PCI DSS 3.1 TLS Requirements Change

The Payment Card Industry Security Standards Council has revised their original sunset date for SSL and early versions of TLS. The revisions state:

- All processing and third party entities – including Acquirers, Processors, Gateways and Service Providers must provide a TLS 1.1 or greater service offering by June 2016.
- Consistent with the existing language in PCI DSS v3.1, all new implementations must be enabled with TLS 1.1 or greater. TLS 1.2 is recommended.
- All entities must cutover to use only a secure version of TLS (as defined by NIST) effective 30 June 2018.

The full announcement can be read here and an formal update to the PCI DSS v3.1 requirements will be made in 2016.

PCI DSS Changes Summary

"SSL has been removed as an example of strong cryptography in the PCI DSS, and can no longer be used as a security control after June 30, 2016." – PCI Security Standards Council

The newest revision of the PCI Security Standards Council policy, PCI-DSS 3.1, establishes a new baseline for strong cryptography, specifically TLS (formerly SSL), required to secure payment card related traffic – TLS 1.2.
This change must be adopted by sites which handle payment card data no later than 30 June 2016. According to the PCI Council FAQ: "The successor protocol to SSL is TLS (Transport Layer Security) and its most current version as of this publication is TLS 1.2," according to the FAQ. "TLS 1.2 currently meets the PCI SSC definition of "strong cryptography". While PCI is specific to payment card information, the PCI guidelines also are used by sites in general for security guidance.

No version of SSL (SSL 3.0 and earlier) is considered "strong cryptography" for the purposes of protecting customer data, but Singledigits has not supported SSL 3.0, since the POODLE vulnerability was identified.

For Singledigits customers, the primary impact of PCI 3.1 is that TLS 1.0 and TLS 1.1 are also insufficient to secure payment card related traffic. Regardless of whether or not your specific site(s) use Credit Card billing or not, we are upgrading the entire cloud system to only support TLS 1.2. *Singledigits will NOT, under any circumstances, provide exceptions to sites wishing to use older deprecated TLS or SSL versions*, as this would lead to PCI non-compliance for our customers that are using or require PCI compliance. To support this Singledigits will be migrating to support only TLS 1.2 by June 30, 2018. Quality Assurance testing is on-going with these changes, and primarily we expect the only issues to be related to older devices that no longer are receiving manufacturer updates and use older TLS versions and cipher suites, one such example is older Blackberry phones.

Implementation extension:

On December 15th, the PCI Council updated its date for when TLS 1.0 (an older security protocol used on SSL secure web pages) would be considered obsolete and a PCI violation. Originally, they listed June 30, 2016 as the End of Life (EOL) date for TLS 1.0. They have now extended that deadline to June 30, 2018. You can read more details on the **PCI Council blog post**.

How this impacts you (and your customers) as a customer of Singledigits:

Your guests / customers will attempt to use the HSIA (and other) services provided by Singledigits, if their devices are relatively new/modern and have been updated to the latest supported software from their respective manfacturers, then there should be no impact at all. For users using older devices that are End-of-Life (EOL) and do not receive any updates and still use TLS 1.0 or SSLv3 will NOT work after June 30, 2018. If your customer call our support center, we can assist them to authenticate and get online without having to visit the Singledigits portal page(s) – however – users with this problem will have additional issues browsing secure sites all over the internet. This means their user experience will be majorly degraded.

Any Customers utilizing the Broadband Authentication Platform (BAP) for administrative functions, such as reports, logs, event management and etc. will be required to use a supported browser, and updated to the latest released version and it should support the latest TLS 1.2 methods.

The PCI DSS v3.1 requirements directly affected are:

- **Requirement 2.2.3** Implement additional security features for any required services, protocols, or daemons considered insecure.
- **Requirement 2.3** Encrypt all non-console administrative access using strong cryptography.
- **Requirement 4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

Both TLS 1.0 and TLS 1.1 have known weaknesses which make them less than ideal for protecting information, although substantially stronger than SSL 3.0. TLS 1.0/TLS 1.1 are widely used today, protecting a substantial fraction of encrypted web traffic.

As a result of the PCI 3.1 changes, Singledigits has implemented a transition plan to migrate al services to TLS 1.2 in advance of the PCI Council requirements.

Links for additional reading:

Migrating from SSL and Early TLS - PCI Security Standards Council

TLS 1.1 encryption or higher - PCI Security Standards Council

https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

https://payment-services.ingenico.com/int/en/ogone/support/products/tls

https://stripe.com/blog/completing-tls-upgrade