Hash Signature Check

1. Introduction:

The goal of this document is to describe the Ezugi hash signature check.

2. Description

An operator will receive on all requests coming from Ezugi a hash signature signed by a secret key that will be issued by Ezugi specifically for the operator. The hash signature will be created by using SHA256 hash algorithm and will create a signature by using a secret key and the request that is sent to the operator. An output format is base64 encoding. The operator should compare the received hash signature with his own signature that will be create by using the secret key and the received request (the signature should be removed from the received request before calculating the signature on the operator's end).

3. Usage example

Below are examples of requests including hash value

Authentication

HTTP Header:

“hash”: “zEZQLOfOkh0cjNZ3/k5cqzVi6BON0bUOXXfmm8Ka9OE=”

Message:

{"platformId":1,"operatorId":13000000,"token":"71d0bd9422353d06cae6af7c41c069e1","timestamp":1506859096084}

Debit

HTTP Header:

“hash”: “qwFZJFbKi5SHI3n6jMLQxW5mT79aIZmfgfv4khYQKWw=”

Message:

{"gameId":1,"debitAmount":10.0,"platformId":9,"serverId":102,"transactionId":"2cf4ea03-be49-4f6c-b27d-9ee442d02d9d","token":"894dfcad8db8045c5fe72e868bd8bac3","uid":"137871","betTypeID":1,"seatId":"s1","currency":"USD","operatorId":13000000,"roundId":15265792,"timestamp":1506859145170

Credit

HTTP Header:

“hash”: “OUD7WRCMMA9DxuevM7jDW58Zx/iKZZbno/26d1mgnCY=”

Message:

{"gameId":1,"gameDataString":"{\"TableId\":\"1\",\"PlayerId\":\"13000000|137871|1\",\"CardInShoe\":105,\"DealerCardHandValue\":\"10\\\/20\",\"BetTypeId\":101,\"BetAmount\":10.0,\"InsuranceDecision\":\"Cancel\",\"SessionCurrency\":\"USD\",\"PlayerCards\":[{\"CardName\":\"Qh\",\"CardValue\":10},{\"CardName\":\"Tc\",\"CardValue\":10}],\"TakenSeatsNumber\":1,\"OperatorID\":\"13000000\",\"DealerCards\":[{\"CardName\":\"Ah\",\"CardValue\":11},{\"CardName\":\"9d\",\"CardValue\":9}],\"PlayerCardHandValue\":\"20\",\"BetsList\":[{\"BetName\":\"RegularBet\",\"BetAmount\":10.0}],\"ServerId\":102,\"Version\":\"1.2\",\"DealerId\":\"20\",\"GameResults\":\"Push\",\"roundId\":15265792,\"WinAmount\":10.0,\"WinningBets\":{\"RegularBet\":10.0},\"GameID\":1,\"SeatId\":\"s1\"}","isEndRound":true,"creditIndex":"1|1","platformId":9,"serverId":102,"transactionId":"055df923-5d5f-4e32-bdc5-b2f3931891f0","token":"894dfcad8db8045c5fe72e868bd8bac3","uid":"137871","returnReason":0,"betTypeID":101,"seatId":"s1","currency":"USD","creditAmount":10.0,"operatorId":13000000,"roundId":15265792,"timestamp":1506859183109}

Rollback

HTTP Header:

"hash": "YGPCrMVmx+kMrAdHs3TY6OK3gbFLydVITPNGDt9ASnI='

Message:

{"gameId":1,"uid":"137871","rollbackAmount":10.0,"currency":"USD","seatId":"s1","platformId":9,"serverId":102,"operatorId":13000000,"roundId":15265844,"transactionId":"708896b8-209a-4360-b7b1-7cfa5c33726f","token":"894dfcad8db8045c5fe72e868bd8bac3","timestamp":1506859334043}

4. Creating base64 Hash Using HMAC SHA256

4.1 Implementation methods for different languages

Java

```
public static String encode(String key, String data) throws Exception {
  Mac sha256_HMAC = Mac.getInstance("HmacSHA256");
  SecretKeySpec secret_key = new SecretKeySpec(key.getBytes(),
"HmacSHA256");
  sha256_HMAC.init(secret_key);
  return
Base64.encodeBase64String(sha256_HMAC.doFinal(data.getBytes()));
}
```

PHP

Use the standard function hash_mac

```
$s = hash_hmac('sha256', 'Message', 'secret', true);
echo base64_encode($s);
```

JavaScript

Use the CryptoJS library.

```
var hash = CryptoJS.HmacSHA256("Message", "secret");
var hashInBase64 = CryptoJS.enc.Base64.stringify(hash);
```

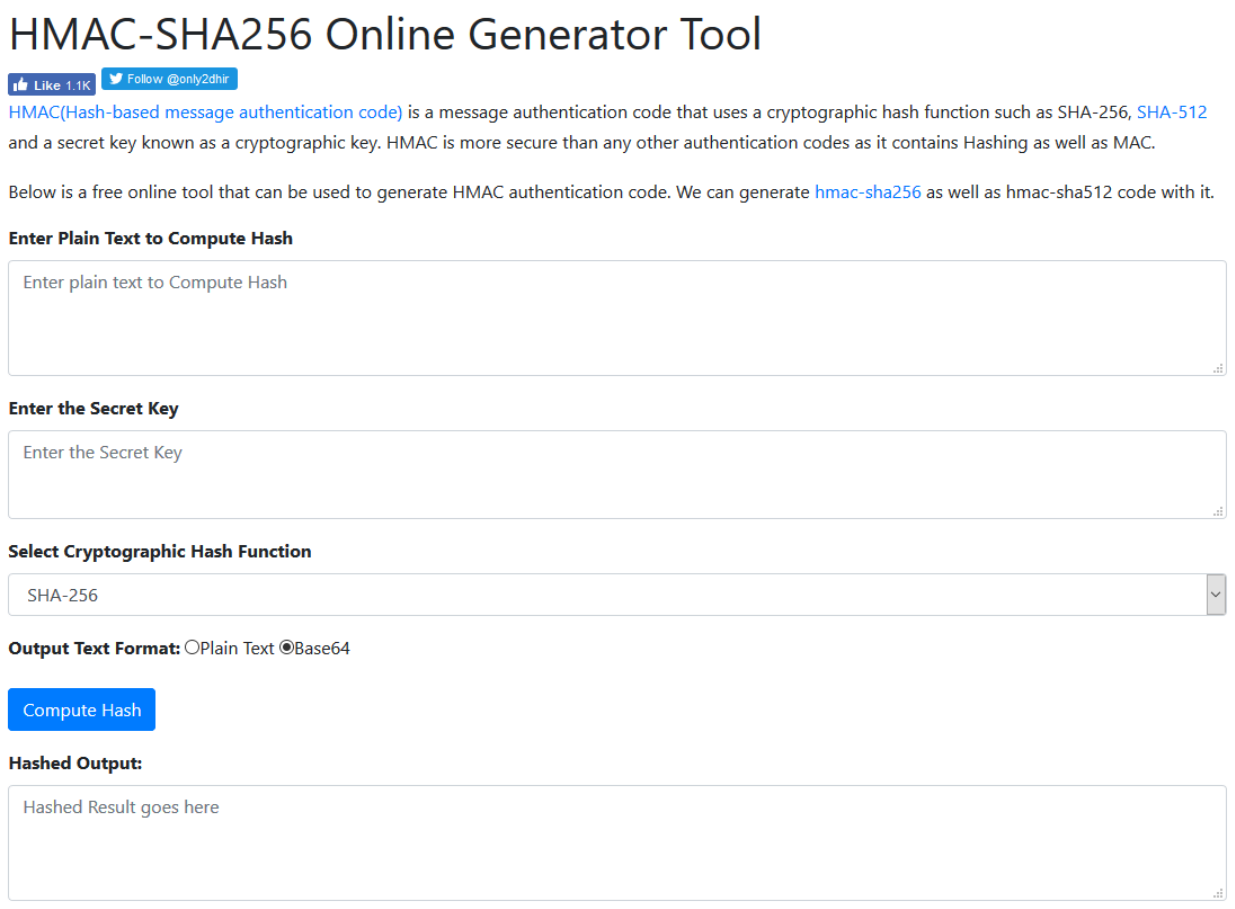
Other

Information about other languages you may find by clicking here.

4.2 External Hashing Tool

We are using SHA-256 algorithm with Base 64 Encoding for output. Below is the tool, which can help you to create manually hash signature.

1. Enter devglan.com/online-tools/hmac-sha256-online



HMAC-SHA256 Online Generator Tool

HMAC(Hash-based message authentication code) is a message authentication code that uses a cryptographic hash function such as SHA-256, SHA-512 and a secret key known as a cryptographic key. HMAC is more secure than any other authentication codes as it contains Hashing as well as MAC.

Below is a free online tool that can be used to generate HMAC authentication code. We can generate hmac-sha256 as well as hmac-sha512 code with it.

Enter Plain Text to Compute Hash

Enter plain text to Compute Hash

Enter the Secret Key

Enter the Secret Key

Select Cryptographic Hash Function

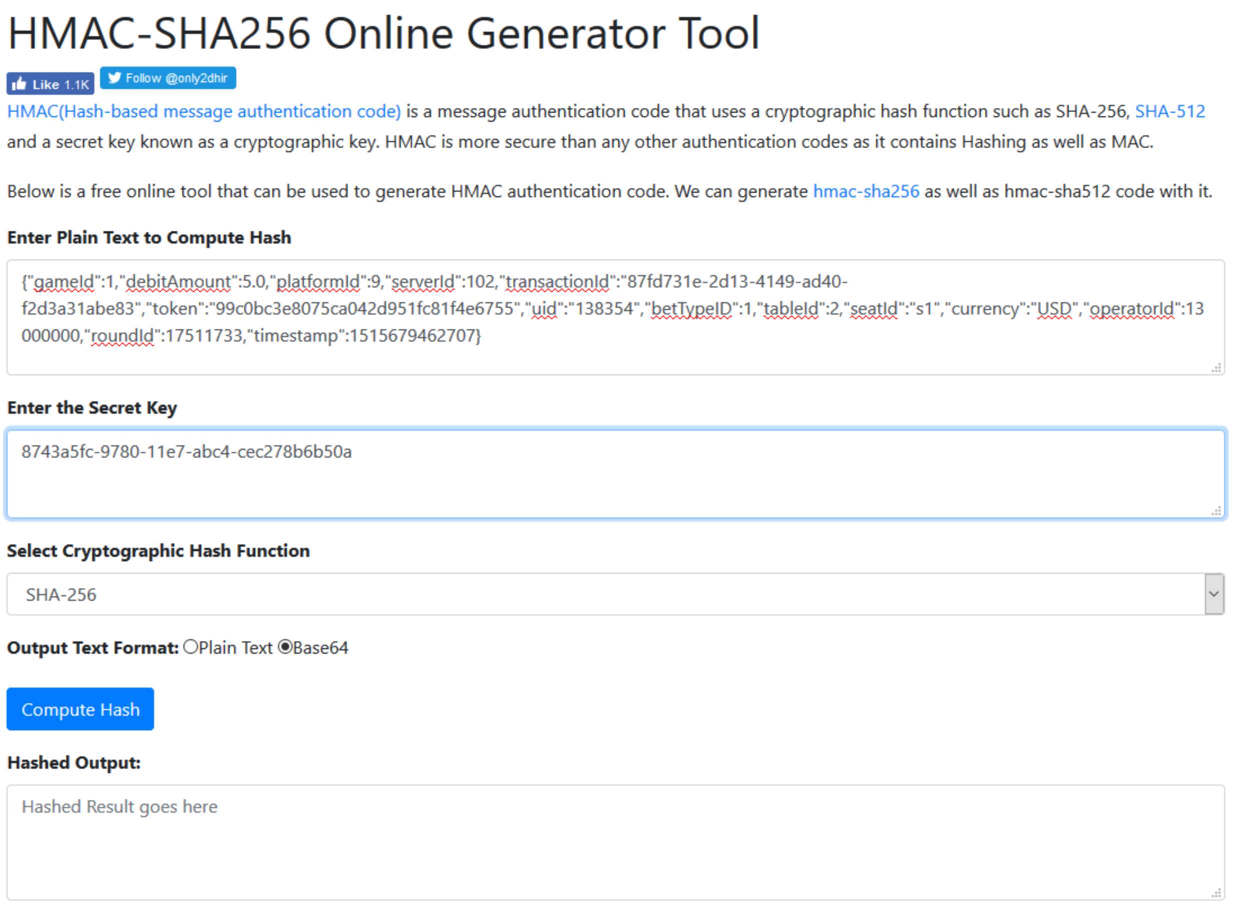
SHA-256

Output Text Format: Plain Text [✓ Base64]

Hashed Output:

Hashed Result goes here

2. Insert the message to be hashed and the Secret Key Note that the message should be inserted "as is", exactly as you got it . For example: *{"gameId":1,"debitAmount":5.0,"platformId":9,"serverId":102,"transactio nId":"87fd731e-2d13-4149-ad40- f2d3a31abe83","token":"99c0bc3e8075ca042d951fc81f4e6755","uid":"1 38354","betTypeID":1,"tableId":2,"seatId":"s1","currency":"USD","operat orId":13000000,"roundId":17511733,"timestamp":1515679462707}*


HMAC-SHA256 Online Generator Tool

HMAC(Hash-based message authentication code) is a message authentication code that uses a cryptographic hash function such as SHA-256, SHA-512 and a secret key known as a cryptographic key. HMAC is more secure than any other authentication codes as it contains Hashing as well as MAC.

Below is a free online tool that can be used to generate HMAC authentication code. We can generate hmac-sha256 as well as hmac-sha512 code with it.

Enter Plain Text to Compute Hash

{"gameId":1,"debitAmount":5.0,"platformId":9,"serverId":102,"transactionId":"87fd731e-2d13-4149-ad40-f2d3a31abe83","token":"99c0bc3e8075ca042d951fc81f4e6755","uid":"138354","betTypeID":1,"tableId":2,"seatId":"s1","currency":"USD","operatorId":13000000,"roundId":17511733,"timestamp":1515679462707}

Enter the Secret Key

8743a5fc-9780-11e7-abc4-cec278b6b50a

Select Cryptographic Hash Function

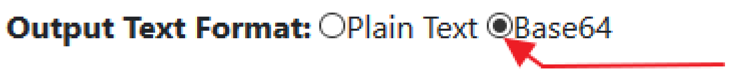
SHA-256

Output Text Format: Plain Text [✓ Base64]

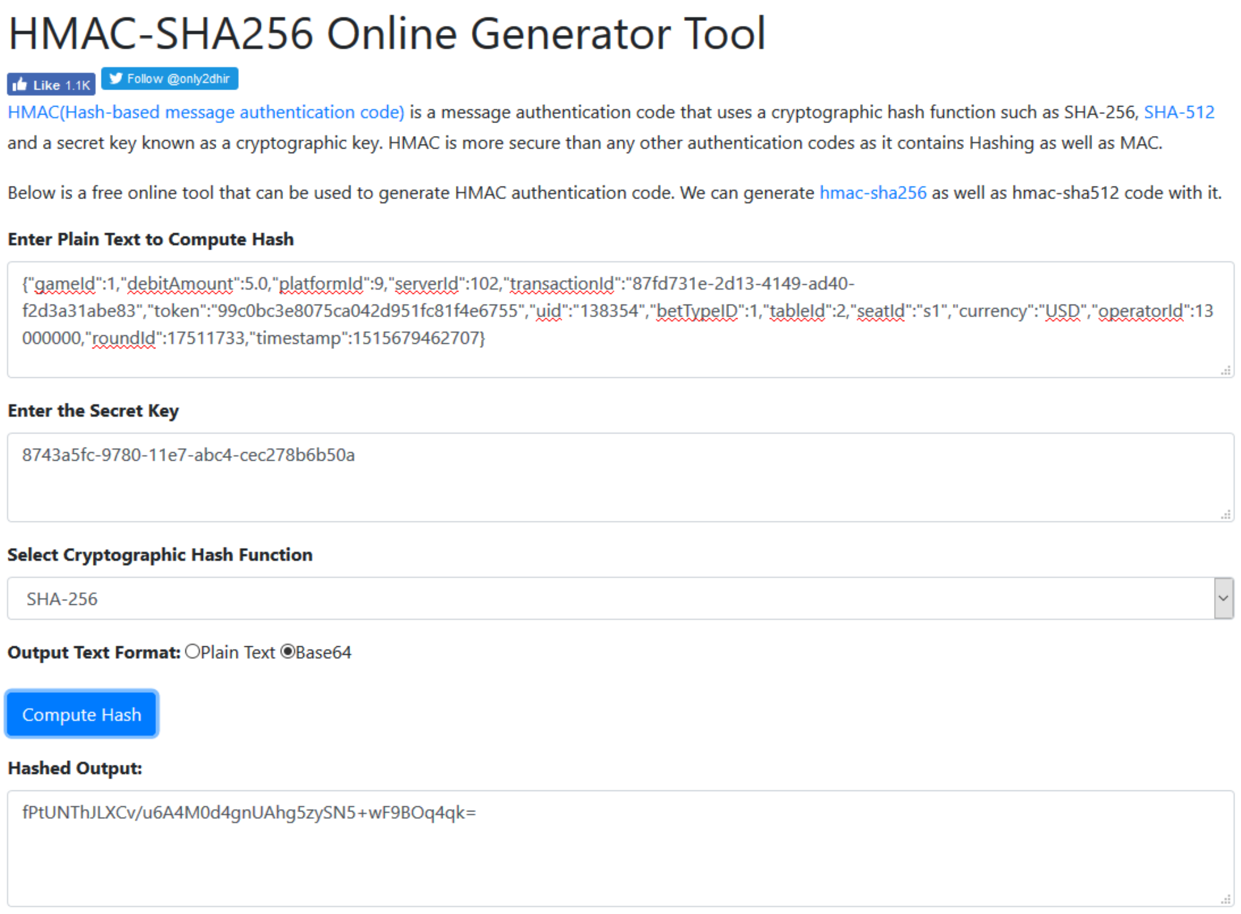
Hashed Output:

Hashed Result goes here

3. Set **Output Text Format** to be Base 64


Output Text Format: Plain Text [✓ Base64]

4. Push the **Compute Hash** and get the result.



HMAC-SHA256 Online Generator Tool

Like 1.1K   Follow @only2dhir

HMAC(Hash-based message authentication code) is a message authentication code that uses a cryptographic hash function such as SHA-256, SHA-512 and a secret key known as a cryptographic key. HMAC is more secure than any other authentication codes as it contains Hashing as well as MAC.

Below is a free online tool that can be used to generate HMAC authentication code. We can generate hmac-sha256 as well as hmac-sha512 code with it.

Enter Plain Text to Compute Hash

```
{"gameId":1,"debitAmount":5.0,"platformId":9,"serverId":102,"transactionId":"87fd731e-2d13-4149-ad40-f2d3a31abe83","token":"99c0bc3e8075ca042d951fc81f4e6755","uid":"138354","betTypeID":1,"tableId":2,"seatId":"s1","currency":"USD","operatorId":13000000,"roundId":17511733,"timestamp":1515679462707}
```

Enter the Secret Key

8743a5fc-9780-11e7-abc4-cec278b6b50a

Select Cryptographic Hash Function

SHA-256

Output Text Format: Plain Text [✓ Base64]

Compute Hash

Hashed Output:

fPtUNThJLXCv/u6A4M0d4gnUAhg5zySN5+wF9BOq4qk=

The result, in this case *fPtUNThJLXCv/u6A4M0d4gnUAhg5zySN5 +wF9BOq4qk=* should be the same as you got with our request.
If so - you did everything correct.