewer user names + passwords
- To introduce role based access management
- To be independant of place and time (IP-adr)

Why federate?

- To provide more services to the users
- To get more users to the services
- To have fewer user names + passwords
- To introduce role based access management
- To be independant of place and time (IP-adr)
- To provide services to others

How to federate

How to federate

- Choose your lingua franca

How to federate

- Choose your lingua franca
- Choose your vocabulary

How to federate

- Choose your lingua franca
- Choose your vocabulary
- Write common rules for the federation

How to federate

- Choose your lingua franca
- Choose your vocabulary
- Write common rules for the federation
- Select an architecture

How to federate

- Choose your lingua franca
- Choose your vocabulary
- Write common rules for the federation
- Select an architecture
- Start building!

Where to federate?

Where to federate?

- National federation

Where to federate?

- National federation
- Intra-institutional federations

Where to federate?

- National federation
- Intra-institutional federations
- Internationally

Where to federate?

- National federation
- Intra-institutional federations
- Internationally



Where to federate?

- National federation
- Intra-institutional federations
- Internationally



教育漫遊

Several ways to federate



Several ways to federate



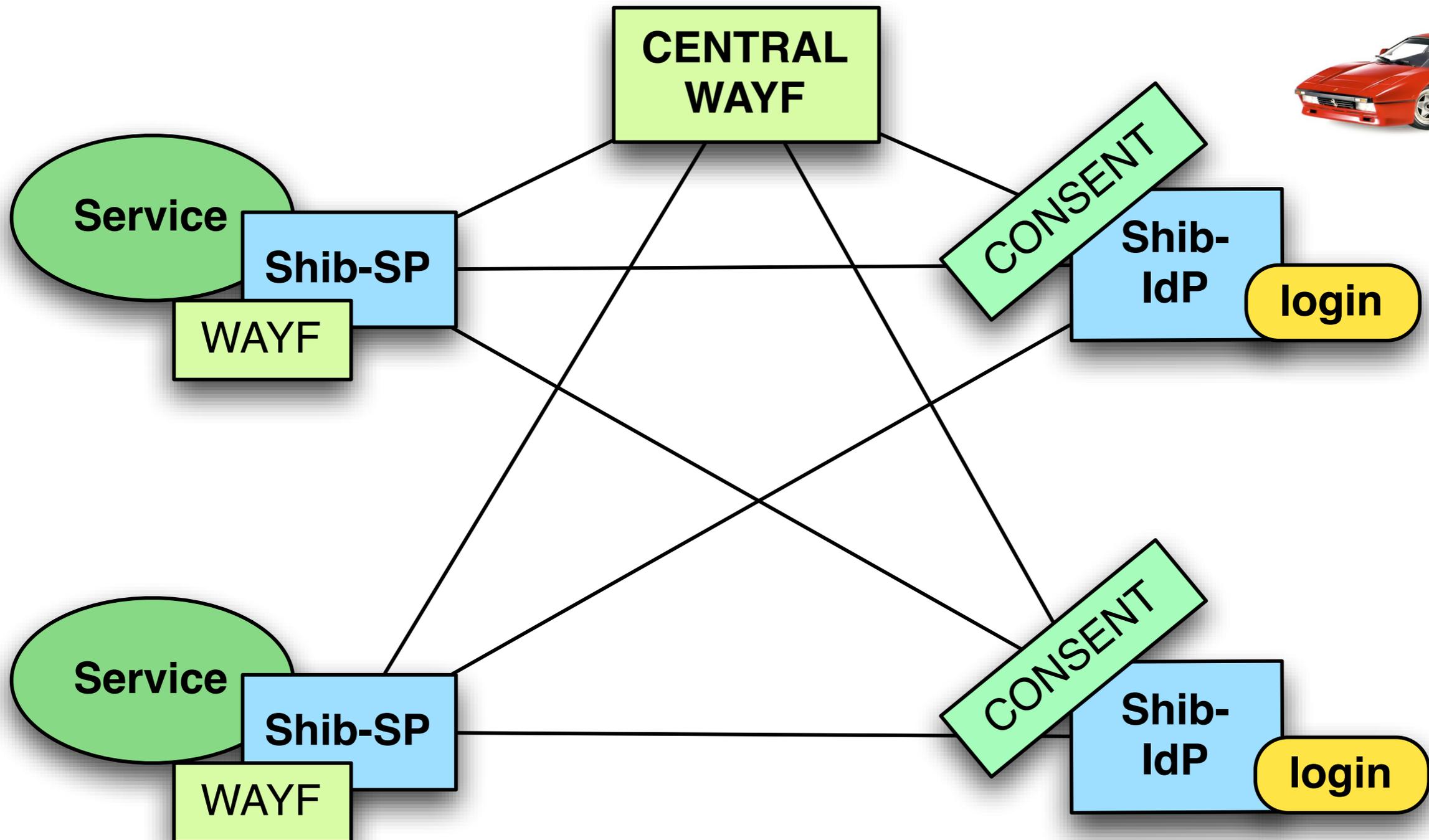
Several ways to federate



Loosely coupled, Shibboleth

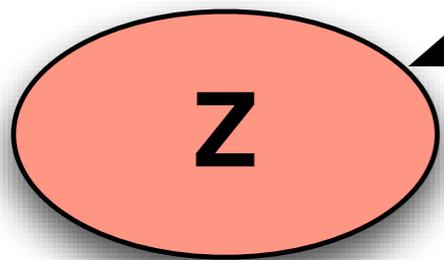
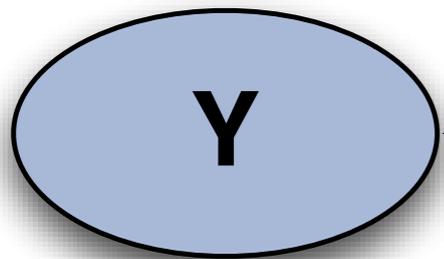
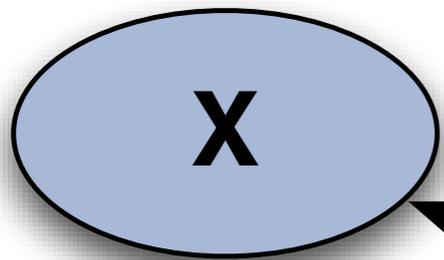
Services

Institutions

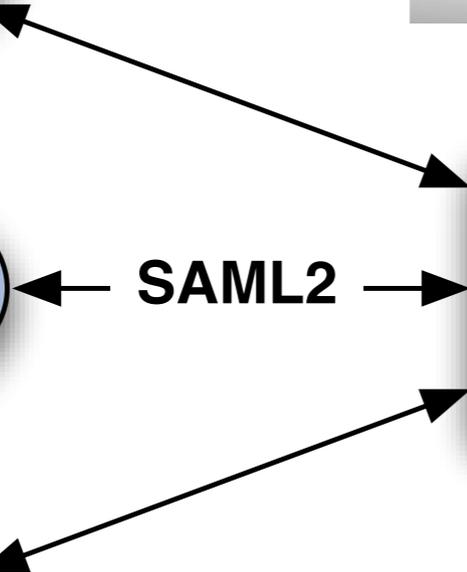
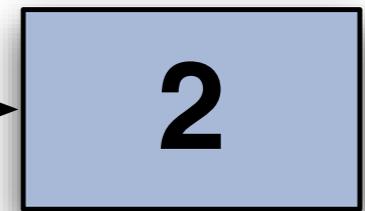


Central login, Norway

Services



Institutions

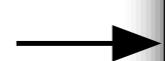


SAML2

LDAP

LDAP

LDAP



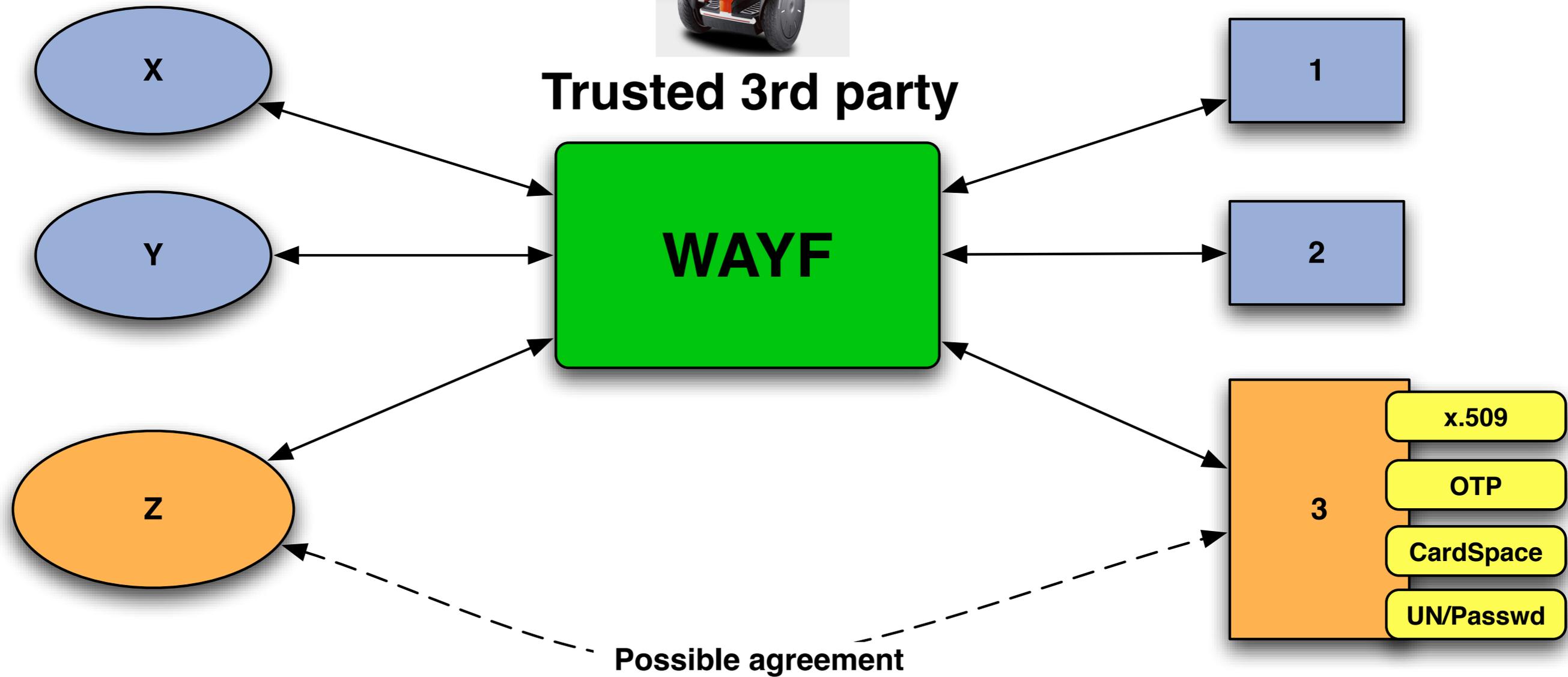
Decentralal login, Denmark



Services

Institutions

Trusted 3rd party



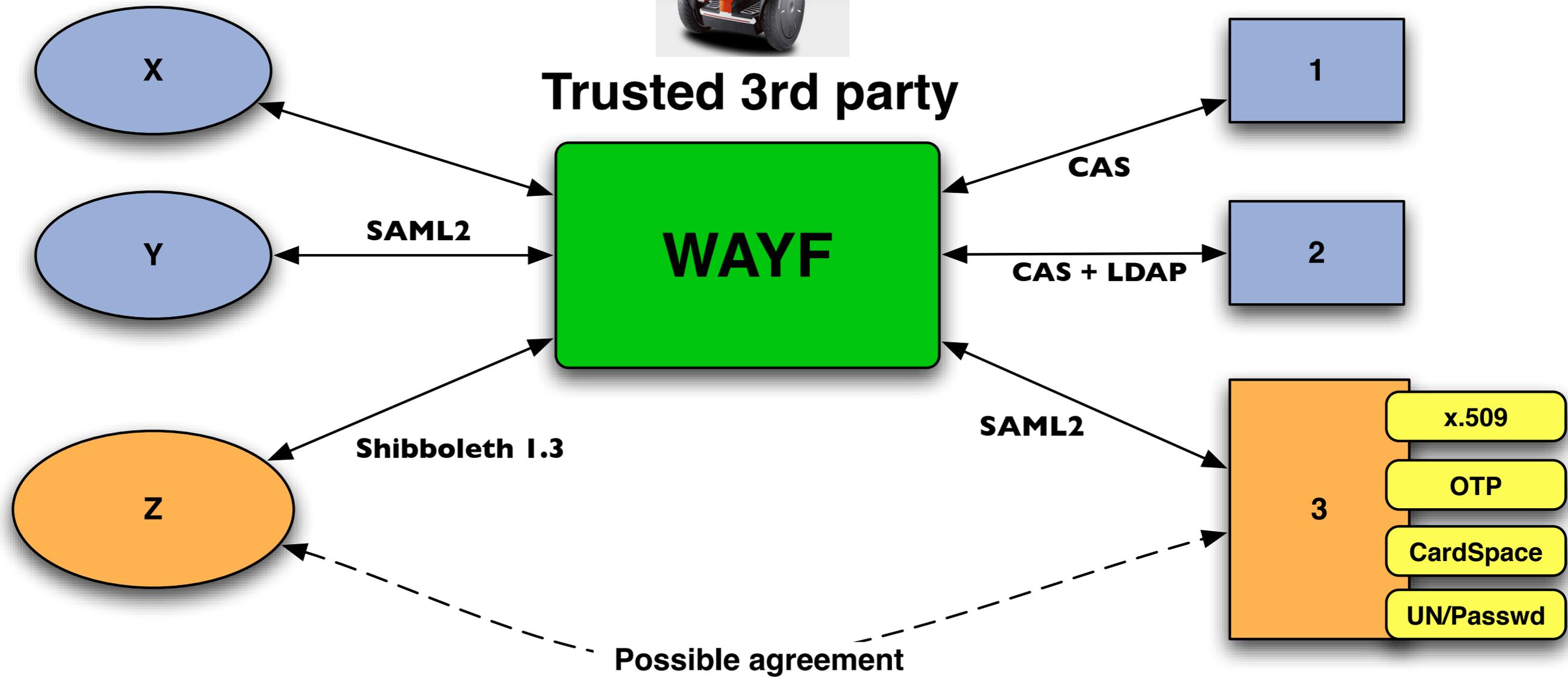
Decentralal login, Denmark



Services

Institutions

Trusted 3rd party



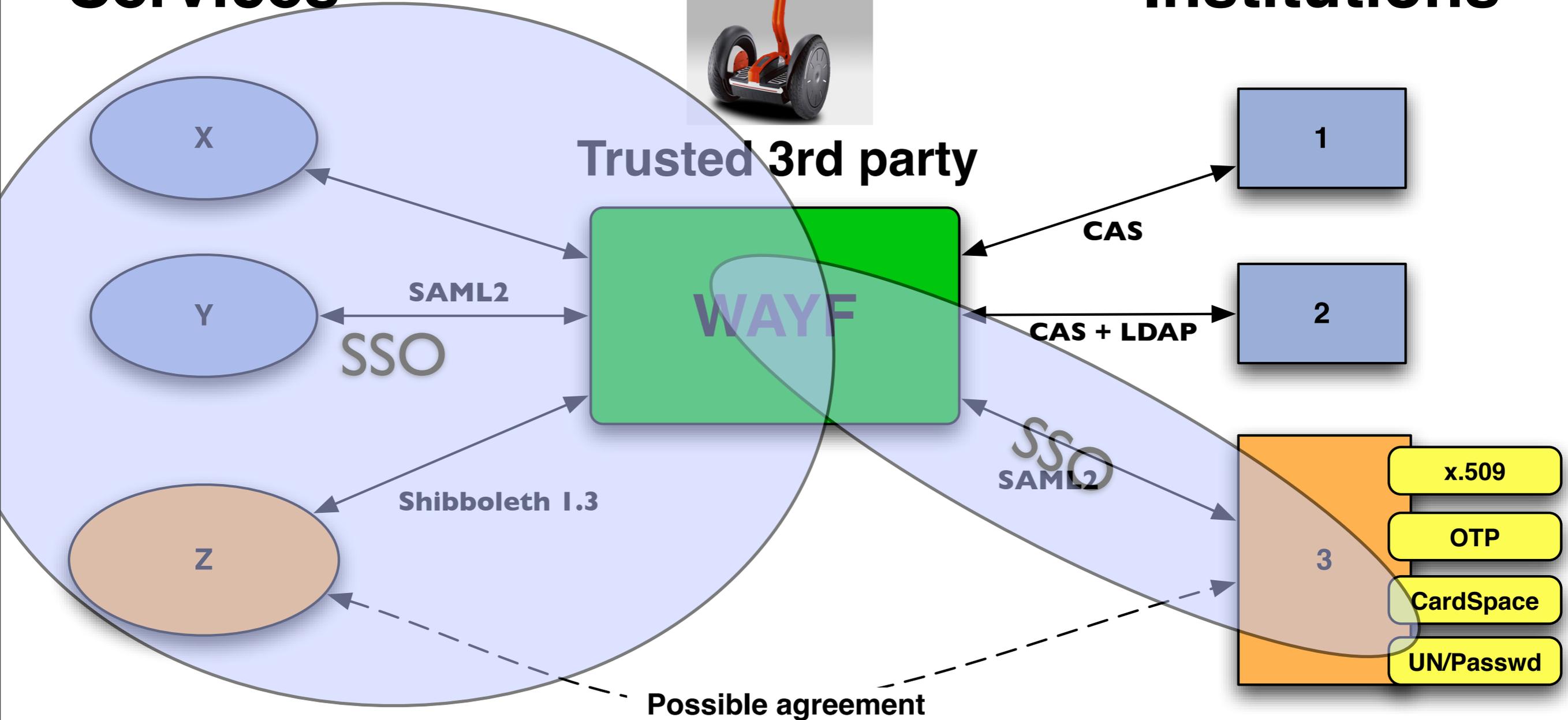
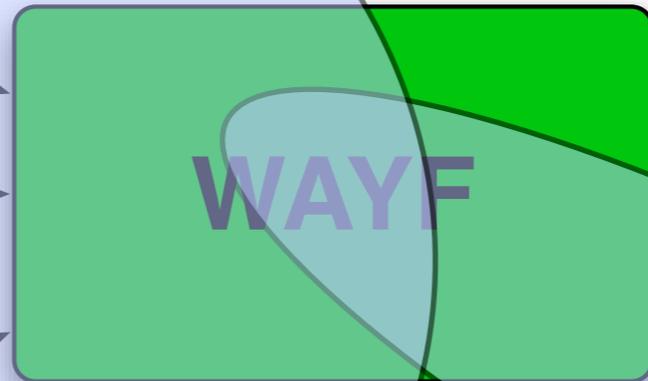
Decentralal login, Denmark



Services

Institutions

Trusted 3rd party



Possible agreement

What gets easy?

What gets easy?

- Connecting services

What gets easy?

- Connecting services
- User management

What gets easy?

- Connecting services
- User management
- Pseudonomisation (a good thing!)

What gets easy?

- Connecting services
- User management
- Pseudonomisation (a good thing!)
- Verification

What stays the same?

What stays the same?

- Authorisation (will I let you in?)

What stays the same?

- Authorisation (will I let you in?)
- Business relations (the bill goes to ...)

What is difficult?

What is difficult?

- Introducing a new concept
 - to institutions
 - to service providers
 - to the users (?)

What is difficult?

- Introducing a new concept
 - to institutions
 - to service providers
 - to the users (?)
- Federation policy

What is difficult?

- Introducing a new concept
 - to institutions
 - to service providers
 - to the users (?)
- Federation policy
- Attribute release policies

What is difficult?

- Introducing a new concept
 - to institutions
 - to service providers
 - to the users (?)
- Federation policy
- Attribute release policies
- User involvement (consent)

Users' informed consent

The consent must be:



Users' informed consent

The consent must be:

- Voluntary (no arm-twisting)



Users' informed consent

The consent must be:

- Voluntary (no arm-twisting)
- Specific (one purpose)



Users' informed consent

The consent must be:

- Voluntary (no arm-twisting)
- Specific (one purpose)
- Informed (understandable)



Users' informed consent

Qui tacet concentire videtur?

The consent must be:

- Voluntary (no arm-twisting)
- Specific (one purpose)
- Informed (understandable)



Users' informed consent

Qui tacet concentire videtur?

The consent must be:

- Voluntary (no arm-twisting)
- Specific (one purpose)
- Informed (understandable)



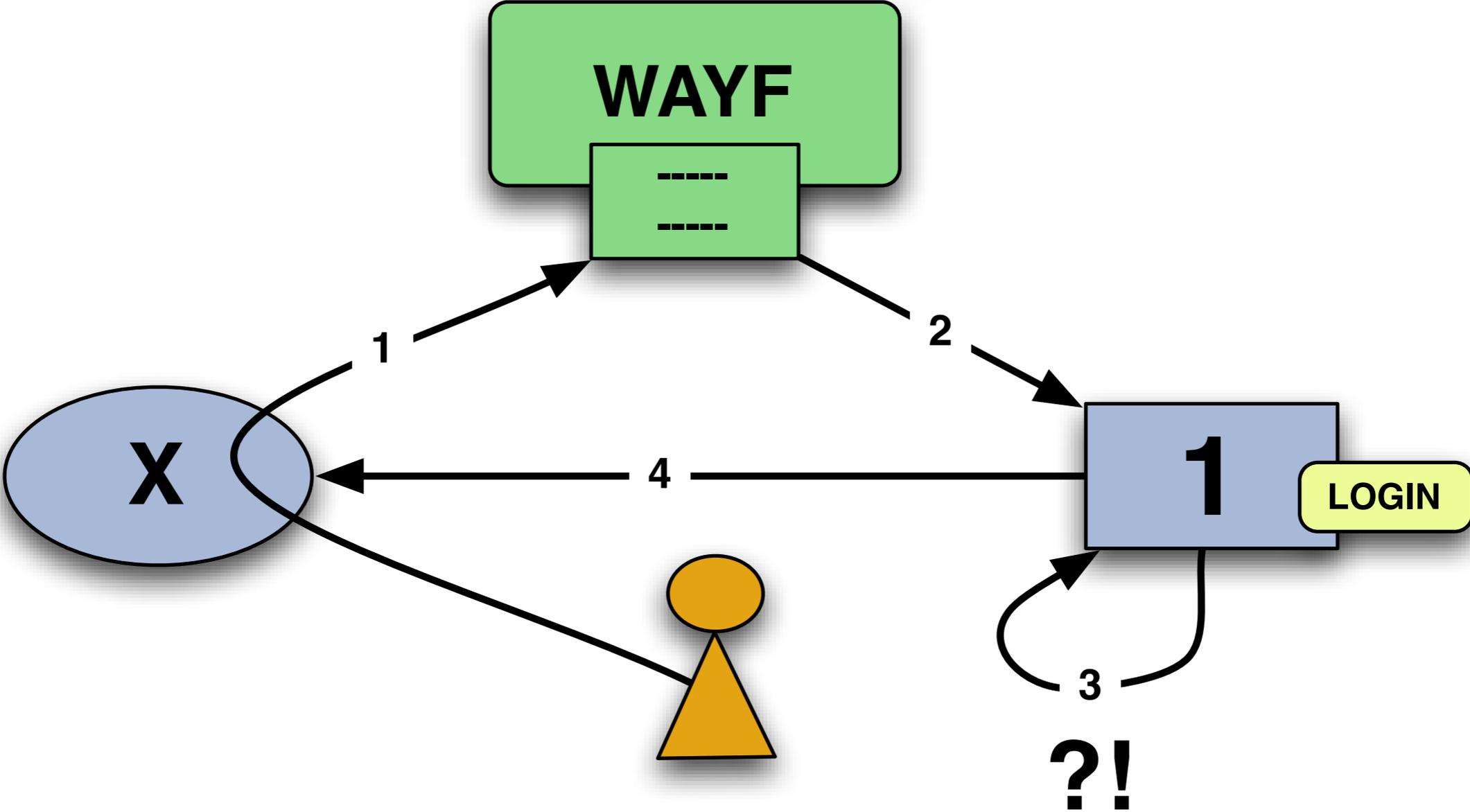
Users' informed consent

- The consent must be
- Voluntary (no coercion)
- Specific (one purpose)
- Informed (understanding)



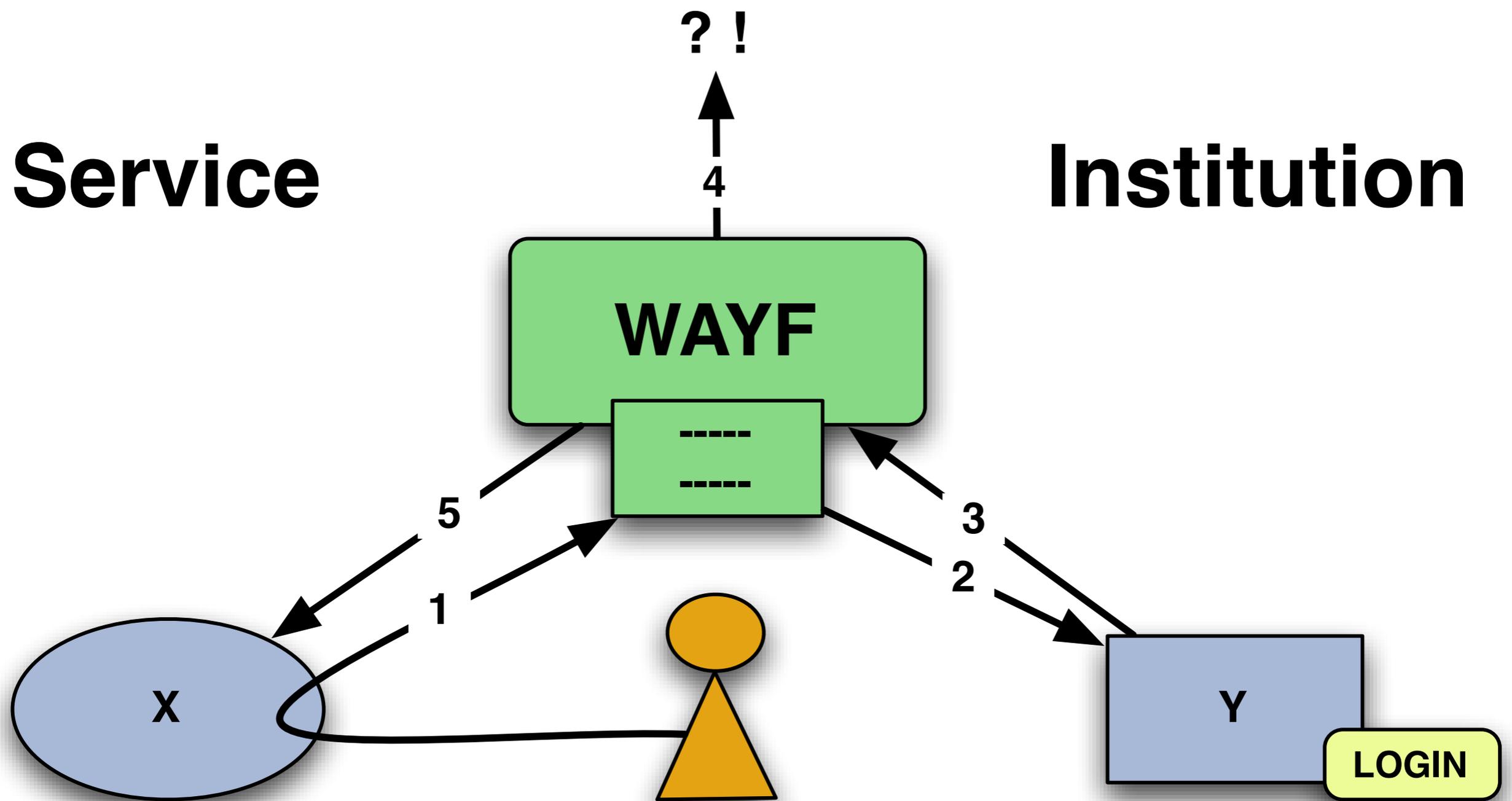
Service

Institution



Service

Institution



Personal pseudonyms

Services

Institution



Personal pseudonyms

Services

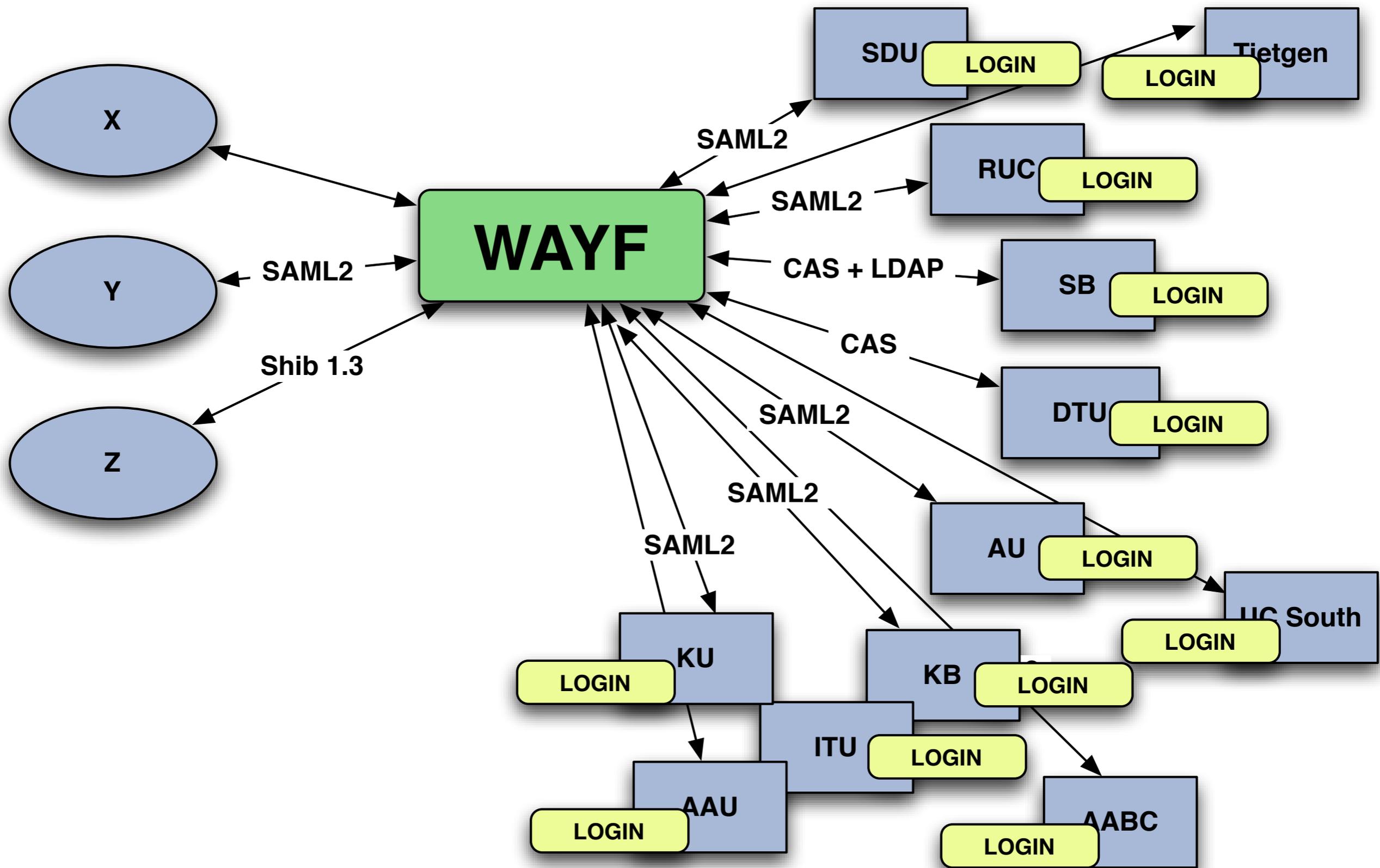
Institution



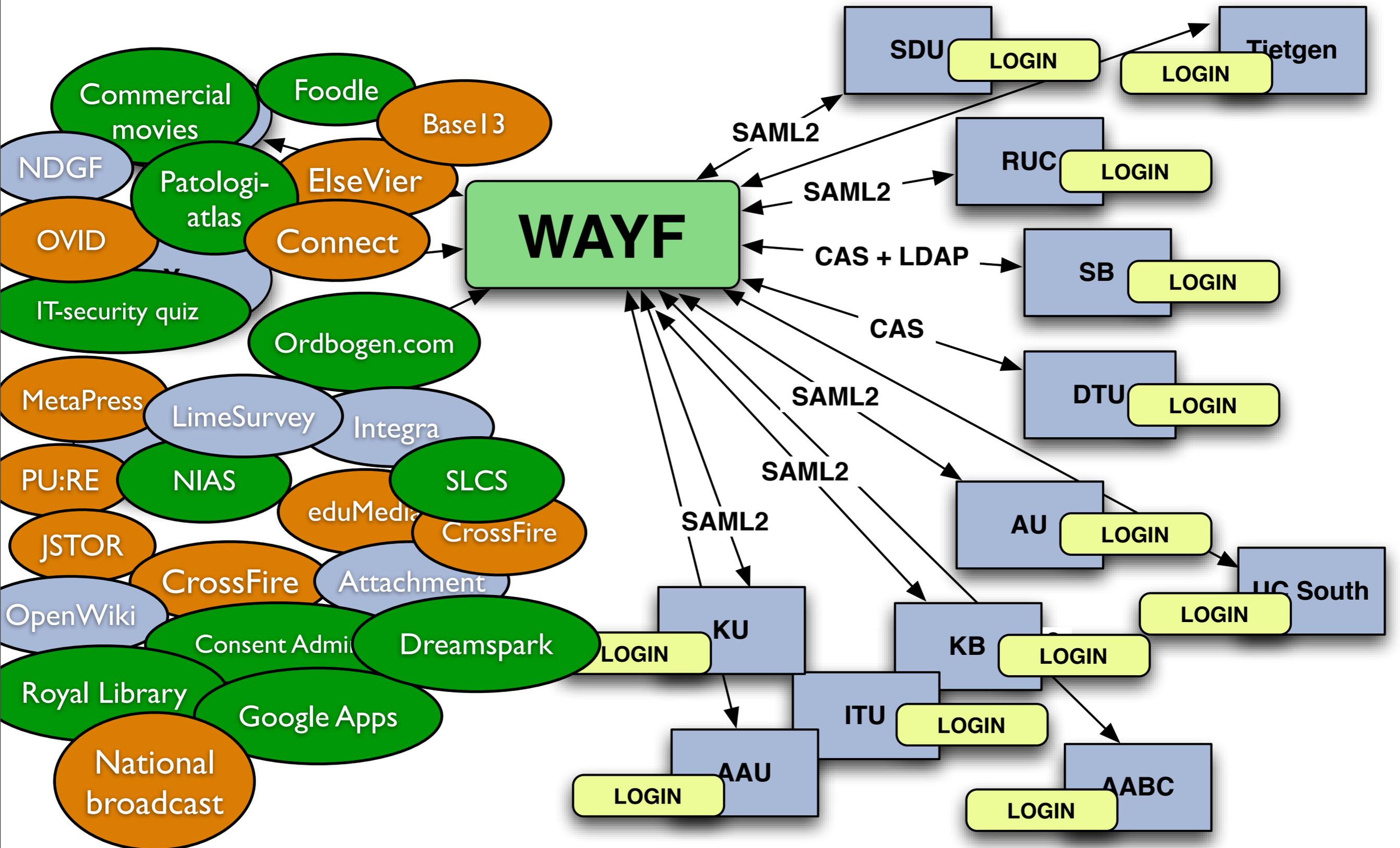
WAYF-DK-e2a67df2a8d2c7ea3891ab66f75acf4f8780850d

WAYF status: 3 years

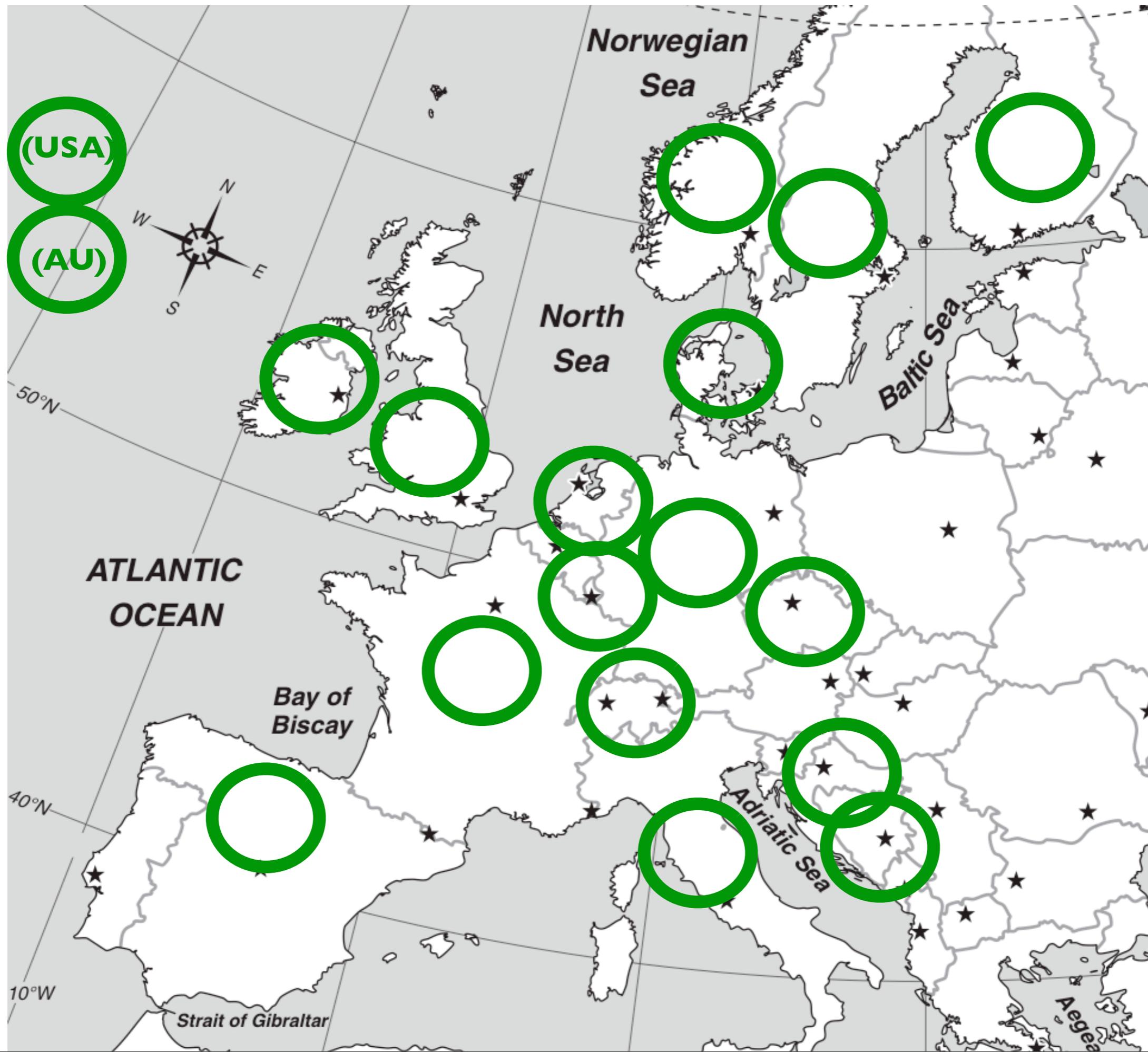
WAYF status: 3 years



WAYF status: 3 years

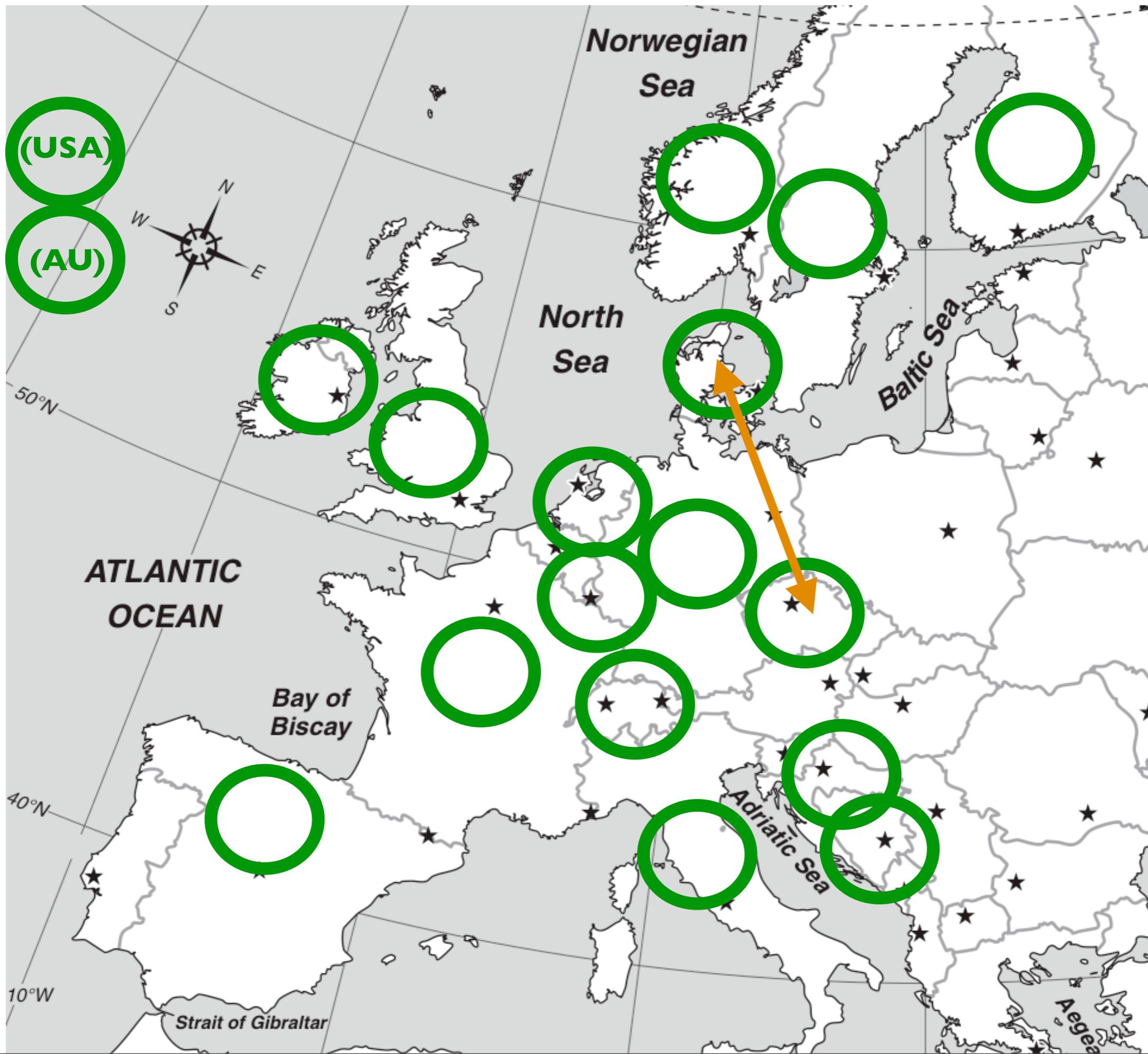


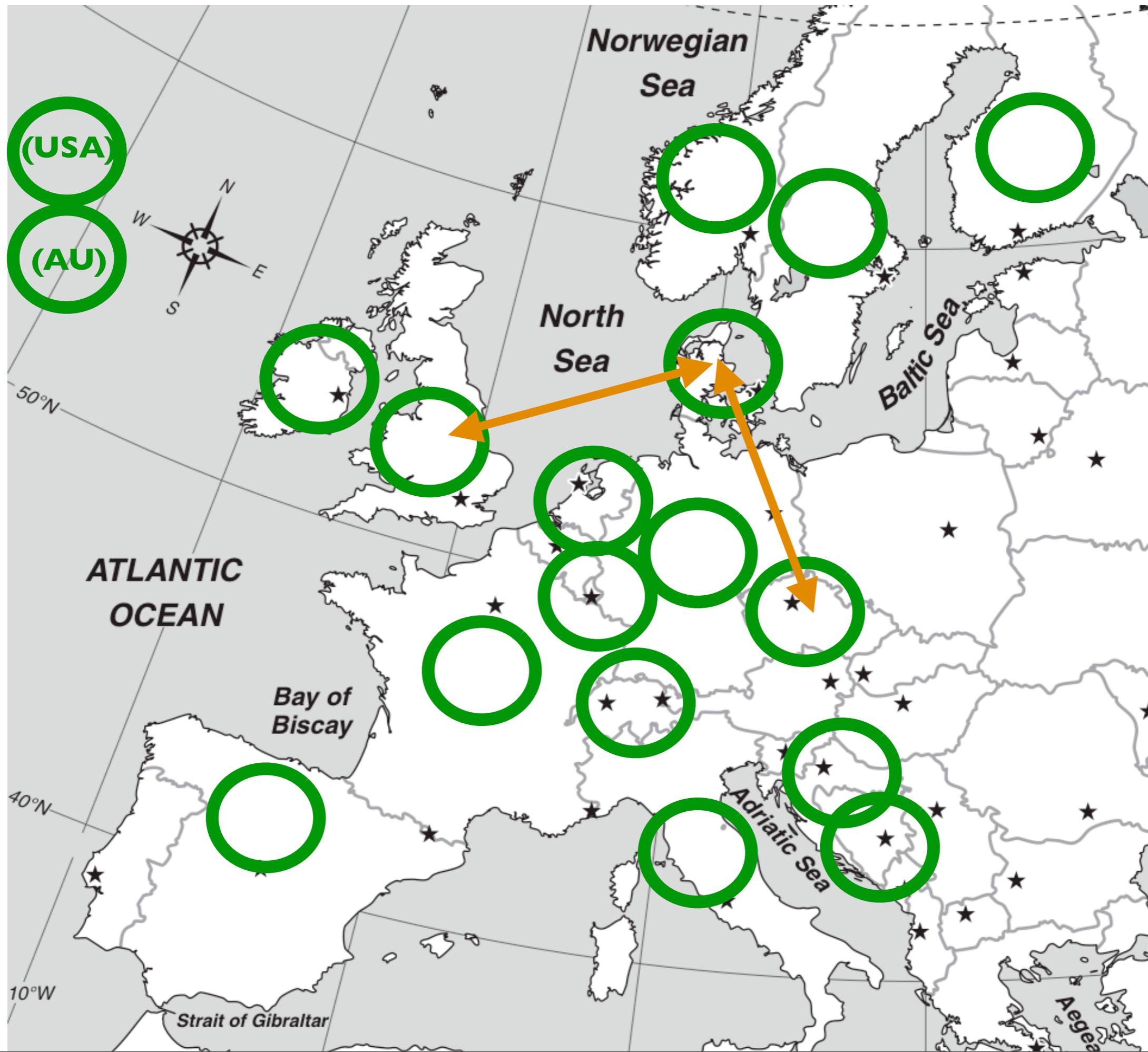
Interfederation

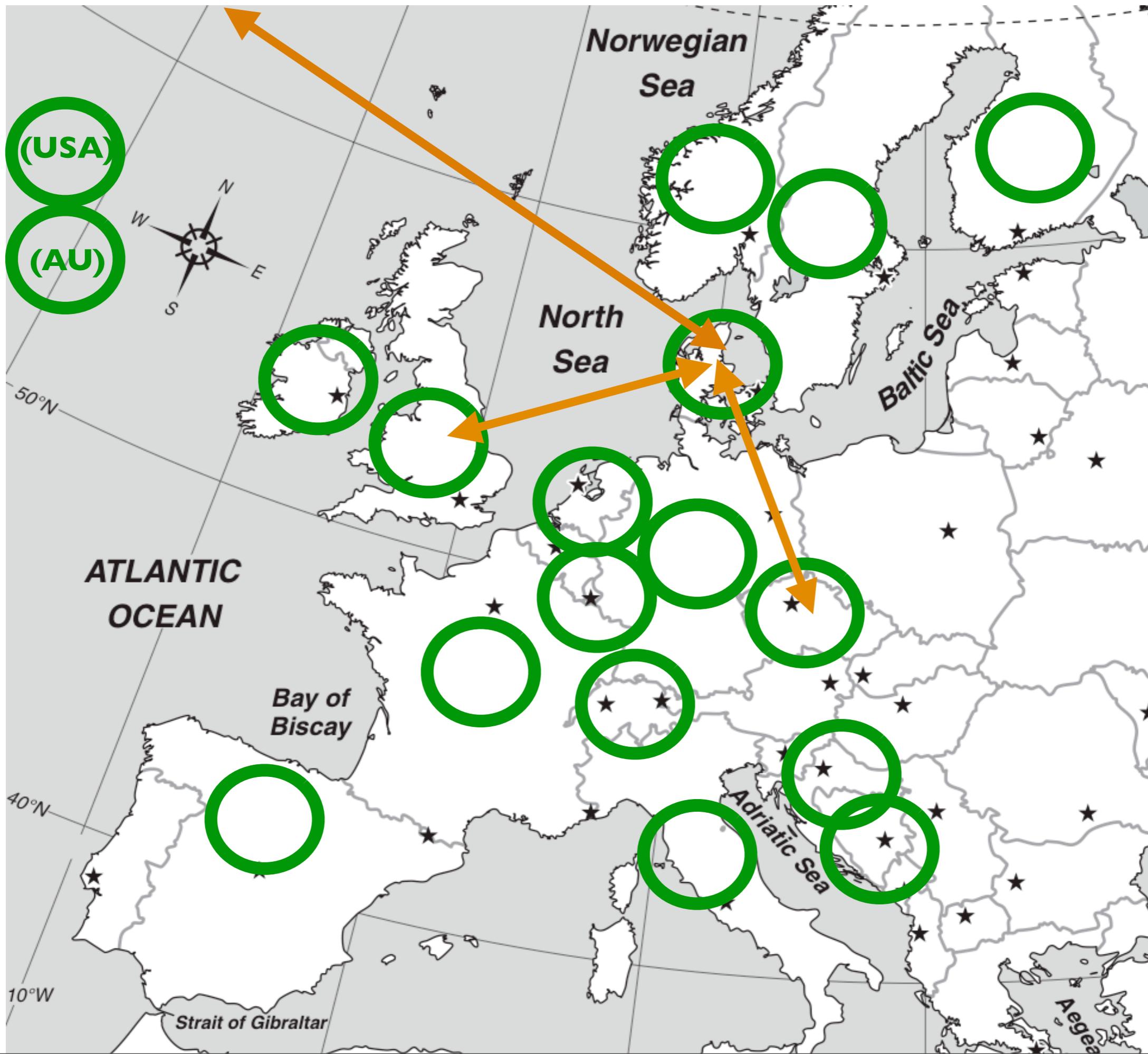


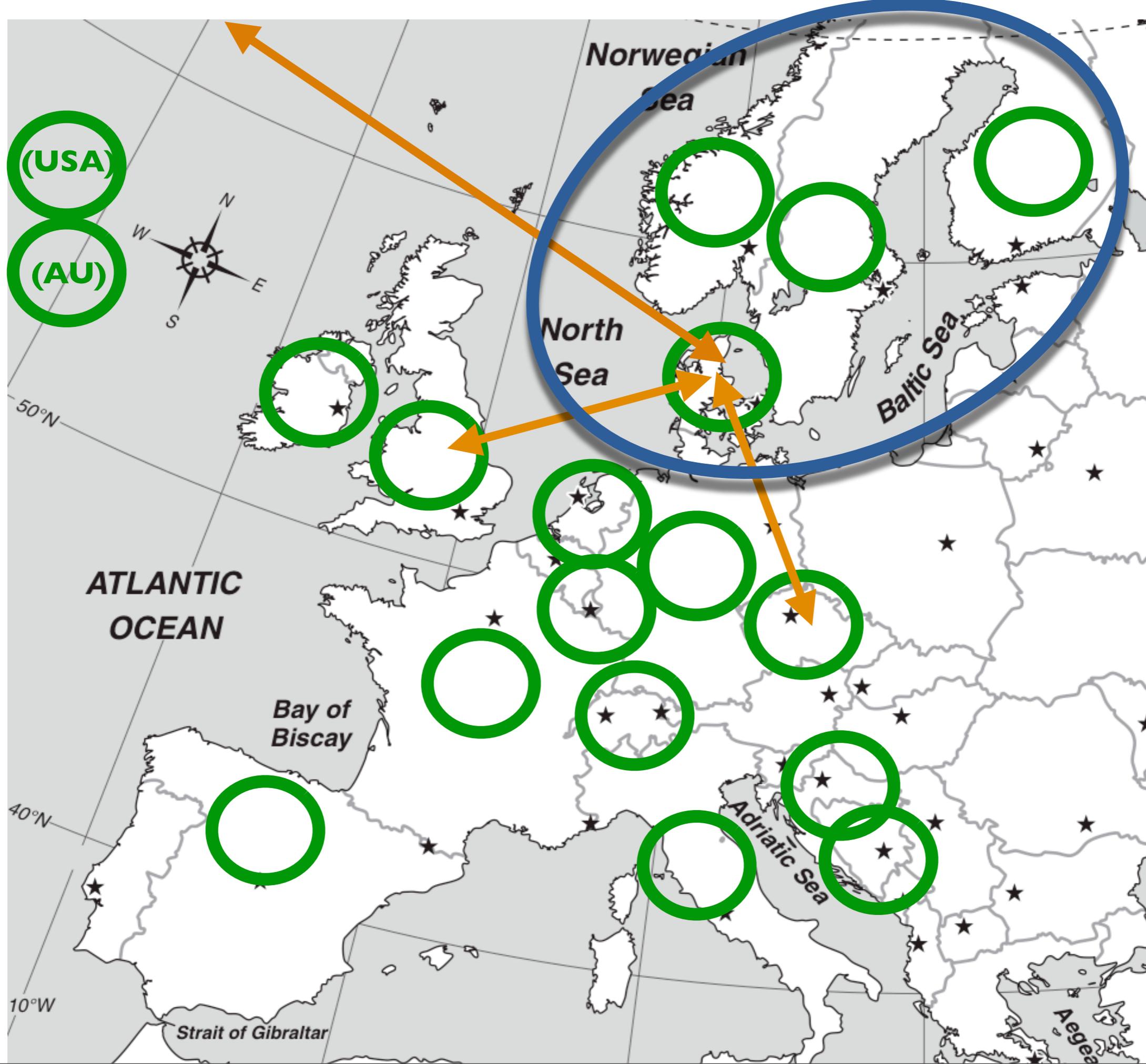
(USA)

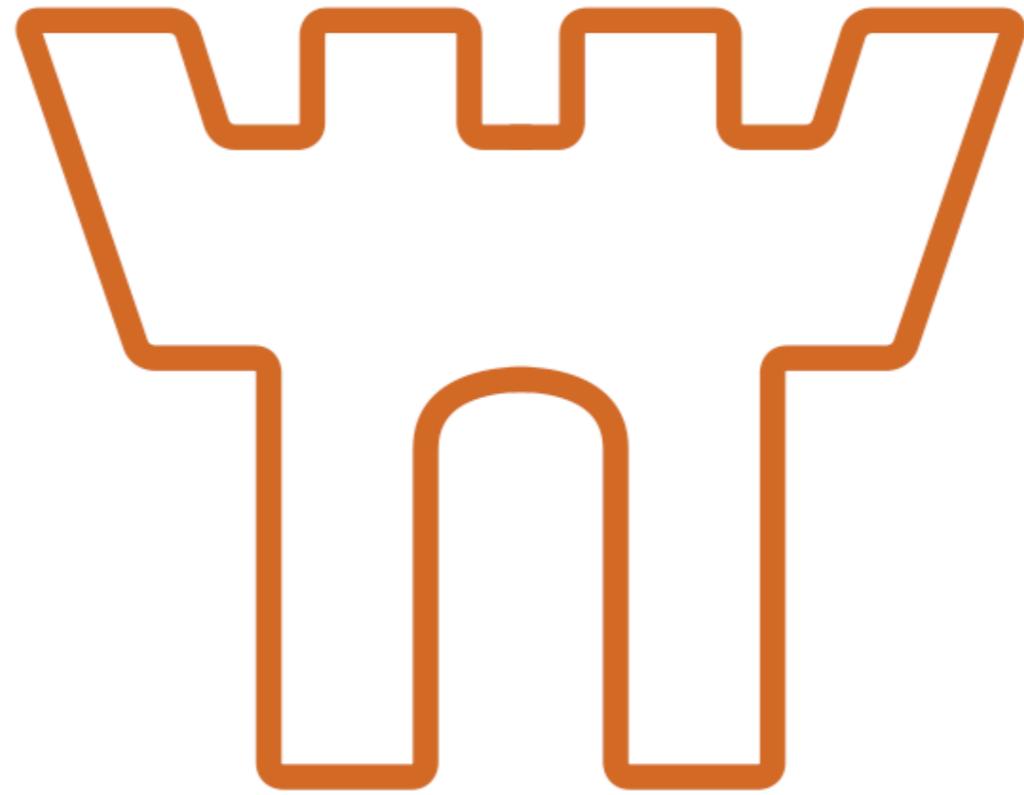
(AU)





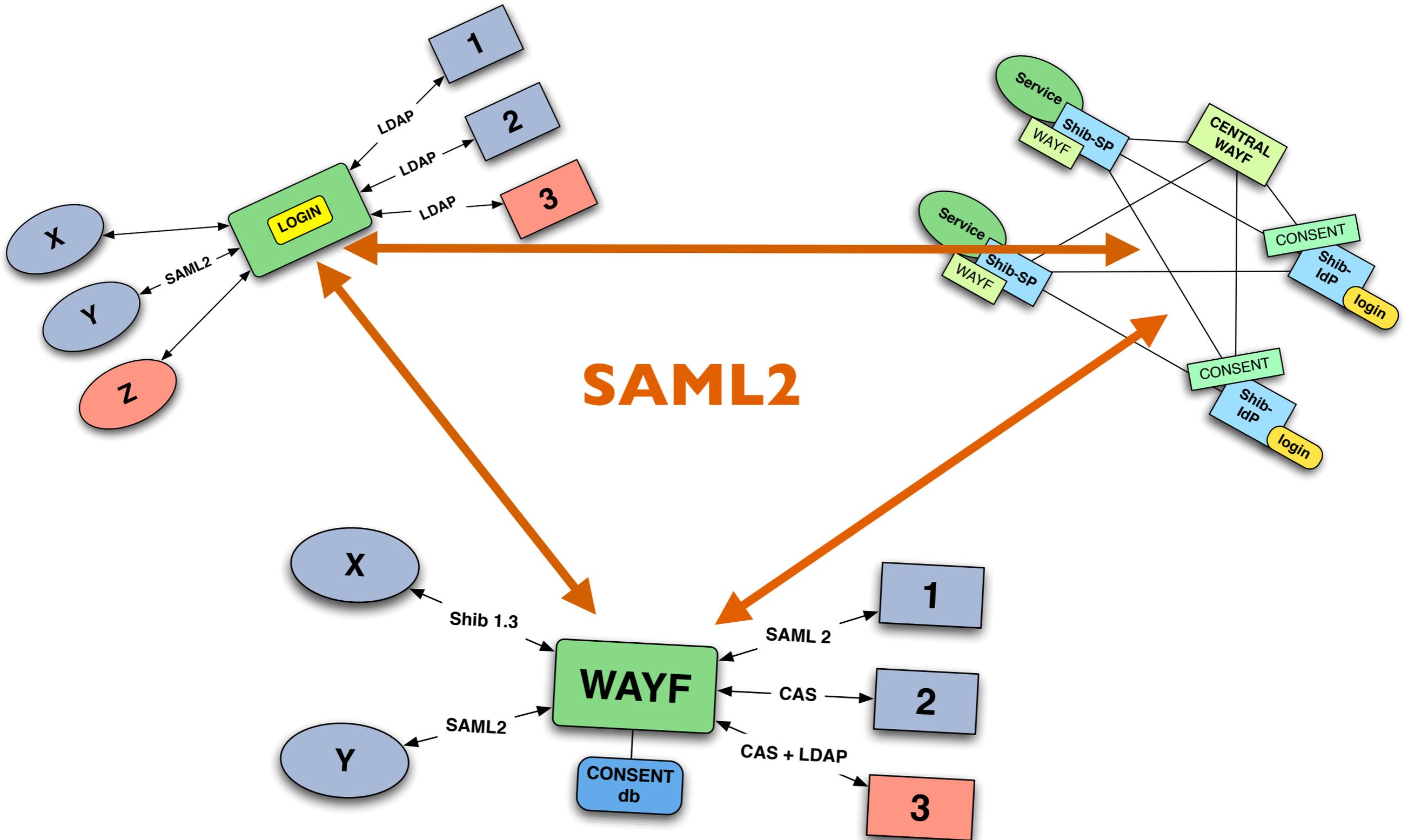


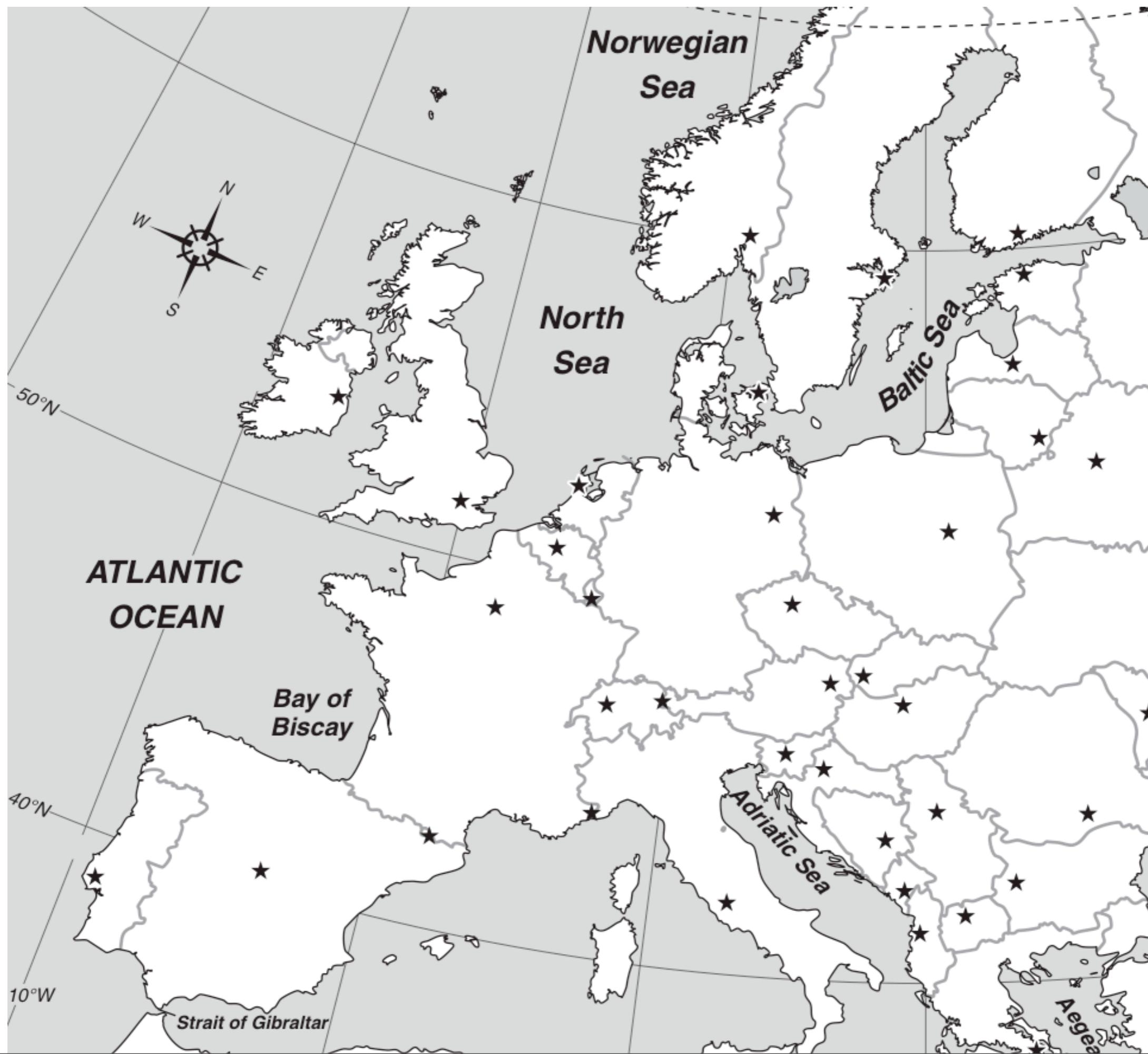


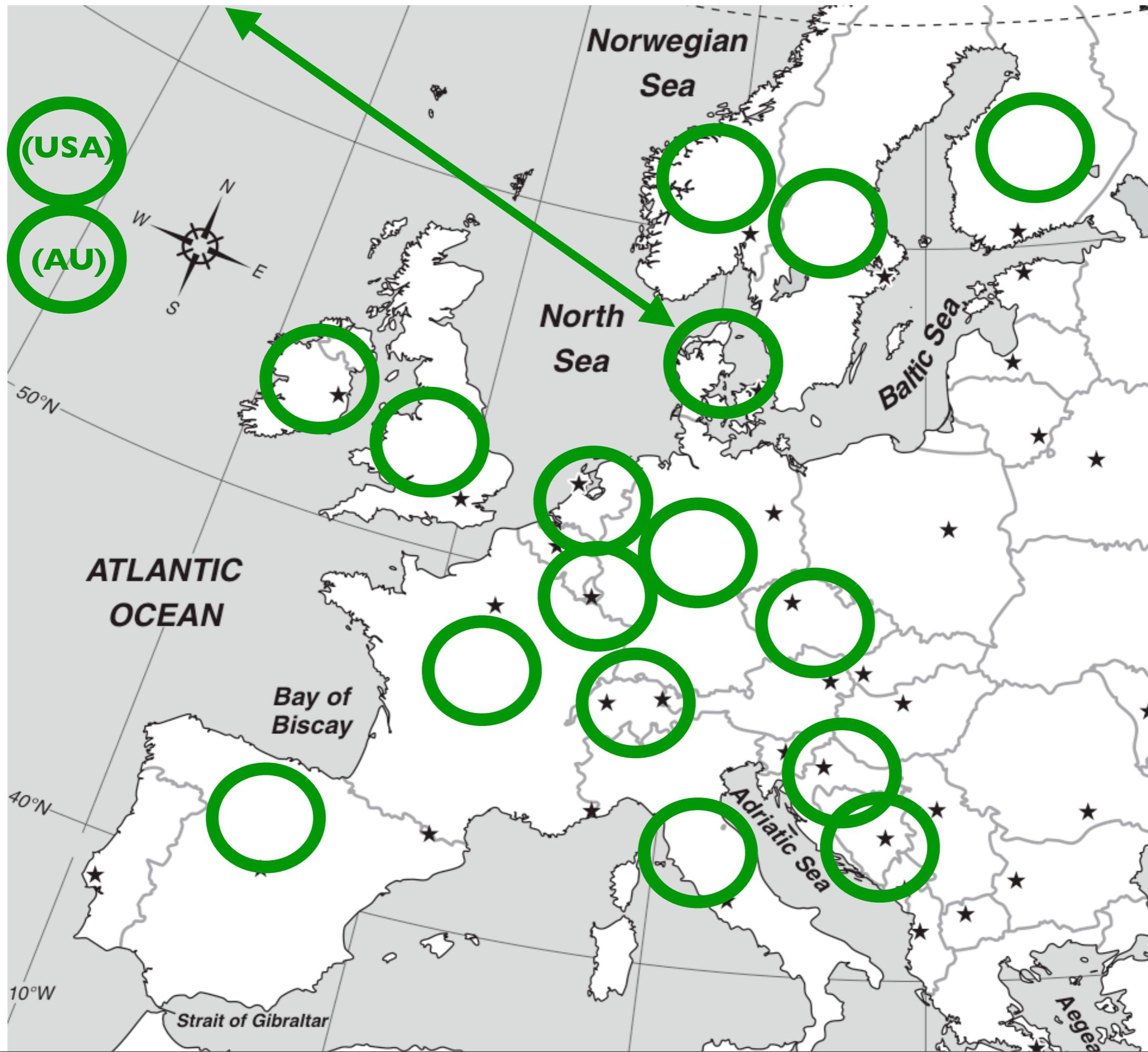


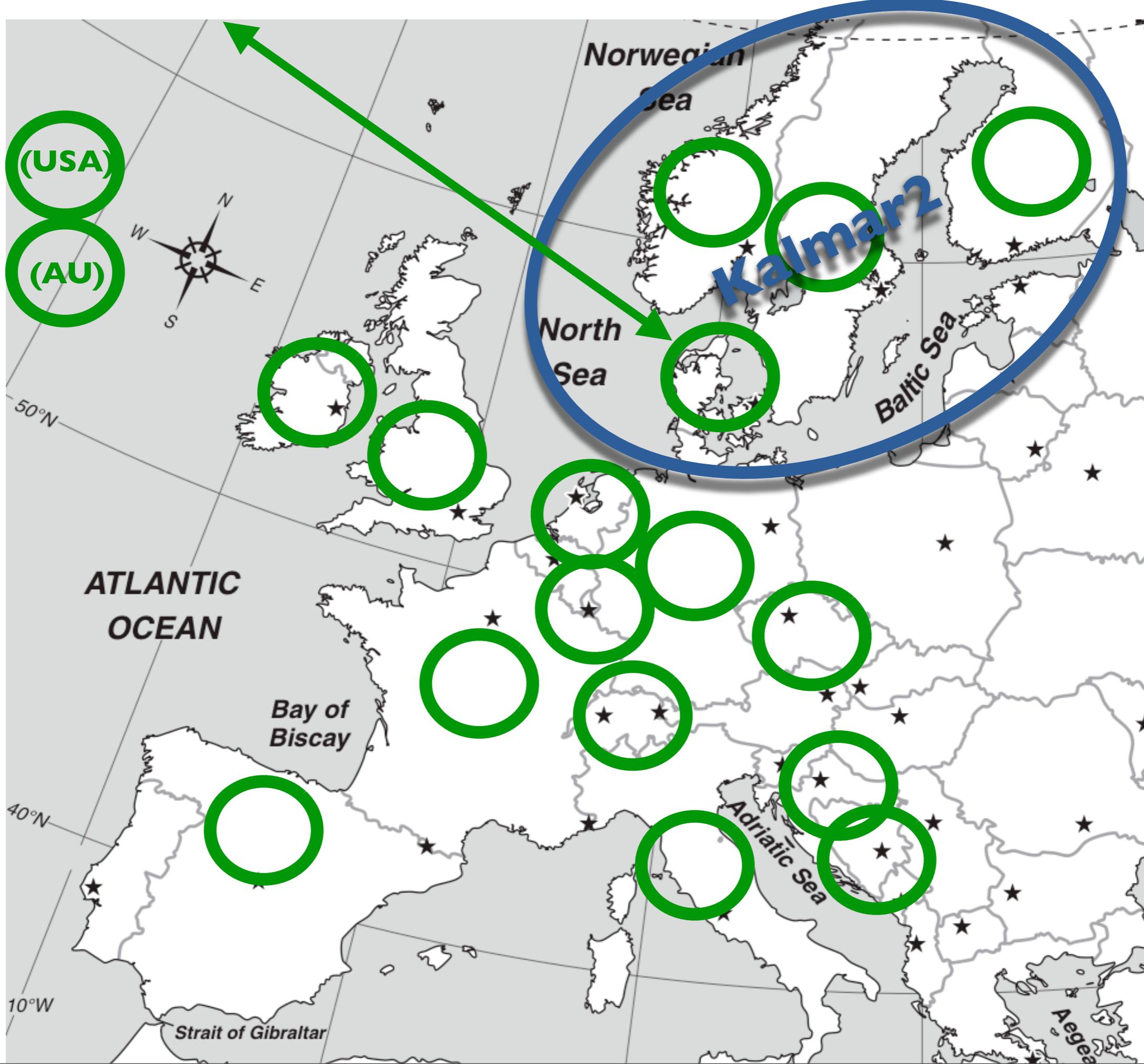
KALMAR2

Interfederation





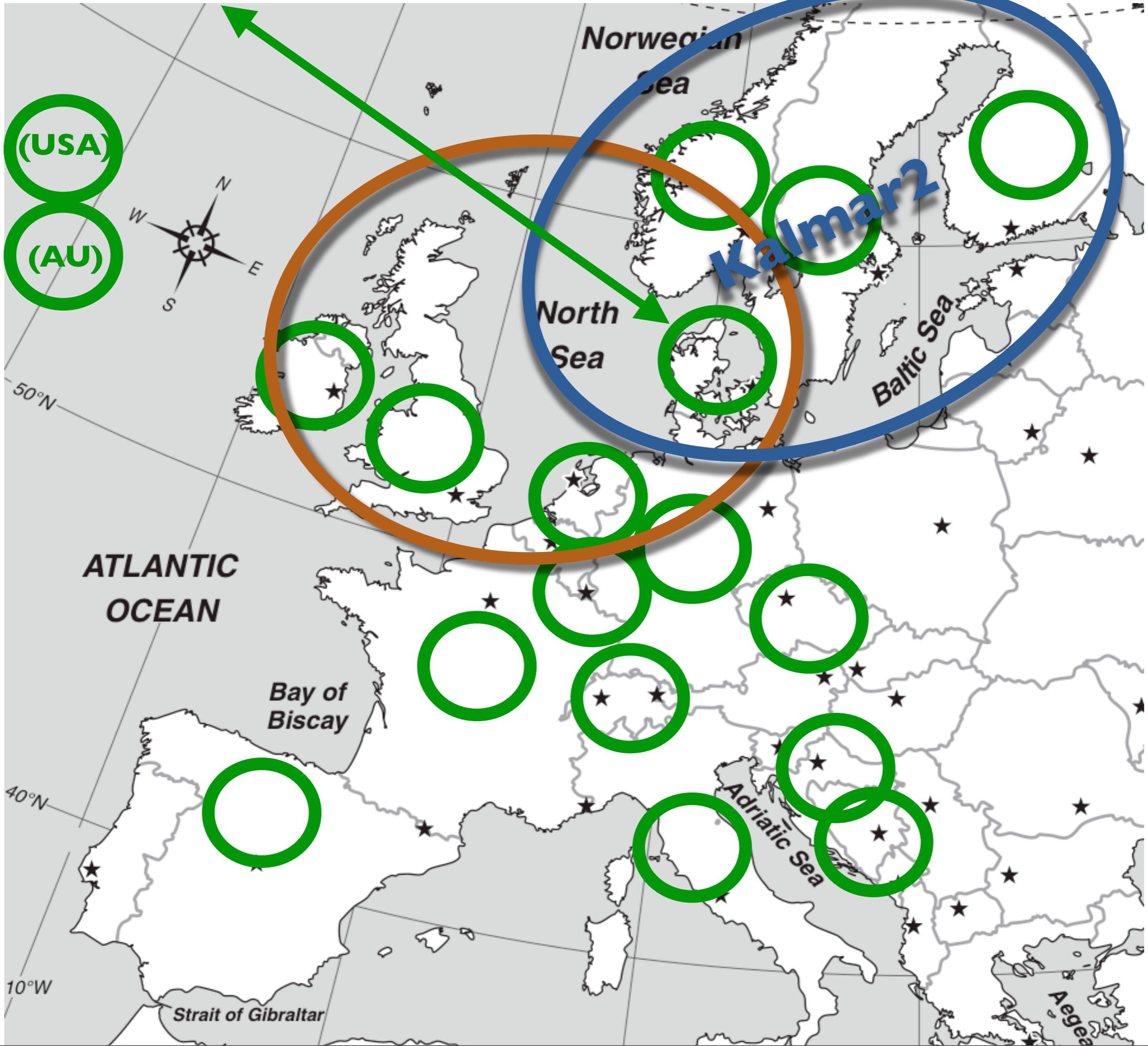




(USA)

(AU)

Kalmar2



(USA)

(AU)

Kalmar2

ATLANTIC OCEAN

Norwegian Sea

North Sea

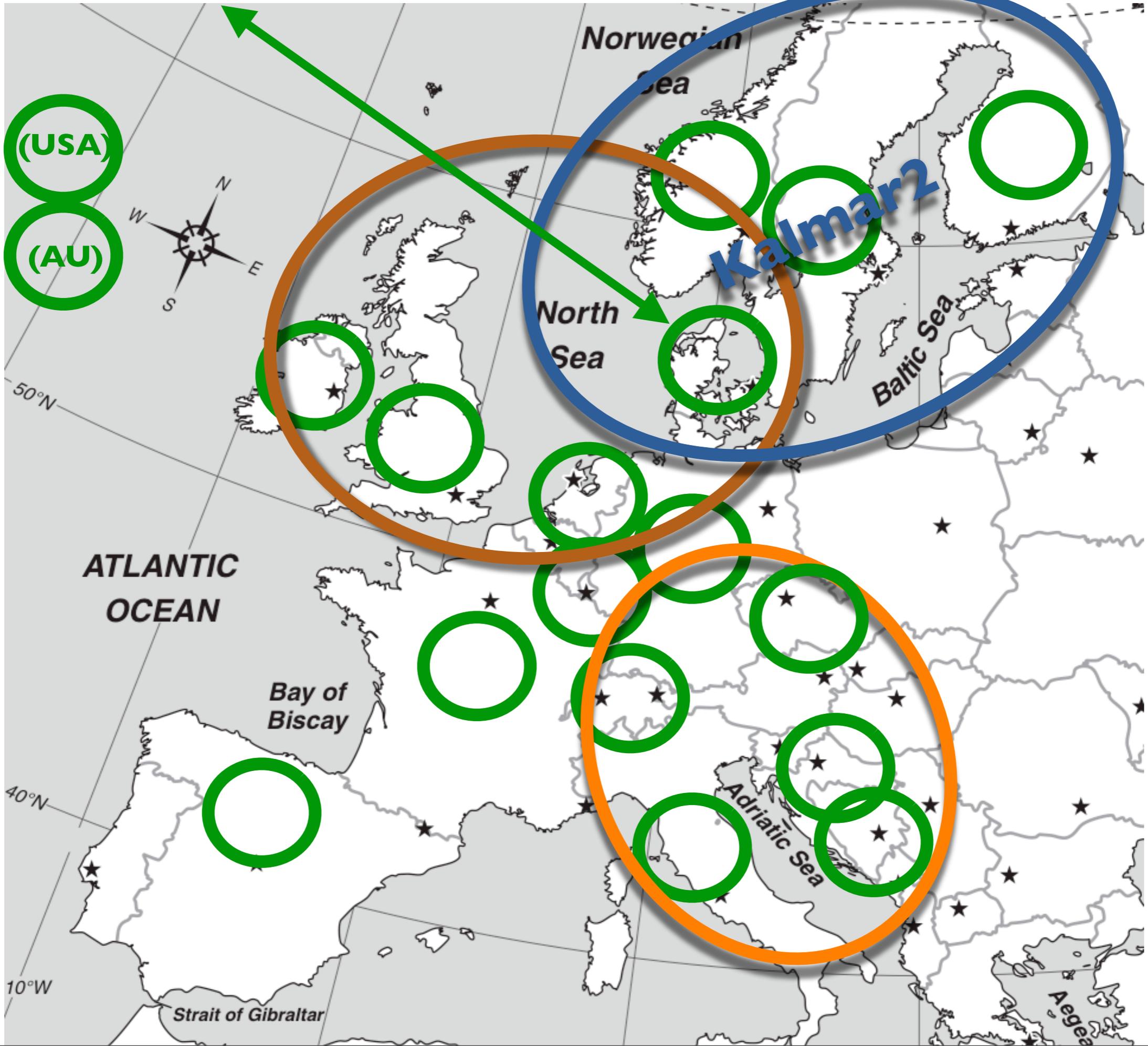
Baltic Sea

Bay of Biscay

Adriatic Sea

Strait of Gibraltar

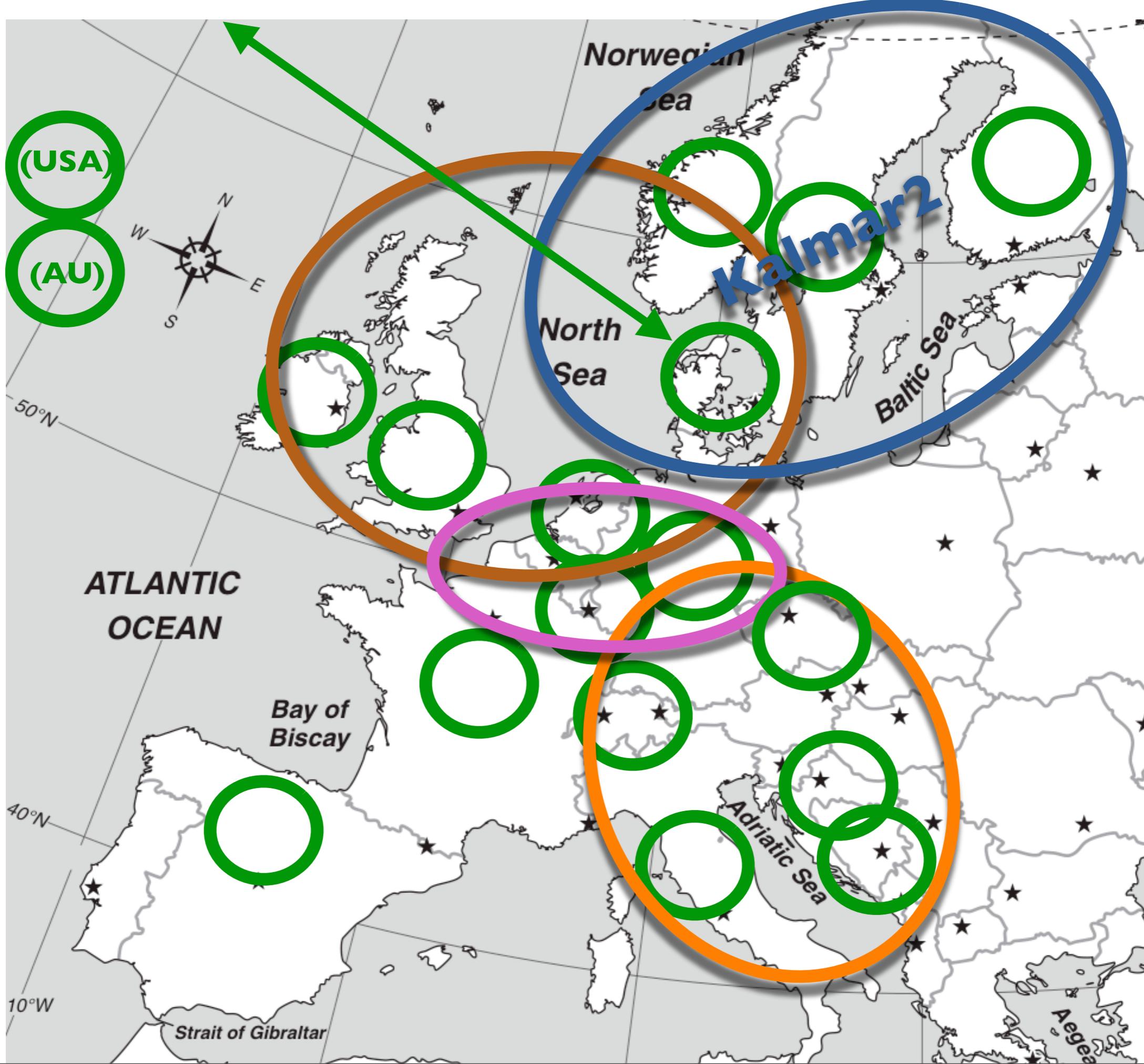
Aegean



(USA)

(AU)

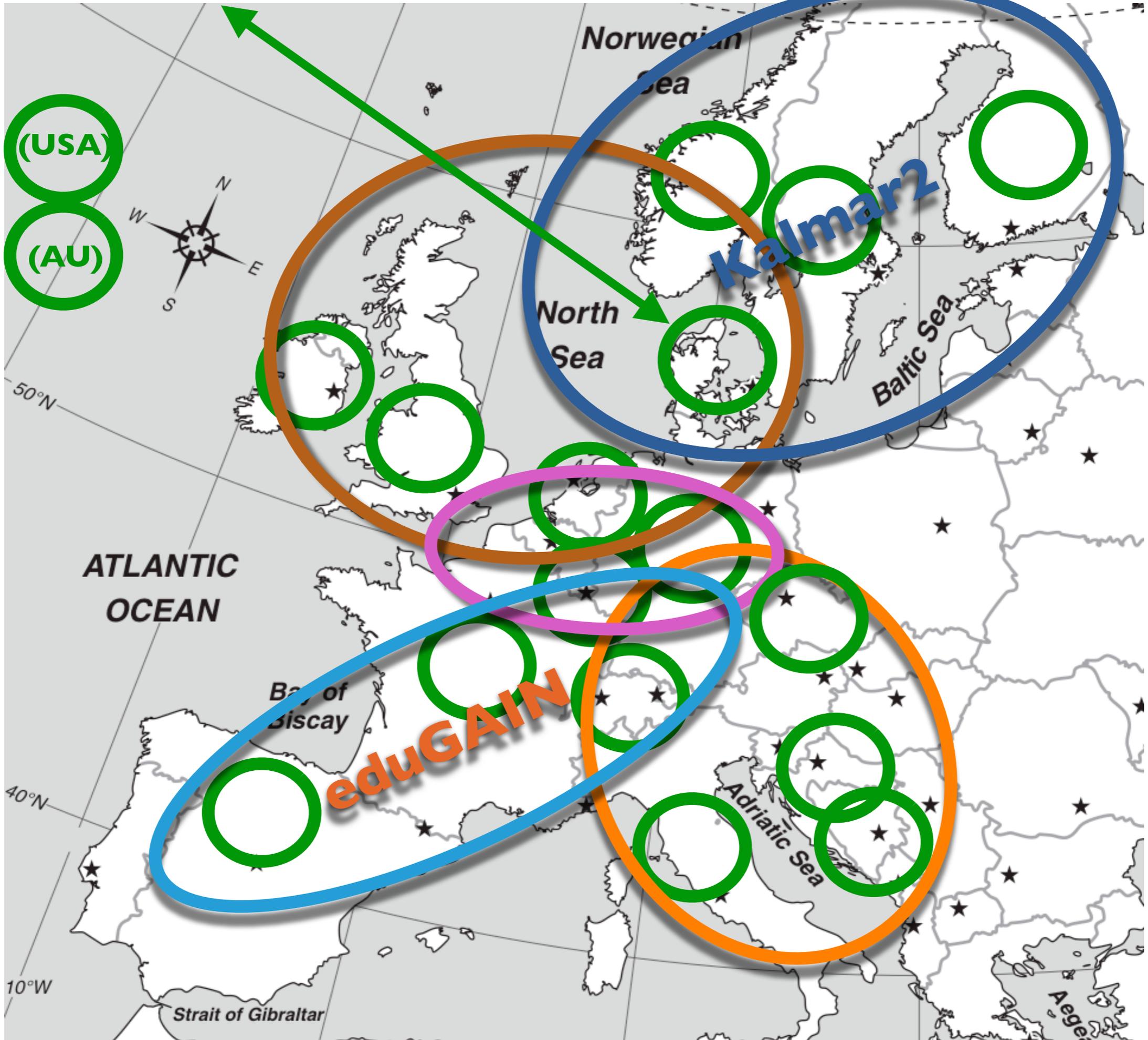
Kalmar2



(USA)

(AU)

Kalmar2



(USA)

(AU)

Kalmar2

eduGAIN

