

Initiate a frictionless payment or request an exemption



An introduction to 3DSV2 is available in the section [3D Secure - Strong Authentication for Secure Payments](#)

The 3DS V2 protocol supports 150 data points transmitted to the issuer. However, processing these data points by the issuers can be time-consuming. Therefore, it is recommended to share the most essential and effective data points with the issuer to benefit from 'frictionless' payments.

In a payment request, the merchant must mandatorily transmit the following data:

- Card data in compliance with PCI DSS requirements
- Transaction data: identification numbers, currency, and amount
- Browser data: User location and connection system (language, screen size, IP address, etc.)
- Cardholder data: User's first and last name
- Recurring payment data (if using recurring payments)

To promote frictionless payments, the merchant can:

- Provide additional data
- Indicate their preference for frictionless payment
- Request an exemption

Provide additional data in the payment request

Some additional data are highly recommended to improve the transaction risk analysis by the issuer:

- **Shipping address details:** city, postal code, country, etc.
- **Delivery details** (delivery date)
- **User account information** (account creation date with the merchant, password reset date, etc.)
- **Basket data** (number of items in the order)
- **Merchant scoring**

The following JSON objects can be added to payment requests:

- customerInfo
- billingAddress
- shipping
- browserInfo

The recommended data are as follows:

- **Cardholder information:**
 - First name and last name
 - Email address
 - Landline phone number
 - Mobile phone number
 - Billing address
 - Delivery address
- **Browser information** (depends on integration):
 - IP address

Note: All this data will be used to secure the online process with the aim of fighting fraud. Issuing banks are regulated in the management of these confidential data.

Example of customerInfo object

```
...
  "customerInfo": {
    "merchantCustomerId": "cus_1234567890abcdef",
    "customerType": "individual",
    "firstName": "Max",
    "lastName": "Mustermann",
    "email": "customer@example.com",
    "phone": {
      "countryCode": "+49",
      "number": "1236547890"
    },
    "salutation": "Ms",
    "title": "Dr",
    "gender": "female",
    "maidenName": "Mustermann",
    "middleName": "sam",
    "birthDate": "2001-01-01",
    "birthPlace": "Bamberg",
    "socialSecurityNumber": "123443534"
  },
  ...
```

Example of billingAddress & shipping objects

```
...
  "billingAddress": {
    "streetName": "Schwarzenbergstr",
    "streetNumber": "4",
    "city": "Bamberg",
    "country": "DEU",
    "postalCode": "96050"
  },
  "shipping": {
    "address": {
      "streetName": "Schwarzenbergstr",
      "streetNumber": "4",
      "city": "Bamberg",
      "country": "DEU",
      "postalCode": "96050"
    }
  },
  ...
```



The addition of these additional data without an explicit request for 'frictionless' payment corresponds to the 'no Preference' case.

In this case, if the payment is 'frictionless', the liability shift to the issuing bank applies.

For more details: [Liability Shift and 3D-Secure Matrices](#)

Indicate a 'frictionless' payment preference

The JSON object **threeDsPolicy** allows the merchant to indicate their preference for offering a frictionless journey to their buyer.

The **challengePreference** parameter indicates the merchant's preference regarding authentication:

- NO_PREFERENCE: The merchant leaves the choice to the issuer to authenticate the buyer
- NO_CHALLENGE: The merchant wants the buyer not to be authenticated (exemption request, frictionless)
- REQUEST_CHALLENGE: The merchant wants to authenticate the buyer
- MANDATE_CHALLENGE: The merchant requests the issuer to authenticate the buyer (for example, for the first transaction of a subscription)

In all cases, the final decision is made by the issuing bank (the cardholder's bank).

Example of frictionless payment request

```
...

"paymentMethods": {
  "integrationType": "HOSTED",
  "type": "CARD",
  "card": {
    "threeDsPolicy": {
      "challengePreference" : "NO_CHALLENGE"
    }
  }
}

...
```



The liability shift to the issuing bank depends on the merchant's choice and the card brand.

For more details: [Liability Shift and 3D-Secure Matrices](#)

Request an exemption

The JSON object `threeDsPolicy` allows the merchant to indicate an exemption request.

The **threeDsPolicy – exemption.reason** parameter indicates the exemption requested by the merchant:

- **LOW_VALUE**: Low-value transactions (less than 30 €)
 - Banks must still request authentication if the exemption has been used five times since the last successful authentication by the cardholder or if the sum of previously exempted payments exceeds 100 €.
- **TRANSACTION_RISK_ANALYSIS**: Low-risk transactions (TRA: Transaction Risk Analysis)
 - An exemption from strong authentication may be granted. This requires prior agreement from the acquirer (based on a real-time risk analysis of each transaction).
 - To benefit from this exemption, the merchant must contact their account manager.

In all cases, the final decision is made by the issuing bank (the cardholder's bank).

Example of LOW_VALUE exemption request

```
...

"paymentMethods": {
  "integrationType": "HOSTED",
  "type": "CARD",
  "card": {
    "threeDsPolicy": {
      "exemption": {
        "reason" : "LOW_VALUE"
      }
    }
  }
}

...
```



The transfer of responsibility to the issuing bank depends on the merchant's choice and the card brand.

For more details: [Transfert de responsabilité et Matrices 3D-Secure](#)