ESCAPE

European Science Cluster of Astronomy & Particle physics ESFRI research Infrastructures

AAI for WP4 CEVO

Sara Bertocco, Marco Molinaro, **Dave Morris**, André Schaaff

for the CEVO members

H2020 ESCAPE Progress Meeting 26 February 2020, Brussels

ESCAPE - The European Science Cluster of Astronomy & Particle Physics ESFRI Research Infrastructures has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement n° 824064.

WP4: C E Virtual Observatory

“**C**onnecting **E**SFRI projects to EOSC through **VO** framework”

- Integrating IVOA architecture into EOSC
  - Promoting the existing VO infrastructure
    - Metadata standards - vocabularies, units, data models
    - Technical standards - data formats, service protocols
    - High level standards - data discovery, data access

Funded by the European Union’s
Horizon 2020 - Grant N° 824064

WP4: C E <u>V</u>irtual <u>O</u>bservatory

“<u>C</u>onnecting <u>E</u>SFRI projects to EOSC through <u>VO</u> framework”

- Integrating IVOA architecture into EOSC
  - Updating and improving the VO infrastructure
    - Some ESFRIs are in areas well represented by the VO
    - Some ESFRIs are in areas new to the VO.
    - New requirements, new workflows, new data structures
    - Common challenges
      - cloud compute data storage, data transfer etc
      - authentication, authorization, identity

Funded by the European Union’s
Horizon 2020 - Grant N° 824064

WP4: C E Virtual Observatory

“Connecting ESFRI projects to EOSC through VO framework”

- The VO is built on IVOA standards
- The ‘I’ in IVOA stands for International
- This implies
  - EU and non-EU users: a requirement for AAI to allow/consider this
  - The VO is a distributed interoperable archive, works on machine actionability

    actionable

    - *adjective*, … information that allows a decision to be made or action to be taken

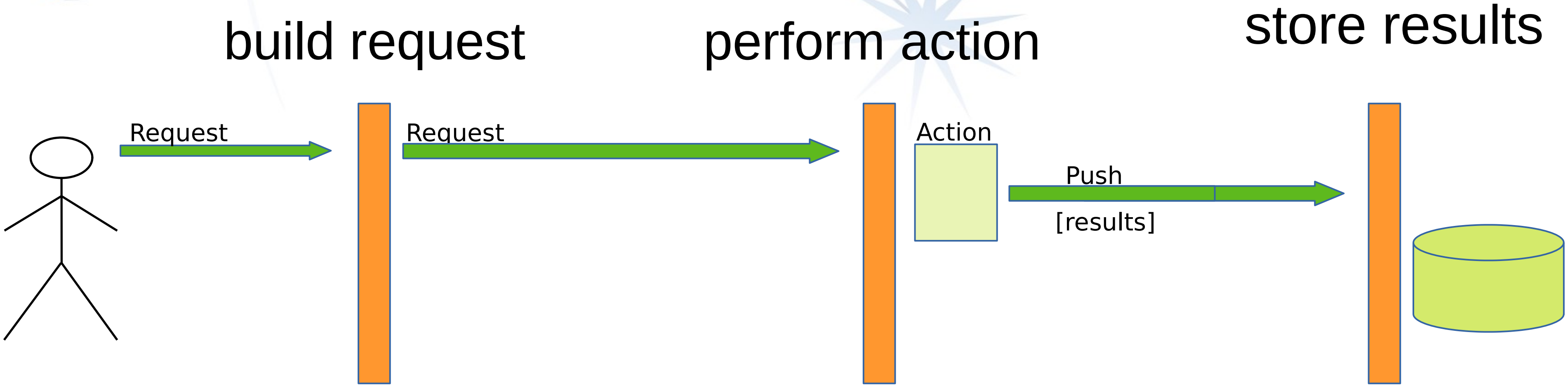
  - Machine readable metadata is a requirement
  - Credential delegation is a requirement

Who I am, what groups do I belong to.

Users want it to *“just work”*

Funded by the European Union’s
Horizon 2020 - Grant N° 824064

Challenge .. storing results

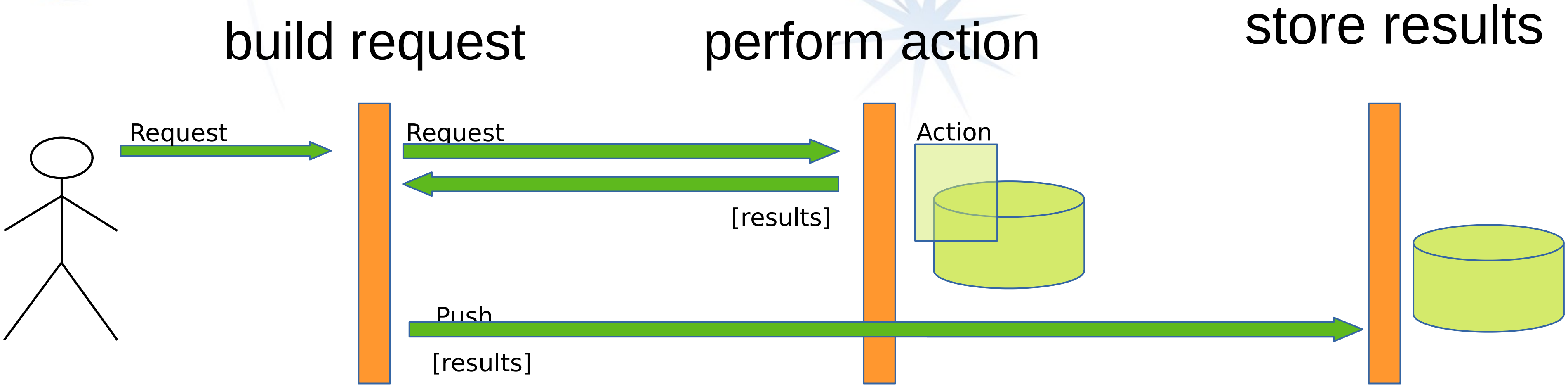


Problems to solve

- How control access to the service ?
- How control access to the storage ?
- How control access to the computation resources ?

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Solution - send data back to portal ?

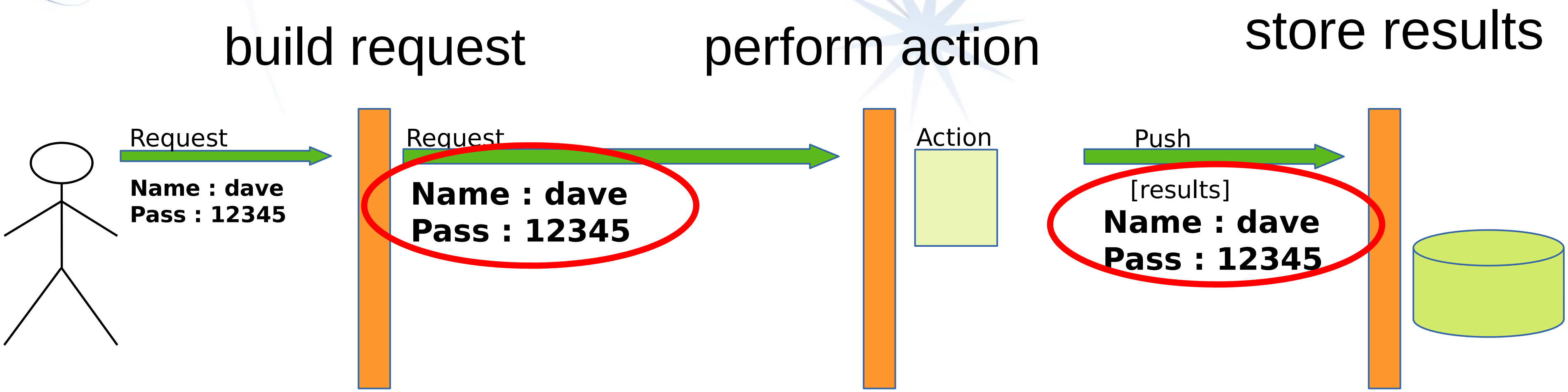


Problem

- All data transfers go via the portal.

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Always send name/password

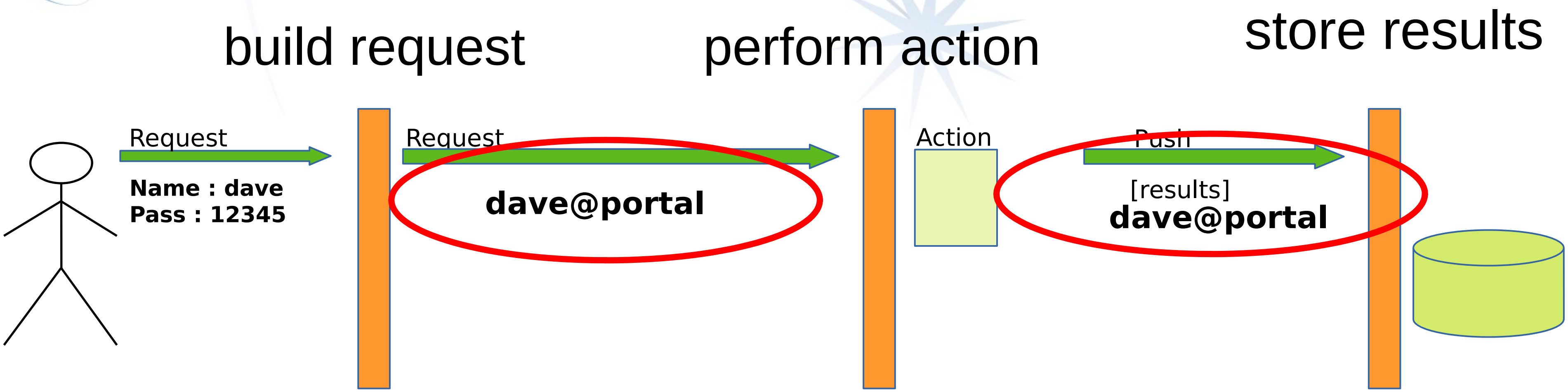


Problem

- Every component gets our password

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Trust the request

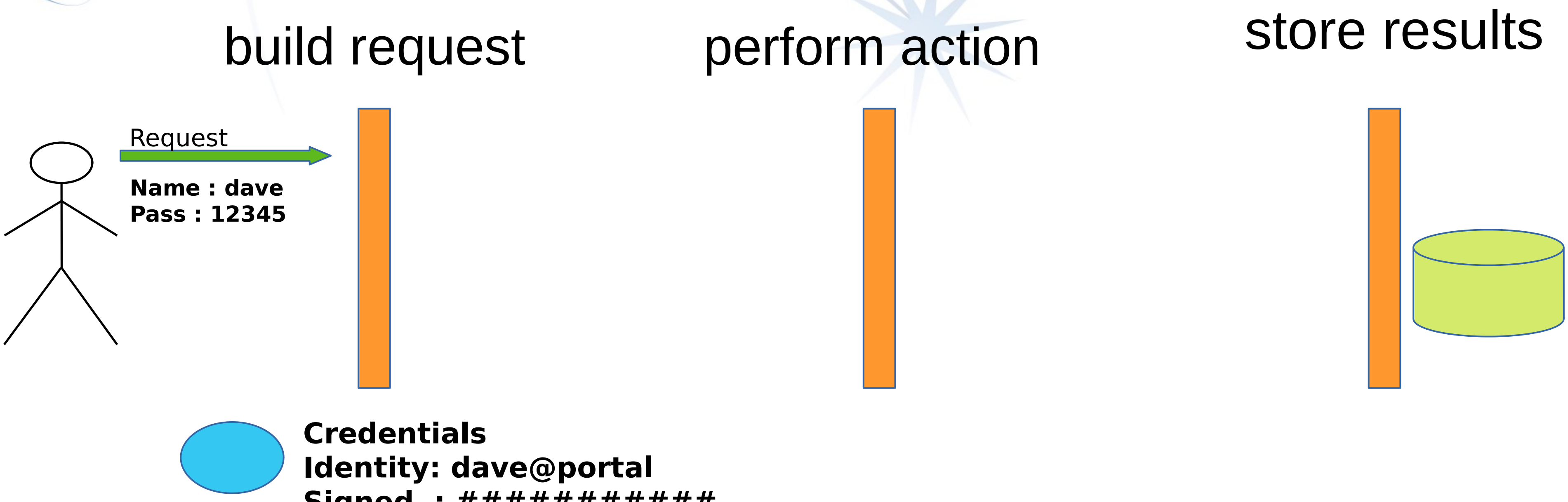


Problem

- Storage system has to trust all the requests.
- A client might be user code in a notebook.

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Signed credentials

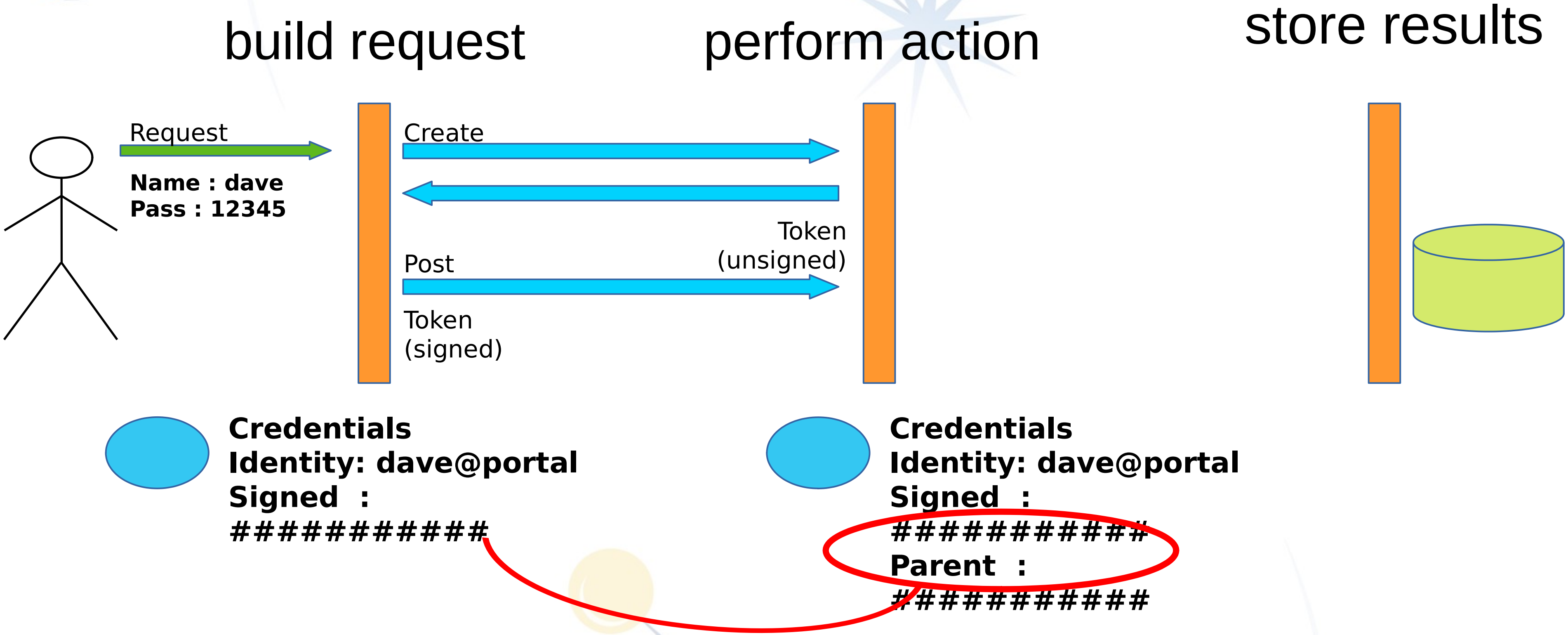


Credentials
Identity: dave@portal
Signed : ###########

Signed token (e.g. x509)

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Delegated signed credentials



Credentials
Identity: dave@portal
Signed : ###########

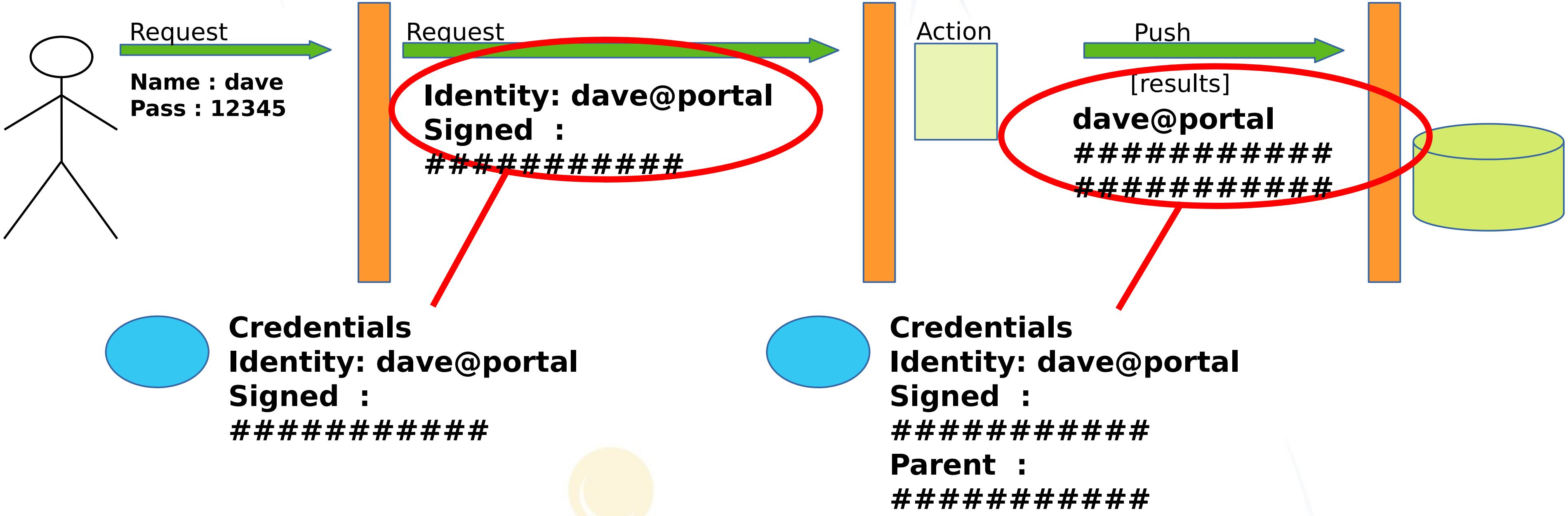
Credentials
Identity: dave@portal
Signed : ###########
Parent : ###########

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Delegated signed credentials

build request

perform action



Request

Name : dave
Pass : 12345

Request

Identity: dave@portal
Signed :
###########

Action

Push

[results]
dave@portal
###########
###########

Credentials
Identity: dave@portal
Signed :
###########

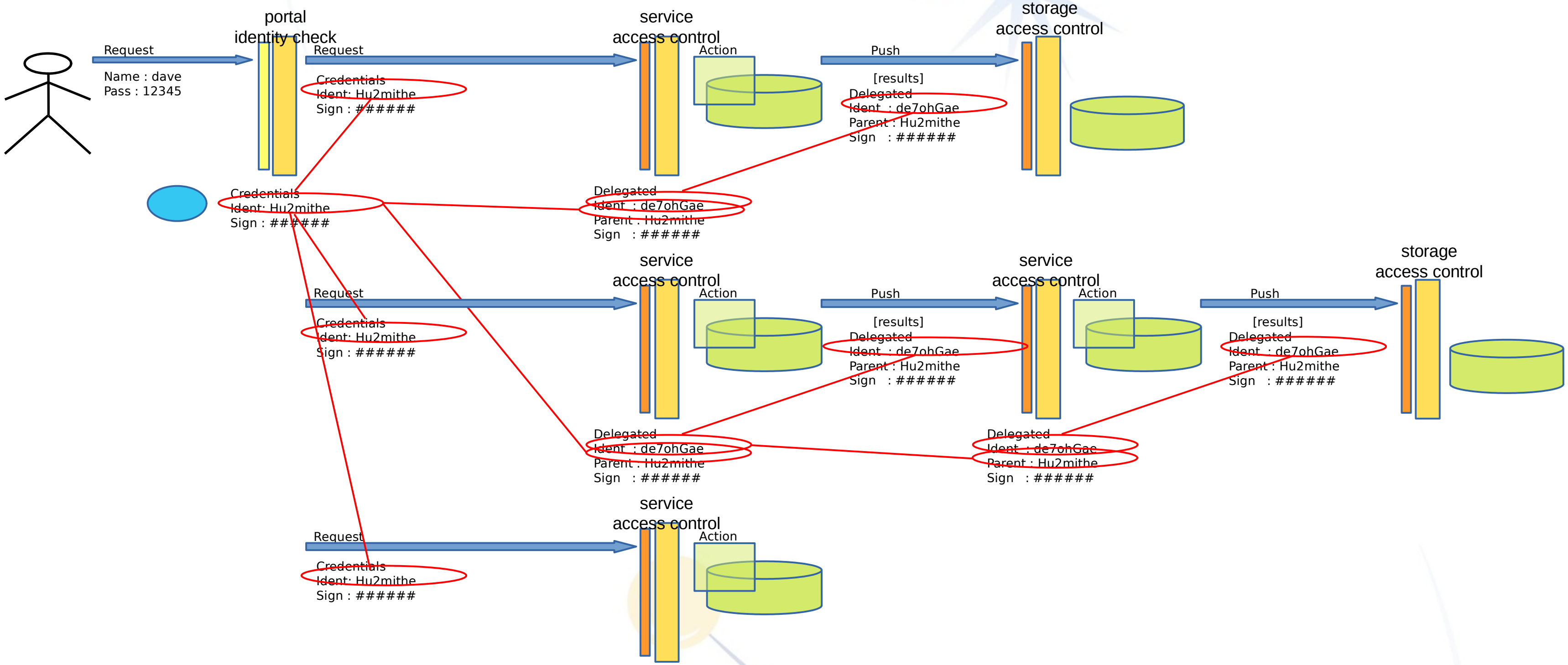
Credentials
Identity: dave@portal
Signed :
###########
Parent :
###########

Services authorised to act on our behalf

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Delegated credentials

Complex workflows



Funded by the European Union's
Horizon 2020 - Grant N° 824064

Existing IVOA efforts

- SSO profile
  - Link to spec: http://www.ivoa.net/Documents/SSO/index.html
- GMS authorization interfaces
  - Link to draft: http://www.ivoa.net/Documents/GMS/index.html
- CDP and evolution
  - Link to draft: http://www.ivoa.net/Documents/CredentialDelegation/

    Version 1.0, 18 February 2010 -> X.509 already there
  - Token usage, including IETF OAuth 2.0 Token Exchange draft specification

    https://tools.ietf.org/html/draft-ietf-oauth-token-exchange-19
- Detailed service metadata to enable secure connections
  - ...ongoing work at IVOA on <securityMethod>

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Thank you for your attention!

Funded by the European Union's
Horizon 2020 - Grant N° 824064