

SWITCH

The Swiss Education & Research Network

AAI - Authentication and Authorization Infrastructure

Task Force Certificate Authority Final Report

Document management

Version/status: 1.0 / final

Date: 15-JUL-03

Author(s): René Hüsler HTA
Alberto Salerno at rete ag

File name: AAI_TF_CA_Report_v10.doc

Replacing:

Approved by:

Table of Content

1.	Management Summary	4
2.	Introduction	4
3.	Aims of the Task Force	4
4.	Survey of Projects	4
4.1	EPFL	4
4.2	ETHZ	4
4.3	CERN	5
4.4	SWITCH	5
5.	Catalog of Requirements	5
6.	Models	6
7.	Policies	7
8.	Certificate Quality and Distribution	7
9.	Conclusions	8
10.	Miscellaneous	8
10.1	Swiss Laws	8
10.2	CA outsourcing	8

1. Management Summary

The SWITCH AAI Certificate Authority Task Force (TF) focused primarily on server certificates since these represent the main usage for the AAI. End-user certificates have to be handled by a separate task force but the basic ideas and structure of the SWITCH Root CA are able to support them in a later stage. Apart from the technical aspects the legal ones have to be specified before the SWITCH Root CA can be set operational.

2. Introduction

This paper summarizes the findings of the AAI Certificate Authority Task Force (TF). The TF met twice during the months of March and April 2003 and was lead by Christoph Graf of SWITCH and René Hüsler of HTA. Its work was supported by a mailing list at <http://chx400.switch.ch/mailman/listinfo/aai-tf-ca>. The list of participants can also be obtained at the same address.

3. Aims of the Task Force

The work of the TF was based on previous work such as:

- Preparatory study (www.switch.ch/aai)
- Shibboleth doc (shibboleth.internet2.edu).

The TF had the following aims:

- Survey of projects requiring PKI services
- Describe Certificate Authority (CA) requirements of those projects; sketch CA architecture candidates
- Find the best CA architecture candidate
 - satisfying a maximum set of projects (including at least AAI)
 - still providing advantages compared with an AAI-only approach
- Use this candidate to draft an architectural CA design covering its services and policies.

4. Survey of Projects

4.1 EPFL

The EPFL deploys its own CA based on open source software. People must be registered and present an ID to be enrolled for an end user certificate. There is no certificate usage policy. The EPFL has wide experience in running a certificate-based authentication infrastructure (GAS-PAR).

4.2 ETHZ

The ETHZ has started a project for distributing server certificates end of last year and stopped it because of SWITCH's activities, expecting that SWITCH will run its own root CA and the ETHZ may use a subordinate CA signed by SWITCH. Certificates for servers are requested through a Registration Authority (RA) located at the ETHZ. The ETHZ is interested in a SWITCH CA pri-

marily in order to avoid self-signed certificates and high costs using “true” certificates (they use currently about 300 server certificates).

4.3 CERN

CERN runs the LCG (Large Hadron Collider Computing Grid) Project and collaborates with other grid projects. Certificates are used in the context of GIS (Grid Infrastructure Security; long-term certificates and short-term certificates created by proxy services in the name of the end user / process) only for authentication / protecting resources (data in the physics environment tends to be moved in unencrypted form and without content authentication).

The GRID project uses different nation-wide CAs. Due to the fact that no nation-wide CA is currently available in Switzerland, they run their own CA. Certificates are used for authentication across the current grid testbeds with multiple sites across Europe (no problem with the browser, batch distribution and so on). The model is not hierarchical at the moment. If SWITCH operates its own CA, CERN would be interested in participating.

CERN, through its participation in the EDG, has experience in developing policies and in dealing with the complex net of trust and relationships a certificate-based authentication mechanism brings. They also provided the policy prototypes for the AAI project.

4.4 SWITCH

SWITCH has experience with server certificates due to the AAI project. In particular the Shibboleth toolkit uses certificates to protect data communication among servers. The AAI project is expected to involve about 200 servers and an estimated 200'000 users.

5. Catalog of Requirements

During the two meetings a general catalog of requirements was drawn up. Due to the different needs and points of view among the participating organizations and people, the catalogue was kept rather general:

- Data encryption and authentication of the service on the wire in a manageable fashion
- Hassle-free
- Cheap
- User-friendly
- Hierarchical (it should be possible for each organization to run its own CA)
- Distributed registration authority
- Certificate Revocation should be considered
- End user certificates (at least technically) not to be excluded
- Maximally one certificate chain import should bother the end user

6. Models

Figure 1 summarizes the general model for a CA infrastructure capable of sustaining the AAI project:

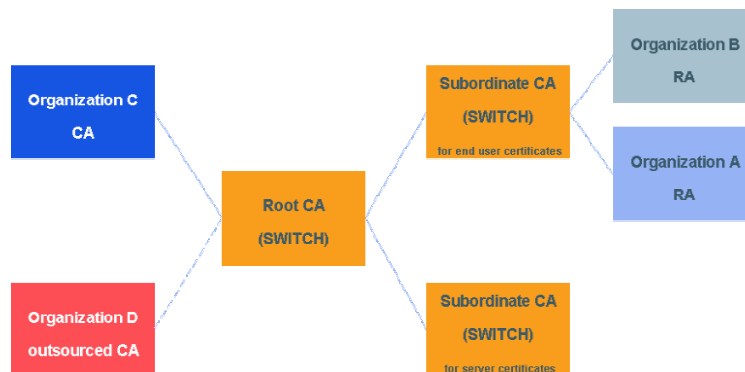


Figure 1: General CA model

The model tries to capture all relevant aspects of a CA supposed to sustain the AAI project. Some of the findings need to be verified through a pilot implementation.

Each organization may choose to:

- use its own CA and do cross-certification (Organization C, which means that Organization C trust all certificates issued by the Root),
- use an outsourced CA and do cross-certification (Organization D, but presumably not implemented in the next two years); or
- use the SWITCH root and subordinate CA for server certificates and generate certificates through locally installed Registration Authorities (RAs).

The general model is the result of merging different models. Even if not strictly necessary, it would be interesting to have a Root CA signing a subordinate CA for server and end user certificates, because this would help to improve the security of the whole architecture. Fact is that subordinate CAs are the ones most likely to be compromised. If a subordinate CA got compromised, only these subordinate CA certificates would need to be revoked along with the publication of a new CRL.

Moreover, using root and subordinate CAs, different security levels could be implemented: the root CA can use a longer private / public key pair (e.g. 4096 bits compared to 2048 or 1024 bits for subordinate CAs), needs to sign much fewer certificates and can be stored more safely than subordinate CAs. Also the time validity of the two certificates differs: a root CA certificate lasts much longer (e.g. 10 years at the EPFL, compared to 4-5 years for subordinate CAs). In addition, it would be possible to experiment with key pair compromise of root and subordinate CAs. A root CA in the design will make it possible to deal with a hacked subordinate CA (e.g. the private key is compromised).

Using two subordinate CAs for servers and end user certificates mimics the model used in the business world (all the major CAs have such a model, e.g. Swisskey or Verisign).

It is not clear if CRLs are going to be used for server certificates. If a certificate is reissued every year – maybe along with a key pair renewal – the older one will be unusable for authentication purposes. In any case, the RFC 2510 mandates that a certificate renewal should be feasible.

A variation of the general model may include the use of two separate root CAs for server and end user certificates. This would simplify the architecture and their management, minimize the certificate import number to just one, but will also reduce the security level and the resistance against failure of single branches.

In the next two years, SWITCH will concentrate on server certificates. Nevertheless, the structure and the policy used should not forget end user certificates so that an easy integration will be possible in the future. It is not so much technical but rather legal aspects that make end user certificates difficult to deal with.

7. Policies

The SWITCH Certification Authority Certificate Policy and Certification Practice Statement (CP/CPS) describes the policies and practice statements for the SWITCH Root CA which have to be accepted and adopted by subject CAs. Based on RFC 2527 and the CP/CSP from CERN, a draft version of SWITCH's CP/CPS¹ has been defined.

8. Certificate Quality and Distribution

Certificate costs depend on the quality of the certificates (how difficult it is to get a certificate and how securely the private keys are stored).

On the one hand, it is easier to use certificates from well-known CAs (e.g. Thawte), because the end user does not have to install the self-signed root certificate in his/her local certificate store and, moreover, does not have to deal with pop-up windows pointing out invalid certificates (one certificate import means one button click).

On the other hand, it is also a matter of price: if the AAI widely deploys certificates signed by well-known CAs, it will be very expensive (about USD 300 per server/year, which makes about USD 60K per year for the about 200 servers involved in the AAI project). Yet managing a dedicated CA for the AAI project could also generate high costs.

In the EPFL's experience, some users complain about importing certificates, and generally end users DO NOT understand certificate technology and will not in the long run. A mixed model could be the solution. Nevertheless, the end users should be instructed how to import certificates in their local store. As a means of support, the AAI could provide detailed instructions on a dedicated web page.

Other means of promoting root certificate distribution are:

- unencrypted front-ends that advises the end user to install the server root certificate, and
- code signing.

It appears to be very difficult for Swiss academic institutions to get Verisign certificates, because it is difficult to convince Verisign to trust them (academic institutions are not the same as commercial companies).

¹CP/CPS Version 0.3/draft, OID 2.16.756.1.2.6.1.0.3, dated 29. April 2003 (<http://www.switch.ch/aaai>)

SWITCH prefers a more local approach rather than well-established commercial CAs; yet if a favorable arrangement including good support can be found, it will be considered.

9. Conclusions

- This task force has only dealt with server certificates till the end of April; the issue of end user certificates and the appropriate policies was delegated to a new task force.
- The time horizon for the first deployment of server certificates is about 2-3 years. The time horizon for end user certificates will be 3-5 years. Nevertheless, CERN needs end user certificates for all preparation and deployment in the EDG project.
- Basic policies both for root and subordinate CA should be effective from the beginning.
- Start with a basic design and a prototype as soon as possible.
- It will be easier to build up trust if every organization involved uses the same policy (like in the IDG project, same source); SWITCH's policies could use CERN's policy as a prototype.

Open issues:

- Distribution of certificate chains: If locally run CAs are allowed, each organizational root CA certificate chain should be distributed.
- It should be possible to distribute one single bundle instead of many certificate chains. If a new CA comes into play, bundling and distributing could be a problem. A solution would be to find out which organizations are interested in running their own CA and include their certificate chains as soon as possible in the distributed bundle.

10. Miscellaneous

10.1 Swiss Laws

A Swiss order law ("Verordnung") on certification services exists, but it deals only with the requirements to be certified by the "Amt für Akkreditierung". The assessment is on a voluntary basis. The certification assessment is outsourced to KPMG and is not only intended for commercial purposes.

A discussion had taken place in Switzerland whether or not the Swiss government was appropriate to run its own CA, which resulted in the decision that the government should merely put in place a quality standard for CA, but not own one. At the moment no certified CA is known.

Nation-wide companies operating in the CA and certificates business are SwissSign and Wisekey.

Swiss data protection laws may have an influence if end user certificates are used. Policies should therefore include statements on end user certificates.

10.2 CA outsourcing

Outsourcing of CA services will be considered, if such services are available with adequate cost and quality

Appendix A: Sources

- Preparatory study (www.switch.ch/aai)
- Shibboleth documents (shibboleth.internet2.edu)
- RFC 2510 “Internet X.509 Public Key Infrastructure Certificate Management Protocols” (<http://www.ietf.org/rfc/rfc2510.txt>)
- RFC 2527 “Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework” (<http://www.ietf.org/rfc/rfc2527.txt>)
- CERN CA Certificate Policy and Certification Practice Statement (<http://globus.home.cern.ch/globus/>)
- AAI-CA-TF meeting minutes
- Presentation slides

Appendix B: Abbreviations

CA	Certificate Authority
CERN	Centre Européen pour la Recherche Nucléaire
CRL	Certificate Revocation List
EDP	European DataGrid Project
EPFL	École Polytechnique Fédérale de Lausanne
ETHZ	Eidgenössische Technische Hochschule Zürich
TF	AAI Certificate Authority Task Force