User Manual of 3D Mastercard SecureCode™ - more secure online payment service

Content

1 Introduction 3
2 Prerequisites for the use of 3D service - MCSC 3
3 Procedure to activate 3D service - MCSC 4
4 The process of using 3D service - MCSC 7
5 Possible problems in using 3D service - MCSC 9

1 Introduction

Mastercard SecureCode™ (hereinafter referred to as MCSC) is a more secure online payment system based on 3D Secure protocol developed by MC International. In order to implement the safest and simplest payment models, MasterCard Worldwide has selected 3D Secure protocol and based on it developed its service.

The system is based on the idea, that in the process of the transaction, Cardholder and the Bank shall exchange information only known to them confirming their authenticity and the result of such a check deliver to an online trader who further, on the basis of the results obtained, decides to continue or abort the transaction. In the entire process of authentication the important issue is the fact that, regardless of the fact that the transaction is conducted on the site of the online trader, the online trader does not have an access to the content of the confidential data being exchanged between the Customer and the Bank. Classified information exchanged between the Customer and the Bank is One Time Password by which the Customer confirms his/her authenticity.

Preconditions for using MCSC services are:

− Online Trader who supports payments via MCSC;
− Bank Card of the issuer who supports MCSC method of payment;
− Previously performed activation of the service of usage of MCSC service.

If one of those conditions is not met, the course of a transaction will take place in the usual (traditional) way, without authentication check on the relation Customer - Bank. In other words, if the online trader supports payment via MCSC services, and the card of the Customer does not support it, the transaction will be carried out in the usual way. Also, if the Holder of a card participating in the program of MCSC makes a purchase on the website of the online trader who does not support the method of payment using MCSC services, the course of transaction will be performed as in the previous case described. Thus the customers are in no way deprived of the possibility of using the card on the Internet.
Outlets of the online traders that support payments system through MCSC services are usually characterized with a distinctive logo.

Picture 1 - MCSC logotype

2 Prerequisites for the use of 3D service - MCSC

In order to make an online trader support the method of payment through MCSC, its bank must be certified by Mastercard. Due to the large number of standards which must be met, method of certification is quite complex and time consuming, and there are still a number of traders that do not support this method of payment through MCSC, although the tendency of payment card regulations is to prepare an increased number of online traders to offer such a service. The online trader is obliged to point out on its website the information about whether the online trader is in MCSC program and what type of cards it accepts (usually in the part that relates to information on payment methods).

Next prerequisite for using MCSC service is a card that has the possibility of using MCSC (Maestro debit, Mastercard debit, Mastercard Standard, MasterCard Business Credit, MasterCard Business Debit) services. Banks that want to allow the use of their cards in MCSC program must meet strict standards set by the credit card company - MasterCard. Erste Bank AD Podgorica has completed certification procedures and provided that all the cards in its portfolio can be used to make payments on Internet sites that support payments through the MCSC services.

In order to leave users an opportunity to gradually adapt to the new technology or a new payment method, Erste Bank offers the clients a possibility of choosing the option of using MCSC services. With every purchase on the Web site that supports payments through MCSC services, the Bank will, if the

Customer had not activated the service, offer him the possibility to activate such a service. If the user wishes to activate the service, this can be done by accepting the General Terms and Conditions for using the 3D MCSC services that appear on the screen during the first purchase on the website that supports payment through the MCSC service. From the standpoint of the user, the activation and use of MCSC service does not require the use of special programs or upgrade of a computer. MCSC service can be used by all users who own a computer with some of the most popular Internet browsers with latest update version (Internet Explorer, Mozilla Firefox, Opera, Safari, Chrome, Edge etc.). Activation and use of MCSC service is completely free and one does not need to come to the Bank to start the activation process.

3 Procedure to activate 3D service - MCSC

The process of activation of MCSC services is performed exclusively during the shopping process on the Internet. The procedure itself is an intermediate step in the payment process in which Erste Bank offer the possibility of activating the service itself or further use of the card in the usual way. Given that some traders do not want to continue with the process of purchase if the card is not activated in the MCSC program, there may be cases that users will not be able to conclude the purchase without activation.

The steps of activation of the card are as follows:

1. The Cardholder selects desired goods and/or services and go to the site (link) for payment.
2. The Cardholder enters the requested information - personal data and/or data on the card (Picture 2).

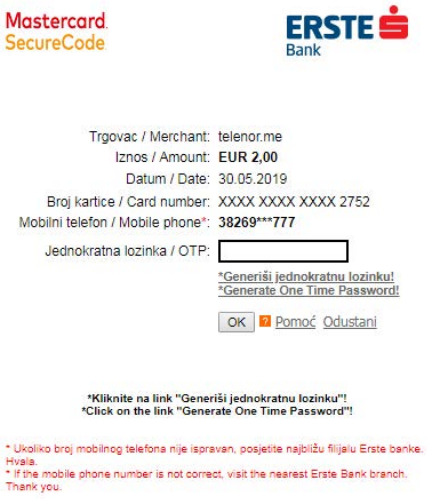
Picture 2. - Shopping on the Internet site - entering data of the card

1) Online trader automatically connects with the Bank that checks whether the card is activated to use MCSC service and if not, on the screen of the Customer there will appear a window with an offer to activate the service with the associated General Terms and Conditions (Picture 3).

Picture 3 - Activation of the card in the MCSC program - accepting of the General Terms and Conditions

2) Accepting General Terms The user selects the activation extension and on the next screen generates a "One-time password" by clicking the "Generate One Time Password" button (Picture 4).

Picture 4. - Activation of the card in the MCSC program - The entry of the One Time Password



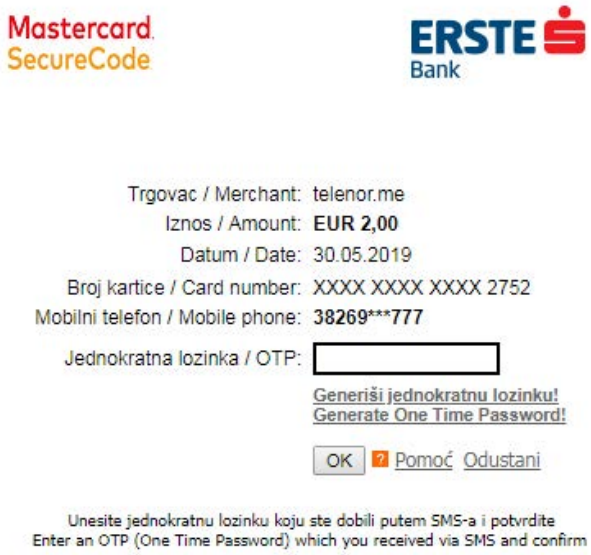
NOTE: It is very important for the Cardholder to verify that the mobile phone number displayed on the screen is correct before making a one-time password. In case the user's mobile phone number is not correct, the transaction will not be able to continue. The user should visit the nearest branch of Erste Bank and update the information off his mobile phone number. The user can also update the data off his mobile phone number without visiting the bank, if he has activated some of the electronic banking services for retail clients (Nebanking or mBanking).

3) By selecting the "Generate One Time Password" option, the user receives a 6-digit One Time Password via SMS on the mobile phone number shown on the screen that's registered with the Bank (picture 5).

Picture 5 - Activation of the card in the MCSC program - One Time Password

4) The user enters the 6-digit One Time Password in the field provided for this and confirms by pressing OK.

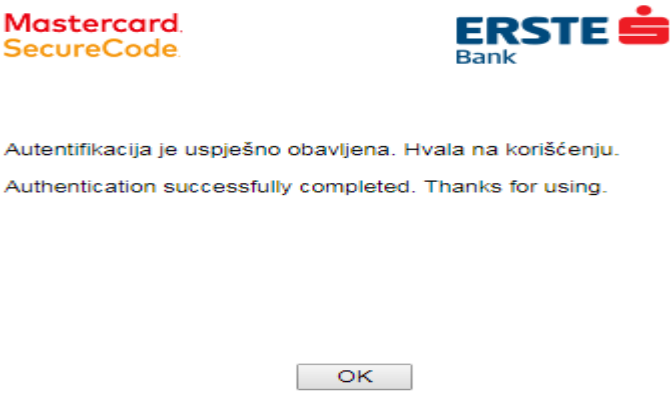
Picture 6 - Activation of the card in the MCSC program – Enroll and confirm One Time Password



NAPOMENA: The time provided for entering and confirming the entered One-time password is 120 seconds, and after that time, the password expires and new must be generated. The total number of allowed attempts to generate a one-time password is three, and if it is not used, the service is temporarily blocked for 60 minutes. After the expiration of that period, the service will be automatically unblocked and three new attempts will be allowed.

5) The bank checks whether the One Time Password is correct and displays a message about successfully executed authentication on the screen (Picture 7).

Picture 7 - Activation of the card in the MCSC program – Information about successful authentication



6) The bank returns to the Internet merchant information that card has been successfully activated and the user authentication process has been performed.

7) An Internet trader continues to process the transaction by sending an authorization request to the Bank regarding the status of the card and the available amount on the account.

8) The bank checks the availability of funds on the account, as well as the validity of the card data and, depending on the verification results, approves or rejects the transaction.

NAPOMENA: The activation of the MCSC service is for the card, not for the User. If it wants to use the MCSC service, it is necessary for the User to activate the service for each card individually.
After the User has been issued a new card for some reason (loss, theft, damage, reissue, etc.), the service must be reactivated.

4 The process of using 3D service - MCSC

Once the User has activated the card in the MCSC program in previous transactions with the Internet merchant, the same card does not require further activation, as further authentication will be performed by checking the validity of the **One Time Password**. This will reduce the number of steps that need to be taken to complete the purchase and the order is as follows:

1) The Cardholder selects desired goods and/or services and go to the site (link) for payment.
2) The Cardholder enters the requested information - personal data and/or data on the card (Picture 8).

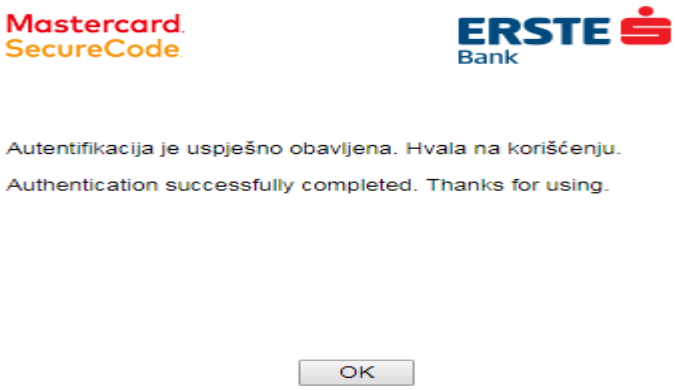
Slika 8 - Shopping on the Internet site - entering data of the card

3) The Internet Merchant automatically connects to the Bank to verify that the card is activated for the use of the MCSC service, and if yes, the User's screen displays the basic details of the transaction and the request to generate and enter a One Time Password (Picture 9).

Picture 9 – Enroll and confirm One Time Password

4) The bank checks whether the One Time Password is correct and displays a message about successfully executed authentication on the screen (Picture 10).

Picture 10 - Information about successful authentication



5) The bank returns to the Internet merchant information that card has been successfully activated and the user authentication process has been performed.
6) An Internet trader continues to process the transaction by sending an authorization request to the Bank regarding the status of the card and the available amount on the account.
7) The bank checks the availability of funds on the account, as well as the validity of the card data and, depending on the verification results, approves or rejects the transaction.

5 Possible problems in using 3D service - MCSC

Problems in using 3D MCSC services can be divided into two groups:

a) Problems caused by a system error;
b) Problems caused by user errors;
c) Misuse.

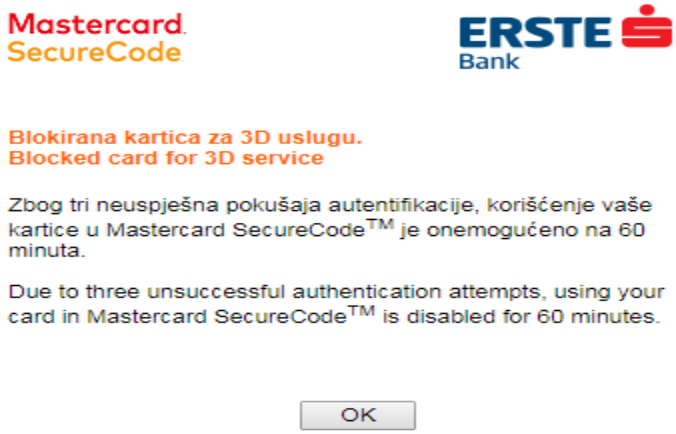
a) During regular operations it is realistic to expect the system of support/processing of the MCSC services will, on rare occasions, be unavailable or will not work in line with the expectations. The Bank has tried to anticipate such situations and solution procedures thereof. In situations when the system is unavailable (the merchant has the MCSC logo displayed, and the MCSC verification screens do not appear), Cardholders will not be damaged in such a way that they will not be able to use the card as all the transactions will be carried out in the usual way, but without the check of the MCSC One Time Password. Such situations may temporarily reduce the level of safety of realization of the transaction, but the Customers will still have the chance of using the card and the realizing the transaction.

Incorrect functioning of the system potentially poses a greater problem and in case of doubt it is necessary to immediately inform the Bank. In such situations, Users will be able to see the screen on which a system error message is shown (Picture 11).

Picture 11 - The message on the system error occurred

b) During the activation or authentication process, in most cases, errors occur because the User has entered the One Time Password incorrectly, or the time elapsed for entering a One Time Password has expired. Therefore it is important to take care about input rules to be followed, in order to successfully complete activation or authenticate transactions.

Picture 12 - Blocked card message



c) The introduction of 3D services MCSC, the level of security of payment via cards was raised to a higher level, but will nevertheless, the abuse still remain possible. When a customer suspects a possible misuse of the card, it is required to urgently inform the Bank by calling the Call Centre on the phone number 020 409 490 or 020 409 491, so as to react in as shorter period as possible and prevent any possible damage.

The User has the ability to enter the One Time Password three times. If it fails to enter the correct one in the third attempt, the service of using the MCSC service will be disabled for the next 60 minutes (Picture 12). After the expiration of that time, the service is automatically unblocked and the number of attempts to enter is set to three. Such situations can be repeated three times, after which the card is permanently blocked for use in the MCSC program and for unblocking it is necessary to contact the Bank.

- The first three (3) wrong entries - temporary blocking for 60 minutes
- The next three (3) wrong entries - temporary blocking for 60 minutes
- The last three (3) wrong entries - permanent blocking (you need to contact Bank for unblocking)

In other words, the card is still active for use at ATMs, points of sale, and Internet merchants that are not included in the 3D MCSC program, but it is not possible to activate the MCSC service until the Bank allows it. In case the Cardholder blocks the card due to unsuccessful entries, it is necessary to contact the Bank.
If you want the card to be unblocked and new attempts allowed, send the Request for Unblocking 3D MCSC Services to the Card department email ***cards@erstebank.me.*** The Request is available on the Bank's website ***www.erstebank.me.***
The service will be unblocked during the same business day in the working hours of 08:30-15:30h or at the latest on the first following working day, as the User will receive a return notification in the e-mail.