IVOA Delegation protocol

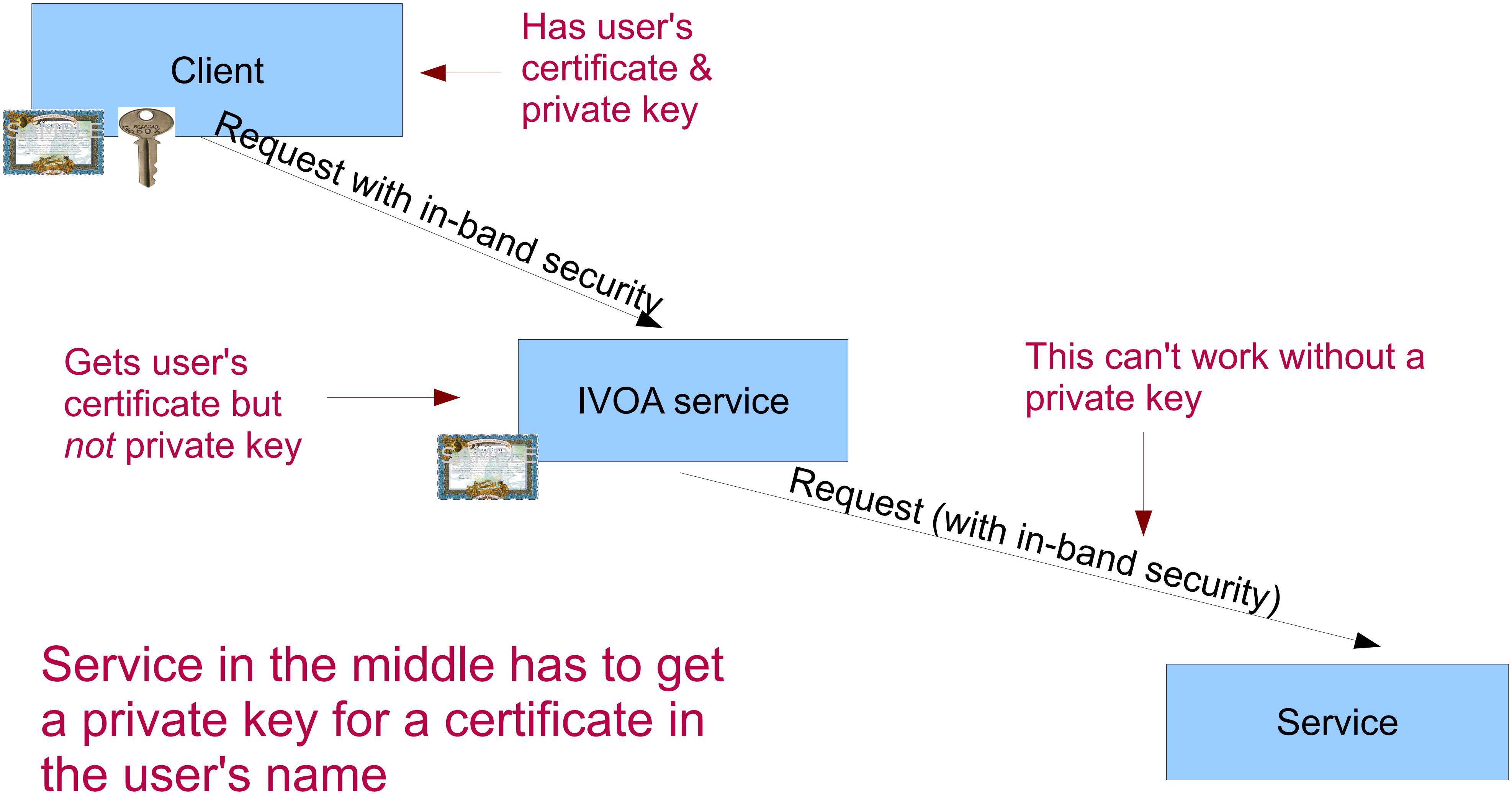
Guy Rixon

Presentation to IVOA Interoperability meeting
Cambridge, September 2007

Topics

- Why delegation?
- Three different approaches
- How the IVOA protocol works
- Prototyping

Secured service chain



Client

Has user's certificate & private key

Request with in-band security

Gets user's certificate but *not* private key

IVOA service

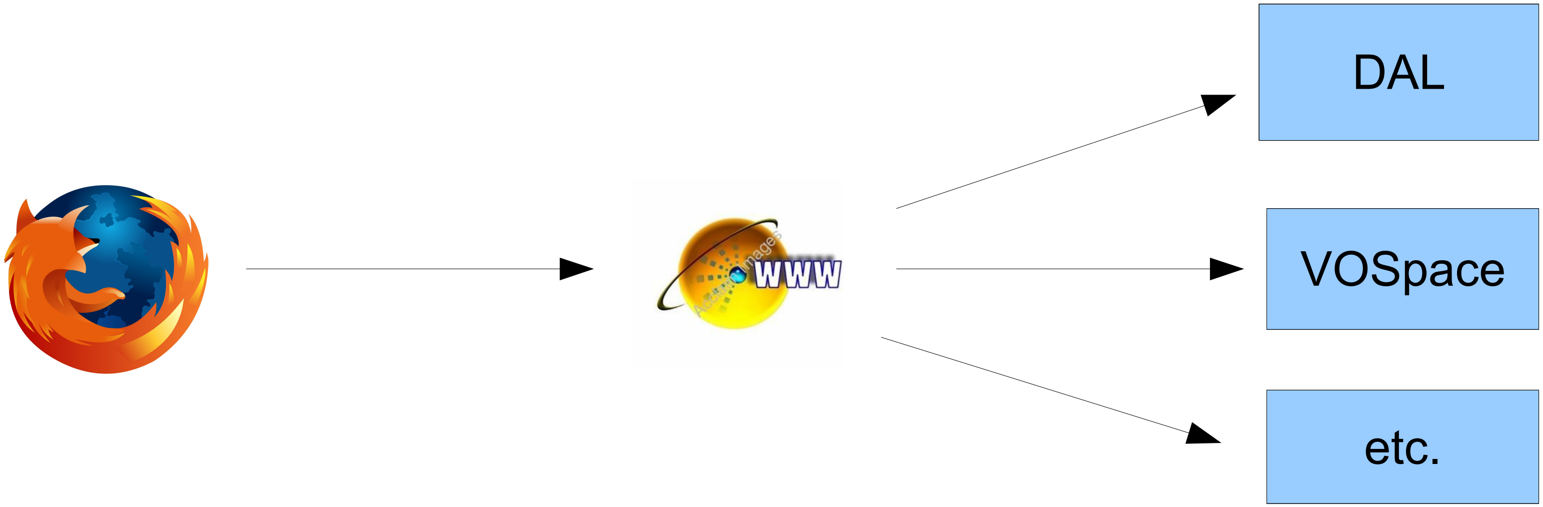
This can't work without a private key

Request (with in-band security)

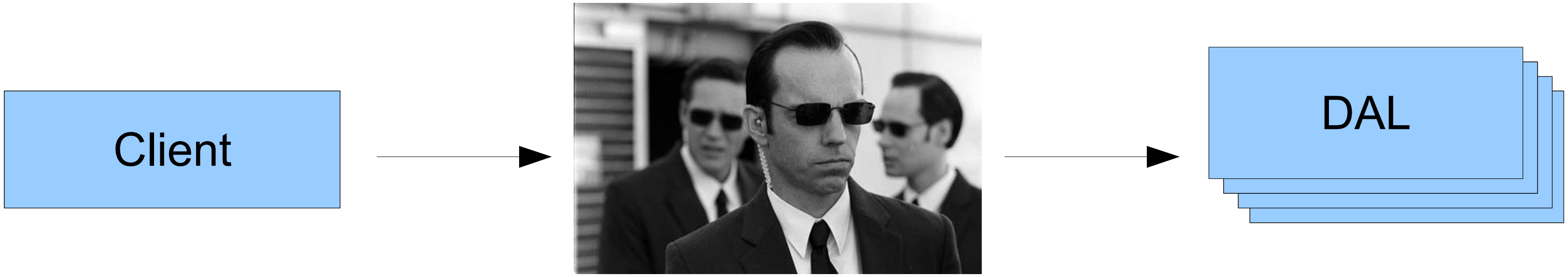
Service

Service in the middle has to get a private key for a certificate in the user's name

Use case: web portal



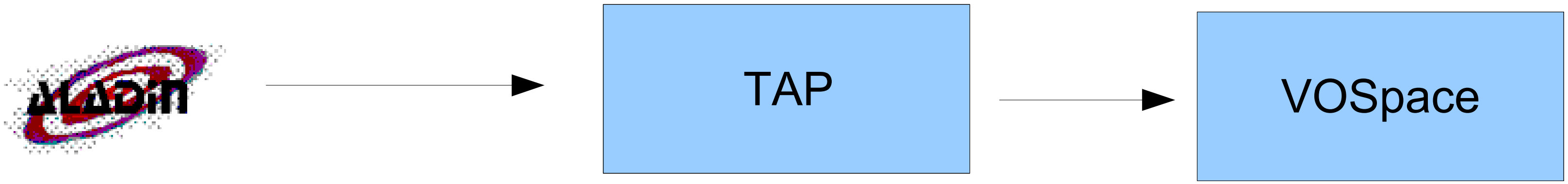
Use case: broker agent



Client

DAL

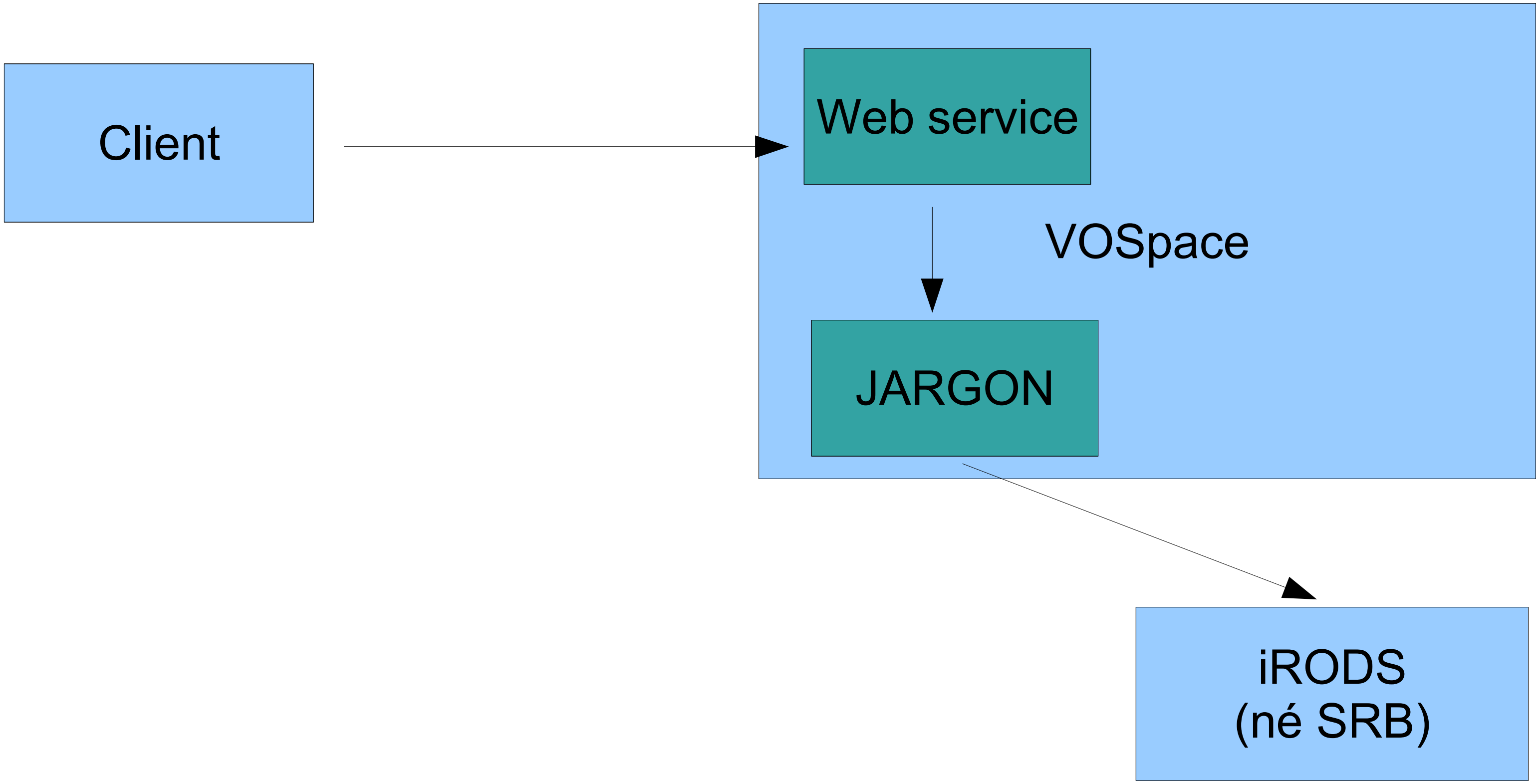
Use case: DAL →VOSpace



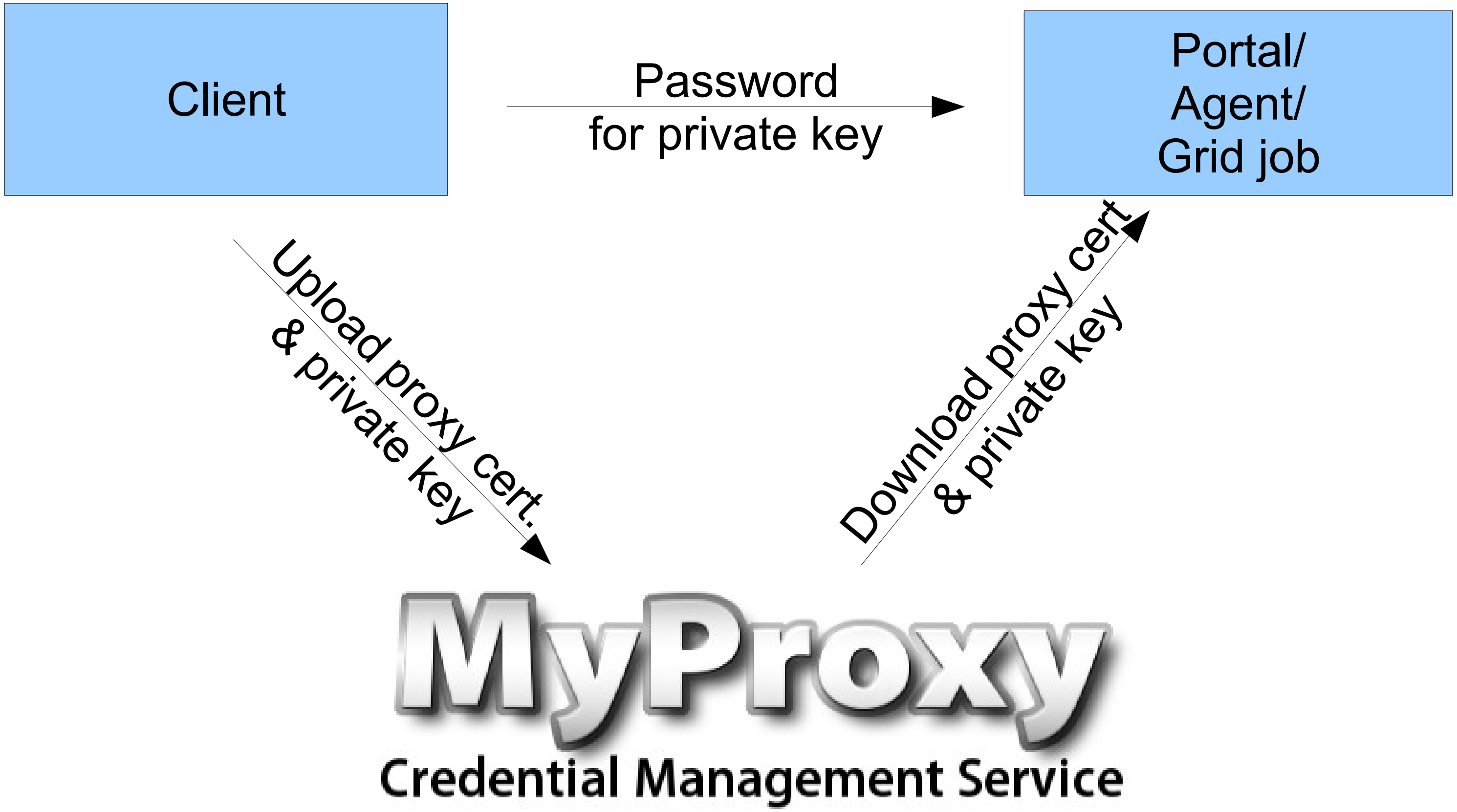
TAP

VOSpace

Use case: VOSpace → iRODS



MyProxy approach



Client

Password
for private key

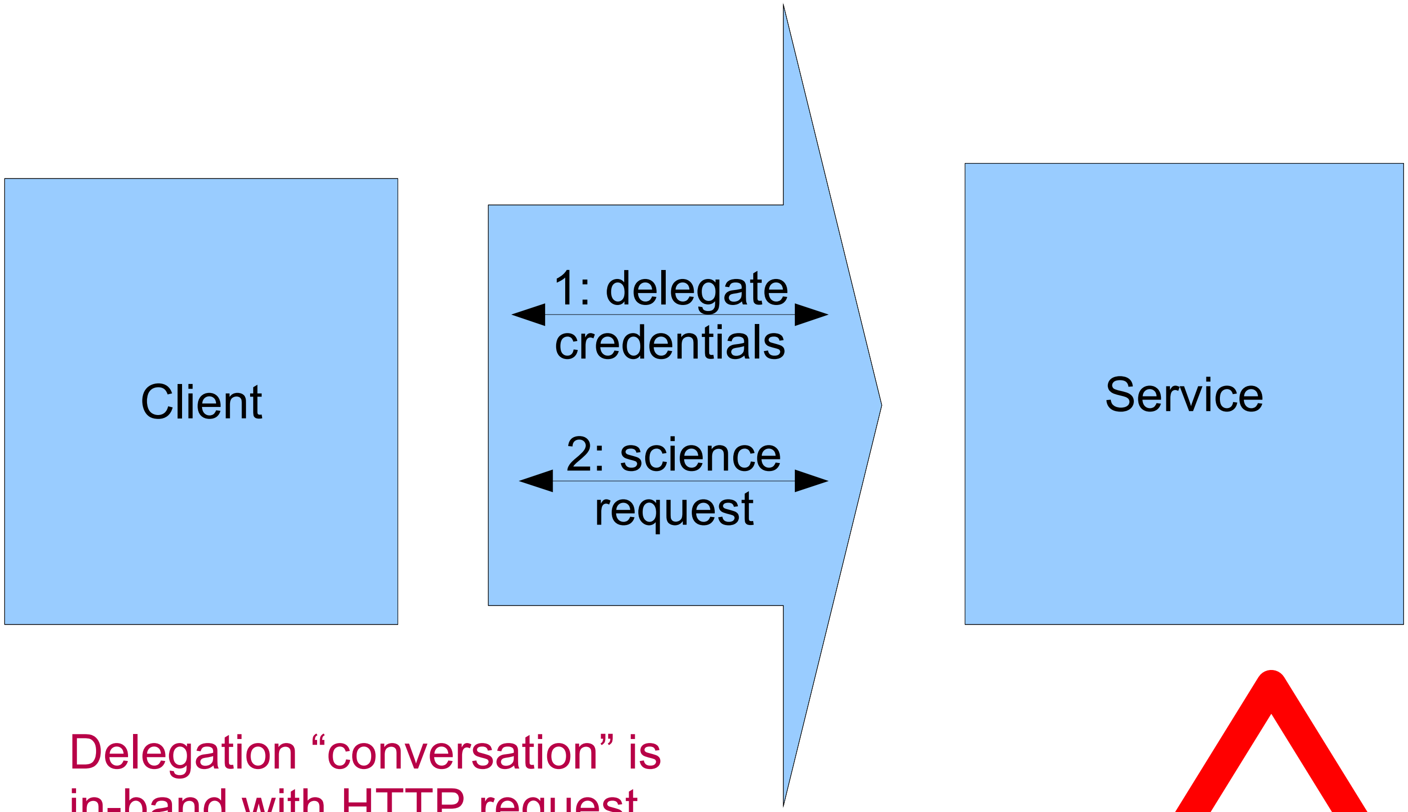
Portal/
Agent/
Grid job

Upload proxy cert.
& private key

Download proxy cert
& private key

MyProxy
Credential Management Service

HTTPG



Client

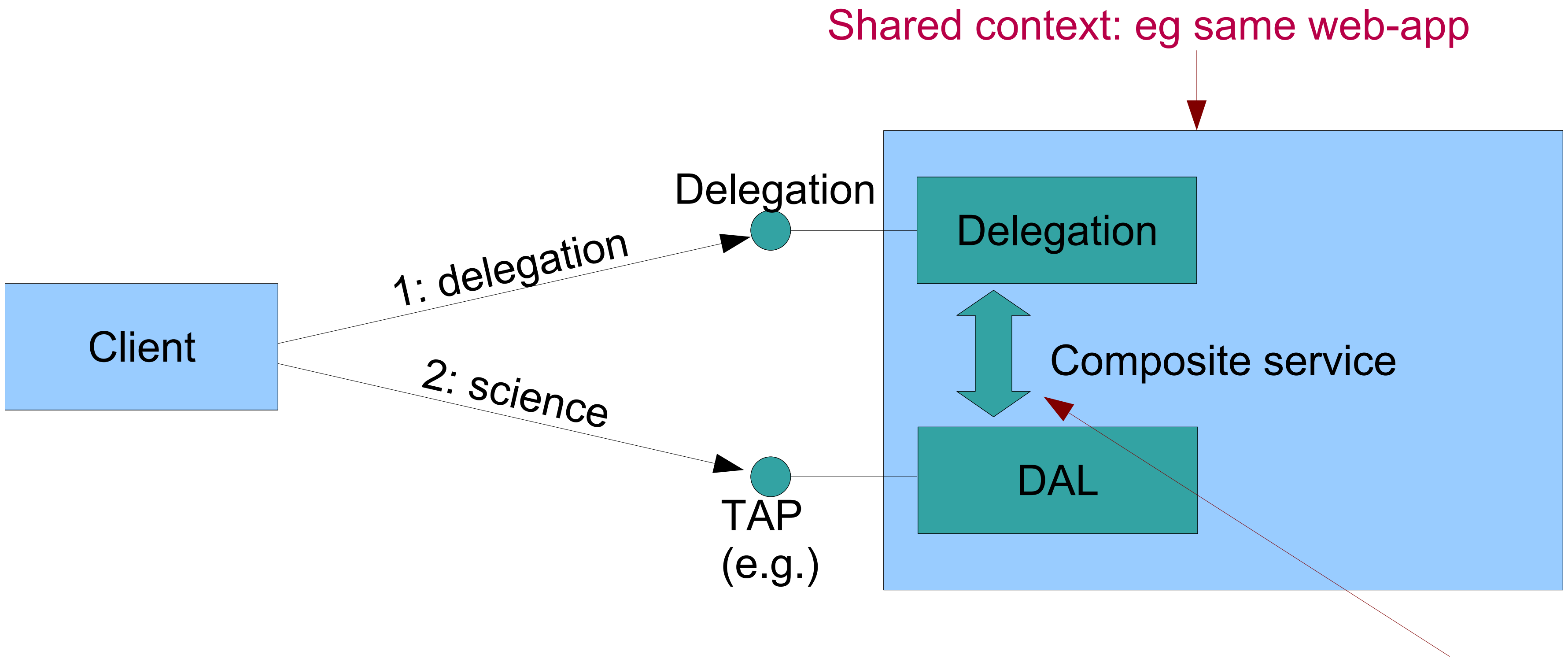
1: delegate credentials

2: science request

Service

Delegation “conversation” is in-band with HTTP request. Globus-specific; no longer supported?

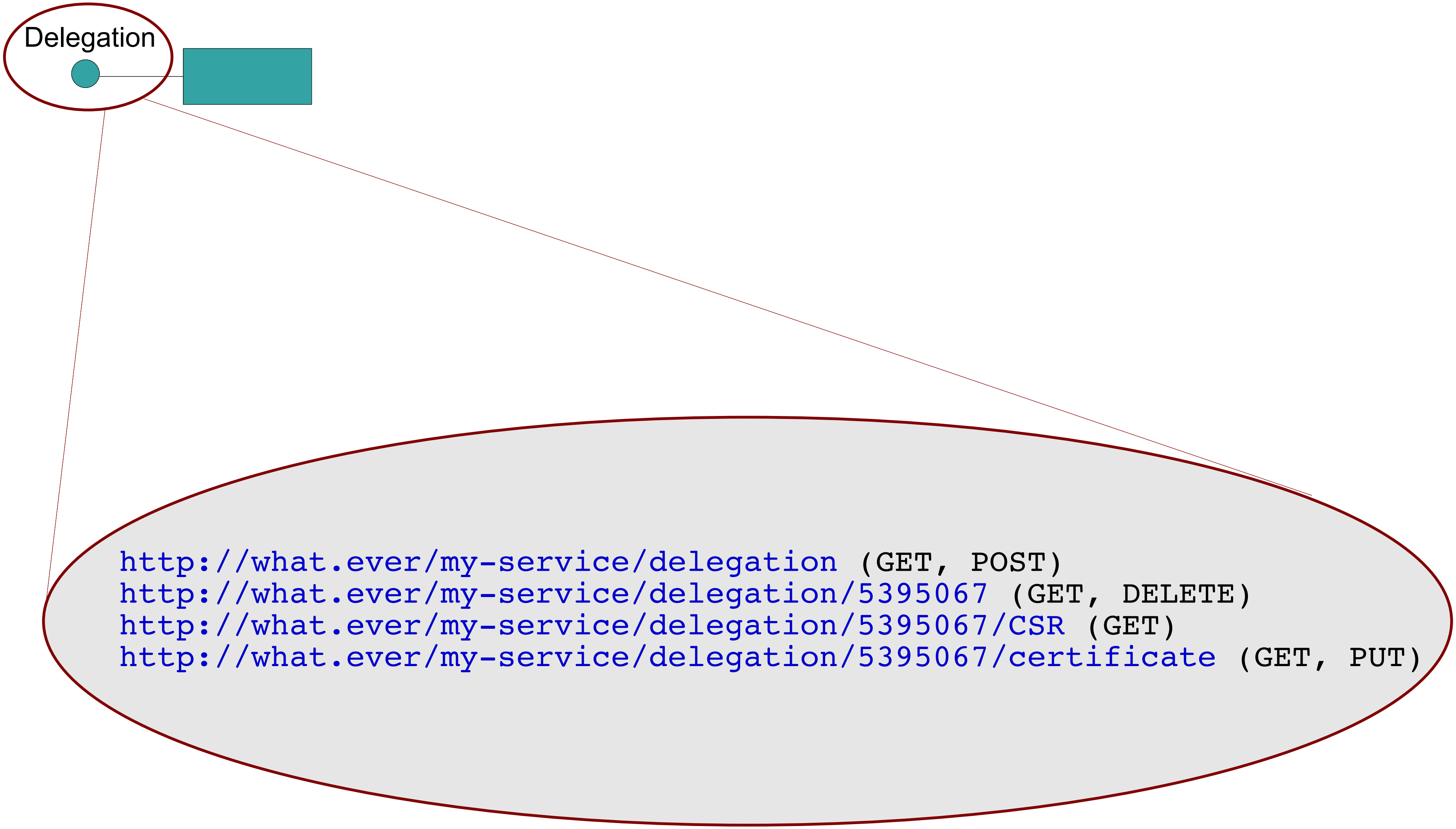
“Symbiotic delegation service”



This is the basis of the IVOA delegation protocol v0.1

Credentials shared here.
Implementor defines
this interface; e.g. method
call within same JVM or
HTTP behind firewall.

IVOA protocol (1)



```
http://what.ever/my-service/delegation (GET, POST)
http://what.ever/my-service/delegation/5395067 (GET, DELETE)
http://what.ever/my-service/delegation/5395067/CSR (GET)
http://what.ever/my-service/delegation/5395067/certificate (GET, PUT)
```

IVOA protocol (2)

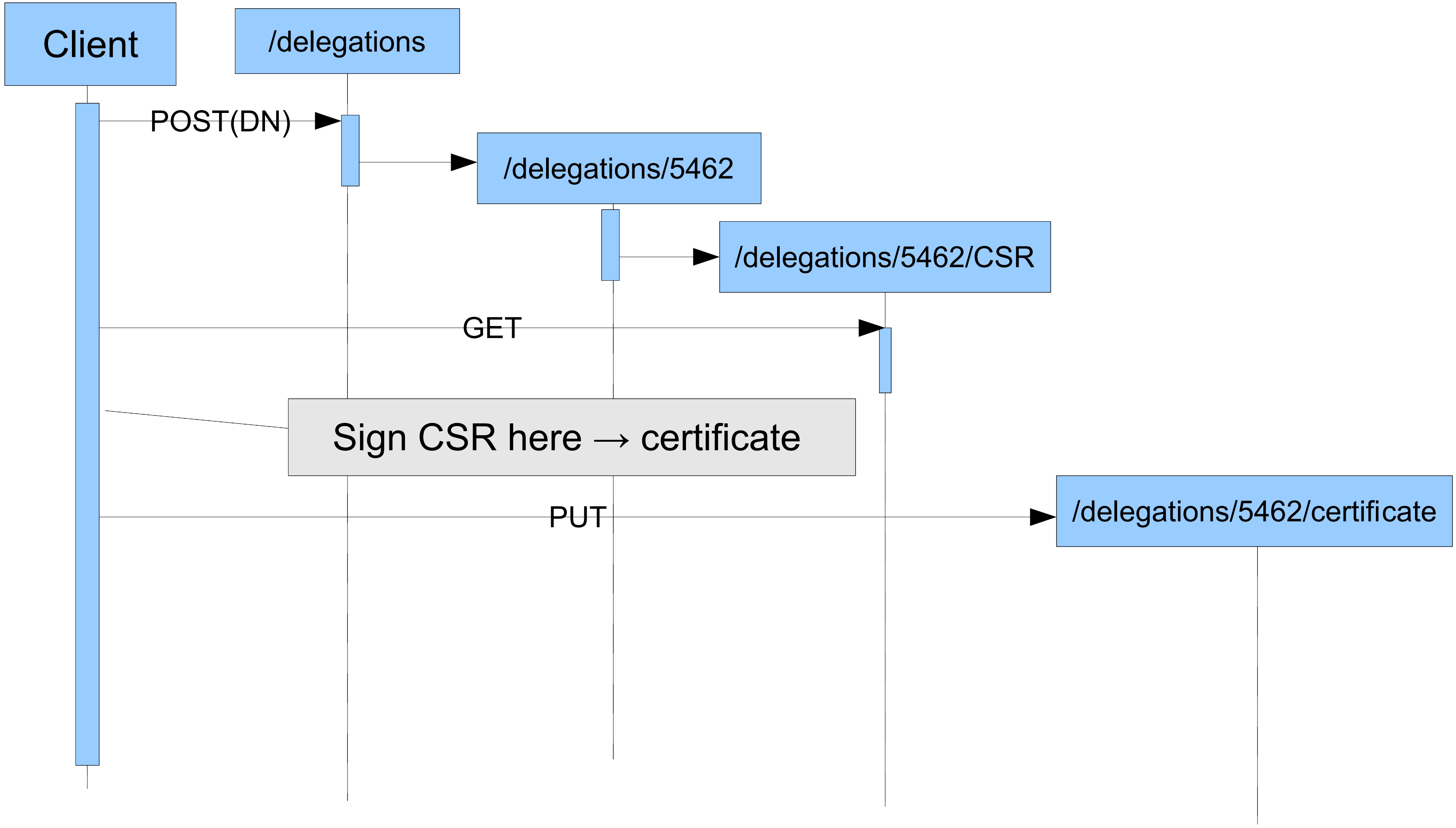
- List of delegated identities
  - e.g. http://what.ever/my-service/delegations
  - GET: list of DNs
  - POST: adds identity to the list; creates identity resource
- Identity resource
  - e.g. http://what.ever/my-service/delegations/5464935
  - GET: DN (text/plain)
  - DELETE: removes identity; cancels delegation
  - Last part of name chosen by service; e.g. hash of DN

IVOA protocol (3)

- Certificate signing request
  - e.g. http://what.ever/my-service/delegations/5464935/CSR
  - GET: PKCS#10 CSR

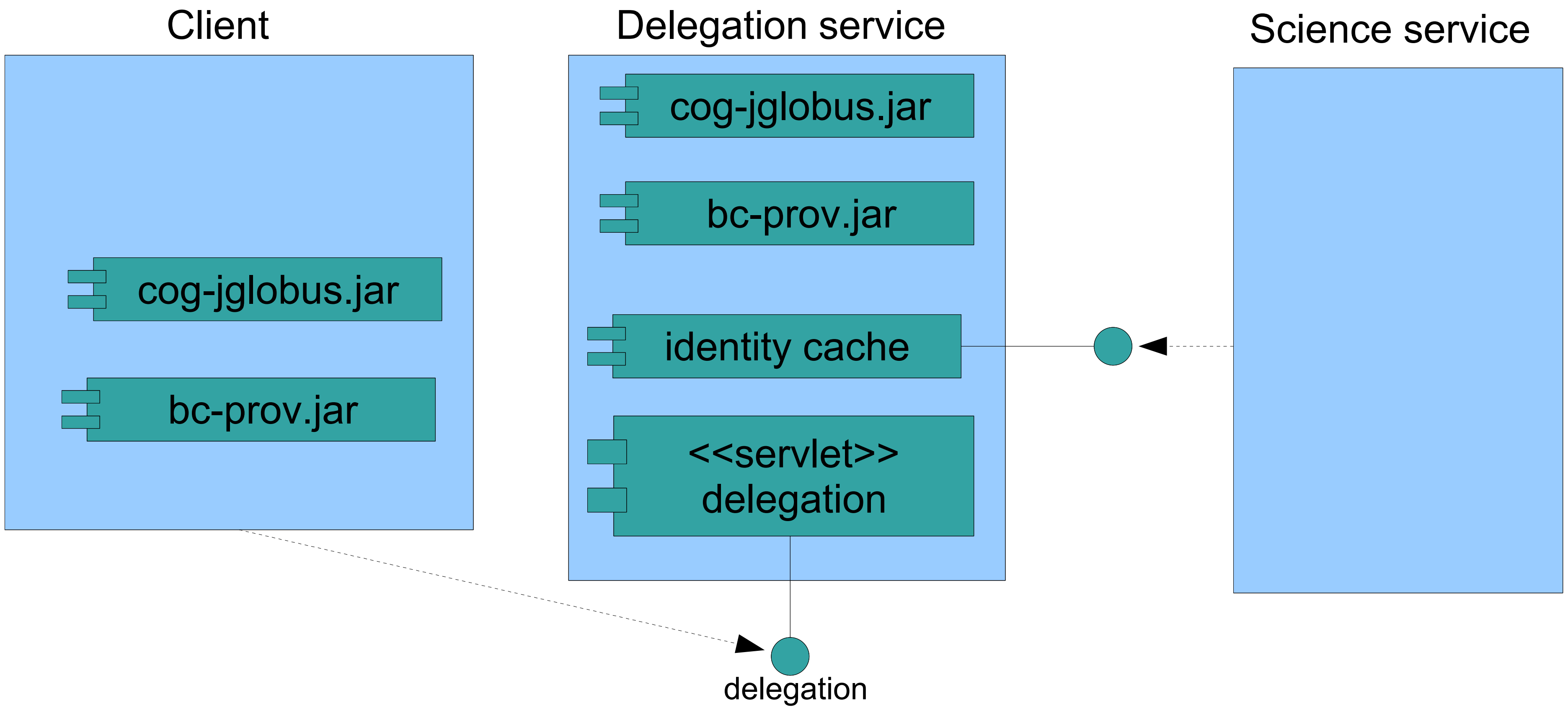
- Certificate
  - e.g. http://what.ever/my-server/delegations/5464935/certificate
  - GET: X.509v3 certificate, RFC 3820 impersonation proxy
  - PUT: upload certificate as above

IVOA protocol (4)



Prototype implementation

Warning: contains traces of Globus.


Client
Delegation service
Science service
cog-jglobus.jar
bc-prov.jar
cog-jglobus.jar
bc-prov.jar
identity cache
<<servlet>>
delegation
delegation