Handlarsäkerhet

Handledning till systemuppgradering

Klicka HÄR för information om hur du uppfyller SHA-256.

Säkra din integrering för framtiden

Säkerhetshoten förnyas ständigt och säkerheten för våra handlare har som alltid högsta prioritet. Som skydd mot nuvarande och framtida hot ber vi våra handlare att göra följande uppgraderingar i sina integreringar:

1. Sluta använda VeriSign G2-rotcertifikat
2. Uppdatera din integrering så att den stödjer certifikat med SHA-256-algoritmen

Varför ska vi byta?

Offentliga certifikatutfärdare fortsätter att förbättra säkerheten i SSL-certifikat. På grund av förberedande ändringar för användning av SHA-256-signeringsalgoritmen under 2016 kommer det inte längre att finnas stöd för VeriSign G2-rotcertifikat som tidigare använts för att ansluta till PayPal API och Avisering om direktbetalning (IPN).

När behöver jag göra ändringen?

Vi rekommenderar att du vidtar åtgärder så snart som möjligt för att förbereda dig inför dessa ändringar. På mikrowebbplatsen för byte av SSL-certifikat under 2015–2016 finns en detaljerad tidsplan med datum för uppgraderingar av API-slutpunkter för Live och Sandbox.

NOTE: Ändringarna görs för att åtgärda säkerhetsproblem som finns i hela branschen. De är inte unika för PayPal. När de genomförts kommer de att förbättra sekretessen och tillförlitligheten i dina PayPal-integreringar. Eftersom förändringarna ser lite olika ut beroende på system rekommenderar vi att de görs av en kvalificerad systemadministratör.

1. Sluta använda VeriSigns G2-rotcertifikat

Problemet: Tidigare utfärdade VeriSign SSL-certifikat med en certifikatkedja som signeras av ett 1024-bitars G2-rotcertifikat. På senare år har amerikanska regeringen och den offentliga CA-industrin bytt till säkrare 2048-bitars certifikat. Nu använder VeriSign därför SSL-certifikat med en certifikatkedja som signeras av ett 2048-bitars G5-rotcertifikat, från 2006.

Vår åtgärd: I enlighet med branschstandarderna kommer PayPal inte längre att godkänna säkra anslutningar till API/IPN-slutpunkter som behöver en certifikatkedja som signeras av G2-rotcertifikat. Vi kommer bara godkänna anslutningar som använder certifikatkedjor som signeras av G5-rotcertifikat.

Att göra

Avbryt användning av SSL-anslutningar som använder VeriSign-rotcertifikatet med en G2-identifierare, om du för tillfället använder det till ditt system. Branschen arbetar aktivt för att avveckla användningen av 1024-bitars rotcertifikat under det här året.

- Säkra anslutningar som är beroende av att vår certifikatskedja signeras av ett G2-rotcertifikat kommer inte att stödjas:

Organisationsenhet	Offentlig primär certifikatutfärdare i klass 3 – **G2**
Serienummer	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Certifikat med SHA1-fingeravtryck	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Säkra anslutningar som använder en certifikatskedja som signeras av ett G5-rotcertifikat stöds:

Generisk benämning	VeriSign – offentig primär certifikatutfärdare i klass 3 – **G5**
Serienummer	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Certifikat med SHA1-fingeravtryck	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Följ de här anvisningarna och kontrollera att du har en säker anslutning som stödjer VeriSign G5-rotcertifikat:

1. **Kontrollera ditt certifikatarkiv.** Be att din webbplatsvärd eller systemadministratör kontrollerar om VeriSign G5-rotcertifikatet finns i rotarkivet som din verifieringskod använder. Om det finns där krävs ingen åtgärd.
    - Använd följande länkar och kontrollera om din KeyStore innehåller G5-rotcertifikat som använder Java, Linux eller Windows.
2. **Kontrollera dina felloggar.** Om VeriSign G5-rotcertifikat inte har hämtats för att ersätta G2-rotcertifikatet visas ett felmeddelanden som ungefär lyder så här:
    - SSL-handskakningsfel: Inga tillförlitliga certifikat hittades.
    - Resultatkod -31: Certifikatskedjan verifierades inte. Inget lokalt certifikat hittades.
    - Resultatkod -8: SSL-anslutning misslyckades.
    - -1 fel

    Om du vill lösa de här problemen gör du något av följande:

    - Uppdatera din programvara till senaste versionen med stöd för SHA-256.
    - Om en KeyStore används för att verifiera certifikat ska VeriSign G5-rotcertifikatet installeras i din KeyStore.
3. **Hämta ett VeriSign G5-rotcertifikat.** Om ditt certifikatarkiv eller din Java-klient inte innehåller VeriSign G5-rotcertifikatet ber du att din systemadministratör hämtar det från VeriSign och sparar det i certifikatarkivet tillsammans med alla andra autentiseringspaket till SSL-anslutningar.
    - Hämta Symantecs VeriSign G5-rotcertifikat
    - Hämta serverspecifika SSL-certifikat om servern kräver det

2. Uppdatera till en signeringsalgoritm som använder SHA-256

Problemet: SHA-1 är en 22 år gammal kryptografisk algoritm som inte är anpassad för ökad datorkraft. SHA-256 använder en starkare algoritm med 256-bitars hashvärden.

Vår åtgärd: PayPal uppgraderar SSL-certifikat på alla slutpunkter för Live och Sandbox från SHA-1 till det starkare och kraftigare SHA-256, under mitten av 2016.

Att göra

Följ anvisningarna och övergå från SSL-certifikat som använder SHA-1-signeringsalgoritmen till den starkare SHA-256-signeringsalgoritmen:

1. **Kontrollera din miljö.** Se till att din miljö stöder SHA-256-certifikat.
   - I DigiCert's SHA-2 Compatibility Guide (kompatibilitetshandledning för DigiCert SHA-2) och Symantec's Supported Browser and Server List (lista över webbläsare och servrar som stöds av Symantec) finns information om vilken maskinvara och programvara som stöds.
   - Om delar av din miljö inte stödjer SHA-256 måste du ersätta eller uppgradera de olika delarna innan du kan börja använda de nya certifikaten.
   - Windows 2000 Server och vissa versioner av Windows XP kanske inte är kompatibla med SHA-2. Den här bloggen om Windows PKI med SHA-2 kan bidra med korrigeringsfiler och rekommendationer för att uppgradera din miljö.
2. **Kontrollera dina certifikat.** Om din miljö stöder SHA-256 kontrollerar du att du har VeriSign G5-rotcertifikatet i din KeyStore.

Har du några frågor?

På mikrowebbplatsen för byte av SSL-certifikat under 2015–2016 finns mer information och vanliga frågor och svar.

Tack

Tack för att du tar tag i problemet så snabbt och för att du har förståelse för vår strategi. Vi förstår att de här åtgärderna kan innebära kompatibilitetsproblem men de är övergående och vägs upp av fördelarna med att vi fortsätter att skydda våra kunders konton och betalningsuppgifter på bästa sätt.