

Version: 0.43
Last Updated: 08-18-2004
By: Nick Lewis

Internet2 Certificate Authority for the InCommon Federation System Technical Reference

ABSTRACT

This document describes the system to manage the InCommon certificate authority. This system is intended to be low cost, easily set up, easily replicated by others, yet highly secure and dependable. This document is primarily a technical reference. Policy issues are not discussed here, but can be found in the Internet2 InCommon Certificate Policy, Certificate Practice Statement, and other related documentation.

1. Introduction

A certificate authority is a fundamental part of any Public Key Infrastructure. The root authority is the most important component, because the security of the root determines the maximum amount of security available. Traditional solutions have involved the purchase of expensive proprietary hardware and software. We are using a laptop computer, together with open-source software and good physical security. This system should offer equivalent security at much less cost.

2. CA hardware

We have a laptop dedicated to the CA. In order to function as a CA, the laptop runs Openssl (open source free software). Openssl runs under the Linux operating system (open source free software). The CA software CSP will be used. (<http://devel.it.su.se/projects/CSP/>). The laptop is used for no other purpose. When not in use, it will be kept in a safe at the Internet2 Ann Arbor office. Keeping the entire computer physically secure ensures that people can not tamper with the hardware or the software running on the machine.

The laptop will never be attached to any network. The only way the laptop will communicate with the external world is via keyboard, display screen, floppy drive, CDRW drive, or USB storage device. After the initial installation of software, the laptop should not need any further software upgrades. It may be necessary to update individual software as required to support critical security fixes or features needed by the InCommon Federation. The general reasons to do software upgrades are for software improvements, better hardware support, and security fixes. None of these should be important for this laptop, but if an update to the software is needed, it will be logged with the exact changed software.

The laptop is used on the premises of Internet2 to sign new InCommon Federation end entity certificates which are copied to a USB storage device for transport and the laptop is then returned to the safe. CA best practice requires that two people be necessary in order to access and use the CA. We require two people to access the InCommon CA. To access the CA, 2 separate keys will be needed to unlock access to the safe and no person will have both keys. The private key will also have a password specified to use for signing certificate signing requests that Operators of the CA will know. The CA keys are stored on the hard disk which is stored in the laptop in the safe. The laptop is stored with a hardcopy of all necessary procedures. The documentation also includes any necessary operating system passwords, but not the passwords required to decrypt the CA private key. The password to decrypt the CA private key will be stored in its own safe deposit box apart from all other data. In addition, the procedure to restore the CA from backup media is also documented. A copy of these procedures, except for passwords and actual location of the safe, will be published in a public location.

In order to ensure that the laptop security is not accidentally compromised, it will 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 will be securely destroyed before discarded and will not be reused for any other purpose.

3. Disaster recovery

The private key itself and all the procedures and software that were installed on the laptop are necessary for disaster recovery. This is stored on a combination of floppies and CD's, such that if the original laptop is destroyed or fails, CA services can be quickly restored 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 will be kept separately in a safe deposit box at a local bank. Ideally, the disaster recovery data should be divided into "secret" and "non-secret" portions. The operating system and operational details are a "non-secret" part. It should be a known and trusted copy, but is not secret. The private key is the "secret" part. The private key must be kept highly guarded at all times. The operating system should 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 that the machine is functioning properly, the private key should be installed as the last step. Once these steps are done, 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. The floppy disk must be securely destroyed before discarded and will not be 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:

InCommon Certificate issue: How to issue an end entity certificate for the Internet2 InCommon Federation. This is included in the CSP User Guide.

Top level certificate generation/renewal. This is included in the CSP User Guide.

Disaster Recovery

The certificate issue functions will be used on a daily operational basis by the Internet2 Technical Services Group (TSG). The system restore function may be used either directly by the Internet2 TSG group as necessary.

The Internet2 InCommon self-signed certificate will be used at most for 10 years, but will be re-keyed every 5 years. Therefore, there needs to be a procedure to update the top level certificate every 5 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 are verified from the Storefront Operations Procedures. Procedures should include a description of how to copy a certificate request from the secure database to floppy, and how to extract the results from floppy and post them in the secure database. The procedure for handling a certificate request must include a description of how the request is authenticated. The actual data being communicated back and forth does not need to be hidden, it merely needs to be authenticated and tamper-proof. The generation of a certificate signing request will also be described. The final signed certificate will be e-mailed to the requestor. The only secret is the private key of the requestor, which shall never be seen by the Internet2 InCommon 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 additional 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 it can not be misused to forge certificates. This is contained on the hard disk in the laptop, and in any removable media that contain the key. For both storage media, it is important to securely destroy them. This may seem unnecessary, but research has shown that simply overwriting the data 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 Internet2 TSG Group should be contacted:

This should be described and documented in the 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 with minimum hardware necessary to run Linux, but no network card will ever be present in the system.
- Floppy and CDRW drive required and USB storage device as needed.
- All necessary equipment for the secure operation of the storefront and secure database.
- Safe in Internet2 office and safe deposit box at local bank

7. Acknowledgements

This document is based on a document that Marcus Watts, Dan Hyde, Bill Doster, and Mike Graham wrote for the University of Michigan. IJ Kim and Mike LaHaye were instrumental in producing this document.