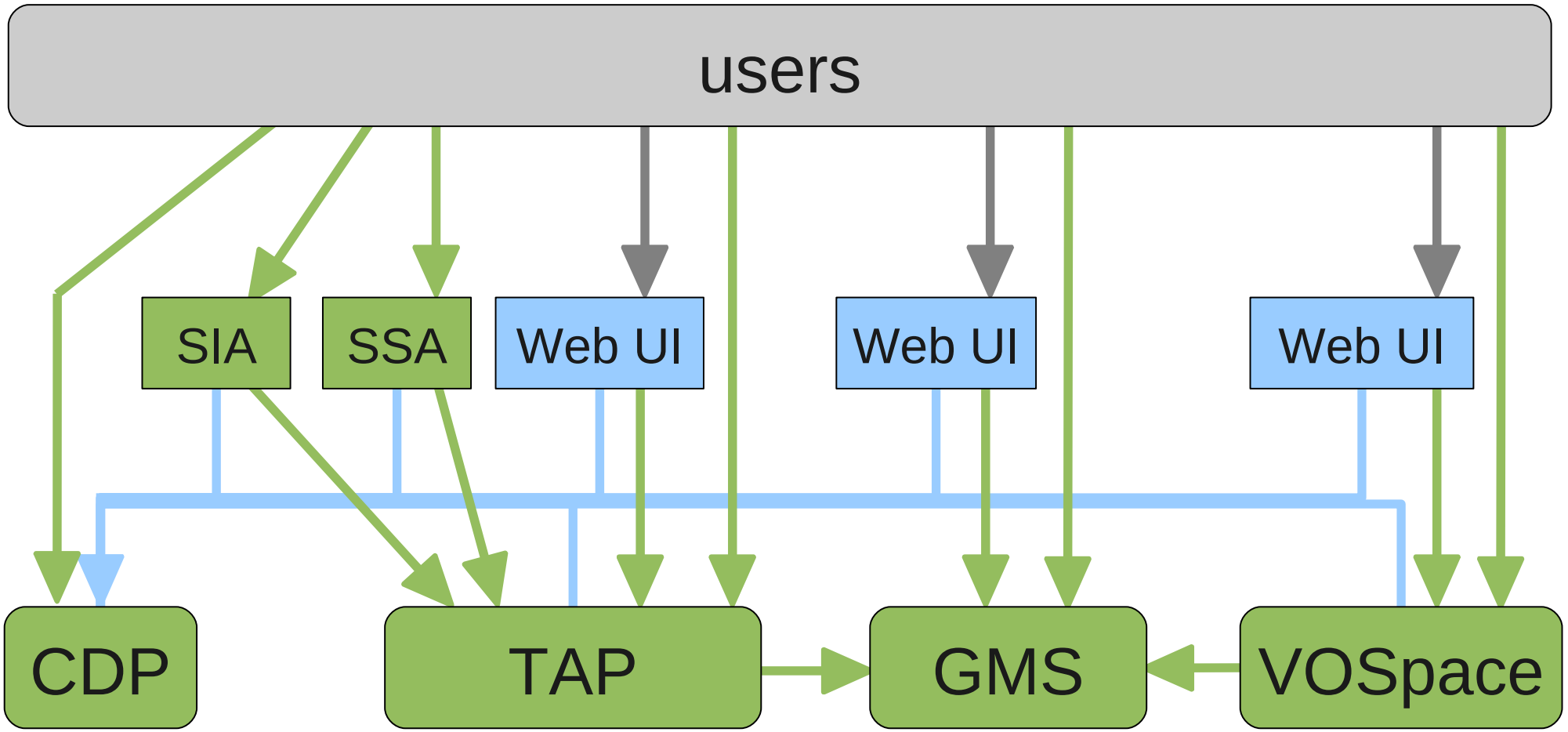
Credential Delegation

- web services support anonymous (http) and authenticated (SSO: https+X509) access
- web services need to call other web services:
  - VOSpace calls GMS to verify membership in group(s)
  - VOSpace calls another VOSpace for server-to-server transfer
  - TAP calls GMS to get group(s) for a user
  - TAP calls VOSpace to persist query results (coming soon)
  - SIA calls TAP to execute queries

Credential Delegation

- we are implementing web-based UI for most of our web services
  - users can be anonymous
  - authenticate with username/password (http)
  - authenticate with certificate (https)
- web apps calling web services:
  - AdvancedSearch -> CAOM TAP
  - VOSpaceBrowser -> VOSpace
  - GroupManagementUI -> GMS

Service Interactions



Credential Delegation

- requirements
  - need to call the underlying service on behalf of the user
  - defer all authorization checks to the web service
  - need a usable X509 proxy certficate from SSO: this is CDP
  - need usable X509 proxy certficate from username/password: custom but easy to fit in

implementation

- a separate service that is used by all our other services and web apps
  - persist all proxy certificates in RDBMS so state is shared across load-balanced web servers
- able to store and return proxy certficates signed by users with certficates: CDP
- able to return proxy certificates for regular CADC users that do not have certficates
  - create a default certificate for all CADC users, create proxy certs

beyond the spec

- implementor makes their own private API for use by trusted services
  - trusted: service-specific X509 certficate to authenticate, authorization check
  - can get proxy cert by DN or user ID

    `GET /cred/priv/dn/<distinguished name>`

    `GET /cred/priv/user/<user ID>`
  - returns a valid X509 proxy certficate (PEM)
  - may be called more remotely by cloud computing infrastructure

Summary

- regular users use webapps (anon or auth) and never experience any certificate use
- users with X509 certificates connect DN with their CADC account (user ID)
  - consistent identity using cert or login to webapps with username
  - users have to manage proxy certficates via CDP
- web services only support SSO (X509)
  - web services perform relevant authorization

Using open-source code from Astrogrid
(thanks to Guy Rixon for excellent advice)