i.t.solutions
uahuntsville

OBTAINING SSL CERTIFICATES

AUDIENCE

This document is for web server administrators. If you have any questions about the following process or need a SSL certificate for a server other than a web server, please contact i.t.solutions.

SECURE SOCKETS LAYER (SSL) FOR WEB SERVERS

SSL is the industry-standard for protecting communications with web servers. SSL should be used in all applications where users are required to authenticate to access a service, when privileged data is displayed or required for authentication, or when verification of the authenticity of the server is required. SSL is supported in all major web servers and web browsers. SSL also works with IMAP, LDAP, code verification and other applications.

Whenever confidential information is transmitted over the network, including passwords, SSNs, financial information, or any data protected by legislation such as FERPA, HIPAA, or any information deemed sensitive by university policy, it should be encrypted using Secure Sockets Layer with at least 128 bit encryption. In test or development environments it is sometimes sufficient to use what is called a "self-signed" certificate. However, this type of certificate should not be used whenever off-campus access of the server is available.

Implementing SSL on a system requires that a digital certificate be obtained for each server on which an SSL-protected application resides. SSL certificates are used in encrypting communications, verifying the identity of the site and conveying a level of trust to those who visit the site. The authentication process involves confirming the identity of the server with an independent third party (certificate authority).

There are 3 basic types of web server certificates, based on the level of verification of the server identity.

- Domain validation certificates -- Verify the right of the applicant to use a specific domain name.
- Organization validation certificates -- Verify the right of the applicant to use a specific domain name in addition to verification of the organization.
- Extended Validation SSL Certificates -- Verify the right of the applicant to use a specific domain name AND conduct a ***thorough*** vetting of the organization by the Certification Authority.

OBTAINING A VERISIGN CERTIFICATE

UAHuntsville participates in a managed certificate program with Verisign, Inc. Should you choose to purchase a Verisign certificate, i.t.solutions will provide installation support as well as expiration notification. To purchase a Verisign certificate, first determine the date when the certificate needs to be implemented, the Operating System, the application which requires SSL, the name and contact information for the responsible person for the server, and the DNS name of the server.

Proceed as follows:

1. Contact TAG (824-3333) to generate an incident concerning the purchase of a certificate. You will need to communicate the following information.
   - Operating system
   - Software running web server (e.g. IIS or Apache, etc) and VERSION
   - Administrator's name
   - Administrator's email
   - Administrator's phone number
   - Server name in DNS
   - Number of years for which the certificate is to be issued
2. TAG will forward the request to Jerry Brown (824-2627) in i.t.solutions.
3. Arrange for a budget transfer.
4. Generate a Certificate Signing Request (CSR) according to instructions. These will be emailed to you by Jerry.
5. Send the CSR to jerry.brown@uah.edu.
6. When generated, the certificate will be sent to the administrator registered with the certificate information.
7. Install the certificate according to instructions. These will be emailed to you by Jerry.

OTHER SSL CERTIFICATES

If you need a certificate for a critical UAHuntsville service and choose not to purchase a VeriSign certificate through i.t.solutions, purchase a certificate from a valid and trusted source and a certificate type and certificate authority which performs at least checking of domain and organization. Not all CA's are automatically recognized in common web browsers, so be sure to choose a CA which is commonly recognized. Encryption should be no less that 128 bit. Instant or automatically-generated certificates do no verification of the purchaser, so it is possible that your site may not be viewed as trustworthy if you use this type of certificate. Choose a certificate authority which does not use MD5 encryption algorithms.