TAKING DIGITAL IDENTITY TO THE NEXT LEVEL

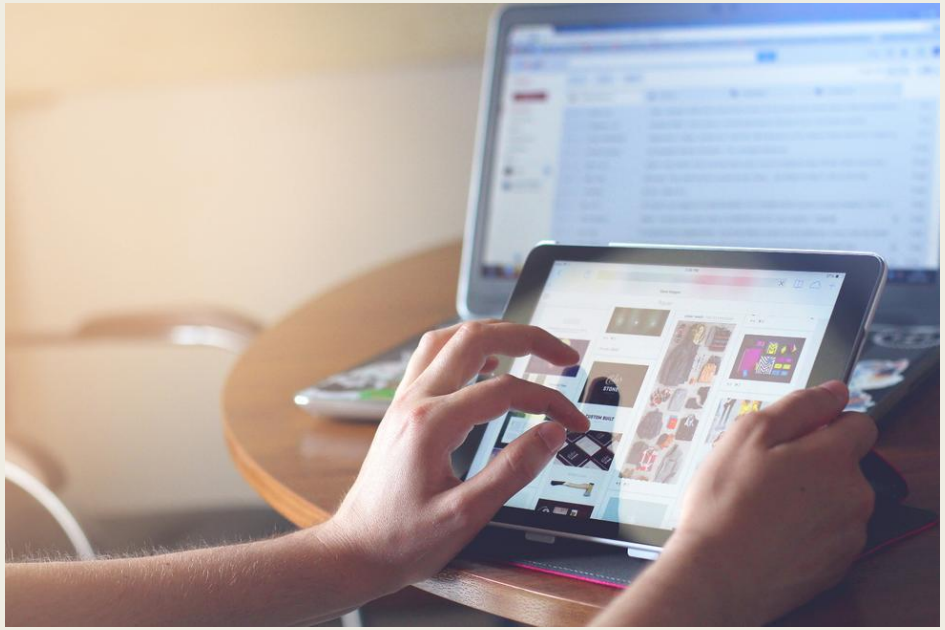
Developing and Expanding identity Federations

Heather Flanagan,
Principal at Spherical Cow Consulting,
IAM Coordinator and Technical Editor at NSRC

Digital Identity is About People

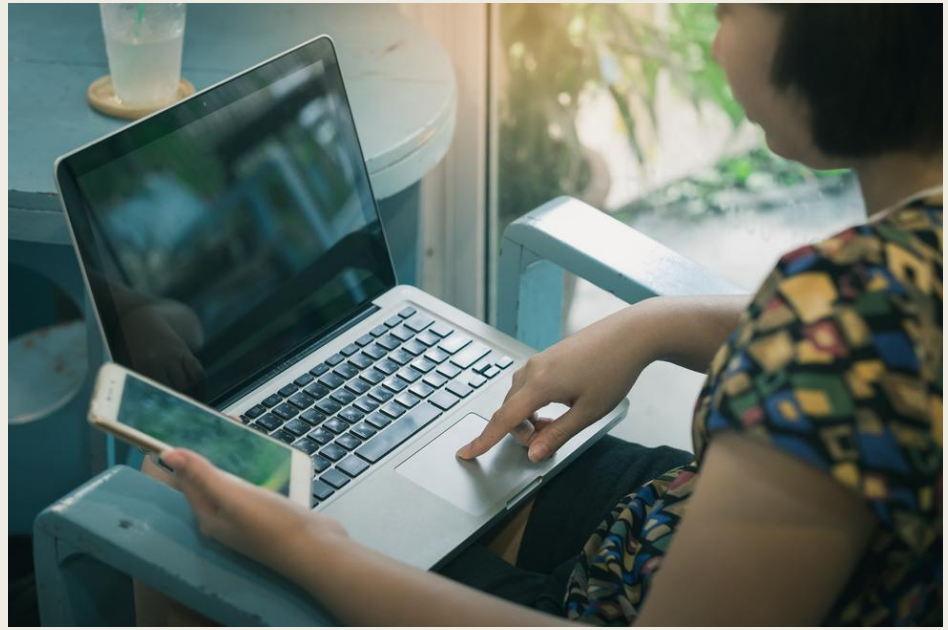
Digital Identity Solves Problems: Access

- Users want seamless access to online resources from any device, from any location for services coming from or associated with their institution
- A patchwork of solutions exist to provide off-campus access: proxy servers, VPNs, Shibboleth, however the user experience is inconsistent and confusing



Digital Identity Solves Problems: Network Security

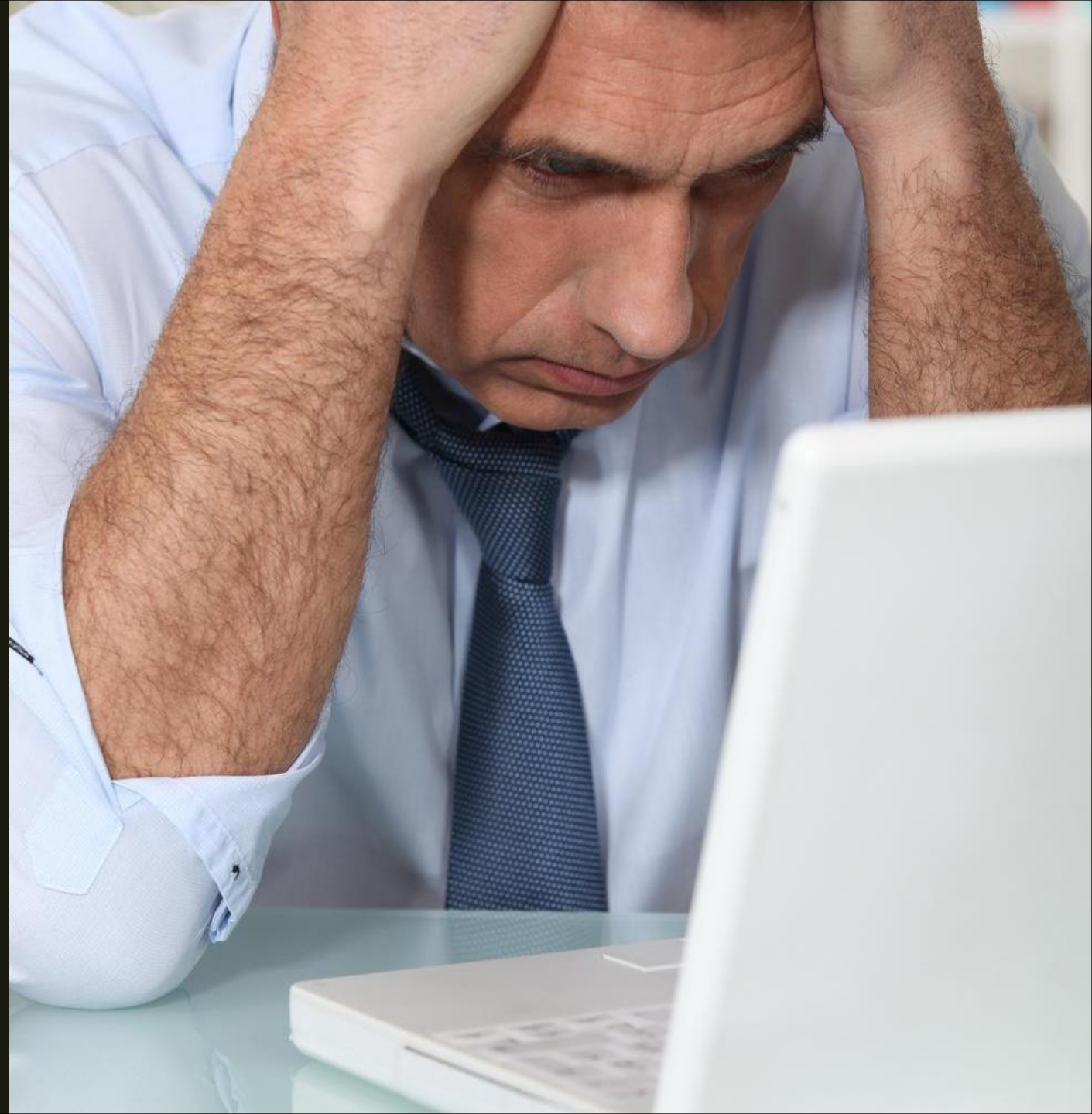
- The increase in fraud, coupled with privacy concerns, also poses a significant risk to campus information security
- Identity can be as detailed or as general as the context requires: you can preserve privacy by just checking for “studentness”



Digital Identity Solves Problems: Costs

- Service providers are facing an increasing volume of illegal downloads and piracy and fraud is difficult to track and trace because of insufficient information about the end user
  - *This will only raise the ultimate costs of providing services as service providers pass along their costs to the subscribers*

If it was easy, we would have done it already.



Biggest Challenges

- Covering costs
  - *Before you get to identity federation, the campuses need to have an IAM infrastructure*
- Understanding how to work with international privacy regulations
  - *It's not just your own country's laws*
- Meeting the needs of the user
  - *Before they outsource everything to Google, Weibo, or some other third party*
  - *Users do not care about cost of infrastructure, they care about immediate service costs*
  - *User privacy is contextual*
- Getting buy in from all stakeholders (administration, librarians, etc.)
  - *Political as well as financial barriers*

Costs versus Benefits

- Campus level costs:
  - *Establishing an IAM infrastructure*
  - *Enabling SSO and federated services*
- Federation level costs:
  - *Infrastructure costs*
  - *Business models*
  - *Governance models*
  - *Legal costs*

- Campus level benefits:
  - *Improves granularity of network security*
  - *Improves understanding of network resource allocation*
  - *Manages users more efficiently without duplicating accounts*
- Federation level benefits:
  - *Collective bargaining, policies, experience*
  - *Shared experiences across federations*

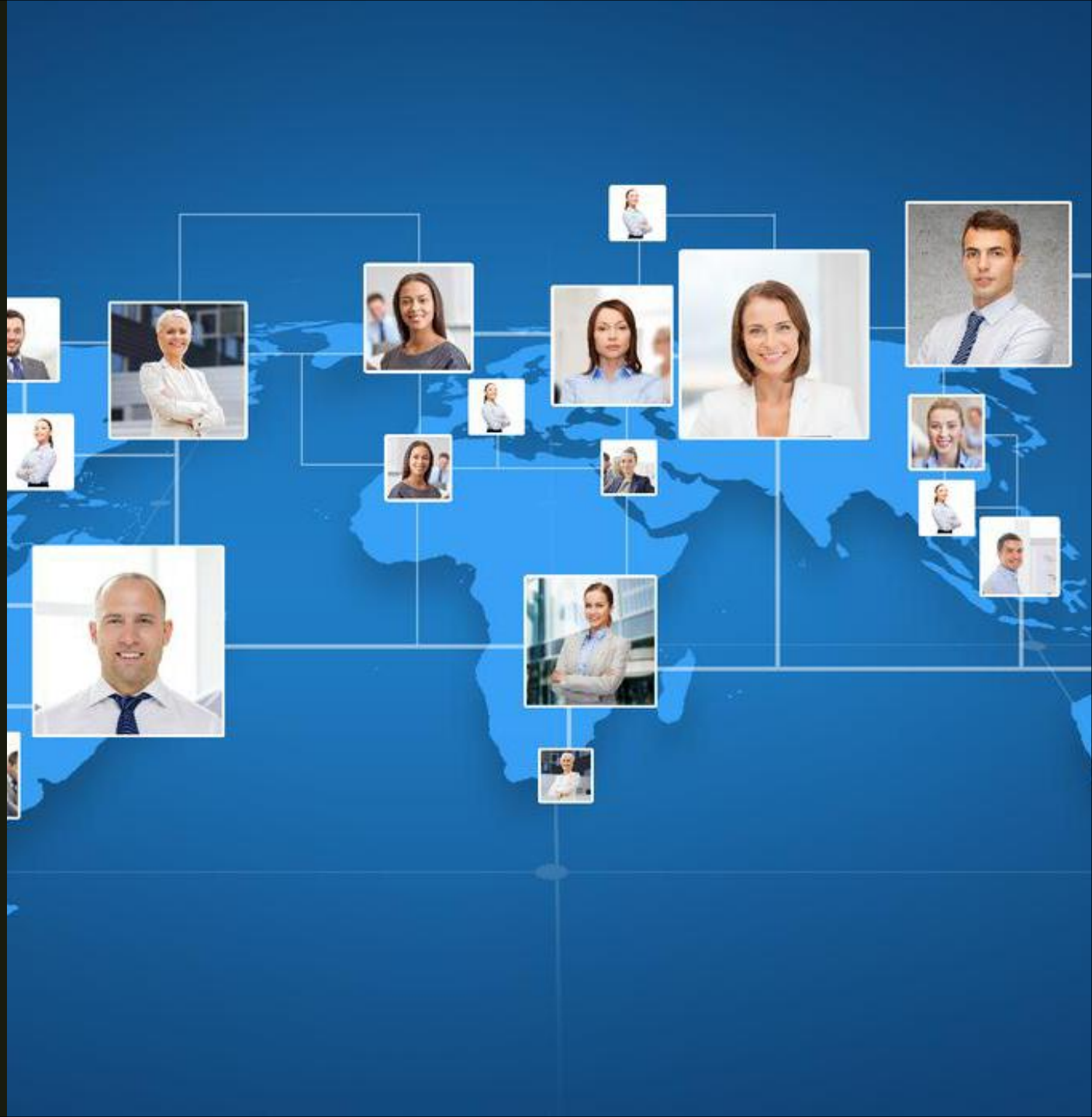
Common Misunderstandings

- “Doesn’t federated identity mean all the security eggs are in one basket?”
  - *Yes and no: The institution almost always has better security practices than the users, who will often decrease the security of their accounts by using a common username and password*
- “If a user can log in, they must have access, right?”
  - *No: Just because they can log in does not mean means they can, or should, access everything*
- “Doesn’t federated identity mean I have to share all the information about my users?! Attributes cannot be released due to privacy regulations!”
  - *See the GDPR “legitimate interest” argument; it may apply in your jurisdiction*
- “My institution already supports eduroam – doesn’t that mean we support all federated services?”
  - *No: There is a difference between a common service that supports federation and it being a federation in and of itself*

Services to Target

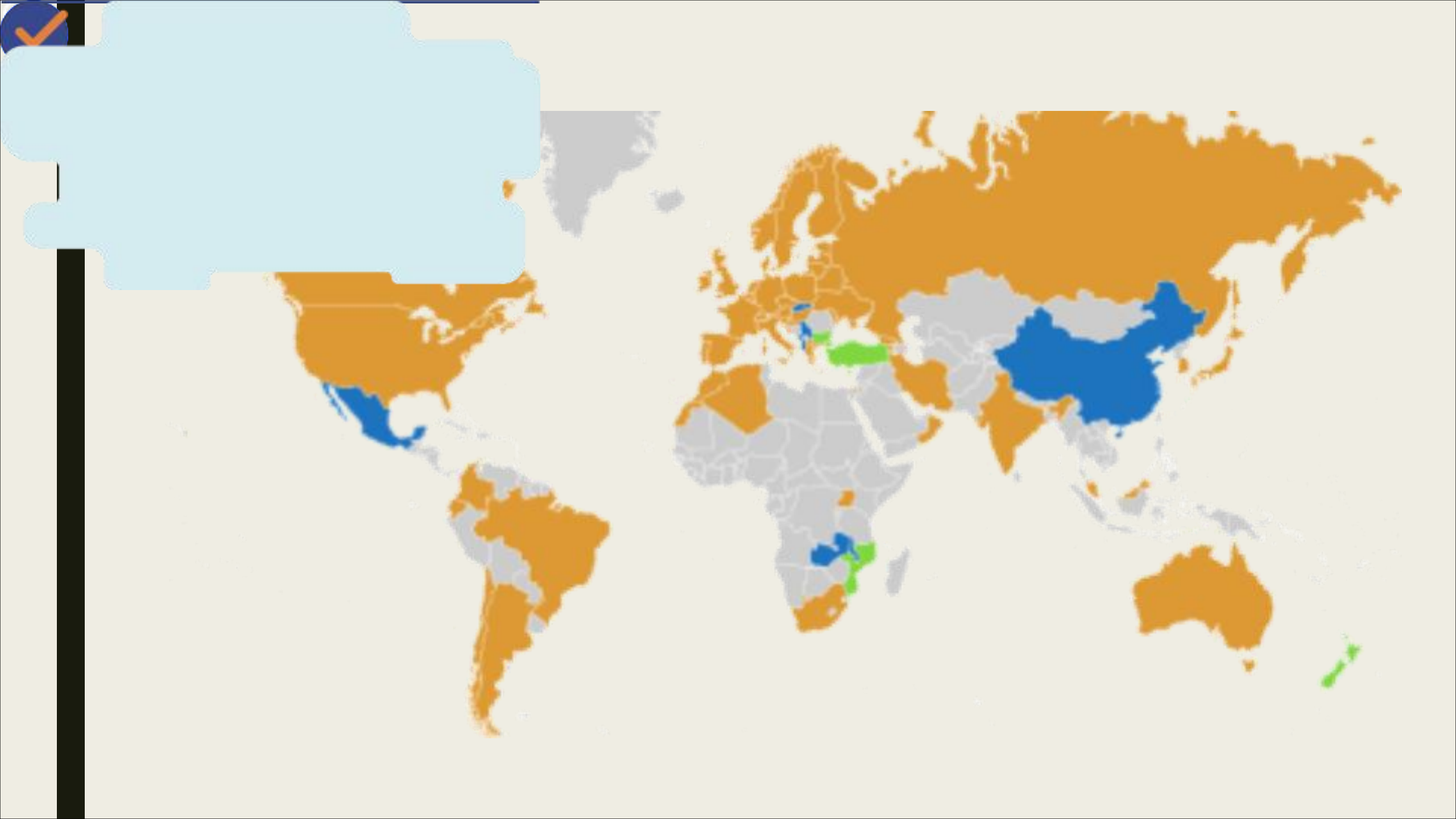
- eduroam
- Outsourced cloud services
  - *Outsourcing services does not mean outsourcing control and responsibility*
- Scholarly publication access
  - *Even OpenAccess benefits from identity federation*
- Educational discounts
  - *e.g., Apple, Microsoft, other companies that provide academic discounts*
- Research and scientific collaborations
  - *LIGO and NIAID research can't happen without federated access and collaboration*

Digital Identity happens at a global scale.

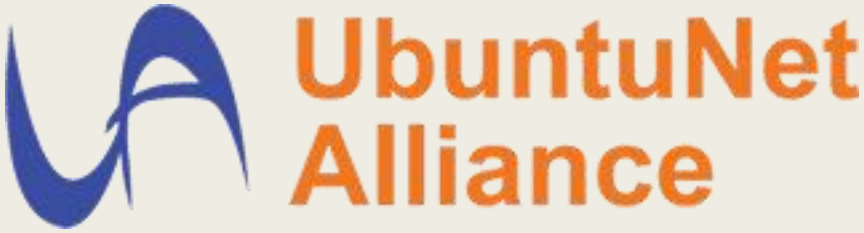


Identity Federations Exist Around the World

- Report from the Metadata Explorer Tool (https://met.refeds.org)
  - *4942 Identity Providers*
  - *11236 Service Providers*
  - *64 Federations*
- Report from eduGAIN (https://edugain.org/participants/federations-in-edugain/)
  - *53 Participating Federations*
  - *6 Voting-only Federations*
  - *12 Candidate Federations*



Where Federation Discussions Happen



- Federations at different levels of maturity
- Templates and best practices are freely available
  - https://wiki.refeds.org/display/FBP
- Email lists, slack channels, meetings – so many ways to find others working in this same space

Standards and Architectures

Where Standardization Happens

- Entity Categories and Federation Best Practice = https://refeds.org
- OpenID Connect Specifications and Federation Model = http://openid.net/connect/
- SAML2 Specification = https://www.oasis-open.org/standards
- Interoperability profiles = https://kantarainitiative.github.io/SAMLprofiles/fedinterop.html and https://kantarainitiative.github.io/SAMLprofiles/saml2int.html

If you want interoperability and standards that take into account your use cases, you need to participate in the standards process!

Famous Last Words

Always design for interfederation and interoperability: things will go wrong when you build things that solve local problems without thinking about interoperability and scale.

With many thanks to