Keamanan pedagang

Panduan peningkatan system

Klik DI SINI untuk informasi tentang kesesuaian dengan SHA-256.

Persiapkan integrasi Anda

Ancaman keamanan global selalu berubah, dan keamanan pedagang selalu menjadi prioritas utama kami. Agar terlindung dari ancaman saat ini dan di masa mendatang, kami menyarankan agar Anda melakukan peningkatan berikut terhadap integrasi Anda:

1. Hentikan penggunaan VeriSign G2 Root Certificate
2. Perbarui integrasi Anda untuk mendukung sertifikat menggunakan SHA-256 algorithm

Mengapa berubah?

Industri CA (Certificate Authority atau Otoritas Sertifikat) publik terus meningkatkan keamanan sertifikat SSL. Dalam persiapan diwajibkannya penggunaan SHA-256 signing algorithm pada 2016, VeriSign G2 Root Certificate tidak akan didukung lagi. Sertifikat ini sebelumnya digunakan untuk menyambung ke titik akhir API PayPal dan PIP (Pemberitahuan Instan Pembayaran).

Kapan saya harus melakukannya?

Sebaiknya Anda bertindak sesegera mungkin agar siap dengan perubahan ini. Untuk jadwal terperinci, termasuk tanggal peningkatan titik akhir API Live dan Sandbox, lihat situs mikro Perubahan Sertifikat SSL 2015-2016 kami.

NOTE: Perubahan tersebut ditujukan untuk mengatasi masalah keamanan di seluruh industri dan tidak khusus hanya bagi PayPal. Saat diterapkan, perubahan tersebut akan meningkatkan privasi dan keandalan integrasi PayPal Anda. Karena perincian perubahan berbeda menurut sistem, kami menyarankan agar perubahan dibuat dengan bantuan administrator sistem yang terkualifikasi.

1. Hentikan penggunaan VeriSign G2 Root Certificate

Masalah: Di masa lalu, sertifikat SSL terbitan VeriSign yang memiliki rantai kepercayaan yang ditandai oleh G2 Root Certificate 1024-bit. Dalam beberapa tahun terakhir, pemerintah dan industri CA publik telah beralih ke sertifikat 2048-bit yang lebih aman, sehingga VeriSign kini menerbitkan sertifikat SSL dengan rantai kepercayaan yang ditandai oleh G5 Root Certificate 2048-bit terbitan tahun 2006.

Tanggapan kami: Sesuai dengan standar industri, kami tidak akan lagi menerima sambungan aman ke titik akhir API/PIP (Pemberitahuan Instan Pembayaran) yang mengharapkan sertifikat/rantai kepercayaan ditandai oleh G2 Root Certificate. Hanya permintaan sambungan aman yang mengharapkan sertifikat/rantai kepercayaan ditandai oleh G5 Root Certificate yang akan menghasilkan sambungan aman.

Tindakan yang harus Anda lakukan...

Jika sistem Anda saat ini menginstruksikan penggunaan VeriSign Root Certificate tersebut, hentikan penggunaan sambungan SSL yang mengandalkan sertifikat dengan pengidentifikasi G2. Industri berupaya aktif untuk secara bertahap menghapus Root Certificate 1024-bit tahun ini.

- Sambungan aman yang mengandalkan rantai sertifikat yang ditandai oleh G2 Root Certificate tidak didukung:

Unit organisasi	Class 3 Public Primary Certification Authority - **G2**
Nomor seri	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Certificate SHA1 fingerprint	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Sambungan aman yang mengandalkan rantai sertifikat yang ditandai oleh G5 Root Certificate didukung:

Nama Umum	VeriSign Class 3 Public Primary Certification Authority - **G5**
Nomor Seri	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Certificate SHA1 Fingerprint	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Ikuti pedoman ini untuk memastikan Anda tersambung secara aman dengan menggunakan VeriSign G5 Root Certificate yang didukung:

1. **Periksa penyimpanan sertifikat Anda.** Minta host atau administrator sistem situs web Anda untuk memverifikasi bahwa VeriSign G5 Root Certificate tercakup dalam root store yang digunakan oleh kode Anda untuk logika validasi. Jika demikian, maka Anda tidak perlu melakukan tindakan apa pun.
    - Lihat tautan berikut untuk memeriksa keystore keberadaan G5 Root Certificate menggunakan Java, Linux, atau Windows.
2. **Periksa log kesalahan Anda.** Jika VeriSign G5 Root Certificate belum diunduh untuk menggantikan G2 Root Certificate, Anda mungkin akan melihat pesan kesalahan seperti:
    - Kesalahan handshake SSL, "Sertifikat terpercaya tidak ditemukan"
    - Kode hasil -31, "Rantai sertifikat belum memvalidasi, sertifikat lokal tidak ditemukan"
    - Kode hasil -8, "Sambungan SSL gagal"
    - Kesalahan -1

    Untuk menyelesaikan masalah ini:

    - Perbarui perangkat lunak Anda ke versi terbaru yang mendukung SHA-256, atau
    - Jika keystore digunakan untuk validasi/autentikasi sertifikat, instal VeriSign G5 Root Certificate di keystore Anda.
3. **Dapatkan VeriSign G5 Root Certificate.** Jika penyimpanan sertifikat atau klien Java Anda tidak mencakup VeriSign G5 Root Certificate, minta administrator sistem untuk mengunduhnya dari VeriSign dan simpan di penyimpanan sertifikat, serta paket autentikasi sambungan SSL lainnya.
    - Unduh VeriSign G5 Root Certificate milik Symantec
    - Unduh sertifikat SSL server khusus, jika diminta oleh server Anda

2. Perbarui ke SHA-256 signing algorithm

Masalah: SHA-1 adalah algoritme kriptografis yang telah ada selama 22 tahun, namun keberadaannya terancam seiring peningkatan kemampuan komputasi. SHA-256 menggunakan algoritme yang lebih kuat dengan nilai hash 256-bit.

Tanggapan kami: Kami akan meningkatkan sertifikat SSL di semua titik akhir Live dan Sandbox dari SHA-1 ke SHA-256 yang lebih tangguh dan lebih canggih pada pertengahan 2016.

Tindakan yang harus Anda lakukan...

Ikuti pedoman ini untuk beralih dari penggunaan sertifikat SSL yang memanfaatkan SHA-1 signing algorithm ke SHA-256 signing algorithm yang lebih tangguh:

1. **Periksa lingkungan Anda.** Pastikan lingkungan Anda mendukung sertifikat SHA-256.
   - Lihat sumber informasi online, seperti Panduan Kompatibilitas SHA-2 DigiCert serta Daftar Browser dan Server Symantec yang Didukung, untuk daftar perangkat keras dan perangkat lunak yang didukung.
   - Jika sebagian lingkungan Anda tidak mendukung SHA-256, Anda harus mengganti atau meningkatkan bagian tersebut agar dapat menerapkan sertifikat baru.
   - Windows 2000 Server dan beberapa versi Windows XP mungkin tidak kompatibel dengan SHA-2. Blog PKI Windows di SHA2 dan Windows dapat membantu dengan patch dan rekomendasi untuk meningkatkan lingkungan Anda.
2. **Periksa sertifikat Anda.** Jika lingkungan Anda mendukung SHA-256, pastikan Anda memiliki VeriSign G5 Root Certificate di keystore.

Pertanyaan?

Untuk perincian tambahan dan tanya jawab, kunjungi situs mikro Perubahan Sertifikat SSL 2015-2016 kami.

Terima kasih!

Terima kasih atas tindakan Anda dalam menangani masalah ini dan memahami pendekatan kami. Meskipun kami menyadari bahwa langkah-langkah ini dapat menimbulkan masalah kompatibilitas, namun ketidaknyamanan jangka pendek ini ditujukan untuk memenuhi janji kami kepada masing-masing pelanggan bahwa kami akan menjaga keamanan informasi rekening dan informasi keuangan mereka.