

HMAC Authentication (Request)

Hash MAC-Authentication in Request

To protect against unauthorised manipulation of your payment transactions, the checks with the aid of a Hash Message Authentication Code (HMAC) whether your payment enquiry is authentic and has not been manipulated. For this purpose you transfer an HMAC value to the with each transaction in the parameter MAC.

Background: Unlike the HMAC procedure every encoding method has the disadvantage that there is a matching decoding method. Anyone who possesses the correct key or cracks the encryption can read and manipulate the data. Therefore, no encryption method is ever 100% safe. In the case of the Hash procedure, conversely, decoding is impossible, so that a Hash value can confirm the authenticity of the message free of doubt.

The uses a Hash Message Authentication Code (HMAC) to check the authenticity of your payments. The HMAC SHA-256 algorithm is used with a 32-digit key length (256 bits) for this. The additional password makes the HMAC procedure particularly safe.

The following table describes how you can generate the Hash values for your payment:

Step	Task																																	
1	Please log on to , which supplies you with the Hash password.																																	
2	<p>The HMAC value is calculated with the aid of the password and several parameter values. For the calculation, the parameters PayID, TransID, MerchantID, Amount and Currency are used and separated with asterisks:</p> <p>PayID*TransID*MerchantID*Amount*Currency</p> <table><tr><th>Key</th><th>Value</th><th>Comments</th></tr><tr><td>PayId</td><td>Referenced PayId</td><td>May be empty, e.g. for creating an initial payment process or risk management request; is used with subsequent requests like capture/refund.</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 identifying this request.</td></tr><tr><td>Amount</td><td>Amount in smallest unit of currency, e. g. 123=1,23</td><td>Amount of this request; may be empty if not used, e.g. for status inquiries.</td></tr><tr><td>Currency</td><td>Currency of payment process in ISO 4217, e.g. EUR, USD, GBP</td><td>Currency of this request; may be empty if not used, e.g. for status inquiries.</td></tr><tr><td>YourHmac Password</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> <p><u>Notice:</u> If a transaction does not support all of these parameters, you can simply omit the missing value.</p> <p>For example, there is no PayID yet with the first transaction, so you do not have to transfer this. The PayID is a component of the Hash calculation in subsequent transactions:</p> <table><tr><th>Samples for MAC calculation</th><th>Formula</th><th>Result</th></tr><tr><td>without PayId, with amount/currency</td><td>HmacSHA256(" *TID-4453732122167114558*YourMerchantID*1234*EUR" , "mySecret")</td><td>0522F1AF6A88597D396A5A877499F3C9087EBCF103B1B47D7E4D13421CC7EA36</td></tr><tr><td>without PayId, without TransId, with amount /currency</td><td>HmacSHA256(" **YourMerchantID*1234*EUR" , "mySecret")</td><td>1427748D983478080F22BE0878BD99AF7BE3E1C4B19C07AFD1B372BA552ADC08</td></tr><tr><td>with PayId, without amount/currency</td><td>HmacSHA256(" fe3f002e19814eea8aa733ec4fdacafe*TID-4453732122167114558*YourMerchantID**" , "mySecret")</td><td>6ED0CFDCE92CE13399552C4221B44E5B036DE943D7F84E33D1E73DF9871AE7C8</td></tr></table>	Key	Value	Comments	PayId	Referenced PayId	May be empty, e.g. for creating an initial payment process or risk management request; is used with subsequent requests like capture/refund.	TransId	Your transactionId to reference / identify your request	Your own reference to identify each request / payment process.	MerchantID	Your MerchantID assigned to you by	Your MerchantID identifying this request.	Amount	Amount in smallest unit of currency, e. g. 123=1,23	Amount of this request; may be empty if not used, e.g. for status inquiries.	Currency	Currency of payment process in ISO 4217, e.g. EUR, USD, GBP	Currency of this request; may be empty if not used, e.g. for status inquiries.	YourHmac Password	Your HMAC-password assigned to you by	Your HMAC-password assigned to a specific MID; if you have different MIDs you will have different HMAC passwords, too.	Samples for MAC calculation	Formula	Result	without PayId, with amount/currency	HmacSHA256(" *TID-4453732122167114558*YourMerchantID*1234*EUR" , "mySecret")	0522F1AF6A88597D396A5A877499F3C9087EBCF103B1B47D7E4D13421CC7EA36	without PayId, without TransId, with amount /currency	HmacSHA256(" **YourMerchantID*1234*EUR" , "mySecret")	1427748D983478080F22BE0878BD99AF7BE3E1C4B19C07AFD1B372BA552ADC08	with PayId, without amount/currency	HmacSHA256(" fe3f002e19814eea8aa733ec4fdacafe*TID-4453732122167114558*YourMerchantID**" , "mySecret")	6ED0CFDCE92CE13399552C4221B44E5B036DE943D7F84E33D1E73DF9871AE7C8
Key	Value	Comments																																
PayId	Referenced PayId	May be empty, e.g. for creating an initial payment process or risk management request; is used with subsequent requests like capture/refund.																																
TransId	Your transactionId to reference / identify your request	Your own reference to identify each request / payment process.																																
MerchantID	Your MerchantID assigned to you by	Your MerchantID identifying this request.																																
Amount	Amount in smallest unit of currency, e. g. 123=1,23	Amount of this request; may be empty if not used, e.g. for status inquiries.																																
Currency	Currency of payment process in ISO 4217, e.g. EUR, USD, GBP	Currency of this request; may be empty if not used, e.g. for status inquiries.																																
YourHmac Password	Your HMAC-password assigned to you by	Your HMAC-password assigned to a specific MID; if you have different MIDs you will have different HMAC passwords, too.																																
Samples for MAC calculation	Formula	Result																																
without PayId, with amount/currency	HmacSHA256(" *TID-4453732122167114558*YourMerchantID*1234*EUR" , "mySecret")	0522F1AF6A88597D396A5A877499F3C9087EBCF103B1B47D7E4D13421CC7EA36																																
without PayId, without TransId, with amount /currency	HmacSHA256(" **YourMerchantID*1234*EUR" , "mySecret")	1427748D983478080F22BE0878BD99AF7BE3E1C4B19C07AFD1B372BA552ADC08																																
with PayId, without amount/currency	HmacSHA256(" fe3f002e19814eea8aa733ec4fdacafe*TID-4453732122167114558*YourMerchantID**" , "mySecret")	6ED0CFDCE92CE13399552C4221B44E5B036DE943D7F84E33D1E73DF9871AE7C8																																
3	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.																																	
4	Use the MAC parameter to transfer the hexadecimal encoded Hash value to the with each transaction in the encoded data field.																																	



Notice: Note that the MAC parameter is obligatory for all subsequent transactions (e.g. capture, credit note) if it was transferred with the first transaction (e.g. authorisation).



Important: The rejects transactions with wrong or missing HMAC values promptly without further processing, because this is an indication of hacker attacks. Therefore, transactions which the rejects with the error codes 20100044 or 20120044 do not appear in .



Important: The MerchantID used in HMAC calculation must be identical with the MerchantID provided in plain request (parameter MerchantID). Handling of "MerchantID" is case-sensitive - "YourMerchantId" and "YourMerchantID" must not be mixed up.

Listing with HMAC examples

Request without PayID:

MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=<https://www.shop.de/ok.html>&URLFailure=<https://www.shop.de/failed.html>&OrderDesc=My purchase

String for MAC generation:

*100000001*YourMerchantID*11*EUR

Request with MAC (Secret: "mySecret"):

MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=<https://www.shop.de/ok.html>&URLFailure=<https://www.shop.de/failed.html>&OrderDesc=My purchase&MAC=0A125E070BD4D7AE614BCB2D5A48FB80E1C4441E262A1024AE7F2A1819052A6F

Request without TransID:

MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD

String for MAC generation:

8ee4e922c39446ac9ee66095a4a4b475**YourMerchantID*100*USD

Request with MAC (Secret: "mySecret"):

MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD&MAC=4016FD6C705399A024D8B4CCB0018814E05A5490DDEBEC04909E6DA138CB5AF8