

User Manual of 3D Services MasterCard SecureCode™ - more secure online payment services

Content

1. INTRODUCTION	3
2. PREREQUISITES FOR THE USE OF 3D SERVICES - MCSC	3
3. PROCEDURE TO ACTIVATE 3D SERVICE - MCSC.....	4
4. THE PROCESS OF USING 3D SERVICES - MCSC.....	7
5. PROBLEMS IN THE USE OF 3D SERVICES - 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 are comprised of a personal message and unique 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 SERVICES - 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 contactless, 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 Customer wants to activate the service, he can do so by entering the required data, after which the Bank will make the verification thereof, and confirm the activation. This method of activation is called Activation During Shopping and it only occurs in cases where the customer is purchasing with a card that has not been completed the activation for of the Web site that supports payments through MCSC services. 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, 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 Customer selects desired goods and/or services and go to the site (link) for payment.
2. The user 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

2014. prosinac 05 12:46:36

Unesi podatke o platnoj kartici

Detalji plaćanja

Broj narudžbe	141285
Trgovac	http://www.bonbonijera.hr
Opis	kupovina bona
Iznos	16.50 HRK
Broj kartice	6769820100070019 *
Datum isteka	11 / 2018 *

Vratite se na [Stranice trgovca](#) (plaćanje neće biti provedeno)

Napomena : Slijedeći ekran koji vidite može biti provjera kartice od strane izdavatelja kartice / banke

>> Proslijedi

3. 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

MasterCard SecureCode. **ERSTE Bank**

Aktivacija korisnika u MasterCard SecureCode™ programu

OPŠTI USLOVI ZA KORIŠĆENJE 3D USLUGE
(SecureCode usluga za Maestro/MasterCard kartice)

1. ZNAČENJE POJMOVA

Banka - izdavalac Opštih uslova je Erste Bank AD Podgorica, registrovana kod Centralnog registra privrednih subjekata u Podgorici pod brojem: 4-0001817 i Poreskim identifikacionim brojem (PIB): 02351242, sa sjedištem u Podgorici, ulica Studentska bb, račun: 907-54001-10, SWIFT: OPPOMEPG, internet stranica: www.erstebank.me, info telefon: 020 440 440, e-mail: info@erstebank.me;

Kartica – debitna ili kreditna, Maestro ili MasterCard kartica koja, omogućuje Korisniku raspolaganje sredstvima sa Računa na

[Pomoć](#)

Do not activate **Proceed**

4. By accepting the General Terms and Conditions, the Customer selects the continuation of the activation on the next window he enters the requested information, thus defining the "Personal Message" (Picture 4)

Picture 4. - Activation of the card in the MCSC program - the entry of the basic data from the card

MasterCard SecureCode. **ERSTE Bank**

Aktivacija korisnika u MasterCard SecureCode™ programu

U toku je postupak Vaše aktivacije u MasterCard Secure Code™ program koji Vam omogućava besplatno korišćenje sistema za sprječavanje neautorizovanog korišćenja kartice. Nakon aktivacije, prilikom svakog korišćenja kartice na Internet stranicama koje učestvuju u MasterCard SecureCode™ programu prilikom potvrđivanja biće zatražena Vaša MasterCard SecureCode™ lozinka.

Ime i prezime (velikim slovima):

Datum isteka kartice: MMGG

JMBG/Interni broj stranca:

Lična poruka:

[Pomoć](#)

Activation of the Customer in the MasterCard SecureCode™ program

It is on the course the procedure of Your activation in the MasterCard SecureCode™ program, which allows You a free of charge usage of the system for prevention of unauthorized card usage. After the activation, in the process of every usage of the card on the web pages that participate the MasterCard SecureCode™ program, during the confirmation, there would be required Your MasterCard SecureCode™ program password.

Name and Surname (capital letters): DANILO MIRKOVIĆ

Card expiry date: 1118 MMYY

Personal unique ID/Internal foreigner number: 10198000001

Personal message: TEST 1

Do not activate **Proceed**

5. The Bank checks the entered data and if those are correct, the screen shows the basic details of the transaction and the fields in which the Customer has to create his "Password"

Picture 5. - Activation of the card in the MCSC program - creating a password






Trgovac: IPT DOO
 Iznos: HRK 16,50
 Datum: 05.12.2014
 Broj kartice: XXXX XXXX XXXX 0019
 Lična poruka: TEST1

Da biste kreirali svoju lozinku unesite 6 - 20 znakova bez razmaka.
 Zapamtite svoju lozinku - ona će se koristiti prilikom svake online
 kupovine kod trgovaca koji podržavaju MasterCard SecureCode™
 trgovinu.

Lozinka:
 Lozinka ponovo:

Trgovac nema uvid u sadržaj tajnih podataka koje unosite.

Trader: IPT DOO

Amount: HRK 16,50

Date: 05.12.2014.

Card Number: xxxx xxxx xxxx 0019

Personal message: TEST 1

In order to create Your password, please, enter 6-20 marks without space. Remember Your password – it shall be used at every online shopping at traders that support the MasterCard SecureCode™ program.

Password:

Retype password:

Accept Do not activate

The trader does not have an access to the security data you are entering.

6. Bank checks whether the password is created in accordance with the rules and the window displays a screen (Picture 6) with a message on successfully completing the activation.

Picture 6. - Activation of the card in MCSC program - information on successfully completing the activation



Autentifikacija je uspješno obavljena. Hvala na korišćenju.

OK

Authentication has been successfully performed. Thanks for using.

1. Bank returns to the online trader the information that the card has been successfully activated and the process of authentication of the User has been successfully completed;
2. The online trader continues with processing the transaction so that it sends to the bank an authorization request on the status of the card and the available amount on the account;
3. The Bank checks the availability of funds on the account, as well as the accuracy of the data on the card and, depending on the outcome of checks, it approves or rejects the transaction.

NOTE: The MCSC service is linked to the individual card, not the Customer. If you want to use MCSC service, the Customer must activate the service for all cards with which he wants to use the service.

The Customer having been, due to some reason, issued a new card (loss, theft, damage, reissue, etc.) need to reactivate the service.

4. THE PROCESS OF USING 3D SERVICES - MCSC

After the Customer in prior transactions at the online trader made the card activation in the MCSC, the same card does not require further activation, as the further authentication is done by checking the correctness of the **Personal message** and **Password**. This will reduce the number of steps that need to be done to conclude the purchase and the order is as follows:

1. The user selects the desired good and/or service and then goes to the site (link) for payment.
2. The user enters the requested information - personal data and/or data from the card (Picture 7).

Picture 7. - Shopping on the Internet site – entry of the data from the card

2014. prosinac 05 12:46:36

Unesi podatke o platnoj kartici

Detalji plaćanja

Broj narudžbe	141285
Trgovac	http://www.bonbonijera.hr
Opis	kupovina bona
Iznos	16.50 HRK
Broj kartice	6769820100070019 *
Datum isteka	11 ▼ 2018 ▼ *

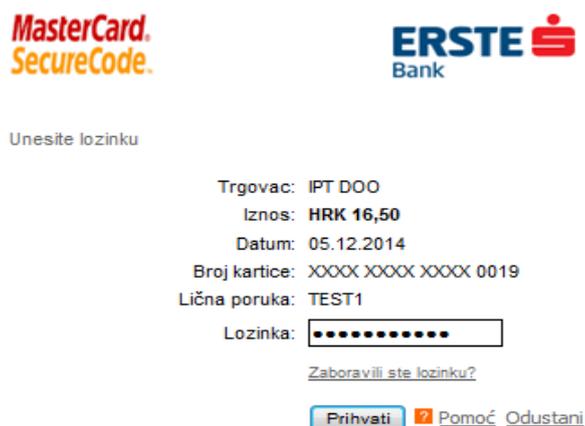
Vratite se na [Stranice trgovca](#) (plaćanje neće biti provedeno)

Napomena : Slijedeći ekran koji vidite može biti provjera kartice od strane izdavatelja kartice / banke

>> Prosljedi

3. Online trader is being automatically connected to the Bank, which checks whether the card is activated for the use of MCSC service and, if it is registered, on the screen of the Customer a window will appear with the basic details of the transaction and the personal message and password requirement for entry (Picture 8).

Picture 8. – Password entry



Unesite lozinku

Trgovac: IPT DOO
Iznos: **HRK 16,50**
Datum: 05.12.2014
Broj kartice: XXXX XXXX XXXX 0019
Lična poruka: TEST1
Lozinka:

[Zaboravili ste lozinku?](#)

Trgovac nema uvid u sadržaj tajnih podataka koje unosite.

Trader: IPT DOO

Amount: HRK 16,50

Date: 05.12.2014.

Card Number: xxxx xxxx xxx 0019

Personal message: TEST 1

Password:

[Forgotten password?](#)

Accept [Help](#) [Cancel](#)

The trader does not have an access to the security data you are entering.

- The Bank checks the validity of the entered password and, if it is correct, a screen with the message about successfully completed authentication appears. (Picture 9).

Picture 9. - Information on successfully completed activation



Autentifikacija je uspješno obavljena. Hvala na korišćenju.

Authentication has been successfully performed. Thanks for using.

5. The Bank returns to the online trader the information that the user activated the card and online trader continues with processing the transaction so that it sends to the bank an authorization request on the status of the card and the available amount on the account.
6. The Bank checks the availability of funds in the account and the accuracy of the data on the card and depending on the result of the inspection it approves or rejects the transaction.

NOTE: The user has three attempts to enter the password after which the services are temporarily or permanently blocked.

In case of unsuccessful authentication, the Bank will notify the online trader, who will decide whether he wants to proceed with processing the transaction (step 6) or to terminate the transaction.

5. PROBLEMS IN THE USE OF 3D SERVICES - MCSC

Problems in use of MCSC services can be divided into two groups:

- a. The problems arising from system failure
 - b. Problems caused by mistakes of the Customer
 - 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, Customers 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 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.

Improper operation of the system is potentially the greater problem and, in a case of doubting it, it is necessary to immediately alert the Bank. In such situations, there will be visible a screen which will include a written message on the system error (Picture 10)

Picture 10. – The message on the system error occurred



System error

There has occurred an error in the application operating. Please, try again later or contact us via e-mail

Proceed

- b. Problems resulting from the misuse of the system by the Customer can be divided into two groups:
 - Errors in the process of activation;
 - Errors while using the service.

During the activation process, in the most number of cases the errors occur due to incorrect data entered by the Customer, it is necessary to take account of the entry rules to be followed in order to successfully complete the activation. Some of the possible problems and ways of resolving those can be found in the following table (Table 1):

Table 1 - Possible Customer errors when activating 3D services MCSC.

Where	What	How – Manner of Solving
The screen for activation – entry of the basic customer data	Name and surname of the Customer	Full name is entered using large printed letters in a way to literally copy the data printed on the card. Diacritics marks (ć,č,š,ž,đ...) and hyphens are also entered if those are printed on the card. In the case that the name of the Cardholder is shortened due to its length, it is also entered as printed on the card. <i>*In the event that the keyboard does not support the entry of diacritical marks, we recommend that you set your computer to enter those or copy the data exactly listed on the card and confirmed by You to the Bank.</i>
The screen for activation – entry of the card data	CVC	CVC2 (for Maestro/MasterCard cards) is a three-digit number printed on the back of the card (in the signature line or box next to it).
The screen for activation – entry of the card data	Date of the card expiration	Card expiration date should be entered in the format month year (MMYY) without using the spaces, dashes, slashes and colons between months and years. For the year of expiration only the last two digits shall be entered. Eg, for the card with the expiration of the 12th month of 2014, please, enter 1214.
The screen for activation – entry of the basic data	Personal ID/Intern number of the foreigner	Into the field it should be entered only personal identification number (for residents) or Internal Number for a foreigner (non-resident) being the Cardholder without any spaces at the end. <i>*Internal Number of the foreigner is an internal number in the bank systemically granted for non-resident client of the Bank during its first registration in the Bank. Information about his number is available at the bank counter. The internal number should be entered as a 13 digits number, so if it is less than 13 it needs to be added leading zeroes to fulfil it.(Eg.0000000xxxxx)</i>
The screen for activation – entry of the basic data	Personal message	This is the message arbitrarily created by the Customer and it serves as a message to appear to the Customer every time with the request for entry of a password. This field is allowed to enter the letters, characters and spaces to the maximum length of 30 characters.
The screen for entry (creation) of the password	The password	The password is secret information created by the Cardholder and is designed to check the user authentication when making payments on web sites that support payments through the MCSC services. Password length must be from 6 to 20 characters and there can be used only the letters and characters without spaces, special or diacritic characters.

NOTE: You need to pay attention to the fact that, in the process of activation, the Cardholder has the option of three attempts of data entering. If the third attempt of the Cardholder results in a failure to perform the activation (due to incorrect data entry), a further option of the activation of a card in the MCSC will be disabled for that transaction. You need to close the payment application and start again.

In other words, the card is still active for use at ATMs, points of sale and at online traders, but it is not possible to perform the activation of MCSC service until the Bank allows so. In case that the Cardholder block the card due to unsuccessful entries, it is necessary to contact the Bank.

Once the Cardholder has previously successfully completed the activation of 3D services, in the future work there can be expected the claims related to an incorrect password input by the Customer or forgotten password. If the cardholder has forgotten his password, it is necessary to select the option "*Forgotten password?*" on the screen for entering the password, where there would be offered a new activation and password creation.

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 and/or that someone else knew his password and/or personal message misrepresents, 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.

NOTE: The user has the option to enter the password three times. If in the third attempt he fails to enter the correct one, the service of the MCSC services use had been cancelled for the next 180 minutes. After the expiry of that time, the service is automatically unblocked as well as the number of attempts that is being set to three again.

These situations can be repeated three times, after which the card is permanently blocked for use in MCSC program and, to unblock it, it is necessary to contact the Bank:

- The first three (3) incorrect entries - temporary blockage for 180 minutes;
- The next three (3) incorrect entries - temporary blockage for 180 minutes;
- The last three (3) incorrect entries - permanent blockage (un-blockage required)