TLS 1.2 FAQ

For Bluefin Partners and Merchants

Issued on 8/01/2017

Q: What is SSL/TLS?

Transport Layer Security (TLS) (which was preceded by Secure Socket Layer (SSL)) 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.

Flaws have been discovered in TLS 1.0, so the Payment Card Industry (PCI) Council has listed TLS 1.0 as an insecure method to use for secure transactions.

PCI has established a date of June 30, 2018 for all payment processors, merchants and vendors to upgrade to a secure version of TLS (1.1 or higher).

Note that as a software provider and/or merchant, you have an established TLS connection with Bluefin to communicate with our PayConex gateway to process your customers' payments. In order to continue this communication, we must have all providers and merchants update to TLS 1.2 by October 1, 2017.

The reason why we are mandating upgrade to 1.2 and not 1.1 is that 1.1 will soon be obsolete. You will avoid two integrations (one to 1.1 and then another to 1.2) by just updating to 1.2 now.

Get more information on TLS 1.2.

Q: What are the SSL/TLS vulnerabilities?

Because of its widespread use online, SSL and TLS have been targets by security researchers and attackers. Many vulnerabilities in SSL and TLS have been uncovered over the past 20 years.

Q: What are the impacts of vulnerabilities?

Loss of confidentiality or integrity: Many of the attacks, particularly protocol vulnerabilities, allow for Man-in-the-Middle attacks allowing an attacker to decrypt sensitive information.

Loss of cryptographic keys: In some of the most serious cases, vulnerabilities could allow an attack to steal long-lived cryptographic keys.

Q: What do I do now?

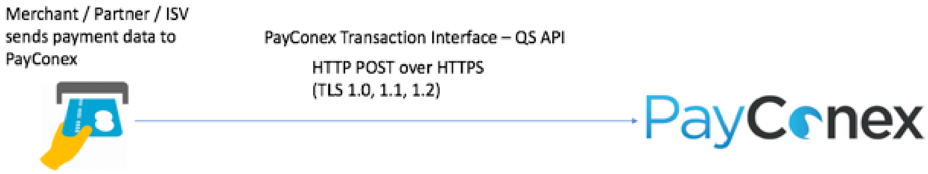
Migrate to TLS 1.2. Bluefin requires that you have TLS 1.2 in place by October 1, 2017. If you have not made the switch by that date, we may need to cease your payment processing.

Note that PCI has mandated that Bluefin, as your payment processor, must be in compliance with new TLS protocols by June 30, 2018 or we will not be able to process payments for any of our 15,000+ merchants

Also, our CERT environment ONLY supports TLS 1.2 at this time. Thus, you can use this environment to test if your solution is TLS 1.2 compliant. If it is not, you will get a connection error.

Q: How do I migrate to TLS 1.2?

Our customers that integrate into PayConex do so through the QSAPI (PayConex Application Programming Interface/API) interface that uses encryption (HTTPS - TLS 1.0, 1.1, 1.2) for the HTTP POST method (how the data is submitted). A diagram of this flow is below.


Merchant / Partner / ISV sends payment data to PayConex
PayConex Transaction Interface – QS API
HTTP POST over HTTPS (TLS 1.0, 1.1, 1.2)
PayConex

How your organization migrates to 1.2 depends on how you chose to integrate with PayConex via our QSAPI API.

Additionally, the PCI Council provides guidance on how to begin the migration process.

- Identify all system components and data flows relying on and/or supporting the vulnerable protocols
- For each system component or data flow, identify the business and/or technical need for using the vulnerable protocol
- Immediately remove or disable all instances of vulnerable protocols that do not have a supporting business or technical need
- Identify technologies to replace the vulnerable protocols and document secure configurations to be implemented
- Document a migration project plan outlining steps and timeframes for updates
- Implement risk reduction controls to help reduce susceptibility to known exploits until the vulnerable protocols are removed from the environment
- Perform migrations and follow change control procedures to ensure system updates are tested and authorized
- Update system configuration standards as migrations to new protocols are completed

It is important to build a communications element into migration planning. Consider how much leg work it will take to get agreement on changing.

For additional FAQ's, please visit the PCI Council's website.

If you have other questions, please contact your Bluefin Relationship Manager.