Use of Shibboleth by ARCS

Neil Witheridge
Manager, ARCS Authorisation Services

Internet2 Members Meeting, Fall, October 2009
Overview

• Australian HE Research & ARCS Background
• ARCS reliance on AAF: Current AAF Status
• ARCS & Other Research Services
  – Grid, Data, Collaboration; Research Domain Specific
• AAF interoperability with the Grid
  – Grid Security Infrastructure, Short Lived Credential Service
• Authentication and Authorisation Scenarios
• ARCS Authorisation Services Strategy
• Future Plan: Patterns and Solutions

HE: Higher Education
ARCS: Australian Research Collaboration Service
AAF: Australian Access Federation
Australian HE Research Infrastructure Investment

- 1998: Australian Partnership for Advanced Computing
  - APAC responsibility included Australian Grid Services
- 2001: Systemic Infrastructure Initiative
  - Focus on Data, Repositories, Access (included MAMS project)
- 2005: National Collaborative Research Infrastructure Strategy (NCRIS)
  - Delivery of National, Discipline-based capabilities
    - Platforms for Collaboration (PfC) (includes ARCS, taking over APAC role)
- 2009: Education Investment Fund - Super Science
Platforms for Collaboration (PfC)

- **PfC** is an NCRIS “Capability”
- Whole-fabric research collaboration infrastructure
  - Grid (HPC, Data), Data, Federation, Collaborative tools, Network
- **ARCS**: Australian Research Collaboration Service
  - Established 2007
- **ANDS**: Australian National Data Service
- **NCI**: National Computational Infrastructure
- **AAF**: Australian Access Federation
- **NREN**: National Research & Education Network (AARNet)
ARCS Overview

• ARCS Services Teams
  • Systems Services (Grid Services, Systems deployment)
  • Data Services (ARCS Data Fabric)
  • Collaboration Services (collaborative tools e.g. VideoConf, CMS, SW Dev)
  • Authorisation Services (Research group authN & authZ requirements analysis, authorisation advice & infrastructure, exemplars, solutions)

• ARCS Mission “long-term eResearch support, services and tools”

• Members of ARCS - state based research infrastructure
  • VPAC, Intersect, QCIF, iVEC, SAPAC, TPAC, ANU, CSIRO

• Customers: Research groups and service providers
  • National, discipline-based research groups, including PfC partners (AAF, ANDS, NCI)
ARCS Authorisation Services Role

• Support Research Groups and Service Providers in delivering services relying on authentication and authorisation (authNZ)
• Analyse requirements, and provide expertise, advice, exemplars
  • Exemplars (demonstrate what can be done to protect resources)
• Implement (procure/develop) and deploy authNZ solutions
  • satisfying research groups’ and service provider’s security requirements
• Provide customer support for ARCS Authorisation Services
  • ARCS CA’s, ARCS IdP, ARCS SLCS Server & Clients, ARCS Access Service
• Develop and pursue a ‘unified strategy’ for authNZ
  • Apply secure technologies and protocols
    • Apply Federated Access (i.e. Shibboleth) to achieve integration with the AAF
    • Apply Grid Security Infrastructure
  • Analyse access scenarios and identify patterns & solutions
Australian Access Federation

• Origins of Aust’n HE use of Shibboleth
  • MAMS project delivered an ‘operational’ Federation
    • MAMS Level-2 Testbed Federation
    • ‘zero-policy’ federation (no policy-based Trust)

• Now, CAUDIT’s Pilot AAF Project
  CAUDIT: Council of Australian University Directors of IT
  • Adopting SWITCH Federation infrastructure
    • Resource Registry, Discovery Service, uApprove etc.
  • Policy framework established “Rules for Participants”

• AusCERT will provide a PKI for Australian HE
AAF Schedule

- Pilot AAF Status
  - Technical Infrastructure & Policy Framework in place
  - Currently Migrating IdPs and SPs from MAMS Level-2 Testbed to Pilot AAF
  - Requirement for IdPs and SPs to agree to Rules for Participants
    - Best Endeavours i.e. self-asserted compliance (as described in )
  - AAFInc incorporated as an Association
    - Domain names, Trademarks etc. being procured
  - Tendering process for AAF Operators will commence 4Q09
- Production AAF due to be deployed 1H10
  - Updated Policies, stricter compliance, auditing
Attribute Usage in the AAF

• **auEduPerson schema**

• **AAF Mandatory Attributes** (as described in [Rules for Participants](#))
  
  • End-user attributes
    
    • `eduPersonTargetedID`, `auEduPersonSharedToken`
    
    • `o`, `cn`, `mail`, `displayName`
    
    • `eduPersonAffiliation`, `eduPersonScopedAffiliation`
    
    • `eduPersonEntitlement`
    
    • `eduPersonAssurance`

• **Other “attributes”**
  
  • `AuthenticationMethod`
ARCS use of auEduPersonSharedToken

• User Identifier required by ARCS Services (esp. Grid)
• Non-targeted, federation-unique, persistent identifier
  • IdP releases same aEPST value to all ARCS services for an end-user
• ARCS Auth Svcs delivers technical components and processes for generation and portability of aEPST
  • Generation
    • Uniqueness relies on statistical properties of hash function & unique inputs used to create
    • aEPST generated at IdP & stored in directory/database
  • Portability
    • When end-user moves to different IdP, takes aEPST value
      • Use of signed “statement of ownership” for porting to new IdP
      • Other mechanisms, including IdP-IdP protocol, under investigation
ARCS IdP

• ARCS has established an IdP
  • for users of ARCS services without a Federation IdP

• Registration web-interface and process
  • ARCS Registration Authority
    • Identity proofing involves internal vouching for identity
    • User confirmation required by email

• Shibboleth IdP
  • Supports AAF mandatory attributes
    • Generation & Portability of SharedToken
**ARCS IdP Workflow**

1. **Registration Request**
   - Web Browser
   - end-user

2. **Confirmation by email**
   - Change password

3. **On approval**
   - Registration Interface
     - uid + password + attributes
   - ARCS IdP Directory
     - On approval
   - ARCS IdP

4. **Password Management**
   - Change password

5. **Join ARCS IdP**
   - Password Management
   - Federated Access to Service

6. **Discovery Service**
   - Select IdP
   - Web Browser

7. **Service Provider**
   - End-user
   - attribute acceptance/mapping policy
   - Access

8. **Member of AAF**

---

Neil Witheridge  
Internet2 Members Meeting, Fall, October 2009
ARCS & Related Services (to date)

- **ARCS Services**
- **Grid Services** (Grid Security Infrastructure, Virtual Organisations)
- **Data Fabric** (WebDAV client/server, iRODS service, Groups)
- **Collaboration Services**
  - Comms & CMS/framework Tools (Web-app’s, Community/Groups)
  - CMSs requiring integration with the Data Fabric
- **Research Services**
  - Web-enabled Grid Portals (Web portals requiring delegated authentication to Grid Services)
  - OPeNDAP Services (Shib-enabled server, access via Matlab, incl. scripted)
- **Goal is for all to be accessible via the AAF**
Grid Services Use of PKI

- International Grid Trust Federation (IGTF)
- APGridPMA, EuGridPMA, TAGPMA (CA accreditation agencies)
- Grid Security Infrastructure (implemented by Globus toolkit)
  - **IGTF X.509 Certificate profiles:**
    - Classic X.509 (i.e. long-lived, defined Registration process)
    - Short-Lived Credential Service (**SLCS**)
    - Member Integrated Credential Service (**MICS**)
- APAC CA issues classic X.509 Cert’s (following Registration)
  - CA CP/CPS (Certificate Policy / Certification Practices Statement)
    - Specify identity management requirements, format for distinguished names (DNs), private key management policy
- SLCS & MICS Certificates (generate certs from Shib credentials)
Research Services Access Patterns

• Patterns encountered so far:
  • Federated access to Grid Services
  • Federated access to Web-applications
  • Federated access integration with non-web-applications
    • Access via standalone (e.g. Java) Applications
    • Access via Operating System Components
  • Federated Access involving Delegated Authentication
  • Integrating Federated Authentication & batch-mode (i.e. scripted) access
Marriage of Shibboleth and GSI

- Use of AAF Access, SLCS and Proxy Certificates
- Grid interoperability using SLCS
- SLCS and Proxy certificates deliver key authentication capabilities
- SSO for non-web services (SLCS and Proxy cert’s)
- Delegated authentication using Proxy Certificates
- Issues remain
  - SLCS certificate is cached authentication event
  - SLCS certificates without passwd protection
Grid Security Infrastructure

• Issuance of trusted X.509 Certificate
  • Signed by trusted root CA  e.g. APAC CA, IGTF accredited
  • IGTF policy requires password protection of private key for long-lived certificates

• **Use of Proxy Certificates**
  • Grid has pioneered use of proxy certificates
    • Certificate signed by private key of end-entity certificate to be proxied
  • Provides for Single-Sign-On
    • Short-lived certificate, hence no need to password protect private key
  • Delegated Authentication
    • Proxy certificate issued to service for delegated authentication
“Classic” Grid Certificates

**Grid Service (GSI-enabled)**
- **PrivGS**
- **PubGS**
- X.509 Certificate
- **DN**:
  - **PubGS**
  - **PrivGS**
  - **host**

**Grid Client (GSI-enabled)**
- **end-entity**
- **PubEE**
- **PrivEE**
- **X.509 Certificate**

**IGTF**
- **PrivCA**
- **PubCA**
- X.509 Certificate
- **DN**:
  - **PubCA**
  - **PrivCA**
  - **Root CA**

**Grid-User Registration Authority**
- **end-user**

**Registration Process**
- 1.1 Request Grid Certificate
- 1.2 Approval
- 1.3 Certificate Signing Request
- 1.4 Grid Certificate "classic" X.509
  - Lifetime ~ 1 year

**Certificate Issuance**

**Mutual Authentication**

Note: password protection of private key

**Registration Authority Operator (RAO)**

**Trusted CA Bundle**

**Trusted CA certs**

**Access Grid Service**

**Grid Client**

**Grid Service (GSI-enabled)**

**Registration Process**

**Certificate Issuance**

Neil Witheridge  Internet2 Members Meeting, Fall, October 2009
Proxy Certificates – Storing a credential
Provides for SSO and Delegation

Grid Client (GSI-enabled)

MyProxy Server

1.1 Request Put Proxy (with Grid Cert and authN credentials for retrieval)
1.2 Create Keypair
1.3 Certificate Signing Request
1.4 Sign Proxy Certificate

Trusted Grid CA
Proxy Certificates – retrieving a proxy for SSO

Grid Client (GSI-enabled)

- Request Get Proxy (with MyProxy authentication credentials)

- Create Keypair

- Retrieve Proxy Certificate Chain

MyProxy Server

- Certificate Signing Request

- Sign Proxy

Note:
No password protection of private key
Proxy Certificates – retrieving a proxy for Delegation

Service (GSI-enabled)

1.2 Create Keypair

1.3 Certificate Signing Request

1.4 Sign Proxy

1.5 Download Proxy Certificate Chain

Access Grid Service on behalf of end-user

Mutual Authentication, Delegatee Service authN with Proxy

Request Get Proxy (with MyProxy authentication credentials)

Delegation

Authorises Service to download proxy (provides credentials to authenticate to MyProxy to download proxy)
Grid Authentication and Authorisation

- Certificate DN is mapped to local account on cluster
  - Use of “AuthTool” and GUMS (Grid User Management System)
  - Several different architectures for authentication, but each convert to local account name under *nix.

- Authorisation and Virtual Organisations
  - Virtual Organisation Management System (VOMS)
    - VOMRS extended utility by allowing delegated admin and multiple VO membership
  - Extension of use of Proxy Certificates (VOMS Certificates)
    - VO membership and role stored in non-critical extension of certificate
    - VO membership and role mapped to local user/group account
VOMS Proxy Example

- ARCS uses VOMRS for Virtual Organisation Administration

voms-proxy-info -all

subject: /C=AU/O=APACGrid/OU=VPAC/CN=Graham Jenkins/CN=proxy/CN=proxy/CN=proxy/CN=proxy/CN=proxy
issuer: /C=AU/O=APACGrid/OU=VPAC/CN=Graham Jenkins/CN=proxy/CN=proxy/CN=proxy/CN=proxy/CN=proxy
identity: /C=AU/O=APACGrid/OU=VPAC/CN=Graham Jenkins/CN=proxy/CN=proxy/CN=proxy/CN=proxy/CN=proxy
type: proxy
strength: 1024 bits
path: /tmp/x509up_u1000
timeleft: 11:59:53

=== VO ARCS extension information ===

VO: ARCS
subject: /C=AU/O=APACGrid/OU=VPAC/CN=Graham Jenkins
issuer: /C=AU/O=APACGrid/OU=ARCS/CN=vomrs.arcs.org.au
attribute: /ARCS/StartUp/Role=NULL/Capability=NULL
attribute: /ARCS/Role=NULL/Capability=NULL
attribute: /ARCS/NGAdmin/Role=NULL/Capability=NULL
attribute: /ARCS/VPAC/Role=NULL/Capability=NULL
attribute: /ARCS/NRI/Role=NULL/Capability=NULL
attribute: /ARCS/Cloud/Role=NULL/Capability=NULL
timeleft: 23:55:09
uri: vomrs.arcs.org.au:15001
ARCS Short Lived Credential Service

• ARCS Grid/AAF Integration: SLCS Service (Shib SP)
  • IGTF Authentication Profile
  • SLCS X.509 Profile
  • Generation of Grid trusted X.509 certificates based on end-user attributes obtained via AAF authentication
  • Access control based on IdP agreement to Usage Policy
• SLCS Client implementation
  • ARCS Auth Svcs has implemented SLCS client java libraries
    • Grid desktop clients, Grix and Grisu, include SLCS client in order for users to authenticate via AAF
    • Users need know nothing about key-pairs, certificates
SLCS Certificate Format

• Plan for Level-1 and Level-2 CA’s (Level-2 accredited by IGTF)
  – SLCS Level-1 certificate trusted within Australian Grid Services
  – Level-1 certificate issued if `eduPersonAssurance` value is not provided or equal to value for Identity LoA = 1

• Subject distinguished name (DN)
  – DC components corresponding to SCLS CA (only Level-1 currently)
    i.e. DC=au,DC=org,DC=arcs,DC=slcs
  – O component consisting of “o” attribute value
    e.g. O=ARCS IdP
  – CN component consisting of “cn” attribute value and “auEduPersonSharedToken” attribute value
    e.g. CN=John Citizen ZsiAvfxa0BXULgcz7QXknbGtfxk
  – Example DN value
    DC=au,DC=org,DC=arcs,DC=slcs, O=ARCS IdP,
    CN=John Citizen ZsiAvfxa0BXULgcz7QXknbGtfxk

• altSubjectName
  – “mail” attribute value (valid email address for user)
SLCS Client Implementation

• SLCS Client needs to generate key-pair in secure file-system location

• Current java library implementation, and command-line implementation using java library

• Client relies on
  • Built in http client to interact with DS, IdP
  • Screen-scraping of IdP authentication interface
  • Users entering IdP credentials into non-browser interface

• ARCS Grid clients: Grix and Grisu
SLCS Grid Certificates Workflow

1. Enter IdP username & password

2. Discover Service
3. Identity Provider
4. VOMRS
5. Startup VO
6. SLCS Level-1 CA
7. SLCS Level-2 CA
8. ARCS Security Infrastructure

Attributes used:
- auEduPersonSharedToken
- CN
- mail
- eduPersonAssurance

end-user
ARCS Data Fabric

• Effective Data Management and Storage
  • Critical capability for Researchers, PfC focus

• Data Storage Solution: ARCS Data Fabric

• Distributed storage aggregated using iRODS
  (Integrated Rule-Oriented Data System)

• Interfaces to iRODS
  • CLI (iCommands), GUI (iRODS Explorer), Web (iRODS Web Browser)
    • Username/password or GSI authN
  • DAVIS
    • WebDAV and HTTP access
Data Fabric Workflow
(access via DAVIS)

Enter: IdP, username & password (a)

(a) Considering using an ARCS Username and Password generated by ARCS Access Service for use in accessing ARCS Data Fabric
ARCS Collaboration Tools

• Content Management Systems & Frameworks
  • Plone, Twiki, Confluence, Sakai, Drupal
    • Integration with AAF and Data Fabric (links to DF resources)

• Communications Tools
  • EVO, Access Grid, Jabber
    • What are the authentication and authorisation requirements
      • Cost/benefit of integration with AAF authentication
        • How much work, internal refactoring, to integrate

• Collaborative Software Development Tools
  • Trac, SVN, Git, Hudson
    • Web interfaces protected by Shibboleth. CLI’s?
Plone Integration with AAF + Data Fabric

• **AAF Integration Plone** (Shibboleth-enabled authentication)
  • Attribute requirements for Plone
    - SharedToken, mail, cn, displayName (generation of WikiName)

• **Data Fabric Integration** (requires GSI *and* Shibboleth)
  • **Requirement:** Search for DF resource to link to
    - Access iRODS via GSI to view and select DF resource
      - Obtain user’s SLCS certificate, authenticate with iRODS
      - iRODS delivers list of resources accessibly by user
  • **Requirement:** Access DF resource via link
    - Link to protected resource, maybe user can’t access
      - Access via Davis, using Shibboleth SSO
      - If authorised to access, Davis provides download dialog
Web Portal Access To Grid Resources

• Development by auScope of an AAF-enabled Web Portal which requires delegated authentication to access Grid Service
  • How can a portal obtain the user’s SLCS certificate proxy without user creation of SLCS?
  • It can’t.

How about the portal generating the user’s SLCS certificate?

• IGTF SLCS Profile specification (Private Key Management)

The SLCS authority shall issue X.509 short-lived certificates to end-entities based on cryptographic data generated by the applicant, or based on cryptographic data that can be held only by the applicant (e.g. on a secure hardware token; generated from a transient yet unique session handle retrieved from the applicant’s encrypted session).

(RFC3647:§6.1)
Approaches Considered & Prototyped

- **SLCS Delegation Service**
  - Portal generates the user credentials i.e. keypair & requests and is issued a certificate under the users DN
    - Portal generates and manages the user’s credentials

- **SLCS Proxy Service**
  - ARCS SLCS Proxy Service generates the user credentials & requests a SLCS certificate under the user’s DN, & uploads the SLCS certificate to MyProxy allowing the portal to retrieve a proxy cert signed by the user’s SLCS cert.
    - ARCS Service generates and manages the user’s credentials
    - Portal obtains a proxy certificate
SLCS Delegation

ARCS Security Infrastructure

1. EU Access
2. Redirect to SLCS Delegation Service
3. authenticate
4. attributes
5. http POST
6. SLCS Certificate Signing Request
7. CSR
8. SLCS certificate
9. Access GSI Service with Delegated Authentication

Web Portal Service
- EU key-pair & SLCS cert

Grid & Delegation Service Client

Shib SP
- SLCS Delegation Service

Shib IdP
- attributes

SLCS CA
- SLCS certificate

GSI

end-user
- web-browser

EU Client

Authorisation token

Redirect to SLCS Delegation Service

Authenticate
Web Portal Delegated Access

• Becoming a common requirement
• **Proposed change** to IGTF Guidelines
  • Generation and Storage of Private Keys on an appropriate computer system that is administered by a third party
  • To be discussed at OGF27 next week.
  • Still stringent requirements on 3rd Party handling of user’s private keys
  • If passed, SLCS Delegation OK if Portal conforms to guidelines, and SLCS Proxy OK as ARCS will conform.
Access to OPeNDAP resources

• OPeNDAP server (Shibboleth-enabled)
  • Access to GeoSpatial Data
    (Integrated Marine Observing System IMOS)
  • Access typically via non-web client tools such as Matlab
    • Matlab uses OPeNDAP client library (Java, Python)
• Integrating AAF Authentication & Matlab access
  • Considered Shibboleth Proxy
    • Requires storing user’s IdP cred’s in a config file.
• Batch-mode access to OPeNDAP resources
  • Scripted invocation of Matlab with no end-user interaction
• Solution: use of SSL AuthN (user’s SLCS Certificate)
Matlab batch-Mode Access

To OPeNDAP resources (Use of SLCS Certificate for SSL Authentication)
Recap: Authentication Scenarios Examined

- Browser to web applications (not many yet, Grid focus)
- SLCS Access to Grid Services (Certificate life-time issues, still need to support access via classic certificates)
- SLCS Client workflow (entering IdP credentials into non-browser UI’s)
- Data Fabric access (passing IdP cred’s to DAVIS via WebDAV)
- Web portals access to Grid Services (Delegation issue)
- CMS (e.g. Plone)/AAF/Data Fabric Integration
- Non-Web Client access to OPeNDAP services (Matlab)
- Batch-mode access to OPeNDAP services
- These address Authentication, not Authentication
ARCS Authorisation Scenarios

• How is authorisation currently performed for ARCS Services?
  • Virtual Organisation Management for Grid
    • VOMRS
  • Data Fabric: Groups in iRODS
  • Collaboration Services: Groups in CMS’s
• Recognition of need for Services to control access and authorisation rights
  • Information from IdPs not useful in general for authZ
ARCS Access Service

- ARCS Access Service for ARCS Services
- Registration (assignment of Default Authorisation Rights)
  - Tracking user communities (auEduPersonSharedToken)
  - Allocate ARCS Username (ARCS Services unique name)
    - consistent user naming across ARCS Services
  - Caching attributes at time of registration
    - Detecting attribute change (e.g. IdP, affiliation)
- Authorisation Rights Management
  - For non-default Authorisation Rights
    - Authorisation Rights tokens urn:<ServiceIdentifier>:<Token value>
ARCS Access Service

Shib-enabled Services

SP

Response (authZ rights, ARCS username, Δatts)

non-Shib-enabled Services

ARCS Username

Registration

Specify Services

ARCS Registrar

Registration Process

IdP

ARCS LDAP

Shib attributes

Shibboleth attributes

ARCS username & pwd

Authorisation Rights Management

Attribute Change Detection

Shib AuthN

Query (SP, aEPST, atts)

ARCS username & pwd AuthN

Authorisation Rights

ARCS Access Service

Default

Registration approval for chosen SPs

ARCS Username

Specify Services

ARCS Access Service

IdP

Shib AuthN

end-user

ARCS Registrar

Registration Process

ARCS Username

ARCS Registrar

Registration approval for chosen SPs

ARCS Username

Registration Process
ARCS Authorisation Services Strategy

• Avoid deviating from proven protocols
  – Security analysis difficult, costly (so minimise)

• Analyse research services access and chains of authNZ information flow
  – Identify patterns and formulate solutions
  – Adopt proven (security analysed) mechanisms
    • Shibboleth
    • GSI (X.509 certificates, Proxy Certificates)
      – Classic, SLCS & MICS certificates (IGTF profiles)

• Differentiate Authentication and Authorisation patterns
ARCS Authorisation Services Strategy (cont’d)

• Identify “secure enough” (e.g. take lead from Grid)
• Hide PKI from end-users
• Take heed of HE identity management policies
  • Don’t require entry of credentials into untrusted interfaces of storage in file-system
  • Prohibit shared identities (e.g. shared “test” account)
• Keep usage logs, allow self auditing
• Provide production quality components to implement usable & reliable solutions.
• Track international trends and adopt & adapt
Abstraction and Classification

• ARCS Authorisation Services is seeking to abstract Authentication and Authorisation workflows in HE research domain

• Identify & document patterns & implement solutions
  – Deliver (or recommend 3rd party) production quality libraries & tools for research service developers
  – Acquire or construct required Middleware
    • Shibboleth, GSI (or plain old SSL) enablement
  – Apply incremental and iterative analysis and development to patterns & solutions
  – Keep track of and in sync with global trends
Auditing and Auditability

• Importance of detecting intrusion & compromise
• Emphasize logging and auditing from ground–up
  – Allow self-audits
  – Email reports to users on activities?
    • Signed & encrypted email for security
• Automated Detection
  – Reporting unexpected activity
• Respond to compromise alerts, identify responsibility for forensics
• Open Questions
  – Would self-auditing actually work in research community?
  – Ultimately, automated auditing is an important goal.
ARCS Auth Svcs Future Directions

• Authentication
  • Understand Shibboleth Roadmap and implications
    • New Shibboleth profiles (ECP, key-holder)
  • Understand Grid ‘Roadmap’ and implications
    • Changes to Grid (OGSA i.e. Web Services, SOA)
  • Use MICS (Long-lived credentials from Shib) & SLCS

• Authorisation
  • Develop and utilise the ARCS Access Service
  • Investigate CoManage for Authorisation Rights Mgmt
  • Investigate and deliver exemplars of use of XACML
ARCS Auth Svcs Future Directions

Tracking international trends in authN/Z technology interoperability

Authentication:

Shibboleth SAML future profiles
Shibboleth SAML current profiles
Grid GSI SSL X.509 & Proxy Certs
OGSA SOA WS ws-security

Current focus in ARCS

Authorisation:

Authorisation Rights Mgmt: ARCS Access Service CoManage, Grouper, PerMIT?
Authorisation processing: XACML?
End of Presentation

Questions?

Thankyou

Supported by the Australian Government