Authentication and Authorisation for Research and Collaboration

WP JRA1: Architectures for an integrated and interoperable AAI

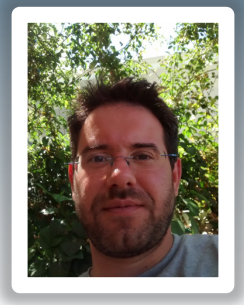
Christos Kanellopoulos

Agenda

- Structure and administrative matters
- Objectives
- Task Achievements
- JRA1 in AARC2

Activity Structure

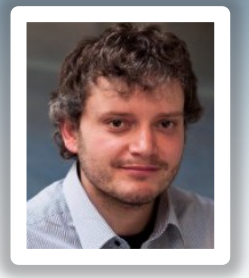
Activity Lead



Christos Kanellopoulos

T1

Requirements Analysis



Peter Solagna
EGI

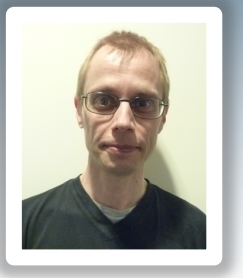
T2

Blueprint Architectures

Marcus Hardt
KIT

T3

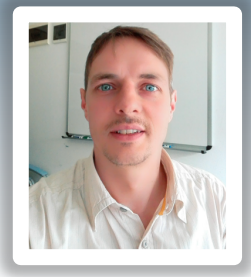
Models for supporting guest Identities



Jens Jensen
STFC

T4

Models for implementing APs and TTS



Davide Vaghetti
GARR

Partners

grnet Networking Research and Education

Consortium GARR

Karlsruhe Institute of Technology

Science & Technology Facilities Council

JÜLICH FORSCHUNGSZENTRUM

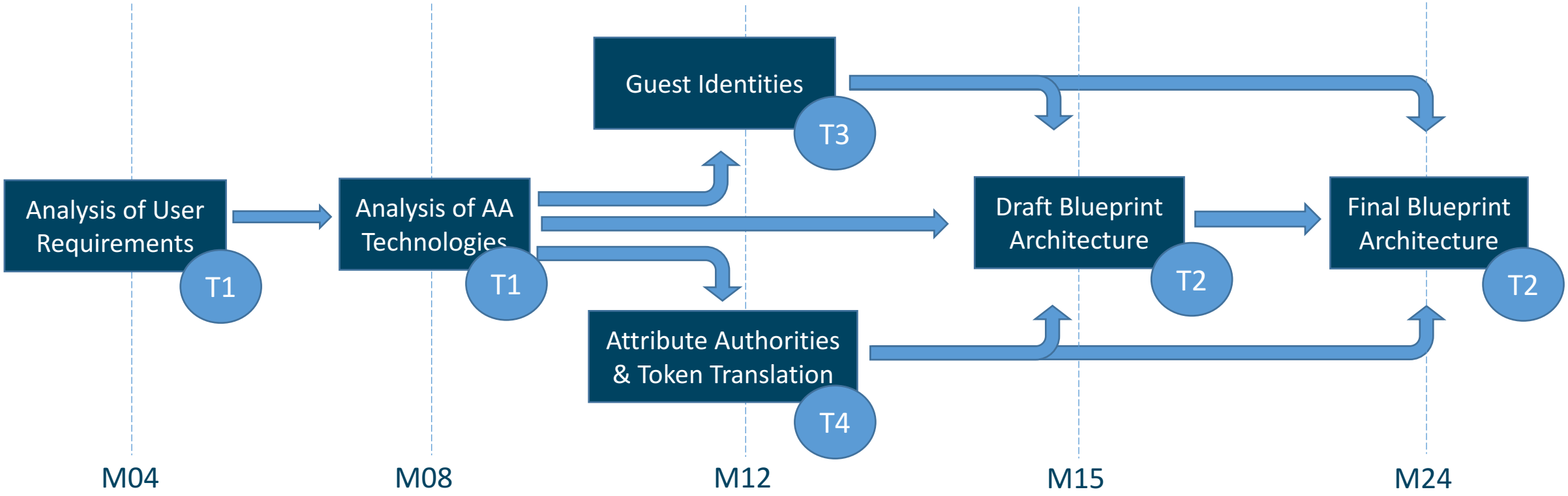
DAASI International

CSC

SURF NET

CESNET

Activity Structure



Resources (1 May 2016 – 30 April 2017) and deliveries

Total Year 2 effort	***75 PM for 2 years: Y2 (upd) forecast: 40.2 PM*** *(????? FTE)*	***???? PM used*** ***???% of resources in flat distribution***

1 of 1 deliverables delivered in PY2

DJRA1.2 – Blueprint Architectures ✓

Other key documents and results

- Recommendations on expressing Group Membership and role information ✓
- Guidelines on attribute aggregation ✓
- Guidelines on token translation services ✓
- Best practices for managing authorization ✓
- Guidelines on non web-access ✓
- Recommendations on implementing SAML authentication proxies for social IdPs ✓
- Recommendations on credential delegation ✓
- Account linking uses cases and LoA elevation ✓

High-level objectives (1/2)

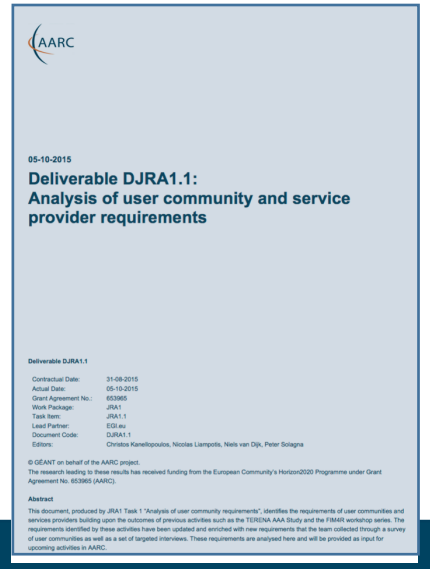
- Analyse how much has been developed to leverage federated access with other authentication systems used in the R&E communities, in the eGov space and in the commercial sector;
- Research a possible solution to link identities in the contest of higher levels of assurance, attribute providers and guest identities;
- Assess existing technologies to provide SSO for non-Web applications (cloud, storage and so on) and offer recommendations for their usage;
- Develop a risk-based model for existing AAI solutions;

High-level objectives (2/2)

- ***Propose models for supporting guest identities*** (NRENs' in-house solutions vs commercially-offered solutions should be explored);
- ***Define a blueprint architecture to enable web and non-web SSO capabilities across different infrastructures, integrating attribute providers/group management tools operated by user-communities;***
- ***Provide models for federated authorisation: how to integrate attributes and permissions from diverse communities, making them available at the federation level in a consistent and secure way.***

Feedback from PY1 Review

- **Comments on eID**
  - Interop issues with EU eGov and activities outside of EU (Brazil, Korea)
  - Articulate a clear goal for eGov IDs in the context of AARC (service provider oriented)
- **Consent and how we handle it in the AARC Architecture**
  - Look at the ANCHOR project
- **Authorization**
  - AuthZ is missing from this version of the Blueprint Architecture
  - Develop a plan for defining a blueprint architecture for authZ after AARC


AARC

05-10-2015

Deliverable DJRA1.1:
Analysis of user community and service provider requirements

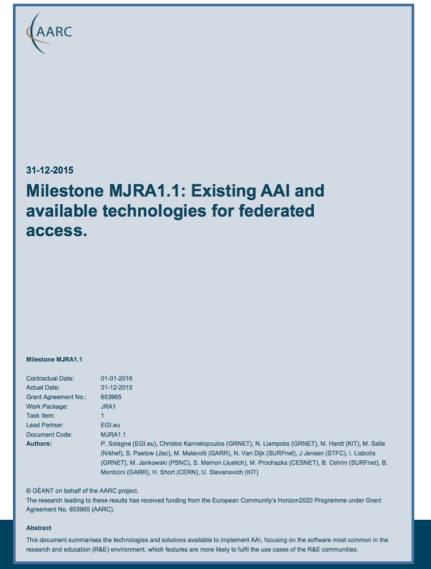
Deliverable DJRA1.1

Contractual Date:	31-08-2015
Actual Date:	05-10-2015
Grant Agreement No.:	653965
Work Package:	JRA1
Task Item:	JRA1.1
Lead Partner:	EGI.eu
Document Code:	DJRA1.1
Editors:	Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and services providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FIM4R workshop series. The requirements identified by these activities have been updated and enriched with new requirements that the team collected through a survey of user communities as well as a set of targeted interviews. These requirements are analysed here and will be provided as input for upcoming activities in AARC.


AARC

31-12-2015

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

Milestone MJRA1.1

Contractual Date:	01-01-2016
Actual Date:	31-12-2015
Grant Agreement No.:	653965
Work Package:	JRA1
Task Item:	1
Lead Partner:	EGI.eu
Document Code:	MJRA1.1
Authors:	P. Solagna (EGI.eu), Christos Kannelopoulos (GRNET), N. Liampotis (GRNET), M. Hardt (KIT), M. Salle (Nikhef), S. Paetow (Jisc), M. Malavolti (GARR), N. Van Dijk (SURFnet), J Jensen (STFC), I. Liabotis (GRNET), M. Jankowski (PSNC), S. Memon (Juelich), M. Prochazka (CESNET), B. Ozirmi (SURFnet), B. Monticini (GARR), H. Short (CERN), U. Stevanovich (KIT)

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document summarises the technologies and solutions available to implement AAI, focusing on the software most common in the research and education (R&E) environment, which features are more likely to fulfil the use cases of the R&E communities.

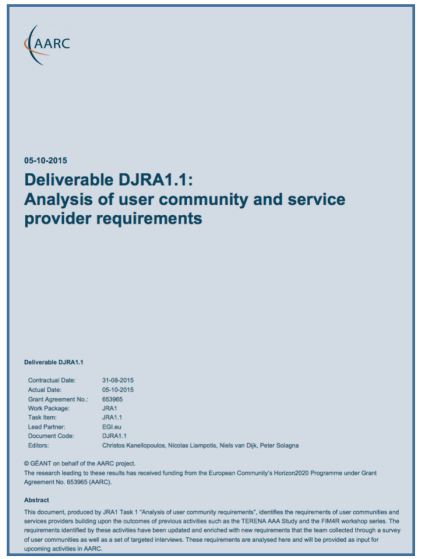
Achievements:
Task 1 | Requirements Analysis

Architectures for an integrated and interoperable AAI
Objectives for: Task 1 Requirements analysis

Objectives from Technical Annex	Community Requirements	AA technologies & Standards	Investigate interoperation activities and support for cross domain collaboration	AAI in R&E sector, Libraries and eGOV
Year 1 Results	Completed ✓	Completed ✓	Completed ✓	Completed ✓

✓ **KPI: Analyze at least 5 e-Infrastructures and VOs. (14)**

Achievements – Task JRA1.1 Requirements Analysis (1/2)


AARC

05-10-2015

Deliverable DJRA1.1:
Analysis of user community and service provider requirements

Deliverable DJRA1.1

Contractual Date:	31-08-2015
Actual Date:	05-10-2015
Grant Agreement No.:	653965
Work Package:	JRA1
Task Item:	JRA1.1
Lead Partner:	EGI.eu
Document Code:	DJRA1.1
Editors:	Christos Kanellopoulos, Nicolas Liampotis, Niels van Dijk, Peter Solagna

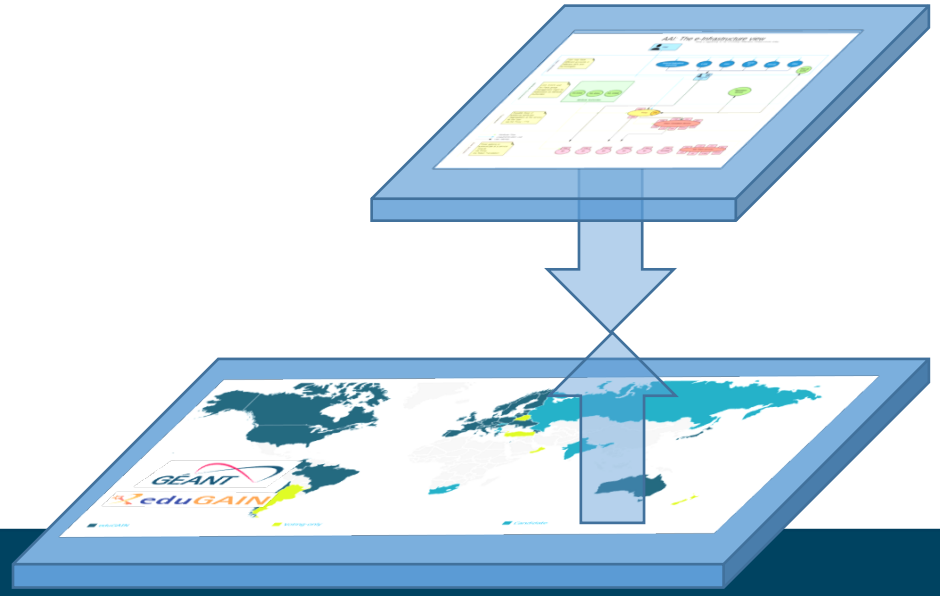
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

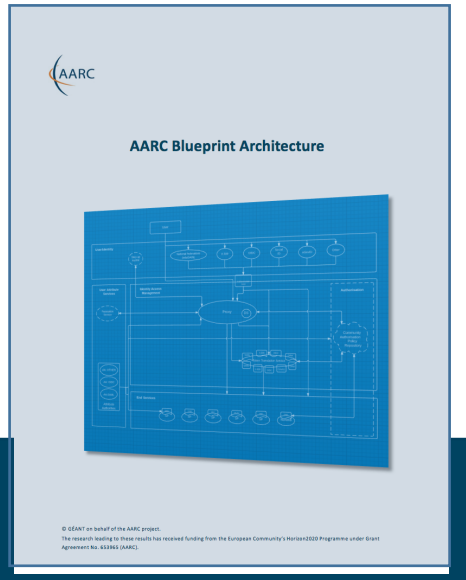
Abstract

This document, produced by JRA1 Task 1 "Analysis of user community requirements", identifies the requirements of user communities and services providers building upon the outcomes of previous activities such as the TERENA AAA Study and the FIM4R workshop series. The requirements identified by these activities have been updated and enriched with new requirements that the team collected through a survey of user communities as well as a set of targeted interviews. These requirements are analysed here and will be provided as input for upcoming activities in AARC.

Attribute Release	Attribute Aggregation	User Friendliness	SP Friendliness
Persistent Unique Id	Credential translation	Credential Delegation	User Managed Information
Levels of Assurance	Guest users	Step-up AuthN	Best Practices
Community based AuthZ	Non-web-browser	Social & e-Gov IDs	Incident Response

Architectures for an integrated and interoperable AAI

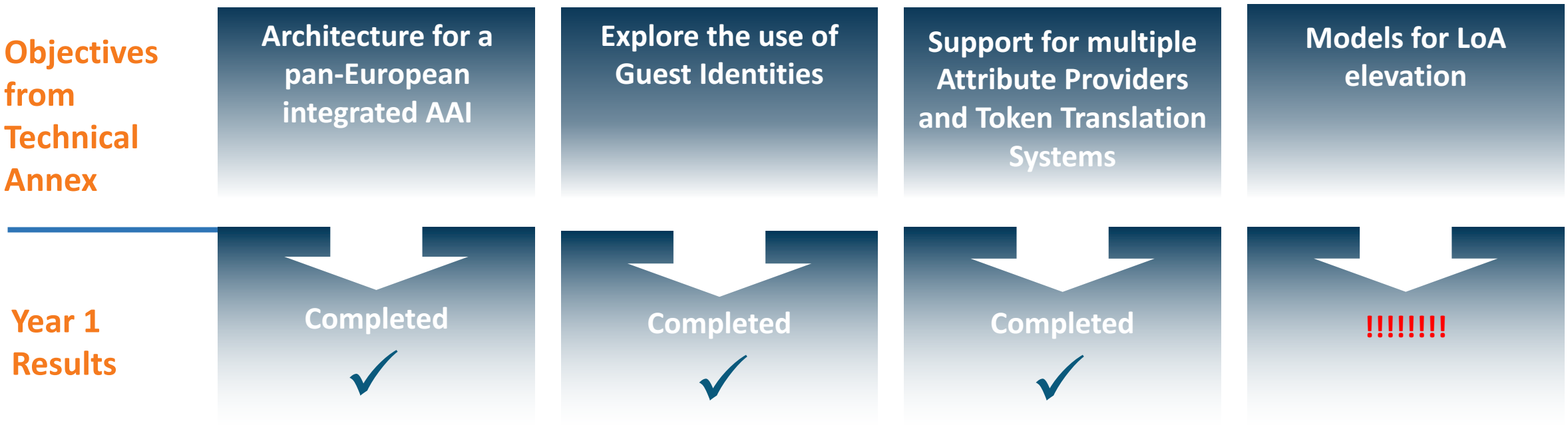




Achievements:

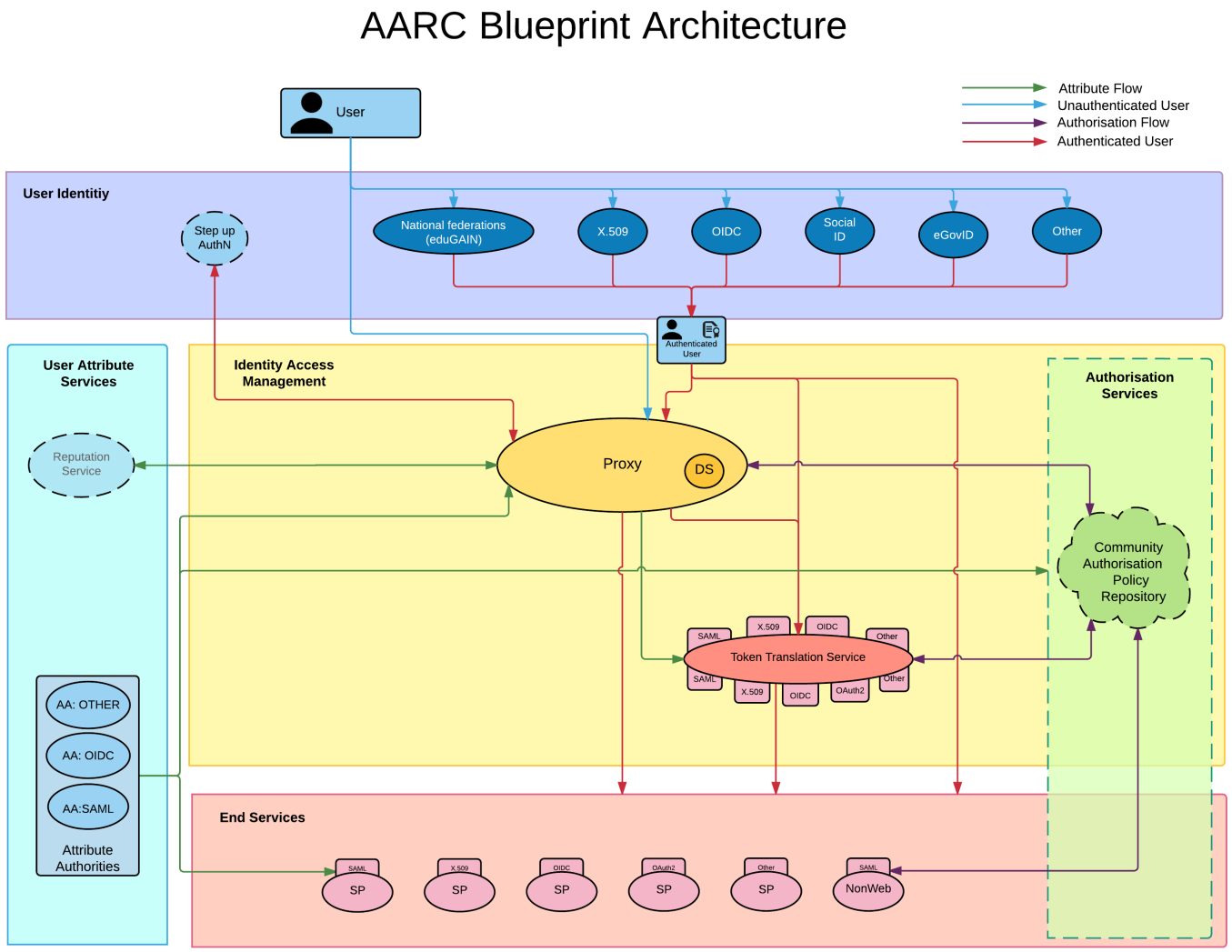
Task 2 | Blueprint Architectures

Architectures for an integrated and interoperable AAI
Objectives for: Task 2 Blueprint Architectures



KPI: Deliver at least 3 iterations of the Blueprint Architecture (5)

Achievements - Task JRA1.2 Blueprint Architectures



3rd iteration (June 2016)

- TNC2016 (Prague – June 2016)
- MJRA1.4 1st Draft version of the Blueprint Architecture

4th iteration (November 2016)

- AARC All-Hands Meeting (CERN – November 2017)
- AARC Infoshare on the Blueprint Architecture (January 2017)
- FIM4R Workshop (Vienna – February 2017)

5th iteration (March 2017)

- 5th AARC General Meeting (Athens – March 2017)
- Internet2 Global Summit (Washington D.C. – April 2017)

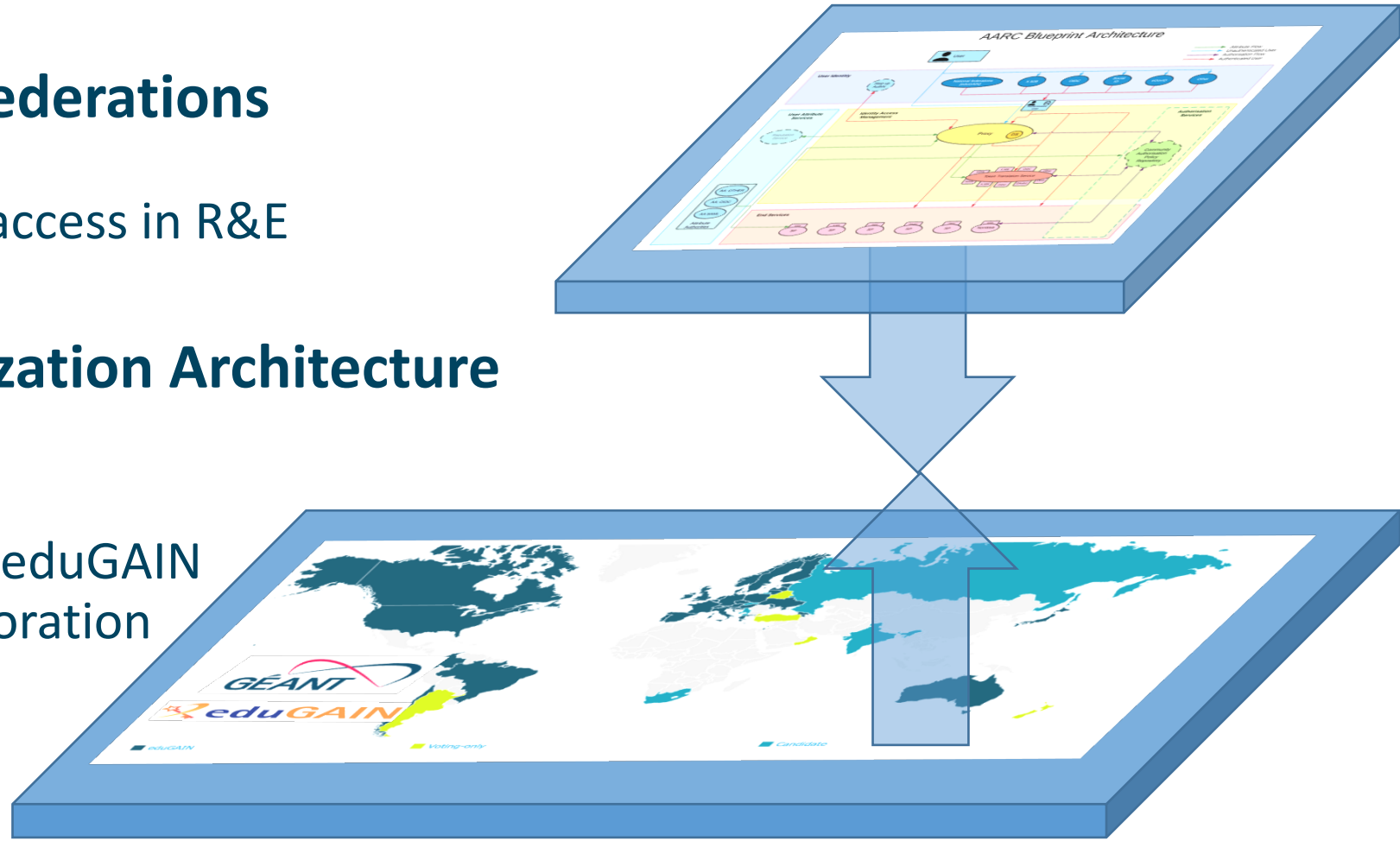
Blueprint Architecture

eduGAIN and the Identity Federations

A solid foundation for federated access in R&E

Authentication and Authorization Architecture for Research Collaboration

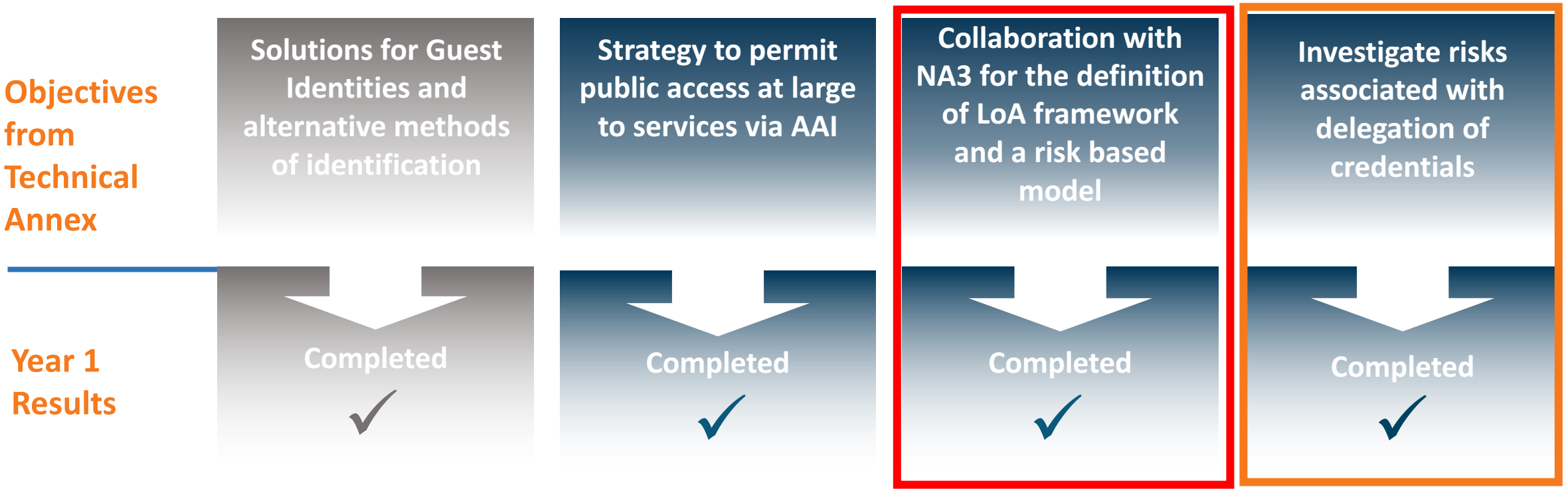
A set of building blocks on top of eduGAIN for International Research Collaboration



Milestone MJRA1.2:
Design for Deploying Solutions for "Guest Identities"

Achievements:
Task 3 | Models for supporting Guest Identities

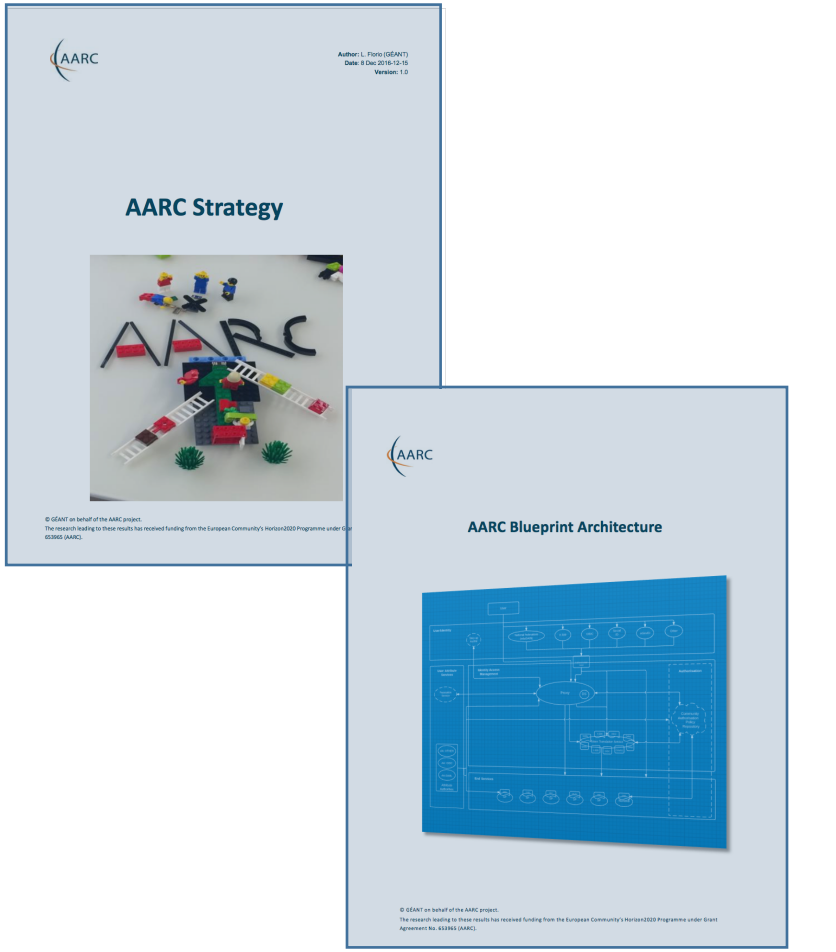
Architectures for an integrated and interoperable AAI
Objectives for: Task 3 Models for supporting Guest Identities

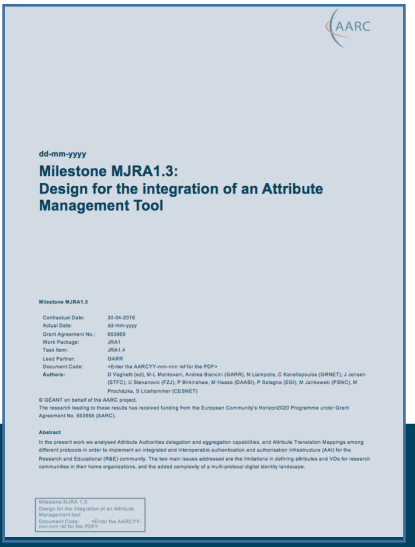


KPIs: Document, test and compare external (non-federated IdPs) of 5 communities and 3 social media (6/4)

Achievements – Task JRA1.3 Models for supporting Guest Identities

- **AARC Strategy for enabling public access at large**
  - In collaboration with all AARC WPs
  - https://goo.gl/7kL338
- **Recommendations on the use of Guest Identities**
  - Available in AARC-BPA-2017
- **Recommendations on credential delegation (!)**
  - https://goo.gl/i5SZtP
- **eIDAS and eGOV IDs in the context of AARC (?)**





Achievements:

Task 4 | Models for implementing attribute providers and token translation services

Architectures for an integrated and interoperable AAI
Objectives for: Task 4 Models for implementing attribute providers and token translation services

	Models for implementing Attribute Providers & Guidelines for Attribute Release	Integration of Community based Attribute Providers & Guidelines for expressing group membership	Technologies for Token Translation Services and credential delegation	Best practices for managing authorization
Objectives from Technical Annex				
Year 2 Results	Completed ✓	Completed ✓	Completed ✓	Completed ✓

✓ **KPIs: Deliver at least 3 models for implementing attribute providers (3)**
Document, test and assess at least 3 delegation schemes /technologies (5)

** MJRA1.3 was delivered in June, technically in PY2*

Achievements – Task JRA1.4 Models for implementing attribute providers and token translation services

Recommendations & Best Practices

- Expressing group membership and role information
- Attribute aggregation
- Token Translation Service
- Managing authorisation
- Credential Delegation – **Ongoing**
- Non-browser access
- Account linking use cases & LoA elevation **– Ongoing**
- SAML authentication proxies for social IDs **– Ongoing**

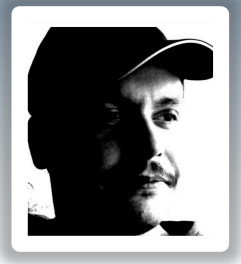
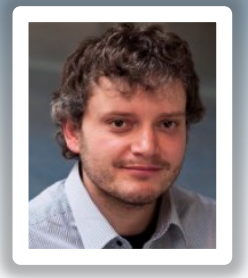
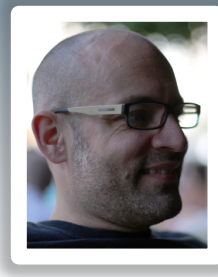
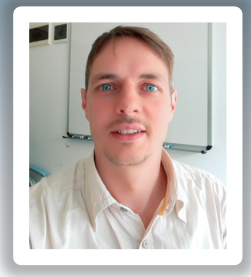
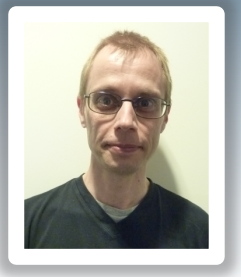
JRA1 in AARC2

- Work with existing e-infrastructures and ESFRI projects to deploy and enhance (JRA1) the integrated AAI
  - focus on the integration aspects of the blueprint architecture that will be delivered by the AARC project;
  - provide recommendations and guidelines for implementers, service providers and infrastructure operators on implementing scalable and interoperable AAIs across e-infrastructures and scientific communities

- Expansion of the blueprint of the integrated AAI to explore authorisation and delegation aspects in such a complex environment as well as the support for alternatives to SAML.
- Expand support for new technologies and policies (JRA1 and NA3).
  - Follow a user-driven approach: development driven by use-cases and continuous community feedback on AARC2 work

- Work in close collaboration with NA3, SA1, the Competence Centre and the training and outreach activities of AARC2.

JRA1 in AARC2

Activity Lead	T1	T2	T3	T4
	Tools and Services for Interoperable Infrastructures	Service Provider Architectures and Authorization in multi-SP Environments	Models for the Evolutions of AAIs for Research Collaboration	Scalable VO Platforms
				
Nicolas Liampotis GRNET	**Peter Solagna** EGI	**Marcus Hardt** KIT	**Davide Vaghetti** GARR	**Jens Jensen** STFC

Partners

Thank you

Any Questions?

http://aarc-project.eu/

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