

## InCommon CA Audit Log

Version: 0.42

Date: 08-18-2004

By: Nick Lewis

There will be 4 CA audit logs. Three will be paper and one electronic.

The first paper audit log will be used to record the chain of custody and actions taken with the equipment necessary to operate the Internet2 InCommon CA (CA hardware). This log will be stored in the safe that will be securely stored in the Internet2 Ann Arbor office. The log will be completed every time that the CA hardware is accessed. The log will include Username, Date, Signature of the Actor, and an entry indicating the action(s) that were taken with the CA hardware.

Logged actions will be:

- Open safe
- Remove hardware from Safe
- CSR, Metadata, and CRL steps were taken
- CA state was backed up
- Return Hardware to safe

The second paper log will be stored in the primary Operational data safe deposit box where CA operational data will be stored. It will log access to the Operational data.

Logged Actions will be:

- Open safe deposit box
- Recovery of necessary hardware
- Access of stored data

The third paper log will be stored in the private key password safe deposit box. It will log access to the private key password or physical keys.

Logged Actions will be:

- Open safe deposit box
- Access of private key password
- Access physical keys

The electronic log will be used to record the actions taken in the secure database. This log will be stored with the Storefront Log. This log will be completed every time the batch process is used accessing the secure database. The log will include Username, Date, and an entry indicating the action(s) that were taken with the secure database.

Logged actions will be:

- Rudimentarily validate syntax of CSR, Metadata, and CRL
- Imported signed CSR into database

Publish CRL  
Compile metadata on test WAYF and test  
Push metadata to WAYF