IRIS Security

Trust Framework and Operational Security

David Crooks
EGI CSIRT
IRIS Security Team
david.crooks@stfc.ac.uk

IAM Users Workshop January 2021

Topics

1 Trust Framework

2 Operational Security

3 Distributed Research Trust and Security

Science and Technology Facilities Council

iris

AAI and Security for IRIS

- High level requirements

- Identity Management
  - Authentication of our users with an appropriate level of assurance
  - Coupled with appropriate service authorisation mechanisms
- Policy
  - Rules of engagement and expectations for participation in the infrastructure
- Operational security
  - Supporting the prevention of incidents and coordinating incident response

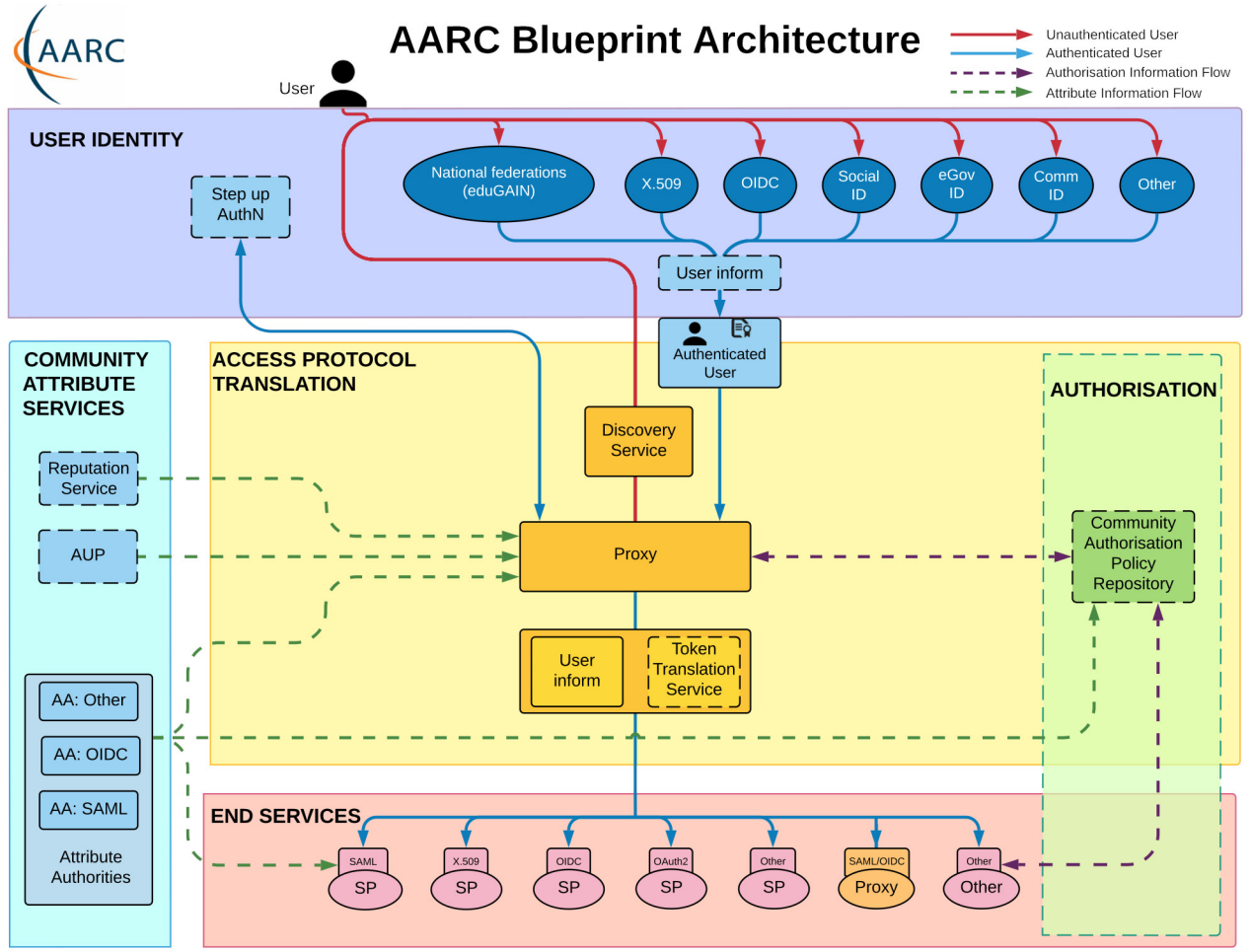
AARC Blueprint Architecture

- Authentication and Authorisation for Research Collaboration
- Recently completed EU projects

- AARC BPA

“A set of software building blocks that can be used to implement federated access management solutions for international research collaborations”

- https://aarc-project.eu/architecture/



Science and Technology Facilities Council

iris

Identity Management: IRIS IAM

- IRIS IAM is very successfully operating as an AARC Blueprint Architecture identity proxy

- Part of UK Access Management Federation and eduGAIN
  - Provides access to global network of identity providers (IdPs)
  - Authentication by users' home institutions

- Capability to act as Identity Proxy of last resort
  - For users that don't have a suitable eduGAIN Identity Provider

Science and Technology Facilities Council

iris

Context and requirements

- IRIS contains a range of resource providers with existing policy frameworks
  - Need to develop a framework that sits alongside these and enables secure distributed operations
- Some providers are already connected within the wider federated world
  - Particularly GridPP/WLCG
- However: it does represent a new community in its own right
  - And exists within a distributed, federated infrastructure landscape
- Establish the necessary policies to allow interoperation between resource providers, services and user groups
  - And relationships to existing policy

Policy Roadmap

- Policy underpins all other security activity
- Acts to engender trust both within an infrastructure, but also with neighbours
- IRIS IAM follows AARC Blueprint Architecture
- AARC Policy Development Kit is therefore excellent starting point

Science and Technology Facilities Council

iris

AARC PDK

- AARC Policy Development Kit
- 9 documents aimed at best practice bootstrap for infrastructures & communities deploying the AARC Blueprint Architecture
  - Federated IDPs with services/resources ‘behind’ an AAI Proxy
- Policies intended to co-exist with local policies where applicable

Science and Technology Facilities Council

iris

WISE

- Wise Information Security for Collaborating e-Infrastructures
  - https://wise-community.org/about-wise/
- Global collaborative community of security experts
- People interesting in taking part are welcome!
- IRIS policy work takes place as part of WISE community

  - Benefit to IRIS of considerable experience
  - Benefit to WISE and wider community of new requirements and context

- Building on PDK in SCI-WG

Science and Technology Facilities Council

iris

WISE COMMUNITY

AARC Policy Development Kit

Document	Who should complete the template?	Audience	Description
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.

Challenges

- IRIS is a relatively new collaboration but with well established participants
  - What implications does this have?
- Well established policies in place at individual institutions
  - New operational workflows being developed
- Bootstrap security policy set
  - Challenge of deciding best order of work while governance structures being established
    - Infrastructure Security Policy provides foundation
  - Need to show end users AUP/Privacy Notice so these are a priority
    - Already established *working* versions to enable IRIS IAM

Science and Technology Facilities Council

iris

AARC Policy Development Kit

Document	Who should complete the template?	Audience	Description
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.

Status

- IRIS Infrastructure Policy now approved
  - Provides high-level framework for other subordinate policies
  - Defines roles and responsibilities
- Review of working AUP and Privacy Notice underway in light of approval
  - IRIS IAM users sign AUP
  - Present AUP to other users to make them aware of provisions
- Drafting in progress on Service Operations Security Policy

- Work has begun on a risk assessment for services connected to IRIS IAM to inform the assurance profiles appropriate for IRIS
  - Informs Community Security Policy and Acceptable Authentication Assurance Policy

UKRI Science and Technology Facilities Council

iris

Operational Security

- Operating a secure infrastructure
  - Depends on and works alongside Identity Management and Policy
- Capabilities and processes
  - Risk management
  - Patching
  - Vulnerability management
  - Security tools and monitoring
  - Access controls
  - Traceability (who, what, where, when, how)
  - Incident response

Science and Technology Facilities Council

iris

IRIS Operational Security capability

- IRIS Security Team
  - Membership from GridPP, Cloud, HPC
  - Common understanding of IRIS technology stacks
  - All active members agree to CSIRT Code of Practice
  - Share sensitive information appropriately within team
  - Key contact point with other CSIRTs
    - Jisc/Institutions/Other CSIRTs
- Communication channels
- Security contact information
  - GOCDB

Science and Technology Facilities Council

iris

IRIS Operational Security capability

- Next steps
  - Communications challenge
  - Additional workshops and training materials
  - Build on access to threat intelligence for IRIS sites

- In the future
  - Service security challenge
  - Evaluate our procedures
  - IRIS IAM is a vital part of this process
    - Also backs MISP threat intelligence

Science and Technology Facilities Council

iris

Distributed Research Trust and Security

- Within STFC in SCD and PPD we have people working on all areas of distributed security
  - Security Coordination
  - Identity Management
  - Trust and Policy
  - Operational Security
- Collectively many years of experience
  - National and international contacts
- Working to bring together a new team representing all these areas
  - Single point of contact to support communities in a distributed federated landscape

UKRI Science and Technology Facilities Council

iris

Science and Technology Facilities Council

Questions?