AAI in EGI
Current status

Peter Solagna – EGI.eu

Operations Manager

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

User authentication in a federated environment

- Local environment (e.g. one institution, one cluster)
  - Users have local accounts, validated often in a F2F verification with the system administrator
  - All the needed information are filled in at the moment of the registration
- Federated environment (e.g. distributed infrastructure)
  - Users do not have local accounts on every service/cluster/ centre
  - Users own credentials that are recognized by all the service providers in the federation
  - Identity providers and service providers must agree on the:
    - Information provided to the SP
    - Level of assurance of the credentials
    - Operations of the IdP

User's identity

- A user must be able to authenticate with the same identity on the distributed services
- From the user's point of view
  - Uniform authentication enable cross-site workflows
  - Use of distributed resources using the same credential
- From the service provider's point of view
  - Uniform authentication improves security operations in a federated environment
  - Easier management of users, and their access to resources

Delegation

- For some workflows and use cases, delegation is an important capability
  - Applications that in general need to: access data stored by the user and not publicly accessible or to save data in the user's storage area
  - Portals and scientific gateways do actions on behalf of the user, like job submission to compute resources.
- This is usually implemented by impersonating and delegating
  - Impersonation: the application/service acts as the user (using user's temporary credentials). Done at authentication level.
  - Delegation: the user enables the service to work on his/her behalf. Done at authorization level

Level of assurance

Not all the credentials are the same!

Examples:

- Very high level of assurance: eID
- High level of assurance with ID verification:
  - X509 certificates, many institutional IdP
- Social media credentials
  - Everyone with an email account can have one

- Not always the highest LoA is required: for some low-risk activities low assurance credentials are usable!
- The minimum LoA required is determined by the user community and the service provider requirements

Level of assurance: examples of use cases

- Strong authentication
  - Submit and manage virtual machines
  - Access sensitive protected data
- Medium authentication
  - Submit pre-defined applications through science gateways
  - Use PaaS on the cloud
- Low authentication
  - Access open data
  - Perform read-only operation on non-sensitive data

Authorization in a federated environment

- In a federated environment individual user authorization cannot be handled by the service provider
  - Service provider does not know the user and if him/her should be allowed to perform a specific action
- Rules for the authorization must use information associated with the user
  - Provided by the IdP
  - Provided by the research collaboration who grants users access to resources

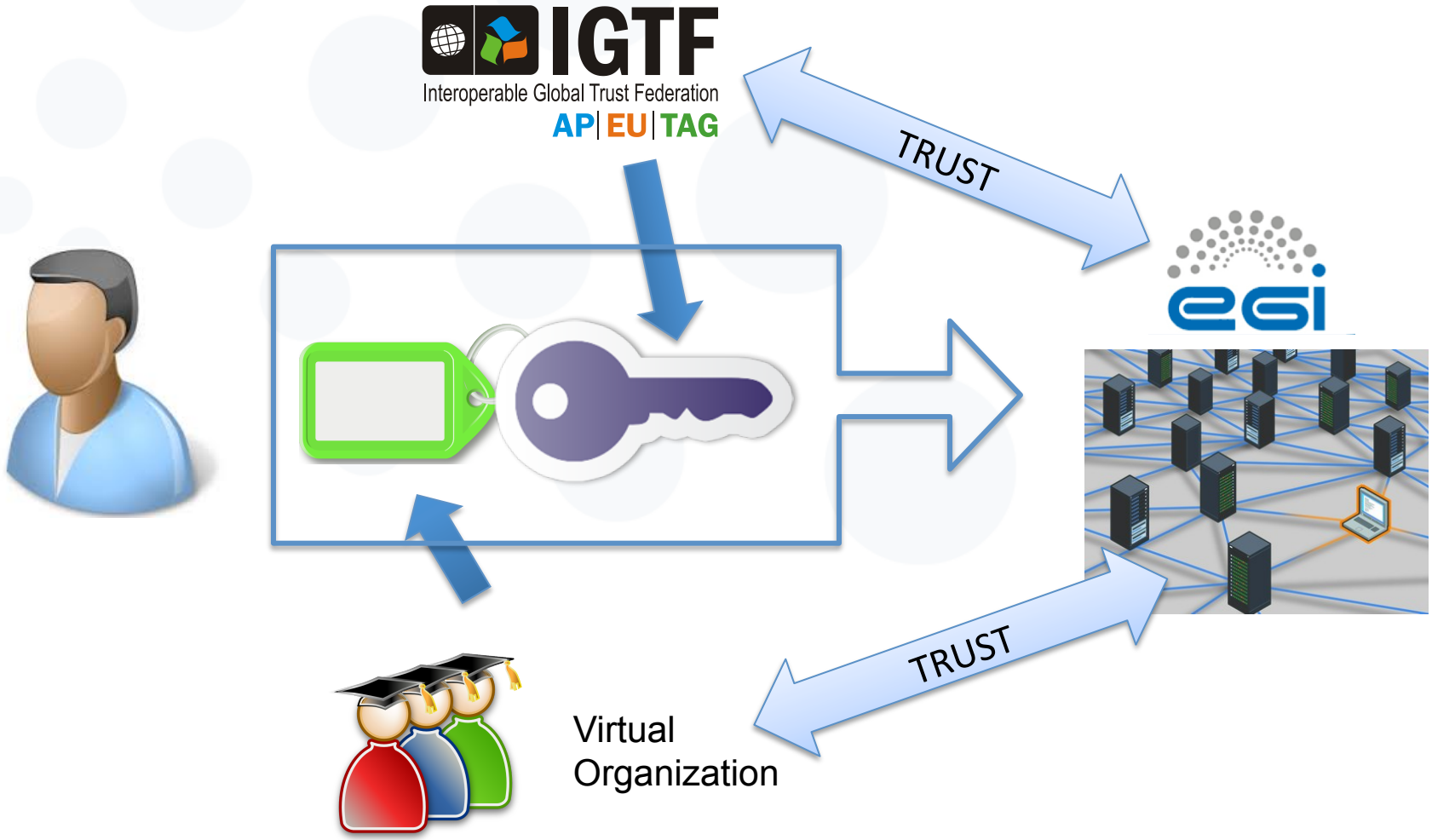
Distribute collaboration management in EGI: Virtual Organization

- Virtual Organization: *A group of researchers with common interests, requirements and applications, who need to work collaboratively and/or share resources.*
- Service providers enable users to access services and resources based on the VO membership and additional attributes such as roles within the VO and sub-groups of users within the VO
- The VO membership is managed by the VO Manager(s) who is the main contact with EGI and who knows the users and the groups in the collaboration
  - New users can be added and removed enabling/disabling their access rights, without direct intervention of service providers
  - VO Manager usually does not manage users credential, a VO is not an IdP

EGI user authentication: X509 certificates

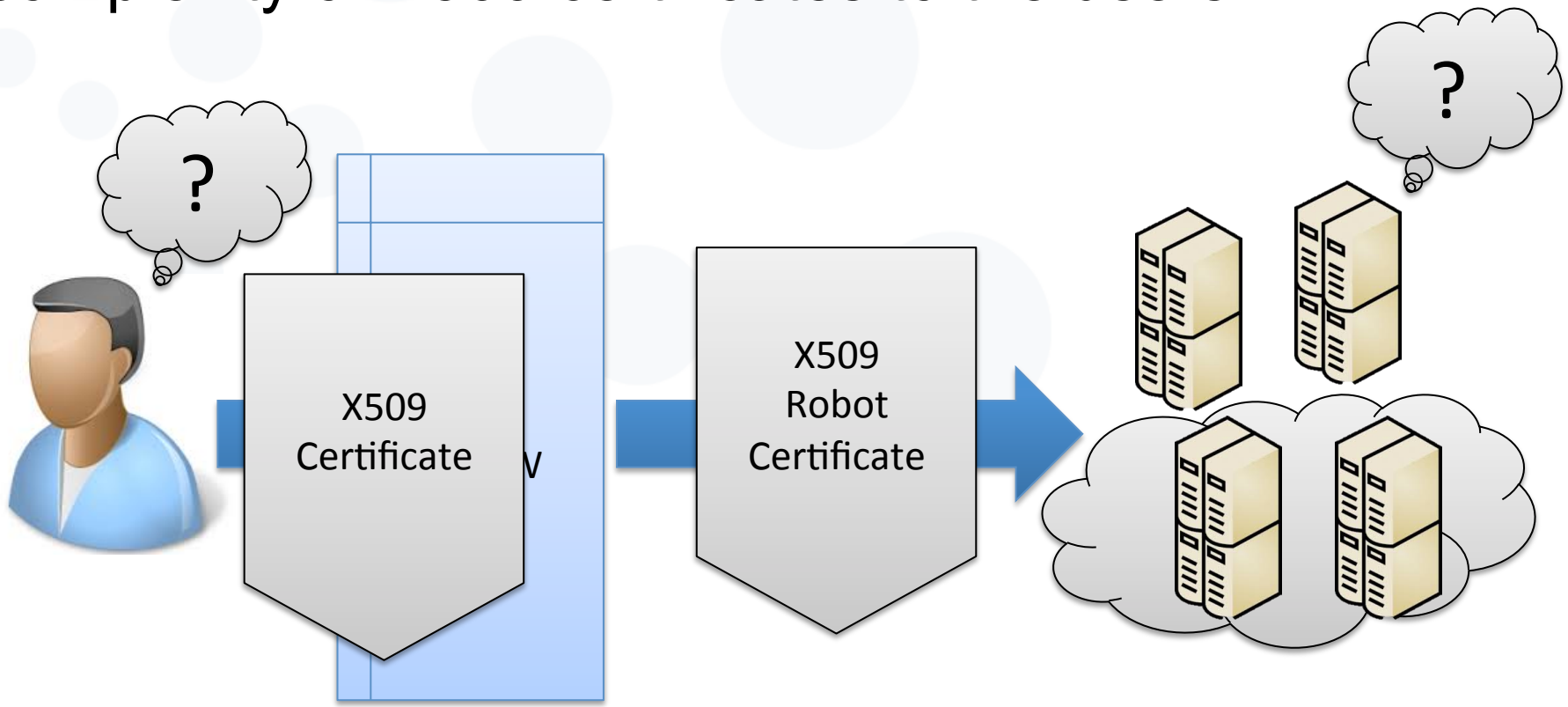
- X509 certificates are the main authentication technology used in EGI
  - Trust network of certification authorities (IGTF/ EUGridPMA)
  - EGI services are configured to accept certificates released by the Certification Authorities federated within IGTF
- You have one IGTF personal certificate → you can authenticate wherever in EGI

Authentication and Authorization workflow

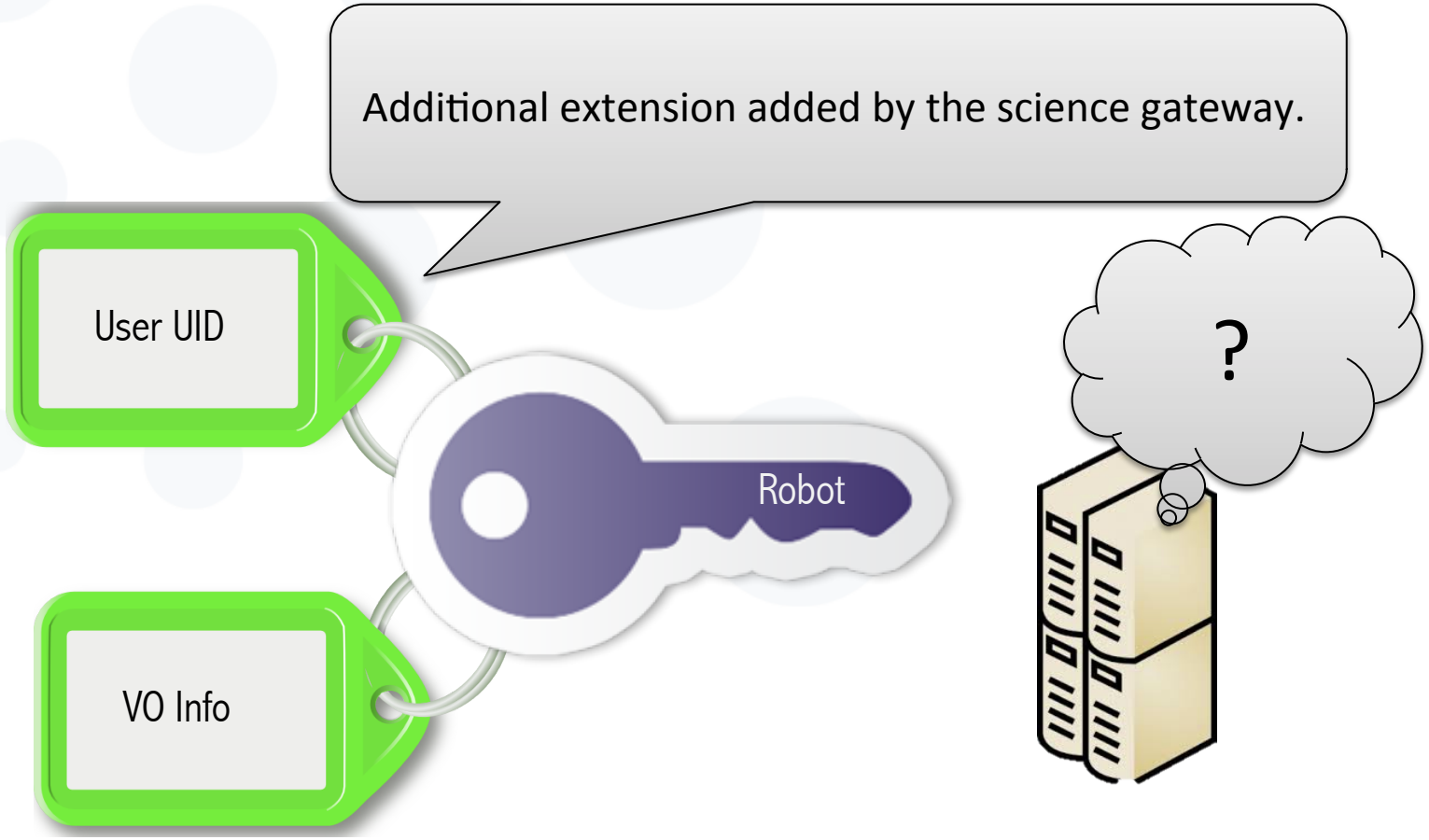


Robot certificates and science gateways

Portals and Scientific Gateways can hide the complexity of X509 certificates to the users



Improving the use of robot certificates



Extend the X509 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
- More in the next talk!

Summary: Current EGI Services for AAI

- EUGridPMA network of Certification Authorities operated by the NGIs
- All EGI services are configured to accept EUGridPMA certificates
  - Certificates enable: web authentication, command line authentication and delegation
- VOMS services to manage VO membership and attributes
- Science gateways to use other types of authentication (username/password) and robot certificates to access EGI services

Thank you for your attention.

Questions?

www.egi.eu