IdP - Best Current Practices
Status Update

AAI Operations Committee, 13. November 2008, Berne

SWITCH

Serving Swiss Universities

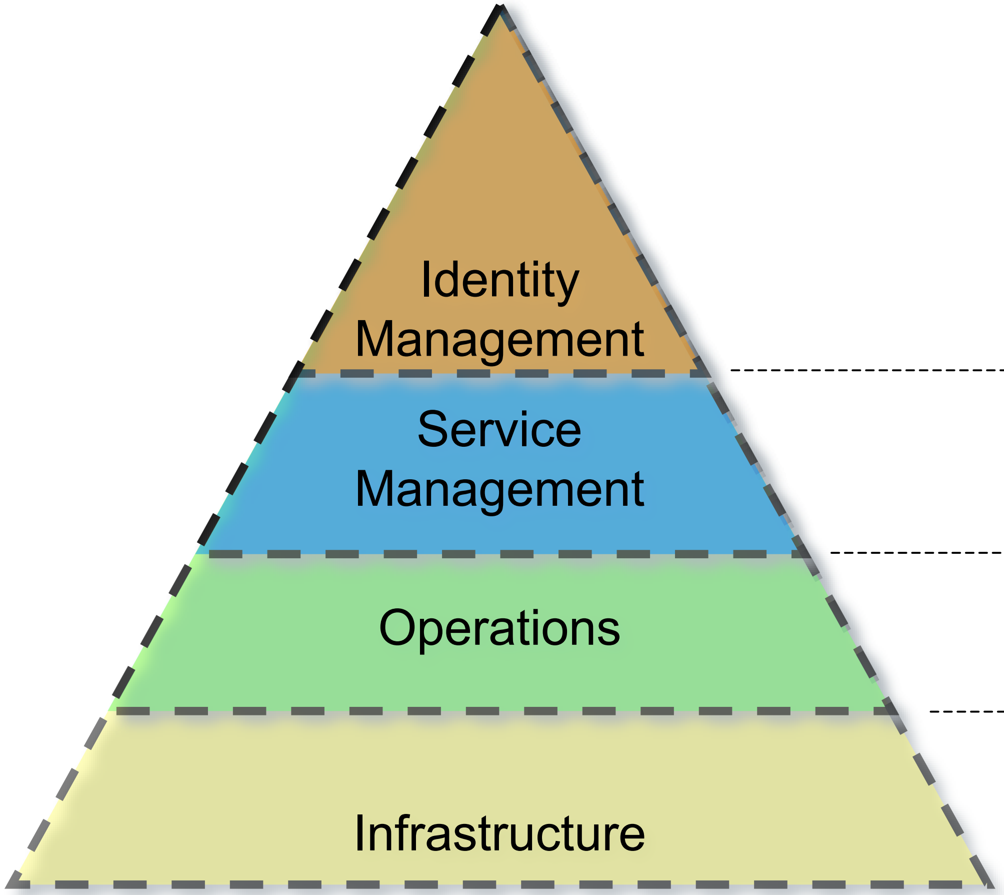
Halm Reusser
halm.reusser@switch.ch

Idea & Motivation
as repetition from OpCom Q2/08

- Collected best current practices about SWITCHaai Identity Provider operations.
- Concretes requirements and recommendations due to the AAI Policy.
- Check list for *self audits* specifying *a service level for IdPs*

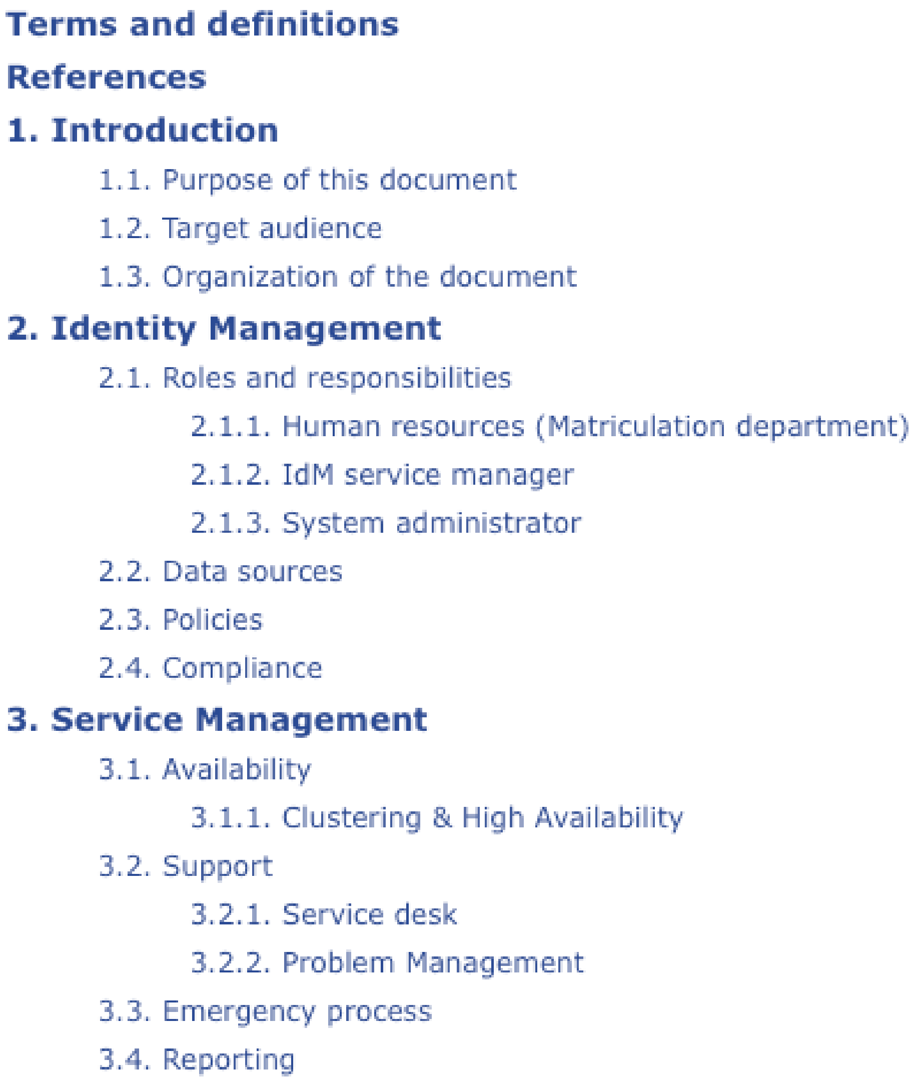
Document structure & content

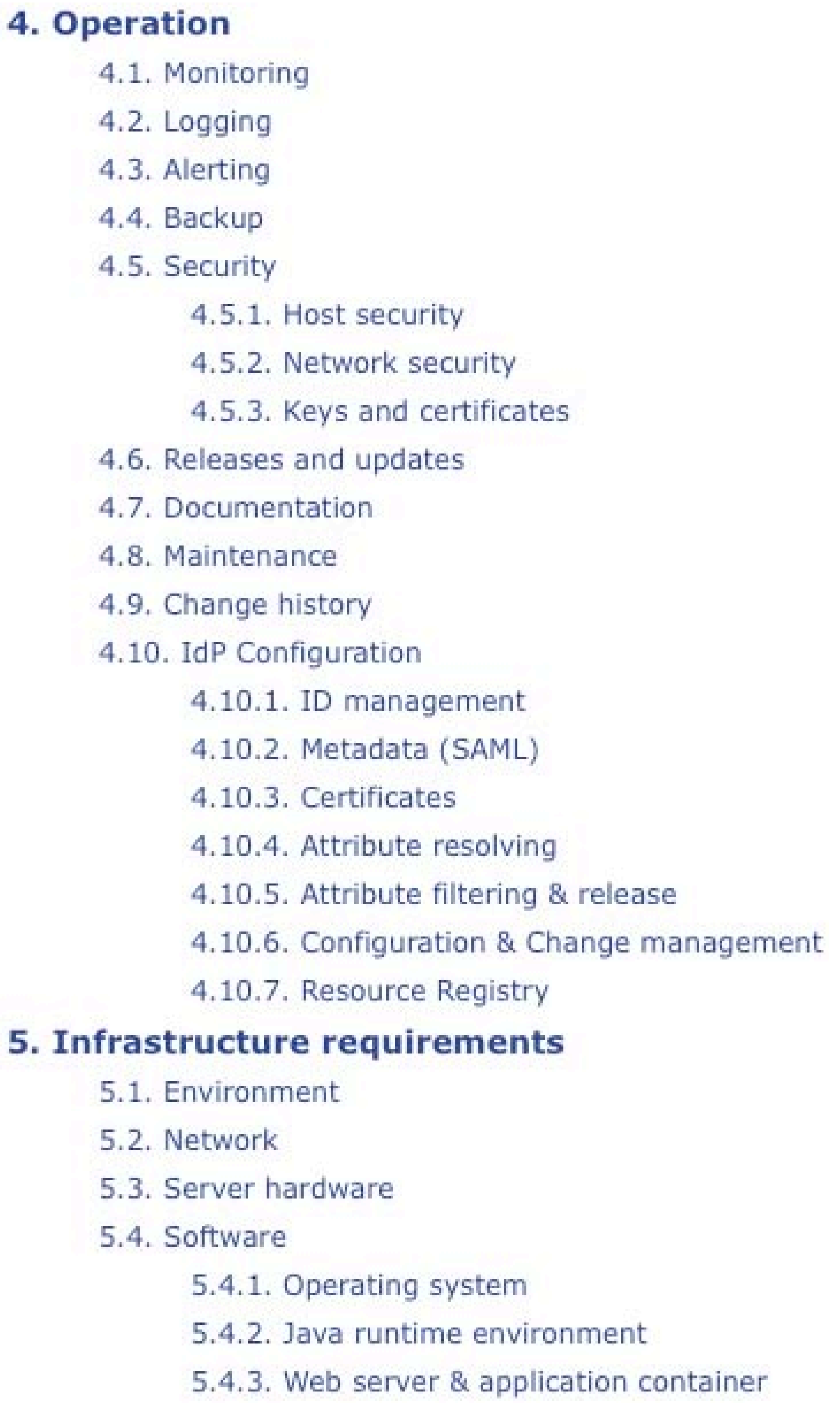
Requirements & recommendations about:



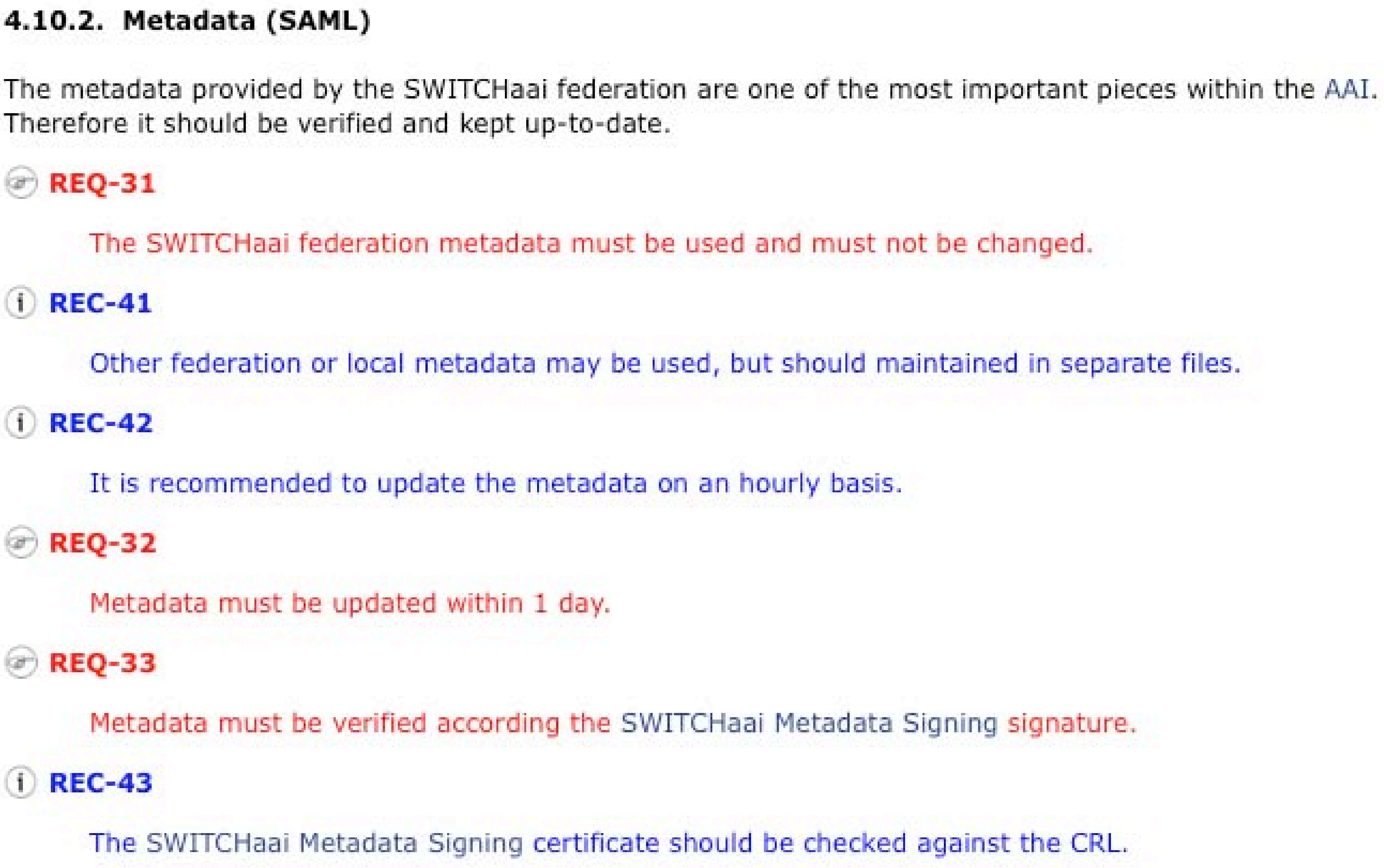
- Roles, Data sources, Policies, Compliance, …
- Availability, Support, Reporting, Emergency, …
- Monitoring, Backup/Restore, Security, Documentation, …
- Environment, Network, Hardware, Software, …

Table of contents





Example paragraph (I)



4.10.2. Metadata (SAML)

The metadata provided by the SWITCHaai federation are one of the most important pieces within the AAI. Therefore it should be verified and kept up-to-date.

REQ-31

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

REC-41

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

REC-42

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

REQ-32

Metadata must be updated within 1 day.

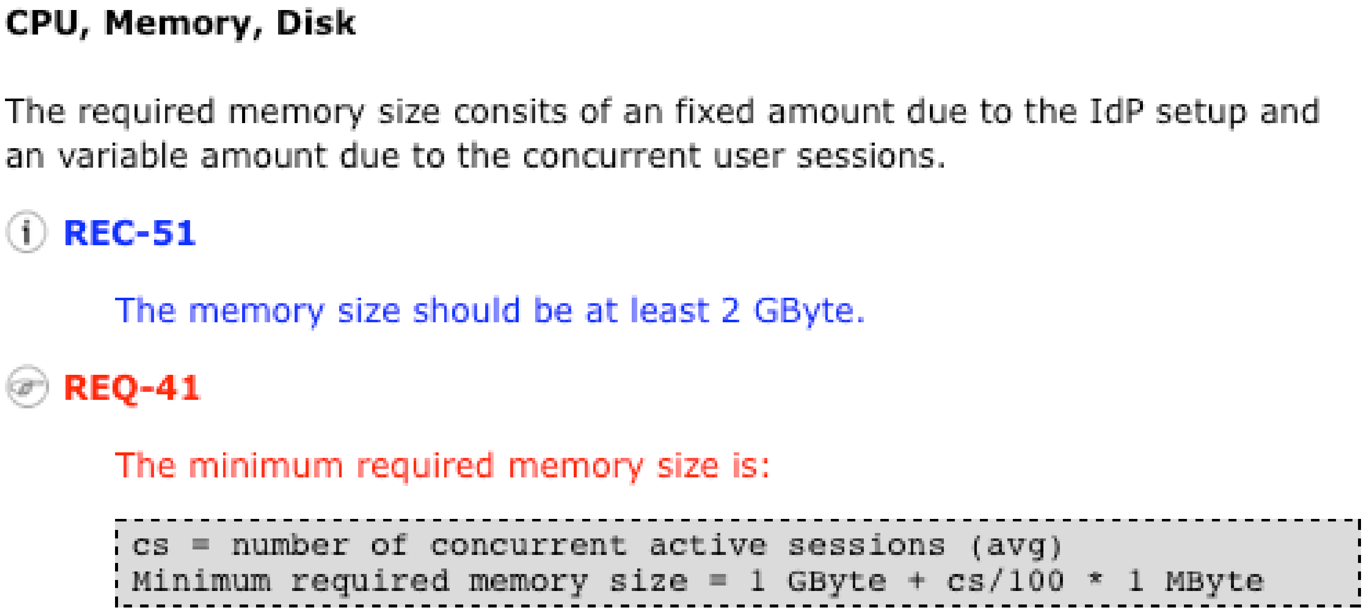
REQ-33

Metadata must be verified according the SWITCHaai Metadata Signing signature.

REC-43

The SWITCHaai Metadata Signing certificate should be checked against the CRL.

Example paragraph (II)



CPU, Memory, Disk

The required memory size consits of an fixed amount due to the IdP setup and an variable amount due to the concurrent user sessions.

ⓘ **REC-51**

The memory size should be at least 2 GByte.

☞ **REQ-41**

The minimum required memory size is:

```
cs = number of concurrent active sessions (avg)
Minimum required memory size = 1 GByte + cs/100 * 1 MByte
```

Work progress and current state

State after OpCom meeting Q2/08:

- Draft of a table of contents with some keywords to each topic
  → Proposal for document scope in breadth and depth.

⇒ No feedback from the community side.

Current state:

- Some topics are described and enhanced with concrete requirements and recommendations.
- Structure and keywords refined

Next steps

- Finding interested people
  - Who is interested to contribute to or review the document?
  - Please join the mailing list (last slide)

- Review current draft
  - SWITCH publish document draft and distributed it through the mailing-list
  - Getting feedback from the community about the already described topics
  - Discussions on the mailing list
  - SWITCH maintains the document

- Further tasks
  - Interview (optionally by phone) with people from the community about some concrete topic due to your commitment
  - Interview with some expert units within SWITCH (NOC, CERT, Legal, …)
  - SWITCH announces new releases through the mailing list

Resources

- Current version of the document
  - https://www.switch.ch/aai/docs/BCP-SWITCHaai-IdP/current.html
- Mailing list
  - aai-bcp-idp@switch.ch
  - Web interface: https://lists.switch.ch/mailman/listinfo/aai-bcp-idp/
  - Join by E-Mail: aai-bcp-idp-join@switch.ch
- Document drafts
  - Document drafts are distributed via the mailing list in RTF Format (MS Word revision control)