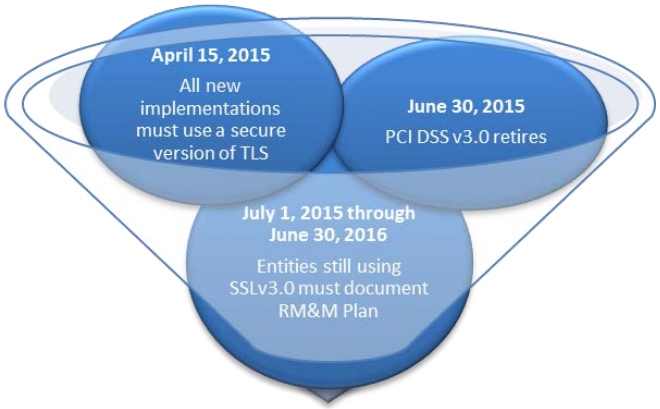
The End of SSL

ADVANCING COMMERCE™

National Institute of Standards & Technology (NIST): "TLS 1.1 configured with FIPS-based cipher suites as the minimum appropriate secure transport protocol."

BACKGROUND

Recently standards bodies such as the National Institute of Standards & Technology (NIST), the PCI Security Standards Council (PCI SSC) and others have disallowed SSL and early TLS to be used as a security control. As the predecessor to the Transport Layer Security (TLS) protocol, SSL was developed *over 20 years ago*, has numerous security vulnerabilities, and therefore no longer meets the needs of modern day security requirements.



RESPONSE

The best response is to disable SSL/Early TLS and migrate to a more modern encryption protocol, which at a minimum is TLS v1.1. Guidance on how to properly implement TLS can be found in NIST Special Publication 800-52.

Per the PCI DSS v3.1 (released April 2015) new system implementations must not use SSL or early TLS effective immediately, while existing implementations must either immediately migrate to a secure version of TLS or document a formal "Risk Mitigation and Migration Plan" with a firm roadmap to migrate by June 30, 2016. After June 30, 2016 SSL and early TLS can no longer be used as a security control.

These timelines and requirements do not apply to POS/POI terminals that can "be verified as not being susceptible to all known exploits", or the systems dedicated to supporting only those terminals.

For further detail on the new requirements related to the migration from SSL and/or early TLS as well as further the applicability to POS/POI terminals, please reference the PCI SSC's Information Supplement entitled: Migrating from SSL and Early TLS.