

How to obtain a certificate from the AusCERT CA under the Australian Access testbed Federation for a Service Provider (SP) or an Attribute Authority (AA) under the MAMS Testbed Federation.



This certificate is only to be used to sign the internal federation SAML requests and assertions.

The Attribute Authority (AA) is commonly associated with the Identity Provider (IdP), and is typically installed on the same host. The Identity Provider service is a combination of the Shibboleth Handle Service, which provides the authentication of a user's credentials and supplies a Shibboleth Handle to the Service Provider, and the Attribute Authority, which provides a signed attribute assertion to the Service Provider about a Shibboleth Handle.

The information required to issue a certificate in the AAF Shibboleth Federation Level 3 Hierarchy is as follows.

Whether this is for a Service Provider (SP) or an Attribute Authority (AA) you are required to provide the following information along with your request.

E-Mail Name	(for the certificate management - alias or person)
IP address	FQDN of the Host for this certificate (ie. shib-sp.test.uq.edu.au)
DNS name	of host (all IP address if multi-homed)
	(all DNS names of this host)
User Data Name	(Person requesting Certificate)
Email	(First and Last name)
Department	(Official Institution work email)
Telephone	(Full Institution and Department)
	(+61...)

Generate a Certificate Signing Request (CSR) for the AAF Shibboleth CA and send the CSR and your user information to **pilot-level3-shibca@auscert.org.au**.

To generate the CSR you must use the openssl configuration file. You will be required to edit the file to enter the correct information about your Service Provider (SP) or Attribute Authority (AA).

Once you have edited and saved the openssl configuration file, you will be required to execute the following command to generate a new private key and CSR for your Shibboleth Host.

```
openssl req -new -config openssl_shiblv13ca_certs.cnf \  
-out shib-sp_test_uq_edu_au.csr
```

Once completed, send your details and attach the CSR in an email to

pilot-level3-shibca@auscert.org.au.

Detailed instructions on this process can be found in the openssl configuration file below.