

Instructions for Requesting a SSL:

Step 1: Collect information needed to generate/renew an SSL Certificate

For all new SSL Cert requests you will need to provide the following general information.

1. Where the server is physically located (if the server is not OIT managed)?
2. What kind of application is it?
3. What kind of data will be stored?
4. Who will have access to it and how will the users gain access (if the server is not OIT managed)?

For all new SSL Certs and SSL Cert Renewals requiring Certificate Signing Requests (CSRs), please provide the following information:

1. Application Name utilizing the cert
2. IP Address
3. CSR including the following:

C = US

S = Texas

L = Arlington

O = The University of Texas System

OU = The University of Texas at Arlington

1024 bit key length

IP address

Full domain name of system

NOTE! The Certificate Signing Request (CSR) cannot contain the *, ?, :, or spaces in the Common Name field. The Common Name must be a fully qualified domain name without '*', '?', ':', space, http://, or :port number. For example, owa.uta.edu or www.uta.edu are fully qualified domain names. The Certificate Signing Request (CSR) submitted must be greater than 512 bits. There are known vulnerabilities of keys up to this length. Please submit the CSR with a longer key (1024 bits recommended).

Step 2: Complete Form (Online) www.uta.edu/security/ssl.htm

Type of ssl – New, Renewal, Change (radio button)

OIT Managed server, Departmental Managed server (radio button) – if Departmental Managed, text pop up to provide additional information about charge/rpt etc.

- Server Name –
- Server IP Address –
- Name -
- Department –
- Title -
- Server OS (drop down)
- Use old CSR, Use new CSR (radio button) – if new, download CSR