Federations: As a Concept

What is Federation ?

“A means to enable users to access the systems and applications of multiple organizations using one login credential” - NIST

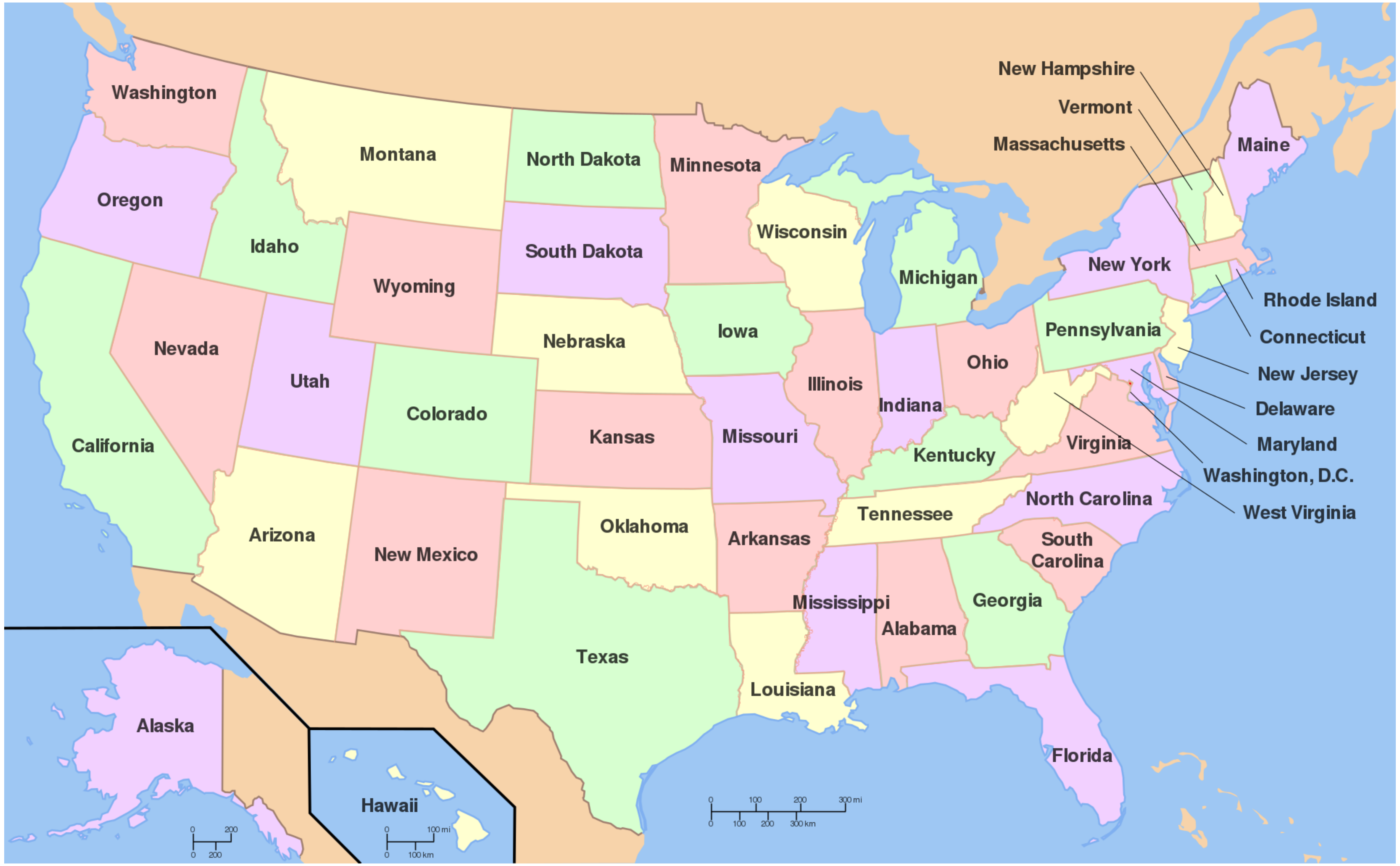

Image Source: https://commons.wikimedia.org/wiki/File:Map_of_USA_with_state_names.svg

Image Source: https://thehill.com/

Why do Federations exist ?

How does Federation work ?

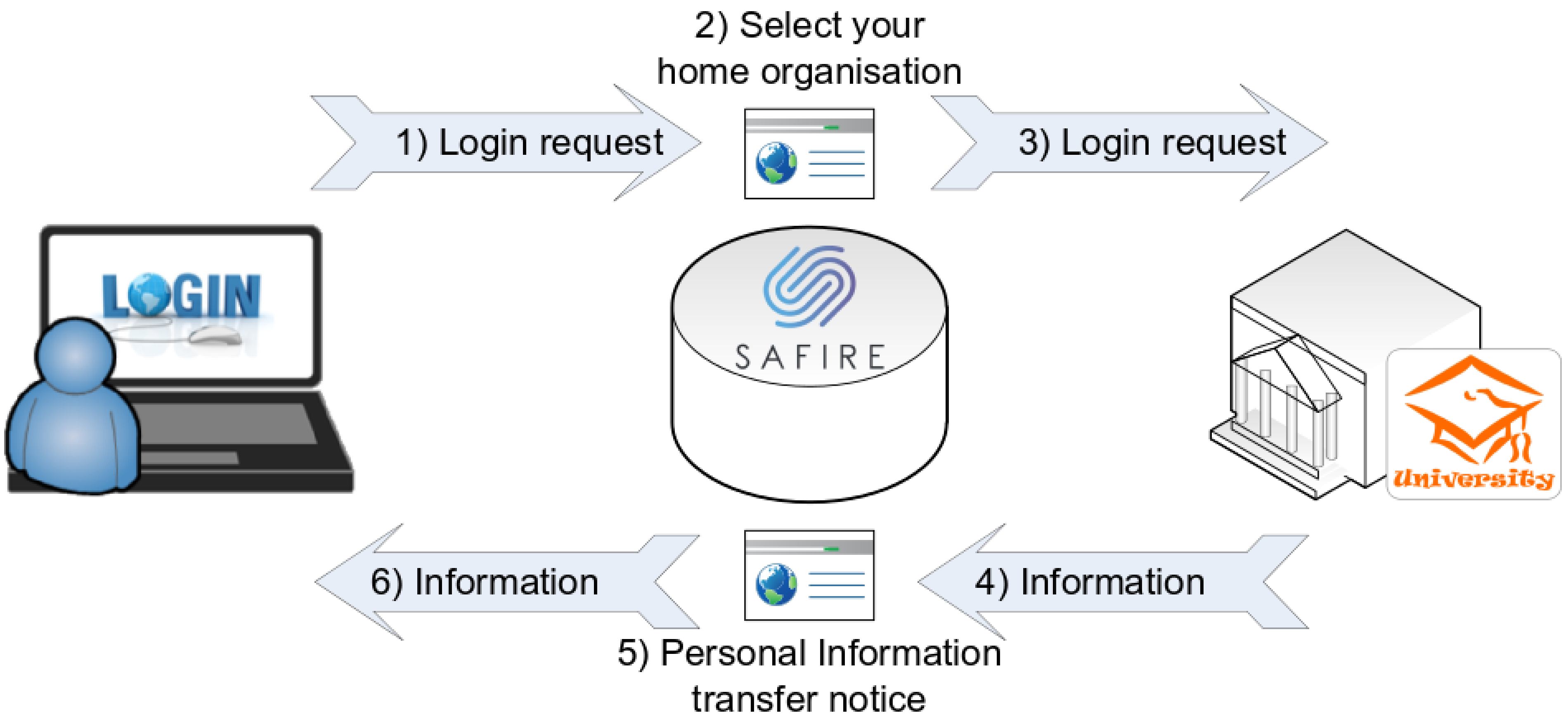

Image Source: https://safire.ac.za/users/how/

TRUST!!

- We need to be able to trust one another, and trust that what we are doing with users data is considered, lawful, and ethical

Federations are built on Trust Frameworks

So what is a Trust framework ?

- Exists to make sure everyone understands their roles
- Helps manage expectations
- Ensures IdPs and SPs do the right thing
- Will evolve and get more stringent over time

Source: Governance, Policies & Privacy - UbuntuNet TI 18

“Trust amongst members of an identity federation is foundational to its operation and is established through the set of agreements and associated rules that are specific to that community”

reference: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8149.pdf

Privacy

Legal basis for privacy

- POPI arriveth!
  - IdPs and SPs in Europe are bound by the General Data Protection Regulation (GDPR), and South Africa has signed POPI into law….albeit, without a commencement date,….for now…..
  - This does affect your users and your services

Federation Entities, and The Roles they play

Identity Provider

- Also known as: IdP, Home Organization Home Institution, (Responsible Party in POPI, and Data Controller in the GDPR.)
- The role of the IdP at it’s core is to provide login credentials for it’s users (Data Subjects)
- The trust that is put on the IdP is that it has proper Identity management lifecycles in place, meaning, it is responsible for the user data that is asserted to the Federation
- To have sufficient policy in place as to govern users, ie. An acceptable use policy.

Service Provider

- Also known as: SP, Visited Organization.
- To offer a service, or an application that requires restricted access
- Trust that the data they receive from IdP’s is accurate to be able to make such decisions as to authorize, or deny access …which brings us back to IdP’s having Identity management lifecycles in place…
- Publish a privacy policy in which it is outlined how they handle Personal Information. Ie. POPI/GDPR responsibilities!

Federation Operator

- also known as the Roaming Operator (as can be seen in the case of eduroam)
- Broker Trust between members of the federation
- Governance of the Federation (policies, and documentation)
- POPI/GDPR
- Rules surrounding the trust framework
- Manage Participation
- Maintain the federation infrastructure/Architecture

Interfederation Operator

- Also known as the confederation
- Much the same as a Federation Operator, except that it is that one step higher, someone like eduGAIN performs much of the same functions as a federation operator, except with federations, rather than individual Identity Providers, or Service Providers.