

# Network Tokenization

## REST API Integration Guide



© 2021 Fiserv, Inc. or its affiliates. All rights reserved. This work is confidential, and its use is strictly limited. Use is permitted only in accordance with the terms of the agreement under which it was furnished. Any other use, duplication, or dissemination without the prior written consent of Fiserv, Inc. or its affiliates is strictly prohibited. The information contained herein is subject to change without notice. Except as specified by the agreement under which the materials are furnished, Fiserv, Inc. and its affiliates do not accept any liabilities with respect to the information contained herein and are not responsible for any direct, indirect, special, consequential or exemplary damages resulting from the use of this information. No warranties, either express or implied, are granted or extended by this document.

<http://www.fiserv.com>

Fiserv is a registered trademark of Fiserv, Inc.

Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

## Introduction

Network tokens are surrogate values that replace Primary Account Number (PAN) stored electronically throughout the payments system. Network Tokens can be used to conduct payment transactions securely and can provide improved protection against fraud, because network tokens can require cryptogram validation or be limited to use in a specific domain or circumstance, such as token requestor, device or channel.

The purpose of this guide is to describe the process how to use the network tokens in the Gateway.

In case you are using an external Token Service provider and plan to send authorization request to the Gateway, you need to submit the token and cryptogram obtained from your Token Service provider in the below fields

Field	Description
paymentCard -> number	Used to submit the network token number
expiryDate -> month	Used to submit Network token expiry month
expiryDate -> year	Used to submit Network token expiry year
tokenCryptogram	Used to Submit Token Cryptogram

In a case of 3DS Flow, it is important to send the "tokenCryptogram" in all the requests.

The following JSON document represents an example of a 3DS sale transaction submitted to our Gateway with network token and cryptogram obtained from external Token service Provider.

### Request Payload Example

```
{
  "requestType": "PaymentCardSaleTransaction",
  "storeId": "330995118",
  "transactionAmount": {
    "total": "178.00",
    "currency": "INR"
  },
  "transactionOrigin": "ECOM",
  "paymentMethod": {
    "paymentCard": {
      "number": "5204736200113910",
      "securityCode": "006",
      "cardFunction": "DEBIT",
      "expiryDate": {
        "month": "12",
        "year": "24"
      }
    }
  }
}
```

```

    },
    "authenticationRequest": {
      "authenticationType": "Secure3DAuthenticationRequest",
      "termURL": "https://test.ipg-online.com/webshop/simulator/secure3d/return",
      "methodNotificationURL": "https://test.test/notify",
      "messageCategory": "01"
    },
    "order": {
      "tokenCryptogram": "AGX1lvbYlypcAAFHV22IGgADFA=="
    }
  }
}

```

### 200 Response Example

```

{
  "clientRequestId": "2838649",
  "apiTraceId": "YbsF-DfjEh@p8a4GDb3JSQAAA2Y",
  "ipgTransactionId": "84385055093",
  "orderId": "R-f98d11be-9bea-419b-9645-1c4404971c10",
  "transactionType": "SALE",
  "paymentToken": {
    "reusable": true,
    "declineDuplicates": false,
    "brand": "MASTERCARD",
    "type": "PAYMENT_CARD"
  },
  "transactionOrigin": "ECOM",
  "paymentMethodDetails": {
    "paymentCard": {
      "expiryDate": {
        "month": "12",
        "year": "2024"
      },
      "cardFunction": "DEBIT",
      "bin": "520473",
      "last4": "3910",
      "brand": "MASTERCARD"
    },
    "paymentMethodType": "PAYMENT_CARD"
  },
  "transactionTime": 1639646716,
  "transactionStatus": "WAITING",
  "approvalCode": "?:waiting 3dsecure",
  "authenticationResponse": {
    "type": "3D_SECURE",
    "version": "1.0",
    "params": {
      "payerAuthenticationRequest": "xxxxxxxxxxxxxx",
      "termURL": "https://test.ipg-online.com/webshop/simulator/secure3d/return",
      "merchantData": "yyyyyyyyyyyy",
      "acsURL": "https://test3.3ds.firstdata.com/fs3ds-dsacs/acs/pareq"
    }
  }
}

```

In the next step you need to perform PATCH operation on the original transaction

#### Request Payload Example

```
{
  "authenticationType": "Secure3D10AuthenticationUpdateRequest",
  "storeId": "330995118",
  "payerAuthenticationResponse": "aaaaaaaaaaaa",
  "merchantData": "bbbbbbbbbb",
  "tokenCryptogram": "AGX1lvbYlpcAAFHV22IGgADFA=="
}
```

#### 200 Response Example

```
{
  "clientRequestId": "2838649",
  "apiTraceId": "YbsG@MItoj0b3pFHVNW0ygAAA7w",
  "ipgTransactionId": "84385055093",
  "orderId": "R-f98d11be-9bea-419b-9645-1c4404971c10",
  "transactionType": "SALE",
  "paymentToken": {
    "reusable": true,
    "declineDuplicates": false,
    "brand": "MASTERCARD",
    "type": "PAYMENT_CARD"
  },
  "transactionOrigin": "ECOM",
  "paymentMethodDetails": {
    "paymentCard": {
      "expiryDate": {
        "month": "12",
        "year": "2024"
      },
      "cardFunction": "DEBIT",
      "bin": "520473",
      "last4": "3910",
      "brand": "MASTERCARD"
    },
    "paymentMethodType": "PAYMENT_CARD"
  },
  "terminalId": "00001115",
  "merchantId": "470000032001125",
  "transactionTime": 1639646716,
  "approvedAmount": {
    "total": 178,
    "currency": "INR",
    "components": {
      "subtotal": 178
    }
  },
  "transactionStatus": "APPROVED",
}
```

```
"approvalCode": "Y:006973:4385055093:PPX :121609639289",
"secure3dResponse": {
  "responseCode3dSecure": "1"
},
"processor": {
  "referenceNumber": "121609639289",
  "authorizationCode": "006973",
  "responseCode": "00",
  "responseMessage": "Function performed error-free",
  "avsResponse": {
    "streetMatch": "NO_INPUT_DATA",
    "postalCodeMatch": "NO_INPUT_DATA"
  }
}
}
```