

# Card processing

## About card payments

### General information about card payments

Computop Paygate processes all major cards and currencies worldwide. Card data is protected against unauthorised access by TLS encryption. Additional security functions are integrated fraud prevention and risk management. Our standardized settlement files guarantee a straightforward reconciliation processes in your accounting.

Visa Secure and MasterCard SecureCode secure your payment claim by password validation if a customer disputes the payment later. American Express SafeKey also uses the 3-D Secure technology, which means that the card holder must confirm their identity with a password.

Transaction processing can be made via Paygate standard form, via customized forms, via server-to-server-connection or via batch transfer. Likewise Paygate can process transactions from stationary terminals.

Using the card form provides several advantages:

1. Merchants can bypass the costly PCI-security authorisation
2. The programming of 3-D Secure with forms is much easier and quicker than via Server-to-Server connection

- About card payments
  - General information about card payments
  - Process of 3-D Secure payments
    - Process of a transaction with 3-D Secure via form interface
      - Simplified Sequence Diagram
    - Process of a transaction with 3-D Secure via Server-to-Server-connection
  - Credit card brands
- Integration
  - Credit card - common form
  - Card processing - common Server-to-Server
  - Card processing - Capture / Credit / Reversal / PayNow / Batch
  - EMV 3-D Secure

Cookie-/session - handling

Logo	Card processing
Info	Computop Paygate processes all major cards and currencies worldwide. Transaction processing can be made via Paygate standard form, via customized forms, via server-to-server-connection or via batch transfer. Likewise Paygate can process transactions from stationary terminals.
Type	Payments by Credit Card

### Process of 3-D Secure payments

MasterCard SecureCode (UCAF), Visa Secure, Diners ProtectBuy, JCB J/Secure and American Express SafeKey are authentication methods which verify the identity of the card holder before making the payment. The name 3-D Secure used by technicians describes only the protocol. The correct brand names are Visa Secure, MasterCard SecureCode, SafeKey, ProtectBuy and J/Secure.

Merchants benefit from authentication with 3-D Secure because the card schemes provide a liability shift: If you are using Visa Secure, MasterCard SecureCode, Diners ProtectBuy, JCB-Card J/Secure or American Express SafeKey, the burden of proof and thereby generally the liability is shifted from the merchant to the card issuing bank, should the customer dispute the payment. Irrespective of whether the card holder actually uses the authentication you obtain a very high protection against payment defaults / chargebacks in case the customer states they have not authorised the card payment. Your Acquirer will be able to discuss the details of 3-D Secure and the cover that it provides.

From a technical perspective 3-D Secure is not a payment method but an authentication process which precedes the payment: Once the credit card data has been entered, Paygate checks the identity of the card holder and does not process the payment until after the authentication.

For further steps it is crucial if the credit card connection is made via form interface or via Server-to-Server-connection. In the first case the Computop Paygate form assumes the further authentication process, with Server-to-Server-connection the merchant has to manage the authentication through a separate interface.

**Notice:** Please make sure to review our [EMV 3D Secure Specification](#) to integrate according to the newest standards.



Please notice that in case of Fallback to 3-D Secure 1.0 the URLSuccess or URLFailure is called with GET. Therefore your systems should be able to receive parameters both via GET and via POST.

## Process of a transaction with 3-D Secure via form interface

When requesting card payments via Computop hosted forms the complexity of 3-D Secure is completely removed from the merchant implementation.

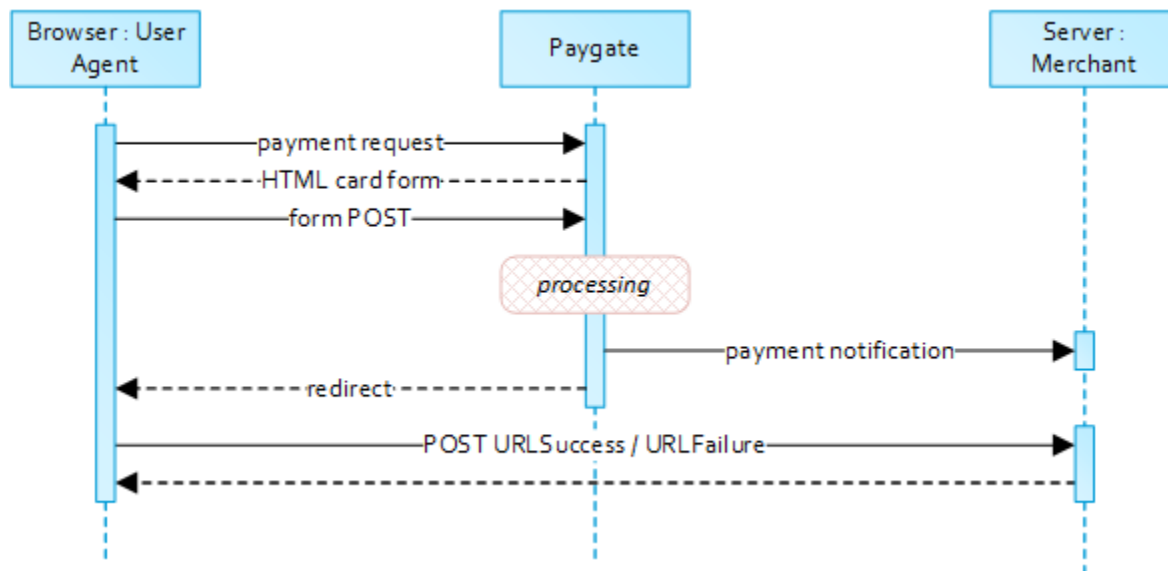
From a merchant point of view the sequence itself does not differ between 3DS authenticated and non-authenticated payments though 3DS requires consideration of additional data elements in the request and response.



### Notice about Cookie-/Session Handling

Please note that some browsers might block necessary cookies when returning to Your shop. [Here](#) you will find additional information and different solution approaches.

## Simplified Sequence Diagram



When requesting card payments via Computop hosted forms the complexity of 3-D Secure is completely removed from the merchant implementation.


From a merchant point of view the sequence itself does not differ between 3DS authenticated and non-authenticated payments though 3DS requires consideration of additional data elements in the request and response.









### Notice about Cookie-/Session Handling


Please note that some browsers might block necessary cookies when returning to Your shop. [Here](#) you will find additional information and different solution approaches.

Computop Paygate will return an HTML document in the response body representing the requested card form. The form may be included in the merchant checkout page or used as a standalone page to redirect the card holder to.









### Please enter your card data:




### Or choose alternative payment method:

<

>

AlipayBancontactbitpayDragonpayDirect DebiteNETS

Transaction secured by


© 2020 Computop  
[Terms & Conditions](#) | [Data Privacy](#) | [About Computop](#)

Card holder authentication and payment authorization will take place once the the cardholder entered all required card details and submitted the form data to Computop Paygate.

**Note:** In case you are using your own templates (Corporate Payment Page), please make sure you include Cardholder name on your custom template. Cardholder name is mapped to Paygate API parameter "CreditCardHolder". Cardholder name field must not contain any special characters and must have minimal length of 2 characters and maximum length of 45 characters.

When the payment is completed Computop Paygate will send a notification to the merchant server (i.e. **URLNotify**) and redirect the browser to the **URLSuccess** respectively to the **URLFailure**.

The blowfish encrypted data elements as listed in the following table are transferred via **HTTP POST** request method to the URLNotify and URLSuccess/URLFailure.



**Notice:** Please note that the call of URLSuccess or URLFailure takes place with a GET in case of fallback to 3-D Secure 1.0. Therefore your systems should be able to **receive parameters both via GET and via POST**.



The credit card form can be highly customized by using your own template.

Details are available here: [Corporate PayPage and templates](#)

If the password is correct Computop Paygate obtains confirmation in the form of a signature. Only after confirmation does Paygate start the payment and send the transaction with the signature to the Acquiring Bank.

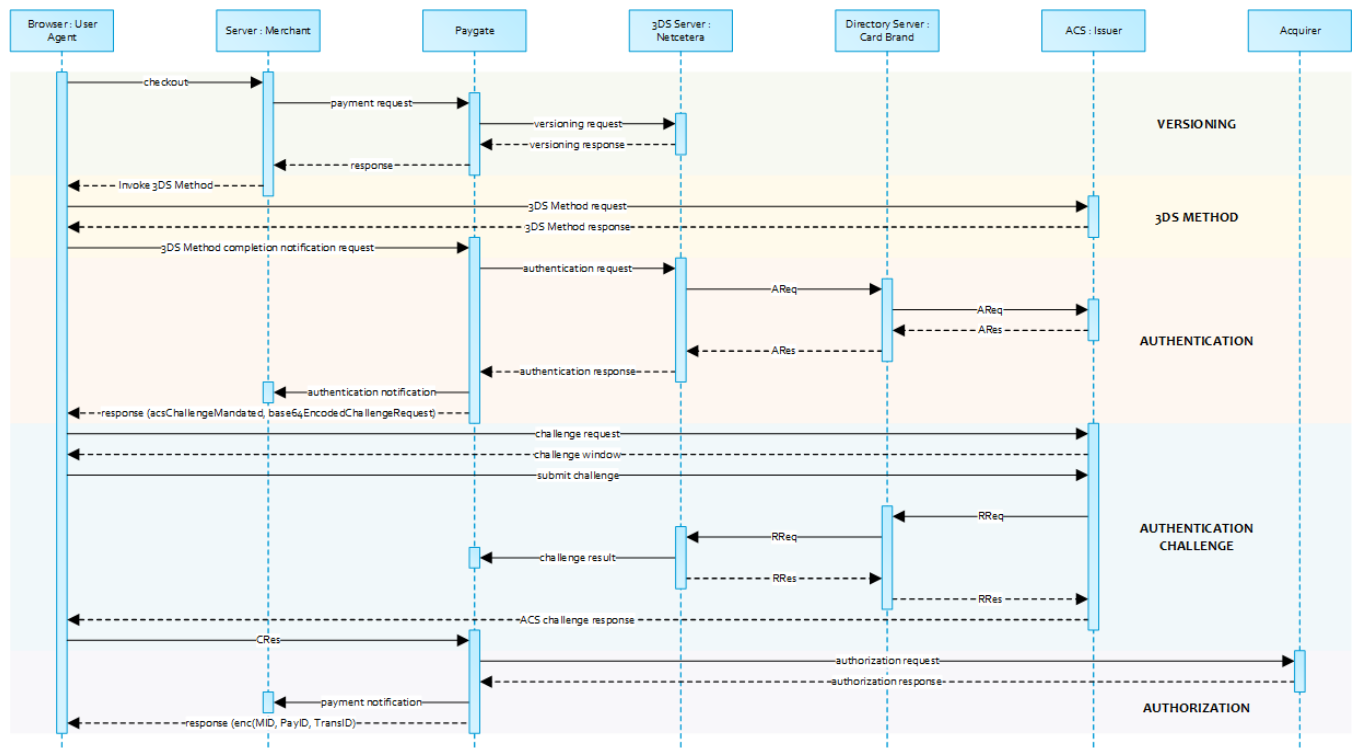


Details on the integration can be found here: [Credit Card Form \(paySSL\)](#)

## Process of a transaction with 3-D Secure via Server-to-Server-connection

A 3-D Secure 2.0 payment sequence may comprise the following distinct activities:

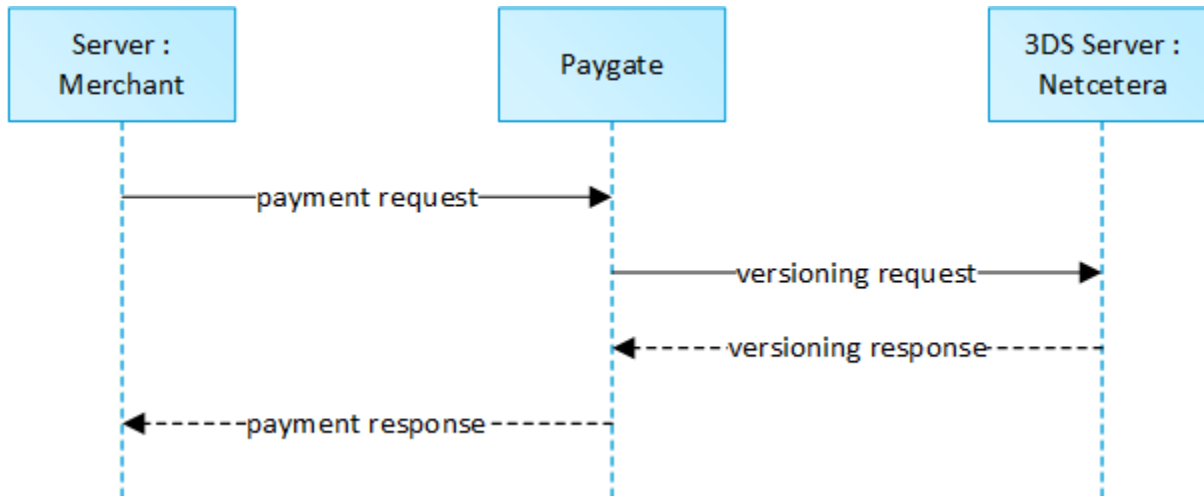
- Versioning
  - Request ACS and DS Protocol Version(s) that correspond to card account range as well as an optional 3-D Secure Method URL
- 3-D Secure Method
  - Connect the cardholder browser to the issuer ACS to obtain additional browser data
- Authentication
  - Submit authentication request to the issuer ACS
- Challenge
  - Challenge the card holder if mandated
- Authorization
  - Authorize the authenticated transaction with the acquirer



**i** Please note that the the communication between client and Access Control Server (ACS) is implemented through iframes. Thus, responses arrive in an HTML subdocument and you may establish correspondent event listeners in your root document.

Alternatively you could solely rely on asynchronous notifications delivered to your backend. In those cases you may have to consider methods such as long polling, SSE or websockets to update the client.

The initial request to Computop Paygate will be the same regardless of the underlying 3-D Secure Protocol.



In order to start a server-to-server 3-D Secure card payment sequence please post the following key-value-pairs to <https://www.computop-paygate.com/direct.aspx>.

**i** Details on the integration can be found here: [Server-2-Server Integration](#)

## Credit card brands

A list of all supported card schemes can be found here: [Card schemes](#)

## Integration

Please find here further information for

### [Credit card - common form](#)

Detailed information of integration via Payment forms

### [Card processing - common Server-to-Server](#)

Detailed information of integration via Server-to-Server API

### [Card processing - Capture / Credit / Reversal / PayNow / Batch](#)

Detailed information how to integrate further processes

### [EMV 3-D Secure](#)

