

InCommon CA Revoke Process

Version: 0.11

Last Updated: 08-30-2004

By: Nick Lewis

This is the current process for revoking an InCommon CA issued certificate. We have stated that we will revoke a certificate and issue a Certificate Revocation List within 1 business day. Admin Contact or Executive Liaison for a participant can revoke a certificate currently.

1. Admin contact contacts the Storefront notifying them that they need to have a certificate revoked.
 - a. This contact can be via e-mail or a telephone call.
2. MADA calls Admin contact at their phone number that we have stored for them already to confirm that the certificate needs to be revoked and what the serial number is of the certificate that needs to be revoked.
 - a. To find the serial number, the certificate needs to be decoded with either OpenSSL, using a browser, or another tool.
 - b. The MADA should also recommend that the Admin contact submit a CSR for the server in question.
3. MADA notifies TSG that a certificate needs to be revoked.
4. MADA and TSG access the CA using the steps to access the CA.
5. Run the daily batch steps as needed, but do not generate the CRL yet.
6. Issue the command: `csp InCommon revoke <serial number>`. This will revoke the certificate.
7. Now issue this command: `csp InCommon gencl`. This will generate the CRL.
8. Now follow the steps to publish the CRL as a part of the daily batch steps.

This is a planned process for revoking an InCommon CA issued certificate in the future. Technical contacts for a Credential Provider or Resource Provider may be able to revoke a certificate. This will be a self-service model similar as what was discussed on the 08-25-2004 HEPKI-TAG called and discussed internally. The InCommonCA web interface could also have an option for revoking a certificate based on the serial number.

1. InCommon issues a certificate revocation certificate signed a special online certificate revocation certificate. This certificate will be signed by the InCommon CA.
2. The Admin contact or Technical contact also has a username and password to the InCommonCA web interface where they manage their participation in InCommon.
3. Either form of authentication could be used.
4. The web interface could have an option for revoking a certificate based on the serial number.
5. By submitting the serial number to be revoked, it will be written to a database for certificates to be revoked.

6. This will trigger (or be a part of the application) the command to revoke the certificate.
7. An additional option will be to display the certificates that a specific contact is responsible for and let them select the certificate to be revoked.