How is HMAC-SHA256 calculated?

- The SHA-256 HMAC calculation includes all NON-EMPTY fields.
- All transaction fields are concatenated in alphabetical order of the ASCII value of each field string, with '&' after every field except the last.
- Integrity Salt/Hash Key/Hash is appended to the concatenated string.

Consider the following example:

Consider the following payment parameters and their respective values and assuming the Integrity Salt/Hash Key/Hash as "**3vv9wu3a18**":

Sorted Hash Array
{
pp_Amount: "25000"
pp_MerchantID: "MC25041"
pp_MerchantMPIN: "1234"
pp_Password: "sz1v4agvyf"
pp_TxnCurrency: "PKR"
pp_TxnRefNo: "T20220518150213"
}

In ascending alphabetical order and separating each value with '&', the transaction request fields would be:
25000&MC25041&1234&sz1v4agvyf&PKR&T20220518150213

After prepending the Integrity Salt/Hash Key to the message, the transaction request fields would be:
3vv9wu3a18&25000&MC25041&1234&sz1v4agvyf&PKR&T20220518150213

Now calculating the hash with the hashing scheme 'HMAC-SHA256' with the secret key: **3vv9wu3a18**

Resultant hash:
[2C595361C2DA0E502D18BFBAA92CF4740330215E5E8AD0CF4489A64E7400B117]