Replacing back-channel certificate and key on an IdP

If the back-channel certificates on an existing IdP need to be replaced (e.g., due to the private key being possibly compromised or for any other reason), this sequence of steps does this key replacement without any impact on the IdP users (i.e., login works through all the steps).

These instructions are strongly based on the Shibboleth Project IdP Key Rollover instructions - but elaborate some of the generic steps into easy-to-follow guidelines.

The steps are:

1. Generate the new keypair on IdP. This can be done by re-running the IdP installer with the `renew-cert` argument. The command generates new certificate and private key into separate files (with the `.new` suffix); these can be deployed on the IdP as needed. So run the following (assuming the same directory naming convention as in the IdP Installing manual):

   ```
   cd /root/inst/shibboleth-identityprovider-${IDP_VERSION}
   ./install.sh renew-cert
   ```

   - Answer `"yes"` to proceed
   - Press Enter to use the same directory as where the shibboleth IdP is installed
   - Press Enter to use the same FQDN (hostname)
   - Enter the same pass-phrase (literally: `"changeit"`)

   - This generates the following files in $IDP_HOME/credentials:
     - `idp.crt.new`
     - `idp.key.new`
     - `idp.jks.new`
   - Fix the permissions on the files:

     ```
     cd $IDP_HOME/credentials
     chmod idp.key.new idp.jks.new 600
     chown -R tomcat.tomcat .
     ```

2. Add the new key in the Federation Registry for the IdP:
   - Log into the Federation Registry (at https://registry.tuakiri.ac.nz/federationregistry/)
   - Navigate to the details page for your IdP
   - On the Certificates tab (under SAML in FR2 used in Tuakiri-TEST), add the new certificate.
     - Use the default settings of only adding the "signing" use for the certificate.

3. Wait for the updated metadata to propagate through the federation. To be sure all SPs have loaded the new metadata, wait for 4 hours.

4. Switch the IdP to use the new certificate:

   ```
   cd $IDP_HOME/credentials
   for FILE in idp.{crt,key,jks} ; do mv $FILE $FILE.old ; mv $FILE.new $FILE ; done

   # restart Apache and Tomcat
   service httpd restart
   service tomcat7 restart
   # (use the appropriate service name depending on Tomcat version)
   ```

5. Remove the old certificate from the Federation Registry
   - Again, log into the Federation Registry
   - Navigate to the details page for your IdP
   - On the Certificates tab (under SAML in FR2 used in Tuakiri-TEST), remove the old certificate (make sure this is the old one and not the new one).

6. This completes the certificate replacement process. After another metadata refresh (4 hours maximum), no SP would be trusting the old IdP certificate.