Check MIT Certificates on a private web server

Check MIT Certificates on a private web server

- I have a web server. How can I authenticate clients based on certificates?
- I want to know when someone has an MIT web certificate.

Advisory
While certificate-based authentication is still used on some older servers at MIT, Touchstone-based authentication is more widely supported on more modern servers. If you're not sure which is right for you, please contact the IS&T Service Desk.

On this page:

Answer

This is an advanced topic that is outside of what the IS&T Help Desk can support. The basic idea of the answer is that you need two things:

- Your webserver needs to have a server certificate, which will allow it to serve HTTPS encrypted web pages. You have multiple options for how to get a server certificate:
  - You may create a self-signed certificate; clients visiting your site will see a prominent warning when they first use SSL, so this is not suitable for production use, but is helpful for testing configurations.
  - You may request a certificate via MIT's InCommon site license. This will give you a certificate that will be trusted by most default configurations.
  - You may request a certificate via MIT's own CA authority; since 2012, this is depreciated, but available for some very limited cases.
- Your webserver needs a copy of the "Client CA v1" public key, which it can use to verify whether visitors have proper MIT certificates.

Server certificate

Your server certificate does not need to be MIT-signed, but using an MIT-signed one is a good idea for MIT sites.

If your server is in the mit.edu domain, you can get an official MIT-signed server certificate by generating a Certificate Signing Request (CSR), and emailing the CSR to mitcert@mit.edu.

Verify whether visitors have MIT certificates

To verify MIT certificates, your server needs to check to see whether the visitors certificate was created by the "Client CA v1". You will need the public key of this CA:

Client CA v1 https://web.mit.edu/apache-ssl/certificates/mitCAclient.pem

For the apache web server, you will need use this file in conjunction with the **SSLVerifyClient require**, **SSLVerifyDepth**, and **SSLCACertificateFile** apache options.

Touchstone

Installing and Configuring Shibboleth 2.x on Mac OS X 10.6.x Server

Further resources

- Wiki on obtaining a server certificate: https://wikis.mit.edu/confluence/x/ZZl4Aw

- Creating SSL Certs for ISDA servers