

Technical Operations Steps

Version: 0.43

Last Update: 08-18-2004

By: Nick Lewis

1. Provisioning of password to Admin Contacts
 - a. Username will be e-mail address
 - b. Password will be chosen by the Admin contact
 - c. The MADA will set the password that the Admin Contact requests initially.
 - d. A web based password change interface will be created for contacts to change their password for the InCommon web interface.
 - e. Passwords or pass phrases will need to conform to these standards and will be enforced by the MADA initially. The guidelines will be:
 - i. 12 characters long
 - ii. Combination of letters, numbers, or punctuation.
 - iii. Not be their username
2. Admin Contact submits CSR, revokes Cert, or updates Metadata
 - a. This data will be submitted via a web form under SSL where the contact is authenticated with the credentials that they are provided in the Application process.
 - b. A second CSR request will be added in the future to help protect end entities from potential lengthy downtime from compromised private keys. The additional certificate will need to be protected at the same level as the original certificates, but will need to be stored in a different secure location.
3. E-mail response to Admin Contact, MA and TSG
 - a. This e-mail will confirm with the Admin that a request was made and will inform MA and TSG that there is a need to follow the batch process
4. Batch process now starts
 - a. This batch process will be done once a day at the end of the day.
5. TSG Validates CSR or CRL and submits questions to MA to contact Admin
 - a. This is to check that DNS names match and the URL's conform to standards. If there are questions about data that was submitted, MA will contact the Admin to get the answer to the question(s). Once adequate response has been received, the request can be processed. If the adequate response is not obtained, the request will be held without action until adequate response has been obtained. An individual request error will not delay the rest of the process.
 - b. If the data submitted was structured incorrectly, we may change as necessary to conform to established formats. If the data would be changed, then notify the user and ask if the changes can be made on their behalf.
 - c. This step will be automated as much as possible with checking on the submission of the data.
6. TSG Logs that the CSR or CRL was rudimentarily technically validated

- a. This will be logged in the electronic log
 - b. When the validation step is automated, this step will unnecessary.
7. MA opens key box, gets safe key
8. TSG opens machine room
9. Format Thumb drive in secure DB
 - a. This is done to ensure that there is no unknown data on this device.
10. Export CSR, Metadata, or CRL onto thumb drive
 - a. The data is exported from the secure database in the format that it needs to be signed in. It will be easier to put into the format needed when exporting initially rather than manipulating the raw data on the thumb drive.
11. TSG enters safe PIN
12. MA opens safe with key
13. Remove CA hardware from safe
14. Prepare hardware and login into CA
 - a. This includes connecting the power, thumb drive and any other accessories
15. Recommendation for consideration: Check tripwire database of hard drive and verify that it matches tripwire database of hard drive
 - a. This is done to verify that the hard drive has not been tampered with and that the hard drive has not had any data corruption.
 - b. This step would only need to be done when the operation data is sent to be archived at the safe deposit box for operational data.
16. Sign CSR's on CA machine on thumb drive
 - a. All of the CSR's will be signed while still on the thumb drive. They will be signed using openssl and the private key of the root.
17. Sign Metadata on CA machine on thumb drive
 - a. All of the Metadata will be signed while still on the thumb drive. They will be signed using openssl and the Metadata signing key of the root.
18. Sign CRL's on CA machine on thumb drive
 - a. All of the CRL's will be signed while still on the thumb drive. They will be signed using Scott's java metadata signing utility and the private key used for metadata signing.
19. Backup CA state onto CDRW
 - a. This is done to aid in the quick recovery from physical failure of the CA hardware
 - b. Backups will be sent monthly to the Operational data safe deposit box and this action logged.
20. Recommendation for consideration: Regenerate tripwire database of hard drive and CA operational data and write to tripwire log
 - a. This tripwire database is generated incase the Operational data needed to be restored and that what was restored was what was backed up.
21. Shutdown CA
22. Remove thumb drive from CA
23. Store CA hardware back in safe
24. Log actions

- a. MA and TSG will log that they followed this procedure and other logging details to be defined. This log will then be store in the safe.
 - b. Log that the CSR, Metadata, and CRL steps were taken.
 - c. Log that the CA state was backed up
25. Lock safe
26. Put thumb drive in secure db
27. Import signed CSR into DB
- a. Signed CSR's will be imported into the secure DB and notification e-mailed to the Admin Contact with the certificate attached.
28. Push metadata to test wayf
- a. Metadata will be pushed to the test wayf
 - b. Compile wayf software on test server and test functionality
 - c. Metadata will be compiled on the test wayf and tested for syntactical validity
 - d. Metadata will be downloaded to a test target and tested with the test target to ensure that it can consume the updated metadata.
 - e. The test WAYF will also be tested to ensure that a target is reachable.
 - f. Metadata will be pushed to the production WAYF and the WAYF service will be restarted to make the new Metadata available
29. Push CRL to CRL locations
- a. CRL data will be pushed to the CRL publishing location to be published
 - i. <http://incommoncrl1.incommonfederation.org/crl/eecls.crl>
 - ii. <http://incommoncrl2.incommonfederation.org/crl/eecls.crl>
 - b. Test that test target can utilize updated CRL