

PPF BANKA A.S. DEBIT CARDS

Guide for paying online using a Card

Contents:

1.	General information	1
2.	User support	1
3.	Paying online with a Card	2
4.	3D Secure	2
5.	Detailed Card settings including enabling E-commerce Transactions and setting up and amending contact details for 3D Secure	4
6.	Making E-commerce Transactions with 3D Secure authentication	5

1. General information

The conditions for using Debit Cards ("Card") are set out in the *Business Conditions of PPF banka a.s. for Debit Cards* ("SBC"), in the Card contract documents, in the *General Business Conditions of PPF banka a.s.* ("GBC") and in this Guide.

Capitalised terms, abbreviations and phrases have the meanings assigned to them in the GBC, the SBC, or this Guide. The current version of this Guide is available at www.ppfbanka.cz.

2. User support

User support for Cards is provided by Customer Service, which can be contacted by phone at +420 224 175 902 or by email at customer.service@ppfbanka.cz. The Customer Service Business Hours are available on the Bank's website. The phone line is unavailable outside of Customer Service Business Hours. Customer Service will handle queries sent by email outside of business hours on the next Business Day (during Business Hours).

The phone line +420 222 244 266 is available 24/7 for Card cancellations.

3. Paying online with a Card

E-commerce Transactions, enabling online payments to the Merchants who accept this payment method, can be allowed on any Card issued by the Bank. The payment is made as a payment without the physical presence of the Card.

The Merchant may request the following details for E-Commerce Transactions:

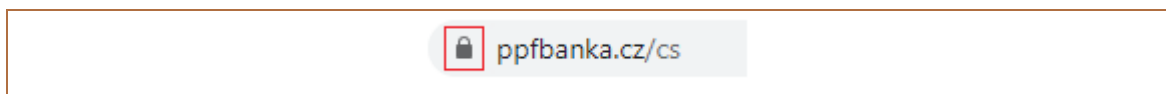
- Card number and validity (expiration) date;
- The card company that has issued the Card; in the case of PPF banka a.s., it is Mastercard (In most cases, however, this information is not necessary to enter);
- First name and surname of the Holder;
- The CVC/CVC2 code (Card Verification Code): a three-digit security code on the back of a Card (may also be called CVV/CVV2). **Do not disclose your PIN or your e-PIN to a Merchant under any circumstances; your PIN and e-PIN are not security codes;**
- The email address to which the payment confirmation is to be sent.

By entering the requested details on the Merchant's website or providing them to the Merchant by other means (by fax, email, etc.) you authorise the Payment Transaction. The Payment Transaction cannot be stopped (revoked) after that.

Merchants use various security systems for E-commerce Transactions:

- **3D Secure: Usually, you are not providing your Card details to the Merchant but to a 'payment gateway'.** Only Providers certified by Card companies (MasterCard, VISA), who are audited on a regular basis for compliance with the security rules for data protection, may operate payment gateways.
- **Secure connection to the website**

If you want to know if it is safe to visit a Merchant's website, you can check if there is a padlock icon next to the website URL.



If so, information you send to the website is secure.

Even so, always be careful when sharing private information. It is important to check in the address bar that you are really on the website that you wanted.

If you want to pay online using a Card, chose a Merchant who supports secure data transfers. If you are having any doubts about the Merchant's credibility, we recommend you use another payment method.

We do not recommend shopping at unsecured Merchants.

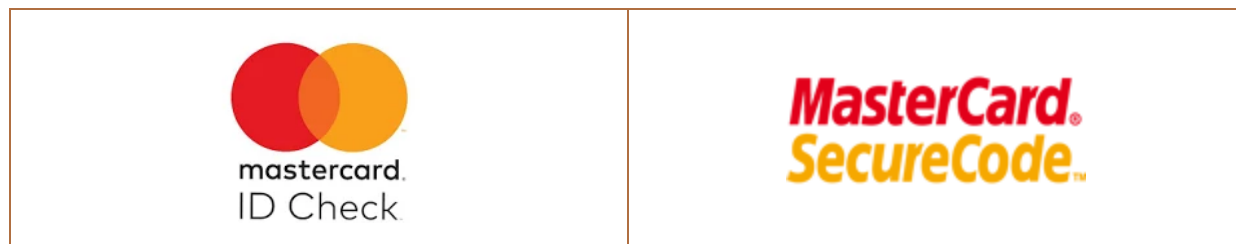
4. 3D Secure

4.1 What is 3D Secure?

3D Secure is an international standard for improving the security of E-commerce Transactions. It is a security method that protects the Card Holder and their data against unauthorised Payment Transactions when paying online at a Merchant supporting the 3D Secure service.

Card details are not provided directly to the Merchant but are entered on a payment gateway, where they are encrypted and transmitted for verification directly to the Bank that has issued the Card; the Merchant will therefore not have access to the Card details and cannot abuse them.

Websites of Merchants using 3D Secure bear the "Mastercard Secure Code" (older version) or "Mastercard ID Check" (new version) logo.



4.2 Benefits of 3D Secure

- It provides enhanced security in order to protect online Card payments, strongly preventing later abuse of the data from the Card used.
- There are two ways to confirm payments:
 - via the PPF banka e-Token app (“e-Token”)
 - If you use e-Token you don’t need to remember any codes or passwords, you can simply confirm payments using biometrics.
 - If you do not wish to use biometrics for payment authentication, you can set up a PIN in your e-Token that you can then use to confirm payments; or
 - you can use a static e-PIN and Single-use code sent by SMS or email.

Details about the authorisation of E-commerce Transactions are also available on our [website](#).

- Every Merchant in the EU now has the obligation to support this security standard. Although it is not mandatory for Merchants outside the EU, many Merchants have introduced the 3D Secure standard in order to make payments safer and to boost their own credibility.
- By shopping from a 3D Secure Merchant, you eliminate the risk that the Merchant could leak sensitive data about your Card and that it could be misused by an unauthorised party as a result. You are not entering the Card details on the Merchant’s website but on a secure payment gateway which is better guarded against data leaks.

4.3 How do 3D Secure payments work?

- You select the goods or services at an e-shop, you choose to pay by Card and you confirm your order.
- You enter the Card details in the payment gateway form (see point 3).
- The Card details are then encrypted and sent via a secure connection between the buyer and the payment gateway.
- The request is then checked with the Bank.
- If E-commerce Transactions are enabled on the Card, you confirm the payment using e-Token or an e-PIN and a Single-use code.
- The Bank then authorises the E-commerce Transaction and transmits this information back to the payment gateway, which sends a message to the Merchant that the payment has been confirmed.
- This process is very quick and usually only takes a few seconds.
- For recurring payments (e.g. regular subscription payments, software licenses, etc.) 3D Secure verification is required only once – when you make the first transaction. Future recurring payments do not require verification.

4.4 Setting up 3D Secure for Cards issued by the Bank

Using 3D Secure is mandatory for all Holders.

That is why we recommend that Users install e-Token for an easy and safe confirmation of E-commerce Transactions.

The backup option is that the Holder must provide the Bank with their mobile phone number and email address:

- A static e-PIN is made available to the Holder in Internet or Mobile Banking, and at the Holder’s request it can be sent to the Holder’s email address,
- Single-use Codes will be sent to their mobile phone number.

The Holder then has to enter these two pieces of information to confirm E-commerce Transactions whenever they encounter problems confirming them using e-Token or if they do not wish to use e-Token at all.

If the Merchant does not support 3D Secure, it will still be possible to pay using a Card without e-Token or e-PIN and Single-use confirmation. **However, we do not recommend shopping from such Merchants** (see point 3 above).

5. Detailed Card settings including enabling E-commerce Transactions and setting up and amending contact details for 3D Secure

You can find whether E-commerce Transactions are enabled or disabled on a Card in your Internetbanking (“IB”) or Mobile banking (“MB”), including the contact details (i.e. mobile phone number and, if applicable, email address) provided by the Holder for receiving the Single-use codes for the 3D Secure verification of E-commerce Transactions (see below).

Contact details always relate to the Holder (a natural person) and apply to all of that person’s Cards regardless of the Payment Accounts for which a Card has been issued. Thus, Cards can be issued for Payment Accounts of different companies or even different natural persons, but the Holder’s contact details will always be the same. It is not possible for one Holder to state different contact details for their various Cards.

Only the Client can enable E-commerce Transactions on a Card, either in person at the Bank’s Place of Business, through IB or over the telephone through their relationship manager.

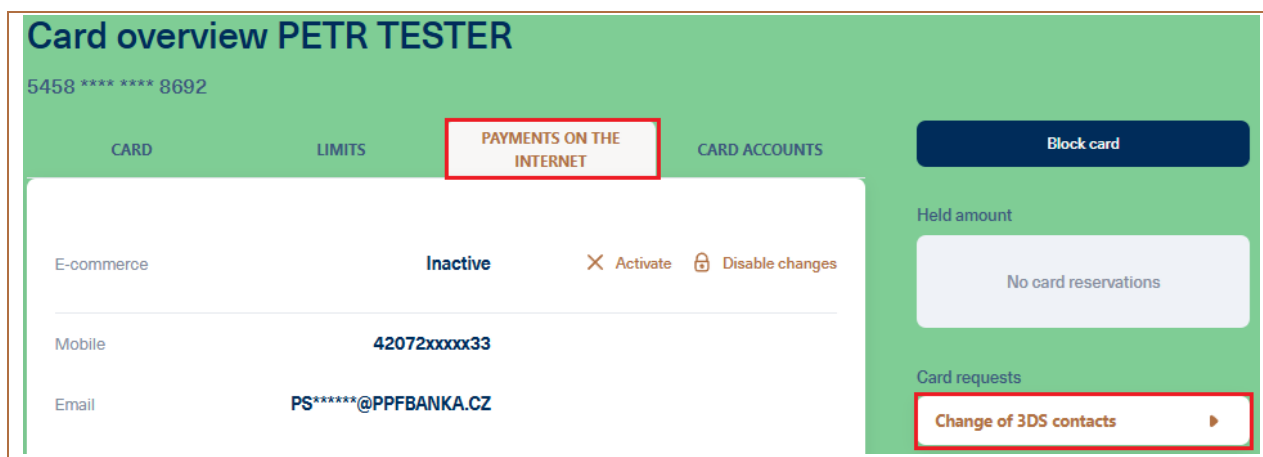
The setting up and/or the change of a Holder’s contact details can be requested in person at the Bank’s Place of Business or through IB and HB. **If a Holder is providing the Bank with a particular type of contact detail for the first time, they must also sign their consent to personal data processing.**

The setting up and/or the change of contact details for receiving 3D Secure Single-use codes will only be effective from the following Business Day.

5.1 Viewing and changes via Internet Banking

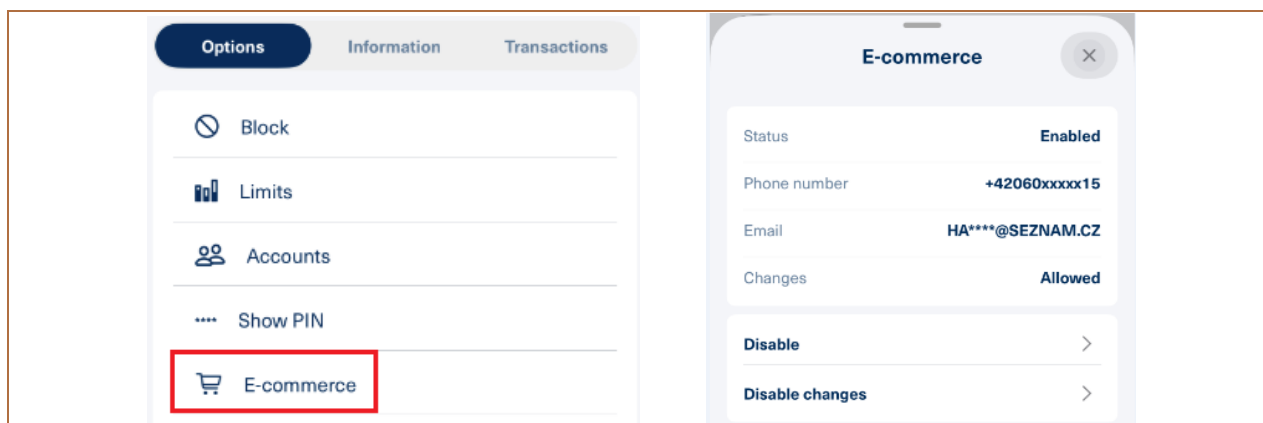
You can check whether E-commerce Transactions are enabled and review the Holder’s contact details (mobile phone number and, if applicable, email address) in IB in the Cards details – **Cards** option, after selecting a specific Card, click on the **Payments on the Internet** tab.

You can change your contact details for 3D Secure directly via a request from IB.



5.2 Viewing and changes via Mobil banking

You can check whether E-commerce Transactions are enabled and review the Holder’s contact details (mobile phone number and, if applicable, email address) in the MB in the Cards details – option **Cards**, after selecting a specific Card in the **Settings** tab, click on the **E-commerce** option.

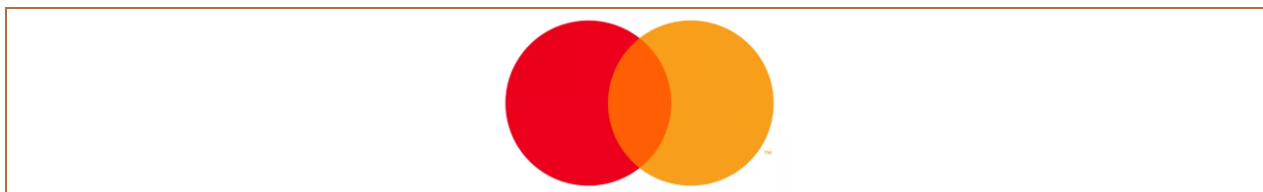


Contact details for 3D Secure can be changed through an unformatted message from MB.

6. Making E-commerce Transactions with 3D Secure authentication

6.1 Entering Card details

In the e-shop, choose the Card payment method with the MasterCard logo.



You will then be redirected to the payment gateway, in which you enter the Card details. Different payment gateways may require different details, but at least the Card number, the validity (expiration) date of the Card and the CVC/CVC2 code must be entered at all times.

To send the payment for 3D Secure verification, click **Pay** or a similar button.

Think carefully whether you allow the Merchant to remember the Card for next time. We recommend you only confirm this option for Merchants where you shop often, and that you do so after you have known for some time that the Merchant is reliable.

The screenshot shows the '3D Secure payment gateway' interface. On the left, there are two tabs: 'Card payment' and 'Safe card payment'. The 'Safe card payment' tab is active, showing logos for MasterCard, Maestro, and Visa. Below the logos, there is a question: 'Does your card permit online payment?' with a question mark icon. The form fields are: 'Your card number:' with the value '1234 5678 9012 3456'; 'Card valid till (month/year):' with values '11' and '23'; and 'Verification code:' with the value '404'. A green 'Pay' button is at the bottom. On the right, a 'Summary of your payment' box shows: 'Merchant: GPE TEST - PPF banka V Olšínách 80/626 10000 - Praha (CZ) www.gpwebpay.cz'; 'Payment number: #1622188029888'; and 'Total: 2,695.90 CZK'. At the bottom right, there are logos for 'mastercard ID Check' and 'VISA SECURE'. The footer contains: 'Powered by Global Payments Europe GP webpay', 'Created in cooperation with MasterCard', and links for 'How does it work?' and 'Principles of secure payment by card.'

6.2 Authorising E-commerce Transactions

The E-commerce Transaction summary is displayed. In the top left corner of the screen, you can change the language in which the authorisation will take place – in Czech or in English. You can also switch the language any time during the authorisation process on any other screen.

The E-commerce Transaction must be authorised within the time limit for entering the code (about 5 minutes). If you can't complete it within the time limit, the E-commerce Transaction will be closed without payment. If that happens, you have to repeat the payment to the Merchant.

Details about the authorisation of E-commerce Transactions are also available on our [website](#).

6.2.1 Authorisation using e-Token

If you have activated e-Token, the system will automatically redirect the E-commerce Transaction authorisation to it. If so, a notification of pending authorisation will be displayed on your phone. Tap the notification or open e-Token and check the E-commerce Transaction details. If the details are correct, authorise the E-commerce Transaction in the manner you have chosen in e-Token. If not, decline it.

You can change the method for authorising E-commerce Transactions – to do so, tap the link.

English | Čeština

Help | Cancel



Payment verification

Merchant: GPE TEST - PPF banka
Amount: 2695,90 CZK
Date: 28.5.2021
Card Number: **** * 7796

Confirm the payment in your mobile application, please.

Don't have the App? Verify your payment via another method - [click here](#).

Time left: 04:58

6.2.2 Authorisation using a Single-use code and the e-PIN

If you haven't activated e-Token or you are unwilling to use it to authorise a payment, you will receive a Single-use code via SMS. Enter the code in the first field, enter the e-PIN in the second field and press **CONFIRM**.

It usually only takes seconds to get the SMS but sometimes it can take longer. If you have been waiting for the SMS for more than a minute, you can have it resent by pressing **RESEND SMS**.

English | Čeština

Help | Cancel



Payment verification

Merchant: GPE TEST - PPF banka
Amount: 2695,90 CZK
Date: 28.5.2021
Card Number: **** * 7796

Please enter received Single-use Code and e-PIN for confirmation of the payment.

Time left: 04:45

Enter Code Here
Enter e-PIN here
CONFIRM
RESEND SMS

This information is not shared with the merchant.

Powered by Global Payments Europe

If you enter the incorrect Single-use code, you can re-enter it. To do so, enter the Single-use code and the e-PIN again in the respective fields and press **CONFIRM**.

You can also ask for a Single-use code resend at this point.

English | Čeština Help | Cancel



Payment verification

Merchant: GPE TEST - PPF banka
Amount: 2695,90 CZK
Date: 28.5.2021
Card Number: **** * 7796

Please enter received Single-use Code and e-PIN for confirmation of the payment.

Single-use Code or e-PIN was entered incorrectly.

Remaining attempts: 4

Time left: 03:09

This information is not shared with the merchant.

Powered by Global Payments Europe

6.3 E-commerce Transaction refusal

If you enter the Single-use code and e-PIN combination incorrectly five times, the E-commerce Transaction will be closed without being paid and at the same time, the possibility of paying online with the Card will be denied.

You will be able to make E-commerce Transactions again on the next Business Day.

English | Čeština Help | Cancel



Refused payment

The payment was refused because you have exhausted the allowed number of attempts to enter the Single-use Code.

For security reasons, all attempts of paying with a payment card on the internet will be rejected today. Possibility of payment will be restored the next day.

If E-commerce Transactions are disabled on the Card, the payment will be refused and the following message will be displayed.

English | Čeština

Help | Cancel



Refused payment

Internet payments are not permitted on the card or the card is not active. Contact your relationship manager for their setting.

In case of need, contact Customer Service, tel. (+420) 224 175 902, e-mail customer.service@ppfbanka.cz.

If E-commerce transactions are enabled on the Card but you have not provided the Bank with your mobile phone number so that the Single-use code could be sent to you, the payment will be refused and the following message will be displayed.

English | Čeština

Help | Cancel



Refused payment

This payment cannot be processed, because you do not set the contact details to send the authorization code.

In case of need, contact your relationship manager or Customer Service, tel. (+420) 224 175 902, e-mail customer.service@ppfbanka.cz.

CONTINUE

6.4 Help

If you need help, tap the link in the bottom left corner of any screen. The Help will open in a new window. To close the Help window, tap the cross button in the upper right corner.

English | Čeština



Help PPF Bank

- We have increased security when paying by card online.
- When paying by card you will receive an authorization code by which you confirm the payment on the internet.
- You may choose method of sending the authorization code: the cell phone or e-mail.
- The authorization code can be sent repeatedly by chosen method, or you can choose other method of its delivery.
- Resending and incorrect entry of an authorization code is limited to 5 attempts. For security reasons, card will be blocked for such a secure internet payment after depletion of these attempts until the end of the day. Possibility of payment will be restored the next day.
- Entering or change of contact details for sending an authorization code will be valid from the next business day.
- In case of need, contact your relationship manager or Customer Service, tel. (+420) 224 175 902, e-mail customer.service@ppfbanka.cz.
- These pages use cookies – detailed information is contained in the Guide for Using Payment Cards of PPF banka a.s. for Payments on the website.