Swiss edu-ID with Shibboleth

A study on building the Swiss edu-ID platform based on Shibboleth or deploying a commercial AM module

Gerhard Hassenstein
Version 1.1

Bern University of Applied Sciences
Engineering and Information Technology
Institute for ICT-Based Management

Version control

Version	Date	Description	Author
0.1	14.01.2015	Initial document	Gerhard Hassenstein
0.8	23.01.2015	Extended version after feedback of CSI-Consulting	Gerhard Hassenstein
0.9	28.01.2015	First version for internal review	Gerhard Hassenstein
1.0	29.01.2015	Adapted version after meeting with SWITCH	Gerhard Hassenstein
1.1	30.01.2015	Final version after feedback by Christoph Graf (SWITCH)	Gerhard Hassenstein

Contents

1. Initial position

Based on the High-Level Architecture Document [1] and the different concepts presented by the Request for Information solution provider [2] some conclusions for a more specific concept begin to emerge.

- The Swiss edu-ID should be gradually developed on the basis of the existing AAI infrastructure.
- A disruptive migration to a new platform might be too risky and would not be accepted by the community.

An alternative option to consider (beside the conceptual and technical approaches, presented by the RFI supplier) might be the development of a Swiss edu-ID platform based on Shibboleth, as the existing SWITCHaai-infrastructure already is.

This study considers itself as an add-on to the detailed RFI report and takes a closer look at the question whether and, if so, how Shibboleth may be used as a central AM component for the Swiss edu-ID platform.

2. Principal objectives

In this section we summarize the main goals and requirements for the Swiss edu-ID that must be primarily covered by any solution. With a Swiss edu-ID the identity management for federated services will become more user-centric and less organization-centric. The main component for this change is a set of new centralized Swiss edu-ID services, like:

- maintaining central identities of the users
- storage of a set of long-term core user-attributes
- support of different authentication methods
- querying and aggregating additional user-attributes from participating organizations (e.g. universities) in a timely close manner.
- supporting connections for non-web resources and mobile applications

3. Working assumption

With this proposal we focus on the AM functionality of the Swiss edu-ID infrastructure because Identity Management (IdM) is not covered by the Shibboleth Identity Provider. Consequently any provisioning of user information (e.g. attributes or credentials) between the Swiss edu-ID platform and the existing AAI-infrastructure is out of scope of this study. This issue must be discussed in the context of an Identity Management evaluation. The AM part of Swiss edu-ID uses favorably a Directory to store user-account information. It is therefore reasonable to select an Identity Management System, which also supports a Directory as primary user database. For this study we presume, that all relevant user data has to be written to/and can be retrieved from a Directory.

In this document we distinguish between *definition-time* and *run-time* as specified in *eCH-0107 "Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)"* [3].

Definition-time: covers all administrative tasks of a user (or administrative person) to create or manage its identity, establish links to external identity or attribute providers, etc.

Run-time: includes the process where a user is authenticated by the Swiss edu-ID IdP, its collection and aggregation of attributes from external sources as well as the return transfer to the requesting application.

4. Proposal for a Shibboleth-based solution

With a high probability we can assume that both Service Provider and Identity Provider of SWITCHaai remain mainly unchanged (except for minor adaption or configuration tasks) in order to be integrated in a Shibboleth-based Swiss edu-ID infrastructure. The protocols used between SP and the Swiss edu-ID Identity Provider as well as the communication to link Identities or to query attributes are plain vanilla SAMLv2 and may be covered by standard Shibboleth IdP and SP components. The main development to fulfill the essential objectives must be done at the Swiss edu-ID IdP/AA side.

Starting from Swiss edu-ID V1.0, we will present a Shibboleth based development path to a Swiss edu-ID platform, which fulfills the main objectives summarized in section 2. The following sections will point out the added functions and components assembled in packets, beginning with the currently being elaborated Swiss edu-ID Version 1.0. The packets do not have strong dependencies and do not need a fixed schedule, so that they can be developed in parallel or in different order.

4.1 Initial version

Swiss edu-ID V1.0 is an initial version to enable students to register a master educational identity before ending their studies to give them continuing access to selected resources. The Swiss edu-ID Identity Provider is a registered IdP in the Resource Registry (RR) and appears in the Discovery Service (DS) list of any AAI-Resource.

With this version (which is still work in progress and should be ready for release in Q1 2015) users have the possibility to register themselves directly on the Swiss edu-ID platform. If a user already has an existing AAI-Account he may link this Identity to his Swiss edu-ID (AAI-Linking). Within this process the Swiss edu-ID platform will also obtain a list of specific attributes of this user from the AAI-IdP. This gives the opportunity to easily bootstrap the Swiss edu-ID account with already verified and confirmed user information.
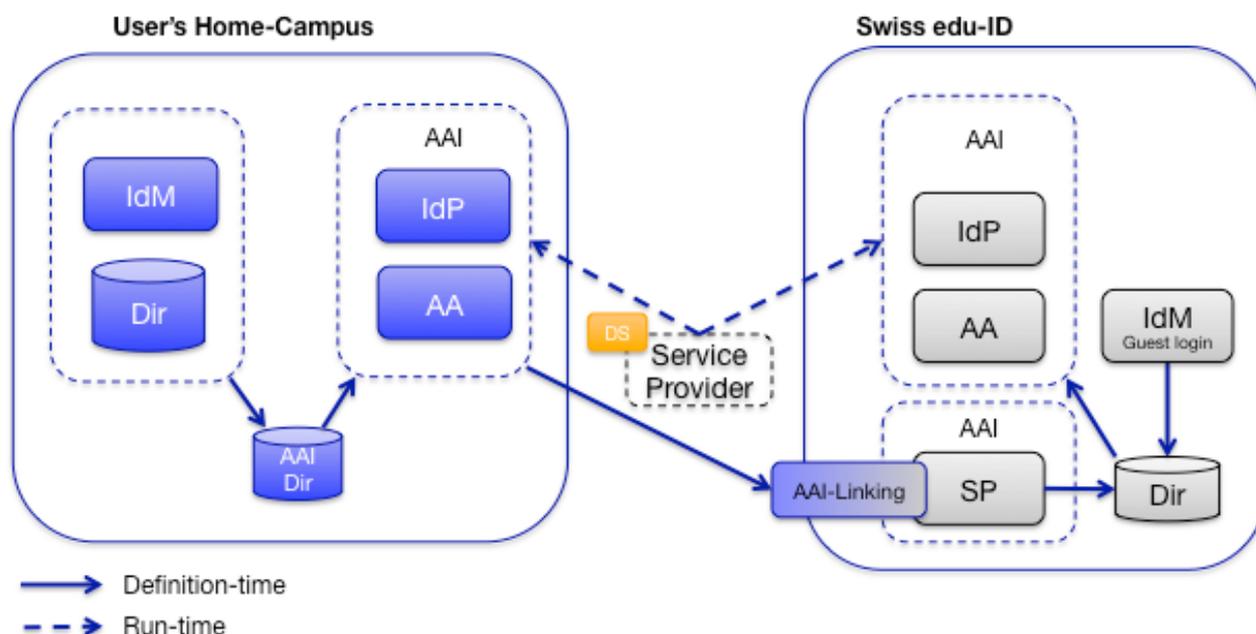

Figure 1: Swiss edu-ID V1.0

Figure 1 depicts the relevant components of the initial Swiss edu-ID V1.0. Special feature is the AAI-Linking, which enables the bootstrapping of the Swiss edu-ID with AAI-based user information. These personal attributes (as well as some data in the organizational context) will be added to the Swiss edu-ID user database (DIR).

4.2 Swiss edu-ID and OAuth2/OIDC support

At this point we would like to state some consideration about the timeline of Swiss edu-ID supporting communication for non-web resources and mobile application in the future. There is no doubt about the need to implement this feature as soon as possible. This objective could be achieved by implementing an AM-stack that already supports OAuth2 and OpenID Connect (OIDC). But if we adhere to Shibboleth as core component for the Swiss edu-ID platform, the integration of OAuth2 and OIDC might not be realized before 2016. The implementation of OAuth2 and OIDC support could also be achieved by a third party solution beside Shibboleth, but this could render unwanted software dependencies and may complicate further development. The implementation of these protocols should therefore be part of a single software stack and Shibboleth - beginning with V3.0 - is designed to support other protocols beside XML-based SAML. Therefore we suggest starting with Shibboleth V3.0 as software base for the development of additional software components for the Swiss edu-ID platform.

Based on these considerations we recommend the following packaging to develop additional functionalities in Shibboleth to realize Swiss edu-ID:

Version/ Package	Features	Swiss edu-ID Components
V 1.0	• Establishing a Master ID (Swiss edu-ID) • A user has only one role per Swiss edu-ID • Linking AAI-ID • Swiss edu-ID provides basic attributes (given name, surname, e-mail address, etc.)	• Shibboleth IdP/AA V2.4 • AAI-ID Linking • Simple Identity Management
Package 1	• Linking other external ID's (e.g. ORCID Google, Facebook, SuisseID, etc.) • Swiss edu-ID provides basic attributes and attributes of affiliated AAI-IDs. • A user may have more than one role per Swiss edu-ID.	• Identity and Attribute Provider Linking • Shibboleth IdP/AA V3 with: o Extended 'attribute filtering' and extended 'attribute resolver'. o Aggregation of attributes from different sources.
Package 2	• Support for additional authentication methods (e.g. SuisseID, OTP-Authenticator, FIDO, Mobile-ID, etc.) • Step-up authentication relative to a Level of assurance (LoA) requested by SP.	• Shibboleth IdP/AA V3 with: o Extended Login handler o External authentication plugins o Step-up authentication feature
Package 3	• Support for non-web resources and mobile application.	• Shibboleth IdP/AA V3 with: o Support for OAuth2/OpenID Connect

Table 1: Swiss edu-ID development packages

4.3 Development Package 1
In all development stages the existing AAI-infrastructure and the Swiss edu-ID remain independent, but fully interoperable. A user, requesting access to a service provider may always select the local AAI-IdP or the new Swiss edu-ID IdP to authenticate himself. The Discovery Service (DS) mainly remains embedded in the application or may optionally be part of the Swiss edu-ID platform. Which one of the Discovery Services is used, depends on the configuration of the Service Provider.

4.3.1 Identity and Attribute Provider Linking
As already described in section 4.1 AAI-Linking enables the Swiss edu-ID platform to acquire specific attributes of a user from the IdP of the user's home organization at definition-time for better bootstrapping the master Identity. Within package 1 this functionality shall be extended to enable "backchannel attribute queries and aggregation" during run-time. The *Identity and Attribute Provider Linking (IAPL)* is a user initiated process, which enables the Swiss edu-ID platform to retrieve a confirmed identifier of the remote user account, which afterwards has to be stored in the Swiss edu-ID user database as a unique linked-ID. IAPL uses standard SAML Authentication Request/Response messages, in which the AAI-IdP returns an identifier of the locally authenticated user. The same component could also be used to link other SAML Identity Provider (e.g. SuisseID).
Additionally this component should extend linking of external Identities over OAuth2 [4] for other Authorization Servers (e.g. ORCID, Google, Facebook, etc.). In this scenario, users must have to authenticate first to an authorization server (e.g. ORCID), which then issues an access token to a third-party client (e.g. the Swiss edu-ID platform) with the approval of the resource owner. During this process the third-party client will receive the user's ORCID-ID (one will be created automatically if it does not already exist) and may ask the user for permission to access limited information of his records. The third-party client must have a registered Client-ID with the Authorization Server prior to use this service.
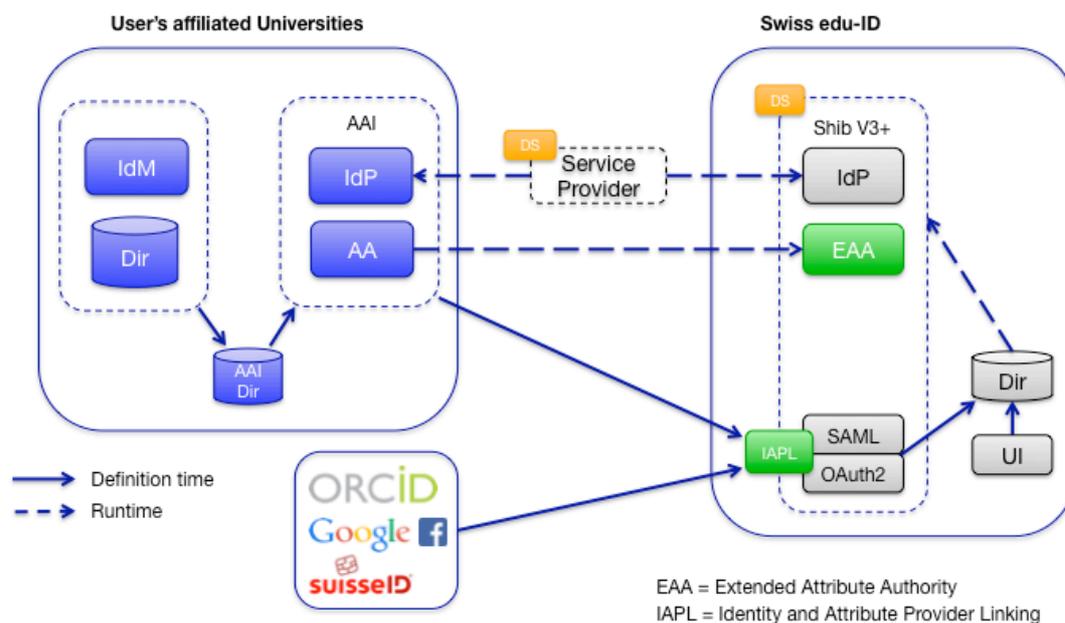
Figure 2: Development Package 1

4.3.2 Extended Attribute Authority

A main part of this package is the *Extended Attribute Authority (EAA)*, which is capable to query AAI-attributes of a user during run-time. This attribute query is running as backchannel communication and takes place without user/browser participation. With this feature it is possible to retrieve attributes of a user from different sources (Attribute Authorities of Home Organizations) and aggregate them together with basic attributes stored in the central Swiss edu-ID directory. For this option the Shibboleth 'attribute resolver' and 'attribute filter' components have to be extended. Proposed Shibboleth process for authentication and extended attribute aggregation:

1. Authentication by Shibboleth "Login Handler" (e.g. Username/Password)
2. Based on the requested set of attributes (defined in Resource Registry) and the attribute release policy an extended "Attribute Filter" selects the appropriate list of to-be aggregated attributes on behalf of the user's affiliated Attribute Providers (previously linked by the user in its database).
3. An "Extended Attribute Resolver" then retrieves and aggregates attributes from the local Swiss edu-ID directory and from the affiliated Attribute Providers.
4. Attribute consent processing.
5. Response builder.

Additionally to the development of the EAA core component, some software and configuration adaption has to be done at the Attribute Authority's side.

4.3.3 Aggregating attributes of different sources

A user may have more than one role in the same organization (e.g. student/employee) or may have affiliations to more than one organization. A user shall be allowed to tie all those remote Identities to his Swiss edu-ID. The reflection of this situation for the Swiss edu-ID platform and for a requesting application might be quite tricky. The simplest way to face this problem is 'let the user choose the appropriate role to be transferred to the application'. In this case the Swiss edu-ID Identity Provider must present possible roles (e.g. in form of an icon of the affiliated organizations) to a user as part of the authentication process. The "Extended Attribute Resolver" will retrieve only attributes from the chosen Home Organization and the selected role and then passes them on to the application. Attribute aggregation of more than one affiliated Home Organization of a user at the same time will be more elaborate to implement. How do we express the merging of a specific attribute of two different sources e.g. user has an affiliation *staff at UZH* and *student at ETHZ* in one response to be sent to the requesting service provider? One solution could be, to use a specific set of attributes with a kind of multivalued scoped semantic. Another approach could be to enhance the attribute assertion syntax as part of the response addressed to the service provider. In this case the Assertion Consumer

Service (ACS) component of the Service Provider need to be adapted in order to be able to disassemble and verify the response. Any way – attribute aggregation of more than role per session must be studied and discussed much more in depth.

4.4 Development Package 2

Another feature set of the Swiss edu-ID may be the extension of the Identity Provider to support additional credentials for user login. The basic authentication method must remain username/password as long as this is the standard in the community. The next few years will reveal which technology becomes more and more established on the market, as an alternative solution for basic username/password authentication.

Possible candidates, who may achieve certain significance for Swiss eID's might be:
- SuisseID (used as 2-way SSL/TLS authentication credential) [5]
- FIDO Alliance U2F/UAF Authenticator Token [6]
- Several OTP-based Authentication methods (Google Authenticator, Yubikey) [7]
- Mobile Signature Service ETSI TS 102 204 based authentication scheme [8] like Swiss Mobile-ID provided by Swisscom [9], Orange and Sunrise.

Most of these methods provide 2-factor authentication (2FA). In general 2FA is not needed for daily access of standard applications. But there will be other providers, which may require secure login based on a 2F-Authentication scheme. For this purpose, sooner or later, Swiss edu-ID must support step-up authentication for secure login. A Service Provider must be able to request secure login (or a specific LOA) as part of the Authentication Request (e.g. in the `<samlp:RequestedAuthn-Context>` element) and the Swiss edu-ID IdP must be able to handle this request.
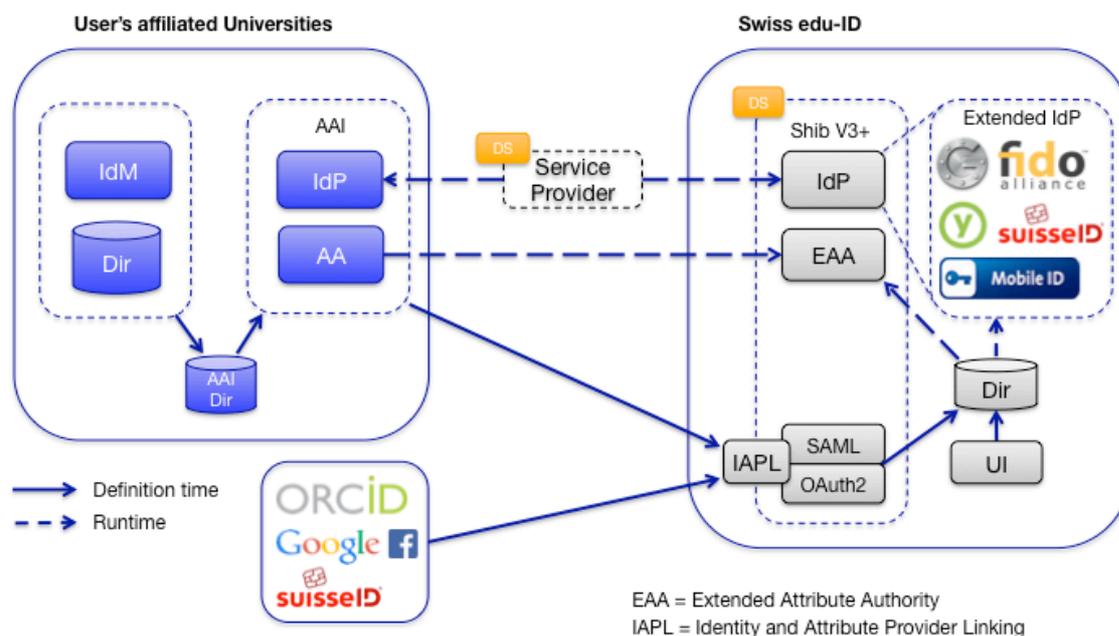

Figure 3: Development Package 2

4.5 Development Package 3

A shortcoming of the AAI-infrastructure is missing support for non-web resources and mobile applications. Therefore it is a main feature request for Swiss edu-ID, to include OAuth2.0 [4] as authorization framework and OpenID Connect [10] as an additional authentication layer on top of OAuth2.0. Both of these technologies extend the Swiss edu-ID platform to expose REST endpoints for authorization and authentication, making non-web application capable to access user information. Depending on whether the support for OAuth2 and OIDC will be an integrated part of Shibboleth, the availability of this feature depends on the project work plan of the Shibboleth development team. Based on the suggested resources and funds the roadmap of Shibboleth plans an implementation of OAuth2.0 and OIDC between 2nd half 2015 and 2016.
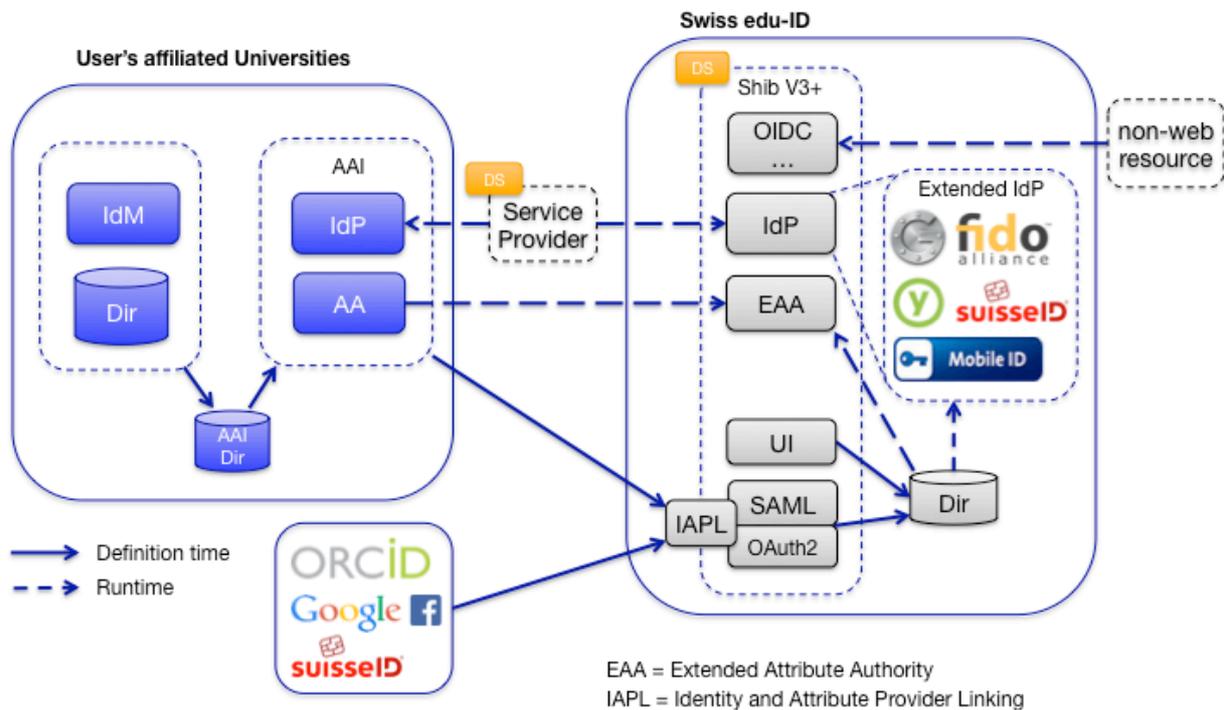see also: https://wiki.shibboleth.net/confluence/display/DEV/Work+Plan.

Figure 4: Development Package 3

5. Risks and mitigation

Shibboleth V3 is the first version designed to support other protocols than XML-based SAML. Although Shibboleth V3 has just been released in December 2014, we proceed from the assumption that the development packages pointed out in section 4, will be based on Shibboleth V3. In the following table we list some technical issues, to compare the eligibility of Shibboleth V3 in contrast to a commercial AM (e.g. candidates of the RFI supplier).

Remark: Based on the available information, it is not possible to estimate the necessary effort and costs more precisely for the implementation of a specific function (neither for a commercial AM nor for the Shibboleth-based solution).

Criteria	Commercial AM	Shibboleth V3 based AM
Integration of Resource Registry, metadata and attribute release policy	• Costs unknown. • Feasibility not definitively confirmed by the solution provider. There might be a high risk migrating existing information and policy rules in a commercial AM module.	• Integrated part of Shibboleth and the update process, which may need some minor adaption. Low risk expected.
Back-channel attribute query at run-time	• Commercial AM solutions focus more on backchannel provisioning (time-based or event driven). • Must be developed by all candidates. Effective effort and costs may vary.	• Must be developed for Shibboleth V3. • *GakuNin Federation* has already done a preparatory work[1]. Low risk expected. Effort and cost seems to be reasonably assessable.

[1] Attribute Query Handler: https://wiki.shibboleth.net/confluence/display/SHIB2/Contributions#Contributions-ServiceProviderExtensions

Criteria	Commercial AM	Shibboleth V3 based AM
Attribute aggregation at run-time with transmission of attribute-release policy on behalf of AAI-Attribute Authority	• Must be developed, tested and integrated by all candidates Effective effort and costs may vary.	• Must be developed, tested and integrated for Shibboleth V3. • Support of more than one role per user and session needs further clarifications. Effort and costs are hardly guessable yet.
Support for OAuth2 and OIDC	• Most of the candidates support OAuth2 and OIDC out of the box (or have it on their roadmap). Low risk expected.	• Must be developed, tested and integrated in Shibboleth V3. • According to the existing work plan of the 'shib development team' tentative date scheduled is 2016. There is a high risk that this feature will not be available at requested time.
Step-up authentication	• Most of the candidates support step-up authentication. Low risk expected.	• Must be developed, tested and integrated for Shibboleth V3. Low risk expected. Effort and cost seems to be reasonably assessable.
Support for additional authentication methods	• Some of the common authentication methods are already implemented in most commercial AM solutions. • The requirements of Swiss edu-ID may not cover the methods supported by the provider. Effort and costs may vary.	• Must be developed, tested and integrated for Shibboleth V3. Effort and costs are hardly guessable yet. The expense to implement specific authentication methods may not be negligible.
Integration of Identity Management (IdM) module	• Most of the candidates already integrate IdM functionality, or have an interface to an external IdM. Low risk expected.	• Interface to IdM must be developed, tested and integrated to support the features of the Swiss edu-ID platform. Effort and costs are hardly guessable yet.

Table 2: Positioning of technical issues and risks

If we assume that Shibboleth will be the core component of the Swiss edu-ID platform we must be aware that:
- Shibboleth only covers AM functionality.
- The AAI-infrastructure and the Swiss edu-ID remain independent, but fully interoperable.
- The Swiss edu-ID only extends SWITCHaai and does not replace existing processes and relationships.

Therefore it must be questioned what Identity Management functions must be offered by Swiss edu-ID and which functions should remain at the Home Organizations. We expect that only very basic Identity Management functions must be provided by the Swiss edu-ID platform.

A simple user interface to be able to manage Identity information, credentials, some attributes and links may be enough; there is no need for workflow management and no need for user data provisioning. Normally users do not have a direct relationship to SWITCH, but they have it to their Home Organization and there they primarily will keep personal data up-to date (as employee or student). Against this background we should avoid building too strong dependencies between Swiss edu-ID and the Home Organizations. Certainly, it would be attractive to have automatic data exchange possibilities (attributes, login credentials, etc.) between the central user directory and local directories

of the Community members. But this increases administrative, organizational and technical complexity and may slowdown the objectives to be reached. Or in other words: "Keep it simple and have courage to leave gaps".
We are aware about the fact, that this estimation may not be correct due to incomplete information about existing requirements. Nevertheless we would like to point out this issue in order to encourage further discussion.

6. Conclusion

As shown in the previous sections Shibboleth seems to be an appropriate candidate for a Swiss edu-ID AM component.

The technological implementation of some mandatory features of the Swiss edu-ID platform (e.g. additional authentication methods, step-up authentication, back-channel attribute query/aggregation) seems to be feasible with some effort in work and costs. The timetable and the expense for the implementation of OAuth2 and OIDC is the main risk of this solution to be considered. Regarding this point SWITCH should search contact to the Shibboleth development team in order to speed-up or change the work plan and possibly invest funds for manpower.
The development of all these functions should be broadly founded to ensure sustainability. Potential partners might be the Swiss University's Community, the Shibboleth development team and other provider of Shibboleth based solutions (in the field of identity management, single sign-on and federations), which might have some of the required functions on their own roadmap.

As pointed out in section 5 the alternative approach - the replacement of Shibboleth by an AM module from the market - offers undisputed advantages but has also some drawbacks and risks. Especially the migration of the existing SWITCHaai resource registry, the metadata and the containing attribute release policies could be a serious problem. All in all, the commercial AM modules bring some of the required functions out of the box, but some special features (e.g. back-channel attribute query and attribute aggregation at run-time) still need to be developed. In contrast to the Shibboleth solution the costs for these enhancements are very difficult to rate.

In general these commercial solutions have many functions and features on board (especially in the particular field of Identity Management), for which the Swiss edu-ID system probably will never have a need for.

7. Glossary

Term	Description
IdM	Identity Management refers to applications of IT technologies in order to manage information about the identity of users and control access to resources.
AM	Access Management is the central system at Swiss edu-ID platform, able to answer requests from service providers, authenticate the user and aggregate attributes from different sources.
AAI	SWITCH Authentication and Authorization Infrastructure
OTP	One-Time-Password
2FA	2-Factor Authentication
RR	Resource Registry (SWITCHaai metadata)
LOA	Level of Assurance
REST	Representational State Transfer is a software architecture consisting of guidelines for creating scalable web services
OAuth2	OAuth 2.0 is used on the web for authorizing resources, and is based on established standards such as HTTP, TLS and JSON.
OIDC	The OpenID Connect protocol is based on OAuth 2.0 and includes an authentication component.
UI	User Interface (e.g. on a web application)
SAML	Security Assertion Markup Language is an XML-based standard for the exchange of authentication, attribute and authorization information.
EAA	Extended Attribute Authority is the component, which supports back-channel attribute querying and attribute aggregation.
IAPL	Identity and Attribute Provider Linking is a request/response protocol in order to register a unique remote identifier as a specific attribute of a centrally managed user account.

8. List of tables

9. List of illustrations

10. Bibliography

[1] SWITCH. Swiss edu-ID high level architecture (July 2014). [Online].
http://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/SwissEduID_Architecture.pdf

[2] SWITCH. RFI Swiss edu-ID (November 2014). [Online].
http://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/Swiss_edu-ID_RFI.pdf

[3] eCH e-Government Standards. (2013) eCH-0107 "Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)". [Online].
http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-

0107&documentVersion=2.0

[4] IETF. RFC 6749. [Online]. http://tools.ietf.org/html/rfc6749

[5] SuisseID Trägerverein. SuisseID. [Online]. http://www.suisseid.ch

[6] FIDO Alliance. FIDO Alliance. [Online]. http://fidoalliance.org

[7] IETF. RFC 6238. [Online]. http://tools.ietf.org/html/rfc6238

[8] ETSI. TS 102 204. [Online]. http://docbox.etsi.org/EC_Files/EC_Files/ts_102204v010104p.pdf

[9] Swisscom. Mobile-ID für Geschäftskunden. [Online].
http://www.swisscom.ch/de/business/mobile-id/technical-details/technical-installation.html

[10] OpenID. OpenID. [Online]. http://openid.net/connect