Accounting for the Authentication and Authorization Infrastructure (AAI)

Pilot Study

Document management

Version/status:	1.0 / final	
Date:	05-01-2006	
Author(s):	Patrik Schnellmann	SWITCH
	André Redard	at rete ag
File name:	A3I_Study_v1_0.doc	
Replacing:		
Approved by:		

Table of Contents

	Management Summary	**ii**
1	**Introduction**	**1**
2	**What is “Accounting”?**	**2**
2.1	Terminology	2
2.2	The AAA services	3
2.3	Accounting technology	4
2.4	E-payment solutions	4
3	**Why “Accounting”?**	**5**
4	**Accounting requirements**	**6**
4.1	Overview	6
4.2	E-journals and databases	7
4.3	E-learning courses	7
4.4	Web-based SMS service	9
4.5	E-conferencing (SWITCH)	10
4.6	E-shops	10
4.7	Printing service	11
4.8	Grid	12
4.9	Network access	13
4.10	AAI service monitoring	13
5	**Conclusion**	**14**
6	**Recommendation**	**15**

Management Summary

In 2001, SWITCH started a project for implementing an authentication and authorization infrastructure (AAI) based on Shibboleth. Today, many Swiss universities have implemented SWITCHaai, as it is called, and many resources can be accessed by users of different organization using it as authentication and authorization mechanism.

SWITCH believes that optional accounting services are important in a shared and distributed environment in order to understand how resources are used and to be able to split costs of shared resources among their users. The goals of this pilot study are to understand the requirements of home organizations, resource owners and SWITCH, to identify accounting technologies compatible with SWITCHaai, to define the terms accounting and auditing in the context of SWITCHaai, and to work out a recommendation for further steps and possible pilot projects.

Results:

While accounting has been a necessity for commercial telecom providers or IT outsourcers, accounting has been rarely implemented in the academic environment. Based on several interviews with representatives of universities and SWITCH, it can be said that there is a demand for accounting solutions.

The major requirements are in the domains of usage statistics, usage-based charging or cost allocation to organizations. Some of the resources requiring accounting services, like e-learning or e-conferencing systems, are already using SWITCHaai for authentication and authorization; other services like e-journals or grids will be integrated with AAI in the future.

There exist also services, like printing, with a demand for end user charging; they are, however, not well suited to integrate with SWITCHaai due to the limitations of the underlying Shibboleth. There are also potential needs with the main focus on billing or e-payment, but these needs could also be met with commercial solutions rather than with an accounting infrastructure.

From the technological point of view, the existing accounting protocols are not designed for the needs of accounting for web-based services with federated identities; and enabling accounting for SWITCHaai is an issue still to be solved.

Recommendation:

Besides the SWITCHaai projects with an accounting aspect already started, we recommend focusing on use cases with a close relationship to SWITCHaai, a limited complexity and a real demand by resource owners. We suggest working out project proposals for the following pilot project candidates and deciding afterwards which of these projects should be started:

- e-learning usage statistics
- e-journal usage statistics
- Accounting for SWITCH e-conferencing
- SWITCHaai monitoring and usage statistics

1 Introduction

In 2001, SWITCH started a project for implementing an authentication and authorization infrastructure (AAI) for higher education in Switzerland, based on Shibboleth [Shibboleth]. Today, many Swiss universities have implemented SWITCHaai [SWITCHaai], as it is called, and many resources can be accessed by users of different organization using it as authentication and authorization mechanism.

Figure 1: Authentication and Authorization Infrastructure (SWITCHaai)

The main purpose of SWITCHaai is to authenticate a user by the authentication system of the user's home organization and to authorize the user to access a particular resource. The authorization decision is made by the resource based on authorization attributes received from the authentication system.

SWITCH believes that optional accounting services are important in a shared and distributed environment in order to understand how resources are used and to be able to split costs of shared resources among their users. Nevertheless, accounting applications like billing, usage reporting etc. were initially deliberately excluded from the SWITCHaai for various reasons. Yet, already the SWITCHaai preparatory study postulated that it would have to interact with these applications.

A billing system for a resource, will need to know e.g. who has used the resource and how it has been used (how many transactions, which information, how long, etc., depending on the tariff model for that resource).

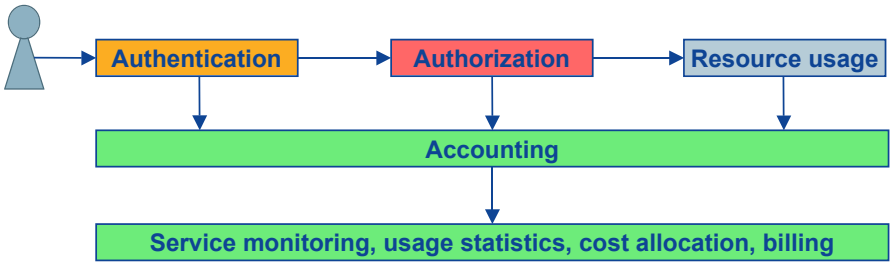

Figure 2: Accounting system interacting with SWITCHaai and the resource

SWITCHaai is able to answer the question of who has accessed the resource because it is able to link the information the resource has about users (e.g. anonymous user IDs) back to real persons only known by the home organization. However, SWITCHaai has no information on the question of how the resource was used. This answer can only be given by the resource itself, which can measure the interactions between a user and the resource.

Therefore, it was a logical step that SWITCH started a project called "Accounting for the Authentication and Authorization Infrastructure (AAI)" in September 2005. The goals of the first project phase are:

- know the requirements of home organizations, service providers and SWITCH
- identify accounting technologies compatible with SWITCHaai
- define the terms accounting / auditing in the context of SWITCHaai
- work out a recommendation for further steps and possible pilot projects

The results of this first project phase are documented in this pilot study.

Chapter 2 introduces the relevant terminology, explains accounting concepts in general and in the context of an AAI and gives a brief introduction to e-payment solutions.

While chapter 3 shows why accounting will become important also for universities, chapter 4 lists typical accounting use cases, defines their requirements, possible solutions, and open issues.

Chapter 5 positions the areas where demand for accounting has been identified; and chapter 6 finally lists four possible pilot projects and gives recommendations of how to proceed.

2 What is “Accounting”?

2.1 Terminology

In the following, basic terms of accounting and related concepts are defined in alphabetic order. The definitions are derived from RFC 2975 ”Introduction to Accounting Management” [RFC2975] and from “A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond: A^{x}” [TIK111].

Term	Definition
Accounting	Accounting is the collection and aggregation of information (accounting records) in relation to a user’s resource utilization. It is expressed in metered resource consumption. The data can be used for capacity and trend analysis, cost allocation, billing or auditing. Note that accounting does not include billing.
Auditing	Auditing is the verification of the correctness of any process regarding the service delivery. Auditing is done by an independent real-time monitoring or examination of logged system data in order to test for correctness of operational procedures and to detect breaches in security. Auditing of accounting records is the base for a proof after the usage of resources and for customer charges.
Billing	Billing is defined as the process of collecting charging records, summarizing their charging content, and delivering a bill or invoice including an optional list of detailed charges (itemization) to a user.
Charge calculation	Charge calculation covers the complete calculation of a price for a given accounting record and its consolidation into a charging record, while mapping technical values into monetary units. Therefore, charge calculation applies a given tariff to the data accounted for.
Charging	The overall term charging is utilized as a summary word for the overall process of metering resources, accounting their details, setting appropriate prices, calculating charges, and providing a fine-grained set of details required for billing. Note that billing as such is not included in this definition. Charging is considered as a dedicated policy to enable a provider to gain revenue for a given service offer.
Cost allocation	The act of allocating costs between entities. Note that cost allocation and charge calculation are fundamentally different processes. In cost allocation the objective is typically to allocate a known cost among several entities. In charge calculation the objective is to determine the amount to be charged for use of a resource. In cost allocation, the cost per unit of resource may need to be determined; in charge calculation, this is typically a given tariff.
Metering	The task of metering determines the collection of data on the usage of resources within end-systems (hosts) or intermediate systems (routers) on a technical level, including quality of service, management, and networking parameters.

Table 1: Terminology for accounting and related concepts

2.2 The AAA services

In general, an authentication, authorization and accounting (AAA) infrastructure provides its services to the resource as shown in Figure 3. During the pre-service phase, the user is authenticated and authorized to use the service offered by a resource on sending it a service request. In the service delivery phase, the usage is metered and usage data is collected.

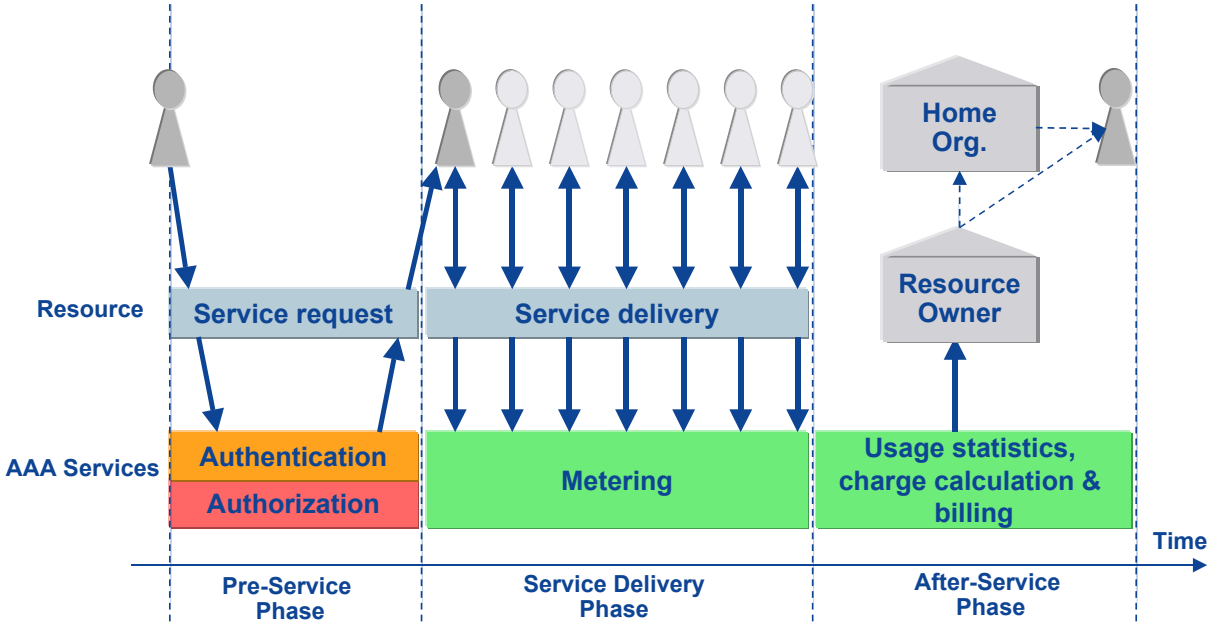

Figure 3: Service interactions

In the after-service phase, the usage data is aggregated into usage statistics or the charge is calculated, depending on the needs of the service provider. Service usage may be billed to the home organization or directly to the user. Usage statistics may be used for internal purposes of the resource owner or is sent to the home organization. Usage statistics may also be used to allocate costs to different home organizations.

SWITCHaai implements the authentication and authorization services. Due to the federated approach of SWITCHaai, home organizations know much about real users, but have limited information about their resource usage. On the other side, resources only know as much as the released attributes about a user, but can meter the resource usage as detailed as necessary. Depending on the design of the resource and the integration with Shibboleth, the resource may act as a black box and the attributes are kept only in the authorization module of Shibboleth. Therefore, data logged at the resource and at the authorization module has to be combined to get valuable information.

Figure 4 gives a brief overview of where the relevant accounting information can be metered, collected and aggregated.

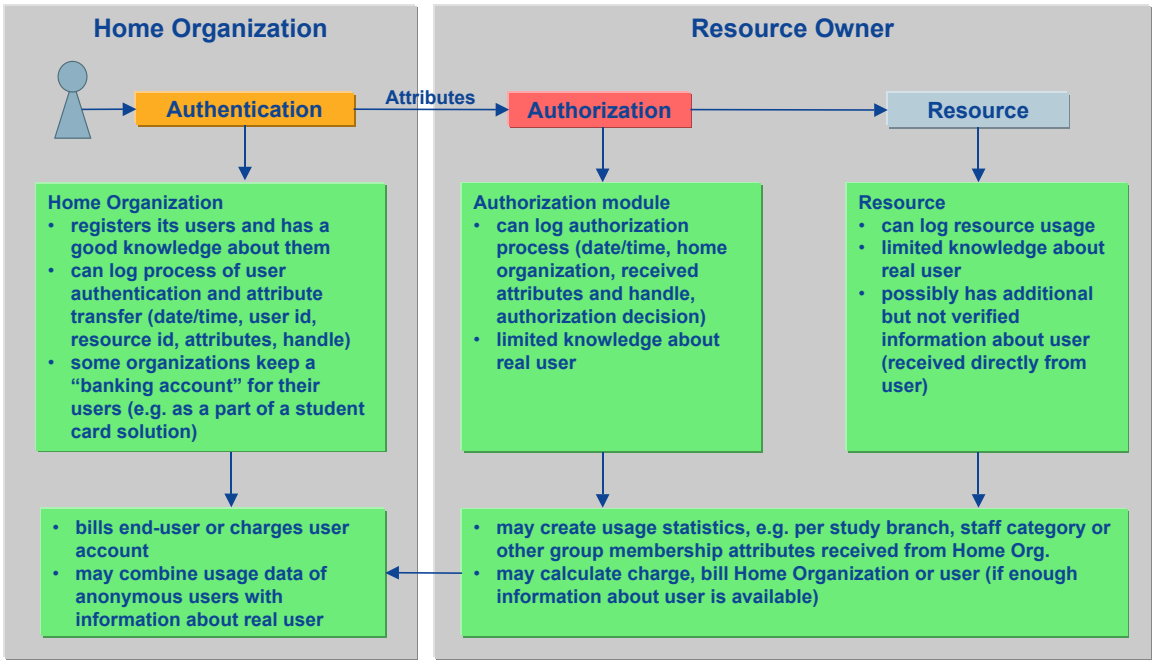

Figure 4: Accounting information available to home organization and resource owner

There is always a trade-off between protecting the user's privacy and sending attributes to the resource in order to enable the resource owner to create relevant usage reports.

Especially in the case of commercial providers like e-journal publishers, the home organizations will only release the minimal set of attributes necessary for access authorization. Therefore, only the home organization may be able to aggregate usage statistics per user group, provided that the commercial resource owner makes available detailed usage data per user, i.e. per unique ID (see [AAIAttr]).

2.3 Accounting technology

Many of the current solutions for AAA make use of "Remote Authentication Dial In User Service" (RADIUS) [RFC2865] or Diameter [RFC3588]. Their application is mainly in networking and with identities that are not federated. The same can be said about Internet Protocol Detail Record (IPDR), which is a standardized record format for different services based on the Internet Protocol (IP). For a Shibboleth based AAI, there currently exists no standardized protocol that could be used for accounting purposes. What concerns standardized reports; there is an effort in the domain of digital content providers, the project COUNTER [COUNTER]. They specify how to measure usage of e.g. e-journals and database searches and the granularity in which the usage data is reported. None of the existing protocols is suitable for the needs of accounting with federated identities and it is open how to enable accounting for the current AAI.

2.4 E-payment solutions

As defined in the terminology above, accounting does not comprehend billing. However, one reason to do accounting may be to charge the users on the basis of the collected usage data. At the universities, bills are usually paid with traditional methods, e.g. semester fees are paid by bank transfer or similar. For online services it may be desirable that a service is paid immediately i.e. online like it is the case for web shops. This section will give an overview about the most popular e-payment methods.

Basically, the payment method depends on the amount of money to be paid. If the sum is large, we speak about macropayment. If the sum is small, the term micropayment is used. For online macropayment, the only globally accepted means of payment are credit cards. The transaction costs for credit card payments

set the limit to distinguish between micropayment and macropayment. If the transaction costs are too high to pay a small sum of money by credit card, micropayment solutions are needed. There are some world-wide used services like paypal [Paypal], but they are not as widespread as credit cards.

Electronic payments reduce administrative tasks, like sending out bills, payment slips and reminders. On the other hand, the initial investment to set up electronic payments has to be made and there are also running costs. The initial costs comprise: an agreement with a “payment service provider” (PSP), an agreement with each issuer of the credit cards to be accepted, a software interface between e.g. a web shop and the PSP. The running costs to be taken into account are: transaction costs for each payment, maintenance costs for the PSP and the administrative task to treat rejected payments.

In Switzerland, several solutions for online (micro-)payment without credit cards are offered. The payment solution providers like Datatrans [Datatrans] and Saferpay [Saferpay] have the most current list.

3 Why “Accounting”?

While accounting has been a necessity for commercial telecom providers or IT outsourcers in order to charge their services, accounting has been rarely implemented in the academic environment.

Today, accounting is also relevant for services provided by the universities and by SWITCH:

- To improve the service offering, resource owners need a better understanding of their users and their resource usage.
- Since organizations cooperate in developing new applications and sharing resources, cost for implementation and operation have to be allocated to the involved parties.
- Budget restrictions require a control of costs and advanced usage statistics for capacity planning.
- A federated service like SWITCHaai is based on trust among the participating organizations. Therefore, the compliance with the SWITCHaai policy has to be auditable.

While many of the accounting requirements can be implemented by organizations on their own, some of the requirements in a federated environment can only be solved in a joint effort of all involved organizations.

4 Accounting requirements

4.1 Overview

One of the goals of this pilot study is to get an overview of the accounting requirements of home organizations, resource owners and SWITCH as the SWITCHaai service provider. The set of use cases shown below is the result of several interviews with representatives of universities and SWITCH.

Accounting requirements have been found for various resources which fall into two main categories. The distinction is made between web resources and non-web resources. Today, in SWITCHaai there are only resources that can be accessed via web browser such as e-learning systems and other web resources. This is because SWITCHaai is based on the Shibboleth implementation of Internet2, which supports only web browsers to access protected web-based resources. There are efforts to overcome this limitation such as LionShare [LionShare], GN2 JRA5 [GN2JRA5], GridShib [GridShib] and the SWITCH engagement within the EGEE project [EGEE]. Therefore, in the future, more and more non-web based resources can be integrated into SWITCHaai.

Application / service	**relationship with SWITCHaai**	**accounting requirements**
E-journals	authN & authZ[1]	usage statistics
E-learning (regular students)	authN & authZ	usage statistics and usage based cost allocation
E-learning (continuing education)	authN & authZ VHO[2]	charging to end users (macropayment)
Web-based SMS service	authN & authZ	charging to end users (micropayment)
E-conferencing (SWITCH services)	authN & authZ	usage statistics, cost allocation and/or charging to organizations
E-assessment	authN & authZ	transfer of examination results to home organization
Grid	EGEE project	usage statistics, usage based cost allocation, charging
University E-shops (scanned journals, printed manuscripts, software licenses, e-learning objects, etc.)	authN & authZ	charging to end users (macro- & micropayment)
Printing	open	charging to end users (micropayment)
Network access, e.g. Public Wireless LAN (PWLAN), Eduroam, iPass	open	usage statistics, cost allocation, charging
other non-web applications, e.g. VoIP	open	open
SWITCHaai	all aspects	service monitoring, usage statistics, abuse detection

Table 2: Use case overview

The following chapters describe representative use cases in further detail.

[1] Authentication and Authorization

[2] Virtual Home Organization

4.2 E-journals and databases

Today, commercial content providers, like Elsevier, JSTOR, etc., authenticate and authorize users of their customers (consortiums, consortium members) based on IP ranges. They deliver IP-based usage statistics to their customers. The format of these statistics is standardized across major content providers [COUNTER].

In the near future, content providers will be able to authenticate and authorize their users based on SWITCHaai. Elsevier has already signed a SWITCHaai Federation Partner agreement; others will follow. IP-based usage statistic will then become useless.

Other content providers are accessed via a shibbolized proxy solution [EZproxy]. Due to the single IP address of such a proxy, the usage statistic provided by the content provider has no significance concerning the origin of the users.

4.2.1 Accounting requirements

Since the subscription of commercial publishing services is expensive, universities need detailed usage statistics to optimize their portfolio of subscribed publishing services. Therefore, usage statistics for shibbolized content provisioning services should have at least the same quality as the statistics received today. In addition, the universities would like to have a better understanding of who is using the subscribed e-journals and databases in order to evaluate the benefit of buying an e-journal service.

4.2.2 Possible solutions

In order to fulfill the privacy policy, the released attributes should have no meaning for the content providers. Therefore, they will have only limited knowledge about the users; but could make usage data per user available to the home organizations. Then, home organizations would be able to combine usage data and user attributes and create aggregated usage reports of e-journals and databases per user group instead of IP ranges.

The usage of e-journals accessed via the EZproxy could be metered and evaluated at the EZproxy itself.

4.2.3 Open issues

- In the shibbolized content provider scenario, only the content provider has the ability to meter the usage of its resource. It is an open question whether the content provider will provide detailed usage statistics to their customers.
- In the EZproxy scenario, it has to be analyzed if the usage metered at the EZproxy is sufficient to create statistics about the resource usage.

4.3 E-learning courses

E-learning courses for regular students and for students in the continuing education are of growing importance. One benefit of such courses is that they can be used by different organizations (due to the independence of place and time). In the past, the implementation of such courses has been financed by subsidies (e.g. Swiss Virtual Campus courses). Very often, these e-learning courses are assisted by faculty staff. Therefore, not only the cost for implementing such courses but also the costs for providing them are not negligible.

In the future, the cost for implementing and providing such courses may have to be paid by the users themselves (continuing education) or by their home organizations (regular students).

For selling courses to individuals, different tariff and charging models are conceivable:

a) fixed fee per course, paid before starting the course

b) fixed annual subscription fee, paid in advance

c) tariff depending on usage, charged periodically

The usage by regular students may be charged based on

d) a usage based cost allocation schema

e) a fixed (not usage based) cost allocation schema

4.3.1 Accounting requirements

Resource owners would like to be able to create meaningful usage statistics in a format interchangeable between organizations. Instead of typical web usage statistics (number of page views, IP-address or domain of user, …), a usage statistic per user or user group (e.g. per organization, study branch, affiliation, …) and per e-learning unit (course, course element, …) is required.

In addition, to support the business models c) and d), the accounting infrastructure has to enable the resource owners to allocate cost to home organizations or calculate charges per user or home organization based on metered resource usage.

Whenever the usage of a resource is charged, the information necessary to verify the correctness of the bill has to be logged, i.e. made auditable.

4.3.2 Possible solutions

Today, there exists no standardized solution to meter the usage of a web-based application, to create usage statistics or to calculate charges. Most of the learning management systems (LMS) have implemented their own statistics module, but the output is neither standardized nor is it based on SWITCHaai attributes.

Similar to the standardization of e-journal usage statistics among publishers [COUNTER], it would make sense to standardize the e-learning usage statistics among universities.

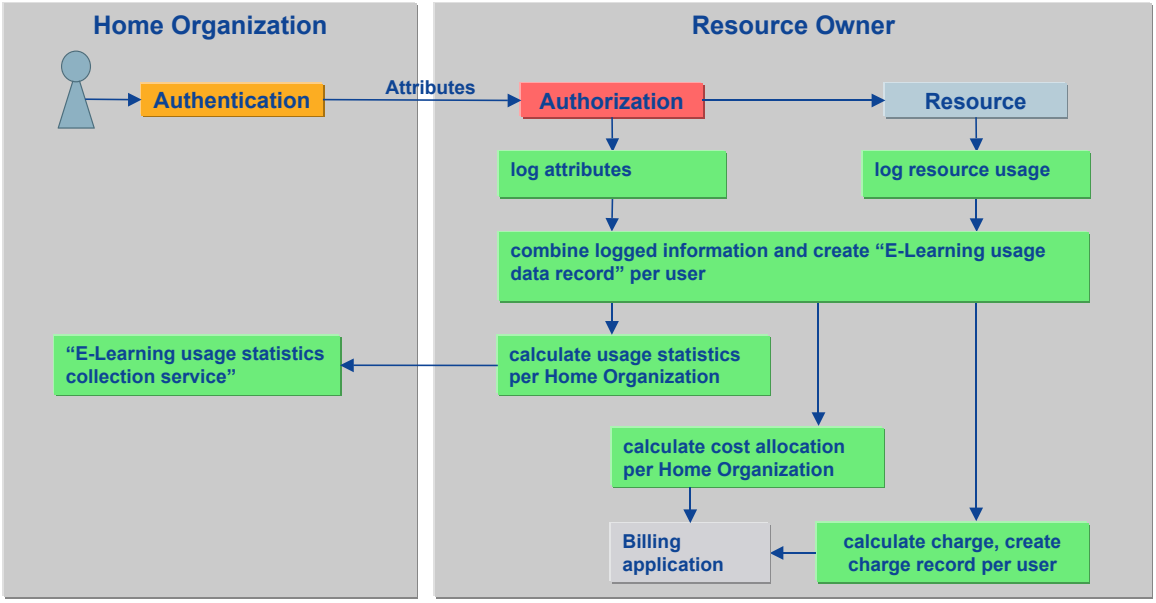

Figure 5: E-learning usage statistics architecture

Based on AAI attributes and the resource usage, a SWITCHaai specific "e-learning usage data record" (EL-UDR) could be defined, which reports the usage of a specific e-learning unit by an individual user. The format of this record could be defined similar to the XML-formatted IP detail record [IPDR]. Exactly how this EL-UDR is created depends on the architecture of the resource. In the case of a black box application which does not get further information about the user, authorization attributes and resource usage data have to be brought together outside the resource as shown in Figure 5. If Shibboleth and the resource are closely coupled, the creation of the EL-UDR could be implemented within the resource itself.

Based on collected EL-UDR, charge calculation per user or cost allocation per organization can be performed and the resulting information can be sent to a billing application. While the creation of charge records is usually part of an accounting infrastructure, the creation of bills and the management of accounts receivable is part of a standard ERP solution, like SAP, and therefore outside the scope of this study.

Usage statistics per home organization could be transferred to a so-called “e-learning usage statistics collector” which collects the usage statistics of all compliant e-learning resources and generates comprehensive university-wide e-learning usage reports. The communication between resource and collector could be implemented as a web service and secured by means of SWITCHaai and SWITCHpki.

For the payment of course fees or subscription fees by individuals (the scenarios a) and b) as defined in chapter 4.3), it is recommended to settle the transaction by integrating a commercial, credit card based payment solution.

4.3.3 Open issues

- The business need for usage based cost allocation is uncertain. Probably, other cost allocation schemes without the need of metering resource usage are good enough and much simpler to implement. Together with the evolvement of the Bologna model, universities implement student administration systems and will have accurate information of how many students are subscribed to study modules linked to e-learning courses. This information may be good enough to split cost among participating organizations.
- As for the usage statistic, the concept of an EL-UDR as postulated has to be further investigated. Is it possible to define a universal EL-UDR content, which is as generic to support different kinds of e-learning resources and as specific to contain significant information about the usage of a particular e-learning resource? Also in this case, the business need has to be confirmed.
- Since participants of continuing education programs are not members of a home organization, the resource owners register them in a virtual home organization (VHO). For a lean provisioning of e-learning courses, the processes of paying a course and creating a VHO account have to be coupled.

4.4 Web-based SMS service

The use case “web-based SMS service” stands as an example for a variety of payable and SWITCHaai-enabled web-based services. The idea is to improve the efficiency and convenience for students and/or to employees by implementing new services provided at cost. Staying with the example of an SMS service, students could send SMS at low rate or subscribe to SMS news services related to their study, e.g. information about changes of lecture time or place.

4.4.1 Accounting requirements

Since the price for sending (or receiving) an SMS is rather low, charging the user requires a micropayment solution. The resource has to be able to check the credit limits of the user, to meter the resource usage, to calculate the charge based on a tariff and to transfer the charging messages to the micropayment system.

4.4.2 Possible solutions and open issues

There are several ways to add micropayment functionality to a shibbolized web resource.

- Universities which have already have implemented a payment solution as part of a student card solution, e.g. Polyright [Polyright] would like to extend their payment solution to web-based services. Integrating the home organization’s payment system and the resource could leverage the functionality of Shibboleth: the secure communication between the resource and the home organization could be used to transfer payment authorization and charging messages.
  It has to be said that, as far as we know, there is neither implementation nor a protocol specification available for such an integrated solution. Also, the settlement between organizations (clearing) is not solved yet.

- Universities without this infrastructure prefer to integrate third party micropayment solutions instead of implementing such a complex payment infrastructure by themselves. In this scenario, the relationship between the micropayment solution and SWITCHaai is not evident. If micropayment solution providers were offering Security Assertion Markup Language [SAML] based federated identity management in the remote future, SWITCHaai could potentially interoperate with their authentication and authorization infrastructure.
  The advantage of a third party solution is that the settlement is part of the provided solution and it does not make a difference if the user is member of the same organization as the resource or not.

4.5 E-conferencing (SWITCH)

SWITCH supports and fosters e-conferencing and virtual collaboration [SWITCHeconf]:

- IP-videoconferencing service, including central infrastructures for multipoint conferencing (MCU)
- Collaboration tool “Breeze” (real-time application sharing, instant messaging, virtual presentations, whiteboard tools and document exchange)
- Live or on-demand streaming media service

SWITCH has implemented a portal which is SWITCHaai enabled and controls access to the three services mentioned above

E-conferencing services will potentially be unbundled from SWITCH’s standard network services and will be charged separately. Today, the service development is still on-going and the business model for such services is not yet defined. For each service, different pricing schemes are under discussion, which vary from “annual package, flat rate per organization” to “usage based (used hardware, network, software, etc.)”.

4.5.1 Accounting requirements

The accounting requirements depend on the chosen pricing schema. When a flat rate schema is applied, there is no need for accounting, except for post calculation and tariff determination. Other pricing schemas require usage metering at the portal (e.g. based on the MCU reservation, independent whether the videoconference has happened) or metering at the infrastructure level (e.g. usage of multipoint control unit, network resources, etc.).

4.5.2 Possible solutions and open issues

Since service access is controlled by the SWITCHaai enabled e-conferencing portal, accounting functionality could be implemented on the portal itself. Metering at the infrastructure level may be more accurate but also much more complex because these services (H.323, etc.) are not shibbolized. The development of a tariff model and the definition of resource metering influence each other; and the optimal solution has to be found.

4.6 E-shops

Universities offer various products to their students and employees, like notebooks, software licenses, printed manuscripts, sweat shirts etc., at a reduced price. To streamline their processes, they would like to sell these products over the Internet. Due to the special contracts with suppliers, e.g. for software licenses, the universities are allowed to sell some of these products only to university members and affiliates, like alumni. Therefore, such e-shops could be protected by SWITCHaai.

It has to be understood that the process of buying and paying products in an e-shop is quite different from using, metering and charging a service, since the total amount to be paid is agreed between the e-shop and the users in advance.

4.6.1 Possible solutions and open issues

There are commercial e-payment solutions available to add e-payment functionality to an e-shop (see chapter 2.4). We believe that the role of SWITCHaai will only be to restrict the access to an e-shop to university members or to apply a specific discount schema, but has no role in the ordering and payment process.

Before implementing an e-payment solution, the expected transaction volume, the implementation cost and the operational cost have to be put to closer scrutiny. While such a solution may not be suitable for selling a few dozens of e-learning courses to participants in a continuing education program, it may be profitable for a university to implement such an infrastructure for all kind of payments, e.g. student fees, sold products and services etc.

4.7 Printing service

Computer rooms accessible for students usually offer printing facilities. While most users print a reasonable amount of copies, some seem to print excessively, which stresses the printing budget. In some universities (e.g. University of Lausanne, University of Geneva), accounting solutions have been put in place, but they are not integrated with SWITCHaai. These accounting solutions are implemented only for members of the home organization and therefore, members of other organization, e.g. mobile students, cannot use these printing services.

4.7.1 Accounting requirements

Accounting requirements are similar as for the SMS services. The printing service has to be able to authenticate the user, check the credit limits of the user, meter the resource usage, calculate the charge based on a tariff and transfer this information to a billing system or a payment solution for pre-paid payments.

4.7.2 Possible solutions and open issues

While SWITCHaai is well positioned for web-based services, it is not yet well positioned for other services like printing as described in chapter 4.1. Consequently there are two possible solutions:

- Shibboleth is extended to allow also to integrate non-web-based services like printing
- A web-based, shibbolized service could control access to the printing service

In both cases, the same solutions as described for the SMS services (see chapter 4.4.2) would be applicable.

Some universities plan to implement student card based accounting solutions where users are authenticated by presenting their student card to the printer (card reader or contactless). Some vendors may also offer roaming capability between organizations using the same student card solution.

We believe that implementing such a commercial solution is much more feasible than implementing a SWITCHaai based solution, even if hardware incompatibility between different solutions makes it complicated, or even impossible, to implement an inter-organizational printing and accounting service.

4.8 Grid

Grid infrastructures already have various modules to implement accounting. There are similarities as well as differences between Shibboleth-based AAIs and grids. Table 3 gives an overview.

	SWITCHaai	Grid
User identification	swissEduPersonUniqueID [AAIAttr]	Certificate Subject/DN
Authentication for resource access	Authentication at the home organization[3]	User authenticates himself by presenting a X.509 user certificate
Participating entities	User, home organization (HO), web-based resource	User, virtual organization (VO), computing resources
Affiliation of the user	Home organization (static affiliation)	The user can be a member of several (possibly short-lived) VOs and may have several roles within a given VO (dynamic affiliation)
Delegation	Currently no delegation built-in. Possible through portals. Release 2 of Shibboleth will support limited delegation (ECP profile[4]).	Delegation through proxy certificates
Types of resources	Large number of different resources (e-learning, libraries, websites, etc.)	Computing resources only (“computing element” and “storage element”).
Pricing of resource usage	Price is mainly determined by resource access (depending on nature of web-based resources)	Market driven prices possible due to interchangeable resources. Price can depend of quality of service demanded by the user
Time when price is known	Before or after resource usage	Price is known after usage as price depends on resource usage

Table 3: AAI and Grid comparison

4.8.1 Situation today

Accounting is an important issue for grid infrastructures. There exist several solutions such as GridBank [GridBank] and DGAS [DGAS]. Accounting standardization efforts take place within the Global Grid Forum [GGF]. Thus, grid accounting architectures can be looked at as a model for AAI accounting. However, there are currently practical limitations due to the lack of interoperability between AAIs and grids.

4.8.2 Possible solutions and open issues

Over the next two years SWITCH will implement interoperability between Shibboleth-based AAIs and the EGEE grid infrastructure. This opens up interesting perspectives for accounting issues. A simple approach could be envisaged where AAIs perform the accounting of the initial job submission procedure. The current accounting of the computing resources on the other hand would be handled by the grid accounting modules. The two information sets would need to be correlated once the job has finished.

[3] username/password is most common, but stronger authentication is possible as needed
[4] Enhanced Client or Proxy profile

4.9 Network access

For the time being, there are several solutions for roaming users to access wireless and wired networks. For users in Swiss higher education, there is SWITCHmobile [SWITCHmobile], which grants network access to users at the major universities in Switzerland, be it for local users at the home organization of the user itself or for users from another home organization. To get network access, users connect to their home organization using a VPN client where they get authenticated using their credentials (username/password, client certificate). The authentication for network access is separated from the authentication for AAI resources. Enabling network access through AAI is an issue that is discussed within the joint research activity within GÉANT2 [GEANT].

For internationally roaming users there is Eduroam [Eduroam] for the academic world and the commercial service iPass [iPass].

4.9.1 Accounting requirements

Accounting for networks can currently be done through various protocols such as Simple Network Management Protocol (SNMP), COPS [RFC2748], RADIUS [RFC2865] or Diameter [RFC3588]. The latter two are the most commonly used ones. As a standard interchange format for network usage, the Internet Protocol Data Record [IPDR] is used by a number of leading vendors. Although there are accounting protocols and formats for network usage, there is no commonly agreed standard. Nevertheless the existing solutions allow accounting.

4.9.2 Open issues

Once authentication and authorization for network access will be done using AAI, the accounting done in networks will be relevant for AAI. It is open how to connect network accounting solutions with the future accounting based on AAI.

4.10 AAI service monitoring

In the AAI, the identity provider (IdP) and service provider (SP) servers produce log files about authentication events, attributes sent from IdP to SP and so on. Nowadays, this information is not systematically analyzed.

4.10.1 Accounting requirements

If a user cannot access a resource as he expects, it may be due to a misconfiguration on the IdP side or on the SP. For administrators, it can be hard to find the error reason quickly due to the distributed nature of the AAI. A systematic collection and analysis of log files from IdP and SP can help to locate malfunction faster and therefore improve the service quality in favor of the users of the AAI. Misuse of the system could be detected by analyzing the log files and even misuse like identity theft might be disclosed.

Moreover a central collection of aggregated data would allow statements about the usage of the whole system.

4.10.2 Possible solutions

The current Shibboleth implementation of Internet2 allows logging of data to a certain extent. Post processing of the log files could be done with standard Unix tools or specifically developed add-on tools.

4.10.3 Open issues

An open standard format for the collected and reported log files has to be defined if the data will be aggregated in a central place. The secure transmission of the log data has to be addressed. If data is not anonymized, data protection issues have to be considered.

5 Conclusion

As we have seen, there are many accounting requirements, but not all of them are in the scope of this project.

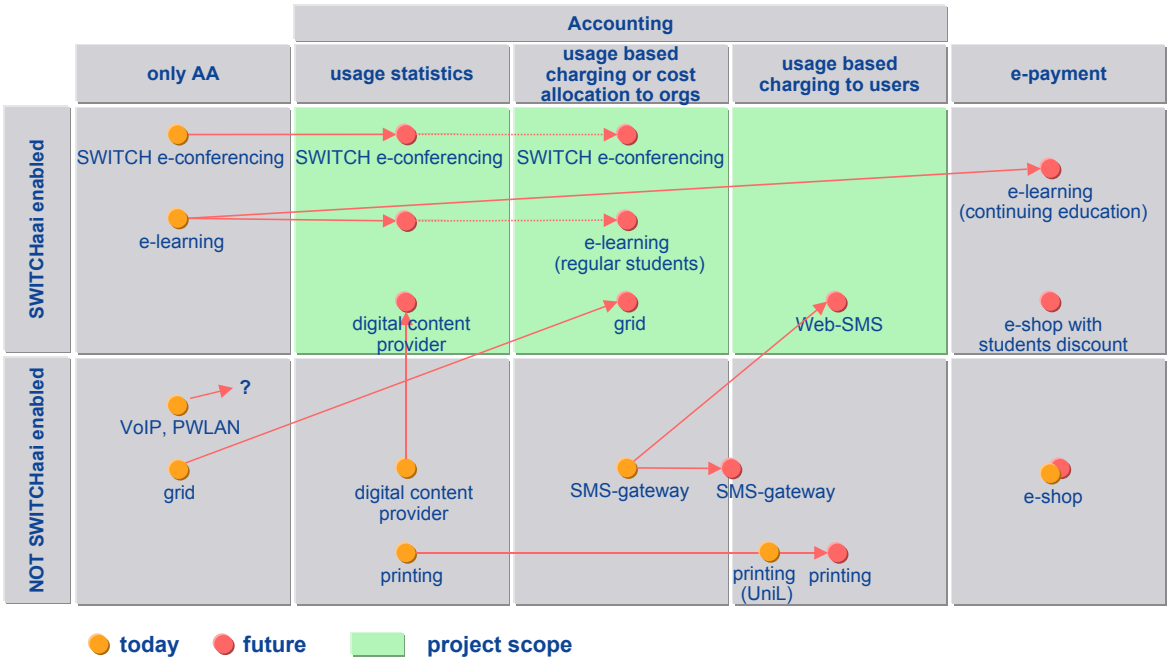

Figure 6: Accounting demand - today and in the future

Figure 6 positions the areas where the pilot study has identified demand for accounting from today's perspective and expectations for the future. The major domains in accounting are usage statistics, usage-based charging or cost allocation to organizations, and usage-based charging to the end users. There are also potential needs with the main focus on billing or payment in the field of e-payment, but these needs could be easily met with commercial solutions rather than with an accounting infrastructure.

In general, the complexity of the solutions as positioned in Figure 6 increases from left to right, i.e. the implementation of accounting for usage statistics is less complex than a solution for usage-based charging or cost allocation, which in turn is less complex to develop than charging to end users. The most demanding would be an infrastructure which allows billing of end users, as this would also involve bookkeeping, flow of money and auditing of all systems involved. However, since accounting does not comprise billing, such an infrastructure would go beyond the scope of this project.

While the needs in the project scope area (light background) above are in the focus of this pilot study, the other areas are also of potential interest to SWITCH and activities in these areas will have to be defined.

6 Recommendation

As we have seen, there is a large variety of accounting requirements and possible solutions. For the next project phase, we strongly recommend focusing on use cases with a close relationship to SWITCHaai and a limited complexity. The use cases have to be driven by a real demand of resource owners or the SWITCHaai community and should have the potential to act as a show case for SWITCHaai accounting.

Out of the use cases described in chapter 4, we have selected four which fulfill the criteria above. Table 4 shows these pilot project candidates, the motivation to start a pilot project and the expected benefits. We suggest working out a project proposal for each of them, i.e. finding project partners, defining project goals and deliverables and setting up the project plan. Based on these results, it should then be possible to decide which projects are the ones to be started.

Pilot project	Motivation	Benefits
SWITCHaai Monitoring and Usage Statistic	• Implementation close to Shibboleth • Development in-house and with well-known partners (IdPs, SPs)	• Improve service quality of AAI • Better understanding of how SWITCHaai is used • Detection of misuse
Accounting for SWITCH e-conferencing	• SWITCH's services stand as a model for resources that are largely consumed by other organizations • Costs generated by third parties (mainly software licenses) are to be allocated to the user's home organization on the basis of usage statistics • The process to bill the organizations has already been established (network usage, SMS/fax/pager-gateway) • Optimal coordination as it is an in-house project (development of tariff model and definition of resource metering influence each other)	• Improve know-how on implementing SWITCHaai-related accounting • Better understanding of how the service development/tariff modeling and accounting influence each other • Potential to be a show case for usage-based cost allocation
E-journal usage statistics	• Accounting is already an established process with a standardized reporting format (project COUNTER) but has to be extended to SWITCHaai enabled resources • Demand for more granular usage statistics, i.e. per user categories supported by SWITCHaai, like affiliation or study branch • In line with the year 2006 initiative of SWITCHaai to increase the number of AAI-enabled library resources	• Gaining experience on combining collected information from various sources (e.g. federation partner, proxy, identity provider) • Involvement of community members

Pilot project	Motivation	Benefits
E-learning usage statistics	• E-learning resources have been the most important ones in SWITCHaai • With the end of the SVC subsidies, financing the cost for content development, course tutors and LMS operation will become important for resource owners. • Interest in accounting and e-payment solutions has been expressed from different parties. Resource owners could satisfy their accounting requirement on their own, provided that an LMS offers the necessary functionality; but for the time being, there is no obvious solution. Thus, discussions with the e-learning resource owners have to continue. • A common format for e-learning resource usage will be needed as soon as usage data is exchanged between organizations. Therefore SWITCH is in the position to coordinate a community effort for a standardized e-learning usage data record.	• Better understanding of the resource owners and home organizations requirements and the role of a SWITCHaai-related accounting in the e-learning context. • Concerning the e-learning platform provided by SWITCH, usage statistics would improve SWITCH's service offering and is essential for cost allocation and capacity planning.

Table 4: Pilot project candidates

Besides new pilot projects, we recommend continuing the cooperation with the accounting-related projects:

- University of Berne: Integration of the student card solution and SWITCHaai in the areas of authentication and e-payment for roaming university members
- Grid: implementation of interoperability between Shibboleth-based AAIs and the EGEE grid infrastructure

As shown above, there are other accounting requirements outside the scope of this project, or where the relationship to SWITCHaai is vague. Although printing facilities have not been in the focus of SWITCHaai, many organizations are interested in an accounting and payment solution. We suggest organizing a community workshop where organizations can present their approach to control printing cost, e.g. by charging them to end users, and where SWITCH can find out its potential role in this area.

And last but not least, micro- and macropayment solutions may become important for universities in the future. SWITCH has been using such solutions from commercial providers for a long time (domain name registration) and has therefore valuable knowledge about implementing such solutions and about the operational processes. This might be an interesting future field of activity for SWITCH.

Appendix A: References

[AAIAttr]	AAI Authorization Attributes, Version 1.1, 15-JAN-2004 http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf
[COUNTER]	Counting Online Usage of NeTworked Electronic Resources (COUNTER) http://www.projectcounter.org
[Datatrans]	Datatrans http://www.datatrans.ch
[DGAS]	The Distributed Grid Accounting System (DGAS) http://www.to.infn.it/grid/accounting/
[Eduroam]	Eduroam http://www.eduroam.org
[EGEE]	Enabling Grids for E-SciencE http://www.eu-egee.org
[EZproxy]	EZproxy by Useful Utilities http://www.usefulutilies.com
[GEANT]	GÉANT2 http://www.geant2.net
[GGF]	Global Grid Forum http://www.gridforum.org
[GridBank]	“GridBank: A Grid Accounting Services Architecture (GASA) for Distributed Systems Sharing and Integration”, Alexander Barmoutta, Rajkumar Buyya, 2003, http://www.gridbus.org/papers/gridbank.pdf
[GridShib]	Integrating Shibboleth and Globus Toolkit http://gridshib.globus.org
[GN2JRA5]	GN2 - JRA5 - Roaming and Authorisation http://www.heanet.ie/research/research.php?serID=143&subID=37
[iPass]	http://www.ipass.com
[IPDR]	Internet Protocol Data Record http://www.ipdr.org
[LionShare]	LionShare, Pennsylvania State University http://lionshare.its.psu.edu
[Paypal]	http://www.paypal.com
[Polyright]	Polyright http://www.polyright.ch
[RFC2865]	Remote Authentication and Dial in User Service (RADIUS) http://www.ietf.org/rfc/2865.txt
[RFC2748]	The (COPS) Common Open Policy Service Protocol http://www.ietf.org/rfc/rfc2748.txt
[RFC2975]	Introduction to Accounting Management http://www.ietf.org/rfc/rfc2975.txt
[RFC3588]	Diameter Base Protocol http://www.ietf.org/rfc/rfc3588.txt
[Saferpay]	Saferpay http://www.saferpay.ch
[SAML]	Security Assertion Markup Language (SAML) http://www.oasis-open.org

[Shibboleth]	Shibboleth Project http://shibboleth.internet2.edu
[SWITCHaai]	SWITCH – Authentication and Authorization Infrastructure http://www.switch.ch/aai/
[SWITCHeconf]	SWITCH e-conferencing http://econf.switch.ch
[SWITCHmobile]	SWITCHmobile http://www.switch.ch/mobile/
[TIK111]	"A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond: A^x", Christoph Rensing, Hasan, Martin Karsten, Burkhard Stiller, TIK-Report Nr. 111, May 2001

Appendix B: Acknowledgement

We would like to thank the following people and their teams for discussing their accounting requirements and/or reviewing this study:

Dr. Andreas Dudler	ETH Zurich
Arlette Piguet	ETH Library Zurich
Hansruedi Born	SWITCH
Christoph Graf	SWITCH
Dr. Martin Sutter	SWITCH
Fabio Vena	SWITCH
Dr. Patrick Chénais	University of Berne
Dominique Petitpierre, Nicolas Rod	University of Geneva
Dr. Pascal Jacot-Guillarmod	University of Lausanne
Dr. Annette Langedijk	University of Zurich (VAM)
Michael Korner, Ivana Lachner	University of Zurich (Swiss Banking Institute)
Dr. Eva Seiler and team	University of Zurich (ELC)
Franziska Schneider, Marc Luder	University of Zurich (OLAT)
Prof. Burkhard Stiller and team	University of Zurich (ifi)