

University of Michigan Certificate Authority System Technical Reference

Marcus Watts

Dan Hyde

Bill Doster

Mike Graham

University of Michigan

ABSTRACT

This document describes the system to manage the University of Michigan institutional certificate authority. This system is intended to be low cost and easy to set up, yet highly secure and dependable. This document is primarily a technical reference; policy issues are not discussed here.

1. Introduction

A certificate authority is a fundamental part of any PKI infrastructure. The root authority of any institution is a very important component, because the security of this component determines the maximum amount of security available. Traditional solutions have involved the purchase of expensive proprietary hardware. The solution we are using is to use an ordinary mass-market laptop computer, together with open-source software and a good physical security system. This system should offer equivalent or superior security at much less cost. This document is intended to satisfy the functional requirements of [OPI] section 3.2 (Overview of the Set of Recommended Practices and Underlying Principles) and 3.5.2 (Security of the Campus Certificate Authority Server).

2. CA hardware

The basic idea is that we have a laptop dedicated to *just* be the hardware for the CA. In order to function as a CA, the laptop runs openssl (open, free software). Openssl runs under the openbsd operating system (open, free software). The laptop is used for no other purpose; when not in use, it is kept locked up in a safe deposit box at a local bank. Keeping the entire computer locked up ensures that people can't tamper with the hardware or the software running on the machine. The laptop will never be attached to any sort of network. The only way the laptop will communicate to the external world is via keyboard, LCD display screen, and floppy drive. After the initial installation of software, the laptop should not need any further software upgrades. The general reasons to do software upgrades are for software improvements, better hardware support, and security fixes. None of these will be important for this laptop.

To protect against both unauthorized use and accidents (such as fire), the laptop is stored in a safe deposit box at a local bank. Arrangements have been made with that bank so that access to the box requires the presense of at least two people from the authorized list. The laptop is used on the premises of the bank to sign new UM CA certificates which are copied to a floppy for transport and the laptop is then returned to the safe deposit box.

CA "best practice" requires that two people be necessary in order to access and use the CA; for instance, this is a recommendation of [OPI] section 3.5.2 (Security of the Campus Certificate Authority Server). We require two people to access the University of Michigan CA. To do this, we assign each person a different password. Then, for each of the possible pairs of people, the private key for the CA is encrypted under both of their keys. All of the resulting doubly-encrypted CA-keys are stored on a

floppy disk which is stored with the laptop in the safety deposit box.

The laptop is stored with a hardcopy of all necessary procedures. One of these procedures is how to create a KCA certificate (which would then issue temporary certificates to kx509). If it is approved, we hope to add a procedure to create web server CA certificates (which would then issue web server certificates). The documentation also includes any necessary operating system passwords, but not the passwords required to decrypt the CA private key. In addition, the procedure to restore the CA from backup media is also documented. A copy of these procedures, complete except for passwords and actual location of the vault, will be published in a public location, either in AFS, or out on the web.

In order to ensure that the laptop security is not accidentally compromised, it should have a notice that reads like this:

This laptop contains important cryptographic secrets.
It must be either physically secured, or guarded by at least two (2) persons at *all* times.
The hard disk *must* be completely erased before being discarded or reused for any other purpose.

3. Disaster recovery

For disaster recovery purposes, a second laptop need not be kept. What is necessary is a copy of the private key itself, and all the procedures and software that were installed on the laptop. This is stored on a combination of floppies and CD-roms, such that if the original laptop is destroyed or fails, everything can be quickly resolved by installing everything on a new laptop. This should include everything down to the OS, such that it can be rapidly restored without any questions about trusted media. A hardcopy of all the procedures should also be kept with the backup data. Since this does not need to be accessed in normal use, and should be very compact, it can be kept separately. We are working with University Internal Audit to determine an appropriate storage location.

Ideally, the disaster recovery data should be divided into "secret" and "non-secret" portions. The operating system is a "non-secret" part; it should be a known and trusted copy, but is not secret. The private key is the "secret" part; it must be kept highly guarded at all times. The operating system ought to be installed first and its operation verified. For instance, a dummy certificate might be installed and tested, and the machine shut down & brought up without errors. Once it is determined the machine is functioning properly, the private key should be installed as the last step. Once this is done is when the laptop, and its security, become particularly important, because it now holds the secret and all the tools necessary to use the secret.

The floppies or other secure media represent a compromise point just like the laptop, and so should have a similar notice affixed to them:

This floppy contains important cryptographic secrets.
It must be either physically secured, or guarded by at least two (2) persons at *all* times.
This floppy *must* be completely erased or destroyed before being discarded or reused for any other purpose.

4. Procedures

Complete procedures should be included with the laptop, so that there is no question on how to use the software. These procedures will include:

- kca cert issue How to issue a certificate for KCA.
- web CA issue How to issue a certificate for a web server CA.
- top level certificate generation/renewal
 A CREN-signed certificate is used which expires every 2 years. The procedure for obtaining a new one from CREN should be fully documented, and done in a timely fashion.

system restore How to load the system from CD-rom, verify operation of the system, and install the certificate from floppy.

The certificate issue functions would be used on a daily operational basis by the IAA team. The system restore function might be used either directly by the IAA team, or perhaps more likely, by technical persons brought in and trusted by the IAA team to perform those operations.

CREN-signed CA certificates normally last for only 2 years. Therefore, there needs to be a procedure to acquire and update the top level certificate every 2 years.

All procedures should include provisions for an audit log. The audit log may be public, and must include all uses of the certificate and laptop.

Procedures should include some description of how the name and other attributes of the certificate is verified.

Procedures should include a description of how to copy a certificate request from e-mail to floppy, and how to extract the results from floppy and post them in e-mail. The procedure for handling a certificate request must include a description of how the request is authenticated. The actual data being shipped back & forth does not need to be hidden, it merely needs to be authenticated and tamper-proof. The way that an end-user might create a certificate request should also be described. The final certificate could be just as easily published on the web; the only secret is the private key, which should never be seen by the CA.

5. Termination

There are two ways in which the need to retire the CA hardware or key from use can arise. The first is that through evolution of normal business practices, it may become obsolete. The second is that it can be actively compromised. In both cases, there are important steps that must be followed to not create new problems.

Retirement of the CA is the simpler case to explain. Even if the CA is no longer being used, the certificates it issued may still be used to protect data. In order to protect the security of that data, the private key used by the CA must be properly disposed of, so that they can't be mis-used to forge certificates. These are contained on the hard disk in the laptop, and in any floppies that contain the key. For both storage media, it is important to *complete* erase the data contained on them. This can be accomplished by overwriting *all* data on the disk 100 times with different patterns, followed by a complete low-level format, or by total physical destruction of the media. This may seem like overkill, but tests have shown that simply overwriting the data once may leave sufficient traces behind that the previous data can be recovered.

If the CA security is compromised, and a person or persons known or unknown have unauthorized access or have had made unauthorized use of the private key of the CA, the following organizations should be contacted:

- DPS University of Michigan Department of Public Safety. 911 via any University phone, or (734) 763-1131.
- Risk University of Michigan Risk Management (734) 764-2200; 400 S. Fourth St; Argus II Building
- CREN Corporation for Research and Educational Networking
 cren@cren.net
 Phone: 202-293-5909
 Fax: 202-293-2853
- police Upon the advice of DPS, or if DPS cannot be contacted, call local police. If the matter appears to be inter-state, also call the FBI. In both cases, if they ask for a dollar amount on the damage, if you do not have better data on the cost, tell them "unknown but could be in excess of \$100,000." It is better to overestimate the expense than to underestimate; the police and FBI will not investigate trivial incidents.
- sub-CA Contact any subsidiary CA's issued by this CA at the university, including KCA and web services. Advise them that the top level certificate has been compromised.

Both of these should be described and documented as procedures, to accompany the other procedures documented and used by the CA.

6. Resources Needed

The resources that are needed to implement this are:

Laptop At least 8M ram required; at least 32M preferred. At least 1G hard disk. 386 or better CPU required; >100 Mhz pentium preferred. Floppy and CD-ROM required. Bios CD-ROM boot capability preferred. Machine must be compatible with some popular distribution of linux or OpenBSD; OpenBSD is preferred.

CD-rom burner

In order to make copies of the OS sufficient to restore the laptop, the temporary use of a machine with a CD-rom burner will be required. This machine is only required during setup, it is not required after that.

PGP If a CREN certificate is used, PGP is the means by which the ICATC transmits the certificate request, and securely receives the signed certificate.

CAEO This is the person who is in charge of the operation of the CA. once it is set up. This person may or may not have access to the laptop.

CA team These are the people responsible for operating the CA once it is set up. They are the only ones who have physical access to the laptop. It is highly recommended that the procedures and physical security require that more than one person from the CA team be present in order to make any use of the laptop.

ICATC If a CREN certificate is used, the ICATC is the person who receives the signed certificate from CREN. This person would need to be one of the members of the CA team.

7. References

[OPI] Cren Certificate Authority Service, "Operations and Practices for Institutions Document (OPI)", 23 March 2000.

[CPS]CREN, "Certificate Practices Statement", 27 January 2000.