THE LOCKSS PROGRAM

# LCAP Over SSL

LOCKSS boxes audit and repair each other via a robust and secure, peer-to-peer polling and reputation system. In order to allow new boxes to join a LOCKSS network without coordination by a central authority, the communications are normally not encrypted, and each box's identity is determined by its IP address.

Private LOCKSS Networks may increase security by adding end-to-end encryption and client authentication via SSL. This ensures that communication will take place only with authorized boxes, and that traffic cannot be intercepted (snooped), even if the network infrastructure is compromised. In order to use SSL, a private key must be generated for each box, and the corresponding public certificates must be distributed to all boxes. It is no longer necessary to create a `runssl` script: SSL will automatically be used if keystore and password files are present in `/etc/lockss/keys`.

See [http://www.lockss.org/lockss/LOCKSS_Network_Administration] for details of the daemon configuration parameters that will be set by the ssl scripts.

## Creating Keystores

To use SSL for a PLN the authority in charge of the PLN must create and distribute Java keystores to each box. Each box receives two keystores: one containing its own private key and another containing public certificates for each of the boxes in the network, plus a password file containing the secret password for the private key. To create keystores and password files for a PLN whose boxes are named *box1.pln.org* through *boxN.pln.org*, use the following instructions:

1. Build a LOCKSS development environment
    1. Setup necessary environment variables
        1. `export CVSROOT=:pserver:anonymous@lockss.cvs.sourceforge.net:/cvsroot/lockss`
        2. `export JAVA_HOME=/usr/local/jdk-1.6.0`
           (This will vary, depending on your system)
        3. `cvs get lockss-daemon`
        4. `cd lockss-daemon`

2. Generate the keystores and password files. Run the following command, substituting the names (FQDN) of all machines in the PLN for *box1.pln.org* through *boxN.pln.org*, and the name of an empty directory for *keydir*. Note that the name of each machine must match the name provided to its LOCKSS daemon configuration.

   `ant run-tool -Dclass=org.lockss.keystore.EditKeyStores -Dargs="-s pub-keystore.jceks -o keydir box1.pln.org ... boxN.pln.org"`

   This will create a public keystore named `pub-keystore.jceks` and, in *keydir*, a pair of files for each box: *boxN.pln.org*`.jceks` and *boxN.pln.org*`.pass`.

3. Securely transmit to each box its two files and the public keystore and store them in `/etc/lockss/keys`. Ensure that the directory and the two private files are owned by and readable only by root, and that the public keystore is readable by others. (Use /opt/lockss/etc/lockss/keys for Solaris machines.) For example, on each box:

(*It is very important to follow the steps below exactly for permissions and ownership)*

1. `mkdir -p /etc/lockss/keys`
2. `scp server:`*`boxN.pln.org`*`.{jceks,pass} pub-keystore /etc/lockss/keys`
3. `chown -R root:root /etc/lockss/keys`
4. `chmod -R 700 /etc/lockss/keys`
5. `chmod 755 /etc/lockss/keys`
6. `chmod -R 644 /etc/lockss/keys/pub-keystore.jceks`

4. Restart the daemon, check that it's now using SSL: the Daemon Status/Comm Channels page should show "SSL: TLSv1, Client Auth". After a few hours check Daemon Status/Comm Peer Data to ensure that each box is successfully originating and accepting connections from all the other boxes.

## Adding Boxes To An Existing PLN

To add one or more boxes to the PLN, rerun the the ant command in step 2 above to create private key(s) for the new box(es) and add the new public key(s) to the public keystore:
`ant run-tool -Dclass=org.lockss.keystore.EditKeyStores -Dargs="-s pub-keystore.jceks -o` *`keydir newbox1.pln.org ... newboxN.pln.org`*`"`
Note that you must have the existing pub-keystore.jceks in place so that the command will add certificates to it, not create a new one.

Distribute the files as above to the new boxes. Distribute only the new public keystore to the existing boxes.