

Miami University

Wildcard SSL Certificates

IT Policy | **IT Standard** | IT Guideline | IT Procedure | IT Informative
Issued by: IT Services

SCOPE:

This standard covers all requests for and uses of wildcard Secure Socket Layer (SSL) certificates used for domains used to support the mission of Miami University, including but not limited to the muohio.edu domain.

RATIONALE:

Because wildcard certificates can be used for any server within a domain, they must be treated in a more secure fashion than regular SSL certificates which are tied to a specific computer name.

IT STANDARD:

A. Valid domains

Wildcard SSL certificates for the muohio.edu domain can only be used on third level domains and below. Wildcard certificates for other Miami domains outside of muohio.edu can be used on second level domains and below.

B. Expiration

Wildcard SSL certificates will be issued with an expiration date 13 months from the date of issue.

C. Requestors

Wildcard SSL certificates can only be requested by faculty and full time employees who have responsibilities which include managing servers on behalf of a division, department, school or other entity within Miami University. Wildcard SSL certificates can only be installed on servers on which the requestor has administrative privileges. The private key associated with the wildcard SSL certificate must have the appropriate access controls to prevent non-administrative accounts on the server from accessing it.

D. Multiple wildcard SSL certificates for the same domain

There are cases in which multiple wildcard SSL certificates are requested for the same domain. There is no technical reason that this cannot be accommodated, but care must be taken to ensure that all individuals in the domain in question are aware of who else holds a wildcard certificate for that domain.

E. Approval process

All wildcard SSL certificate requests require manual approval from the Security Engineering group before the request is granted.

F. Revocation

Anyone who suspects that a server which is using a wildcard SSL certificate has been compromised must report that to the Information Security Officer.

G. Exceptions

Any exceptions to this standard require approval from the Information Security Officer before they are implemented.

H. Review

This standard will be reviewed by the Security Working Group on an annual basis.

DEFINITIONS

Second level domain – A portion of Miami's network address which is listed as *.muohio.edu. The second level domain in which a third level domain exists can be determined by examining the last two portions of the third level domain.

Third level domains – A portion of Miami's network address space which is listed as *.x.muohio.edu, where "x" is the name of the third level domain - for example *.eas.muohio.edu.

APPROVAL(S) AND DATE(S):

Reviewed by: Security Working Group, May 28, 2009
Final Approval by: Information Security Officer
Final Approval on: June 24, 2009
Version number: 1.0

REVISION HISTORY & REFERENCES:

- A. Revision History
June 24, 2009 – First Draft