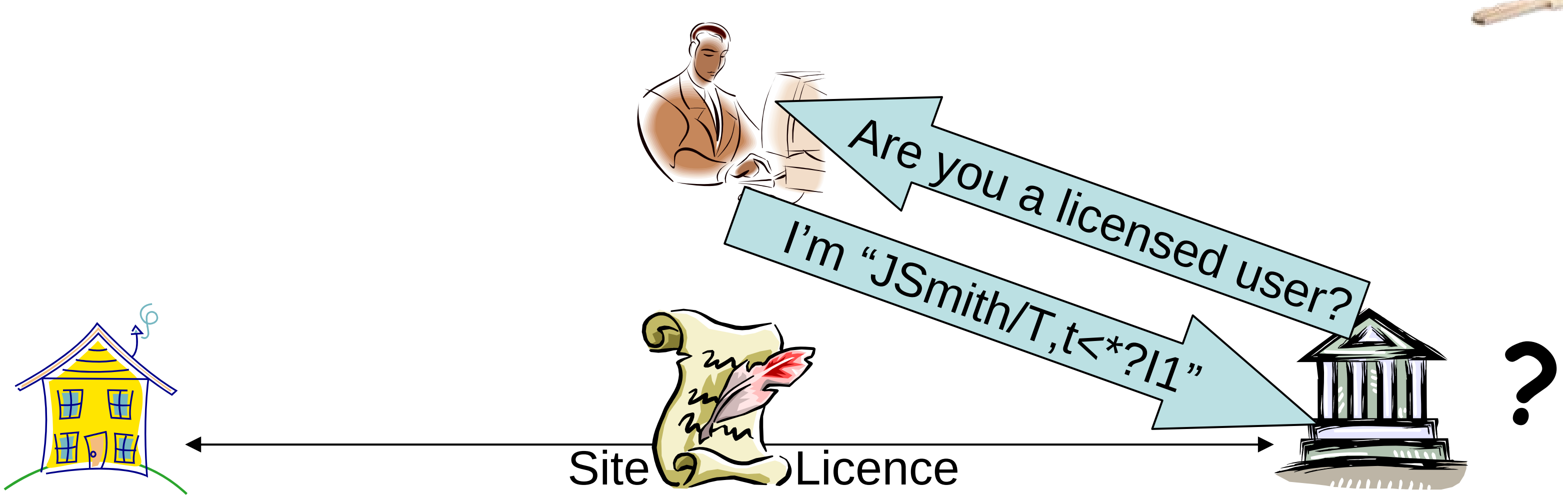
Protecting Privacy with Federated AA

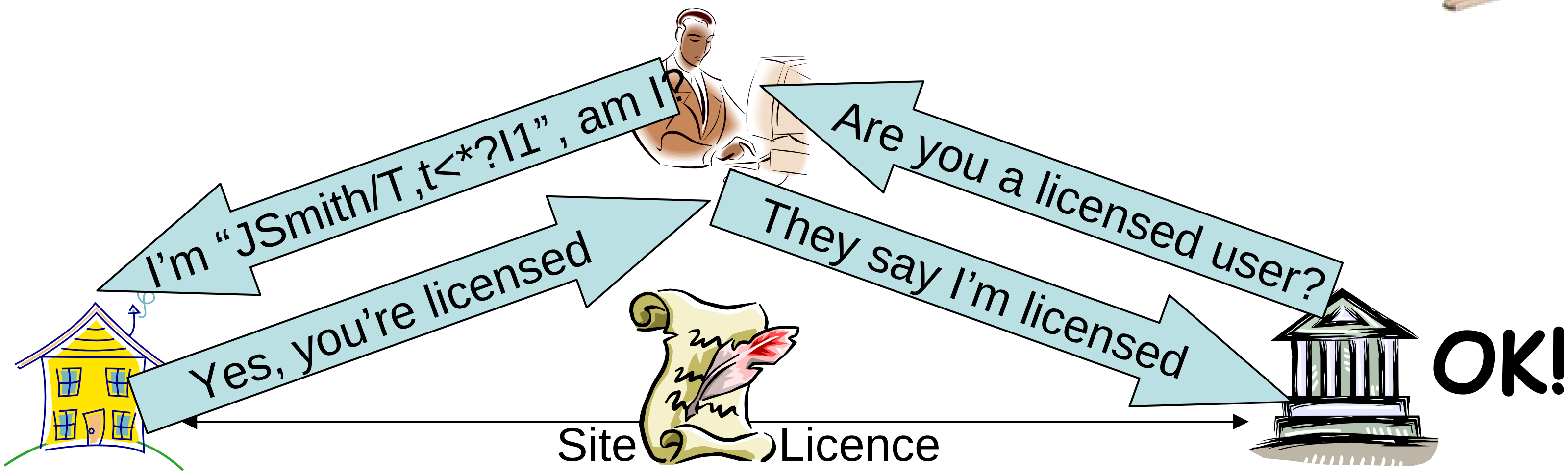
Andrew Cormack
Chief Regulatory Adviser, UKERNA
A.Cormack@ukerna.ac.uk

“AuthZ & AuthN” Today



- User’s identity and personal data are known to all
- Publisher knows more than it wants and less than it needs
- Organisation’s precious credentials given to all publishers

Federated AuthZ & AuthN



- User's identity and personal data are protected
- Publisher knows exactly what it needs
- Distribution of credentials is reduced

Fine-Grained A&A

- Needed for less-than-site licenses
- Publisher can ask for more detail, e.g.
  - User's relationship with organisation (staff, pupil,…)
  - Unique persistent 'handle' for user
  - Well-known identifier (e.g. username) for user
  - Other attributes of user
- These may reveal personal or sensitive details
  - Publisher must only ask for what it needs
  - Organisation must only tell what user permits

Benefits for Users

- Much less need to disclose your identity
- Personal data kept between you and your home organisation
- Publishers can tailor services better
- (At least) one less password to remember
- …

Benefits for Organisations

- Better service offered to users
- Uses existing access management systems
  - And protects the data in them
- Can use same access control for all resources
  - Both internal and external
- Fewer support problems
- Easier to comply with regulatory requirements
  - *Data Protection Act 1998*, etc.
- …

Benefits for Publishers

- No need to maintain your own user database
  - Authentication is done for you by home organisation
  - Can authorise per institution, role, and/or entitlement
- Reduced user support requirements
- Reduced compliance burden
  - Less storage/processing of personal data
- Accurate implementation of licence conditions
- Users take better care of credentials
- Organisations take better care of assertions
- …

What is the Federation?

- A set of Rules that binds members:
  - Make accurate statements to other members
    - If you say you can hold users accountable, do so
  - Keep federation systems and data secure
  - Use personal data correctly (inc. DPA1998)
  - Resolve problems within the Federation
    - Not by legal action
  - Assist Federation Operator and other members

There must be more to it…

There is ☺

- Guidance, examples, support
  - How to comply with the Rules
  - How to inter-work with other members
    - Common definitions, etc.
  - Help in planning the transition
  - Experiences of early adopters
  - Software to implement Federation services
  - Gateways for transition or outsourcing
- All this is advisory, not prescriptive
  - Can use as much or as little as you need