AARC

Authentication and Authorisation for Research and Collaboration

The AARC Project – First 6 months

Christos Kanellopoulos

JRA1 – Architecture WP Leader

GRNET

Service orientation to data and high-performance computing infrastructures

Bari, 12 November 2015

Authentication and Authorisation for Research and Collaboration

- Two-year EC-funded project
- 20 partners
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1st May, 2015
- https://aarc-project.eu/

AARC Vision and Objectives

Avoid a future in which new research collaborations develop independent AAIs

Impacts

- Create a cross-e-infrastructure 'network' for identities
- Reduce duplication of efforts in the service delivery
- Improve the penetration of federated access

Outputs

- Design of integrated AAI built on federated access
- Harmonised policies to easy cross-discipline collaboration
- Pilot selected use-cases
- Offer a diversified training package

Approach

Integration, policy harmonisation, piloting and training

Design an integrated AAI built on production infrastructures

Use existing e-infrastructures in the delivery chain

Work with e-infras and user communities to solve existing challenges, pilot use-cases and get feedback on the results

AARC Work areas

Training and Outreach

Architecture Design

Policy and best practices harmonisation

Pilots and results validation

First Results

Training and Outreach

Requirements & existing material

Repackage and add what is missing

- Value proposition
- Federation 101
- Training for SPs
- Training on AARC results

- First document describing the approach to the training:
  - https://aarc-project.eu/documents/milestones/

- Report on the identified target groups for training and their requirements
  - https://aarc-project.eu/wp-content/uploads/2015/04/AARC-DNA2.1.pdf

- End of the month the first online module on federated access
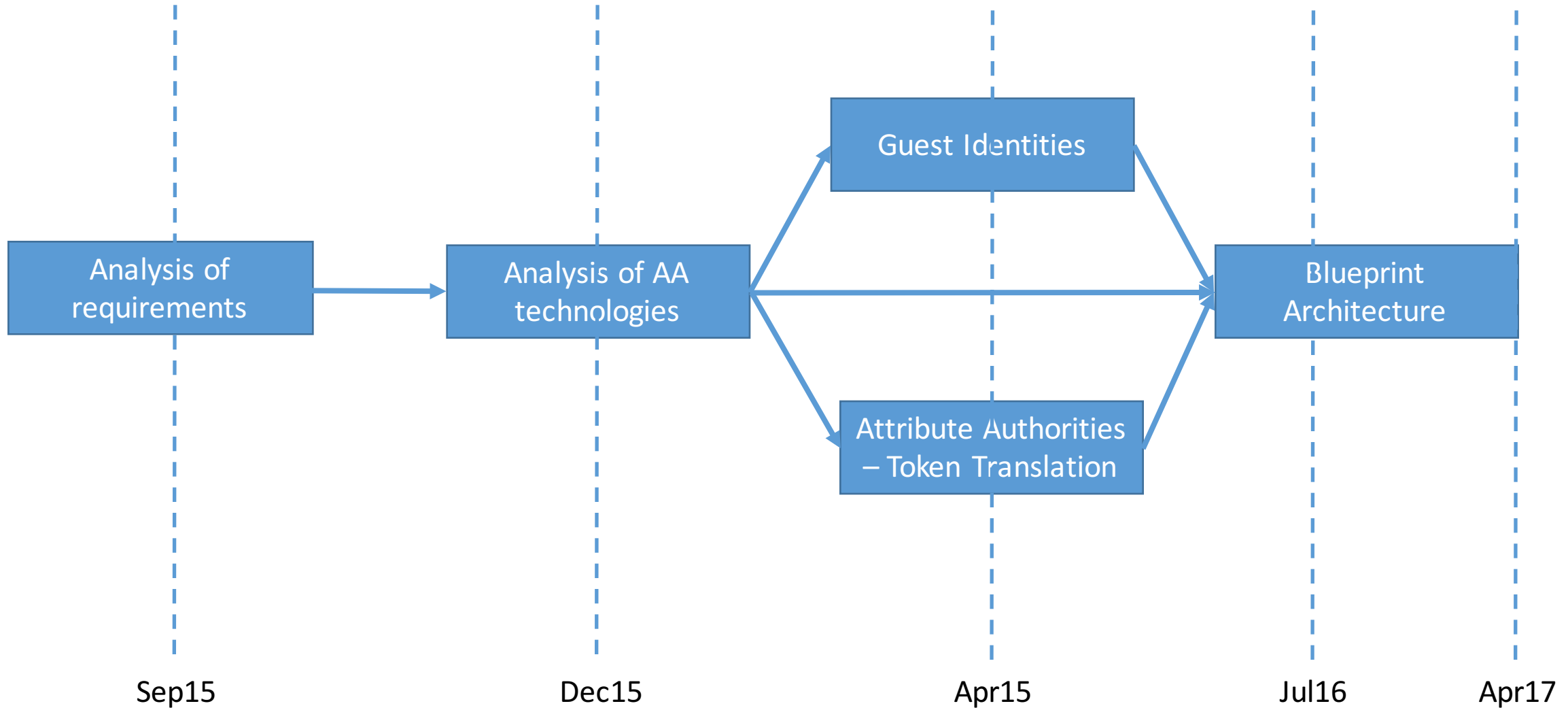 - https://aarc-project.eu/documents/training-modules/federations-101/

Policy and Best Practices Harmonisation

- Security Incident on FIM
  - **To agree on a generic security incident response procedure for federations**
  - Sirtfi Trust Framework to be finalised at the next I2 Tech Exc
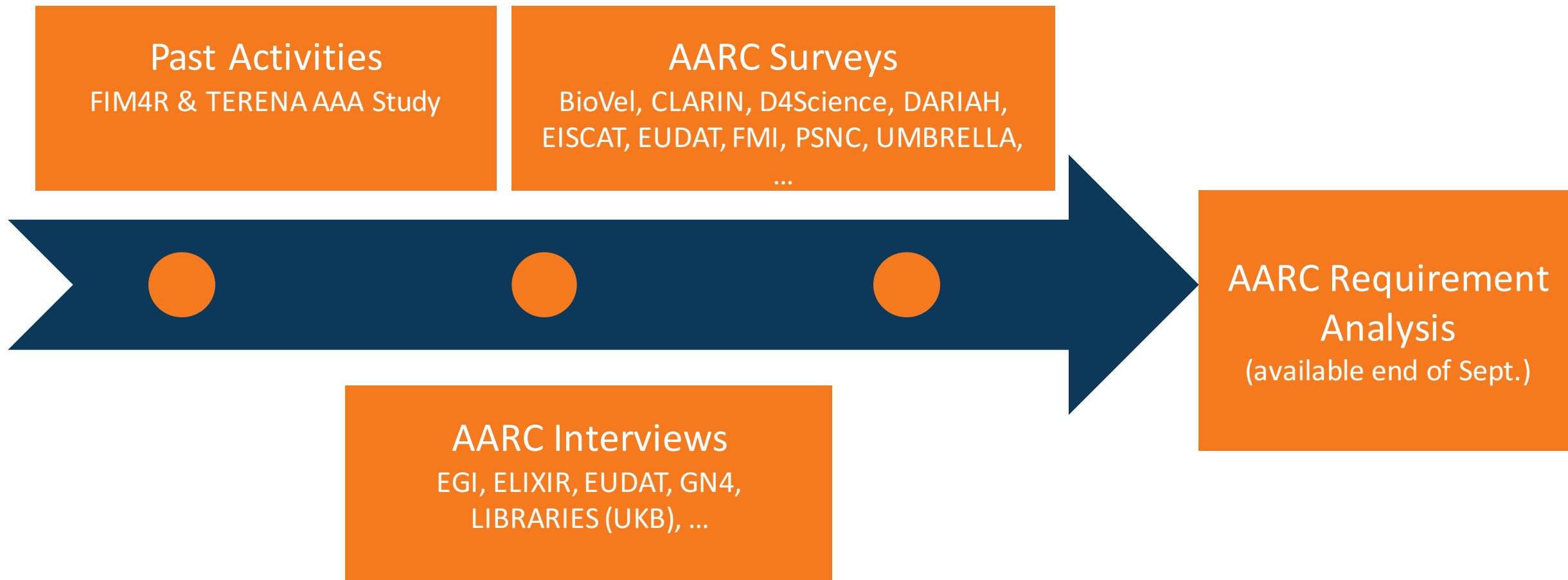
- Sirtfi WG:
  https://wiki.refeds.org/display/GROUPS/ SIRTFI

- LoA work
  - **To agree on a sustainable LoA framework**
  - AARC (through surveys and FIM4R) looking at immediate and longer-term need by SPs and RPs: https://wiki.geant.org/display/AARC/LoA+ survey+for+SP+communities
  - Key challenge is cost of operation, and who bears this costs

- R&E federations and their IdPs looking at the 'service aspect' of providing assurance

Architecture Design

Architecture Design – Analysis of requirements

Past Activities
FIM4R & TERENA AAA Study

AARC Surveys
BioVel, CLARIN, D4Science, DARIAH, EISCAT, EUDAT, FMI, PSNC, UMBRELLA, …

AARC Interviews
EGI, ELIXIR, EUDAT, GN4, LIBRARIES (UKB), …

AARC Requirement Analysis
(available end of Sept.)

Architecture Design – Analysis of requirements

1. User Friendliness
2. Homeless Users
3. Different Levels of Assurance
4. Community based authorization
5. Flexible and scalable attribute release policies
6. Attribute Aggregation & Account Linking
7. Federation solutions based on open and standards based technologies
8. Persistent & Unique User Identifiers
9. User managed Identity Information
10. Up to date identity information
11. User groups and roles
12. Step up authentication
13. Browser and non-browser based federated access
14. Delegation
15. Social media identities
16. Integration with e-Government infrastructures
17. Service Provider Friendliness
18. Effective Accounting
19. Policy Harmonization
20. Federated Incident report Handling
21. Sufficient Attribute release
22. Awareness about R&E Federations
23. Semantically harmonized identity attributes
24. Simplified process for joining identity federation
25. Best practices for terms and conditions

Architecture Design – Analysis of requirements

1. User Friendliness
2. Homeless Users
3. Different Levels of Assurance
4. Community based authorization
5. Flexible and scalable attribute release policies
6. Attribute Aggregation & Account Linking
7. Federation solutions based on open and standards based technologies
8. Persistent & Unique User Identifiers
9. User managed Identity Information
10. Up to date identity information
11. User groups and roles
12. Step up authentication

13. Browser and non-browser based federated access
14. Delegation
15. Social media identities
16. Integration with e-Government infrastructures
17. Effective Accounting
18. Policy Harmonization
19. Federated Incident report Handling
20. Sufficient Attribute release
21. Awareness about R&E Federations
22. Semantically harmonized identity attributes
23. Simplified process for joining identity federation
24. Service Provider Friendliness
25. Best practices for terms and conditions

Architecture Design – Next steps

- Continue the interviews with the AARC stakeholders and the parallel work on Guest Identities and Attribute Authorities (AA) & Token Translation Services (TTS)

- End of October first internal draft release of AARC High Level Architecture

- End of December: Analysis of available AA technologies

- January – February: Consultation with stakeholders around the AARC High Level Architecture

- Arpil: Release work on Guest Identities , AAs and TTS

- July: 1st version of the AARC AAI Architecture Framework

Preparation for AARC 2

- Although the AARC project has only started for a few months, we have started the preparation for AARC2

  - focus on user-driven innovation and pilots on existing e-Infrastructures to respond to user-community challenges

  - Help us identifying use-cases:

    https://docs.google.com/a/terena.org/forms/d/1xHaCINRaizjWfY6K-4-1O9z81NAyBsmxtJNSNGXSICU/viewform

Thank you
Any Questions?

skanct@grnet.gr

AARC

http://aarc-project.eu/