

NOTE: This document is intended only for InCommon users who already have an InCommon user certificate and have been authorized as Department Registration Authority Officer (DRAO). This document has been created as a manual for issuing host and service certificates through the command line tool: `osg-incommon-cert-request` (available in the `osg-pki-tools` software package at <https://github.com/opensciencegrid/osg-pki-tools>).

Requesting and retrieving InCommon IGTF Server CA certificates

A new command line tool: `osg-incommon-cert-request` is available through the `osg-pki-tools` v3.2.1 (<https://github.com/opensciencegrid/osg-pki-tools>). This command line tool makes use of InCommon APIs for programmatic access to request certificates in bulk.

Requirements

1. Before requesting certificates from InCommon Certificate Service, you must be authorized as an InCommon user with the Department Registration Authority Officer (DRAO) role. All InCommon users are provided with authentication credentials: username and password for InCommon Certificate Manager service at <https://cert-manager.com/customer/InCommon>.
2. `osg-incommon-cert-request` requires the use of an InCommon user certificate. This certificate must be configured for the DRAO user as method of authentication. Regularly, your InCommon institutional point of contact will be able to issue an InCommon user certificate for this purpose and configure it as your method of authentication.

Requesting certificates through `osg-incommon-cert-request`

Single certificate requests can be made directly through InCommon CM interface or through the command line tool: `osg-incommon-cert-request`. More details can be found at [Using InCommon Certificate Manager \(CM\)](#).

1. Install OSG repositories as instructed here: <https://opensciencegrid.org/docs/common/yum/>
2. Install `osg-pki-tools` v3.2.1 from OSG repositories.

```
$ yum install osg-pki-tools
```

IMPORTANT: As of April 11th, 2019, `osg-pki-tools` v3.2.2 is available at the OSG repositories. This package was released under OSG Software version 3.4.27 on April 11th, 2019.

3. Run `osg-incommon-cert-request -h` for usage:

```
$ osg-incommon-cert-request --help

usage: osg-incommon-cert-request [--debug] -u username -k pkey -c cert \
      (-H hostname | -F hostfile) [-a altnames] [-d write_directory]
      osg-incommon-cert-request [--debug] -u username -k pkey -c cert -t
      osg-incommon-cert-request -h
      osg-incommon-cert-request --version
```

4. A couple of examples on how to request a certificate using `osg-incommon-cert-request`:

Requesting a certificate for a hostname without Subject Alternative Names

```
$ osg-incommon-cert-request --username <INCOMMONLOGIN> \
      --cert <USERCERT> --pkey <USERPRIVKEY> \
      --hostname <HOSTNAME>
```

Requesting a certificate for a hostname with multiple Subject Alternative names

```
$ osg-incommon-cert-request --username <INCOMMONLOGIN> \
      --cert <USERCERT> --pkey <USERPRIVKEY> \
      --hostname <HOSTNAME> \
      --altname <ALTNAME1> \
      --altname <ALTNAME2>
```

Requesting a certificate for a list of hostnames through a hostfile

```
$ osg-incommon-cert-request --username <INCOMMONLOGIN> \
      --cert <USERCERT> --pkey <USERPRIVKEY> \
      --hostfile <HOSTFILE_PATH> \
```

Testing authentication credentials

```
$ osg-incommon-cert-request --username <INCOMMONLOGIN> \
      --cert <USERCERT> --pkey <USERPRIVKEY> \
      --test
```