Authentication and Authorisation for Research and Collaboration

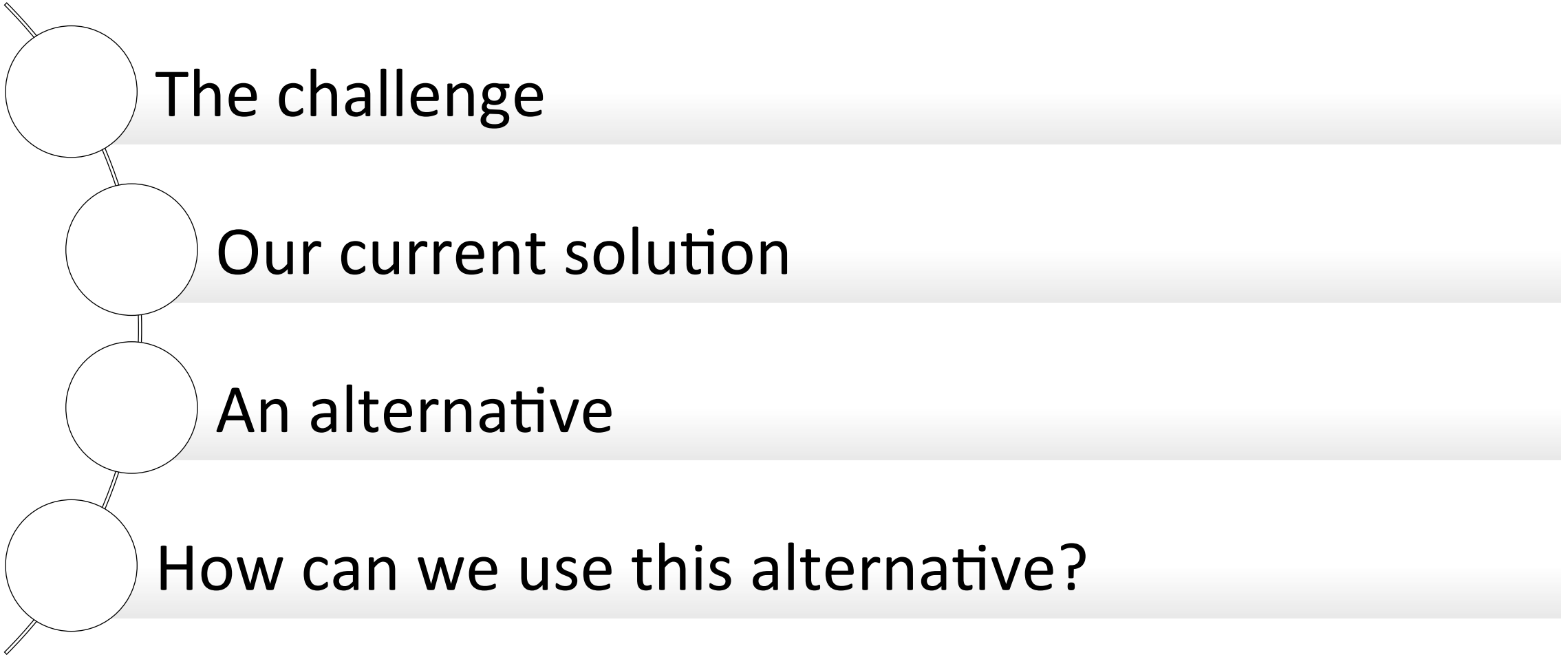
Enabling Federated Access for HEP

Authentication and Authorisation for Research and Collaboration

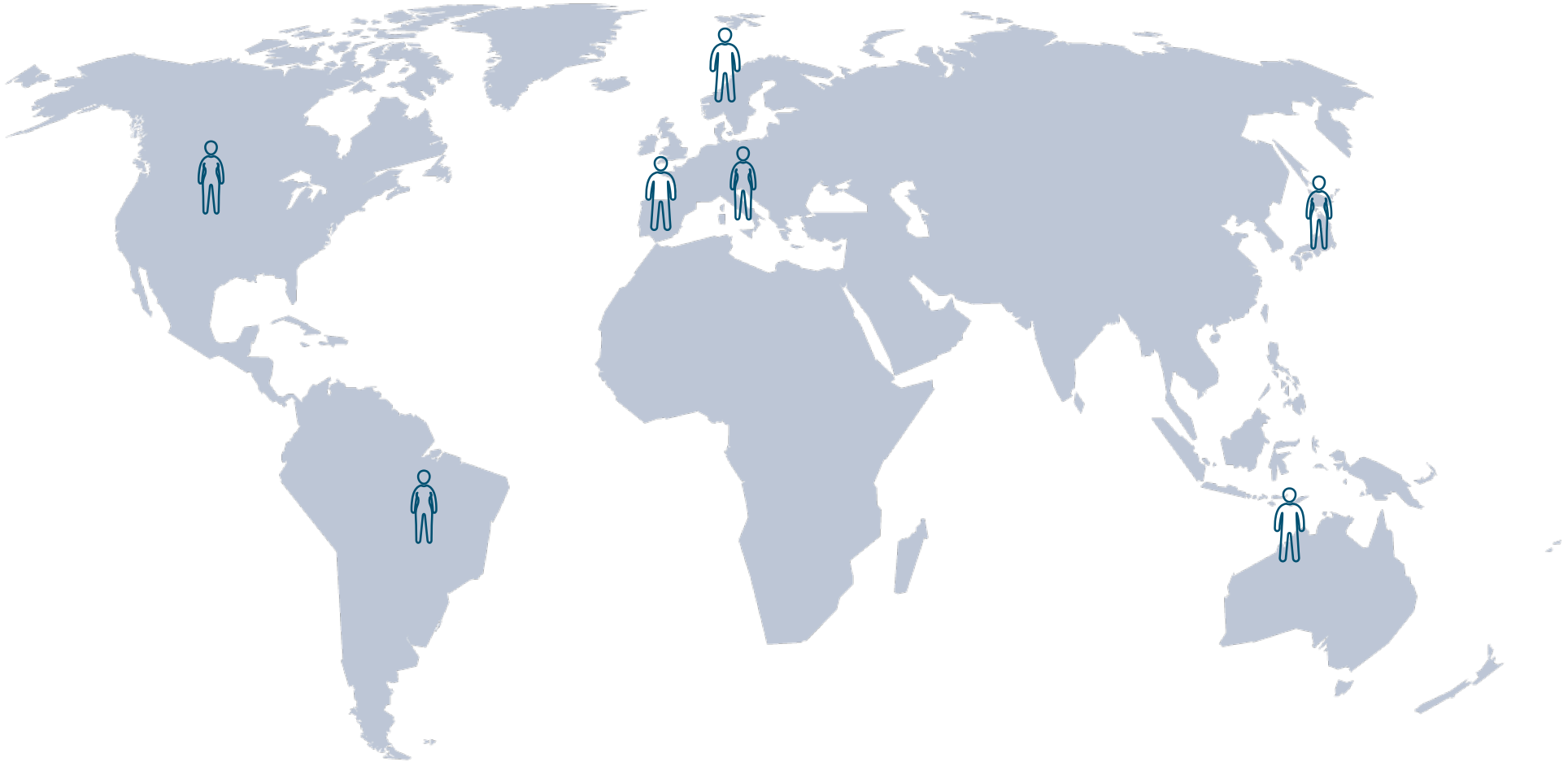
Hannah Short
AARC
Computer Security, CERN

CHEP
10 October 2016

What will we be talking about?



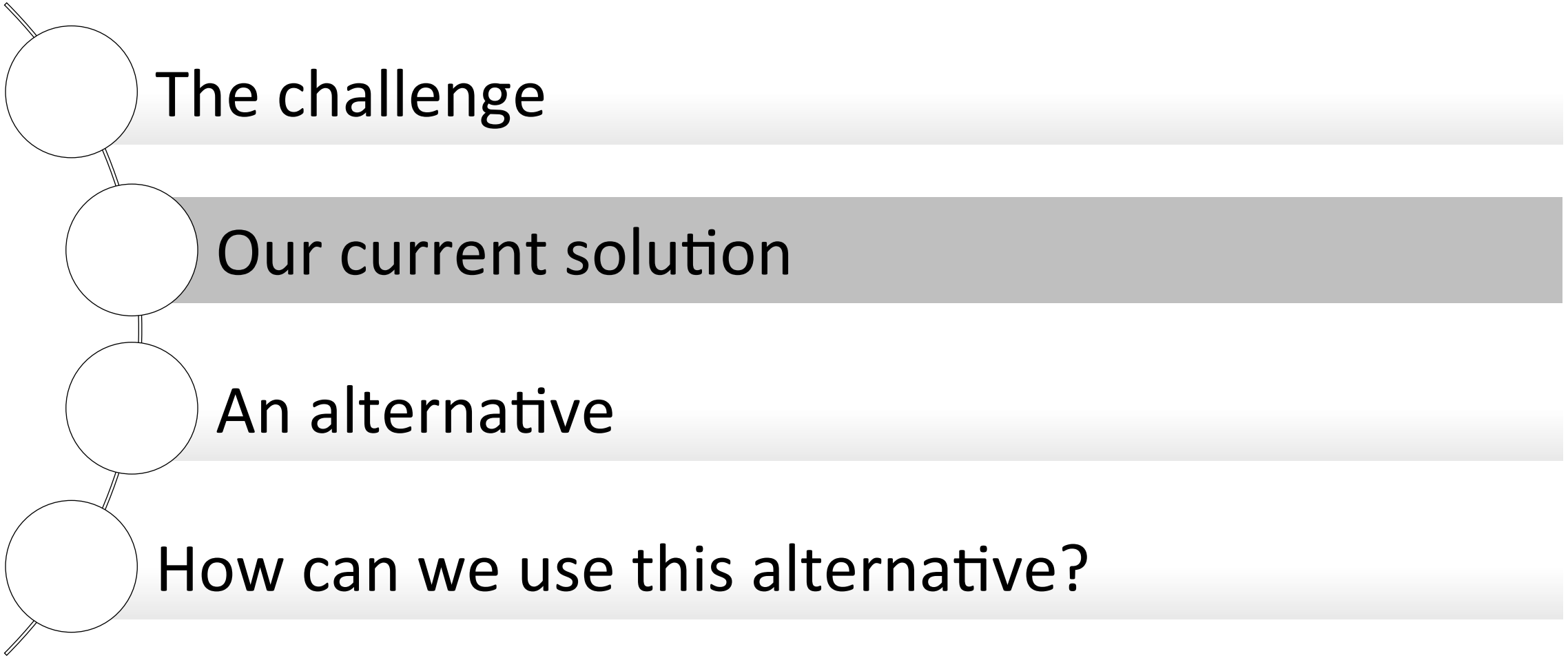
The Challenge



The Challenge

- Many have never met
- They need to work together on the same online resources
- We need to trust their identities!

What will we be talking about?

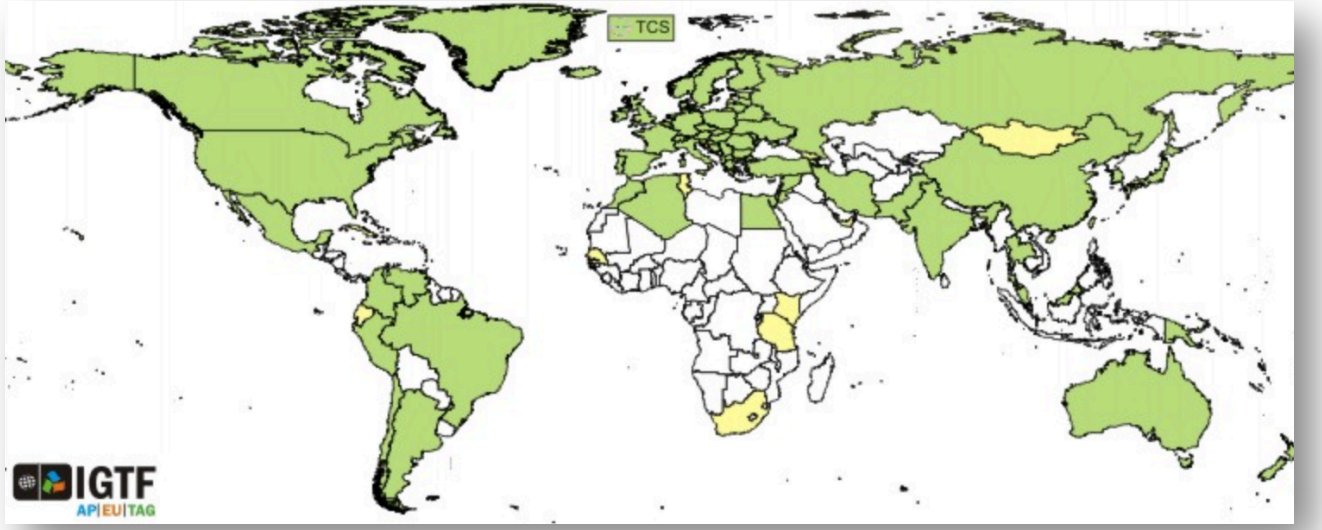


Each user obtains an x.509 certificate

The Interoperable Global Trust Federation (IGTF) controls a list of Certificate Authorities (CAs) able to issue certificates

Users approach their local CA to obtain a personal certificate and undergo identity vetting via a Registration Authority

Users register their new certificate in VOMS



http://www.gridpma.org/pmamap

Certificates have their place…

… that place is not in the hands of the user!

What's wrong with x.509?

Mobility

- Coupling credentials with devices is not necessarily valid for highly mobile researchers
- Burden on users for each new device

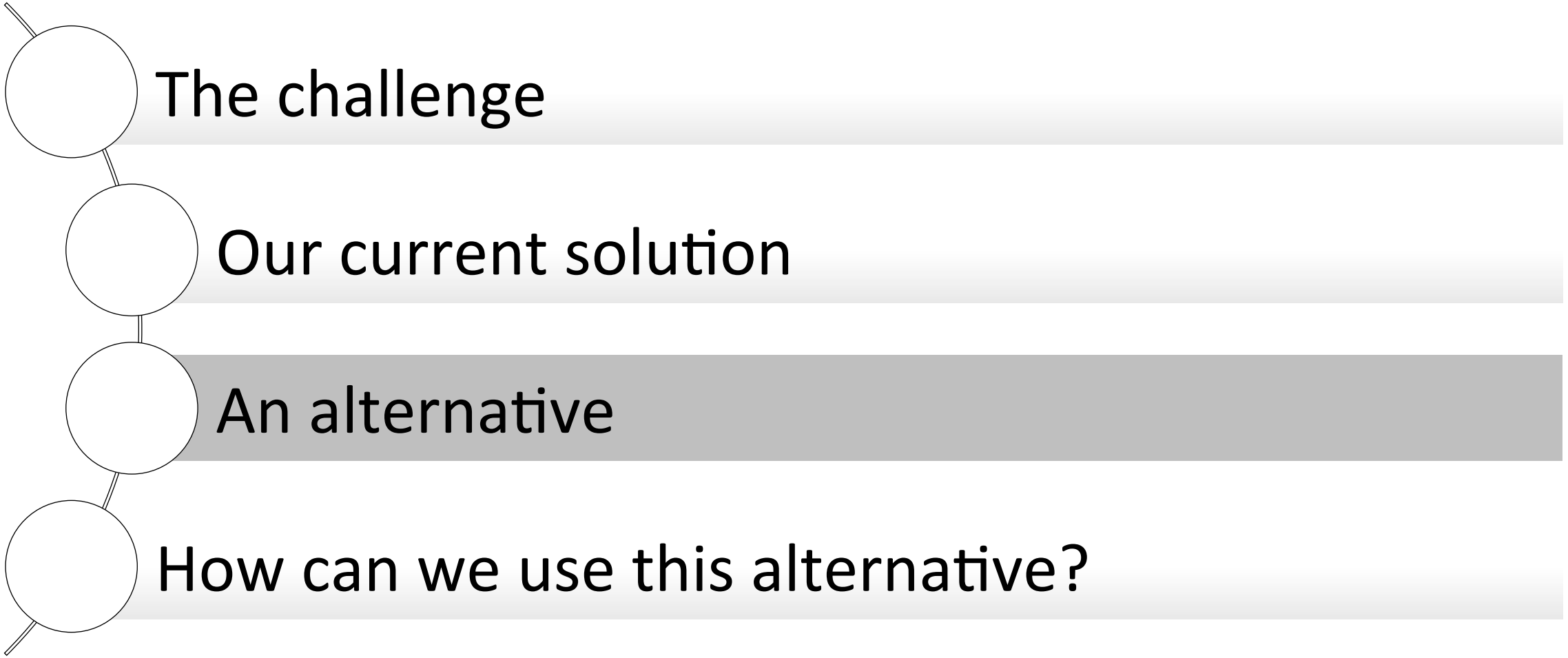
Usability

- Certificate management not in skillset of early career researchers
- One learning curve we can remove
- Users expecting "GAFA" experience, Single-Sign-On across tools

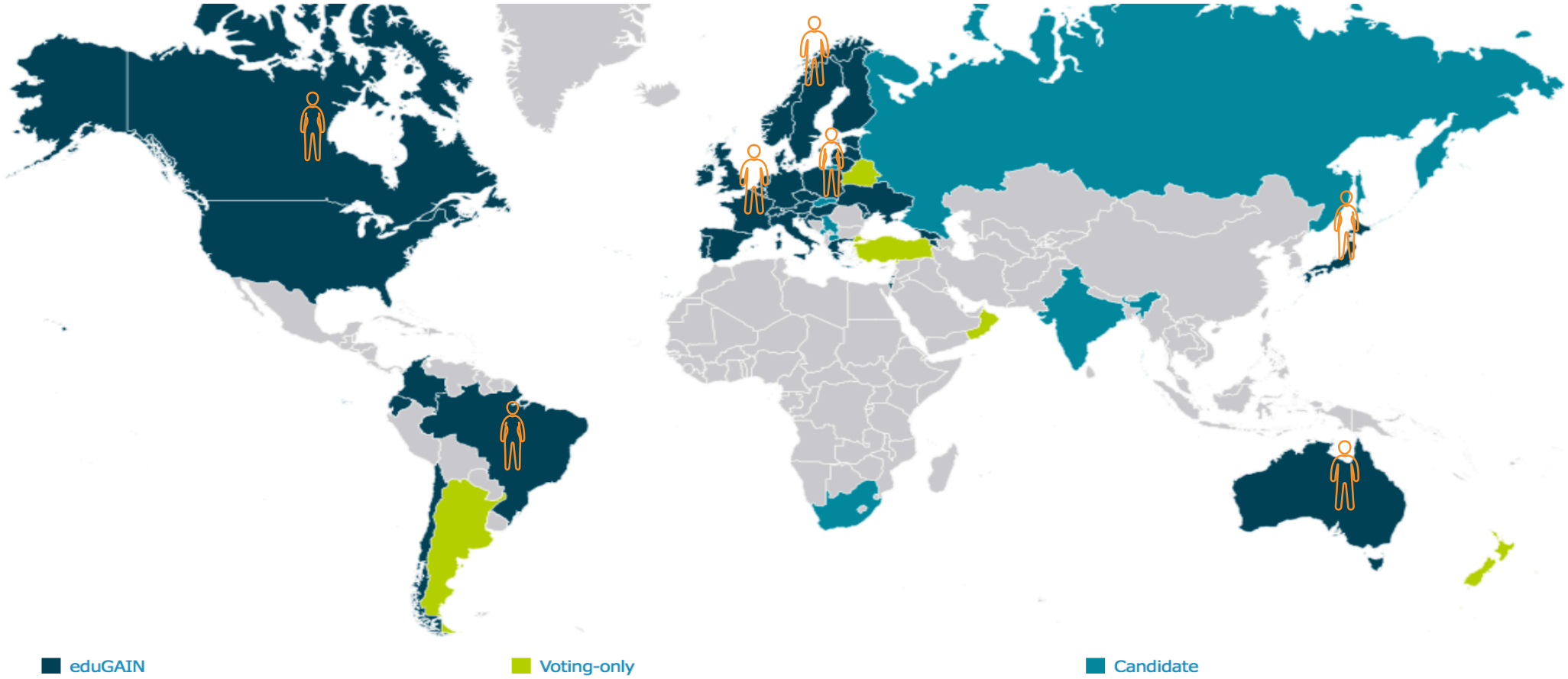
Security

- Certificates are powerful when in the wrong hands
- Private keys leaked by users
- Certificates left on shared devices

What will we be talking about?



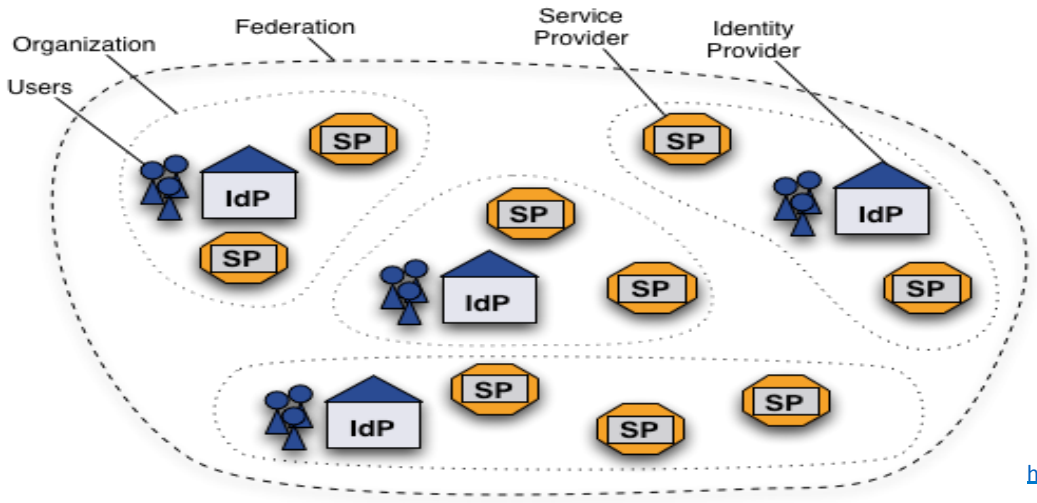
An alternative source of identities, federated identity via eduGAIN



Source: eduGAIN, data taken March 2016

What is a Federation?

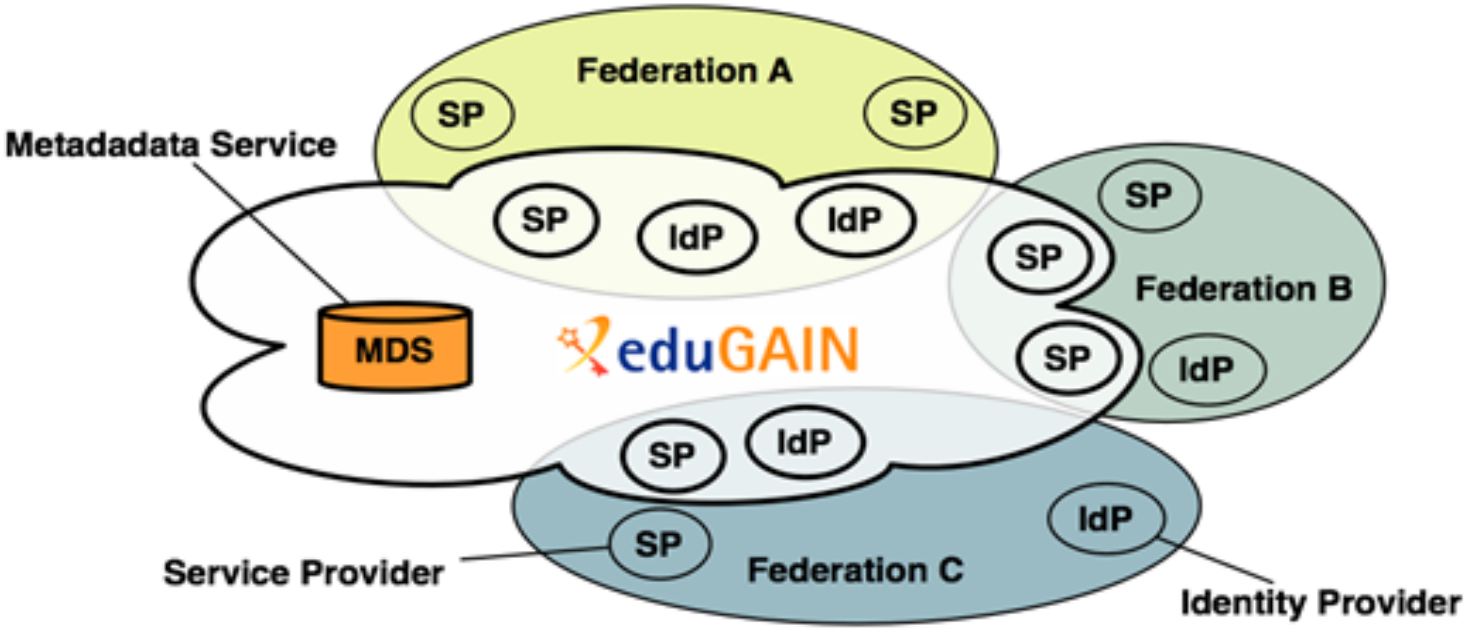
- Federated Identity Mangement (FIM) is the concept of groups of Service Providers (SPs) and Identity Providers (IdPs) agreeing to interoperate under a set of policies
- Federations are typically established nationally and use the SAML 2.0 protocol for information exchange
- Each entity within the federation is described by metadata



https://www.switch.ch/aai/about/federation/

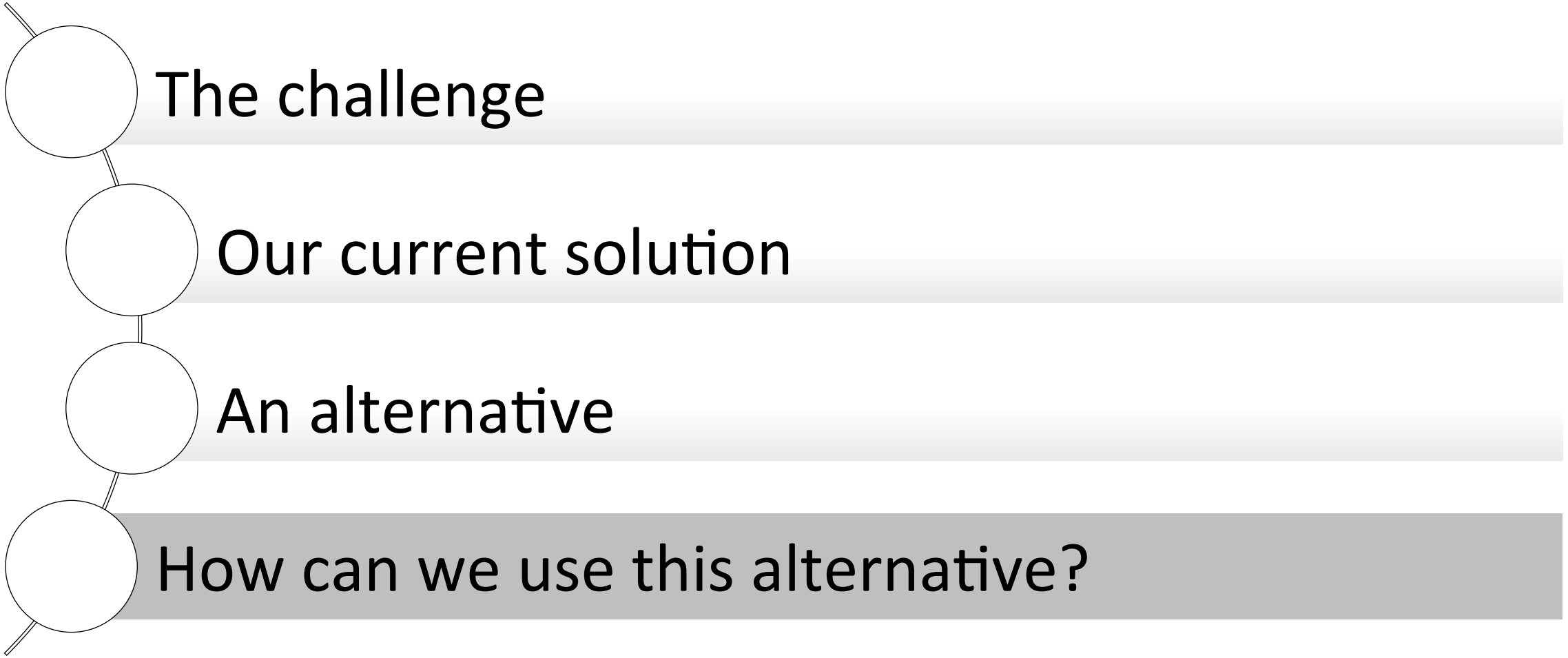
What is eduGAIN?

- eduGAIN is a form of interfederation
- Participating federations share information (metadata) about entities from their own federation with eduGAIN
- eduGAIN bundles this metadata and publishes it in a central location.



Credit to Alessandra Scicchitano – GEANT for this slide

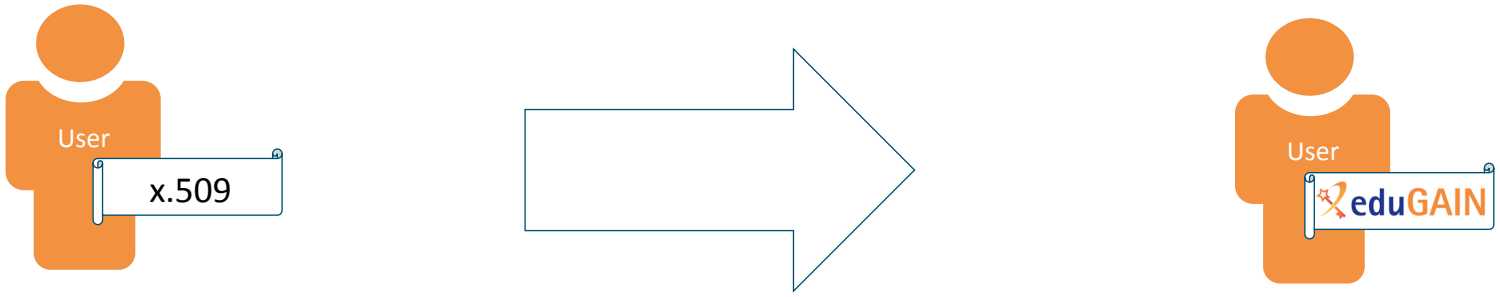
What will we be talking about?



What does WLCG need from Federated Access?

1. Trustworthy eduGAIN users
2. Web and Command Line access
3. VOMS Authorisation

1. Trustworthy eduGAIN Users

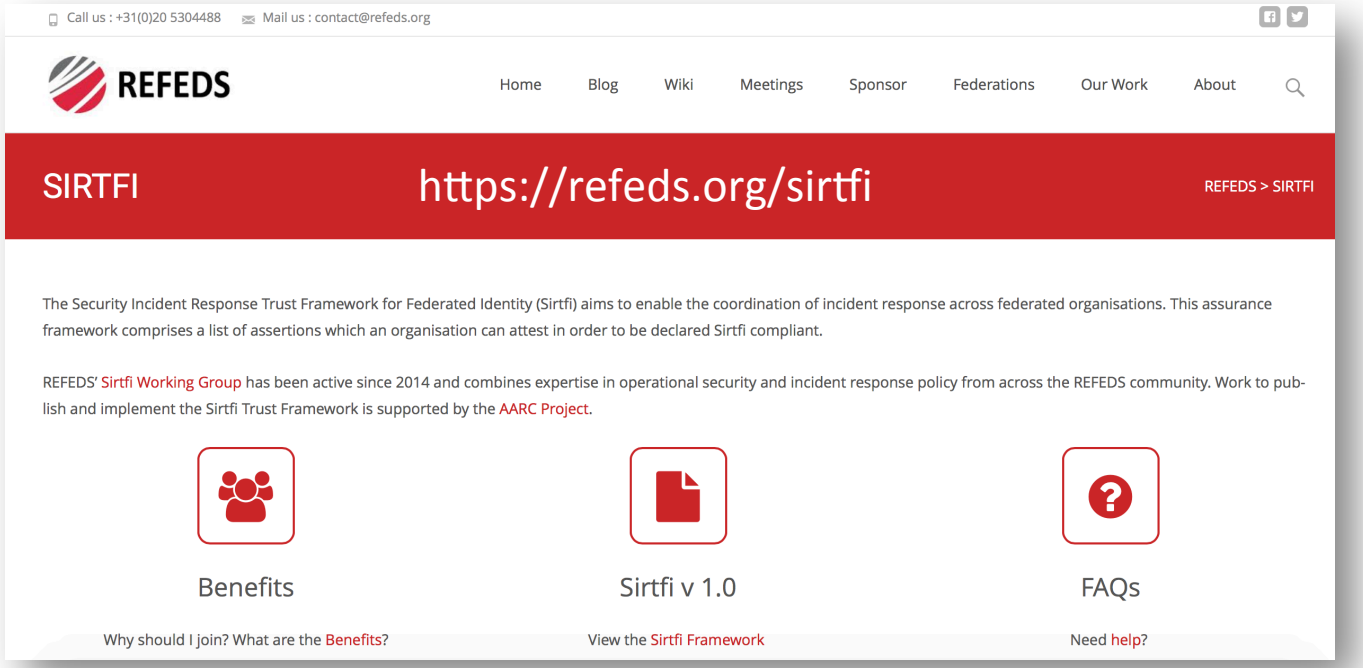


How can eduGAIN tokens be as trustworthy as x.509 certificates?

- Restrict eduGAIN to trusted partners
  - Sirtfi
  - Research & Scholarship
- Restrict access to known users
  - Create token translation layer to convert SAML 2.0 token from eduGAIN to required x.509
  - EduGAIN token transformed into x.509 ONLY if the user is registered in VOMS for the relevant experiment

Sirtfi, Security Incident Response Trust Framework for Federated Identity

- A flag for organisations that
  - Have a good baseline in operational security
  - Provide a security contact point for emergencies
  - Are able and willing to participate in incident response
- These are organisations we want to work with!

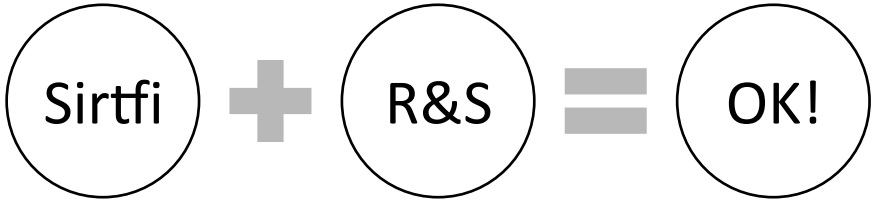


https://refeds.org/sirtfi

Research & Scholarship

- A flag for organisations that
  - Serve the Research & Education community
  - Agree to release the attributes
    - Name
    - Email
    - Unique Identifier

- CERN SSO requires this set of attributes, users from these organisations should be able to log in without a problem

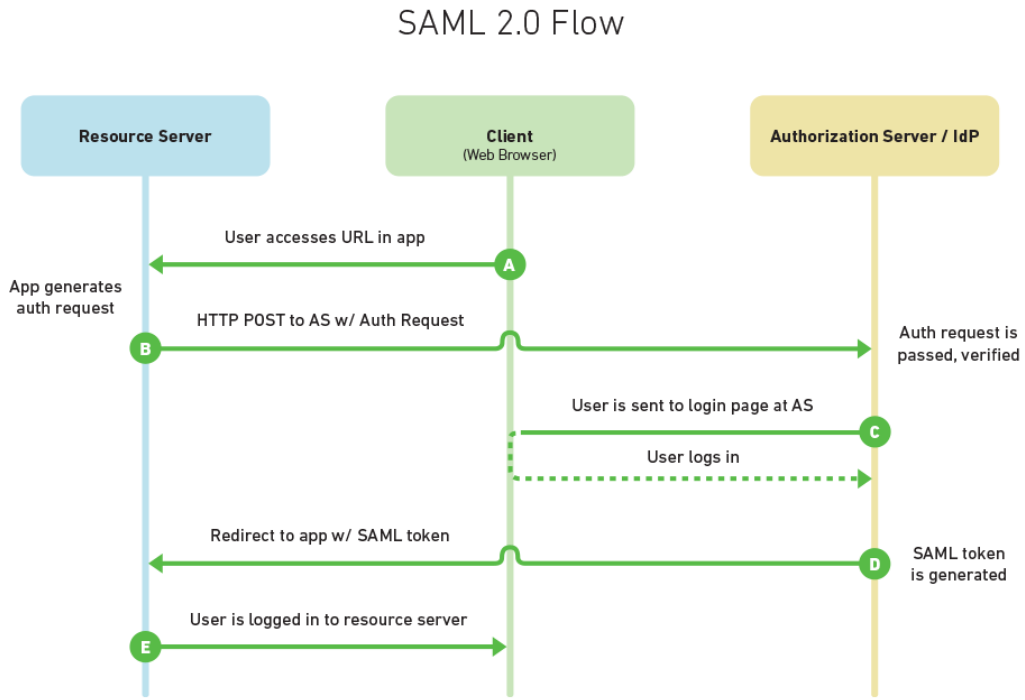


Implement Research and Scholarship Entity Category

https://refeds.org/category/research-and-scholarship

2. Web and Command Line Access

- SAML 2.0 is primarily used for browser authentication
  - Not mobile
  - Not Command Line
- Clearly, much analysis is done on the command line
- Options?
  - ECP Enhanced Client or Proxy – requires configuration at each IdP
  - CiLogon – generates x.509 from your SAML token
  - …



Can we make command line access simpler? See Andrea Manzi's talk later on…

https://www.mutuallyhuman.com/blog/2013/05/09/choosing-an-sso-strategy-saml-vs-oauth2/

3. VOMS Integration

Transparent access to WLCG resources (controlled via x.509) only granted when the identifier from the incoming token matches with a VOMS attribute

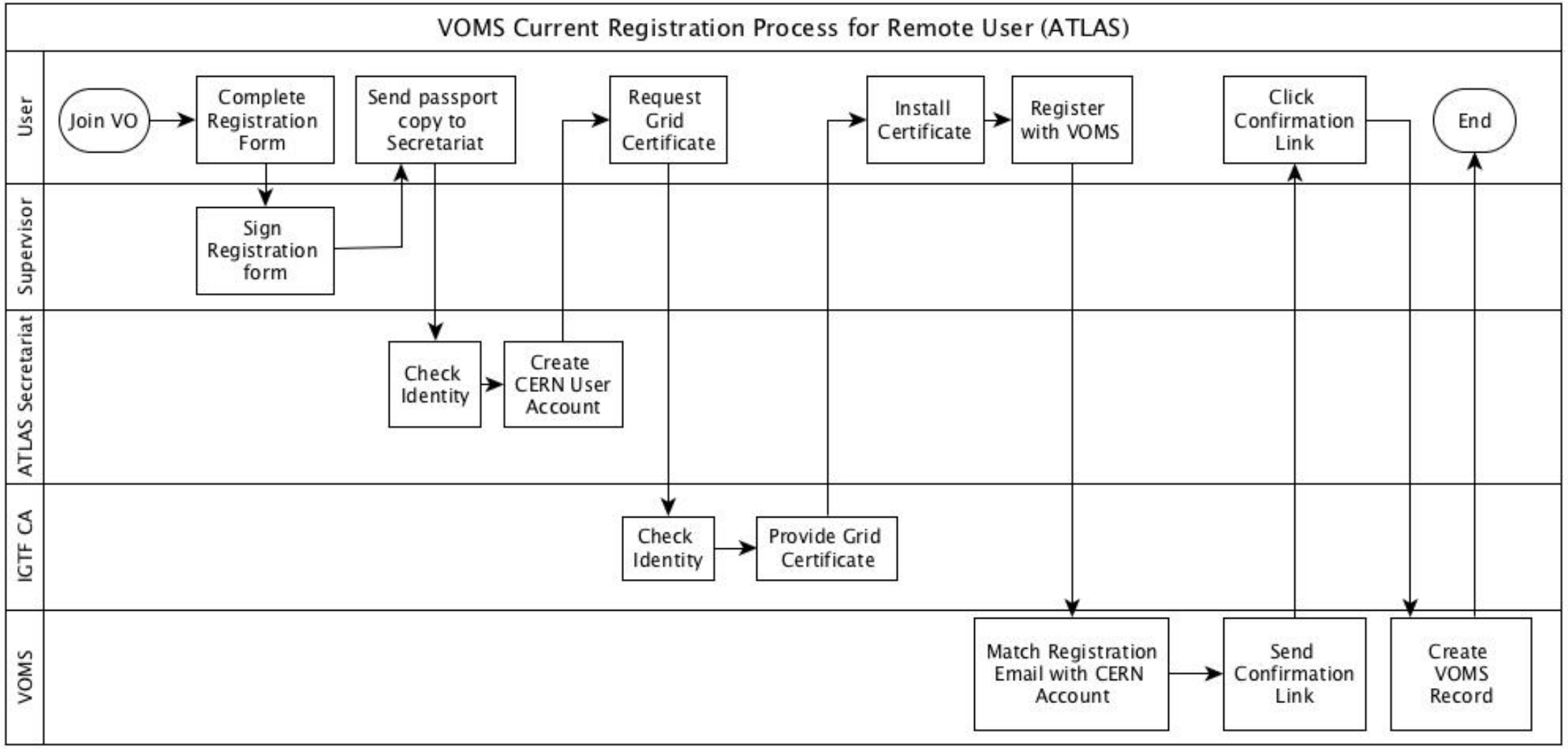
```
<AttributeStatement>
 <Attribute Name="EmailAddress">
  <AttributeValue>hannah.short08@gmail.com</AttributeValue>
 </Attribute>
 <Attribute Name="CommonName">
  <AttributeValue>jsmith</AttributeValue>
 </Attribute>
</AttributeStatement>
```

```
<Record>
 <Personal information />
 <Certificates />
 <Groups and Roles />
 <Attributes >
  <Attribute Name="eduGAINID">
   <AttributeValue>jsmith</AttributeValue>
  </Attribute>
 </Attributes>
</Record>
```

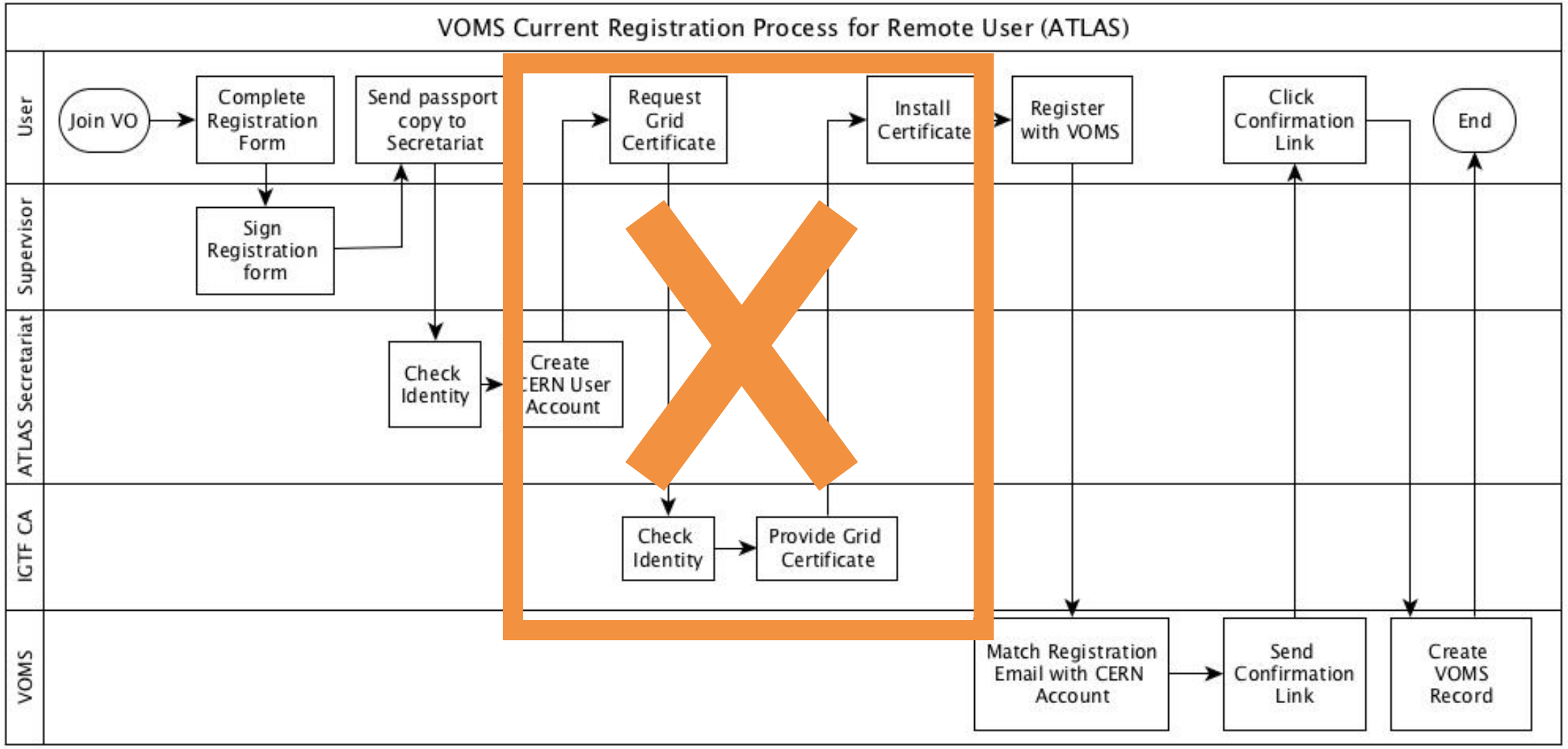
Hang on - I need to have a certificate to register in VOMS in the first place!

How is this going to work?

3. VOMS Integration



3. VOMS Integration



Our puzzle

- Research teams are international
- WLCG has over 10,000 users, many of whom have never been to CERN
- They need to access the same computing services
- We need to know who they are
- How do we do this?
- So far, has been done via personal x.509 certificates and user registration in VOMS
- There are some problems with this method
- Now we have an alternative, eduGAIN…
- … but it's not perfect
- We have identified the gaps
- And we're finding solutions

Thank you

Any Questions?

hannah.short@cern.ch

https://aarc-project.eu

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