What You Need to Know about TLS v1.2 and SHA-2

Due to the ever-evolving nature of security risks, the payments industry is undergoing two major initiatives involving the upgrade of encryption protocols and data security. First, the encryption protocols SSL (Secure Sockets Layer) and early versions of TLS (Transport Layer Security) are being phased out in favor of the more robust TLS v1.2.

At the same time, payment processors are updating the digital certificates on their processing networks from SHA-1 (Secure Hash Algorithm) to a stronger SHA-2 level, increasing the encryption and authentication capabilities to keep payment data secure.

These industry-wide changes affect customers and partners with an IP connection or Internet/browser-based solution. Keeping your payments secure is critical to your business and top of mind for us.

In an effort to educate our customers on this initiative, we've created a microsite that clearly explains the steps to take to ensure a seamless transition to TLS v1.2 and SHA-2. Please visit **www.besha2ready.com** for more information. The site is organized by product for easy navigation.

The following browsers and versions support TLS v1.2/ SHA-2 technology:

- Google Chrome, version 38 and higher
- Mozilla Firefox, version 27 and higher; and ESR version 31.0 and higher
- Internet Explorer, version 11 and higher
- Safari, version 7 and higher
- Opera, version 12.18 and higher

It's important to ensure your operating system supports these protocols as well:

- Microsoft Windows 7 and higher
- Microsoft Windows Server 2008 R2 and higher
- OS X Mavericks (version 10.9) and higher
- Android 5.0 and higher
- iOS 5 and higher
- Windows Phone 8.1, Windows 10 Mobile

A Brief History of Encryption Protocols

1994 – **SSL**: secure sockets layer. First developed by Netscape Communications

1999 – **TLS**: transport layer security. An evolution of SSL 3.0, TLS 1.0 was adopted by the Internet Engineering Task Force (IETF).

2008– **TLS v1.2** released.

2015 – **SHA-1**: secure hash algorithm 1; is no longer considered secure.

Source: www.ibm.com/developerworks/library/ws-ssl-security