Sikkerhed for forhandlere

Vejledning til systemopgradering

Klik HER for information ang. overholdelse af SHA-256.

Gør din integration fremtidssikret

Der kommer hele tiden nye globale sikkerhedstrusler, og derfor prioriterer vi vores forhandleres sikkerhed meget højt. Vi opfordrer derfor til, at følgende opgraderinger bliver udført, så vores forhandlere er beskyttet mod aktuelle og fremtidige trusler:

1. Afbryd brugen af VeriSign G2-rodcertifikatet.
2. Opdater din integration, så den understøtter certifikater med SHA-256-algoritmen.

Derfor skal du opgradere

Den offentlige Certificate Authority-branche gør hele tiden SSL-certifikaterne mere sikre. I 2016 bliver det obligatorisk at bruge SHA-256-signeringsalgoritmen, og derfor vil VeriSign G2-rodcertifikatet ikke længere blive understøttet. VeriSign G2-rodcertifikatet er før blevet brugt til at oprette forbindelse til slutpunkterne PayPal API og IPN (Instant Payment Notification).

Tidsplan for opdateringen

Vi anbefaler, at du handler hurtigst muligt for at forberede dig på disse ændringer. Hvis du vil se en detaljeret tidsplan med datoer for opgraderingen af Live- og Sandbox API-slutpunkterne, kan du gå til 2015-2016 SSL Certificate Change Microsite.

NOTE: Det er vigtigt at bemærke, at det ikke kun er os, der foretager disse ændringer, men at det er hele branchen, og at det sker for at bekæmpe sikkerhedsproblemer. Når ændringerne er gennemført, vil de gøre dine PayPal-integrationer mere sikre. De ændringer, der skal foretages, kan variere, afhængigt af systemerne, og vi anbefaler derfor, at opgraderingen sker i samarbejde med en kvalificeret systemadministrator.

1. Afbryd brugen af VeriSign G2-rodcertifikatet.

Problemet: Tidligere udsendte VeriSign SSL-certifikater med en certifikatkæde, som var signeret af et 1024-bit G2-rodcertifikat. Inden for de seneste år er myndighederne og den offentlige CA-branche begyndt at bruge de mere sikre 2048-bit certifikater, hvilket betyder, at VeriSign nu udsteder SSL-certifikater, som har en certifikatkæde signeret af et 2048-bit G5-rodcertifikat, der er udstedt i 2006.

Vores løsning: Ifølge branchestandarder accepterer vi ikke længere sikre forbindelser til de API-/IPN-slutpunkter, som forventer, at vores certifikat/certifikatkæde signeres af G2-rodcertifikatet. Det vil kun være anmodninger om sikre forbindelser, der forventer, at vores certifikat/certifikatkæde signeres af G5-rodcertifikatet, der vil kunne bruges til at oprette sikre forbindelser.

Copyright © 2015 PayPal Inc. Alle rettigheder forbeholdes.

Din opgave

Stands med at bruge de SSL-forbindelser, der bruger VeriSign-rodcertifikater med G2-identifikatorer, hvis dit system i øjeblikket tillader, at dette bestemte rodcertifikat bruges. Branchen arbejder aktivt på at udfase 1024-bit-rodcertifikater i løbet af i år.

- Sikre forbindelser, der afhænger af, at vores certifikatkæde signeres af G2-rodcertifikatet, understøttes ikke:

Organisationsenhed	Class 3 Public Primary Certification Authority – **G2**
Serienummer	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

- Sikre forbindelser, der afhænger af, at vores certifikatkæde signeres af G5-rodcertifikatet, understøttes:

Navn	VeriSign Class 3 Public Primary Certification Authority – **G5**
Serienummer	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

Følg disse retningslinjer for at sikre dig, at du bruger en sikker forbindelse via et understøttet VeriSign G5-rodcertifikat:

1. **Kontroller dit certifikatlager.** Bed din webudbyder eller systemadministrator om at bekræfte, at VeriSign G5-rodcertifikatet findes i det rodlager, som bruges af din kode til valideringslogik. Hvis det er tilfældet, behøver du ikke foretage dig mere.
    - Klik på følgende links for at kontrollere, at dit nøglelager indeholder G5-rodcertifikatet, som bruger Java, Linux eller Windows.
2. **Kontroller dine fejllogfiler.** Hvis VeriSign G5-rodcertifikatet ikke er blevet downloadet for at erstatte G2-rodcertifikatet, kan du få vist fejlmeddelelser i stil med disse:
    - Fejl i SSL-handshake: "Der blev ikke fundet noget certifikat, der er tillid til".
    - Resultatkode -31: "Certifikatkæden kunne ikke valideres. Der blev ikke fundet noget lokalt certifikat".
    - Resultatkode -8: "SSL-forbindelsen mislykkedes"
    - -1-fejl

    Du kan løse disse fejl på en af følgende måder:
    - Opdater din software til den seneste version, der understøtter SHA-256.
    - Hvis et nøglelager bruges til validering/godkendelse af certifikat, skal du installere VeriSign G5-rodcertifikatet i dit nøglelager.
3. **Hent et VeriSign G5-rodcertifikat.** Hvis dit certifikatlager eller din Java-klient ikke indeholder VeriSign G5-rodcertifikatet, skal du bede din systemadministrator om at downloade det fra VeriSign og gemme det i certifikatlageret sammen med eventuelle andre godkendelsespakker til SSL-forbindelser.
    - Download Symantecs VeriSign G5-rodcertifikat.
    - Download bestemte SSL-certifikater til din server, hvis den kræver dette.

2. Opdater til SHA-256-signeringsalgoritmen.

Problemet: SHA-1 er en 22 år gammel kryptografisk algoritme, som ikke kan følge med udviklingen inden for it. SHA-256 bruger en stærkere algoritme med 256-bit-hash-værdier.

Vores løsning: Vi opgraderer SSL-certifikaterne på alle Live- og Sandbox-slutpunkter fra SHA-1 til den stærkere og mere robuste SHA-256.

Din opgave

Følg disse retningslinjer for at udskifte SSL-certifikater med SHA-1-signeringsalgoritmen til den stærkere SHA-256-signeringsalgoritme:

1. **Kontroller dit miljø.** Du skal sikre dig, at dit miljø understøtter SHA-256-certifikater.
   - Du kan se en liste over understøttet hardware og software i DigiCerts SHA-2-kompatibilitetsguide og på Symantecs liste over understøttede browsere og servere.
   - Hvis dele af dit miljø ikke understøtter SHA-256, skal du udskifte eller opgradere disse dele, før du kan implementere de nye certifikater.
   - Windows 2000 Server og visse versioner af Windows XP er muligvis ikke kompatible med SHA-2. På denne Windows PKI-blog om SHA-2 og Windows kan du finde løsninger og anbefalinger til opgradering af dit miljø.
2. **Kontroller dine certifikater.** Hvis dit miljø understøtter SHA-256, skal du sikre dig, at du har VeriSign G5-rodcertifikatet i dit nøglelager.

Har du spørgsmål?

Du kan få flere oplysninger og læse ofte stillede spørgsmål på vores 2015-2016 SSL Certificate Change Microsite.

Tak

Vi sætter pris på din hurtige håndtering af dette problem og for din forståelse. Vi er klar over, at opgraderingen kan give kompatibilitetsproblemer. Det er dog vigtigt at bemærke, at ulemperne på kort sigt opvejes af, at kundernes konti og betalingsoplysninger er sikre.