Change Notice:
Critical – Action Required

PLEASE CASCADE TO OPERATIONAL AREAS AS APPROPRIATE

Replacing SHA-1 with SHA-2 Certificates

At Payment Express we take security seriously. As a part of the industry wide initiative to migrate from SHA-1 to SHA-2 certificates, Payment Express have taken proactive measures to further secure its website: https://www.paymentexpress.com by replacing end-point and intermediate server certificates with SHA-2.

Detailed Background

Microsoft and Google announced SHA-1 deprecation plans that may affect websites with SHA-1 certificates expiring as early as after December 31, 2015. According to Google's blog on "Gradually Sunsetting SHA-1", Chrome version 39 and later will display visual security indicators on sites with SHA-1 SSL certificates with validity beyond January 1, 2016. The production release of Chrome 39 is expected to be in November, 2014. The sites will be treated with one of the following indicators: "secure, but with minor errors" (lock with yellow triangle), "neutral, lacking security" (blank page icon) and "affirmative insecure" (lock with a red X). In order to prevent online users on Chrome version 39 and later from experiencing these indicators, SHA-1 SSL certificates expiring after December 31, 2015 must be replaced with SHA-256 (SHA-2) certificates.

Microsoft's SHA-1 deprecation plan differs in the activation time and browser behavior. Microsoft's security advisory on "Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program" informed us that Windows will cease accepting SHA-1 SSL certificates on January 1, 2017. To continue to work with Microsoft platforms, all SHA-1 SSL certificates issued before or after this announcement must be replaced with a SHA-2 equivalent by January 1, 2017.

The SHA-1 deprecation plans also impact SHA-1 intermediate certificates; SHA-2 end-entity certificates must be chained to SHA-2 intermediate certificates to avoid the adverse browser behaviors described above. SHA-1 root certificates are not impacted.

Source: http://www.symantec.com/page.jsp?id=sha2-transition

What does this mean for your business?

We will be making this change to our production and QA end-points:

https://sec.paymentexpress.com
https://qa4.paymentexpress.com

In order to prepare for this change we suggest that all our partners ensure that this certificate chain is added to all end-points that connect to our payment services.

You can download the new certificate bundle in PEM format from here: https://www.paymentexpress.com/downloads/bundle2014.zip

What do you need to do?

- **If your application requires certificates to be explicitly trusted then you must download the bundle above. This will either need to be applied into a key-store (Java/OpenSSL) or into a certificate store (Windows).**
- **Some servers may already trust the root and intermediary certificates by default, however our client certificate may need to be specifically trusted depending on your security settings.**

paymentexpress®

SSLv3.0 Deprecation

(POODLE – "Padded Oracle" exploit)

Payment Express wishes to advise clients and partners, as a preventative measure the Secure Sockets Layer (SSL) protocol will be disabled on all front-end web servers. The way SSL ciphers encrypt traffic could potentially allow attackers to decrypt information.

This change is in response to the "Poodle" ("Padding Oracle") cyber-attack recently uncovered. The attack exploits SSL which could allow for encrypted data to be revealed.

Google's security team discovered a vulnerability in SSL version 3.0<http://googleonlinesecurity.blogspot.com.au/2014/10/this-poodle-bites-exploiting-ssl-30.html> in October 2014. Historically SSL was supplanted by TLS and the current version is 1.2, but older systems fall back to using SSL 3.0 for compatibility. This is a design flaw in SSL/TLS and there is no patch to fix the bug. Instead, most organisations are disabling support for SSL 3.0, a protocol which is old and deprecated. Many of our business partners may still be using systems that rely on SSL 3.0, we request that these systems be configured/upgraded to support TLS.

Targeted Date & Time for Implementation

Change	Cutover Date	Cutover Time
SHA1 – SHA2 Upgrade Production	1st December (New Zealand) 30th November (Australia) 30th November (United States of America) 30th November (United Kingdom)	00:00:00 (New Zealand) 22:00:00 (Australia Eastern) 19:00:00 (Australia Western) 06:00:00 (Eastern Standard Time) 03:00:00 (Pacific Standard Time) 11:00:00 (Greenwich Mean Time - London)
SHA1 – SHA2 Upgrade QA/development	24th November (New Zealand) 23rd November (Australia) 23rd November (United States of America) 23rd November (United Kingdom)	00:00:00 (New Zealand) 22:00:00 (Australia Eastern) 19:00:00 (Australia Western) 06:00:00 (Eastern Standard Time) 03:00:00 (Pacific Standard Time) 11:00:00 (Greenwich Mean Time - London)
Disable SSLv3.0 Production, already deployed to QA/development environment	24th November (New Zealand) 23rd November (Australia) 23rd November (United States of America) 23rd November (United Kingdom)	00:00:00 (New Zealand) 22:00:00 (Australia Eastern) 19:00:00 (Australia Western) 06:00:00 (Eastern Standard Time) 03:00:00 (Pacific Standard Time) 11:00:00 (Greenwich Mean Time - London)

QUESTIONS?

If you have any concerns or queries regarding these changes, please, contact our Support team:

US 1 877 434 0003 **UK** 0800 088 6040
NZ 0800 729 6368 **AU** 1 800 006 254

Email: support@paymentexpress.com

paymentexpress®