Governance, Policies & Privacy

Trust

Trust derives from governance

Trust derives from governance

and is documented in policy

Federation Policy

- 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

Acceptable Use Policy

- Make sure your providers have one!
- Think about what changes might be needed to cope with federation

- What happens when one of your users abuses a service located in another country?

Identity Management Practice Statement

- Documents the identity management lifecycle in your institution, from provisioning to de-provisioning
- Helps other providers understand your level of assurance
  - How sure are you that your user is who they claim to be?

Identity Management Practice Statement

- Documents the identity management lifecycle in your institution, from provisioning to de-provisioning
- Helps other providers understand your level of assurance
  - How sure are you that your user is wh

Identity Manageme

- Documents the identi
  institution, from pr
- Helps other provid
  assurance
  - How sure are you t

A **Level of Assurance**, as defined by the by ISO/IEC 29115 Standard, describes the degree of confidence in the processes leading up to and including an authentication

- Wikipedia

Identity Management Practice Statement

- Documents the identity management lifecycle in your institution, from provisioning to de-provisioning
- Helps other providers understand your level of assurance
  - How sure are you that your user is who they claim to be?

- Be honest! Document what you are **currently** doing, not what you want to do.

Privacy

Legal basis for privacy

- Even of you don’t have privacy laws in your country:
  - IdPs and SPs in Europe are bound by the General Data Protection Regulation (GDPR)
  - This ~~may~~will affect your users and your services

Legal basis for privacy

- Even of you don’t have privacy laws in your country:
  - IdPs and SPs in Europe are bound by the General Data Protection Regulation (GDPR)
  - This ~~may~~will affect your users and your services

- You can expect your country to get privacy laws sooner or later...

The German privacy virus

- The world's first computer-specific data protection law was passed by the German federal state of Hessen.
- The Bundesdatenschutzgesetz or Data Protection Act

https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz

Privacy

- It is better to think about privacy from the beginning, rather than as an after though when laws compel you

- And it’s the right thing to do anyway…

Privacy: Just Do It.

- Use pseudo-anonymous, opaque, targeted identifiers instead of usernames wherever possible
- Don’t release more attributes than you need to
  - But don’t release fewer than you need to either!!!
- Let users know what you’re doing with their PI
  - In a privacy statement/policy
  - During attribute release

Federation & the law

Federation & the law

- IANAL, nor do I know your law…
- … so lets use South African law as an example of things you may need to think about

Federation & the law: logging

- In South Africa, the Regulation of Interception of Communications and Provision of Communications-Related Information Act…
  - Requires [identity] providers to keep a copy of the identity document of their users for five years
  - Requires [service] providers keep “adequate” logs
  - Allows for an judge to issue an interception order

Federation & the law: section 212

- In South Africa, section 212 of the Criminal Procedure Act allows a judge to issue a subpoena compelling a service provider to provide information about a user
- But what happens when a pseudo-anonymous identifier is used?

Federation & the law: minors

- In South Africa, the Film & Publications Amendment Act requires that service providers take steps to protect minors
- This particularly impacts eduroam