

CA Disaster Recovery Procedure for recovery from root key compromise

Version: 0.31

Last Update: 08-18-2004

By: Nick Lewis

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

There are five sections in this document:

1. Definition of root key compromise
2. What to do if there is a compromise of the root key – non-technical steps
3. Technical steps root key compromise
4. Metadata signing key compromise
5. Compromise of the secure database

1. Definition of root key compromise

The root key will be considered compromised if the key leaves the control of the operators of the InCommon CA.

2. What to do if there is a compromise of the root key – non-technical steps

Communications will need to be sent from the Storefront to the participants indicating that a compromise occurred and that they will be contacted with new certificates.

3. Technical steps root key compromise

If the CA key is compromised, we assume we would need to take the collected CSRs, generate a new root key, generate new certificates and distribute them to participants. The CSRs will be restored from the secure database.

4. Metadata signing key compromise

If the Metadata private key is compromised, the certificate will be revoked, a new certificate will be generated, and the Metadata will be signed with the new certificate.

5. Compromise of the secure database

If the secure database is compromised, a forensics analysis will be done, but the first priority will be restoration of federation related services.