CASE STUDY OF THE USAGE OF AN AUTHENTICATION AND AUTHORIZATION INFRASTRUCTURE (AAI) IN AN E-LEARNING PROJECT

Aurelius Baier[1], Thomas Bernoulli[2], Torsten Braun[2], Christoph Graf[3], Ulrich Ultes-Nitsche[1,4]

[1]University of Fribourg

[2]University of Berne

[3]SWITCH

[1]Department of Computer Science, University of Fribourg, Boulevard de Pérolles 90, CH-1700 Fribourg, Switzerland, {aurelius.baier,uun}@unifr.ch

[2]Institute of Computer Science and Applied Mathematics, University of Berne, Neubrückstrasse 10, CH-3012 Berne, Switzerland, {bernoulli,braun}@iam.unibe.ch

[3]SWITCH, CH-8021 Zurich, Switzerland, christoph.graf@switch.ch

ABSTRACT

Authentication and Authorization Infrastructures (AAIs) are single sign-on systems. Their purpose is authenticating a user once, i.e. locally at the user's so-called home organization, and then checking authorization of requested resource accesses based on user attributes the user's home organization delivers. AAIs are just about being widely employed, and Switzerland is playing a pioneering role in AAI deployment as the national research and education network provider SWITCH has managed to get all Swiss universities involved in setting up an AAI. In that context, the SWITCH AAI is used, for instance, to control access to e-learning resources.

We will report in this paper on SWITCH AAI and its use in the VITELS (Virtual Internet and Telecommunications Laboratory for Switzerland). By doing so, we will discuss how the AAI middleware Shibboleth is used to implement a concrete AAI. After explaining how Shibboleth is used to implement SWITCH AAI, we will discuss how VITELS integrates into SWITCH AAI, including server (or better: service) integration of VITELS into SWITCH AAI as well as discussing which attributes are delivered cross organizations.

KEY WORDS

Single sign-on systems, Authentication and Authorization Infrastructures, cross-organizational authorization, web-resource protection.

---

[4] corresponding author

CASE STUDY OF THE USAGE OF AN AUTHENTICATION AND AUTHORIZATION INFRASTRUCTURE (AAI) IN AN E-LEARNING PROJECT

1 INTRODUCTION

Authentication and Authorization Infrastructures (AAIs) are single sign-on systems. Their purpose is authenticating a user once, i.e. locally at the user's so-called home organization, and then checking authorization of requested resource accesses based on user attributes the user's home organization delivers. AAIs are just about being widely employed, and Switzerland is playing a pioneering role in AAI deployment as the national research and education network provider SWITCH has managed to get all Swiss universities involved in setting up an AAI. In that context, the SWITCH AAI is used, for instance, to control access to e-learning resources.

We will report in this paper on SWITCH AAI and its use in the Swiss Virtual Campus (SVC) funded project VITELS (Virtual Internet and Telecommunications Laboratory for Switzerland) in which, among others, the universities of Berne (leading house) and Fribourg (project partner) participate. By doing so, we will discuss how the AAI middleware Shibboleth is used to implement a concrete AAI, explaining which features and modes of operation of Shibboleth are used and why they are used. After explaining how Shibboleth is used to implement SWITCH AAI, we will discuss how VITELS integrates into SWITCH AAI, including server (or better: service) integration of VITELS into SWITCH AAI as well as discussing which attributes are delivered cross organizations (here: cross universities) and how the data protection act restricts delivery of user attributes from one organization to another.

We believe that by presenting the case of SWITCH AAI and the integration of a concrete project into the infrastructure, readers who either currently are or in the future will be working on AAI will benefit from the experiences we will report on. It will be of general interest which design decisions have been made in both the establishment of SWITCH AAI and the integration of VITELS into SWITCH AAI.

2 AUTHENTICATION AND AUTHORIZATION INFRASTRUCTURES

2.1 Single sign-on systems

The basic motivation for creating AAIs is the creation of an efficient so-called *single sign-on system*. Users in single sign-on systems authenticate themselves only once using one set of credentials to one authentication service, and then the underlying infrastructure authorizes each single access request to a resource. This avoids having to remember several passwords for accessing several resources and by that increases security: It is much easier to convince users to create and remember *a single* good password than creating many good passwords and keeping them reasonably secret.

Figure 1 illustrates the differences between an old-fashioned multi sign-on system and a single sign-on one. It is not surprising that the example scenario in Figure 1 is an academic environment in which multiple resources exist some of which are accessed fairly infrequently. In particular in these situations, people tend to write down and store their passwords insecurely.

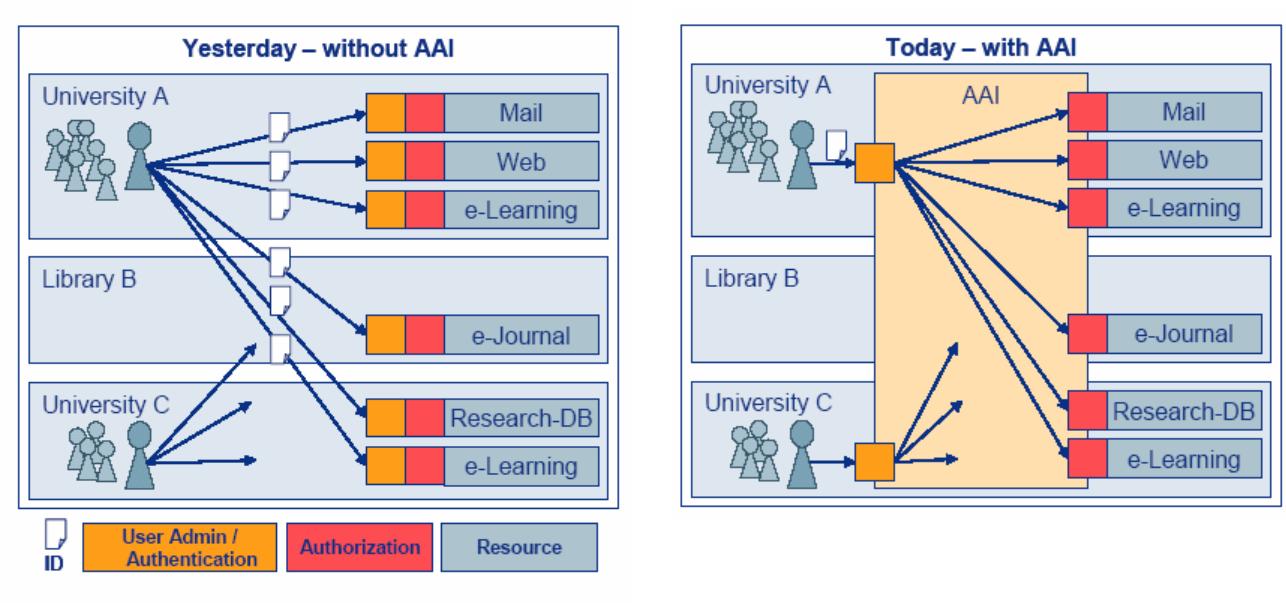

Figure 1. Multi- versus single sign-on. (SWITCH, 2006)

2.2 AAI

Having discussed single sign-on systems very briefly in the previous section, what are then the particularities of Authentication and Authorization Infrastructures? People knowing the Kerberos *(Neumann & Ts'o, 1994)* system, for instance, will well remember that the idea of single sign-on dates back to the 1980s. However, in Kerberos, the entire security system is controlled by a single institution. The ticketing system of Kerberos works cross-platform but not really cross-organization. And that is the major advantage of AAI: *cross-organizational authorization*.

Referring back to the example sketched in Figure 1, we see that a resource may be hosted by University A whereas the student requesting access to the resource may be enrolled in a programme at University C, and at the same time ordering books from a library B. AAI enables single sign-on systems which allow cross-organizational resource access authorization.

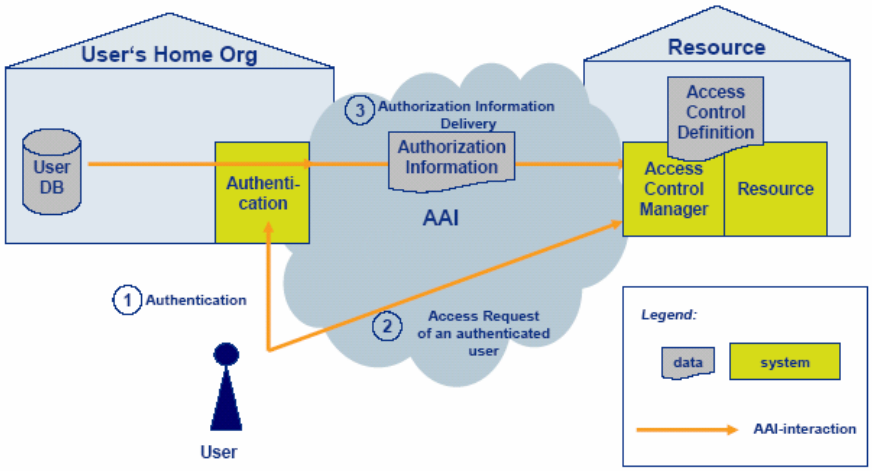

Figure 2. The most simplistic AAI model. (SWITCH, 2004)

The basic functionality of an AAI can be seen in Figure 2. A user will authenticate himself or herself to the user's home organization. When a user aims to access a resource, the home organization will deliver the necessary authorization information to the resource which will then grant or revoke user access based on the provided authorization information.

2.3 Shibboleth

Shibboleth *(Erdos & Cantor, 2001)* is an Internet2 (http://www.internet2.org) project implementing an AAI middleware based on the OASIS SAML specification (Security Assertion Mark-up Language) *(OASIS, 2006)*. In a nutshell, Shibboleth implements the AAI depicted in Figure 2 by adding all necessary components which render the scenario in Figure 2 possible.

In Shibboleth in contrast to Figure 2, user authentication does not necessarily happen before an access request to a resource. If a user attempts accessing a resource, the resource must find the authority which can deliver user attributes. It does so by prompting the user a "Where are you from?" question (WAYF). The answer to the WAYF reveals the user's home organization. The resource will ask the user's home organization, or more precisely: the home organization's attribute authority, to deliver the attributes required for granting resource access. The home organization will ask the user to authenticate himself/herself, if he or she has not done so before. When the user is authenticated, the home organization will send the requested attributes for that user to the resource which will then decide on the user's access request.

In order to create a secure AAI for all Swiss universities the national research and education network provider SWITCH has set up its own AAI based on Shibboleth, which is called SWITCH AAI.

3 SWITCH AAI

SWITCH AAI is a concrete AAI for all Swiss universities. The goal is obviously providing a secure AAI which is easy to use. Figure 3 shows the architecture of SWITCH AAI including all message exchanges necessary for a successful resource request in greater detail.

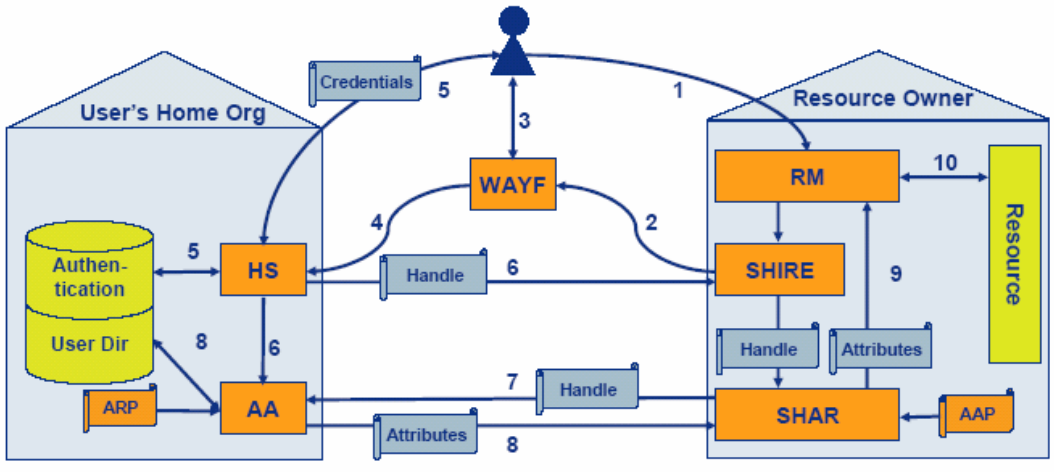

Figure 3. Structure of and message exchanges in SWITCH AAI. (SWITCH, 2004)

The abbreviations used in Figure 3 have the following meaning:

- HS: handle server (authenticates user and provides handle (pointer) identifying user)
- WAYF: where are you from server (redirects user back to the HS)
- AA: attribute authority (delivers attributes to the SHAR according to the ARP)
- ARP: attribute release policy (defines which attributes can be delivered to a SHAR)
- RM: resource manager (decides resource access request based on what was received)
- SHAR: Shibboleth attribute requester (requests attributes from AA according to AAP)
- AAP: attribute acceptance policy (defines which attributes are accepted to access resource)
- SHIRE: Shibboleth indexical reference establisher (ensures that resource receives handle (pointer) to user)

The data exchanges presented in Figure 3 are the following:

1. user connects web browser to resource web site
2. resource server redirects request to WAYF
3. user selects home organization
4. WAYF redirects user to home organization's HS
5. user authentication to the home organization
6. HS creates handle for user and redirects user to SHIRE which passes it on to SHAR
7. SHAR sends handle, resource address, and attribute requests to AA
8. AA sends attributes (ARP-controlled) to SHAR
9. attributes are verified against the AAP and are passed to RM
10. user accesses resource

It should be fairly obvious that the above data exchanges implement in more detail the simple Shibboleth scenario which we discussed in Section 2. The additional data exchanges are only internal data exchanges which enable realizing the visible steps of Section 2.

4 SWITCH AAI AND E-LEARNING: THE VITELS PROJECT

VITELS (Virtual Internet and Telecommunications Laboratory for Switzerland; http://www.vitels.ch) *(Zimmerli et al., 2003)* is an e-learning project *(Ultes-Nitsche et al., 2004)*, creating a virtual laboratory which allows students to run practical sessions with real, distributed networking equipment. Figure 4 depicts the general structure of the VITELS system.

In this system, different servers exist. These are:

- one **course server**, where the theory sections of all e-learning modules are located,
- eight **portal servers**, which control the access to the lab hardware
- and one **LDAP server** *(Wahl et a., 1997)*, which stores information about lab hardware reservation

The client of the student is connected to all servers through the internet. Also the portal servers are connected through the internet to the LDAP server.

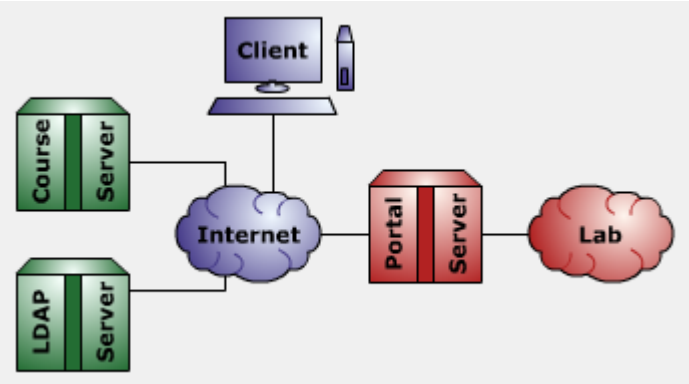

Figure 4. The VITELS e-learning infrastructure.

The theory sections, which are integrated into a WebCT e-learning system and the hands-on session represent intellectual property and may only be accessed by authorized users. As authorized students will not only come from a single university, cross-organizational authorization is mandatory. These are the reasons why the Swiss Virtual Campus (SVC) decided to use SWITCH AAI as the underlying security infrastructure for VITELS as well as for each other e-learning project funded by the SVC.

When a student wants to access the course server or any of the portal servers, he/she has to authenticate himself/herself at his/her home organisation, which then sends, in accordance to its ARP (attribute release policy), attributes of the student to the accessed resource. The accessed resource then decides according to its AAP (attributes acceptance policy) whether or not the received attributes are sufficient and whether or not the attributes received contain the required value. The attributes needed for a VITELS course are:

- given name
- surname
- unique ID
- e-mail address

These are the only attributes sent to the accessed resource. One should, however, note that the unique ID can be used to easily re-identify visitors across sessions. Up to this point, the entire scenario corresponds precisely to the process described in Section 3: SWITCH AAI. A problem occurs when a student wants to access the lab infrastructure through a portal server and the lab hardware (e.g. a hardware firewall which must be configured as part of the course) cannot be accessed by more than one user at a time. To solve this problem, VITELS uses the LDAP server where each student can allocate a timeslot for each specific lab device. The student reserves the timeslot using the web interface shown in Figure 5. When accessing the lab device, the portal server checks the permissions for the authenticated user on the LDAP server. No data is stored on the portal server; all the necessary information needed for authorization is stored on the LDAP server. Recall that to access the VITELS scheduling web interface – an AAI resource – users have already proved their authorization for accessing the lab resource.

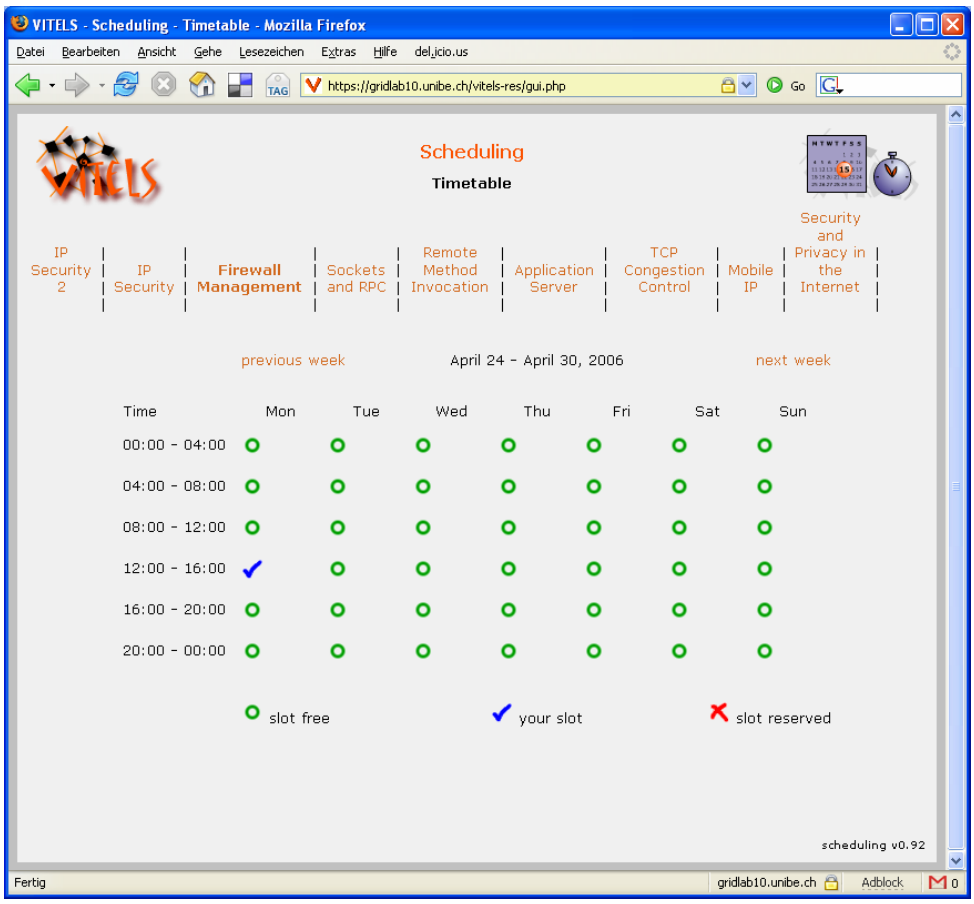

Figure 5. The VITELS scheduling web interface.

5 DISCUSSION

5.1 Security of AAIs

AAIs are secure systems. Initially the users and then the involved subsystems must always authenticate themselves properly.

5.1.1 User Authentication

In principle, users can authenticate themselves to their home organization in all imaginable ways. To date, the most widely used way of user authentication is still giving a username and password. The weakest link, as in many other systems, is thus again the user. If he or she does not use good passwords or does not keep passwords secure, the entire system is compromised. As we are dealing with a single sign-on system, a cracked password opens up all resources for exploitation to which the user whose password was cracked had access. This problem is apparently inherent to all single sign-on systems based solely on username/password, including also Kerberos.

5.1.2 Resource Authentication

SWITCH AAI uses a public-key infrastructure (PKI) and a resource registry for resource authentication. Therefore each resource is only accepted within VITELS if it is in possession of a valid SWITCH AAI certificate and registered in the SWITCH AAI resource registry. The certificate will expire every year. Only if the institution responsible for the resource actively renews the certificate will the resource remain available within the AAI.

Resource authentication helps avoiding rogue resources e.g. aiming at maliciously replacing valid resources in the AAI, e.g. with the aim of trying to trick users or home organizations into

giving away confidential information. It is well known that certification does not solve information security but it provides an additional security layer within the AAI.

5.1.3 Main Benefits

At first glance, because of a cracked password opening up a bunch of resources at once, AAIs could be regarded as less secure than multi sign-on systems. But is that really true?

As already discussed before, it is much easier for a user to create a single good password and memorize and manage it well. With multi sign-on systems, the likelihood of bad password creation and management increases with each additional resource. In addition, users tend to re-use the same password for multiple resources, again opening them all up when the password is cracked. In particular if a rogue resource manages to get user-authentication information, with some likelihood it can maliciously use it to access other resource.

So by facilitating resource access in an AAI, it is easier to make users aware of potential security problems (opening access to one web resource sounds less threatening than opening access to a multitude of resources at once), giving them an incentive and an easy-to-use technical infrastructure for sticking with a given security policy.

Since authentication takes only place at the home organisation's authentication server, resources never get hold of passwords. This further reduces risks arising from rogue resource managers.

We have already mentioned the problem of rogue resources trying to get confidential user information. As AAI implements resource authentication, this problem vanishes or is at least reduced to good certificate management. In VITELS and SWITCH AAI in general, the process of applying for a resource certificate is quite involved, requiring clear justification of why the resource should be included into the AAI before delivering a certificate, which significantly reduces the risk of giving a certificate to a not trustworthy resource. So in essence, sensibly using an AAI helps securing an infrastructure.

5.2 AAI and E-learning

From our point of view, AAI is ideal for e-learning environments. Whoever wants to join an e-learning system and access the e-learning resources is confronted with moderate initial costs of setting up a client-side AAI. After that it is only up to the agreements between different learning centres, e.g. universities, which users may access which learning resources. This can be controlled easily by the attributes required to access the resource. This, of course, holds only true, if some entity is organising the AAI for all potential resources and students.

Our case study reports on an e-learning project in the fairly small and reasonably homogeneously populated country of Switzerland. Taking in contrast South Africa, a vast country with very varied population density, the benefits of setting up an e-learning AAI appear even more to outweigh the necessary initial investments. In addition, South Africa could act as an AAI enabler for other African countries, offering well-secured e-learning services. For that reason we belief that the presented case study may interest both the South African security specialist who is interested in securing on-line resources such as web services and the South African e-learning expert who wishes setting up a well protected e-learning infrastructure.

5.3 Data Protection Issues

When using AAI in the e-learning project VITELS, we were initially completely unaware of being confronted with problems of data protection beyond controlling access to confidential data in the usual way. However, taking into account that resources can request from the WAYF-server

arbitrary user attributes the resources' managers consider necessary for accessing a resource, the requests may ask for attributes protected by a country's data protection act. Interestingly enough, at the different universities involved in the VITELS project, data protection was treated quite differently. At one university in particular, the person in charge of implementing information security had to be convinced in many meetings that sending information about the degree programme in which a student is enrolled may not conflict with the Swiss data protection act.

What can be learned from this experience is that besides the technical issues, setting up an AAI requires a good analysis of which data is really needed to authorize an access request to a resource; the famous need-to-know principle must be respected.

6 CONCLUSIONS

We reported on the e-learning project VITELS, highlighting the usage of SWITCH AAI, an Authentication and Authorization Infrastructure, for controlling accesses to learning resources. The case study we presented is applicable to any type of web-based service provisioning, even though secure access to e-learning resources is the main focus of this paper. AAI can definitely build an interesting framework for e-science and grid-computing infrastructures, too.

We believe that the way Shibboleth is used within SWITCH AAI is well chosen for many applications besides e-learning. It is the aim of the paper to motivate people to consider AAI as an option for creating cross-organizational collaboration environments, which are flexible, ergonomic, and secure.

7 REFERENCES

B. Clifford Neuman, Theodore Ts'o. *Kerberos: An Authentication Service for Computer Networks*. IEEE Communications, 32(9): 33-38, 1994.

M. Erdos, S. Cantor. *Shibboleth-Architecture DRAFT v04*. Internet2, 2001. http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v04.pdf

OASIS. *OASIS Security Services (SAML)*. OASIS, 2006. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

SWITCH. *AAI – Authentication and Authorization Infrastructure System and Interface Specification*. SWITCH, 2004. http://www.switch.ch/aai/docs/AAI_System_Specs.pdf

SWITCH. *Authentication and Authorization Infrastructure (AAI) in a nutshell*. SWITCH, 2006. http://www.switch.ch/aai/docs/AAI-Flyer_en.pdf

U. Ultes-Nitsche, A. Baier, M. Mäder, T. Braun, M.-A. Steinemann, A. Weyland, P. Joye, R. Scheurer. *Online Practical Telecommunications Training – The VITELS Project*. 33rd International IGIP / IEEE / ASEE Symposium. Pages 385-390, 2004.

M. Wahl, T. Howes, S. Kille. *Lightweight Directory Access Protocol (v3)*. IETF, RFC 2251, 1997. http://www.ietf.org/rfc/rfc2251.txt.

S. Zimmerli, M.-A. Steinemann, T. Braun. *Resource Management Portal for Laboratories Using Real Devices on the Internet*. ACM SIGCOMM Computer Communications Review, 33(3): 145-151, 2003.