HMAC-Authentisierung (Notify)

Hash MAC-Authentisierung im Notify

Der Shop muss überprüfen, ob eine Benachrichtigungsanfrage wirklich von Computop Paygate stammt. Anderenfalls kann ein Angreifer eine Transaktion initialisieren und dann diese Benachrichtigung fälschen. Ein Shop-Betreiber wird nicht manuell prüfen, ob in jedem Fall eine entsprechende Transaktion durchgeführt wurde. Deshalb muss das Modul dies automatisch machen.

Derzeit ist die Benachrichtigungsanfrage nur verschlüsselt. Diese Verschlüsselung garantiert jedoch nicht die Authentizität einer Nachricht. Sie garantiert nur, dass eine Nachricht nicht mitgehört werden kann. Daher ist diese Sicherheitsmaßnahme unzureichend.

Deshalb wird der Antwortparameter MAC verwendet, der mit demselben Algorithmus wie der MAC in der Anfrage gebildet wird. Nur die Datenparameter unterscheiden sich.

Für die Hash-Generierung gilt hier folgendes Datenmuster: `PayID*TransID*MerchantID*Status*Code`

Der Parameter MAC wird nur an URLSuccess oder URLFailure sowie für URLNotify zurückgegeben.

Ihre Integration muss prüfen, ob die erhaltene Antwort authentisch ist.

Folgende Tabelle beschreibt, wie Sie die Hash-Werte erzeugen, um die erhaltene Antwort vom Computop Paygate zu validieren:

<table>
<tr><th>Schritt</th><th>Aufgabe</th></tr>
<tr><td>1</td><td>Melden Sie sie bitte beim Computop Helpdesk an, der Ihnen das Hash-Kennwort mitteilt.</td></tr>
<tr><td>2</td><td>Der HMAC-Wert wird mit Hilfe des Kennworts und mehrerer Parameterwerte berechnet. Zur Berechnung werden die Parameter PayID, TransID, MerchantID, Status und Code verwendet und mit Sternchen getrennt:

<code>PayID*TransID*MerchantID*Status*Code</code>

<table>
<tr><th>Key</th><th>Wert</th><th>Anmerkungen</th></tr>
<tr><td>PayID</td><td>Referenzierte PayID</td><td>Zurückgegebene PayID von Computop Paygate</td></tr>
<tr><td>TransID</td><td>Ihre Transaktions-ID zur Referenzierung / Identifikation Ihrer Anfrage</td><td>Ihre eigene Referenz zur Identifikation jeder Anfrage / jedes Zahlungsvorgangs.</td></tr>
<tr><td>Merchant ID</td><td>Ihre von Computop vergebene MerchantID</td><td>Ihre MerchantID zur Identifikation dieser Anfrage. Bitte verwenden Sie den Wert des Parameters MID aus der Benachrichtigungsanfrage von Computop Paygate.</td></tr>
<tr><td>Status</td><td>Status in der Antwort</td><td>Status der Antwort, z.B. AUTHORIZED, FAILED, OK, ...</td></tr>
<tr><td>Code</td><td>Code in der Antwort</td><td>Code der Antwort, z.B. 00000000, 22720040, ...</td></tr>
<tr><td>YourHmacPassword</td><td>Ihr von Computop zugeteiltes HMAC-Kennwort</td><td>Ihr zu einer bestimmten MID zugeordnetes HMAC-Kennwort; falls Sie mehrere MIDs haben, haben Sie auch verschiedene HMAC-Kennwörter.</td></tr>
</table>

<table>
<tr><th>Beispiele zur MAC-Berechnung</th><th>Formel</th><th>Ergebnis</th></tr>
<tr><td>Autorisierte Zahlung</td><td><code>HmacSHA256("7bbb448155234d8cbee323778952ce28*TID-1203317532127017023 2*YourMerchantID*AUTHORIZED*00000000", "mySecret")</code></td><td>F1DE7608013C1E3FD3CC9964A049E26703137C0A6F29448545C700B4695EABE5</td></tr>
<tr><td>Gescheiterte Zahlung</td><td><code>HmacSHA256("7bbb448155234d8cbee323778952ce28*TID-1203317532127017023 2*YourMerchantID*FAILED*22720040", "mySecret")</code></td><td>1D9A8AAA306316359B8192070237670950DB77073F9F34ED7EB483D9B59DE1DD</td></tr>
</table>
</td></tr>
<tr><td>3</td><td>Verwenden Sie den HMAC SHA-256-Algorithmus, den fast alle Programmiersprachen unterstützen, um den Hash-Wert mit dem Kennwort und den Parameterwerten zu berechnen.</td></tr>
<tr><td>4</td><td>Überprüfen Sie

• den erhaltenen HMAC-Wert aus der Antwort vom Computop Paygate
• dessen Übereinstimmung mit dem selbst berechneten MAC-Wert

um sicherzustellen, dass die erhaltene Nachricht authentisch ist.</td></tr>
</table>

Ihre Implementierung prüfen

Eine einfache Anwendung zur Überprüfung der Umsetzung Ihrer HMAC-Berechnung finden Sie hier: https://computop.com/paygate-test

Mit der Anwendung können Sie mit unserer Paygate API spielen – verwenden Sie einfach Ihre MerchantID und Ihr Blowfish-Kennwort, die Sie bereits erhalten haben.

Der Parameter MAC wird nur an die URLSuccess oder URLFailure und für Notifys zurückgegeben.

Wichtig: Der Shop muss überprüfen, ob eine Benachrichtigungsanfrage wirklich von Computop Paygate stammt. Dazu muss aus den übermittelten Werten für PayID, TransID, MerchantID, Status und Code mit Ihrem HMAC-Passwort ein HMAC-Wert errechnet und dieser mit dem MAC-Wert der Anfrage verglichen werden. Sind die Werte nicht identisch, so darf die Benachrichtigungsanfrage nicht verarbeitet werden.

Wichtig: Zur Berechnung wird dieses Mal die von Computop Paygate in der Benachrichtigungsanfrage übermittelte MID verwendet.

Wichtig: Kennwörter dürfen **niemals** per E-Mail versendet werden, weil in diesem Fall **sofort** die Sicherheit verschlüsselter Anfragen /Antworten nicht mehr gewährleistet ist. Falls versehentlich Kennwörter per E-Mail versendet wurden, müssen neue Kennwörter auf Kosten des Händlers oder bei der nächsten Standardfreigabe hinterlegt werden. Computop **weist ausdrücklich auf das Risiko** der weiteren Verwendung **solcher kompromittierter MIDs hin**. Falls ein Händler eine solche kompromittierte MID dennoch weiter verwendet, trägt er selbst das Haftungsrisiko für mögliche Verluste durch die kompromittierten Kennwörter.