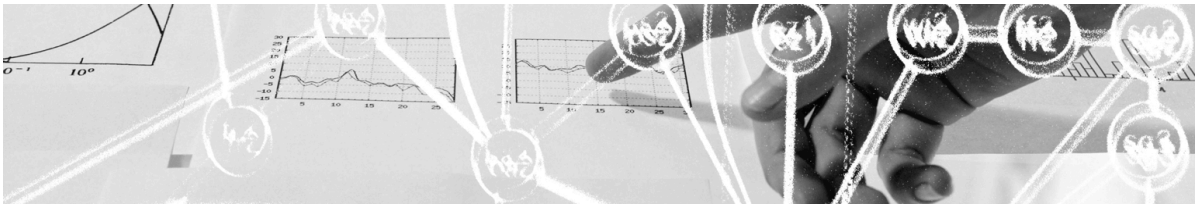
SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

AAI Maturity Scan

Report for pilot phase 2011



Thomas Lenggenhager, SWITCH

Thomas Siegenthaler, Daniela Roesti, CSI Consulting AG

Version: V1.00
Created: 21 September 2011
Last change: 17 February 2012

SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

1 Summary

SWITCH devised a questionnaire to perform an AAI[1] Maturity Scan whose purpose is to enable each Home Organization of the SWITCHaai federation to assess their AAI maturity level. This report describes the results of the pilot phase (phase 1) of this AAI Maturity Scan in which a limited number of Home Organizations answered the questionnaire. It shall also provide to the other Home Organizations sufficient information for deciding about their participation in the main investigation (phase 2) planned for 2012.

The following figure shows the results of phase 1 for the participating Home Organizations (Universität Basel, Université de Fribourg, Université de Lausanne and Fachhochschule Nordwestschweiz).

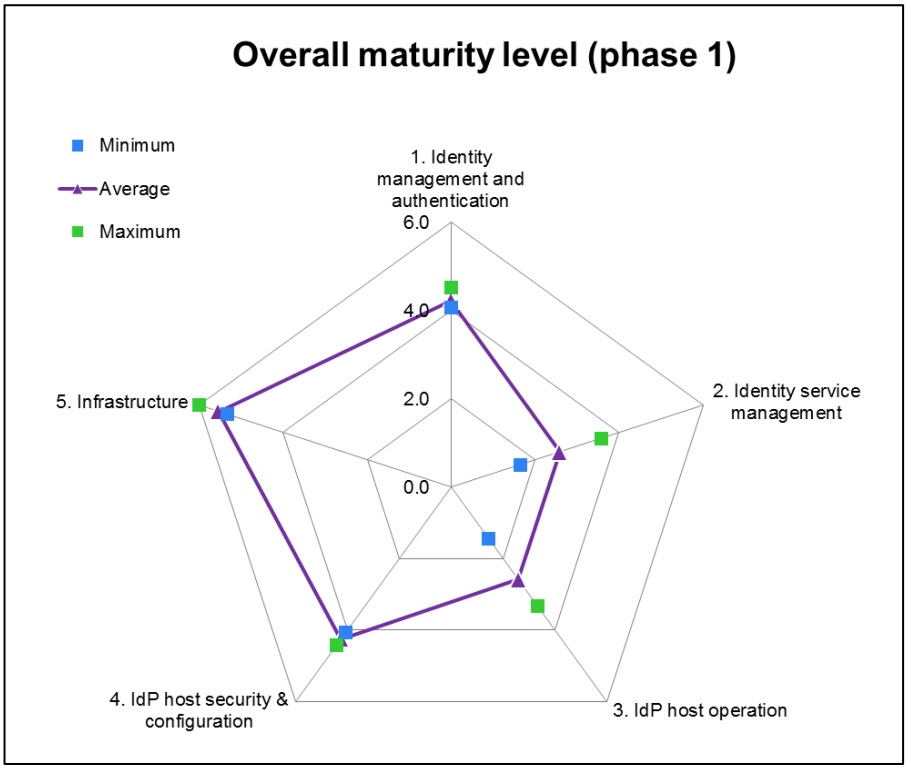


Figure 1: Evaluated maturity level for pilot phase 2011

The strengths of participating organizations are in the areas of 'Identity management and authentication', 'IdP host security and configuration' and 'Infrastructure'. Their identity management can be improved especially in the areas of 'Identity service management' and 'IdP host operation'.

Each participating Home Organization received a detailed report with their results together with recommendations for optimization steps.

Phase 2 will start with the opportunity for all Home Organizations to participate in the AAI Maturity Scan in the second and third quarter of 2012. Home Organizations interested in participating should sign up with SWITCH by 31 March 2012. The interviews of phase 2 will then be scheduled between April and September 2012.

[1] Authentication and Authorization Infrastructure.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

2 Investigation

The purpose of the maturity scan is to gain a better understanding about trust levels of SWITCHaai enabled accounts at volunteer institutions. The investigation is done in two phases:

- Pilot Phase (phase 1)
- Interview Phase (phase 2)

In the pilot phase a questionnaire was developed and tested by interviewing four Home Organizations. The results are an optimized questionnaire and its evaluation tool together with the evaluated maturity level for each organization. It concludes with this report.
In the following interview phase all interested Home Organizations within the AAI federation can take part in the investigation to evaluate their AAI maturity level.

3 Objectives of the maturity scan

In Switzerland, AAI is well established and in production use since 2005. More than 40 Home Organizations are operating an Identity Provider (IdP)[2] in SWITCHaai, so that more than 97% of all higher education users have an AAI enabled account. The identity management is an essential basis for the operation of an IdP. The Service Providers (SP) which protect the access to their web applications trust the IdP and identity management of the corresponding Home Organization.

After having reached good coverage, the next goal is to take a closer look at the quality of AAI. First steps into this direction were the Best Current Practices Documents [1] for operating an IdP and SP within the SWITCHaai federation. As next activity the AAI Maturity Scan is now undertaken, motivated by the experience of a similar study in The Netherlands: In 2009, the Dutch national research and education institution SURFnet performed an identity maturity scan for Dutch universities, which was well received. In the future, optional Identity Assurance Profiles will enable SPs knowing more about the quality of an identity. Identity Assurance Profiles define requirements to an IdP Operator regarding the digital identities it manages and about which its IdP issues assertions.

The maturity scan has three benefits for the administrator of a participating Home Organization:

- Compare the maturity of their identity management with the one of other Home Organizations
- Determine where they can improve their identity management
- Determine their maturity level as a mean to provide Service Providers (SP) an indication on the level of trust they can have towards their Home Organization.

[2] The terminology of SWITCHaai understands the IdP as a software unit, which technically performs the authentication and makes the authentication attributes available to the Service Providers as a SAML assertion.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

4 Participating Home Organizations in phase 1

The following Home Organizations volunteered and enabled the pilot phase. From each Home Organization participated the IdP administrator as well as the IdM service manager or another person involved in identity management:

- Universität Basel, 26th August 2011,
- Université de Lausanne, 30th August 2011,
- Fachhochschule Nordwestschweiz, 7th September 2011,
- Université de Fribourg, 20th September 2011.

The interviews were taken by an interview team, guided by

- Thomas Lenggenhager, SWITCHaai project manager, SWITCH

with the support of

- Thomas Siegenthaler, CSI Consulting AG
- Daniela Roesti, CSI Consulting AG

5 Applied methodology

In order to guarantee a professional IdP operating within SWITCHaai, SWITCH published the document "Best Current Practices for operating a SWITCHaai Identity Provider" (BCP) [1], which contains requirements and suggestions (reflecting best common practices) for the IdP operators. The BCP is the result of a consultation process. SWITCH drafted and edited the document. Volunteers from universities' IT services reviewed the requirements and suggestions. The final version incorporates their feedback. This BCP document was the basis to elaborate the questionnaire [2] for the structured interview. The questionnaire consists of five main criteria:

1. Identity management and authentication,
2. Identity service management,
3. IdP host operation,
4. IdP host security & configuration
5. Infrastructure.

Accordingly, the maturity level consists of five values, which allow a more specific comparison between the different participating organizations.
These five main criteria are composed of sub criteria and their criteria according to the questionnaire. Every criterion was rated with four grades:

6 'fulfilled': all requirements and most suggestions fulfilled[3]
4 'partly fulfilled': requirements/suggestions are partly fulfilled
2 'insufficiently fulfilled': requirements not fulfilled, few suggestions fulfilled
0 'not fulfilled'.

The individual weights of the criteria and sub criteria were determined by considering the amount of corresponding requirements and suggestions in the BCP.

[3] 'All suggestions fulfilled' – in cases where only suggestions (and no requirements) are rated.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

6 Scope of the AAI Maturity Scan

The scope of the identity management maturity scan for AAI is shown below in Figure 2. SWITCHaai is composed of central elements (components and processes), the IdP elements of each Home Organization and all SP elements of AAI Federation Members and Federation Partners. The maturity scan (shaded area) focuses on the IdP elements of the Home Organization and the identity management for all data sources that can be accessed within the Home Organization.

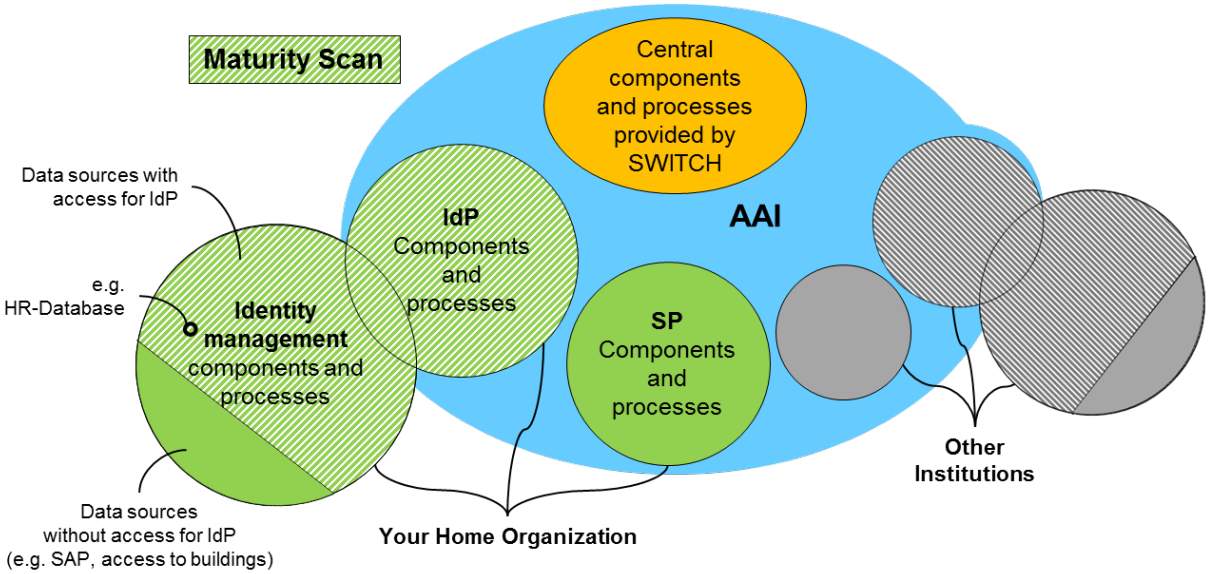
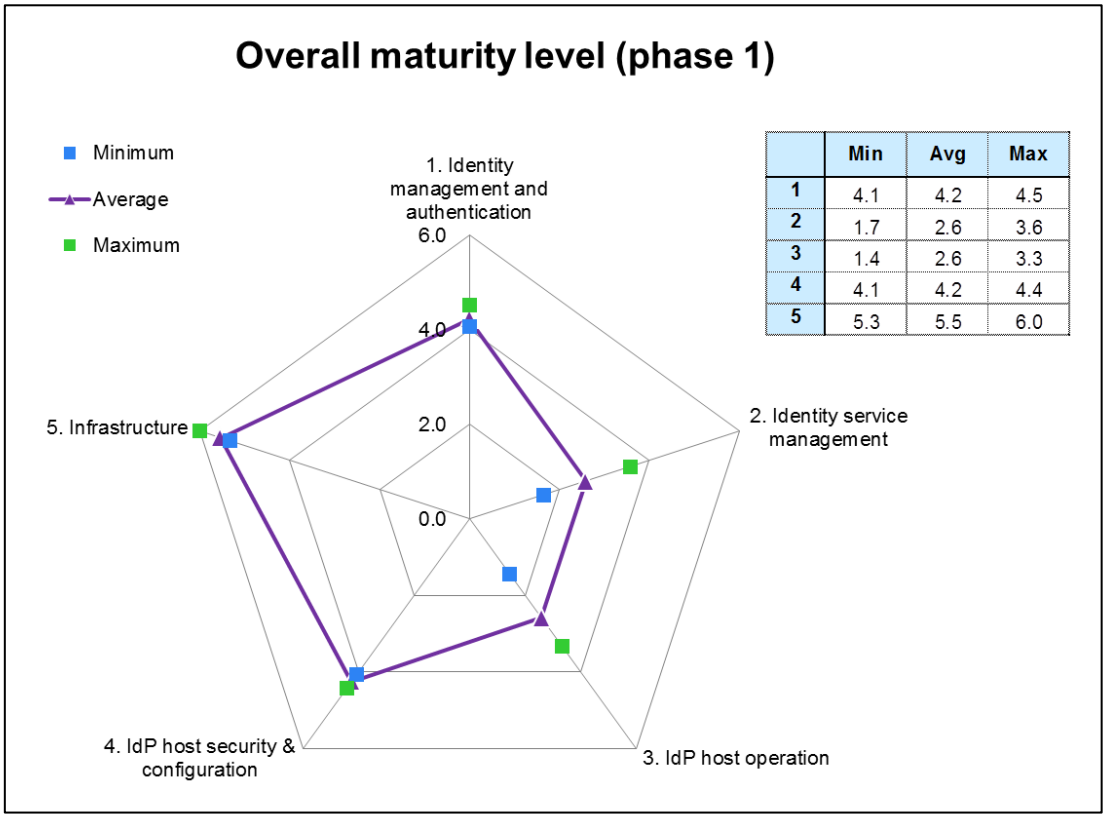


Figure 2: Scope of maturity scan

7 Evaluated maturity levels (results of phase 1)

Figure 3 shows for all five main criteria the average maturity level reached in the pilot phase by the four participating Home Organizations. The minimum and maximum values reached for each main criterion are also shown. A rating value of 4 indicates that the criterion is only 'partly fulfilled' and optimizations are necessary.



	Min	Avg	Max
1	4.1	4.2	4.5
2	1.7	2.6	3.6
3	1.4	2.6	3.3
4	4.1	4.2	4.4
5	5.3	5.5	6.0

Figure 3: Evaluated maturity level for pilot phase (four participants)

According to Figure 3 the best results were reached for the main criterion 'Infrastructure'. The average value is close to 'fulfilled'. Only the server room access control could be optimized in some cases.

The two criteria 'Identity management and authentication' (criterion 1) and 'IdP Host Security & Configuration' (criterion 4) reached average values of only 4.2 (i.e. 'partly fulfilled') which means that optimizations are necessary. Criterion 1's problem areas are: policy, processes, reporting, review and audits as well as strong authentication. Criterion 4's problem areas are: access to IdP, management accounts, process for revoking keys and regular review of the information in the Resource Registry.

The two main criteria 'Identity Service Management' (criterion 2) and 'IdP Host Operation' (criterion 3) reached only weak average values of 2.6 (i.e. 'insufficiently fulfilled') with a considerable variance in the results. Here, optimizations are urgently needed.
Criterion 2's problem areas are: disaster recovery procedure, maintenance windows, service level descriptions and statistical data reporting. Criterion 3's problem areas are: monitoring, alerting, access control to log-files, test of restore procedure and documentation.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

8 Procedure and deliverables

The following procedure was applied in phase 1 together with the below-mentioned deliverables.

Preparation of the interview:

- The Home Organization signs up at SWITCH for the AAI Maturity Scan.
- The Home Organization receives the questionnaire 'Identity Management Maturity Scan for SWITCHaai' and meeting date is set up.
- The Home Organization identifies its representatives. They prepare the interview. During preparation internal consultation may be necessary. However, there is no need to prepare written answers prior to the interview.

During the interview:

- Introduction and first questions to better understand the local environment
- The interviewer elaborates on the questions and ensures that they are properly understood and the answers can be consistently evaluated with respect to the other institutions. The interview lasts at most 3 hours. The Home Organization is typically represented by the two roles 'IdM service manager' and 'IdP administrator'.
- The interview team takes written notes, which are a SWITCH-internal document to support the evaluation procedure. They are not handed over to the Home Organization.

After the interview:

- The interviewing team evaluates the maturity level for all main criteria through a standardized evaluation procedure
- The results are reported in a dedicated 'AAI-Maturity report' which is delivered to each participating Home Organization (see Addendum to this report).

No changes in these procedures are foreseen for phase 2.

9 How to participate in phase 2?

SWITCH distributes this report to all Home Organizations of SWITCHaai in order to raise their interest in participating in phase 2 of the investigation (interview phase).

It is planned to undertake phase 2 of the AAI Maturity Scan with the same objectives and the procedures as described in this report.

Home Organizations interested to participate should sign up with SWITCH until 31 March 2012. The start for phase 2 is scheduled for second quarter 2012.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

10 Referenced documents

[1] ‘Best current practices for operating a SWITCHaai Identity Provider’
see: http://www.switch.ch/aai/bcp
[2] Questionnaire of the Identity Management Maturity Scan for SWITCHaai
see: http://www.switch.ch/aai/docs/Maturity_Scan_Questionnaire.pdf
[3] AAI-Website
see: http://www.switch.ch/aai

SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Addendum

Structure of the report 'AAI Maturity Scan' delivered to the Home Organization

The report delivered to the Home Organization contains its evaluated maturity level with a spider graph like in Figure 3 and specific recommendations to the Home Organization for improvements and has the following structure:

1 Summary
2 Interview
3 Objectives of the AAI maturity scan
4 Applied methodology
5 Scope of the AAI maturity Scan
6 Evaluated maturity scan
7 Recommendations for improvements
7.1 General recommendations
7.2 Specific Recommendations for the Home Organization
8 Referenced Documents
9 Appendix

The Appendix chapter contains a detailed overview of all criteria which have been rated as 'insufficiently fulfilled' such that the Home Organization can evaluate their own measures for improvements. The following is a sample how the chapter 9 (appendix) of the report looks like. The table below shows as example how the specific recommendations for criterion 3 'IdP host operation' could look like.

3. IdP host operation

Criterion	Recommendation
3.1.2	Alert if CPU, memory or disk usage exceeds 60, 80 resp. 75%. (S071-73)
3.1.4	Monitor webserver log files. (R076)
3.1.5	Monitor application container log files, IdP log files and data source log files for error or warning entries. (R077 and S078)
3.2.1	Ensure by documentation and verify that only permitted staff have access to the log files regularly. (R083)
3.2.3	Define a process which ensures that user identifying data is anonymized when copies of log files leave the organization. (R088)
3.3.2	Ensure that backups are stored in an offsite and secure location. (S093)
3.3.3	Test the restore procedure at least twice a year on your IdP. (S095)