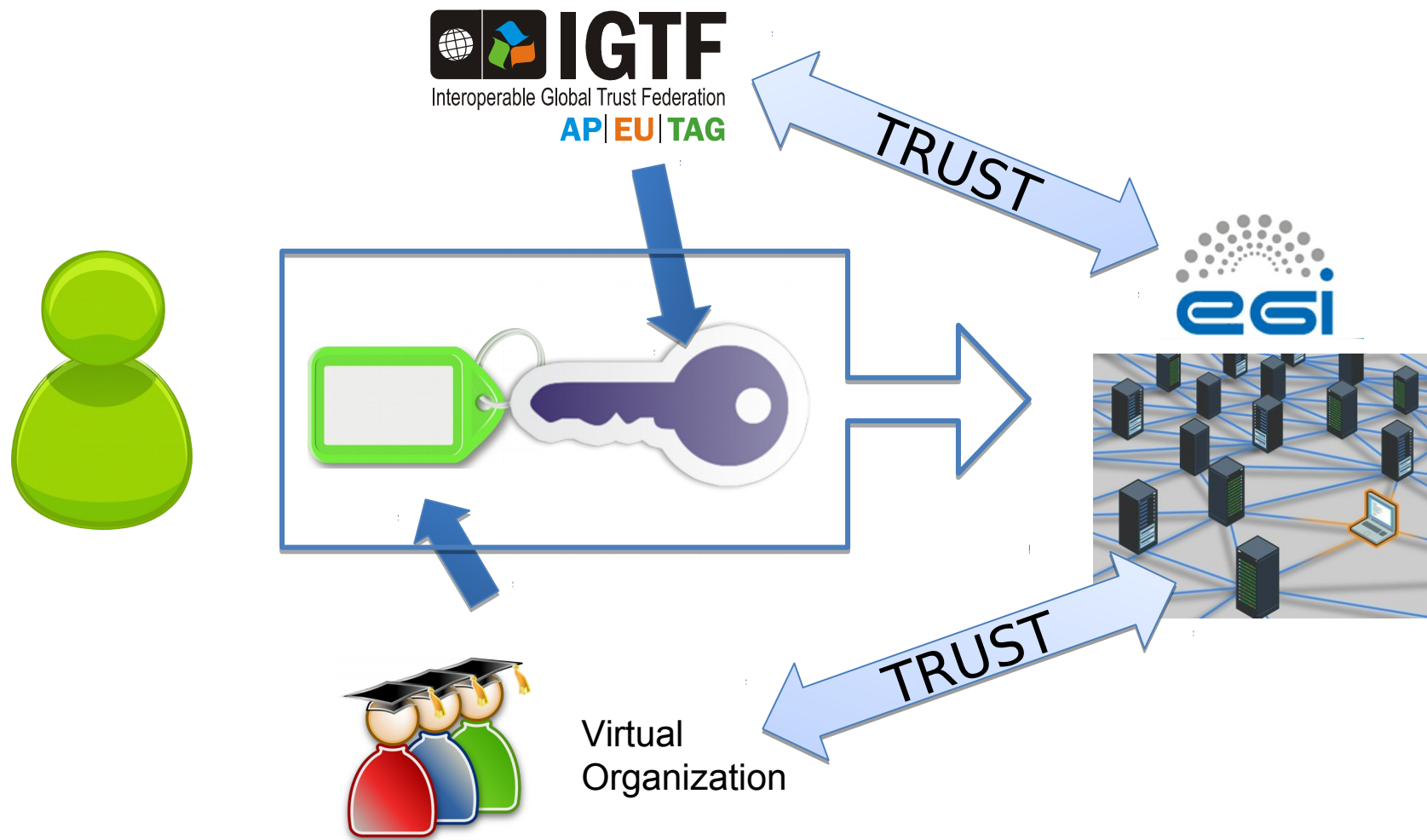# AAI in EGI
Status and Evolution

Peter Solagna

Senior Operations Manager

peter.solagna@egi.eu

Disclaimer: the content of this presentation has not been yet endorsed by any EGI body.

e-infrastructure

www.egi.eu

TRUST

TRUST

Virtual
Organization

The key is: collaboration

- Authentication and Authorization workflows scale with the number of service providers and users
  - User identity is verified by the IGTF Certification Authorities who release the X509 certificates
  - The certificate enable **uniform authentication** of the user across resource centres

- User communities have the tools to manage the membership of their users and their structure
  - Collaborate to the trust chain and to integrate the information provided by the Identity Providers
  - Authorization is based on the Virtual Organization membership and attributes not on the single user identity
  - The user capabilities based on groups and roles within the VO are reflected into **uniform access rights** across the sites that support the VO

Extend the AuthN mechanism

- For some users approaching EGI the X509 mechanism is a barrier
  - They do not have easy access to a Certification Authority
  - They would prefer to continue using their institutional credentials
  - VOs and Resource Providers implement portals to ease the access to the resources

- The most effective solution is to bridge other identity federations (eduGAIN, institutional IdP) with the EGI AAI
  - Technical bridge: credentials translation, support in the middleware for other AuthN protocols
  - Policy bridge: build trust between SP and IdP, enable different level of trust

Extend federated AuthZ

- Provide tools to the users to manage their user communities
  - Distributed Attribute Authorities connected with the user's IdPs
  - Can be used also within application-specific environments for user authorization

- Maintain uniform authorization across multiple service providers
  - Based on the attributes provided by the user communities

- Apply the collaborative trust approach of EGI to new authentication technologies

AARC project
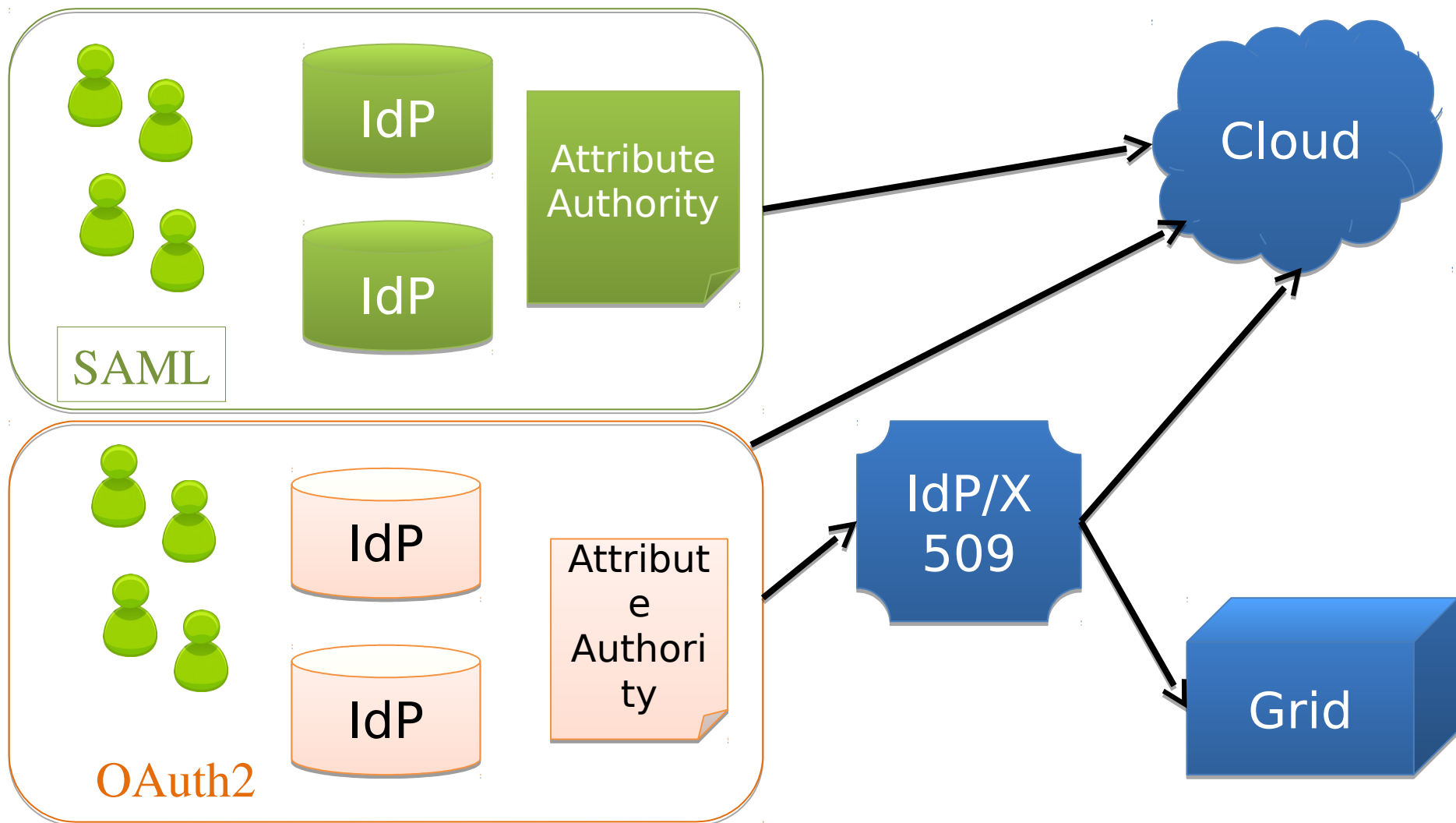
- IdP and E-infrastructures must collaborate the process of evolving AAI
- Collaboration supported by an H2020 EINFRA-7 action

Ultimate goal:

- Enable SSO for users who has access to multiple infrastructures
  - Enable a European Authentication and Authorization Infrastructure that can be used by multiple resource federations and application specific frameworks

AARC Objectives

- Increase the coverage of the European identity federations
  - Training dissemination
- Achieve interoperability among AAI infrastructures
  - Technical architecture
  - Policy framework
- Test SSO capabilities among service providers
  - Analyze users requirements
  - Deploy pilots in inter-einfrastructures test-beds