HMAC Authentication (Notify)

Hash HMAC-Authentication in Notify

The shop must verify that a notification request really comes from . Otherwise an attacker can initialise a transaction and then falsify this notification. A shop operator will not manually check whether a corresponding transaction was performed in each case. Therefore, the module must do this automatically.

Currently, the notification request is only encrypted. However, this encryption does not guarantee the authenticity of a message. It only guarantees that a message cannot be listened in on. Therefore, this safety measure is insufficient.

As a result, the response parameter MAC is used, which is formed via the same algorithm as the MAC in request. Only the data parameters differ.

The following data pattern applies here for hash generation: `PayID*TransID*MerchantID*Status*Code`

The MAC parameter is only returned to the URLSuccess or URLFailure and for URLNotify.

Your integration must check whether the response received is authentic.

The following table describes how you can generate the Hash values to validate response that you received:

<table>
<tr><th>Step</th><th>Task</th></tr>
<tr><td>1</td><td>Please log on to , which supplies you with the Hash password.</td></tr>
<tr><td>2</td><td>The HMAC value is calculated with the aid of the password and several parameter values. For the calculation, the parameters PayID, TransID, MerchantID, Status and Code are used and separated with asterisks:

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

<table>
<tr><th>Key</th><th>Value</th><th>Comments</th></tr>
<tr><td>PayID</td><td>Referenced PayID</td><td>PayID returned by</td></tr>
<tr><td>TransID</td><td>Your transactionId to reference / identify your request</td><td>Your own reference to identify each request / payment process.</td></tr>
<tr><td>MerchantID</td><td>Your MerchantID assigned to you by</td><td>Your MerchantID identifiying this request. Please use the value of parameters MID from notification request.</td></tr>
<tr><td>Status</td><td>Status in response</td><td>Status of response, e.g. AUTHORIZED, FAILED, OK, ...</td></tr>
<tr><td>Code</td><td>Code in response</td><td>Code of response, e.g. 00000000, 22720040, ...</td></tr>
<tr><td>YourHmacPasswort</td><td>Your HMAC-password assigned to you by</td><td>Your HMAC-password assigned to a specific MID; if you have different MIDs you will have different HMAC passwords, too.</td></tr>
</table>

<table>
<tr><th>Samples for MAC calculation</th><th>Formula</th><th>Result</th></tr>
<tr><td>Authorized payment</td><td><code>HmacSHA256("7bbb448155234d8cbee323778952ce28*TID-12033175321270170232*YourMerchantID*AUTHORIZED*00000000", "mySecret")</code></td><td>F1DE7608013C1E3FD3CC9964A049E26703137C0A6F29448545C700B4695EABE5</td></tr>
<tr><td>Failed payment</td><td><code>HmacSHA256("7bbb448155234d8cbee323778952ce28*TID-12033175321270170232*YourMerchantID*FAILED*22720040", "mySecret")</code></td><td>1D9A8AAA306316359B8192070237670950DB77073F9F34ED7EB483D9B59DE1DD</td></tr>
</table>
</td></tr>
<tr><td>3</td><td>Use the HMAC SHA-256 algorithm, which nearly all programming languages support, in order to calculate the Hash value with the password and the parameter values.</td></tr>
<tr><td>4</td><td>Verify

• the MAC-value from response that you received
• with the MAC value that you calculated yourself

to ensure that the message you have received is authentic.</td></tr>
</table>

The MAC parameter is only returned to the URLSuccess or URLFailure and for Notifys.

Important: Your system has to ensure that a notification request has really be sent by . Therefore the received values for PayID, TransID, MerchantID, Status and Code have to be hashed using your HMAC-password and this HMAC-value must be identical with MAC-value from request. If these values do not match the request must not be processed.

Important: To calculate HMAC-value please use the value of parameter MID which has be sent by .

Important: Password (like HMAC-password) must never be sent via email, because email is not a secure way of data transmission. If passwords are sent or forwarded via email new passwords need to be established at the expense of the merchant or will be changed with next release of MerchantID-changes. **The page DE:Wording was not found** -- Please check/update the page name used in the MultiExcerpt-Include macro expressly points out the risk of further use of such compromised MIDs. If a merchant continues to use such a compromised MID, he himself bears the liability risk for possible losses caused by the compromised passwords.