SSL/TLS PROTOCOL

The SSL and TLS protocols are used in conjunction with a SSL web certificate to encrypt traffic between a browser and web application. This is to **allow secure communication** over the internet for **keeping private data private**.

- PCI has mandated that **SSLv3 as well as TLS 1.0 not be used** anymore and to use only TLS1.1 or higher. **Sabre is mandating TLS 1.2 or higher.** The original mandate for this was changed to allow, in certain circumstances, the use of SSLV3 and TLS1.0 until June 30th 2018.
- SHS no longer supports SSLv3 for incoming connections but will allow outgoing SSLv3 for reservation delivery. All customers need to upgrade their servers to support TLS1.2 to ensure future connectivity.
- SHS no longer supports SHA1 for secure connections in favor of SHA2 (SHA256). All customers need to upgrade their servers to accommodate this requirement in order to ensure connectivity.
- SHA1 certificates are no longer renewable by any certificate authorities. Therefore, any certificate renewals performed by SHS will be SHA2. This is in line with industry wide security measurements and SHS will abide by industry regulations.

DETAILED EXPLANATION OF SSL AND TLS

(Source: https://en.wikipedia.org/wiki/Transport_Layer_Security)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, instant messaging, and voice-over-IP (VoIP). Major web sites use SSL/TLS to secure all communications between their servers and web browsers.

The primary goal of a SSL/TLS protocol is to provide privacy and data integrity between two communicating computer applications. When secured by SSL/TLS, connections between a client (e.g., a web browser) and a server (e.g., gc.synxis.com) have one or more of the following properties:

- The connection is private because symmetric cryptography is used to encrypt the data transmitted.
- The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).
- The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

FURTHER INDUSTRY ARTICLES/ RESOURCES

- http://www.tenable.com/blog/pci-ssc-announces-the-end-of-ssl-usage-for-the-payment-card-industry
- http://blog.pcisecuritystandards.org/migrating-from-ssl-and-early-tls
- https://technet.microsoft.com/en-us/library/cc781476(v=ws.10).aspx
- https://www.us-cert.gov/ncas/alerts/TA14-290A