



Authentication and Authorisation for Research and Collaboration

Deliverable DNA3.3

Recommendation for service operational models for enabling cross-domain sustainable services

Peter Gietz, David Hübner, Heiko Hütter,

NA3

DAASI International



5th AARC General Meeting, Athens

20-22 March 2017

Summary

- Part 1: Framework to define sustainable services
 - Guidelines to operate services in a sustainable way
 - Template to evaluate services
- Part 2: Policy Recommendations
 - For national research and education federation operators
 - For research and e-infrastructure service providers

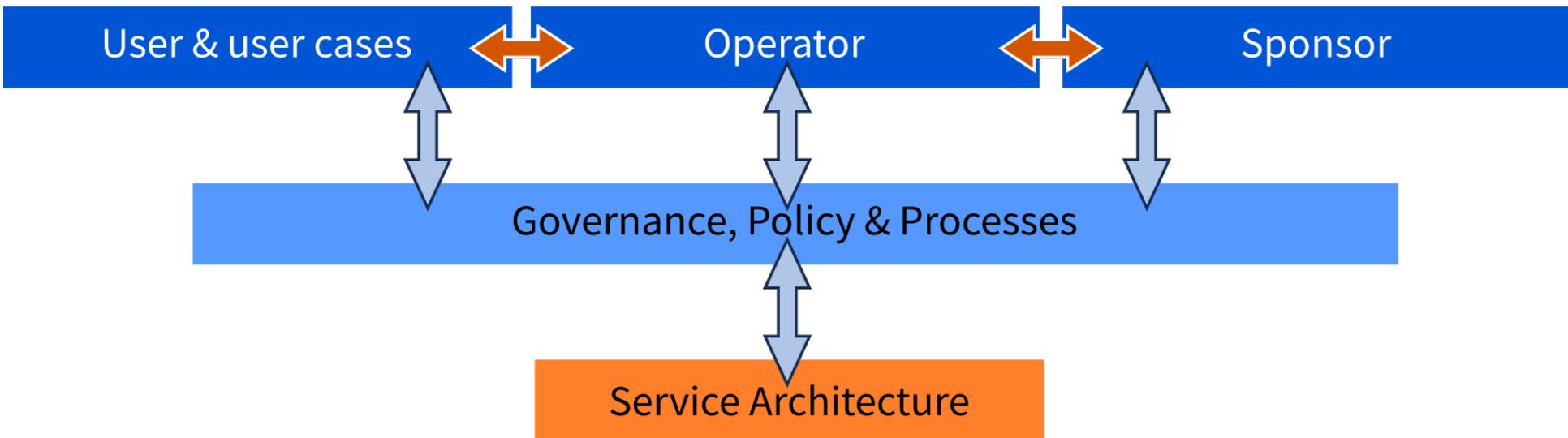
History

- Basically we now have two texts:
 - A first longer (28 p) version that
 - Gives a detailed report on the policy survey (The current landscape of R&E federations wrt governance and policies)
 - And then has a more elaborated Framework for research projects to develop a service operational model
 - <https://docs.google.com/document/d/192eP5PixHkIcGrs1AG4lv68p0V-brVGlecbd8rQp6U/>
 - A second sort of rewrite (12 p) that
 - Has a revised Version of the Framework / Template
 - Has only a summary of the policy survey
 - Gives a number of recommendations for SPs and for federation operators
 - <https://docs.google.com/document/d/1wOPjCCiRxk1fTfo8xAw7AeIJ0dEgBsb5DuBdEje844>
- Question: does it make sense to put the survey Text of version 1 into a appendix in version 2

Part 1: Framework to define sustainable services

Framework to define sustainable services

- Five critical aspects to consider



Thanks to Gerben Venekamp for this diagram

Framework to define sustainable services

- 1. Use Case and User base
 - What is the service about?
 - Estimated user base?
 - Existing services?
- 2. (Service) Operator
 - Who should operate the service? Why?
 - Who does training/support/promotion?
 - Basis for the operator to estimate costs

Framework to define sustainable services

- 3. Sponsor / Funding model
 - What are the plans for long term cost recovery?
 - Risks?
- 4. Governance, policies and processes
 - Specific policy/security aspects to consider?
 - Availability requirements?
 - Monitoring? Accounting? Documentation?
- 5. Service implementation
 - What is the current architecture?
 - What elements compose the service?
 - Required Equipment?

Framework to define sustainable services

- Template with questions for these five aspects
- Aims:
 - assess compatibility with federated IdM infrastructure(s)
 - assess sustainability of services
 - explore deployment scenarios
 - estimate costs and efforts to run the service
- Some questions might be difficult to answer in early project phases
- Difficult to find questions that apply to all services
- Selected AARC pilots were asked to fill out the template
- Template is still work in progress
 - → <https://bit.ly/2mzgU85>

Framework to define sustainable services

- Already some answers
 - LDAP Facade
 - Social IDs to SAML proxy
 - WATTS
- Generally good answers
 - Use case and user base
 - Operator (especially initial costs)
 - Service implementation
- Problematic aspects
 - Sponsor / Funding model (especially long term cost recovery)
 - Governance, Policies and processes

Todos in this part of the document

- We only have the AARC RAUTH service as example pilot, with filled out template, yet, and that is not in-line with the new set of questions
- We need a space in the document for the Guest IdP risk analysis.
 - I propose to first fill out the template for the Guest IdP running productively in DARIAH (although not an AARC pilot)
 - then add language from the two JRA1 documents that should be included into NA3.3:
 - Enabling Guest Identity Access to Services
 - Managing Risks of using guest Identities
- Should't we put all the answers (RCAuth, LDAP Facade, Social IDs to SAML proxy, WATTS) in an appendix and just put a summary in the actual text

Part 2: Policy Recommendations

Policy Recommendations

National Research and Education Federation operators

- Only aspects that have implications for SP are considered
- Interviews with different federations operators
- Changing policies takes time & effort
- Limit policy recommendations to most important ones

Policy Recommendations

National Research and Education Federation operators

- Support eduPersonUniqueId as unique identifier
- Consume eduGAIN metadata
 - Instead of adding services manually
- Promote adoption of R&S entity categories
 - To standardize attribute release
- Ensure that home organizations do not reuse user identifiers
- Promote and support participation to Sirtfi to handle incident response
- eduGAIN should create a support virtual desk

Policy Recommendations

Research and e-infrastructures service providers

- Recommendations for service providers:
 - support CoCo whenever possible
 - comply with Sirtfi
 - apply for R&S entity category
 - be prepared to handle user identities with low or no assurance
 - be prepared to manage users relying on social IdPs
 - follow REFEDS discovery guidelines
- Two proposals:
 - Have an extra recommendation on LoA (by now it is handled at the zero LoA recommendation). Is Espresso and Cappuccino ready for being recommended to SPs?
 - Have a recommendation on (not or only carefully) joining more than one federation

Thank you

Any Questions?

info@daasi.de



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).