АТ ”ДЕРЖАВНИЙ ОЩАДНИЙ БАНК УКРАЇНИ”

Специфікація обміну повідомленнями між ПЗ Торговця та Системою Інтернет-еквайринга АТ "Ощадбанк"

ЗМІСТ

1. Загальні положення

Система Інтернет-еквайринга АТ "Ощадбанк" (Далі – Система) використовується для здійснення обміну даними між Торговцем, Покупцем та Банком при здійсненні розрахунків з використанням платіжних карток у мережі Інтернет.

Обмін інформацією між Торговцем та Системою здійснюється по протоколу HTTPS (на момент написання специфікації з використанням протоколів TLS 1.1 та TLS 1.2). Для аутентифікації Торговця та захисту даних від модифікації в процесі передачі дані захищаються з застосуванням MAC-підпису (Message Authentication Code).

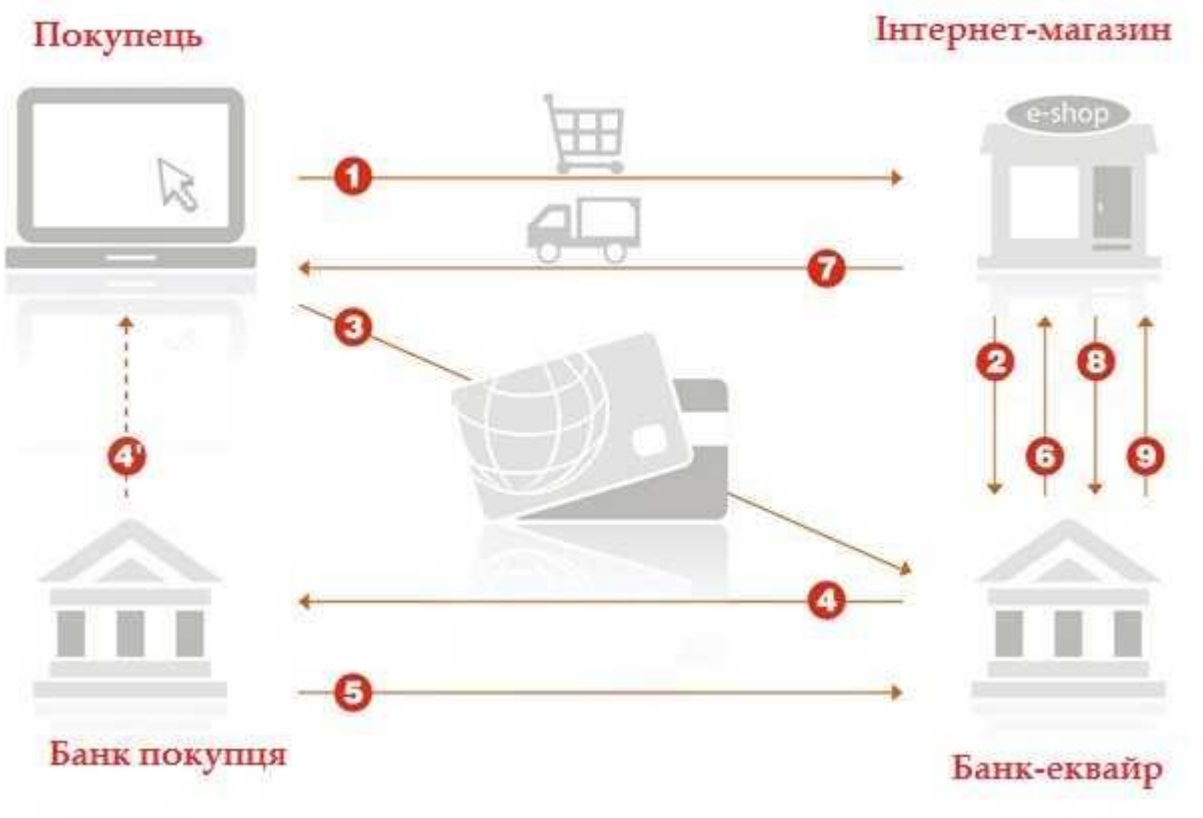
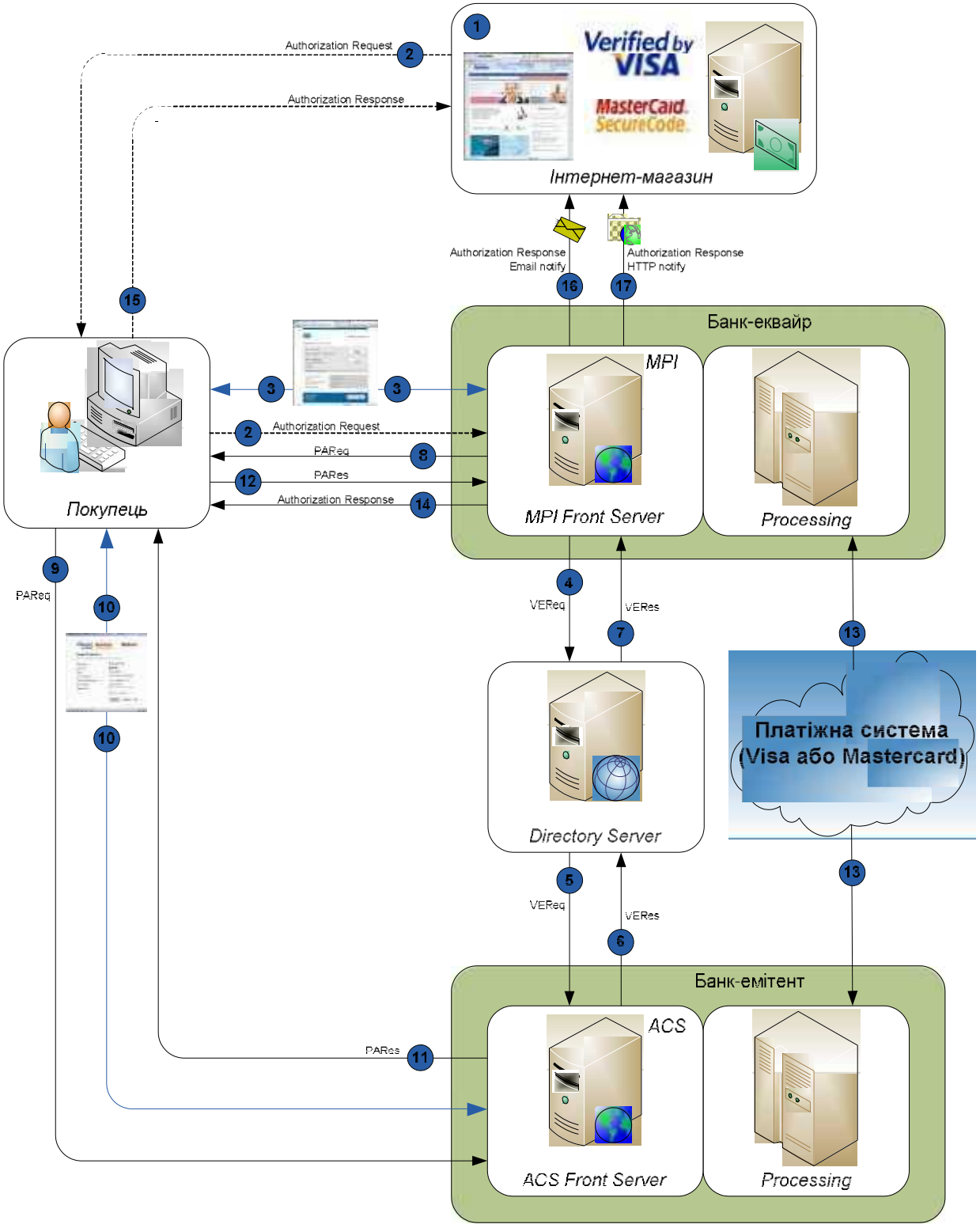


Схема проведення авторизаційного запиту по технології 3-D Secure:



1. На сайті Інтернет-магазину Покупець вибирає товар або послуги та активізує функцію оплати платіжною карткою.
2. Інтернет-магазин виконує підготовку авторизаційного запиту (Authorization Request) та надсилає його на шлюз електронної комерції Системи (MPI Front Server). Одночасно Інтернет-магазин перенаправляє Покупця на сайт Системи для введення інформації про платіжну картку.
3. MPI-сервер Системи відображає Покупцю веб-сторінку, на якій запитується інформація щодо реквізитів платіжної картки (номер картки, термін дії картки та

CVC2). Покупець вводить всі необхідні реквізити та продовжує роботу Системи натисканням кнопки "Сплатити".

4. MPI-сервер Системи, провівши попередню ідентифікацію Інтернет-магазину та перевірку MAC-підпису авторизаційного запиту, виконує запит до Directory Server`а платіжної системи (Visa чи Mastercard в залежності від типу картки Покупця) на предмет перевірки чи входить номер картки Покупця в інтервал номерів карт, що беруть участь в програмі 3-D Secure (VEReq-запит).

5. Directory Server направляє VEReq-запит на ACS-сервер банка-емітента.

6. ACS-сервер банка-емітента надає Directory Server`у платіжної системи відповідь VERes.

7. Directory Server направляє VERes-відповідь MPI-серверу Системи. У випадку коли картка бере участь у програмі 3D-Secure ця відповідь також містить URL-адресу на сайт банка-емітента.

8. MPI-сервер Системи готує запит аутентифікації Покупця (PAReq-запит).

9. MPI-сервер Системи направляє PAReq-запит через браузер Покупця разом з перенаправленням Покупця на отриману URL-адресу сайта банка-емітента.

10. ACS-сервер банка-емітента відображає Покупцю веб-сторінку на якій пропонується пройти аутентифікацію. Наприклад ввести слово-пароль.

11. Результат аутентифікації Покупця банк-емітент формує у вигляді PARes-відповіді, яка містить також криптографічні величини CAVV/AAV.

12. Банк-емітент " повертає" Покупця назад на MPI-сервер Системи разом з PARes-відповіддю.

13. Процесингова система банка-еквайра формує стандартний авторизаційний запит до платіжної системи. Цей запит містить в собі також криптографічні величини CAVV/AAV. Платіжна система передає запит далі до банка-емітента. Процесингова система банка-емітента, отримавши запит від платіжної системи, в доповнення до стандартних перевірок платоспроможності Покупця, виконує перевірку достовірності величини CAVV/AAV та формує відповідь, яка через мережу платіжної системи надходить назад до процесингу банка-еквайра.

14. Процесингова система система банку еквайера передає відповідь емітента (Authorization Response) до MPI серверу.

15. Далі MPI сервер передає відповідь до браузеру картотримача у вигляді звіту по транзакції.

16. В свою чергу інтернет магазин отримує повідомлення про стан транзакції через HTTP або email нотифікацію на адресу, вказану в конфігураційних файлах MPI-серверу.

2. Вимоги до змісту предавторизаційного запиту (PreAuthorization Request)

Предавторизаційний запит відправляється Торговцем до Системи методом "HTTP POST" та повинен містити дані, які описано в **Таблиці** 2. Після перенаправлення до Системи, Покупцю відображається сторінка „Введення реквізитів картки" де авторизаційний запит доповнюється даними по платіжній картці (**Таблиця** 1). Засобами JavaScript виконується попередня перевірка полів, що заповнюються Покупцем на предмет відповідності вимогам Специфікації.

Система на сторінці „Введення реквізитів картки" показує Покупцю наступні поля, які отримані від Торговця: Адреса сайту Торговця (MERCH_URL), Торговець (MERCH_NAME), Сума покупки (AMOUNT), Валюта покупки (CURRENCY), Опис замовлення (DESC), Номер замовлення (ORDER). Введення CVV2/CVC2 не є обов'язковим для держателів платіжних карток, які підтримають послугу 3d –Secure.

Таблиця 1 "**Поля запиту,що заповнюються Покупцем на сторінці Системи**"

Поле	**Розмір**	**Опис**
CARD	9-19	Номер платіжної картки
EXP	2	Місяць закінчення строку дії картки (цифрова 2-значна величина).
EXP_YEAR	2	Рік закінчення строку дії картки (цифрова 2-значна величина)
CVC2	3	Код верифікації картки (останні 3 цифри на стрічці для підпису на зворотній

Таблиця 2

Поле	Розмір	Опис
25(AMOUNT)	1-12	Загальна сума покупки у форматі з відокремленням копійок крапкою.
26(CURRENCY)	3	Валюта покупки: 3-х буквений код валюти (UAH)
27(ORDER)	6-20	Цифровий ідентифікаційний номер покупки. Останні 6 цифр мають бути унікальними в проміжку однієї дати (доби).
58 (DESC)	1-50	Опис покупки (кодування Win1251) 2
53(MERCH_NAME)	1-50	Назва Торговця.
55(MERCH_URL)	1-250	Адреса Сайту Торговця
29(MERCHANT)	15	Ідентифікатор Торговця присвоєний Банком.
21(TERMINAL)	8	Ідентифікатор V-POS-термінала присвоєний Банком.
37(EMAIL)	80	E-mail Торговця. Повинен відправлятись торговцем.
22(TRTYPE)	1	Має дорівнювати "**0**" 1
54(COUNTRY)	2	2-х буквений код країни магазина Торговця.
56(MERCH_GMT)	1-5	Часова зона Торговця.
47(TIMESTAMP)	14	Часовий штамп транзакції у GMT: РРРРММДДГГХХСС. Якщо часовий штамп транзакції відрізняється від часу на сервері Банку більш ніж на 500 секунд, такий запит буде відхилено Системою (з кодом RC = -20)
61(NONCE)	16-64	Випадкова величина, що генерується Програмою Торговця. Має бути заповнена випадковим чином 8-32 байтами у шістнадцятиричному форматі.
41(BACKREF)	1-250	URL-адреса Торговця на яку буде направлено відповідь з результатами по авторизаційному запиту.
44(P_SIGN)	1-256	MAC-підпис Торговця в шістнадцятиричному форматі

1. У разі успішної обробки авторизаційного запиту TRTYPE=0 кошти за операцією блокується на рахунку Покупця до моменту надходження запиту «Про завершення продажу» і списуються лише після надх-оджененя такого запиту і подальшої обробки. У випадку ненадходження запиту «Про завершення продажу» блокування коштів скасовується після спливу строку, визначеного банком – емітентом.
2. Поле DESC не повинно закінчуватися символом «пробіл»

3. Вимоги до змісту авторизаційного запиту (Authorization Request)

Після введення Покупцем даних на сторінці „Введення реквізитів картки”, Система перевіряє повний запит на відповідність його вимогам специфікації.

У разі відповідності запиту вимогам – запит направляється на обробку до авторизаційної системи банку і, при необхідності, далі до міжнародних платіжних систем.

Результат обробки авторизаційного запиту Система направляє Торговцю.

У разі успішної обробки запиту, відповідь Системи Торговцю містить набір унікальних значень (RRN, INT_REF, APPROVAL), з використанням яких Торговець повинен виконати запит „Про завершення продажу”.

Отримавши позитивну відповідь на авторизаційний запит, Торговець може надавати Покупцю замовлену послугу, або виконувати доставку товару Покупцю.

Авторизаційний запит відправляється Торговцем до Системи аналогічно редавторизаційному запиту але на відміну від останнього поле TRTYPE = “1” та повинен містити дані, які описано в **Таблиці** 3. Авторизаційний запит не потребує запиту „Про завершення продажу”.

Таблиця 3 "**Поля відповіді Системи на авторизаційний запит**"

Поле	Розмір	Опис
AMOUNT	1-12	Загальна сума покупки у форматі з відокремленням копійок крапкою.
CURRENCY	3	Валюта покупки: 3-х буквений код валюти (UAH)
ORDER	6-20	Цифровий ідентифікаційний номер покупки. Останні 6 цифр мають бути унікальними в проміжку однієї дати (доби).
DESC	1-50	Опис покупки (кодування Win1251)
MERCH_NAME	1-50	Назва Торговця.
MERCH_URL	1-250	Адреса Сайту Торговця
MERCHANT	15	Ідентифікатор Торговця присвоєний Банком.
TERMINAL	8	Ідентифікатор V-POS-термінала присвоєний Банком.
EMAIL	80	E-mail Торговця. Повинен відправлятись торговцем.
TRTYPE	1	Має дорівнювати "**1**"
COUNTRY	2	2-х буквений код країни магазина Торговця.
MERCH_GMT	1-5	Часова зона Торговця.
TIMESTAMP	14	Часовий штамп транзакції у GMT: РРРРММДДГГХХСС. Якщо часовий штамп транзакції відрізняється від часу на сервері Банку більш ніж на 500 секунд, такий запит буде відхилено Системою (з кодом RC = -20)
NONCE	16-64	Випадкова величина, що генерується Програмою Торговця. Має бути заповнена випадковим чином 8-32 байтами у шістнадцятиричному форматі.
BACKREF	1-250	URL-адреса Торговця на яку буде направлено відповідь з результатами по авторизаційному запиту.
P_SIGN	1-256	MAC-підпис Торговця в шістнадцятиричному форматі

4. Відправка Торговцем до Системи запиту „Про завершення продажу” (Sales Completion Request)

Для фактичного завершення операції та списання коштів з рахунку Покупця Торговець має відправити до Банку запит „Про завершення продажу”.

Запит „Про завершення продажу” передається програмою Торговця до Системи методом "HTTP POST".

Банк засобами Системи, відправляє до Торговця результат обробки запиту "Про завершення продажу”.

5. Формат запиту Продавця „Про завершення продажу”

Формат запиту „Про завершення продажу” наведено у **Таблиці** 4.

У цьому запиті всі поля заповнюються Торговцем. Запит "Про завершення продажу" може формуватись Торговцем як автоматично, в момент надходження позитивної відповіді на авторизаційний запит, так і ініціюватись працівником Торговця (менеджером) зі свого браузеру через деякий час після доставки товару Покупцю.

Таблиця 4 "**Набір полів повідомлення** „**Про завершення продажу**”

Поле	Розмір	Опис
TRTYPE	2	Має дорівнювати "**21**"
ORDER	6-20	Має дорівнювати значенню поля ORDER відповіді на авторизаційний запит
AMOUNT	12	Має дорівнювати значенню поля AMOUNT відповіді на авторизаційний запит
CURRENCY	3	Має дорівнювати значенню поля CURRENCY відповіді на авторизаційний запит
RRN	12	Має дорівнювати значенню поля RRN відповіді на авторизаційний запит
INT_REF	1-32	Має дорівнювати значенню поля INT_REF відповіді на авторизаційний запит
TERMINAL	8	Дорівнює значенню поля TERMINAL авторизаційного запиту
TIMESTAMP	14	Часовий штамп запиту в GMT: РРРРММДДГГХХСС.
NONCE	1-64	Випадкова величина, що генерується Програмою Торговця. Має бути заповнена випадковим чином 8-32 байтами у шістнадцятиричному форматі.
EMAIL	80	E-mail Торговця.
BACKREF	1-250	URL-адреса Торговця.
P_SIGN	1-256	MAC-підпис Торговця в шістнадцятиричному форматі

6. Відправка Торговцем до Системи запиту „Про скасування продажу” (Reversal advice)

Торговець може відправити до Банку запит „Про скасування продажу”. Наприклад у випадку, коли Торговець не може виконати замовлення Покупця (зокрема доставити товар, надати послугу) або Покупець скасовує замовлення на етапі, дозволеному Торговцем, або Покупець повертає товар Торговцю. Для операцій з TRTYPE 1 та 21 цей запит може бути відправлений впродовж 24 годин з моменту здійснення оригінальної операції, після 24 годин необхідно виконувати запит повернення.

Запит відправляється Торговцем до Системи методом "HTTP POST" та має містити набір значень параметрів, які однозначно характеризують транзакцію, отриманих у відповіді на авторизаційний запит (значення полів RRN та INT_REF). Запит використовується Банком для скасування операції або повернення коштів на картковий рахунок Покупця.

7. Формат запиту Продавця „Про скасування продажу” (Reversal advice)

Формат запиту „Про скасування продажу” складається з елементів з таблиці 4.1. Поле TRTYPE, має дорівнювати "24". Запит „Про скасування продажу” передається програмою Торговця до Системи методом "HTTP POST".

Отриманий запит перевіряється на відповідність вимогам Системи. У разі відповідності – Система направляє запит до авторизаційної системи банку і, при необхідності, далі до міжнародних платіжних систем.

Таблиця 4.1

Поле	Розмір	Опис
ORDER	6-20	Має дорівнювати значенню поля ORDER відповіді на авторизаційний запит
ORG_AMOUNT	12	Сума оригінальної транзакції
AMOUNT	12	Сумма на яку проводиться реверсал
CURRENCY	3	Валюта покупки: 3-х буквений код валюти (UAH)
RRN	12	Має дорівнювати значенню поля RRN оригінальної транзакції
INT_REF	1-32	Має дорівнювати значенню поля INT_REF оригінальної транзакції
TRTYPE	2	Має дорівнювати «24»
TERMINAL	8	Дорівнює значенню поля TERMINAL авторизаційного запиту
BACKREF	1-250	URL-адреса Торговця
TIMESTAMP	14	Часовий штамп запиту в GMT: РРРРММДДГГХХСС.
NONCE	1-64	Випадкова величина, що генерується Програмою Торговця. Має бути заповнена випадковим чином 8-32 байтами у шістнадцятиричному форматі.
P_SIGN	1-256	MAC-підпис Торговця в шістнадцятиричному форматі

8. Відправка Торговцем до Системи запиту повернення (Refund)

Торговець може відправити до Банку запит повернення. Наприклад у випадку, коли Торговець не може виконати замовлення Покупця (зокрема доставити товар, надати послугу) або Покупець скасовує замовлення на етапі, дозволеному Торговцем, або Покупець повертає товар Торговцю. Цей запит виконується лише для операцій з TRTYPE 1 та 21.

Запит відправляється Торговцем до Системи методом "HTTP POST" та має містити набір значень параметрів, які однозначно характеризують транзакцію, отриманих у відповіді на авторизаційний запит (значення полів RRN та INT_REF). Запит використовується Банком для скасування операції або повернення коштів на картковий рахунок Покупця.

9. Формат запиту Продавця повернення (Refund)

Формат запиту повернення складається з елементів з таблиці 4.2. Поле TRTYPE, має дорівнювати "14". Запит повернення передається програмою Торговця до Системи методом "HTTP POST".

Отриманий запит перевіряється на відповідність вимогам Системи. У разі відповідності – Система направляє запит до авторизаційної системи банку і, при необхідності, далі до міжнародних платіжних систем.

Таблиця 4.2

Поле	Розмір	Опис
ORDER	6-20	Має дорівнювати значенню поля ORDER відповіді на авторизаційний запит
ORG_AMOUNT	12	Сума оригінальної транзакції
AMOUNT	12	Сумма на яку проводиться реверсал
CURRENCY	3	Валюта покупки: 3-х буквений код валюти (UAH)
RRN	12	Має дорівнювати значенню поля RRN оригінальної транзакції
INT_REF	1-32	Має дорівнювати значенню поля INT_REF оригінальної транзакції
TRTYPE	2	Має дорівнювати «14»
TERMINAL	8	Дорівнює значенню поля TERMINAL авторизаційного запиту
BACKREF	1-250	URL-адреса Торговця
TIMESTAMP	14	Часовий штамп запиту в GMT: РРРРММДДГГХХСС.
NONCE	1-64	Випадкова величина, що генерується Програмою Торговця. Має бути заповнена випадковим чином 8-32 байтами у шістнадцятиричному форматі.
P_SIGN	1-256	MAC-підпис Торговця в шістнадцятиричному форматі

10. Особливості аутентифікації запитів із використанням MAC-підпису

Для аутентифікації Торговця та захисту даних від модифікації в процесі передачі, дані захищаються з застосуванням MAC (Message Authentication Code). У Системі реалізовано MAC-алгоритм HMAC_SHA1.

Усі запити, що відправляються Торговцем до Системи повинні бути підтверджені MAC-підписом.

MAC-рядок для кожного типу запиту формується зі значень полів цього запиту. Поля MAC-рядка та послідовність їх з'єднання для кожного типу запиту, визначені в **Таблиці** 5. В MAC-рядку значення кожного поля починається з коду, що у десятичному форматі визначає довжину поля. Ці значення надаються у форматі ASCII та з'єднуються у визначеному в **Таблиці** 5 порядку. У разі відсутності значення даного поля, на його місці має бути присутній знак дефісу '-' без значення довжини поля (Див. Розділ 13).

Таблиця 5 " Перелік та послідовність полів, з яких складається MAC-рядок "

Порядковий номер	Authorization Request, PreAuthorization Request	Reversal Request, Reversal Advice, Refund	Sales Completion Request	MAC-підпис відповіді серверу Банку
1	AMOUNT	ORDER	ORDER	TERMINAL
2	CURRENCY	ORG_AMOUNT	AMOUNT	TRTYPE
3	ORDER	AMOUNT	CURRENCY	ORDER
4	DESC	CURRENCY	RRN	AMOUNT
5	MERCH_NAME	RRN	INT_REF	CURRENCY
6	MERCH_URL	INT_REF	TRTYPE	ACTION
7	MERCHANT	TRTYPE	TERMINAL	RC
8	TERMINAL	TERMINAL	BACKREF	APROVAL
9	EMAIL	BACKREF	TIMESTAMP	RRN
10	TRTYPE	TIMESTAMP	NONCE	INT_REF
11	COUNTRY	NONCE		TIMESTAMP
12	MERCH_GMT			NONCE
13	TIMESTAMP			
14	NONCE			
15	BACKREF			

11. Приклад формування MAC-підпису авторизаційного запиту

Наприклад, Торговець відправляє до Системи такий авторизаційний запит, поля якого мають наступні значення: (див. Таблиця 6):

Таблиця 6 Приклад полів авторизаційного запиту.

Поле	Фактичний розмір	Опис
ORDER	6	952044
DESC	8	Test pay
MERCH_NAME	10	PAY ONLINE
MERCH_URL	20	https://payonline.ua
MERCHANT	8	20000005
TERMINAL	8	20000005
TRTYPE	1	1
COUNTRY	2	UA
MERCH_GMT	2	+3
TIMESTAMP	14	20170322173639
NONCE	32	260e07c3504b7beb9c2f7831f3dd2c9e
BACKREF	47	3ds-test.oschadbank.ua/payonline/payonline.html
AMOUNT	5	20.00
CURRENCY	3	UAH
EMAIL	17	example@email.com

Значення поля P_SIGN Торговцю необхідно розрахувати використовуючи послідовність, що визначена в Таблиці 5 для повідомлення Authorization Request, складаємо MAC-рядок:

520.003UAH69520448Test pay10PAY ONLINE20https://payonline.ua8200000058200000517example@email.com112UA2+3142017032217363932260e07c3504b7beb9c2f7831f3dd2c9e473ds-test.oschadbank.ua/payonline/payonline.html

Цей рядок є нерозривним та має довжину 204 символ.

Після створення MAC-рядка засобами Програми Торговця має бути виконаний криптографічний алгоритм для створення аутентифікаційного коду запиту (MAC-підпису).

Для даного прикладу MAC-рядка та алгоритму HMAC_SHA1 з шістнадцяти-байтним MAC-ключем: 3A428500000DAE7248B21BD6A1390C42 MAC-підпис (значення поля “P_SIGN”) має бути таким:

P_SIGN: 46c1213177754425185f20ebad76d9ec350f045f

Значення результуючого MAC-підпису має бути написано у верхньому або у нижньому регістрі. Торговець доповнює свій авторизаційний запит полем P_SIGN з розрахованим значенням.

Поле	Фактичний розмір	Опис
P_SIGN	40	46c1213177754425185f20ebad76d9ec350f045f

12. E-MAIL – нотифікація

По завершенні обробки запиту система формує відповідь у вигляді електронного листа, та відсилає цей лист на вказану в налаштуваннях EMAIL адресу.

Характеристики листа:

- тема листа має формат: Order #%27 - %3
- тіло листа має формат:

  Function=TransRespon
  Result=0
  RC=00
  Amount=50.00
  Currency=UAH
  Order=210513000201
  RRN=3**********8
  IntRef=3***************B
  AuthCode=02***0
  URL-адреса Торговця на яку буде направлено відповідь з результатами по авторизаційному запиту.

В процесі експлуатації Системи формат листа може змінюватись без зменшення його
інформативності та зі збереженням загальних принципів автоматичної обробки листа Торговцем.

13. HTTP-нотифікація

По завершенні обробки запиту система формує відповідь у вигляді електронного повідомлення та надсилає його безпосередньо Торговцю через HTTP (або HTTPS) методом POST на адресу, що вказана в конфігураційних файлах системи для конкретного Інтернет-магазину Торговця. Приклад повідомлення має наступний вигляд:

Function=TransRespon
Result=0
RC=00
Amount=50.00
Currency=UAH
Order=210513000201
RRN=3**********8
IntRef=3**********B
AuthCode=02***0

URL-адреса Торговця на яку буде направлено відповідь з результатами по авторизаційному запиту.

Для можливості отримання додаткового повідомлення, Торговець повинен надати технічним працівникам Банку наступні параметри:

- Host - IP-адресу сервера Торговця;
- Port - порт сервера Торговця;
- HTTP_HOST - HTTP-хост торговця;
- HTTP_URL - URL до скрипта обробки відповіді Торговця;

Приклад:
Host=193.227.119.19
Port=80
HTTP_HOST="test-shop.oschad.com"
HTTP_URL="/reply-auto.php"

14. Тестування та підключення V-POS-термінала.

Перед початком роботи з промисловим сервером Системи, розробник Інтернет-магазину Торговця повинен виконати роботи по програмуванню інтерфейсу взаємодії з сервером Системи. Для виконання тестових запитів використовується тестовий сервер системи Інтернет-еквайринга Ощадбанку.

Мета тестування – відпрацювати усі основні процедури роботи V-POS-термінала з тестовим сервером банку.

• Перевірити правильність реалізації MAC-алгоритму HMAC_SHA1;

• Відпрацювати авторизаційний запит (TRTYPE = 0) та відповідь сервера на цейзапит (обов'язково перевіряти MAC-підпис у відповіді);

• Відпрацювати запит завершення продажу (TRTYPE = 21) та відповідь сервера нацей запит (обов'язково перевіряти MAC-підпис у відповіді);

• Відпрацювати запит скасування продажу (TRTYPE = 24) та відповідь сервера нацей запит (обов'язково перевіряти MAC-підпис у відповіді);

• Вміти працювати з відповідями сервера на e - ma i l (обов'язково перевірятиMAC-підпис у відповіді).

Параметри тестування:

Тестовий ідентифікатор TERMINAL:	40000007
Тестовий ідентифікатор MERCHANT:	30000007
Тестовий MAC-ключ:	3A428500000DAE7248B21BD6A1390C42
Тестовий сервер Системи:	https://3ds-test.oschadbank.ua/cgi-bin/cgi_link

Криптографічний ключ потрапляє до співробітників Торговця у вигляді двох 16-ти байтних компонент відповідальним Security – офіцерам (По одній компоненті кожному).

Key Component 1:

Hex Value of Component: 0EEA9B428277300D52E56167688187D2

Key Component 2:

Hex Value of Component: 34A81E42827A9E7F1A577AB1C9B88B90

Після чого Торговець в своїй системі дає змогу кожному з офіцерів вбити значення своєї компоненти. Далі система Торгівця між двома отриманими компонентами виконую операцію XOR, після чого зберігає результуюче значення MAC ключа для підпису транзакцій. Важливо!!! – Значення ключа має довжину 32 символи або 16 байт. Якщо після операції XOR між двома 16-ти байтними компонентами на початку значення ключа(з лівого боку) в розрядах отримуємо значення що дорівнюють 0, важливо не втратити ці значення, наприклад є 2 компоненти:

Component1:AA11223344556677889 9AABBCCDDEEFF
Component2:AA00000000000000000000000000000000
XOR_Result :00112233445566778899AABBCCDDEEFF
Тобто після операції XOR результуюче значення ключа має бути 16 байт.

Приклад коду PHP для обчислення результуючого значення ключа:

```
<?php
   $s1 = '0EEA9B428277300D52E56167688187D2';
   $s2 = '34A81E42827A9E7F1A577AB1C9B88B90';
   $x = bin2hex(pack('H*',$s1) ^ pack('H*',$s2));
echo $x;
?>
```

Результатом виконання цього коду буде розраховане значення ключа:
3A428500000DAE7248B21BD6A1390C42

Приклад Алгоритму HMAC_SHA1 в мові програмування PHP для обчислення поля P_SIGN з MAC рядку:

```
<?php
$data = "520.003UAH69520448Test pay10PAY
ONLINE20https://payonline.ua8200000058200000517example@email.com112UA2+3142017032
217363932260e07c3504b7beb9c2f7831f3dd2c9e473ds-
test.oschadbank.ua/payonline/payonline.html";
$key = pack("H*", '3A428500000DAE7248B21BD6A1390C42');
$res = hash_hmac('sha1', $data, $key);
echo $res;
?>
```

Результатом виконання цього коду буде розраховане значення поля P_SIGN:
46c1213177754425185f20ebad76d9ec350f045f

15. Коди відповіді Системи

Таблиця 8 "**Значення кодів відповіді Системи** (**поле** RC) **при** ACTION=3 (**помилка в обробці транзакції**)"

RC	Опис коду	
-1	Обов'язкове поле в запиті незаповнене	Mandatory field is empty
-2	Запит не відповідає вимогам специфікації	Bad CGI request
-3	Комунікаційний сервер не відповідає або невірний формат файла відповіді	No or Invalid response received
-4	Відсутній зв'язок з комунікаційним сервером	Server is not responding
-5	Зв'язок з комунікаційним сервером не конфігуровано	Connect failed
-6	Помилка конфігурації e-Gateway	Configuration error
-7	Помилкова відповідь від комунікаційного сервера	Invalid response
-8	Помилка в полі "Card number"	Error in card number field
-9	Помилка в полі "Card expiration date"	Error in card expiration date field
-10	Помилка в полі "Amount"	Error in amount field
-11	Помилка в полі "Currency"	Error in currency field
-12	Помилка в полі "Merchant ID"	Error in merchant terminal field
-13	IP-адреса не така як очікується	Unknown referrer
-15	Помилка в полі "RRN"	Invalid Retrieval reference number
-16	Термінал тимчасово заблоковано, спробуйте ще раз.	Terminal is locked, please try again
-17	Доступ заборонено	Access denied
-18	Помилка в CVC2 або в описі CVC2	Error in CVC2 or CVC2 Description fields
-19	Помилка аутентифікації	Authentication failed
-20	Перевищено час проведення транзакції	Expired transaction
-21	Дублікат транзакції	Duplicate transaction
-22	Помилка при аутентифікації клієнта	Error in the request information required for client identification

Таблиця 9 "**Значення кодів відповіді по транзакції** (**поле** RC) **при** ACTION=0,1,2"

RC	Опис коду	
00	Підтвердити (успішне виконання)	Approved
01	Зверніться до емітента картки	Call your bank
02	Зверніться до емітента картки - спеціальні умови	Call your bank
03	Відмовити, підприємство не приймає даний вид карт	Invalid merchant
04	Відмовити, картка заблокована	Your card is restricted
05	Відмовити, операція відхилена	Transaction declined
06	Помилка - повторіть запит	Error - retry
07	Відмовити, картка заблокована	Your card is disabled
08	Необхідна додаткова ідентифікація	Additional identification required
09	Запит в процесі обробки	Request in progress
10	Підтвердити для часткової суми операції	Partially approved
11	Підтвердити для особливо важливої персони (VIP)	Approved (VIP)
12	Відмовити, невідомий тип операції	Invalid transaction
13	Відмовити, некоректна сума операції	Invalid amount
14	Відмовити, картку не знайдено	No such card
15	Відмовити, емітент не існує	No such card/issuer
16	Підтвердити, поновити третю доріжку картки	Approved, update track 3
17	Відмовити, відмова користувача	Customer cancellation
18	Помилка, неприпустимий код відповіді	Customer dispute
19	Відмовити, повторити операцію	Re-enter transaction
20	Помилка, неприпустимий код відповіді	Invalid response

21	Помилка, неприпустимий код відповіді	No action taken
22	Помилка в роботі системи	Suspected malfunction
23	Відмовити, неакцептовані витрати операції	Unacceptable fee
24	Помилка, неприпустимий код відповіді	Update not supported
25	Помилка, неприпустимий код відповіді	No such record
26	Помилка, неприпустимий код відповіді	Duplicate update/replaced
27	Помилка, неприпустимий код відповіді	Field update error
28	Помилка, неприпустимий код відповіді	File locked out
29	Помилка, зв'яжіться з центром обробки	Error, contact acquirer
30	Відмовити, помилка в форматі запиту	Format error
31	Відмовити, емітент тимчасово відключився	Issuer signed-off
32	Часткове закінчення	Completed partially
33	Відмовити, термін дії картки вичерпано	Expired card
34	Відмовити, підозра у шахрайстві	Suspected fraud
35	Відмовити, підприємству зв'язатись з емітентом	Acceptor contact acquirer
36	Відмовити, картка блокована	Restricted card
37	Відмовити, зв'яжіться зі своїм банком	Call your bank
38	Відмовити, перевищено кількість спроб вводу ПІН	PIN tries exceeded
39	Відмовити, кредитного рахунку немає	No credit account
40	Відмовити, функція не підтримується	Function not supported
41	Відмовити, картка загублена	Lost card
42	Відмовити, універсального рахунку немає	No universal account
43	Відмовити, картку викрадено	Stolen card
44	Відмовити, інвестиційного рахунку немає	No investment account
45	Помилка, неприпустимий код відповіді	Reserved
46	Помилка, неприпустимий код відповіді	Reserved
47	Помилка, неприпустимий код відповіді	Reserved
48	Помилка, неприпустимий код відповіді	Reserved
49	Помилка, неприпустимий код відповіді	Reserved
50	Помилка, неприпустимий код відповіді	Reserved
51	Відмовити, недостатньо коштів	Not sufficient funds
52	Відмовити, чекового рахунку немає	No chequing account
53	Відмовити, ощадного рахунку немає	No savings account
54	Відмовити, термін дії картки вичерпано	Expired card
55	Відмовити, некоректний ПІН	Incorrect PIN
56	Відмовити, інформація про картку відсутня	No card record
57	Відмовити, операцію не дозволено	Not permitted to client
58	Відмовити, невідомий тип картки	Not permitted to merchant
59	Відмовити, невірний CVC або термін дії картки	Suspected fraud
60	Відмовити, підприємству зв'язатись з центром обробки	Acceptor call acquirer
61	Відмовити, перевищено ліміт суми операцій	Exceeds amount limit
62	Відмовити, картка блокована	Restricted card
63	Помилка, порушення безпеки системи	Security violation
64	Відмовити, невірна оригінальна сума операції	Wrong original amount
65	Відмовити, перевищено ліміт повторень операції	Exceeds frequency limit
66	Відмовити, підприємству зв'язатись з центром обробки	Acceptor call acquirer
67	Відмовити, якщо операція в АТМ	Pick up at ATM
68	Помилка, немає відповіді у відведений час	Reply received too late
69	Помилка, неприпустимий код відповіді	Reserved
70	Помилка, неприпустимий код відповіді	Reserved
71	Помилка, неприпустимий код відповіді	Reserved
72	Помилка, неприпустимий код відповіді	Reserved
73	Помилка, неприпустимий код відповіді	Reserved
74	Помилка, неприпустимий код відповіді	Reserved
75	Відмовити, перевищено кількість спроб вводу ПІН	PIN tries exceeded
76	Відмовити, невірний ПІН, перевищено кількість спроб	Wrong PIN,tries exceeded
77	Помилка, неприпустимий код відповіді	Wrong Reference No.

78	Помилка, неприпустимий код відповіді	Reserved
79	Помилка, вже відреверсовано	Already reversed
80	Відмовити, помилка авторизаційної мережі	Network error
81	Відмовити, помилка зовнішньої мережі	Foreign network error
82	Відмовити, тайм-аут мережі зв'язку / Невірний CVV	Time-out at issuer
83	Відмовити, помилка операції	Transaction failed
84	Відмовити, перевищено час преавторизації	Pre-authorization timed out
85	Відмовити, необхідна перевірка рахунку	Account verification required
86	Відмовити, перевірка ПІН неможлива	Unable to verify PIN
87	Помилка, неприпустимий код відповіді	Reserved
88	Відмовити, помилка криптографії	Cryptographic failure
89	Відмовити, помилка аутентифікації	Authentication failure
90	Відмовити, повторіть через деякий час	Cutoff is in progress
91	Відмовити, емітент чи вузол комутації недоступний	Issuer unavailable
92	Відмовити, неможлива адресація запиту	Router unavailable
93	Відмовити, порушення закону	Violation of law
94	Відмовити, повторний запит	Duplicate transmission
95	Відмовити, помилка узгодження	Reconcile error
96	Відмовити, помилка в роботі системи	System malfunction
97	Помилка, неприпустимий код відповіді	Reserved
98	Помилка, неприпустимий код відповіді	Reserved
99	Помилка, неприпустимий код відповіді	Reserved

16. **Реквізити**

Адреса сервера **промислової** Системи:

https://3ds.oschadbank.ua/cgi-bin/cgi_link

Адреса сервера тестової Системи:

https://3ds-test.oschadbank.ua/cgi-bin/cgi_link
Робота з тестовою базою можлива в обмежений проміжок часу та після узгодження дати тестового слоту з працівниками процегингового центру.

Тестові картки:

CARD	YY/MM	CVV2	
Ощадбанк:			
4790700000150962	20/01	193	3D (выбрать 3-D Secure пароль и ввести «11111»)
4790700000142837	20/01	453	без 3D
5274100000226882	19/11	560	

VISA (тільки для тестування з 3D, працюють тільки для при тимчасовому налаштуванні співробітником VISA):

4012001037141112	27/12	212
4012001037167778	27/12	990

Контактні телефони Банку:

Підрозділ безпеки Банку…… _____

Контакт-центр Банку…….. _____

Менеджер Клієнта..... _____