



Authentication and Authorisation for Research and Collaboration

AARC

Christos Kanellopoulos

AARC Architecture WP Leader

GRNET

Open Day Event: Towards the European Open Science Cloud

January 20, 2016

Authentication and Authorisation for Research and Collaboration

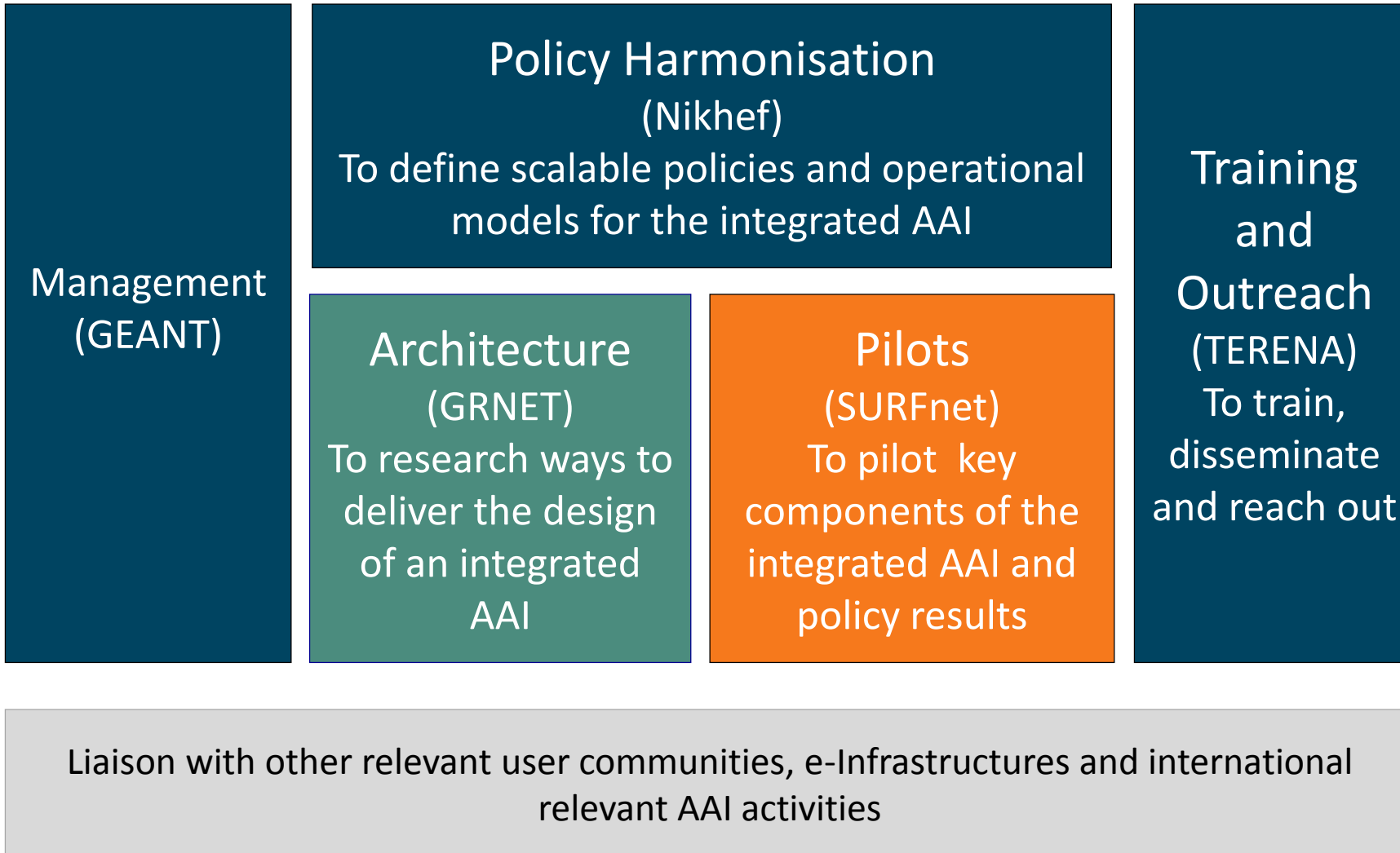


- Two-year EC-funded project
- 20 partners
 - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1st May, 2015
- <https://aarc-project.eu/>



What AARC does

- Help research communities to use federated access
- Address some of the FIM4R requirements
- Deliver a blueprint architecture to enable users to access services operated by different e-Infrastructures
- Prepare documentation and training on AARC and REFEDS results, key aspect of federated access and eduGAIN etc

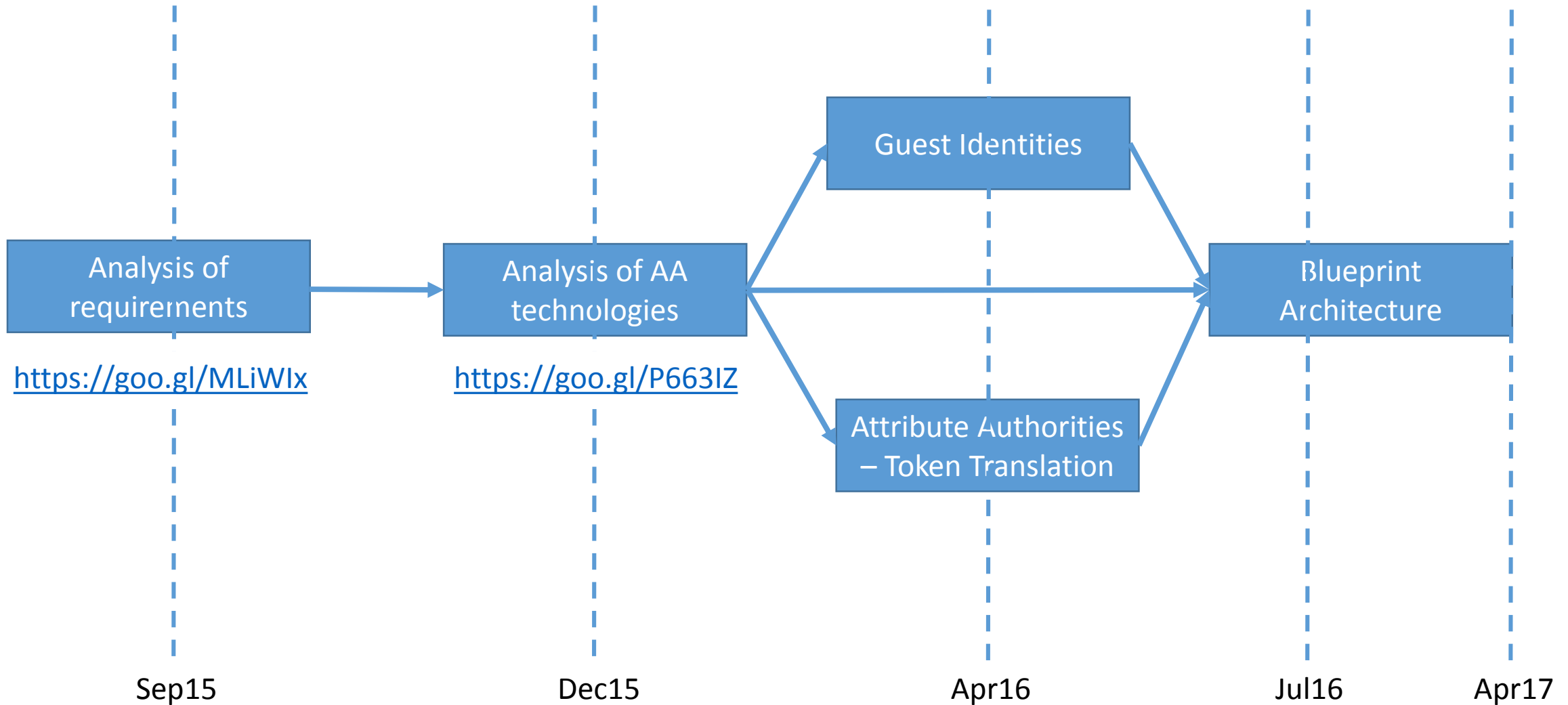


Three decorative arcs are positioned around the central text. A grey arc is at the top left, a purple arc is at the top right, and a yellow arc is at the bottom, all curving towards the center.

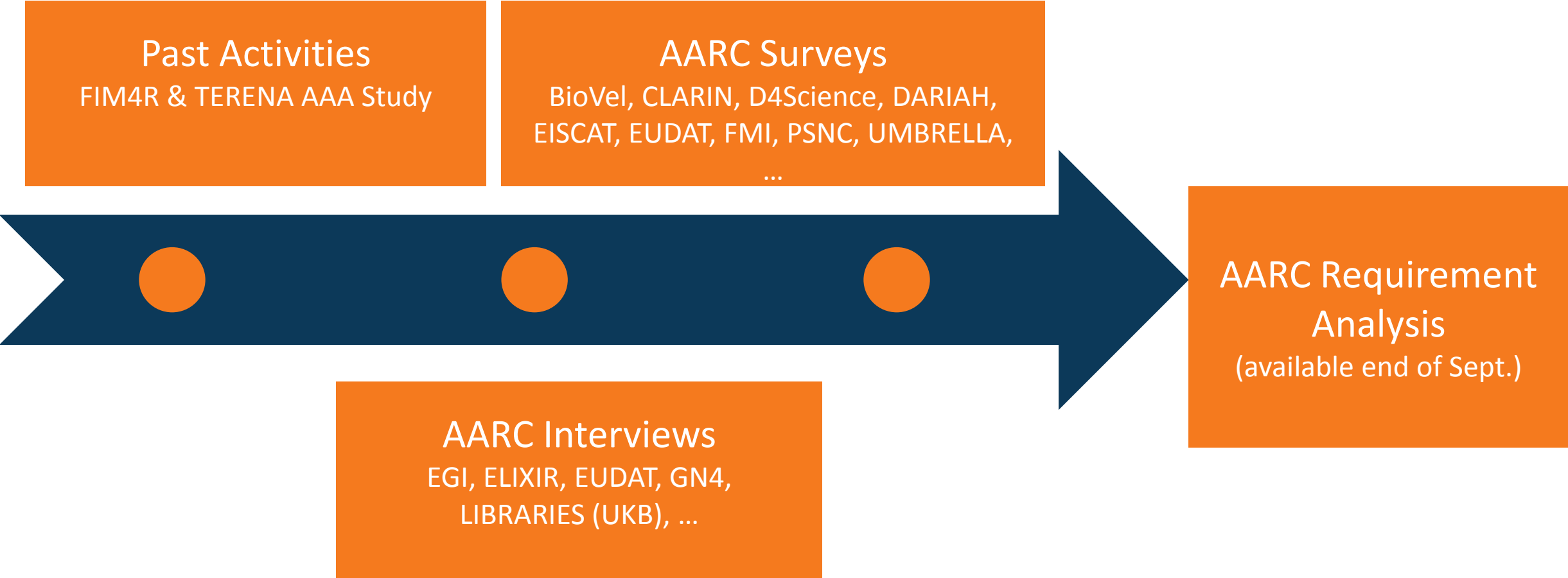
Repackage and add
what is missing

- 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>
- First online module on federated access
 - <https://aarc-project.eu/documents/training-modules/federations-101/>

Architecture Design



Architecture Design – Analysis of requirements



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

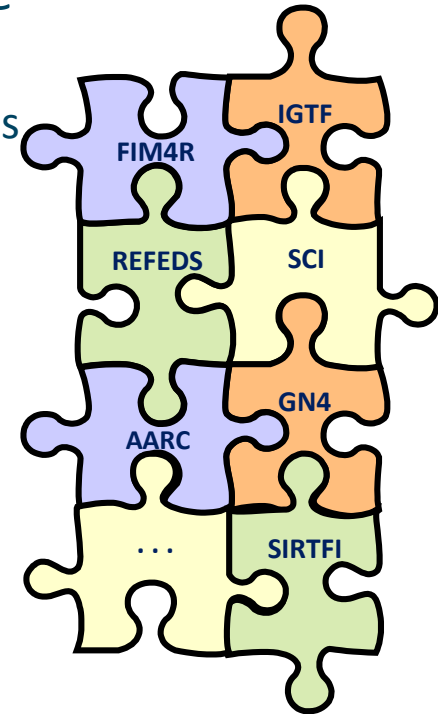
1. User Friendliness
2. Homeless Users
3. Different Levels of Assurance
4. Community based authorization
5. Flexible and scalable attribute release policies
6. Attribute Aggregation & Account Linking
7. Federation solutions based on open and standards based technologies
8. Persistent & Unique User Identifiers
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 – Roadmap

- 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
- February - April: Consultation with stakeholders around the AARC High Level Architecture
- April: Release work on Guest Identities , AAs and TTS
- July: 1st version of the AARC AAI Architecture Framework

The Policy Puzzle

- Many groups and many (proposed) policies, but they leave also many open issues
- via AARC Policy and Best Practice Harmonisation we try tackling a sub-set of these
 - “Levels of Assurance” – a minimally-useful profile and a differentiated set, for ID and attributes
 - “Sustainability models and Guest IdPs” – how can assurance be offered in the long run?
 - “Scalable policy negotiation” – beyond bilateral discussion
 - “Protection of (accounting) data privacy” – aggregation of PI-like data in collaborative infrastructures
 - “Incident Response” – encouraging ‘expression’ of engagement by (federation) partners and a common understanding
<https://wiki.refeds.org/display/GROUPS/SIRTFI>



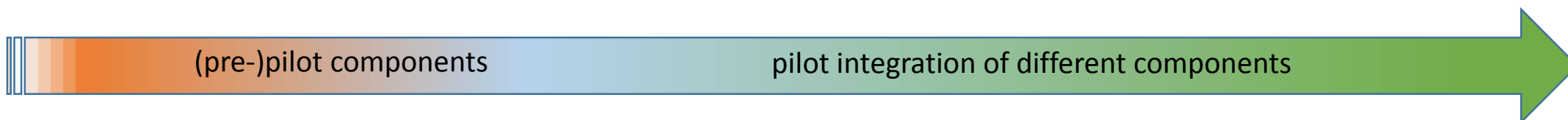
Activities in SA1 Pilots: planning

DJRA1.1
Requirements

MJRA1.1 Existing AAI and
available technologies for federated access.

DJRA1.2 Blue
Print architecture
NA3.1 Differentiated
LoA recomm. DNA3.3 Recomm.
Sustainable models

Q4-2015	Q1-2016	Q2-2016	Q3-2016	Q4-2016	Q1-2017
		guest access pilot M14	first report on pilots M15	attribute provider framework pilot M20	access to R&E resources pilot M23
Pre-pilot work: access to library resources	Guest access: Library proxy (?)	Guest access: Social IDs	Guest access: eGov IDs	Integration test: Community A	Inter-community sharing of resources
Pre-pilot work: e-gov/social ID	Guest access: Community IDs	Guest access: Reputation service?		Integration test: Community B	
Pre-pilot work: attribute management	orcid SP (SN + IDEM)	voPAAS (COmanage) on boarding		Integration test: Community C	
Pre-pilot work: token translation	Attributes: COmanage/other?	Attributes: Aggregation			
Pre-pilot work: commercial provider	Token translation: CI-logon	Attributes: SP consuming attributes?	Token translation & attributes: CI-logon + VOMS (other sources?)		
Pre-pilot work: ?	Commercial service: ?	Orcid as an AA	CI-logon2 + COmanage (aas)		



AARC2

The call for AARC 2 and its implications

“Development of a pan-European identity federation services for researchers, educators and students...Stimulate AAI services supporting communities involved in the emerging data-rich science era to manage and share their resources”

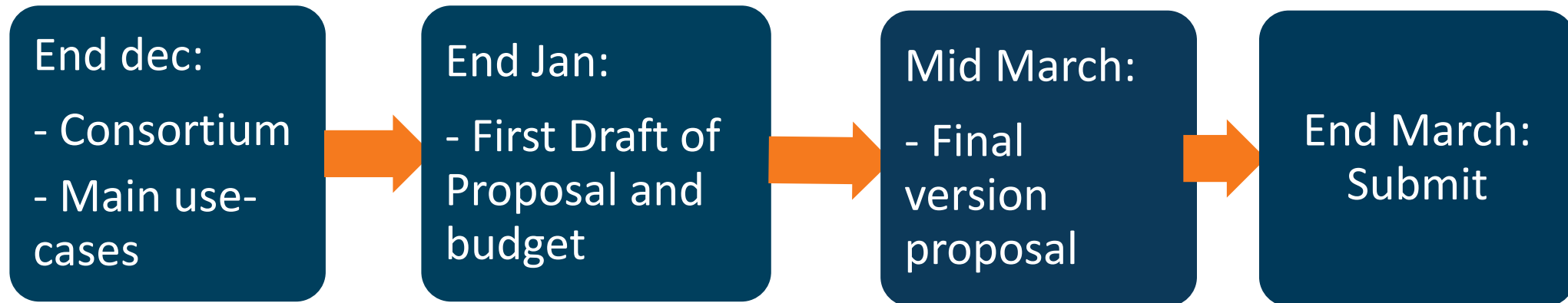
- (Some) AAI innovation with user communities can happen in AARC2 (TRL6 as starting point)
- More user-communities should be in AARC2
- There should be specific pilots to support user-community use-cases and/or to integrate AARC results into existing e-Infrastructures

Partners and Budget

- Budget = 3 M Euro
- Partners = currently 20 (2 of which unfunded)
 - No more unfunded partners, they will become MoUs
 - No more than 25 partners
 - New partners should be research communities
- GEANT Ams to remain the leading partner
- Plans are to maintain the same activity leaders

Structure of AARC2

- NA1: Management
- NA2: Training and Outreach
 - To deliver training on AARC1 final results
 - To deliver training for user-communities
- NA3: Policy and Best Practice harmonisation
 - To work on reference policy templates
 - To define policies for IdPs-SPs proxies
 - To define policies for attribute providers
- JRA1: Integrated architectures for e-Infrastructure AAI
 - To address the integration and interoperability (based on the AARC pilots) of the e-Infrastructure AAI, including the integration with international e-Infrastructures
 - To look at SP Architectures and Authorisation in multi-SP environments
 - To research the integration of non R&E identities into existing federations
- SA1
 - To pilot the integration of the blueprint architecture into existing AAI
 - To support specific community use-cases



Thank you

Any Questions?

skanct@admin.grnet.gr



<http://aarc-project.eu/>

