Migrating from SSL and Early TLS

A Resource Guide from the PCI Security Standards Council

Is your organization still using Secure Sockets Layer (SSL)/early Transport Layer Security (TLS) protocols? Do you work with online and e-commerce partners or customers who have not migrated from SSL/early TLS to a secure form of encryption? Use this guide for information and resources that can help organizations prepare for the **30 June 2018** migration deadline and safeguard payment data in accordance with the PCI Data Security Standard (PCI DSS).

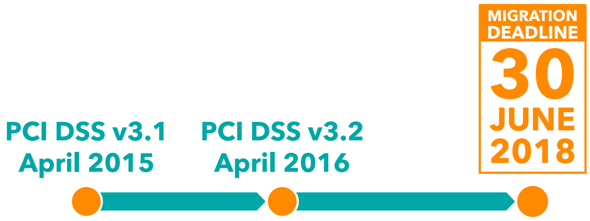
WHAT IS SSL/TLS?

SSL/TLS is a cryptographic protocol used to establish a secure communications channel between two systems. It is used to authenticate one or both systems, and protect the confidentiality and integrity of information that passes between systems.

SSL/EARLY TLS MIGRATION TIMELINE

SSL/early TLS are no longer considered secure forms of encryption for payment card data.

PCI DSS v3.1 published in April 2015 included a June 2016 deadline for disabling SSL/early TLS and implementing a secure encryption protocol. Based on industry feedback, in December 2015 PCI SSC revised the deadline from 30 June 2016 to 30 June 2018. This date is included in Appendix A2 of PCI DSS v3.2, published in April 2016.



PCI DSS v3.1
April 2015

PCI DSS v3.2
April 2016

MIGRATION DEADLINE
30 JUNE 2018

WHAT IS THE RISK?

Because of its widespread use online, SSL/early TLS has been targeted by security researchers and attackers. Many serious vulnerabilities in SSL/early TLS (e.g. POODLE, BEAST, CRIME, Heartbleed) have been uncovered over the past 20 years, making it an unsafe method for protecting sensitive data.

Online and e-commerce environments using SSL/ early TLS are most susceptible to these vulnerabilities and should be upgraded immediately. E-commerce merchants are also encouraged to implement a customer communication strategy to educate their customers about the dangers of using outdated browser software and the risk this poses to customer data.

SSL/EARLY TLS REMAINS IN WIDESPREAD USE TODAY
despite various security vulnerabilities exposed in the protocol

ONLINE AND E-COMMERCE
environments using SSL/early TLS are at highest risk

THERE ARE NO KNOWN FIXES
for protocol vulnerabilities in SSL/early TLS

www.pcisecuritystandards.org

IMMEDIATE ACTION ITEMS FOR ORGANIZATIONS

It is critically important that organizations upgrade to TLS v1.2 or higher as soon as possible, and disable any fallback to SSL/early TLS.

Many PCI DSS requirements require the use of 'strong cryptography' as defined in the PCI DSS glossary (See PCI DSS v3.2 Appendix A2 for current requirements on this subject). **After 30 June 2018 SSL/early TLS should not be used as a security control to meet any PCI DSS requirements attempting to demonstrate strong cryptography:**

New implementations must not use SSL/ early TLS as a security control.

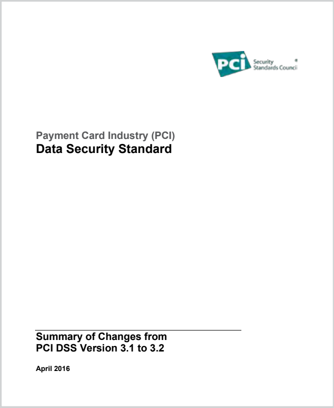
Prior to 30 June 2018, existing implementations that use SSL and/early TLS must have a formal Risk Mitigation and Migration Plan in place.

After 30 June 2018, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described below).

POS POI (point of sale point of interaction) terminals (and the SSL/early TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL/early TLS, may continue using these as a security control after 30 June 2018. Note that new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

ADDITIONAL RESOURCES

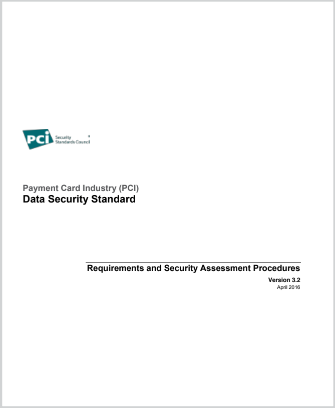
Webinar: Migrating from SSL and Early TLS


Payment Card Industry (PCI)
Data Security Standard

Summary of Changes from
PCI DSS Version 3.1 to 3.2

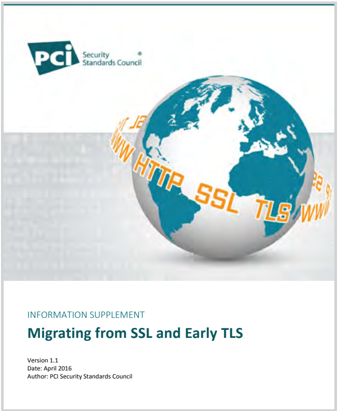
April 2016

Summary of Changes from PCI DSS Version 3.1 to 3.2


Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 3.2
April 2016

PCI Data Security Standard Version 3.2: Appendix A2



INFORMATION SUPPLEMENT

Migrating from SSL and Early TLS

Version 1.1
Date: April 2016
Author: PCI Security Standards Council

Information Supplement: Migrating from SSL and Early TLS