ความปลอดภัยของผู้ค้า

คู่มือการอัปเกรดระบบ

โปรดคลิก ที่นี่ เพื่ออ่านข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตามใบรับรอง SHA-256

เตรียมการผนวกรวมของคุณให้พร้อมสำหรับอนาคต

ภัยคุกคามด้านความปลอดภัยทั่วโลกมีการเปลี่ยนแปลงอยู่ตลอดเวลา
และความปลอดภัยของผู้ค้ายังคงเป็นสิ่งที่เราให้ความสำคัญสูงสุดมาอย่างต่อเนื่อง
เพื่อเป็นการป้องกันภัยคุกคามในปัจจุบันและอนาคต เราขอแนะนำให้คุณทำการอัปเกรดต่อไปนี้ในการผนวกรวม:

1. ยกเลิกการใช้ใบรับรอง Root รุ่น G2 ของ VeriSign
2. อัปเดตการผนวกรวมเพื่อรองรับใบรับรองที่ใช้อัลกอริธึม SHA-256

ทำไมต้องเปลี่ยน

กลุ่มหน่วยงานผู้ออกใบรับรอง (Certificate Authority - CA) แบบสาธารณะได้ปรับปรุงความปลอดภัยของใบรับรอง SSL มาอย่างต่อเนื่อง ในการเตรียมความพร้อมเพื่อขอใช้อัลกอริธึมแบบลงลายมือชื่อ SHA-256 สำหรับปี 2559 นั้น ใบรับรอง Root รุ่น G2 ของ VeriSign จะไม่สามารถรองรับได้อีกต่อไป ใบรับรองนี้เคยใช้เพื่อเชื่อมต่อ Endpoint ของ API ใน PayPal และบริการแจ้งทันทีที่ได้รับเงิน (Instant Payment Notification - IPN)

ต้องดำเนินการเมื่อไหร่

เราขอแนะนำให้คุณดำเนินการโดยเร็วที่สุด เพื่อให้พร้อมสำหรับการเปลี่ยนแปลงเหล่านี้

สำหรับกรอบเวลาโดยละเอียด รวมถึงวันที่ที่อัปเกรดสำหรับ API Endpoint แบบ Live และ Sandbox
สามารถดูได้ที่ไซต์ย่อยของการเปลี่ยนใบรับรอง SSL ปี 2558-2559

NOTE: การเปลี่ยนแปลงเหล่านี้มีขึ้นเพื่อแก้ไขประเด็นปัญหาด้านความปลอดภัยทั่วทั้งภาคธุรกิจและไม่ใช่เฉพาะกับ PayPal เมื่อมีการเปลี่ยนแปลงแล้วจะทำให้การผนวกรวม PayPal มีความเป็นส่วนตัวและมีความน่าเชื่อถือมากขึ้น เนื่องจากรายละเอียดของการเปลี่ยนแปลงเหล่านี้แตกต่างกันไปตามระบบ เราขอแนะนำให้ดำเนินการภายใต้ความช่วยเหลือของผู้ดูแลระบบที่มีคุณสมบัติเหมาะสม

1. ยกเลิกการใช้ใบรับรอง Root รุ่น G2 ของ VeriSign

ประเด็นปัญหา: ในอดีต VeriSign ได้ออกใบรับรอง SSL
ที่มีลำดับความน่าเชื่อถือซึ่งลงลายมือชื่อโดยใบรับรอง Root รุ่น G2 แบบ 1024-bit ในช่วงหลายปีมานี้
หน่วยงานผู้ออกใบรับรองทั้งภาครัฐและมหาชนของสหรัฐได้เปลี่ยนไปออกใบรับรองแบบ 2048-bit
ที่ปลอดภัยกว่า ดังนั้นในขณะนี้ VeriSign จึงได้ออกใบรับรอง SSL
ที่มีลำดับความน่าเชื่อถือซึ่งลงลายมือชื่อโดยใบรับรอง Root รุ่น G5 แบบ 2048-bit ที่ออกในปี 2549

การดำเนินการของเรา: เพื่อให้เป็นไปตามมาตรฐานทางธุรกิจ เราจะไม่ยอมรับการเชื่อมต่อที่ปลอดภัยกับ API/IPN Endpoint ที่คาดว่าเป็นใบรับรอง/ลำดับความน่าเชื่อถือที่ลงลายมือชื่อโดยใบรับรอง Root รุ่น G2 อีกต่อไป
มีแต่คำขอการเชื่อมต่อที่ปลอดภัยที่คาดว่าเป็นใบรับรอง/ลำดับความน่าเชื่อถือที่ลงลายมือชื่อโดยใบรับรอง Root รุ่น G5 เท่านั้นที่ จะทำให้มีการเชื่อมต่อที่ปลอดภัยได้

สิ่งที่คุณต้องทำ...

ถ้าระบบของคุณมีคำสั่งให้ใช้ใบรับรอง Root ของ VeriSign คุณต้องยกเลิกการใช้การเชื่อมต่อ SSL
ที่ขึ้นอยู่กับใบรับรองที่ใช้รหัสประจำตัว G2 ทางหน่วยงานกำลังเร่งดำเนินการเพื่อเลิกใช้ใบรับรอง Root แบบ 1024-bit ในปีนี้

- ไม่รองรับการเชื่อมต่อที่ปลอดภัยที่ขึ้นอยู่กับกลุ่มใบรับรองที่ลงลายมือชื่อโดยใบรับรอง Root รุ่น G2:

หน่วยงานองค์กร	หน่วยงานที่ออกใบรับรองขั้นต้นแบบสาธารณะชั้นที่ 3 - **G2**
หมายเลขลำดับ	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
ลายนิ้วมือใบรับรอง SHA1	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- รองรับการเชื่อมต่อที่ปลอดภัยที่ขึ้นอยู่กับกลุ่มใบรับรองที่ลงลายมือชื่อโดยใบรับรอง Root รุ่น G5:

ชื่อทั่วไป	หน่วยงานที่ออกใบรับรองขั้นต้นแบบสาธารณะชั้นที่ 3 ของ VeriSign - **G5**
หมายเลขลำดับ	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
ลายนิ้วมือใบรับรอง SHA1	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

ปฏิบัติตามคำแนะนำเหล่านี้เพื่อให้มั่นใจได้ว่าคุณกำลังเชื่อมต่ออย่างปลอดภัยโดยใช้ใบรับรอง Root รุ่น G5 ของ VeriSign ที่รองรับ:

1. **ตรวจสอบร้านที่ออกใบรับรอง** ขอให้โฮสต์เว็บไซต์หรือผู้ดูแลระบบตรวจสอบว่ามีใบรับรอง Root รุ่น G5 ของ VeriSign รวมอยู่ในร้านออกใบรับรอง Root ที่ใช้รหัสของคุณในการยืนยันหรือไม่ ถ้ามีอยู่แล้ว ก็ไม่จำเป็นต้องดำเนินการใดๆ อีก
   - ดูลิงก์ต่อไปนี้เพื่อตรวจสอบ keystore ของใบรับรอง Root รุ่น G5 ที่ใช้ Java, Linux หรือ Windows
2. **ตรวจสอบบันทึกที่ผิดพลาด** ถ้ายังไม่ได้ดาวน์โหลดใบรับรอง Root รุ่น G5 ของ VeriSign มาแทนใบรับรอง Root รุ่น G2 คุณอาจเห็นข้อความแสดงข้อผิดพลาด เช่น:
   - ข้อผิดพลาดในการแลกเปลี่ยนสัญญาณ SSL, "ไม่พบใบรับรองที่เชื่อถือได้"
   - รหัสผลลัพธ์ -31, "กลุ่มใบรับรองไม่ยืนยันความถูกต้อง ไม่พบใบรับรองในท้องถิ่น"
   - รหัสผลลัพธ์ -8, “การเชื่อมต่อ SSL ล้มเหลว”
   - -1 ข้อผิดพลาด

   ถ้าต้องการแก้ไขปัญหาเหล่านี้ ให้:
   - อัปเดตซอฟต์แวร์ของคุณเป็นเวอร์ชันล่าสุดที่รองรับ SHA-256 หรือ

- ถ้ามีการใช้ keystore เพื่อตรวจสอบความถูกต้อง/ตรวสอบสิทธิ์ของใบรับรอง ให้ติดตั้งใบรับรอง Root รุ่น G5 ของ VeriSign ไว้ใน keystore ของคุณ

3. **ขอใบรับรอง Root รุ่น G5 ของ VeriSign** ถ้าร้านที่ออกใบรับรองหรือไคลเอ็นต์ Java ของคุณไม่มีใบรับรอง Root รุ่น G5 ของ VeriSign ให้ขอให้ผู้ดูแลระบบดาวน์โหลดใบรับรองดังกล่าวจาก VeriSign และบันทึกในร้านที่ออกใบรับรอง รวมถึงแพคเกจการตรวจสอบสิทธิ์การเชื่อมต่อ SSL อื่นๆ
   - ดาวน์โหลด ใบรับรอง Root รุ่น G5 ของ VeriSign จาก Symantec
   - ดาวน์โหลดใบรับรอง SSL เซิร์ฟเวอร์ที่เฉพาะเจาะจง หากเซิร์ฟเวอร์ของคุณกำหนดไว้

2. อัปเดตเป็นอัลกอริธึมที่ลงลายมือชื่อ SHA-256

ประเด็นปัญหา: SHA-1 เป็นอัลกอริธึมการเข้ารหัสที่มีอายุ 22 ปีซึ่งถูกคุกคามจากกำลังการประมวลผลที่เพิ่มมากขึ้น SHA-256 ใช้อัลกอริธึมที่มีประสิทธิภาพมากขึ้นด้วยค่าแฮชที่ 256-bit

การดำเนินการของเรา: เรากำลังอัปเกรดใบรับรอง SSL บน Endpoint แบบ Live และ Sandbox จาก SHA-1 เป็น SHA-256 ที่แน่นหนาและมีประสิทธิภาพมากขึ้นในช่วงกลางปี 2559

สิ่งที่คุณต้องทำ...

ทำตามคำแนะนำเหล่านี้เพื่อเปลี่ยนจากการใช้ใบรับรอง SSL ที่ใช้ประโยชน์จากอัลกอริธึมแบบลงลายมือชื่อ SHA-1 เป็นอัลกอริธึมแบบลงลายมือชื่อ SHA-256 ที่มีประสิทธิภาพมากขึ้น

1. **ตรวจสอบสภาพแวดล้อมของคุณ** ตรวจสอบให้แน่ใจว่าสภาพแวดล้อมของคุณรองรับใบรับรอง SHA-256
   - อ่านแหล่งข้อมูลออนไลน์ เช่น คู่มือการใช้งานร่วมกับ SHA-2 ของ DigiCert และรายการเบราว์เซอร์และเซิร์ฟเวอร์ที่รองรับของ Symantec สำหรับรายการฮาร์ดแวร์และซอฟต์แวร์ที่รองรับ
   - ถ้าส่วนต่างๆ ในสภาพแวดล้อมของคุณไม่รองรับ SHA-256 คุณจะต้องแทนที่หรืออัปเกรดในส่วนนั้นก่อนจึงจะสามารถนำใบรับรองใหม่ไปใช้งานได้
   - Windows 2000 Server และ Windows XP บางเวอร์ชันอาจไม่สามารถใช้งานกับ SHA-2 ได้ บล็อก Windows PKI บน SHA2 และ Windows

     สามารถช่วยได้ด้วยโปรแกรมการแก้ไขข้อผิดพลาดและคำแนะนำเพื่ออัปเกรดสภาพแวดล้อมของคุณ

2. **ตรวจสอบใบรับรองของคุณ** ถ้าสภาพแวดล้อมของคุณรองรับ SHA-256 โปรดตรวจสอบให้แน่ใจว่าคุณมีใบรับรอง Root รุ่น G5 ของ VeriSign ใน keystore

ถ้ามีข้อสงสัย

สำหรับรายละเอียดเพิ่มเติมและคำถามที่พบบ่อย โปรดดูที่ ไซต์ย่อยของการเปลี่ยนใบรับรอง SSL ปี 2558-2559ของเรา

ขอบคุณค่ะ

ขอบคุณที่เข้าใจถึงความเร่งด่วนของปัญหานี้และแนวทางการดำเนินการของเราค่ะ
ถึงแม้ว่าขั้นตอนที่จำเป็นนี้อาจทำให้เกิดปัญหาเรื่องความเข้ากันได้ แต่เราขอย้ำว่าความยุ่งยากเพียงระยะเวลาสั้นๆ นั้นเทียบไม่ได้เลยกับคำมั่นสัญญาที่ทั้งคุณและเราได้ให้ไว้กับลูกค้าว่าจะดูแลบัญชีและข้อมูลทางการเงินของลูกค้าอย่างปลอดภัย