

CA Disaster Recovery Procedure for Hardware Failure

Version: 0.16

Last Update: 08-16-2004

By: Nick Lewis

This policy will be used for hardware failure only. This will not be used for a compromise of the CA or CA infrastructure. See CA Disaster Recovery Procedure for recovery from root key compromise for procedure related to compromise of the CA or CA infrastructure.

There are four sections to this document:

1. Hardware failure of CA, not including hard drive
2. Failure of the hard drive in CA
3. Procedure to repair hardware securely
4. Destruction of safe and materials in safe including CA, hard drive, and local private key backup

1. Hardware failure of CA, not including hard drive

If the hardware of the CA fails, such as the keyboard, video, or anything other than the hard drive, these steps should be taken (these steps assume the steps to access the CA have been followed):

1. Log failure of the CA hardware
2. Take backup CA hardware out of safe
3. Move hard drive from failed hardware into backup hardware
4. Turn CA on to verify correct functionality of hardware
5. Recommendation for consideration: Check tripwire database of hard drive to ensure no data was damaged
6. If the data was damaged, follow the option for Failure of hard drive

2. Failure of the hard drive in CA

If the hard drive of the CA fails, these steps should be taken (these steps assume the steps to access the CA have been followed):

1. Log failure of the CA hard drive
2. Take backup CA hard drive out of safe
3. Take failed hard drive out of CA and replace with backup hard drive
4. Install or restore operating system and CA software from trusted media
5. Restore operational data from CDRW backup

6. Recommendation for consideration: Check MD5 checksum of operational data
7. Recommendation for consideration: If MD5 checksum of operational data fails to match
 - a. Restore from backup
 - b. Re-verify MD5 checksum.
 - c. If it continues to fail, try older backups until MD5 verifies.
 - d. If MD5 never verifies, replace replacement hard drive and replace CDROM drive.
 - e. If necessary, retrieve secure backup from safe deposit box and try these steps again. Restore and re-generate operational data from secure database.
 - f. If MD5 checksum never matches, follow the procedure to re-key the root key.
8. Recommendation for consideration: Generate new tripwire database of hard drive and record it to the log
9. The failed hard drive should be destroyed securely

3. Procedure to repair hardware securely

If the hardware of the CA fails, such as the keyboard, video, or anything other than the hard drive, follow these steps to have the hardware repaired:

1. Keep failed hardware in secure storage until an authorized repair person has arrived to repair the hardware
2. Once repair person has arrived, follow previous steps to retrieve hardware from secure storage.
3. Remove the hard drive from the CA
4. Monitor the repair of the hardware
5. Replace the hard drive in the CA
6. Log actions.
7. Re-store hardware in safe
8. Log actions

4. Destruction of safe and materials in safe including CA, hard drive, and local private key backup

These specific steps are dependant on the service level agreements for procedures related to Federation and CA. The assumption is 1 day to recover from complete destruction of safe. If the building that the safe is stored in is destroyed, then service will restored as soon as necessary and safe.

1. InCommon contacts will be notified of this event.
2. Replace infrastructure as necessary
3. Procure replacement CA hardware

4. Take trusted CA hardware to safe deposit box at the bank to be able to make copies of the trusted CD media
5. Make 2 copies of trusted CD media
6. Recommendation for consideration: Verify the MD5 checksum of the media to ensure exact copies. This will include the private key and installation media for software and OS.
7. Log that steps have been taken
8. Now, follow the steps outlined in Section 2 for recovering from a failed hard drive.