NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

Office of Information Technology Services Standard	**No:** ITS-S16-003
ITS Standard: **TLS / SSL Certificate Standard**	**Issued:** 09/02/2020
	Issued By: NYS Office of Information Technology Services **Standard Owner:** Chief Technology Office

1.0 Purpose and Benefits

The purpose of this technical standard is to normalize the deployment of Transport Layer Security (TLS) Certificates used to encrypt and authenticate state applications.

2.0 Authority

Section 1 of Executive Order No. 117 charges the State Chief Information Officer with overseeing and supervising the management and operations of the Office of Information Technology Services (ITS). *Section 102(2) of the State Technology Law* gives the Director of ITS responsibility for the administration of ITS. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This standard applies to ITS, its employees and contractors, and ITS supported applications.

4.0 Information Statement

4.1 TLS Certificate Acquisition

All TLS Certificates must be acquired by the designated business unit within ITS.

4.2 TLS Key Management

TLS private keys will be generated in a manner consistent with NYS-S14-007 Encryption Standard. It is recommended that key material be stored in a hardened Hardware Security Module (HSM).

4.3 TLS Session Termination

TLS sessions must be terminated on the application delivery controller at the data center perimeter.

Exceptions will be permitted for any of the following reasons:

- The application is considered an auxiliary perimeter for the data center network
- A demonstrated technical limitation exists that requires TLS to be terminated at the application

4.4 URL Naming Standards for Publicly Verifiable DNS Domains

Application URL naming is governed by NYS-P08-003 Domain Names for State Government Agencies. This policy requires that applications use the "ny.gov" domain structure and comply with approved URL naming patterns.

4.5 Compliant TLS Domains

Certificates shall be issued and maintained for the following compliant domain patterns:

- *.ny.gov
- *.svc.ny.gov
- *.agency_identifier.ny.gov

4.6 Legacy Supported TLS Domains

Support will not be provided to:

- *.state.ny.us
- *.gov

Legacy transitional support may be provided for non-compliant domain patterns, through exception granted by the State Chief Information Officer, to facilitate migration.

4.7 TLS Certificates for Private Namespaces

Applications using private DNS Namespaces (examples: *.nyenet, *.local, etc) will be supported by the ITS Enterprise Certificate Authority (CA).

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	Definition
Transport Layer Security (TLS)	A network protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Secure Sockets Layer (SSL)	An older version of the TLS proto.
Hardware Security Module	A physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.
DNS Namespace	This refers to all the domains and subdomains within the Internet Domain Name System (DNS)

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Technology Office
Reference: ITS-S16-003
New York State Office of Information Technology Services
Empire State Plaza
P.O. Box 2062 Albany, NY 12220
Telephone: 518-402-7000

ITS policies, standards, and guidelines may be found on the Inside Edge at:
https://nysemail.sharepoint.com/sites/myITS/InsideEdge/Pages/Policies.aspx

8.0 Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
02/20/2015	Issued internal document	Chief Technology Office
11/30/2018	Updated scope and authority cursory review	Chief Technology Office
09/02/2020	Scheduled review, updated authority and scope	Chief Technology Office

9.0 Related Documents

NYS-P08-003 Domain Names for State Government Agencies

NYS-S14-007 Encryption Standard