Webhook Example Request:


```
{
  "initiator": "Distributor",
  "transactionNo": "10299304",
  "externalTransactionNo": "434521",
  "qty": 1,
  "value": 20,
  "customer_id": "05ccc908-ba71-4708-a85c-e96ed57a8943",
  "session_id": "92b0f658-03eb-443a-b367-d5b05e121219",
  "name": "Nikos+Karavas",
  "email": "Nikos.karavas@novatti.com",
  "voucherPins": [
    {
      "voucherPin": "6157053239145142",
      "voucherSerialNumber": "52060500000694582"
    }
  ]
}
```


- voucherPins: List of voucher pin(s) to be redeemed towards customer
- transactionNo: Transaction number
- externalTransactionNo: External transaction number
- initiator: Distributor code
- customer_id: This is the same data that the Merchant originally passed to the distributor when the popup was launched. It is needed by the Merchant to redeem the voucher against the correct customer account.
- session_id: This is the same data that the Merchant originally passed to the distributor when the popup was launched. It is needed by the Merchant to redeem the voucher against the correct customer account.

Webhook Responses (Mandatory):

Success:

```
{
  "resultCode" : 0,
  "resultDescription": "Success"
}
```

Failure:

```
{
  "resultCode" : 999,
  "resultDescription": "Merchant's reason"
}
```

Error Handling

Standard HTTP error codes will be populated to indicate whether the API request has been processed. Code 200 indicates a successful response.
The result and result_description provides the application level result of the transaction.

Merchant Webhook Security

A number of options are available and recommended for securing the callback URL:

API Key

Flexepin can submit a secret pre-agreed api_key query parameter when making any request to the callback URL. This can be used to verify that the request came from Flexepin.

For example, **X-API-KEY**: “merchant secret” to be returned in the callback header.

By default, the API key shared by Flexepin can be used – which is provided along with the Merchant credentials.

IP whitelist

Flexepin will share the platform IP address(es) upon request to add to an IP whitelist. This will help to prevent access to unauthorised entities.

HTTPS

HTTPS is highly recommended.