

Version: 0.22
Last Updated: 08-18-2004
By: Nick Lewis

InCommon Federation Infrastructure Technical Reference

Abstract

This document describes the system to manage the Internet2 InCommon infrastructure. This system is designed to be a highly secure and dependable system. 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, Federation policies, and other related documentation.

1. Introduction

The secure operations of the InCommon Federation Infrastructure are paramount to maintaining the trust fabric of the federation. The federation infrastructure is a very important component, because the security of the infrastructure helps determine the maximum amount of security available to the federation.

2. Infrastructure hardware

The procedures to restore the InCommon infrastructure from backup media will also be documented. A copy of these procedures will be published in a public location

A centralized WAYF service will be provided for the InCommon Federation. A secure database will be used for the management of certificate signing requests, certificate revocation requests, Metadata signing, and secure storage of contact data. This server will be protected behind a firewall. A network diagram is available on request. A general service web front-end will be provided for application to and enrollment in the InCommon federation. Contact management, relationship management, and accounting services database in support of subscriptions will be maintained.

Centralized administrative access will be utilized to protect against compromised client interaction with the secure administrative interfaces via a terminal server. Backups will be maintained for all services to ensure data availability.

A Certificate Authority will be maintained. See Internet2 InCommon CA documentation for more details. Secure storage and physical operations of CA services will be maintained in a controlled access environment.

3. Disaster Recovery

For disaster recovery purposes, redundant hardware will be used in the infrastructure. Backups will also be made to protect against loss of data. A hardcopy of all the procedures will 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. Passwords and the CA private key are the “secret” part. The passwords and private key must be kept highly guarded at all times. The operating system will be installed first and its operation verified. Once it is determined the machine is functioning properly, the servers should be put into production as the last step.

4. Procedures

Complete procedures will be developed for the operation of the federation.

These procedures will include:

- HEPKI-LITE Certificate Profile
- HEPKI-LITE Certificate Policy
- HEPKI-LITE Certificate Practice Statement
- Internet2 Certificate Authority for the InCommon Federation System Technical Reference
- Storefront operations
- Disaster Recovery

The infrastructure issue functions will be managed 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 as necessary.

5. Termination

There are two ways in which the need to retire the infrastructure hardware 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 infrastructure is easier to explain. In order to protect the security of that data, the private data used by the federation must be properly disposed of, so that they can not be misused. These are contained on the hard disk and in any removable media. 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 federation security is compromised, and a person or persons known or unknown have unauthorized access, the Internet2 TSG Group should be contacted.

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

6. Resources needed

The resources that are needed to implement this are:

6 servers and a firewall will be maintained. These servers and the associated networking will be provisioned for high availability and future growth. A safe in Internet2 Ann Arbor office and two safe deposit boxes at local banks will also be used.

7. References

<http://www.incommonfederation.org>

8. Acknowledgements

IJ Kim, Mike LaHaye, and Dan Pritts were instrumental in producing the processes and this document.