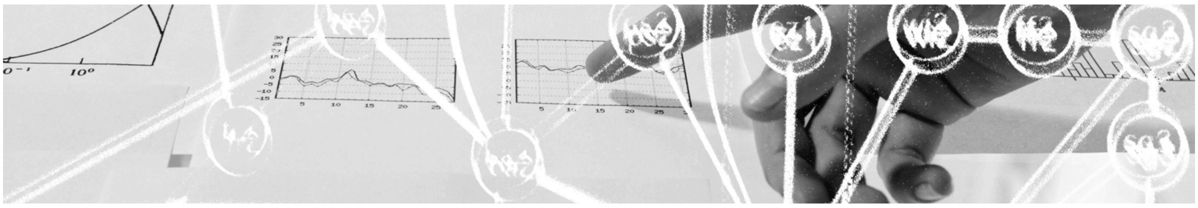
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Towards Swiss edu-ID 2.0

RFI (Request for information) procedure and results



Christoph Graf and Rolf Brugger (Project Manager E-Identity, SWITCH)
Rolf Grau and Andreas Grommek (CSI Consulting)

Document Type:	Documentation
Version:	V1.0
Created:	22.09.14
Last changes:	05.02.15
Classification:	Public

Content

1 Purpose of this document

This document describes procedure and results of the Request for Information (RFI) carried out for gaining necessary insights to plan the next phases of the Swiss edu-ID project[1].

SWITCH may base strategic decisions for the next steps on the results of this RFI, which may include adopting proposed architectures as requirement in a potential future RFP. This document must, however, not be understood as an indication that there will be any Request for Proposal (RFP).

2 Target audience

This document focuses primarily on informing the SWITCH Community about the RFI.

3 RFI Procedure

3.1 Members of the Review Team

Name	Specific Field
Graf Christoph, SWITCH	Project Manager Swiss edu-ID
Brugger Rolf, SWITCH	Deputy Project Manager Swiss edu-ID
Grau Rolf, CSI	Senior Consultant
Grommek Andreas, CSI	Consultant
Hämmerle Lukas, SWITCH	Integration
Hassenstein Gerhard, BFH	Engineering and Information Technology & Representative of the SWITCH Community
Lenggenhager Thomas, SWITCH	Attribute Specification
Witzig Christoph, SWITCH	Head of Central ICT Providers

Table 1: RFI reviewers

[1] A federated identity management solution for the SWITCH Community, building on the existing SWITCH authentication and authorization infrastructure (SWITCHaai): http://projects.switch.ch/eduid/

3.2 Steps and deadlines

No.	Step	Deadline
01	Announcement of RFI to potential RFI-participants	30.10.2014
02	Publishing of RFI through E-Mail and on SWITCH web site	03.11.2014
03	Reception of questions from RFI-participants	11.11.2014
04	Answering of anonymized questions to all RFI-participants	14.11.2014
05	Deadline for answering RFI	28.11.2014
06	Select subset of participants to give a presentation on their answers to SWITCH	04.12.2014
07	Presentations by subset of participants	08. – 12.12.2014
08	Consolidate additional information gained from the RFI	19.12.2014

Table 2: RF steps and deadlines

3.3 Parties interested in the RFI

Starting from a market overview a first list of potential RFI participants was compiled, based on the contact and partner information of their respective web sites. In the case that several partners were listed,

- Swiss partners or otherwise EU-partners were preferred, mainly due to the data protection requirements.
- Partners were preferred whose core competency is identity and access management as integrator and operator; partners specialized in training only were discarded.

Apart from specifically inviting some companies identified through the product sites, the RFI [2] was published on the SWITCH web site, and announced on social media channels.

3.4 Questions and answers regarding the RFI

RFI-participants asked several questions during the RFI-process, which were answered in an anonymized clarification document [3].

4 RFI Outcomes

4.1 Overview of answers and selection for presentation

11 companies handed in a solution proposal (one of them even two).

Through a pre-assessment based on suitability criteria (see chapter 4.2) 5 companies were selected to personally present their proposal.

4.2 Suitability

The answers of all the RFI-participants were compared with regard to the following suitability criteria:

- Licensing model
- Costs: project, operation, and TCO over a period of 5 years
- Benefits
- Risks, drawbacks
- Long-term sustainability of the solution presented
- Time required for implementation
- Possible Legal & Compliance issues

The final presentations were further analysed with regard to

- Suitability of each of the major components, as outlined in section **Error! Reference source not found.**
- Estimated integration effort into SWITCH (complexity, time necessary)
- Major benefit
- Major drawback, risk
- Possible showstopper
- Preferred operation model

The following solutions were shortlisted and further analysed:

1. Solution based on an integrated product covering access management and identity management, which was initially developed for serving financial institutions
2. Solution based on Shibboleth with third party extensions to address missing functionality
3. Solution based on commercial open source product for both access management and identity management
4. Solution based on an integrated configuration and operation frontend for many open source components including Shibboleth
5. Solution based on a comprehensive framework of access and identity management components

The following table summarizes the outcome after final presentations:

Solution:	1	2	3	4	5
Overall costs	High	Low-medium	Low-medium	Medium	High
Drawback	Acceptance of approach in SWITCH Community questionable Vendor lock-in Monolithical approach	Missing professional services Missing features Custom software developments necessary	Unknown compatibility of AM with current SWITCHaai infrastructure	Missing professional services US-focus Unclear sustainability of component	Considerable integration efforts necessary
Strength	Complete solution stack Common administration of functional blocks Professionalism Quality	Solution based on Shibboleth Seamless migration path Familiar with academic IT solutions	Supports many auth protocols Complete IdM/AM software stack Widely used in academia	Includes Shibboleth Supports numerous auth protocols Common admin	Modular architecture Huge number of pluggable modules
Suitability	++	+++	+++	+	+

Table 3: Summary of RFI outcome

4.3 Risks

The following major risks have been identified for Swiss edu-ID:

Risk	Measures
Acceptance problem of a centralised solution: SWITCHaai and Swiss edu-ID are based on a decentralised model, but the Swiss edu-ID is centralising certain elements.	The involvement of identity managers at Swiss universities will be sought in all stages of development of standards and services.
Difficulties to validate users initially: This is not well supported by e-Government processes in Switzerland in an automated manner.	SWITCH will seek expert advice on this topic. New ID Card ’17 is promising, but not short to medium term. Involvement of Universities is crucial.
Integration problems with business processes within universities: Changing registration processes is complex and time consuming.	Addressing registration processes needs to start as early as possible and was a topic in the processes working group.

Risk	Measures
Too low coverage of users (acceptance issue): This is a precondition for service providers to settle on one identity solution for our community.	SWITCH to monitor carefully acceptance level to be able to address such issues in a timely manner.
Low number of available resources for former students: Attractive service portfolio important for adoption.	Good technical support and attractive models for simplified administrative processes for resource owners.
Challenging mobile integration: A shortcoming of SWITCHaai is missing support for non-web and mobile platforms.	The Swiss edu-ID v2.0 is required to support OAuth2, the most promising standard for integration of non-web and mobile platforms.
Single point of failure: The centralized architecture could be a single point of failure, if not well designed. In this case, SWITCH Community members may not be able to work during an outage.	Design a redundant highly available infrastructure, both in technology and processes.

Table 4: Main risks identified during the evaluation of the RFI

5 Recommendations

5.1 Most promising option out of RFI-answers

As outlined in section 4.2, of the answers to the RFI the most promising options seem to be

a) Solution 2, which basically builds on current SWITCH Shibboleth infrastructure, and

b) Solution 3, building on commercial open source product ForgeRock, which would mean changing the system completely.

In the case that SWITCH decided to rather gradually develop the existing SWITCHaai infrastructure, individual components of ForgeRock could be evaluated for providing e.g. for the identity management part of the system.

5.2 Impacts on the Swiss edu-ID Architecture

In addition to identify viable solutions, the RFI gave the opportunity to validate the Swiss edu-ID high-level architecture [1]. If the concepts of the high-level architecture cannot be put in practise with existing products it would have to be revised. Yet, the solution providers confirmed the overall soundness of the Swiss edu-ID high-level architecture and the requirements derived hereof.

The topic of attribute aggregation turned out to be particularly demanding. In a first phase of the Swiss edu-ID it is therefore recommended to maintain a high level of compatibility with the existing SWITCHaai infrastructure. Users with multiple identity contexts (roles) select a preferred context for each service in the user consent process. This makes sure that a service only sees the attribute set of a single role. In a later phase, and if required, attributes of multiple contexts could be merged into a single structured attribute set that complies with a new attribute model.

5.3 Milestones and time frame for implementation

The following table shows the basic steps to be carried out during an implementation project.

Overall duration until go-live for the Swiss edu-ID with an initial group of SWITCH Community members and service providers: 12 to 18 months.

Milestones		
No.	**Work package / project phase**	**Duration**
1	Detailed analysis of the requirements.	1 month
2	Specification of use cases, processes and interfaces.	1 month
3	Design: Specification of data model and technical infrastructure to support the use cases defined in step 1. The use cases also include the details of parallel operations with the existing SWITCHaai infrastructure. Security analysis.	1 month
4	Proof of concept during technical specification phase: Start with a prototype installation to verify the key use cases and data model assumptions, usability, scalability, availability, and security.	1 month
5	Decide on target architecture and carry out procurement incl. RFP	4 months
6	Building of the solution based on the specification and insights of steps 1 to 4.	3 months
7	Testing, incl. stress- and integration-test with SWITCHaai.	2 months
8	Start of a pilot phase with a set of well-selected services and organisations (SWITCH Community members and SWITCH partners).	3 months
9	Improvement phase for shortcomings detected during pilot operations.	2 months
10	Step-wise rollout and parallel operations of SWITCHaai.	3 months for each new entity (can be carried out in parallel)

Table 5: Implementation procedure milestones

Training

Alongside: initially for SWITCH to understand product, later on for SWITCH Community to understand new solution.

Assumptions

Hardware platforms, network security systems, databases and attribute providers are deployed by the customer in time.

A Appendix

A.1 References

[1] "Swiss edu-ID High-Level Architecture", SWITCH, 24.07.2014:
http://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/SwissEduID_hla_summary.pdf

[2] "RFI Swiss edu-ID", SWITCH, 31.10.2014:
http://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/Swiss_edu-ID_RFI.pdf

[3] "Questions received until Nov. 11 2014 and clarifications", SWITCH, 17.11.2014:
http://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/Swiss_edu-ID_RFI-Clarifications_2014-11-17.pdf

[4] Document section of the Swiss edu-ID web presence, SWITCH:
http://projects.switch.ch/eduid/documents/