Datawire Secure Transport

Security Protocol update to TLS v1.2 and SHA 256

FREQUENTLY ASKED QUESTIONS

Version 1.0

October 2016

FREQUENTLY ASKED QUESTIONS
FOR DATAWIRE UPDATE TO TLS v1.2 AND SHA256

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY BLANK

Introduction to Datawire

What is Datawire Secure Transport?

Datawire Secure Transport is used for transporting payment transactions securely and reliably over the Internet

What type of payment solutions use Datawire?

- POS terminals or Software (VAR) that uses the Internet to transmit payments. Datawire requirement that there is at least one of the following Internet connections:
  - Wi-Fi
  - Cable
  - Ethernet
- Software (VAR) POS that uses the Internet to transmit payments.
- MicroNode (Petroleum):
  - 960
  - 1100
  - 1400

What forms of connectivity can be used for Datawire?

POS Systems can use one of the three Datawire Connectivity Solutions:

- API Interface - Terminals / POS Systems
- NAM - Windows Based Systems
- MicroNode - Dial to IP Conversion (petroleum)

What is needed to use Datawire?

- A terminal or software that transmits over the internet.
- An active internet connections via:
    - Wi-Fi
    - Ethernet
    - Cable
- A cryptographic key
    - As of April 1, 2015, First Data's current standard when encrypting traffic over a network, is an asymmetric key at a minimum of RSA 2048 bits.

SHA (Secure Hash Algorithm) 256, starting June 30 2016.

- Currently, Datawire' s cryptographic hashes standard is SHA -1 SSL. Cryptographic protocol suites must be a minimum of TLS v1.2 by June 30, 2016. (*TLS v1.0, TLS v1.1 and all SSL protocol suites are not permitted, after June 30, 2016.)*

What is a cryptographic key?

In cryptography, a key is a variable value of information or a parameter that is applied using an algorithm or cipher to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. Without a key, the algorithm will not yield a successful result. The length of the key is needed to determine how difficult it will be to decrypt the text within a message.

What is the length of the cryptographic key standard for Datawire?

Asymmetric keys must be a minimum RSA 2048 bits

What is an asymmetric key?

A form of encryption where there are two related keys--a key pair. A public key is made freely available to any party who might want to send a message. The second key is a secret and private which is only known by one party so that only one of the parties knows it.

What is an algorithm?

An algorithm is a procedure or formula for solving a problem.

What Security Protocol does Datawire Support?

Currently, Datawire supports SSL v3 and TLS v1.0 and SHA 1.
Starting June 16, 2015, Datawire will begin to support TLS v1.2 and SHA 256. All versions of TLS v 1.0, TLS v1.1 SSL v3 will be retired on November 15, 2016.

What is TLS?

Transport Layer Security (TLS) is a protocol that provides security and privacy between communicating applications and their users on the Internet. TLS is the successor to the Secure Sockets Layer (SSL).

What is SSL?

SSL is a layered protocol and consists of four sub-protocols:

- SSL Handshake Protocol
- SSL Change Cipher Spec Protocol
- SSL Alert Protocol
- SSL Record Layer

Recently Updated

What if I just changed from 1024-bit Secure Socket Layer (SSL) encryption to 2048-bit SSL encryption?

If you changed to 2048-bit, then you are using the current latest key size. However, **you are still required to support TLS v1.2 and SHA 256 by December 28, 2016.**

Why Must I Update My Security Protocol?

The National Institute of Standards and Technology (NIST) identified SSL (Secure Socket Layer) and early versions of TLS (Transport Layer Security, the successor protocol to SSL) as secure network communication protocols that are not acceptable for the protection of data due to inherent weaknesses.

Upgrading to a current, secure version of TLS is the only known way to remediate these vulnerabilities, which have been exploited by browser attacks such as POODLE and BEAST. Therefore, Datawire Secure Transport -l has migrated services to use TLS v1.2 protocol and will be removing TLS v1.0 and SSLv3.
For more information, please go to the PCI standards document, PCI website
https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information_Supplement_v1.pdf.

All Datawire merchants will need to remove SSLv3 and TLS v1.0. The deadline for this change is **June 30. 2016**.

Why is this Security Encryption Required?

Is this a PCI Compliance Requirement?

Yes! According to PCI Council, in PCI DSS v3.1 requirements, SSL and early TLS are no longer examples of strong cryptography or secure protocols. Effective immediately, new implementations must not use SSL or early TLS. For more information, please go to the PCI standards document, PCI website .

What is the PCI Council?

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

How Do I Comply?

What will Merchants Need to do to Comply?

Merchants will need to contact the POS terminal or Software (VAR) provider to make sure your terminal or software has been upgraded to support TLS v1.2 and SHA-256 TLS Certificates. Your POS terminal or VAR is responsible for servicing your POS system and for configuring your software to the new requirements. Please contact your VAR directly and find out what software updates your system will need in order to be compliant with the TLS v1.2 encryption standards and to ensure there will be no interruption to your payment processing. Then, merchants will need to test their system with the updated requirements before June 30, 2016.

What is needed for Vendors (POS or VARs) to Comply?

POS and VARs will need to update their software to support Datawire's new go-forward TLS v1.2 encryption and SHA 256 TLS Certificate standards before December 28, 2016.

When Do I Comply with the New Standards?

ALL Datawire merchants and vendors must comply by December 28, 2016. No exceptions will be made because Datawire will no longer support SSL v3, TLS v1.0 or SHA 1 Certificates.

What will happen if I Do Not Update by December 28, 2016?

For any merchants that do not update their POS system by December 28, you **will not** be able to connect using Internet to Process transactions. To avoid interruptions, you must upgrade to TLS v1.2 and SHA 256 by December 28, 2016. If your terminal supports dial, you may be able to connect to dial to process transactions.

Do MicroNode users have to Comply?

Yes! Currently, MicroNodes models 1100 and 1400 use SSL v3 and TLS v1.0. These MicroNodes will need to be updated to support TLS v1.2 and SHA 256 by June 30, 2016. Any active devices in service will automatically be updated by Q2 of 2016. Any devices that are not active will need to be brought online to be updated prior to June 30, 2016.

SUPPORT

What kind of support is provided for merchants or Vendors?

Merchants will contact DatawireSupport@firstdata.com for any production inquiries related to Datawire or can call Please dial into our 24-hour help desk (877) 274-7915 to update their certificates.

GLOSSARY OF TERMS

Algorithm	An algorithm is a procedure or formula for solving a problem.
API	Application Programming Interface (API)s is a set of routines, data structures, object classes and/or protocols provided by libraries and/or operating system services in order to support the building of applications.
CHD	Cardholder data
DSS	Data Security Standard
NAM	Network Access Module
NIST	The National Institute of Standards and Technology
PCI	The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment
POS	Point of Sale
SAD	Sensitive Authentication Data
SHA	Secure Hash Algorithm-pronounced as “Shaw”
SSL	Secure Sockets Layer
TLS	Transport Layer Security (TLS) is a protocol that provides security and privacy between communicating applications and their users on the Internet. TLS is the successor to the Secure Sockets Layer (SSL)
VAR	Value added Reseller

Security Protocol update to TLS v1.2 and SHA 256

End of Frequently Asked Questions
Version 1.0

October 2016