IdP - Best Current Practices

AAI Info Day 2009

SWITCH

Serving Swiss Universities

Halm Reusser
halm.reusser@switch.ch

Berne, 5. May 2009

Idea & Motivation

- AAI Service Agreement and AAI Policy form the ground rules for the federation.
  - AAI Policy uses rather vague and general terms.
- Need for more substantial requirements and recommendations, also for better guidance
- Collected best current practices for operating an Identity Provider in SWITCHaai.
- Basis for a future check list for *self audits* specifying *a service level for IdPs*
- As a next step: Same for the Service Provider (there are a lot of common requirements and recommendations)

Benefit

- For Identity Providers, it

  specifies a guideline for how to operate the Identity Management service.

- For Service Providers, it

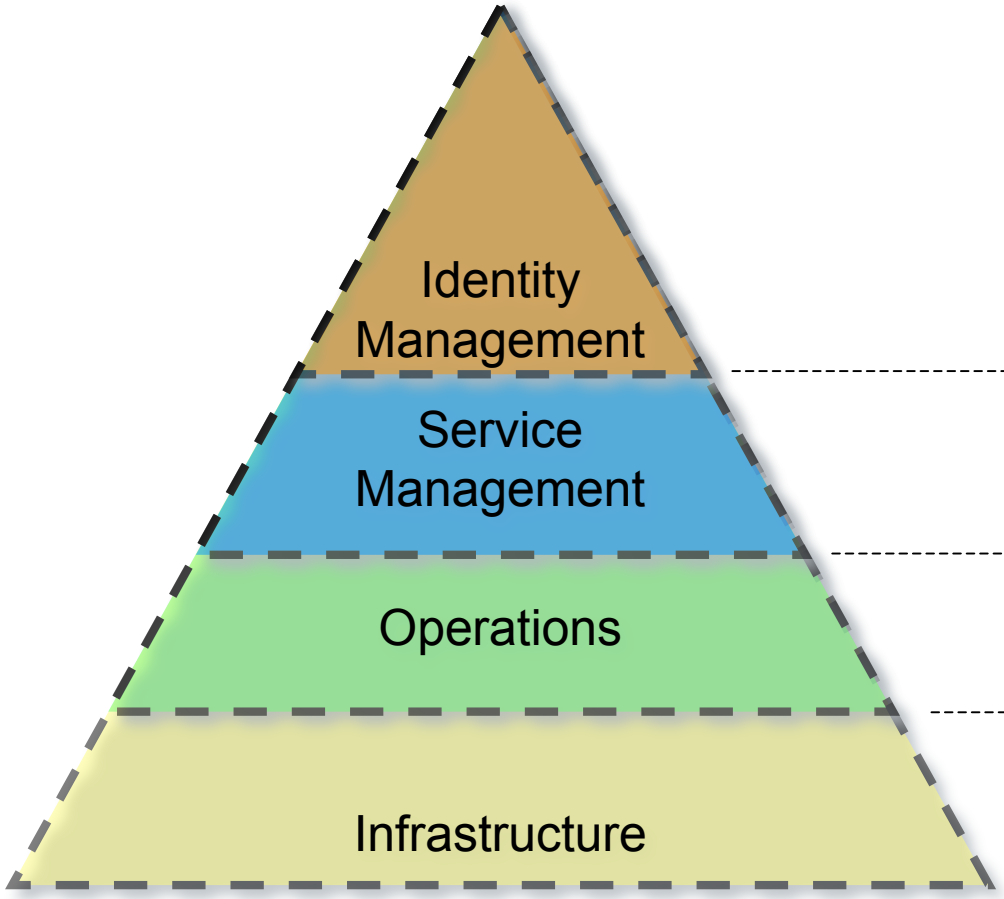
  discloses, what they can expect from Identity Providers.

- For end users, it

  increases the quality of their accounts, and therefore the value of an account.

Document structure & content

Requirements & recommendations about:



- Roles, Data sources, Policies, Compliance, …
- Availability, Support, Reporting, Emergency, …
- Monitoring, Backup/Restore, Security, Documentation, …
- Environment, Network, Hardware, Software, …

Table of contents (Snippet)

Example paragraph: Password Policy

2.3. Policies

2.3.1. Password policy

REQ-12

A password policy must exist and communicated to the staff members and the students.

REC-10

The minimum length of passwords should be 8 characters.

REC-11

The password should be a mix of lower and upper case characters as well as digits and special characters.

REC-12

The password should not be a common dictionary word or a composition of such.

REC-13

It is recommended that a password change be enforced once a year.

REC-14

A password should not be reused within 5 years.

REC-15

A brute-force protection (against login and password changes) should be implemented, which means that an attack against the credentials should be prevented by a time delay for further attempts.

Example paragraph: Metadata

4.8.2. Metadata (SAML)

The metadata provided by the SWITCHaai federation is the most important piece within the AAI. Therefore it should be verified and kept up-to-date. The metadata is signed by the SWITCHaai trust root.

REQ-38

The SWITCHaai federation metadata must be used and must not be changed.

REC-74

Other federation or local metadata may be used, but should be maintained in separate files.

REC-75

It is recommended to update the metadata on an hourly basis.

REQ-39

Metadata must be updated at least 4/6 times per day.

REQ-40

The SWITCHaai trust root must be installed. The trust anchor must be optained in a secure way.

REQ-41

The signature of the Metadata must be verified against the SWITCHaai Metadata Signing certificate.

Resources

- More information and current draft

  → http://www.switch.ch/aai/bcp/

- Feedback is highly appreciated

  → aai@switch.ch