



SSL Certificate Standard

DOC-IT-IS-30
Revision 1.0
NOVEMBER 1, 2025

REVISION HISTORY

This revision history lists all changes to this document, the date of each revision, and the reason for each revision.

<u>Rev.</u>	<u>Rev. Date</u>	<u>Revision Description</u>
1.0	11/01/2025	Initial Version

1 Executive Summary	4
2 Purpose.....	4
3 Scope.....	4
4 SSL Certificate Standard	5
4.1 SSL/TLS Certificate Implementation	5
4.2 Certificate Types	5
4.3 Certificate Validity.....	5
4.4 Server Configuration	5
4.5 Monitoring and Alerts	6
5 Responsibilities	6
6 Compliance	6
7 Exceptions	7
8 Review and Updates.....	7

1 Executive Summary

SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers.

An SSL certificate (also known as a TLS or SSL/TLS certificate) is a digital document that binds the identity of a website to a cryptographic key pair consisting of a public key and a private key. The public key, included in the certificate, allows a web browser to initiate an encrypted communication session with a web server via the TLS and HTTPS protocols. The private key is kept secure on the server and is used to digitally sign web pages and other documents (such as images and JavaScript files).

An SSL certificate also includes identifying information about a website, including its domain name and, optionally, identifying information about the site's owner. If the web server's SSL certificate is signed by a publicly trusted certificate authority (CA), like SSL.com, digitally signed content from the server will be trusted by end users' web browsers and operating systems as authentic.

2 Purpose

The purpose of this document is to establish a standard for securing RXO servers through the mandatory use of SSL/TLS certificates, ensuring all data transmitted over networks is encrypted and server identities are authenticated.

3 Scope

This standard applies to RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, employees, contractors, and third parties acting on behalf of RXO must comply with this policy.

It applies to all servers created, maintained, or operated within the RXO network infrastructure, including internal, external, development, and production environments.

4 SSL Certificate Standard

All servers deployed within RXO, including internal, external, and cloud-based, must have valid SSL/TLS certificates to ensure encrypted communication and prevent unauthorized access or tampering of data.

4.1 SSL/TLS Certificate Implementation

- All servers must be configured with a valid SSL/TLS certificate issued by a trusted Certificate Authority (CA) for public facing servers or an approved internal CA for internally facing servers.
- Certificates must be installed and configured for all applicable communication protocols, including HTTPS, SMTP, and any other protocols that support SSL/TLS.

4.2 Certificate Types

- RXO supports the use of domain-validated (DV), organization-validated (OV), or extended-validated (EV) certificates, depending on the level of trust required.
- Wildcard certificates may be used only when necessary to cover multiple subdomains within a domain. Any use of wildcard certificates must be explicitly authorized by the RXO GRC security team.

4.3 Certificate Validity

- Certificates must have a validity period of no more than 12 months.
- Servers must have a valid certificate at all times, and renewal must be performed at least 30 days before the expiration date.
- Expired, revoked, or self-signed certificates are not permitted unless explicitly approved for specific non-production testing scenarios by the RXO GRC security team.

4.4 Server Configuration

- SSL/TLS must be configured to use strong encryption protocols (e.g., TLS 1.2 or higher).
- Weak ciphers and deprecated SSL/TLS protocols (e.g., SSL 3.0, TLS 1.0, and TLS 1.1) must be disabled.
- Use TLS Fallback SCSV to prevent protocol downgrade attacks.
- Use HTTP Strict Transport Security (HSTS) to prevent protocol downgrade attacks and cookie hijacking.

- Configure TLS 1.2 to use Elliptic Curve Diffie-Hellman (ECDHE) key exchange algorithm, with DHE as a fallback, and avoid RSA key exchange completely when possible.
- Use Perfect Forward Secrecy (PFS) to prevent compromised private keys from compromising past session keys.
- Certificates must be configured with a secure hash algorithm (e.g., SHA-256 or stronger) and key size (minimum 2048 bits).
- If the server supports it, disable TLS Compression to mitigate the Compression Ratio Info-leak Made Easy (CRIME) attack.
- Enable Secure Renegotiation.
- Disable Client-initiated Renegotiation to prevent Denial-of-Service (DoS) attacks.

4.5 Monitoring and Alerts

- Servers must be continuously monitored for the expiration or invalidation of SSL/TLS certificates.
- Automated alerts must be configured to notify administrators at least 60, 30, and 7 days before a certificate expires.

5 Responsibilities

IT and Security Teams

- Ensure the implementation and compliance with this certificate policy across all servers.
- Maintain a list of all active SSL/TLS certificates and their expiration dates.
- Conduct regular audits of server certificates and configurations.

System Administrators

- Install and maintain SSL/TLS certificates on all servers.
- Ensure certificate renewals are processed in a timely manner.
- Notify the IT security team of any issues or breaches involving SSL/TLS certificates.

Development Teams

- Ensure that SSL/TLS certificates are correctly implemented in development environments and during system deployments.
- Test all SSL/TLS configurations as part of the deployment pipeline.

6 Compliance

Non-compliance with this policy may result in access restrictions to affected systems or disciplinary actions as per RXO's guidelines.

7 Exceptions

Any exceptions to this policy must be approved in writing by the RXO Governance Risk and Compliance (GRC) team and must include a valid business justification.

8 Review and Updates

This standard will be reviewed annually, or upon major infrastructure or threat landscape changes, or as required due to changes in business or technical requirements.

Certificate of Review

SSL Certificate Standard

December 18th 2025 10:46:33 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 3:57 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:26 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:46 AM EST