SIRTFI

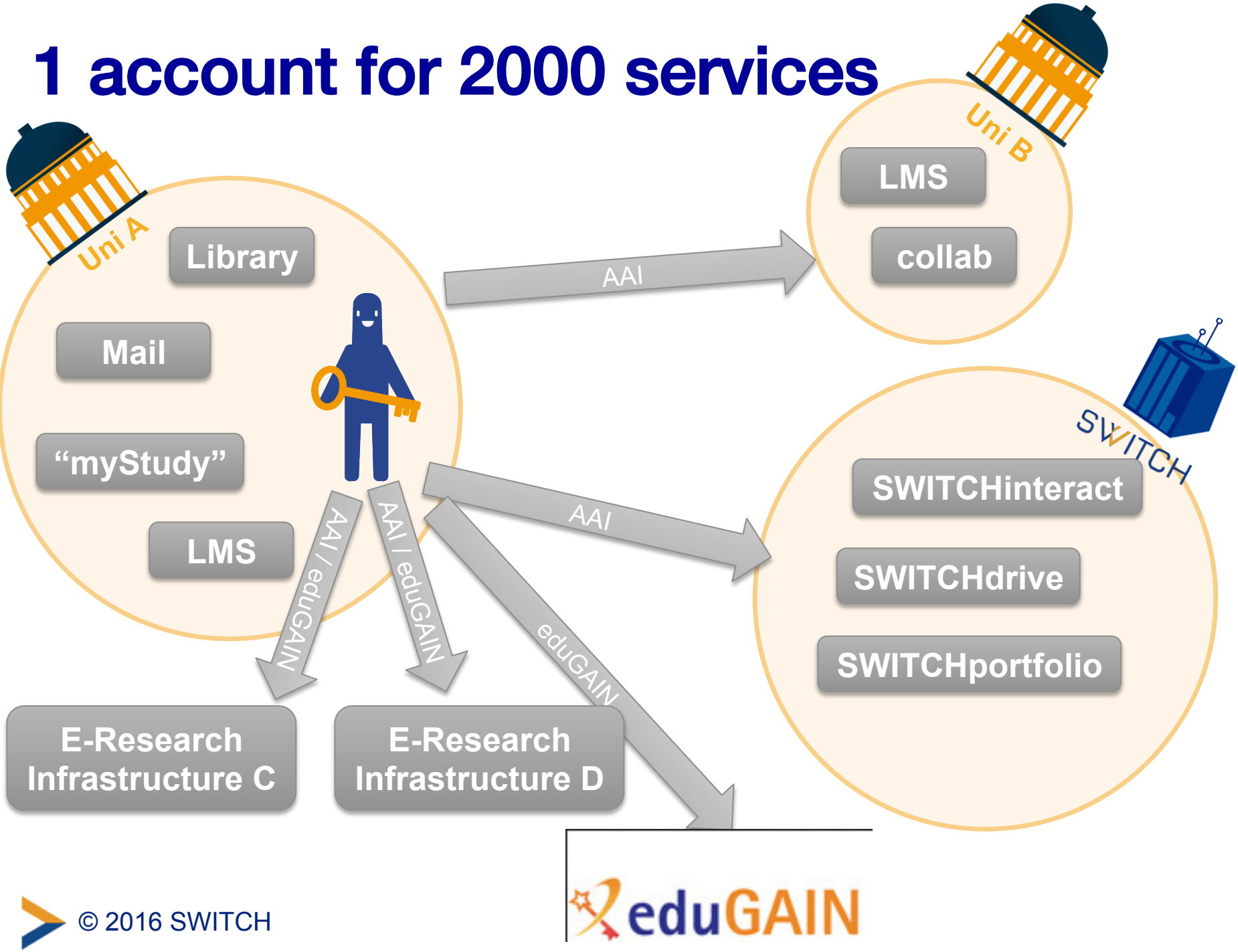
How to handle compromised AAI accounts

SWITCH

Thomas Bärecke
thomas.baerecke@switch.ch

Bern, June 30th, 2016

1 account for 2000 services



SIRTFI - coordinated incident response

A Security Incident Response Trust Framework for Federated Identity

- Operational Security
- Incident Response
- Traceability
- Participant Responsabilities

Operational Security

- Regular patches
- Processes for vulnerability management
- Intrusion detection and information protection
- Possibility of timely user rights changes
- Established contacts for service owners and users
- Security Incident Response

Incident Response

- Security incident response contact information
- Timely reply to other SIRTFI members
- Collaborate in management of security incidents
- Respect SIR procedures of own organisation
- Respect user privacy
- Respect Traffic Light Protocol

Traceability and participants responsibilities

Keep accurate logs of all relevant information available for handling security incidents

Acceptable use policy (AUP)

User consent to AUP

Next steps

SWITCH

- Implement processes to add security contact information
- Publish security contact information in metadata where available

SP and IdP operators

- Read the document at https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
- Decide whether you wish to participate