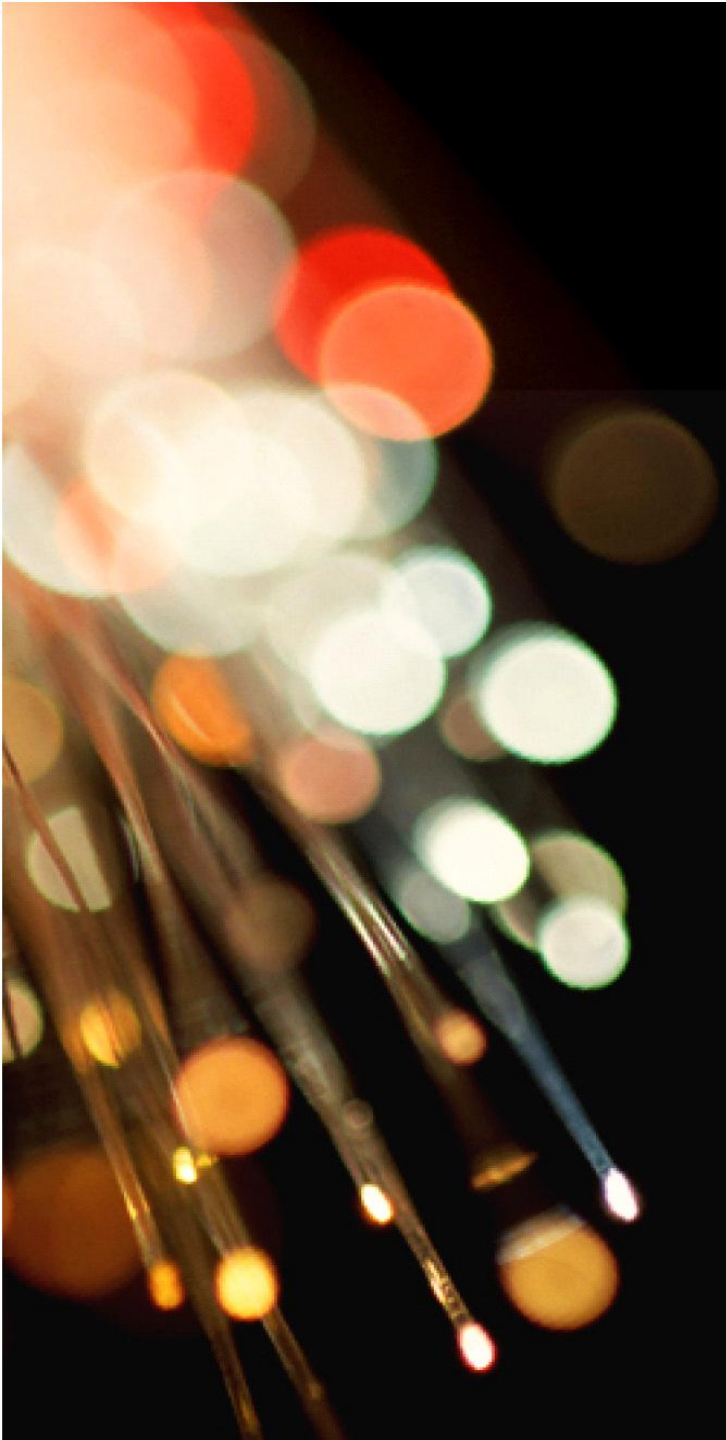


OpenConext

Enabling Team Management, Group-Aware Services, and SP Shop-Fronts

QUESTnet 2013

Neil Witheridge

AARNet, Authentication & Authorisation Services Technical Manager

Francois Kooman

SURFnet, OpenConext Development Team (remote)

4th July 2013

aarnet

Australia's Academic and Research Network

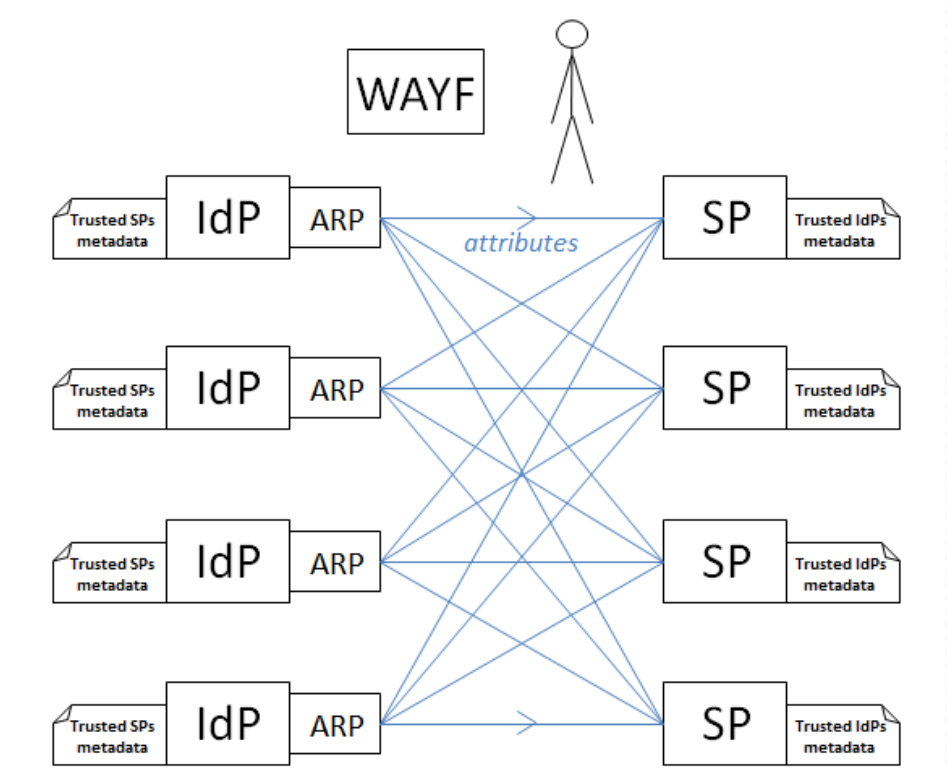
Topics

- Federated Identity and Access, User Attributes & Authorisation
- SURFnet's OpenConext
- Architecture
- Functionality (IdP/SP-Proxy, Group Mgnt & Proxy, Service Registry)
- Group-Proxy & Group Info interface
- OpenConext Security and Sustainability
- AARNet & OpenConext
- OpenConext Roadmap

Federated Identity & Access

- SAML Federated Identity & Access 'state of the art'
  - Service Providers trust Identity Providers & vice versa (via SAML metadata)
  - SPs requests user attributes from the user's IdP (info stored in institution's identity store)
  - IdP delivers according to Attribute Release Policy (ARP), with optional user consent

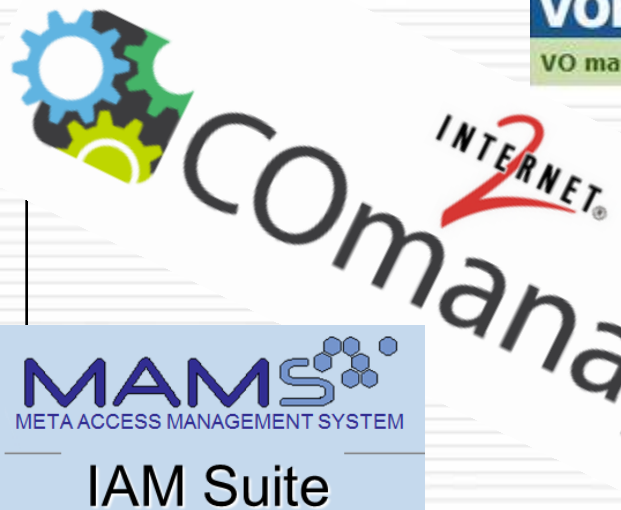
- E.g. AAF



Authorisation

- Importance of group-based access for R&E services
  - Research Team access to federated services
  - VOs for Grid Services
  - Service licensing, restricted access to commercially sensitive info
- User information used by service for authorisation decision
  - IdP user attributes
    - IdP authoritative & owned, directory schema -> namespace
  - Team-attributes (Research Teams, Virtual Organisations)
    - Team authoritative & owned namespace (URN), bilateral agreement with services
      - urn:collab:group:biolabs:au:genome-team
  - Authorisation Rights (e.g. populated in eduPersonEntitlement)
    - Service authoritative & owned namespace (URN), delegates authority to issue
      - urn:service-x:entitlement:foo

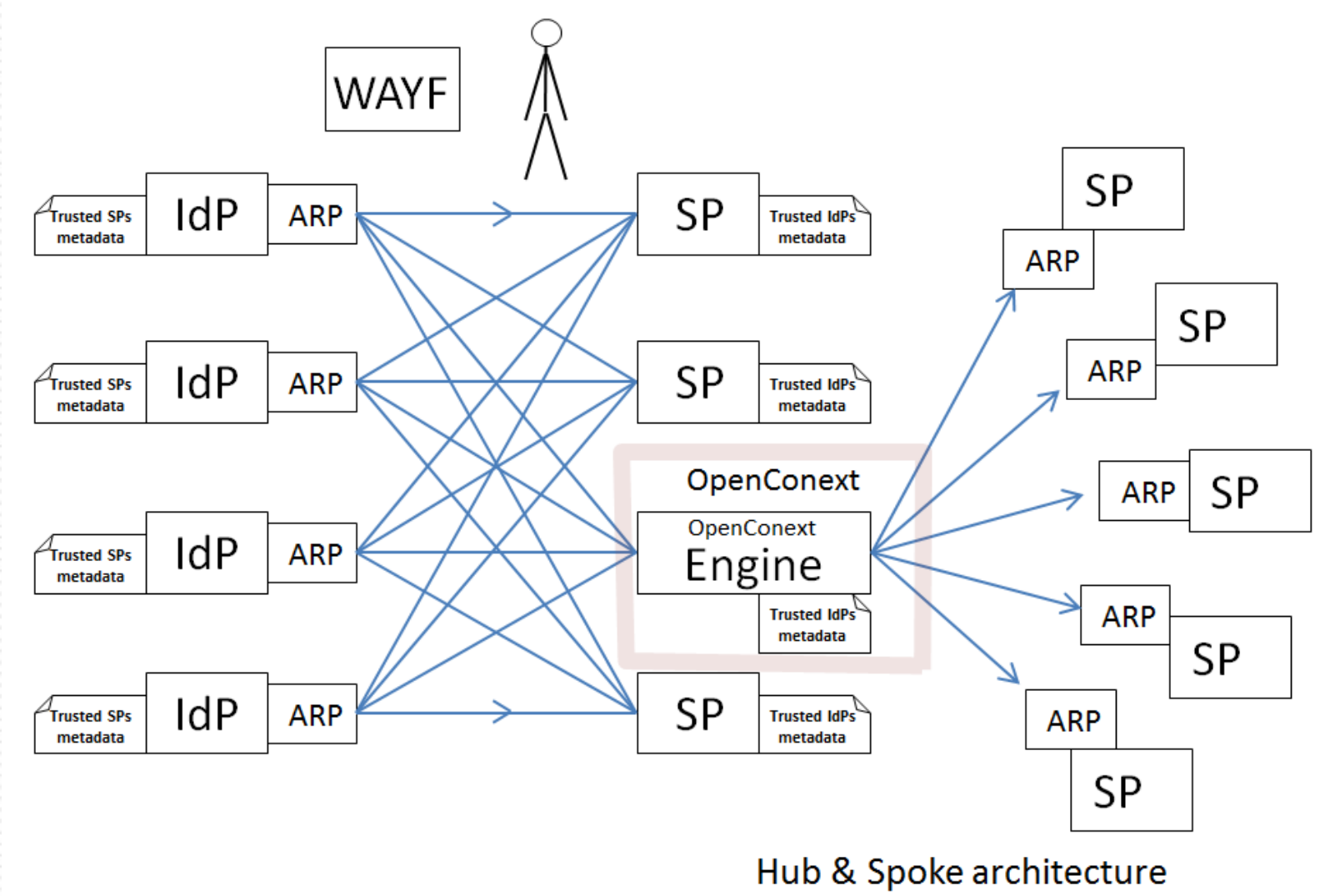
Group-management Systems



Using SAML-Based VOMS for Authorization within Web Services-Based UNICORE Grids

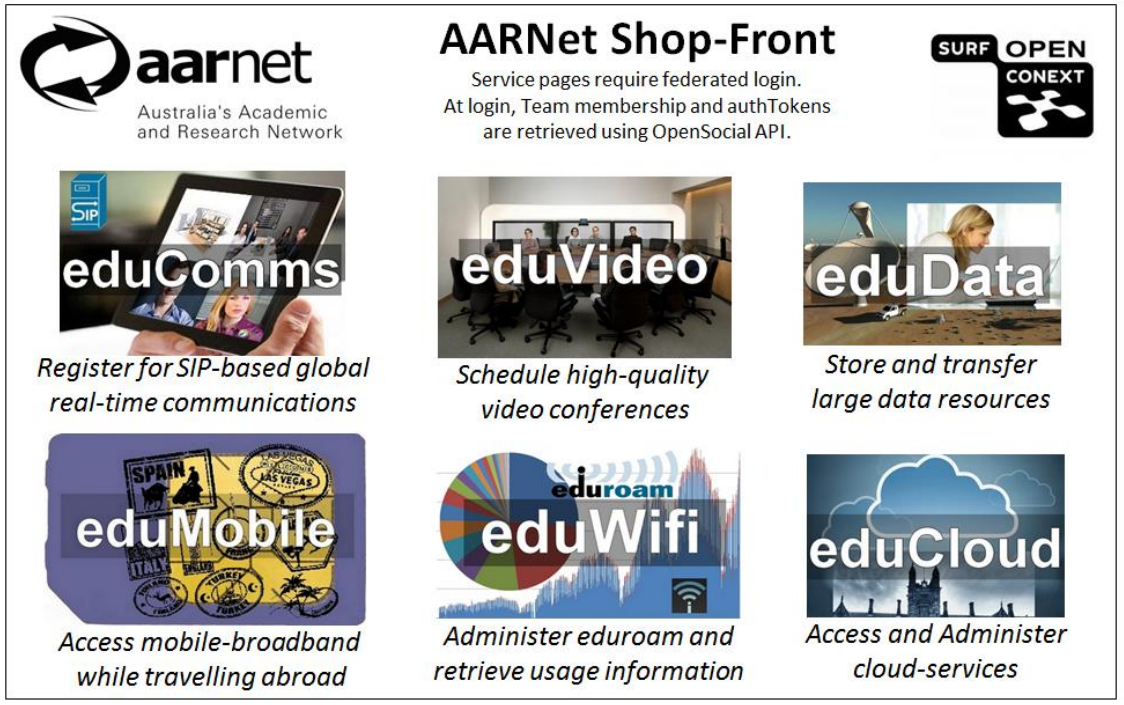
http://www.youtube.com/watch?v=kUpn568NSl0&feature=player_embedded

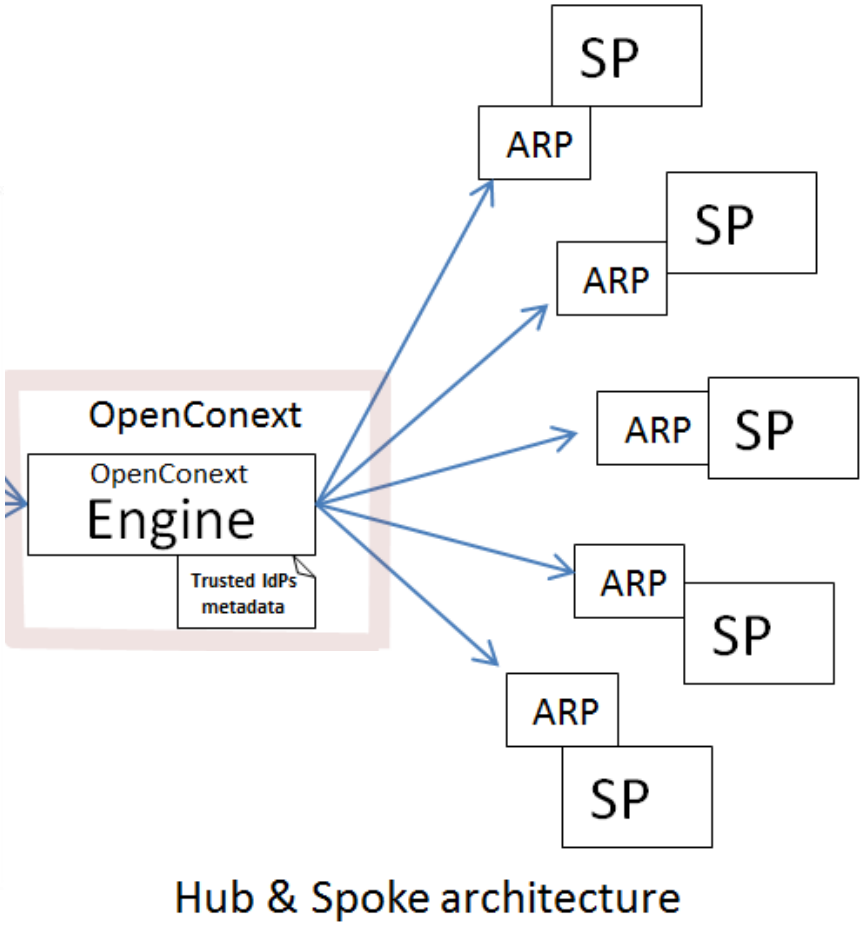
Services Shop Front



Services Shop Front

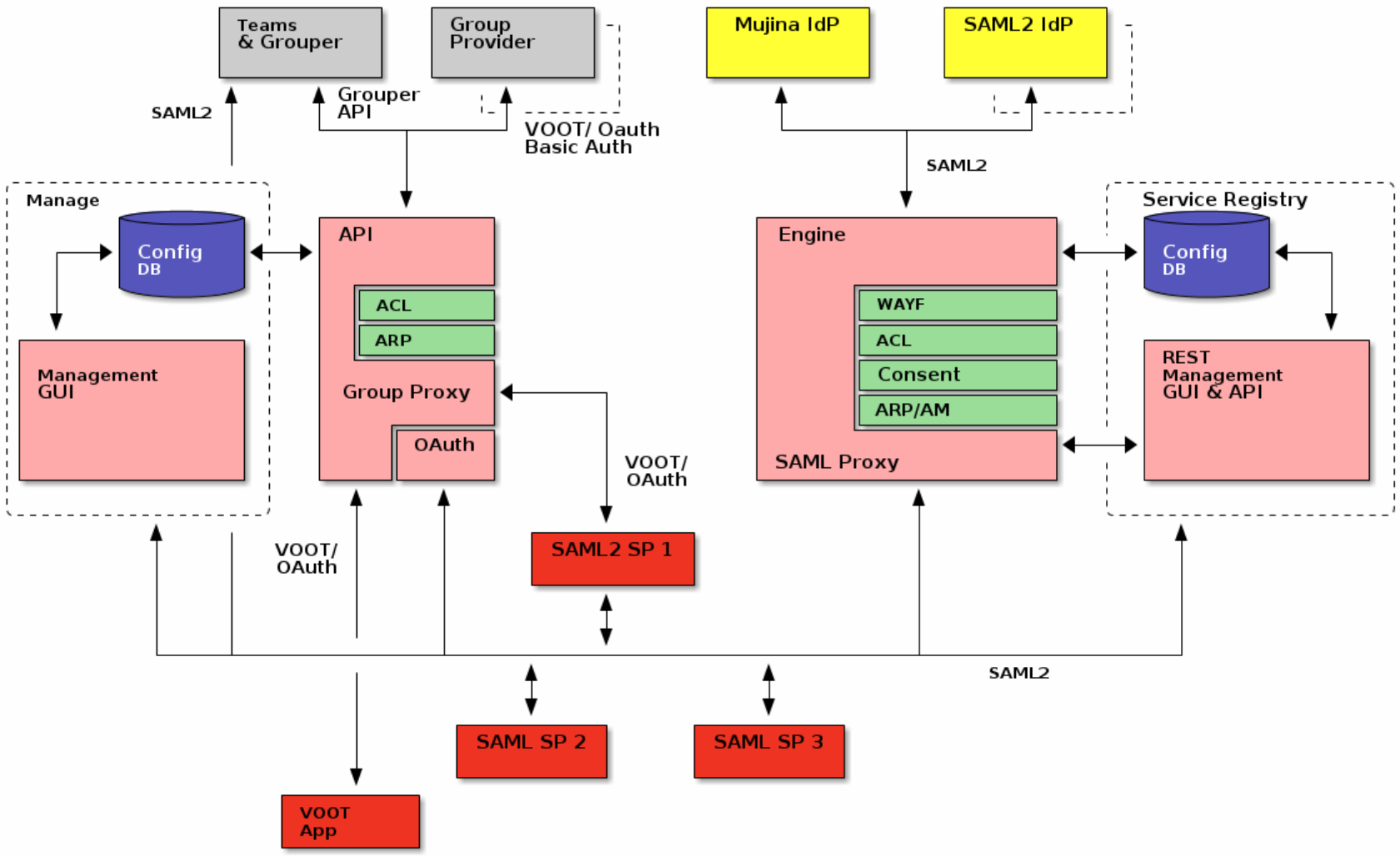
- OpenConext Engine as an IdP/SP Proxy
- Enabler of attribute aggregation





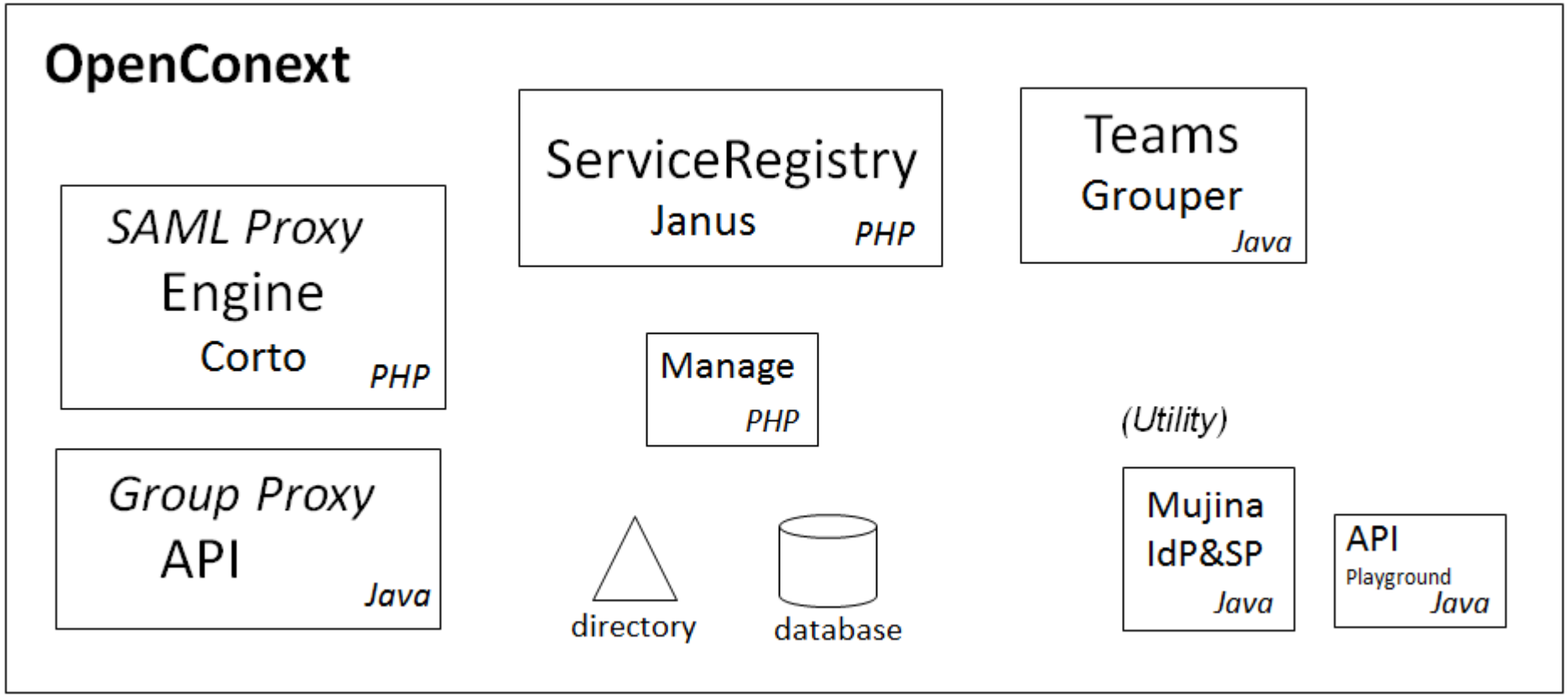
Hub & Spoke architecture

OpenConext Architecture



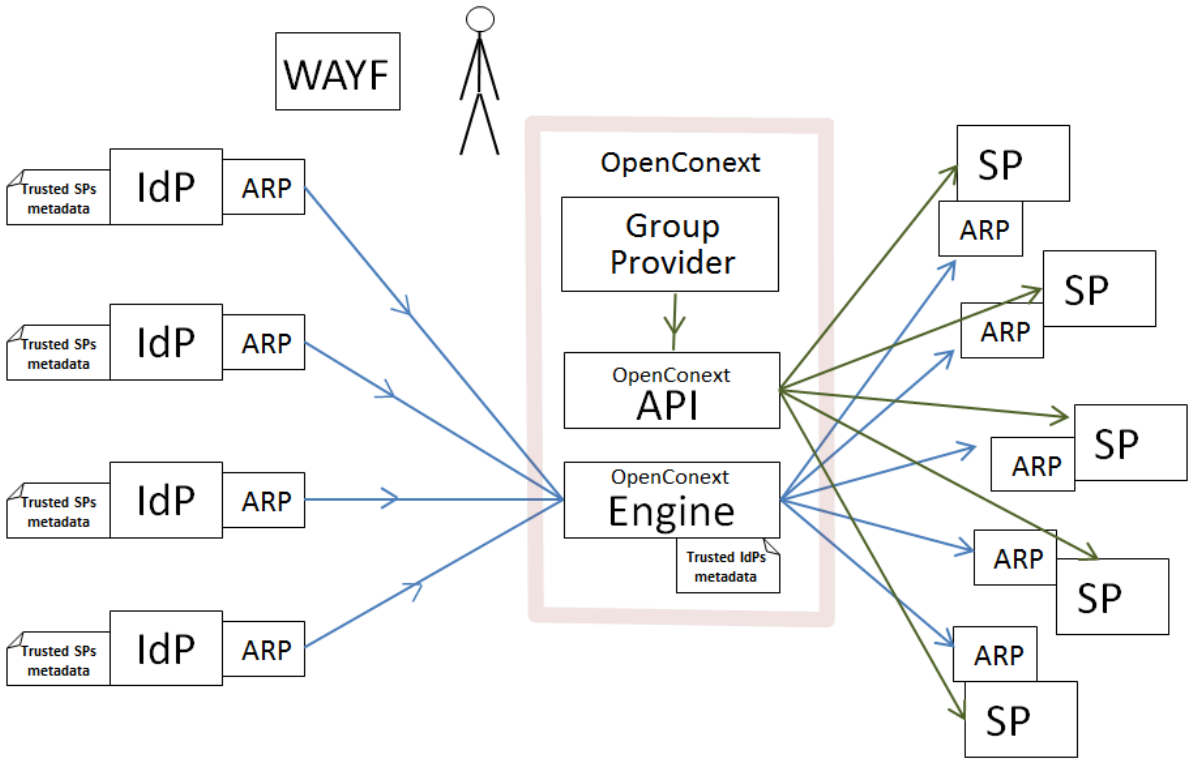
OpenConext Components

- Application components making up OpenConext



Conext Engine and API

- Engine (SAML IdP/SP Proxy)
  - Uses Corto (developed by GEANT)
  - Utilises hub & spoke federation architecture
  - Enables deployment as a “Services Shop Front”
- API – Group Proxy
  - Grouper-based Group Provider ‘built in’.



ServiceRegistry

- ServiceRegistry is used for Metadata Management
  - Uses “JANUS” (developed by WAYF, Denmark)
- SAML Metadata extended for Group Information Retrieval
- Attribute Release Policies for Services
  - Common set of attributes to EngineBlock
  - Release of Attributes to Services according to ARP
- Attribute Manipulation
  - PHP scripted attribute manipulation
- Configurable User Consent

OpenConext Teams

- 'team' synonymous for 'group'
- "Teams" provides secure team management
  - GUI for Internet2's Grouper (default Group Provider)
- Team creation and membership
  - Email based workflow
  - Public and Private (hidden) Teams

- Group Providers
  - "Teams" is GUI for Grouper-based group provider
  - Others can be configured
- Consent for release of group information is configurable

VOOT API

- Exchange of group and person information
  - Standardized REST API based on OpenSocial 1.1 API
    - Subset of OpenSocial 1.1 + {voot_membership_role} attribute
- Supported calls:
  - Retrieve a list of groups the user is a member of
  - Retrieve the list of people that are members of the user's group
- Security
  - OAuth 2.0 protected resource server
  - OAuth 1.0a supported (for now)
  - OpenConext provides an 'API playground' for testing OAuth/VOOT calls

API Example

```
GET /groups/@me?sortBy=title HTTP/1.1

HTTP/1.1 200 OK
Content-Type: application/json
{
    "entry": [
        {
            "description": "Group containing employees.",
            "id": "employees",
            "title": "Employees",
            "voot_membership_role": "admin"
        },
        {
            "description": "Group containing everyone at this institute.",
            "id": "members",
            "title": "Members",
            "voot_membership_role": "member"
        }
    ],
    "itemsPerPage": 2, "startIndex": "0", "totalResults": 2
}
```

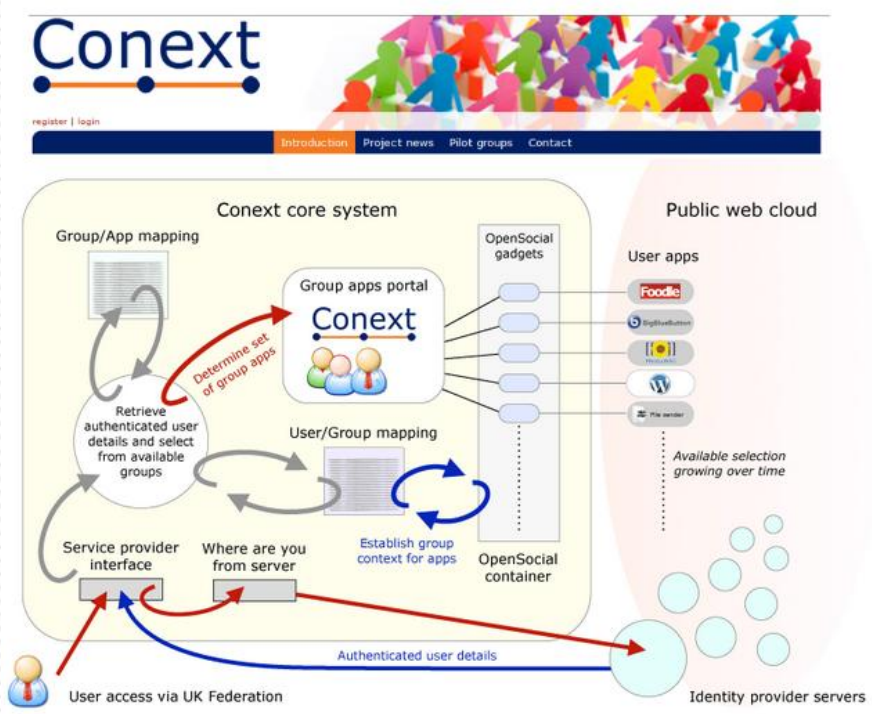
OpenConext Security

- OpenConext Security Mechanisms
  - PKI, Shared Secrets
- Security Analysis
  - undertaken of SURFconext components by 3rd party
- VOOT/OAuth security
  - strong reliance on TLS
- Considerable published work on Oauth Security
  - http://tools.ietf.org/html/draft-ietf-oauth-v2-threatmodel-01
  - Security Analysis of Double redirection protocols http://pomcor.com/techreports/DoubleRedirection.pdf

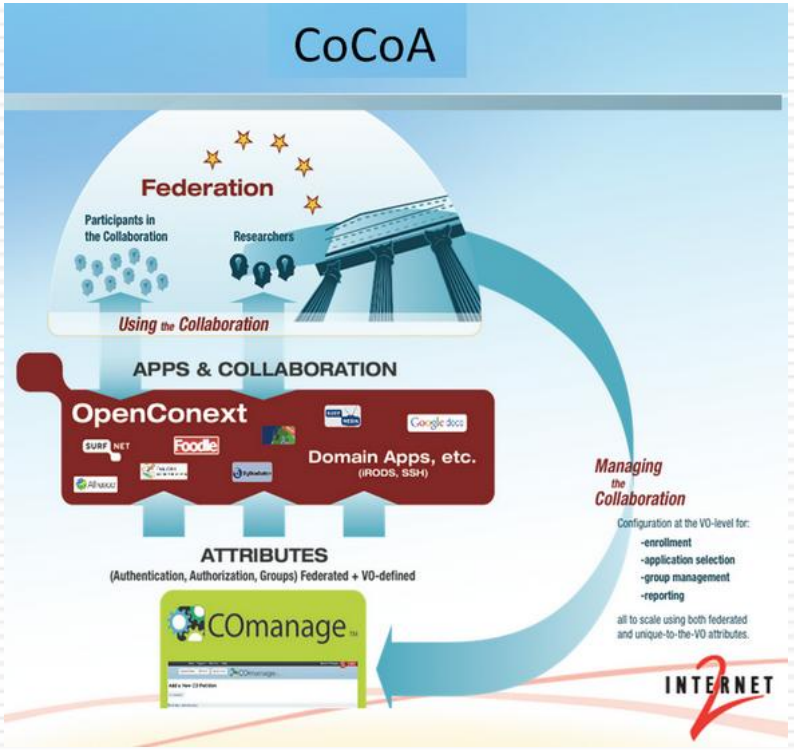
OpenConext Sustainability

- Use by SURFnet for their National Federation
- Global interest & collaboration (e.g. in producing documentation)

JISC



Internet2



AARNet and OpenConext

- AARNet's "above-the-net" service delivery strategy
  - Collaborating via Global NREN CEO Forum on delivery of global services
  - Network Centric Services e.g. Video Conferencing, SIP-based Comm's, Mobility, Customer Info services, "Cloud" services, Cloudstor+ already provided
- Reliance on AAF for Federated Authentication
- AARNet services behind a single shop-front.
  - Shop-front provides for sharing information between services, also branding, cross-marketing, etc.
- AARNet services "group-aware" and "entitlements aware".
- OpenConext enables AARNet's services strategy

Development PoC

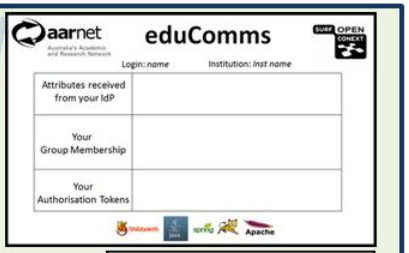
National Federation

OpenConext Demo Components
Neil Witheridge
19/5/2013

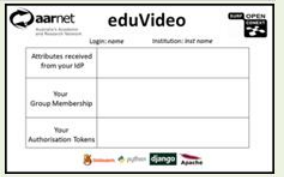
AARNet Shopfront (OpenConext) IdP/SP-proxy

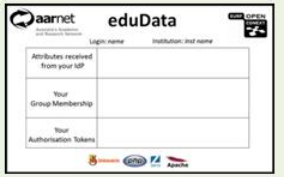
aarnet
Australia's Academic and Research Network

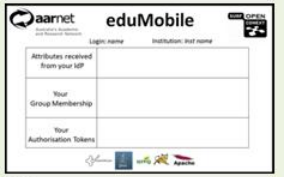
https://educomms.aarnet.edu.au (protected)

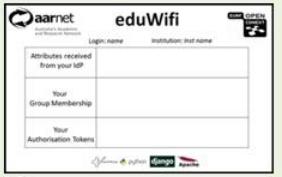


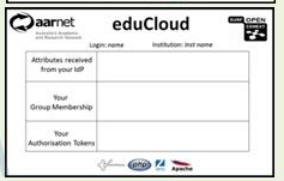
http://shopfront.aarnet.edu.au (open)



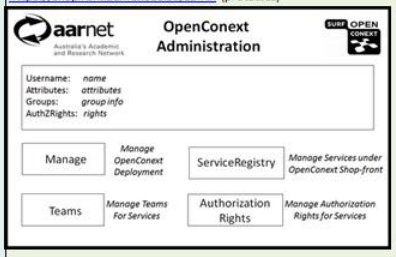








https://shopfront.aarnet.edu.au/admin (protected)



OpenConext Roadmap

- Any ‘recent development’ news from SURFnet, Francois?

Questions ?

neil.witheridge@aarnet.edu.au

francois.kooman@surfnet.nl

More info at https://wiki.aarnet.edu.au/display/CONFWORKSHOPS/OpenConext+Demo