Специфікація обміну повідомленнями між ПЗ Організації та Системою Інтернет-еквайринга АТ "Укрексімбанк"

Редакція від 06.01.2017

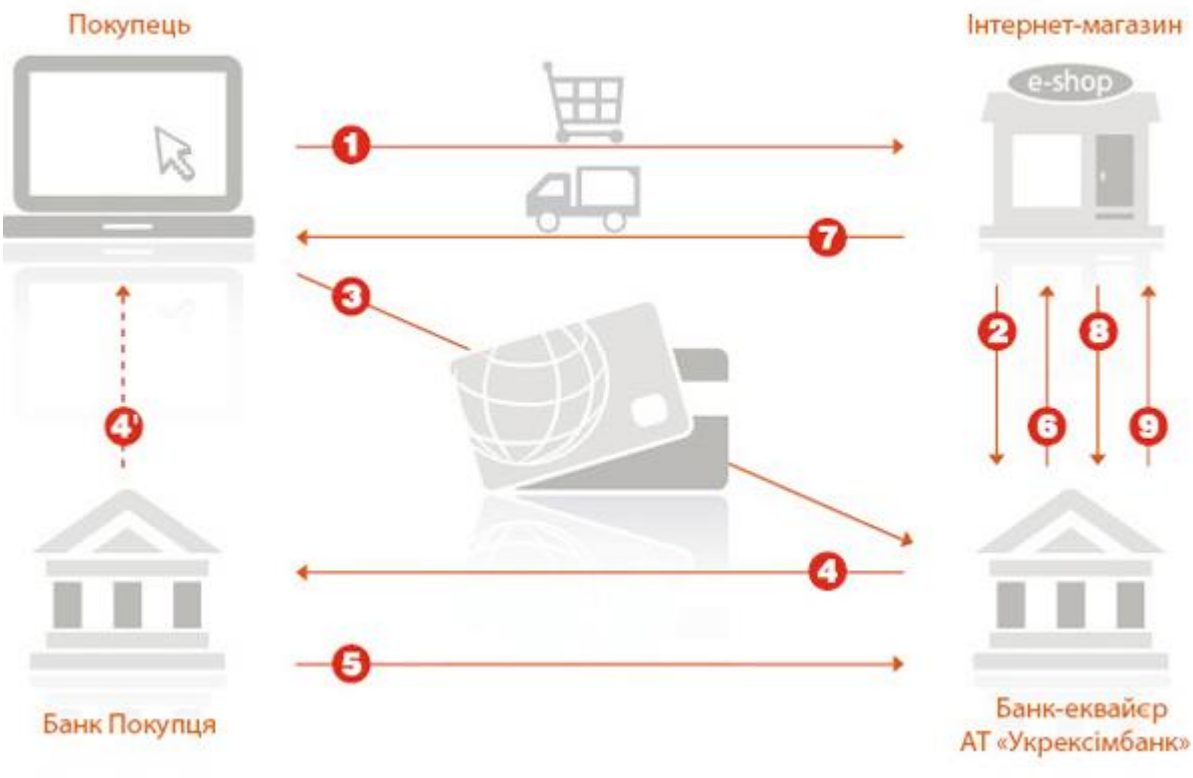
http://www.eximb.com/ia/spec/

ЗМІСТ

1. Загальні положення

Система Інтернет-еквайринга АТ "Укрексімбанк" (Далі - Система) використовується для здійснення обміну даними між ПЗ Організації, яка заключила договір про розрахункове обслуговування за операціями з продажу товарів (Далі - Торговець), Покупцем та Банком при здійсненні розрахунків з використанням платіжних карток у мережі Інтернет. Обмін даними між Торговцем і Банком здійснюється відповідно до вимог стандарту PCI DSS (Payment Card Industry Data Security Standard).

Схема №1. Взаємодія між Торговцем, Покупцем та Банком у випадку введення Покупцем даних про платіжну картку на веб-сторінці Банку:



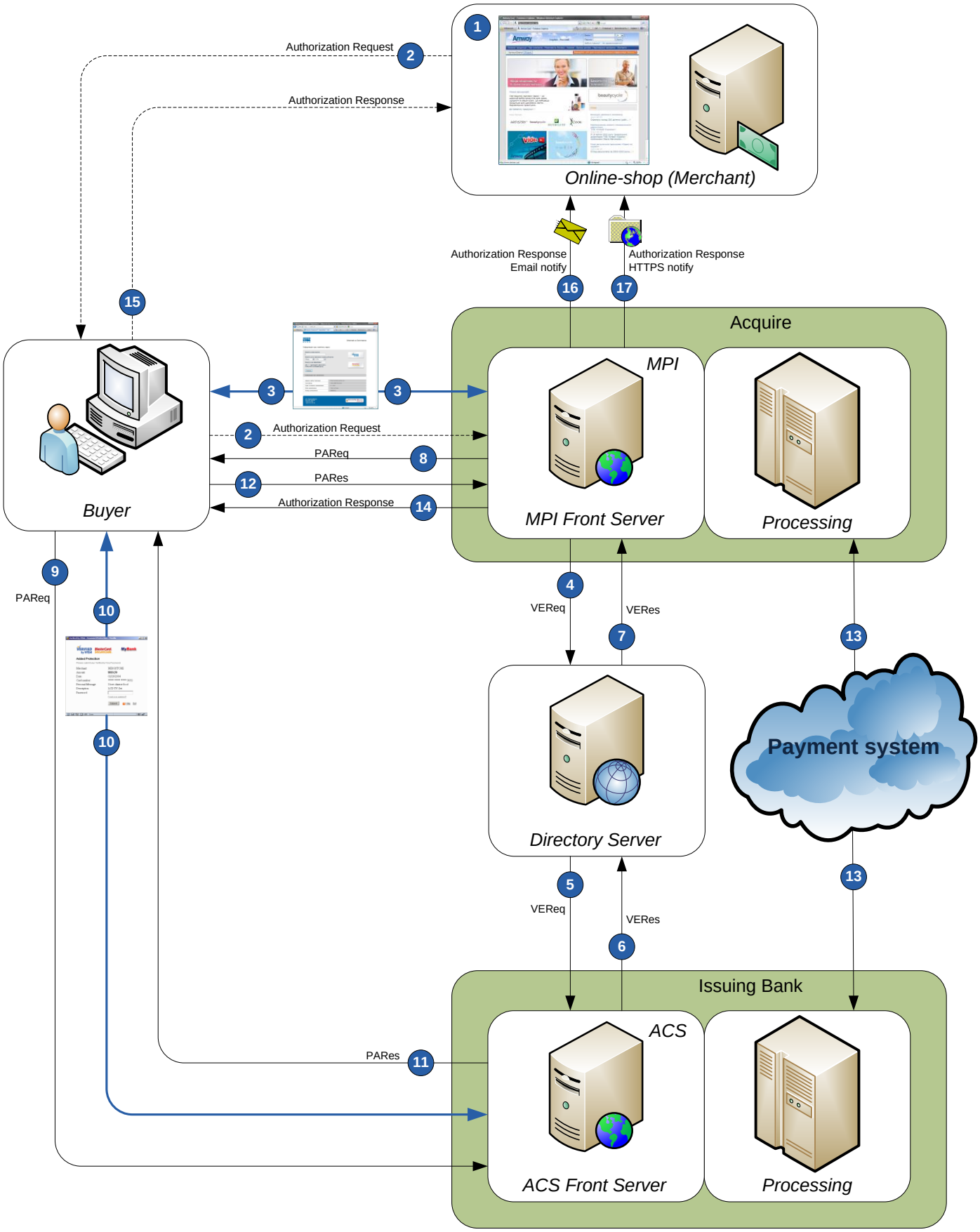
Опис схеми.

1. Покупець, користувач картки, на сайті Інтернет-магазину наповнює «корзину» товарами чи послугами та ініціює процедуру оплати натисканням кнопки «Сплатити».
2. Інформація про замовлення передається з Інтернет-магазину до Банку-еквайєру Укрексімбанк.
3. Покупець автоматично перенаправляється на захищену веб-сторінку Укрексімбанку, де вводить дані про свою платіжну картку: її номер, термін дії та CVV2.
4. Укрексімбанк перевіряє наявність коштів на картковому рахунку для здійснення покупки.

4`. У разі, якщо картка Покупця зареєстрована для проведення електронних платежів за протоколом 3-D Secure, Банк Покупця може запропонувати ввести додатковий пароль для перевірки.

5. При наявності коштів на картковому рахунку Покупця резервується необхідна сума для оплати замовлення.
6. Укрексімбанк передає до Інтернет-магазину результат перевірки для підтвердження або відхилення замовлення Покупця.
7. У разі позитивного результату Інтернет-магазин виконує замовлення Покупця.
8. Інтернет-магазин відправляє в Укрексімбанк повідомлення про виконання замовлення.
9. Протягом наступного банківського дня Укрексімбанк проводить розрахунок з Інтернет-магазином за наданий товар або послугу.

Схема №2. Проведення авторизаційного запиту по технології 3-D Secure у випадку введення Покупцем даних про платіжну картку на веб-сторінці Банку:



Опис схеми

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 на предмет перевірки чи входить номер картки Покупця в інтервал номерів карт, що приймають 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. 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. MPI-сервер Системи, на основі результатів проведення авторизаційного запиту до банка-емітента, формує відповідь (Authorization Response) Інтернет-магазину.
15. Відповідь передається через браузер картотримача разом з перенаправленням картотримача на сайт Інтернет-магазину.
16. Як додатковий сервіс, Інтернет-магазину може надсилатись Authorization Response через email-шлюз на адресу, вказану в авторизаційному запиту.
17. Як додатковий сервіс, Інтернет-магазину може надсилатись Authorization Response через HTTP на адресу, вказану в конфігураційних файлах MPI-серверу для конкретного Інтернет-магазину.

2. Рекомендації щодо організації роботи

Для забезпечення роботи віртуального термінала (V-POS-термінала) Торговець повинен реалізувати три типа запитів до Системи.

- Авторизаційній запит (Authorization Request).
- Запит завершення продажу (Sales Completion Request).
- Запит скасування продажу (Reversal advice).

Обмін інформацією між Торговцем та Системою здійснюється по протоколу HTTPS. Для аутентифікації Торговця та захисту даних від модифікації в процесі передачі дані захищаються з застосуванням MAC-підпису (Message Authentication Code).

Для перевірки платоспроможності Покупця Торговець повинен надіслати до Системи авторизаційний запит (разом з перенаправленням Покупця на сторінку Системи). У разі успішної обробки авторизаційного запиту кошти за операцією блокуються на рахунку Покупця банком-емітентом до моменту надходження запиту завершення продажу і списуються лише після надходження такого запиту і подальшої обробки. У випадку ненадходження запиту завершення продажу блокування коштів скасовується після спливу строку, визначеного банком-емітентом [1].

Сумісно з Покупцем Торговець проводить тільки авторизаційний запит. Позитивна відповідь на авторизаційний запит свідчить про те, що у Покупця на рахунку є потрібна для оплати товару/послуг сума, а також те, що ця сума вже заблокована для подальшого перерахування на рахунок Торговця і не може бути використана Покупцем для інших цілей.

У разі отримання позитивної відповіді на авторизаційний запит, Торговець може надавати Покупцю замовлений товар чи послуги. На цьому етапі завершується процес оплати товару/послуги між Торговцем та Покупцем.

Наступний етап – перерахування заблокованої авторизаційним запитом суми з рахунку Покупця на рахунок Торговця. Цей етап ініціюється Торговцем шляхом надсилання запиту завершення продажу (Sales Completion Request).

⚠ Запит завершення продажу Торговець виконує без участі Покупця. Про результати виконання запиту Торговець не повинен інформувати Покупця. Запит завершення продажу відноситься тільки до взаємовідношень між Торговцем та Системою і ніяким чином не стосується Покупця.

⚠ Отримання негативної відповіді на запит завершення продажу, при умові отримання позитивної відповіді на авторизаційний запит, не повинно призводити до відмови в обслуговуванні Покупця. Фактично негативну відповідь на запит завершення продажу Торговець може отримати тільки у разі неправильного формування запиту, або у разі невірного заповнення полів запиту. У разі отримання негативної відповіді на запит завершення продажу, Торговець повинен проаналізувати поля ACTION та RC відповіді (з застосуванням Таблиці 10 та Таблиці 11 з цієї Специфікації) та на основі зроблених висновків про причини відмови, відкоригувати значення полів запиту та повторити запит завершення продажу ще раз.

На будь який правильно сформований запит від Торговця Система надсилає відповідь з результатами обробки отриманого запиту. Відповідь надсилається трьома різними способами:

- **Спосіб 1**. Відповідь у вигляді html-шаблону з java-скриптом направляється на адресу, з якої прийшов запит, з подальшою переадресацією даних на адресу, вказану в полі BACKREF обробленого запиту.

[1] ⚠ Якщо Договором між Банком та Торговцем передбачено, що Торговець використовує схему у якій не вимагається виконання запиту завершення продажу, то у такому випадку Система відразу виконує усі необхідні дії для підготовки до процедури зарахування коштів на рахунок Торговця.

- **Спосіб 2**. Відповідь методом POST направляється безпосередньо на сервер Торговця, адресу якого на етапі підключення Торговець повідомив технічним працівникам Банку (HTTPS-нотифікація).
- **Спосіб 3**. Відповідь у вигляді листа електронної пошти направляється на адресу, вказану в полі EMAIL обробленого запиту (email-нотифікація).

⚠ ***Увага!*** Під час проведення авторизаційного запиту, Система отримує остаточний набір даних з адреси Покупця (Покупець доповнює запит Торговця даними своєї картки). Тому і відповідь на авторизаційний запит буде направлена на адресу Покупця. Оброблюючи html-шаблон з відповіддю, браузер Покупця виконує java-скрипт і перенаправляє Покупця на адресу з поля BACKREF разом з даними відповіді. Програма Торговця може приймати і обробляти дані відповіді, що отримані цим способом. Але слід врахувати той факт, що на етапі виконання java-скрипта браузер Покупця може «зависнути» через можливі певні обмеження в роботі з java, або через роботу антивірусної програми, встановленої на комп'ютері тощо.

Для уникнення подібної ситуації ***рекомендується у якості основного способу отримання відповідей від Системи використовувати Спосіб 2 – https-нотифікацію***. У такому разі виключається неотримання відповіді Торговцем через проблеми з браузером на комп'ютері Покупця. Спосіб 1 залишається лише для повернення картотримача на сервер Торговця (на адресу BACKREF) і у разі «зависання» браузера не призведе до будь яких наслідків окрім неповернення Покупця на сервер магазину. Покупець може самостійно повернутись на сервер Торговця та перевірити результат виконання запиту.

Спосіб 3 – email-нотифікація залишається як резервний і може використовуватись Торговцем лише для ручного аналізу спірних ситуацій.

⚠ Після отримання відповіді від Системи, Торговець повинен проаналізувати отримані дані, *обов'язково* перевірити MAC-підпис в отриманому повідомленні, та проінформувати Покупця про результат проведеної операції.

Для відображення Покупцю інформації про результат обробки авторизаційного запиту рекомендується використовувати значення наступних полів відповіді:

<u>Для відповіді, у якій поле ACTION = 0, 1, 2[2]:</u>

Ідентифікаційний номер покупки	- значення поля ORDER;
Сума та валюта покупки	- значення полів AMOUNT та CURRENCY;
Код відповіді банку	- значення поля RC;
Інтерпретація коду відповіді	- значення з Таблиці 11;
Код авторизації, що надав банк Покупця	- значення поля APPROVAL;
Ідентифікаційний номер транзакції	- значення поля RRN.

<u>Для відповіді, у якій поле ACTION = 3:</u>

В такому разі достатньо просто відобразити Покупцю наступну інформацію (як приклад): "*Вибачте, з технічних причин запит не було оброблено. Будь ласка спробуйте здійснити оплату ще раз, або зверніться до адміністратора інтернет-магазина.*"

Усі значення полів, які Система прислала у відповідь на авторизаційний запит, Торговець повинен зберегти в своїй базі даних. Ці дані знадобляться при виконанні операції завершення продажу, або скасування продажу, а також можуть бути корисні Торговцю при аналізі спірних операцій.

⚠ Програмне забезпечення Торговця повинно надавати відповідальному менеджеру (адміністратору) Торговця можливість здійснювати перегляд усіх результатів авторизаційний запитів. Менеджер (адміністратор) Торговця повинен мати змогу виконати операцію "Завершення продажу" (якщо така операція не виконується автоматично відразу після отримання відповіді на авторизаційний запит), або операцію "Скасування продажу" для обраного успішного результату авторизаційного запиту.

[2] Якщо отримано відповідь, у якій поле ACTION = 6, 7 або 8, необхідно доповнити інформацію для покупця словами «ПОВТОРНИЙ ЗАПИТ».

3. Вимоги до змісту авторизаційного запиту (Authorization Request)

Авторизаційний запит відправляється Торговцем до Системи методом "HTTP POST" та повинен містити дані, які описано в **Таблиці 1**. У разі необхідності авторизаційний запит може містити галузеві доповнення (*Див. Розділ 3.1 та Розділ 3.1.1*).

Таблиця 1 "Поля запиту, що генеруються Торговцем" (* – обов'язкове для заповнення поле)

Поле	Формат	Опис
TRTYPE	N(1) *	Має дорівнювати значенню '**0**' у разі роботи по схемі, яка вимагає '**Sales Completion Request**', або значенню '**1**' у разі роботи по схемі без '**Sales Completion Request**'.
AMOUNT	N(1..12) *	Загальна сума покупки у форматі з відокремленням копійок крапкою (відображається на сторінці «Введення реквізитів картки»).
CURRENCY	S(3) *	Валюта покупки: 3-х буквений код валюти. Має дорівнювати значенню '**UAH**' (відображається на сторінці «Введення реквізитів картки»).
ORDER	N(6..20) *	Цифровий ідентифікаційний номер операції (покупки). Відображається на сторінці «Введення реквізитів картки». ⚠ Останні 6 цифр мають бути унікальними в проміжку однієї дати (доби).
DESC	S(1..50) *	Опис покупки (відображається на сторінці «Введення реквізитів картки»). ⚠ У разі використання кирилиці необхідне кодування Win-1251.
DELIVERY	S(1)	Метод доставки товару. '**S**' – електронна доставка, '**T**' – фізична доставка. У разі відсутності значення поля метод доставки невідомий.
MERCH_NAME	S(1..50) *	Назва Торговця (відображається на сторінці «Введення реквізитів картки»).
MERCH_URL	S(1..250) *	Адреса Сайту Торговця (відображається на сторінці «Введення реквізитів картки»).
MERCHANT	S(15) *	Ідентифікатор Торговця присвоєний Банком.
TERMINAL	S(8) *	Ідентифікатор V-POS-термінала присвоєний Банком.
EMAIL	S(1..80)	E-mail Торговця для отримання додаткового повідомлення про результат виконання транзакції (*Див. Розділ 13*).
LANG	S(3)	Мова сторінок Системи. Може набувати значення '**UKR**', '**RUS**', '**ENG**'. Від значення цього поля залежить якою мовою Покупцю будуть показані сторінки Системи. У разі відсутності поля використовується значення '**UKR**'.
COUNTRY	S(2)	2-х буквений код країни магазина Торговця. Заповнюється, якщо Торговець знаходиться в іншій країні ніж Банк.
MERCH_GMT	sN(1..5)	Часова зона Торговця (наприклад -3). Заповнюється якщо Торговець знаходиться в іншій часовій зоні ніж Банк.
TIMESTAMP	N(14) *	Часовий штамп транзакції у **GMT**: РРРРММДДГГХХСС. ⚠ Якщо часовий штамп транзакції відрізняється від часу Системи більш ніж на **500 секунд**, такий запит буде відхилено (з кодом **RC = —20**).
NONCE	HN(16..64) *	Випадкова величина. Має бути заповнена випадковим чином у шістнадцятиричному форматі.
BACKREF	S(1..250) *	URL-адреса Торговця на яку буде направлено відповідь з результатами по авторизаційному запиту. Також на цю адресу перенаправляється Покупець з сайту Системи.
CARDMAIL	S(1..80)	E-mail Покупця на який буде направлено лист з результатом виконання авторизаційного запиту (квитанція про оплату).
ADDSTR1 ADDSTR2 ADDSTR3	S(1..250)	Три текстових поля, які не обробляються Системою. Значення цих полів повертається Торговцю у відповіді.
P_SIGN	HN(1..256) *	MAC-підпис запиту (*Див. Розділи 14 та Розділ 15*).

Опис формату полів:

N – числове поле, яке містить лише десяткові цифри 0..9.

HN – числове поле, яке містить лише шістнадцятирічні цифри 0..9, A..F.

sN – числове знакове поле, яке містить символ знаку '+' або '–' та десяткові цифри 0..9.

S – текстовий рядок, який містить символи алфавіту, цифри та спеціальні символи.

⚠ Для символів кирилиці використовувати кодування Win1251.

⚠ ***Увага!*** Разом з даними авторизаційного запиту Торговець повинен перенаправити Покупця на сторінку Системи. В іншому випадку аутентифікація картотримача банком-емітентом при проведенні транзакції по технології 3-D Secure неможлива.

Після перенаправлення до Системи, Покупцю відображається сторінка «Введення реквізитів картки». На цій сторінці Покупець доповнює авторизаційний запит даними по платіжній картці (**Таблиця 2**) та продовжує операцію натисканням кнопки "Сплатити".

Таблиця 2 "Поля запиту, що заповнюються Покупцем" (* – обов'язкове для заповнення поле)

Поле	Формат	Опис
CARD	N(9..19) *	Номер платіжної картки.
EXP	N(2) *	Місяць закінчення строку дії картки (цифрова 2-значна величина).
EXP_YEAR	N(2) *	Рік закінчення строку дії картки (цифрова 2-значна величина).
CVC2	N(4) *	Код верифікації картки.
На сторінці «Введення реквізитів картки» можуть додатково відображатись наступні поля (визначається індивідуально для кожного термінала по попередній домовленості між Банком та Торговцем):		
CARDNAME	S(3..35)	Ім'я власника картки, яке зазначене на платіжній картці. Це поле не обробляється Системою, а повертається Торговцю у відповіді.

⚠ Якщо Договором між Банком та Торговцем передбачено, що Покупець вводить дані по платіжній картці на сайті Торговця, авторизаційний запит, який надсилається Торговцем до Системи, має містити повний набір даних з **Таблиці 1** і **Таблиці 2**. У разі надходження такого запиту та відповідних налаштуваннях термінала, Система відразу починає обробку отриманого авторизаційного запиту без відображення сторінки «Введення реквізитів картки».

3.1.Галузеві доповнення авторизаційного запиту

В деяких випадках на вимогу платіжних систем Торговець повинен надсилати додаткову інформацію відносно операції оплати.

Такі доповнення можуть знадобитись при розгляді скарг Торговця чи Покупця, а також для застосування змін в правилах клірингу та розрахунків з платіжними системами.

Таблиця 3 "Типи галузевих доповнень"

Поле	Формат	Опис
ADDENDUM	S(2)	У разі присутності цього поля, Система оброблює додаткові поля (Див. опис додаткових полів у розділі 3.1.1.). В даний час визначені наступні типи галузевих доповнень: "**AI**" - Airline, Passenger Itinerary.

3.1.1. Додаткові поля для галузевих доповнень типу "AI"

Для авіакомпаній, які продають авіаквитки, використовується значення ADDENDUM='AI'. Торговець повинен надавати наявну інформацію по операції оплати.

Таблиця 4 "Основна інформація по квитку" (* – обов'язкове для заповнення поле)

Поле	Формат	Опис
AI.TICKET.NAME	S(20) *	Ім'я та прізвище пасажира.
AI.TICKET.NUMBER	S(13) *	Номер квитка.
AI.TICKET.RESTRICTED	S(1)	Вказує чи є обмеження на повернення квитка. **0** – немає обмежень. **1** – квиток не підлягає поверненню.
AI.TICKET.SYSTEM	S(4)	Вказує, яка автоматизована система бронювання квитків використовується. DATS = Delta, SABR = Sabre, etc.
AI.TICKET.AGENCY.CODE	S(8)	Код туристичного агентства.

4. Обробка авторизаційного запиту Системою

Після отримання повного авторизаційного запиту, Система перевіряє його на відповідність вимогам Специфікації.

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

У разі успішної обробки запиту, відповідь Системи містить набір унікальних значень (RRN, INT_REF, APPROVAL), з використанням яких Торговець може виконати запит завершення продажу або запит скасування продажу.

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

5. Формат відповіді на авторизаційний запит (Authorization Response)

Після обробки авторизаційного запиту Система відправляє Торговцю відповідь з результатами обробки цього запиту. Відповідь може бути направлена Торговцю трьома різними способами (Див. Розділ 2). Разом з відповіддю Система перенаправляє Покупця на адресу, яка була вказана в полі BACKREF авторизаційного запиту.

Таблиця 5 "Поля відповіді Системи на авторизаційний запит"

Поле	Формат	Опис
TERMINAL	S(8)	Дорівнює значенню поля TERMINAL авторизаційного запиту.
TRTYPE	N(1..2)	Дорівнює значенню поля TRTYPE авторизаційного запиту.
ORDER	N(6..20)	Дорівнює значенню поля ORDER авторизаційного запиту.
DESC	S(1..50)	Дорівнює значенню поля DESC авторизаційного запиту.
AMOUNT	N(1..12)	Дорівнює значенню поля AMOUNT авторизаційного запиту.
CURRENCY	S(3)	Дорівнює значенню поля CURRENCY авторизаційного запиту.
ACTION	N(1)	Може набувати значень: **0** – транзакція успішно завершена; **1** – виявлено дублювання транзакції, первинний запит по якій було успішно оброблено [3]; **2** – транзакцію відхилено; **3** – помилка в обробці транзакції [4]; **6, 7** або **8** – виявлено дублювання транзакції, первинний запит по якій було відхилено.
RC	sN(2..3)	Код відповіді по транзакції (*Див. Розділ 20*).
EXTCODE	S(6..10)	Розширений код діагностики при ACTION=3 (*Див. Розділ 20*).
APPROVAL	S(6)	Код підтвердження транзакції від банку Покупця (код авторизації). Може не заповнюватись якщо карткова система банку Покупця не підтримує таку функцію.
RRN	N(12)	Ідентифікаційний номер транзакції.
INT_REF	HN(16)	Внутрішній номер присвоєний повідомленню Системою.
CARDBIN	N(6)	BIN (Bank Identification Number) картки, якою здійснив оплату Покупець. BIN – перші шість цифр номеру картки.
PAN	S(9..19)	Замаскований номер платіжної картки, по якій відбувся запит (приклад: 4444XXXXXXXX1111).
CARDCOUNTRY	S(3)	3-х буквений код країни банка-емітента.
IP	S(7..15)	IP-адреса з якої було ініціалізовано операцію оплати.
AUTHTYPE	S(3)	Якщо значення '**TDS**' – проводилась 3D-Secure аутентифікація держателя картки.
CARDNAME	S(3..35)	Дорівнює значенню поля CARDNAME авторизаційного запиту.
TIMESTAMP	N(14)	Часовий штамп відповіді Системи у **GMT**: РРРРММДДГГХХСС.
NONCE	HN(16..64)	Випадкова величина, що генерується Системою. Заповнена випадковим чином у шістнадцятиричному форматі.
ADDSTR1 ADDSTR2 ADDSTR3	S(1..250)	Дорівнює значенню відповідних полів з авторизаційного запиту.
P_SIGN	HN(1..256)	MAC-підпис повідомлення (*Див. Розділи 14 та Розділ 15*). ⚠ Обов'язкове поле для перевірки Торговцем (*Див. Розділ 16*)

[3] ⚠ У разі дублювання транзакції грошові кошти повторно не блокуються на рахунку Покупця, а у відповіді на дубльований запит містяться значення полів, які було надано на первинний запит.

[4] ⚠ У відповіді Системи при ACTION=3 поля EXTCODE, APPROVAL, RRN, INT_REF та CARDCOUNTRY можуть бути порожні.

5.1. Контроль унікальності запитів

Кожен запит, що надходить до Системи, контролюється на унікальність комбінації значень полів TERMINAL-ORDER-TRTYPE на протязі останніх трьох годин.

У разі, якщо повторний запит повністю ідентичний первинному запиту, Система надішле ту саму відповість яку було надіслано на первинний запит.

У разі, якщо запит, що надійшов до Системи, визначено як повторний за комбінацією значень полів TERMINAL-ORDER-TRTYPE але відрізняється від первинного запиту по будь якому значенню поля CARD, EXP, CVV2, AMOUNT, CURRENCY, Система відхилить повторний запит як RC= –21 (Duplicate transaction).

Для визначення повторно надісланої відповіді Торговець повинен аналізувати значення поля ACTION в отриманій відповіді (Див. **Таблиця 5**).

6. Відправка запиту завершення продажу (Sales Completion Request)

Якщо авторизаційний запит було зроблено з використанням протоколу який вимагає виконання запиту завершення продажу, то для фактичного завершення операції та списання коштів з рахунку Покупця, Торговець має відправити до Системи запит завершення продажу.

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).

Результат обробки запиту завершення продажу може бути направлений Торговцю трьома різними способами (Див. Розділ 2).

7. Формат запиту завершення продажу (Sales Completion Request)

Формат запиту завершення продажу наведено у **Таблиці 6**.

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

Таблиця 6 "Набір полів запиту завершення продажу" (* – обов'язкове для заповнення поле)

Поле	Формат	Опис
TRTYPE	N(2) *	Має дорівнювати '**21**'.
ORDER	N(6..20) *	Цифровий ідентифікаційний номер операції. Може дорівнювати значенню поля ORDER відповіді на авторизаційний запит.
AMOUNT	N(1..12) *	Має дорівнювати або бути менше ніж значення поля AMOUNT відповіді на авторизаційний запит.
CURRENCY	S(3) *	Має дорівнювати значенню поля CURRENCY відповіді на авторизаційний запит.
RRN	N(12) *	Має дорівнювати значенню поля RRN відповіді на авторизаційний запит.
INT_REF	HN(1..32) *	Має дорівнювати значенню поля INT_REF відповіді на авторизаційний запит.
TERMINAL	S(8) *	Дорівнює значенню поля TERMINAL авторизаційного запиту.
TIMESTAMP	N(14) *	Часовий штамп запиту в **GMT**: РРРРММДДГГХХСС. ⚠ Якщо часовий штамп транзакції відрізняється від часу Системи більш ніж на **500 секунд**, такий запит буде відхилено (з кодом **RC = —20**).
NONCE	HN(16..64) *	Випадкова величина. Має бути заповнена випадковим чином у шістнадцятиричному форматі.
EMAIL	S(1..80)	E-mail Торговця для отримання додаткового повідомлення про результат виконання запиту.
BACKREF	S(1..250)	URL-адреса Торговця для відправки результатів запиту.
LANG	S(3)	Мова сторінок Системи. Може набувати значення '**UKR**', '**RUS**', '**ENG**'. У разі відсутності поля використовується значення '**UKR**'.
ADDSTR1 ADDSTR2 ADDSTR3	S(1..250)	Три текстових поля, які не обробляються Системою. Значення цих полів повертається Торговцю у відповіді.
P_SIGN	HN(1..256) *	MAC-підпис запиту (*Див. Розділи 14 та Розділ 15*).

8. Формат відповіді на запит завершення продажу

Після обробки Системою запиту завершення продажу Торговцю відправляється відповідь, ідентична за складом та форматом відповіді на авторизаційний запит (**Таблиця 5**).

9. Відправка запиту скасування продажу (Reversal advice)

Торговець може відправити до Системи запит 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.

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 скасування продажу може бути виконаний незалежно від того чи виконувався вже запит завершення продажу чи ні. Система у будь якому випадку коректно обробить запит та виконає необхідні взаєморозрахунки з міжнародною платіжною системою.

⚠ Після виконання запиту скасування продажу кошти можуть бути не відразу доступні Покупцю. Рішення щодо зняття блокування на рахунку Покупця, або щодо повернення раніше списаних коштів на рахунок Покупця приймає виключно банк-емітент.

10.Формат запиту скасування продажу (Reversal advice)

Формат запиту скасування продажу є ідентичним за складом та форматом запиту завершення продажу (**Таблиця 6**) за виключенням значення поля TRTYPE, яке повинно дорівнювати '**24**'.

⚠ Якщо значення поля AMOUNT запиту скасування продажу менше значення відповідного поля авторизаційного запиту, то в такому випадку буде виконана часткова відміна. У разі необхідності виконати ще один запит на часткову відміну по одній і тій самій операції, значення поля ORDER повинно відрізнятись від первинного.

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.

11. Формат відповіді на запит скасування продажу

Після обробки Системою запиту скасування продажу Торговцю відправляється відповідь методом "HTTP POST". Відповідь складається з полів ідентичних за складом та форматом відповіді на авторизаційний запит (**Таблиця 6**).

12. Повідомлення по HTTPS про результати обробки запиту (HTTPS-нотифікація)

Система, додатково до відповіді, що надсилається Торговцю через браузер Покупця, може формувати повідомлення та надсилати його безпосередньо Торговцю через HTTPS методом POST на адресу, що вказана в конфігураційних файлах Системи для конкретного V-POS-термінала Торговця.

Для отримання повідомлення про результати обробки запиту, Торговець повинен надати адміністратору Системи наступні параметри:

Host - IP-адреса 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=443
HTTP_HOST="test-shop.eximb.com"
HTTP_URL="/reply-auto.php"

⚠ У відповідь на отримання даних, веб-сервер Торговця повинен надіслати HTTP-код стану **'200 OK'**. Відповідь веб-сервера має бути сформована відповідно до вимог протоколу HTTP 1.1. В іншому випадку Система вважає HTTPS-нотифікацію такою, що не отримана Торговцем та з інтервалом в 15 секунд виконує чотири спроби надіслати дані на адресу Торговця.

⚠ У разі зміни IP-адреси сервера Торговця необхідно завчасно повідомити про це адміністратора Системи та надати нові параметри https-нотифікації.

13. Повідомлення по e-mail про результати обробки запиту (email-нотифікація)

Система, додатково до основної відповіді, що надсилається Торговцю на його запити методом "HTTP POST", формує відповідь у вигляді електронного листа, та відсилає цей лист на адресу , що вказана в полі EMAIL запиту.

Тема листа складається зі значень наступних полів: TERMINAL, TRTYPE, RC, ORDER. Тіло листа складається з переліку назв полів та значень цих полів, що об'єднуються знаком '**=**'. Поля відділяються одне від одного знаком '**&**'.

Приклад сформованого Системою листа:

Тема листа:
```
W0000001:: TYPE=0:: RC=00(Approved) :: ACTION=0:: ORDER=024408
```

Тіло листа:
```
TERMINAL=W0000001&TRTYPE=0&ORDER=024408&DESC=Popovnennia osobistogo rachunka
024408&AMOUNT=300&CURRENCY=UAH&ACTION=0&RC=00&APPROVAL=32253B&RRN=51432170456
2&INT_REF=FF71A5477D0BDAA5&TIMESTAMP=20150525115318&NONCE=3946654338313038&EX
TCODE=NONE&CARDBIN=533875&PAN=5338XXXXXXXX2880&CARDCOUNTRY=UKR&IP=37.153.91.3
&AUTHTYPE=TDS&CARDNAME=IVAN
PETRENKO&ADDSTR1=&ADDSTR2=&ADDSTR3=&P_SIGN=7B9C4D9738C4437ED495B149C58765C9FE
C525FD
```

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

14. 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 та відповіді Системи, що відправляються до Торговця, повинні бути підтверджені MAC-підписом.

⚠ Для кожної отриманої від Системи відповіді Торговець **обов'язково** повинен виконувати перевірку MAC-підпису.

Для кожного запиту зі значень деяких полів цього запиту формується MAC-рядок. Поля MAC-рядка та послідовність їх з'єднання для кожного типу запиту, визначені в **Таблиці 7**.

В MAC-рядку значення кожного поля починається з коду, що у десятинному форматі визначає довжину поля. Ці значення надаються у форматі ASCII та з'єднуються у визначеному в **Таблиці 7** порядку. У разі відсутності значення даного поля, на його місці має бути присутній знак дефісу '-' без значення довжини поля.

Таблиця 7 " Перелік та послідовність полів, з яких складається MAC-рядок "

№ п. п.	Для повідомлення **Authorization Request**
1.	AMOUNT
2.	CURRENCY
3.	ORDER
4.	DESC
5.	MERCH_NAME
6.	MERCH_URL
7.	MERCHANT
8.	TERMINAL
9.	EMAIL
10.	TRTYPE
11.	COUNTRY
12.	MERCH_GMT
13.	TIMESTAMP
14.	NONCE
15.	BACKREF

№ п. п.	Для повідомлення **Authorization Response, Sales Completion Response** та **Reversal Response**
1.	RRN
2.	INT_REF
3.	TERMINAL
4.	TRTYPE
5.	ORDER
6.	AMOUNT
7.	CURRENCY
8.	ACTION
9.	RC
10.	APPROVAL
11.	TIMESTAMP
12.	NONCE

№ п. п.	Для повідомлень **Sales Completion Request** та **Reversal Advice**
1.	ORDER
2.	AMOUNT
3.	CURRENCY
4.	RRN
5.	INT_REF
6.	TRTYPE
7.	TERMINAL
8.	TIMESTAMP
9.	NONCE

15. Приклад формування MAC-підпису авторизаційного запиту

Наприклад, Торговець відправляє до Системи такий авторизаційний запит, поля якого мають наступні значення:

Таблиця 8 "Приклад полів авторизаційного запиту"

Поле	Розмір	Значення
TRTYPE	1	0
ORDER	6	771446
DESC	16	IT Books. Qty: 2
AMOUNT	5	11.48
CURRENCY	3	UAH
MERCH_NAME	17	Books Online Inc.
MERCH_URL	14	www.sample.com
TERMINAL	8	W0000001
MERCHANT	15	EXIM3DSW0000001
LANG	3	UKR
EMAIL	19	pgw@mail.sample.com
COUNTRY	0	
MERCH_GMT	0	
NONCE	16	F2B2DD7E603A7ADA
TIMESTAMP	14	20030105153021
BACKREF	33	https://www.sample.com/shop/reply

Значення поля P_SIGN Торговцю необхідно розрахувати.

Використовуючи послідовність, що визначена в **Таблиці 7** для повідомлення **Authorization Request**, складаємо MAC-рядок:

```
511.483UAH677144616IT Books. Qty: 217Books Online
Inc.14www.sample.com15EXIM3DSW00000018W000000119pgw@mail.sample.com10--
1420030105153021 16F2B2DD7E603A7ADA33https://www.sample.com/shop/reply
```

Цей рядок є **нерозривним** (один суцільний рядок без переносів) і має довжину 190 байт.

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 шістнадцятибайтним MAC-ключем: **00112233445566778899AABBCCDDEEFF** MAC-підпис (значення поля “P_SIGN”) має бути таким:

8E9FA99C66EE36DD3B69A555427C486CD68B54C1

Значення результуючого MAC-підпису може бути написано у верхньому або у нижньому регістрі.

Торговець доповнює свій авторизаційний запит полем P_SIGN з розрахованим значенням.

P_SIGN	40	8E9FA99C66EE36DD3B69A555427C486CD68B54C1

16. Приклад перевірки MAC-підпису в отриманому від Системи повідомленні

Наприклад, Торговець на свій авторизаційний запит отримав відповідь від Системи з такими значеннями полів:

Таблиця 9 "Приклад полів відповіді на авторизаційний запит"

Поле	Розмір	Значення
TERMINAL	8	W0000001
TRTYPE	1	0
ORDER	6	771446
DESC	16	IT Books. Qty: 2
AMOUNT	5	11.48
CURRENCY	3	UAH
ACTION	1	0
RC	2	00
EXTCODE	4	NONE
APPROVAL	6	474819
RRN	12	930901244780
INT_REF	16	2E20537302C787A0
CARDBIN	6	444499
PAN	16	4444XXXXXXXX1111
CARDCOUNTRY	3	NLD
IP	13	195.78.112.67
TIMESTAMP	14	20030105153024
NONCE	16	30443AD44F443C43
P_SIGN	40	D4B217F453BE3C43B4345ABDFF1D5F9B47C39A7A

Використовуючи послідовність, що визначена в **Таблиці 7** для повідомлення **Authorization Response**, складаємо MAC-рядок:

```
1293090124478016 2E20537302C787A08W0000001106771446511.483UAH10200647481914200
3010515302416 30443AD44F443C43
```

Цей рядок є **нерозривним** (один суцільний рядок без переносів) і має довжину 108 байт. Застосовуємо до нього алгоритм **HMAC_SHA1** з MAC-ключем: **00112233445566778899AABBCCDDEEFF**

Отримаємо MAC-підпис:

D4B217F453BE3C43B4345ABDFF1D5F9B47C39A7A

Порівнюємо обчислений MAC-підпис зі значенням поля P_SIGN відповіді Системи. Якщо значення співпадають то перевірка пройшла успішно.

17. Тестування 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 Укрексімбанку.

⚠ Промисловий V-POS-термінал на промисловій Системі знаходиться в заблокованому стані і проведення транзакцій через нього неможливо до закінчення тестування.

Мета тестування – відпрацювати усі основні процедури роботи V-POS-термінала з тестовою Системою:

- Перевірити правильність реалізації MAC-алгоритму HMAC_SHA1;
- Відпрацювати авторизаційний запит (TRTYPE = 0) та відповідь Системи на цей запит (обов'язково перевіряти MAC-підпис у відповіді);
- Відпрацювати запит завершення продажу (TRTYPE = 21) та відповідь Системи на цей запит (обов'язково перевіряти MAC-підпис у відповіді);
- Відпрацювати запит скасування продажу (TRTYPE = 24) та відповідь Системи на цей запит (обов'язково перевіряти MAC-підпис у відповіді);
- Навчитись працювати з відповідями Системи на адресу https-нотифікації (обов'язково перевіряти MAC-підпис у відповіді).
- Навчитись працювати з відповідями Системи на адресу e-mail-нотифікації (обов'язково перевіряти MAC-підпис у відповіді).

Параметри для проведення тестів:

Тестовий ідентифікатор TERMINAL: **W0000001**
Тестовий ідентифікатор MERCHANT: **EXIM3DSW0000001**
Тестовий MAC-ключ: **00112233445566778899AABBCCDDEEFF**
Тестовий сервер Системи: https://3ds.eximb.com/cgi-bin/cgi_test

Тестова Система працює в режимі 24/7 та має налаштування ідентичні налаштуванню промислової Системи.

Тестові картки:
Картка №1 0009999999999661 термін дії: 12/21 cvc2: 716
Картка №2 0009999999999224 термін дії: 12/21 cvc2: 060
Картка №3 0009999999999760 термін дії: 12/21 cvc2: 787

Помилки, що найчастіше зустрічаються при виконанні запитів:

1. Значення деяких полів запиту не відповідає вимогам Специфікації.
   Відповідь системи на такий запит RC = -2.

2. Значення поля TIMESTAMP не у **GMT**.
   Відповідь системи на такий запит RC = -20.

3. Невірне значення MAC-підпису.
   Відповідь системи на такий запит RC = -17.

Невірне значення MAC-підпису може бути за декількох обставин:

1) Для підпису використовується невірний MAC-ключ.
   Перевірте MAC-ключ.

2) Поле DESC запиту не у кодуванні Win1251.
   Кириличні символи у полі DESC слід надсилати лише у кодуванні Win1251.

3) Невірно зібрано MAC-рядок для підпису.
   Перевірте правильність збірки MAC-рядка (*Див. Розділ 14 та Розділ 15*).

4) Невірна реалізація алгоритму HMAC_SHA1.

Для перевірки правильності реалізації алгоритму HMAC_SHA1 необхідно виконати процедуру підпису з використанням тестового MAC-ключа наступного MAC-рядку (рядок між "лапками" є **нерозривним** і має довжину 190 байтів, у рядку 'IT Books. Qty: 2' три пробіли, у рядку 'Books Online Inc.' два пробіли):
$str="511.483UAH6771446616IT Books. Qty: 217Books Online Inc.14www.sample.com15EXIM3DSW00000018W0000001 19pgw@mail.sample.com10--1420030105153021 16F2B2DD7E603A7ADA33https://www.sample.com/shop/reply";

Для заданого MAC-рядка, при використанні алгоритму **HMAC_SHA1** та тестового MAC-ключа, отримаємо наступний MAC-підпис:

8e9fa99c66ee36dd3b69a555427c486cd68b54c1

Алгоритм **HMAC_SHA1** в мові програмування PHP, починаючи з версії 5 (http://ua2.php.net/hash), описує функція **hash_hmac**.

У разі відсутності потрібної версії PHP, функцію hash_hmac можна реалізувати за допомогою наступного прикладу (http://www.php.net/manual/en/function.hash-hmac.php#93440):

```
<?php
function custom_hmac($algo, $data, $key, $raw_output = false)
{
    $algo = strtolower($algo);
    $pack = 'H'.strlen($algo('test'));
    $size = 64;
    $opad = str_repeat(chr(0x5C), $size);
    $ipad = str_repeat(chr(0x36), $size);

    if (strlen($key) > $size) {
        $key = str_pad(pack($pack, $algo($key)), $size, chr(0x00));
    } else {
        $key = str_pad($key, $size, chr(0x00));
    }

    for ($i = 0; $i < strlen($key) - 1; $i++) {
        $opad[$i] = $opad[$i] ^ $key[$i];
        $ipad[$i] = $ipad[$i] ^ $key[$i];
    }

    $output = $algo($opad.pack($pack, $algo($ipad.$data)));
    return ($raw_output) ? pack($pack, $output) : $output;
}
?>
```

Приклад PHP-скрипта, що генерує MAC-підпис (замість **hash_hmac** можна використати заздалегідь описану функцію **custom_hmac**):

```
<?php
$data = "511.483UAH677144616IT Books. Qty: 217Books Online
Inc.14www.sample.com15EXIM3DSW00000018W000000119pgw@mail.sample.com10--
142003010515302116F2B2DD7E603A7ADA33https://www.sample.com/shop/reply";
$key = pack("H*", '00112233445566778899AABBCCDDEEFF');
$res = hash_hmac('sha1', $data, $key);
echo $res;
?>
```

Приклад Java-скрипта, що генерує MAC-підпис:

```
import com.sun.org.apache.xerces.internal.impl.dv.util.HexBin;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
public class Sha1Hmac_v2 {
    public static void main(String[] args) throws Exception {
        byte[] keyBytes = HexBin.decode("00112233445566778899AABBCCDDEEFF");
        SecretKeySpec signingKey = new SecretKeySpec(keyBytes, "HmacSHA1");
        Mac mac = Mac.getInstance("HmacSHA1");
        mac.init(signingKey);
        byte[] rawHmac = mac.doFinal("511.483UAH677144616IT Books. Qty: 217Books Online
Inc.14www.sample.com15EXIM3DSW00000018W000000119pgw@mail.sample.com10--
142003010515302116F2B2DD7E603A7ADA33https://www.sample.com/shop/reply".getBytes());
        System.out.println(HexBin.encode(rawHmac));
    }
}
```

Тестування проводиться шляхом формування запитів Програмою Торговця до тестового сервера Системи з використанням параметрів, що вказані вище.

На тестовій картці №1 встановлено ліміт однієї транзакції у розмірі 150 грн. При перевищенні цього ліміту система сформує відповідь з кодом RC=61, ACTION=2 (Відмовити, перевищено ліміт суми операцій). При правильному заповненні усіх полів запиту, транзакції по тестовій картці №1 завершуються успішно (RC=00, ACTION=0).

По тестовій картці №2 транзакції завершуються з кодом RC=05, ACTION=2 (Відмовити, операція відхилена).

По тестовій картці №3 транзакції завершуються з кодом RC=41, ACTION=2 (Відмовити, картка загублена).

⚠ Під час тестування адміністратор Системи може тимчасово налаштувати https-нотифікацію для тестового термінала W0000001 на адресу, яку буде надано спеціалістами Торговця.

⚠ Питання для самоконтролю після закінчення тестування та готовності до роботи з промисловим сервером Системи:

1. Чи відпрацьовані усі три типи запитів (TRTYPE=0, TRTYPE=21, TRTYPE=24)?
2. Чи перевіряється MAC-підпис у кожній відповіді від Системи (пряма відповідь, відповідь по каналу https-нотифікації, відповідь через email)?
3. Чи фіксуються в системі Торговця запити та отримані на них відповіді? Чи ведеться лог/журнал/історія запитів та відповідей?
4. Чи може менеджер Торговця сформувати в ручному режимі запит завершення продажу або запит скасування продажу по раніше проведеній операції?

18. Підключення до промислової Системи

По закінченню тестування необхідно виконати активацію V-POS-термінала на промисловому сервері Системи. Для активації V-POS-термінала відповідальний працівник Торговця повинен написати листа на email адміністратора Системи (*Див. Розділ 21*).

Форма листа:

Повідомляємо, що [юридична назва Торговця] *виконані умови Специфікації обміну повідомленнями між ПЗ Організації та Системою Інтернет-еквайринга АТ "Укрексімбанк". Програмне забезпечення на сайті* [адреса сайту Торговця] *готове до роботи з промисловою Системою.*

Параметри промислового V-POS-термінала:

TERMINAL: [значення TERMINAL]

MERCAHNT: [значення MERCHANT]

Адреса для надсилання HTTPS-нотифікації: [URL-адреса скрипту обробки відповіді]

Просимо активувати на промисловій Системі термінал [значення TERMINAL].

[Контактна інформація автора листа (ПІБ, посада, телефон тощо)]

Для переведення програми Торговця з тестового сервера на промисловий сервер Системи необхідно змінити наступні параметри:

- адресу сервера Системи на яку надсилаються запити (*Див. Розділ 21*);
- значення параметра MERCHANT;
- значення параметра TERMINAL;
- значення MAC-ключа.

Значення параметрів MERCHANT, TERMINAL та значення промислового MAC-ключа для кожного промислового термінала унікальні та передаються окремо менеджером Банку відповідальному працівнику Торговця.

У разі сумнівів в правильності прочитання окремих символів в ключі, для перевірки значення MAC-ключа потрібно використовувати параметр Merchant Check Value, який міститься в конверті з ключем. Процес перевірки полягає в накладанні MAC-підпису на значення параметру Merchant. Перші шість знаків отриманого результату повинні співпадати зі значенням Merchant Check Value.

Приклад перевірки MAC-ключа.

У конверті містяться наступні значення параметрів:

```
Terminal : W0000001
Merchant : EXIM3DSW0000001
MAC Key  : 0011 2233 4455 6677 8899 AABB CCDD EEFF
Merchant Check Value : 756450
```

Для перевірки MAC-ключа виконуємо процедуру накладання MAC-підпису:

```
$data = "EXIM3DSW0000001";
$key = pack("H*", '00112233445566778899AABBCCDDEEFF');
$res = hash_hmac('sha1', '$data', $key);
```

Отриманий результат:

```
$res = 756450 0284b76fac97f93de0f306b29ac8768f61
```

Перші шість знаків отриманого результату співпадають зі значенням Merchant Check Value, отже MAC-ключ використовується вірний.

⚠ У разі виникнення підозри щодо компрометації MAC-ключа, по запиту Торговця, або з ініціативи Банка, генерується новий MAC-ключ для конкретного промислового V-POS-термінала. Торговець повинен мати змогу оперативно замінити MAC-ключ в своєму програмному комплексі.

Для перевірки правильності роботи програми Торговця відразу після переключення на роботу з промисловою Системою необхідно виконати авторизаційний запит з використанням тестової картки №1. У відповідь на такий запит промислова Система повинна відповісти RC=62 (Відмовити, картка блокована). Така відповідь свідчить про відсутність технічних помилок, пов'язаних з переходом від роботи з тестовою Системою до роботи з промисловою Системою.

⚠ *Банк, в процесі роботи Торговця з промисловою Системою, може періодично вимагати зміни значення параметрів (наприклад періодична зміна MAC-ключа). При розробці V-POS-термінала необхідно забезпечити можливість відповідальному менеджеру Торговця вносити зміни в значення параметрів.*

19. Приклад коду сторінки формування авторизаційного запиту (написаний мовою PHP)

```
<html>
<head>
<title>Простий приклад сторінки електронного магазину</title>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="Cache-Control" content="no-cache">
<meta http-equiv="Expiration" CONTENT="0">
<link rel="stylesheet" href="ow/ow.css" type="text/css">
</head>
<body>

<table width='650' align='center' cellspacing='0' cellpadding='0'>

<tr><td><center><h2>Простий приклад сторінки електронного магазину</h2>
<h2><font color="Red">УВАГА ! НА ПРИКЛАДІ СТОРІНКИ НЕ ПЕРЕВІРЯЮТЬСЯ ДАНІ ВІД
КОРИСТУВАЧІВ!</font></h2>

</center><br>
Час запиту: <?php echo date('d.m.Y,  H:i:s', time())?><br><br>
</td></tr>

<?php
if  (!$_POST['EMAIL'] && !$_POST['AMOUNT'] && $_POST['AMOUNT']==0)  {
?>

<tr><td align="center">

<h3>Будь ласка введіть дані дані Вашої покупки:</h3>
<form name='cardform' action='<?php echo $PHP_SELF; ?>' method='post'>

<table cellpadding='2' cellspacing='2' border='0' width='100%'>

<tr><td width='70%'></td>
<td width='30%'></td></tr>

<tr><td>Мова сторінок LANG</td>
<td><input name='LANG' type='text' size='3' maxlength='3' value='UKR'></td>
</tr>

<tr><td>Тип запиту TRTYPE</td>
<td><input name='TRTYPE' type='text' size='1' maxlength='1' value='0'></td>
</tr>

<tr><td>Ідентифікатор Магазину MERCHANT</td>
<td><input name='MERCHANT' type='text' size='25'  maxlength='15' value='EXIM3DSW0000001'>
</td></tr>

<tr><td>Ідентифікатор Терміналу TERMINAL</td>
<td><input name='TERMINAL' type='text' size='25'  maxlength='8' value='W0000001' MAXLENGTH ='8'>
</td></tr>

<tr><td>Сума AMOUNT</td>
<td><input name='AMOUNT' type='text' size='25' maxlength='12' value='<?php echo  $_POST['AMOUNT'];
?>'>
</td></tr>

<tr><td>Валюта CURRENCY</td>
<td><input name='CURRENCY' type='text' size='3' maxlength='3' value='UAH'></td>
</tr>
```

```
<tr><td>Ідентифікатор Замовлення ORDER</td>
<td><input name='ORDER' type='text' size='25' maxlength='32' value='99880001'>
</td></tr>

<tr><td>Опис Замовлення DESC</td>
<td><input name='DESC' type='text' size='25'  maxlength='50' value='Test purchase.'>
</td></tr>

<tr><td>Електрона адреса держателя картки CARDMAIL</td>
<td><input name='CARDMAIL' type='text' size='50'  maxlength='80' value=''>
</td></tr>

<tr><td>Додатковий рядок ADDSTR1</td>
<td><input name='ADDSTR1' type='text' size='50'  maxlength='80' value=''>
</td></tr>
<tr><td>Додатковий рядок ADDSTR2</td>
<td><input name='ADDSTR2' type='text' size='50'  maxlength='80' value=''>
</td></tr>
<tr><td>Додатковий рядок ADDSTR3</td>
<td><input name='ADDSTR3' type='text' size='50'  maxlength='80' value=''>
</td></tr>

<tr><td>Країна магазину COUNTRY</td>
<td><input name='COUNTRY' type='text' size='25'  maxlength='2' value='' disabled>
</td></tr>

<tr><td>Часовий пояс магазину MERCH_GMT</td>
<td><input name='MERCH_GMT' type='text' size='25'  maxlength='5' value='' disabled>
</td></tr>

<tr><td>Назва Магазину MERCH_NAME</td>
<td><input name='MERCH_NAME' type='text' size='25'  maxlength='50' value='Test Merchant'>
</td></tr>

<tr><td>Сайт Магазину MERCH_URL</td>
<td><input name='MERCH_URL' type='text' size='25'  maxlength='250'
value='http://sample.merchant.com'>
</td></tr>

<tr><td>Адреса електронної пошти Магазину EMAIL</td>
<td><input name='EMAIL' type='text' size='25'  maxlength='80' value='way4notify@gmail.com'> <!--
Вкажіть Ваш email для отримання повідомлення -->
</td></tr>

<tr><td>URL для результатів авторизації BACKREF</td>
<td><input name='BACKREF' type='text' size='50'  maxlength='250' value='http://test-
shop.eximb.com/reply.php'>  <!-- Вкажіть url Вашого обробника відповіді -->
</td></tr>

<tr><td>Часовий штамп TIMESTAMP</td>
<td><input NAME='TIME' TYPE='text' size='50' MAXLENGTH='14' VALUE='<?php echo gmdate("YmdHis",
time()); ?>'></input>
</td></tr>

<tr><td>Випадкова величина NONCE</td>
<td><input NAME='NONCE' TYPE='text' size='50' MAXLENGTH='64' VALUE='<?php $var = unpack("H*r",
strtoupper(substr(md5(uniqid(30)), 0, 8))); echo $nonce = $var[r];?>'></input>  <!-- використовуйте
свій алгоритм генерування випадкової величини -->
</td></tr>

<?php
}

else {
        $amount = strlen ($_POST['AMOUNT']);
        $cur = strlen  ($_POST['CURRENCY']);
        $order = strlen  ($_POST['ORDER']);
        $desc = strlen ($_POST['DESC']);
        $m_name = strlen ($_POST['MERCH_NAME']);
        $m_url = strlen ($_POST['MERCH_URL']);
        $merchant = strlen ($_POST['MERCHANT']);
        $terminal = strlen ($_POST['TERMINAL']);
        $email = strlen ($_POST['EMAIL']);
        $trtype = strlen ($_POST['TRTYPE']);
        $country = strlen ($_POST['COUNTRY']);
        $merch_gmt = strlen ($_POST['MERCH_GMT']);
        $time = strlen ($_POST['TIME']);
        $nonce = strlen ($_POST['NONCE']);
        $backref = strlen ($_POST['BACKREF']);
        $key = pack("H*", '00112233445566778899AABBCCDDEEFF');
?>
```

```
<tr><td align="center">
<h3>Будь ласка перевірте дані Вашої покупки:</h3>
<form name='cardform' action='https://3ds.eximb.com:443/cgi-bin/cgi_test' method='post'>  <!--
Адреса тестового сайту Інтернет-еквайрингу АТ Укрексімбанк -->

<table align='center' cellpadding='2' cellspacing='2' border='0' width='100%'>

<tr><td width='70%'></td>
<td width='30%'></td></tr>

<!------------------------>

<tr><td>LANG</td>
<td><?php echo  $_POST['LANG']; ?>
</td></tr>

<tr><td>TRTYPE</td>
<td><?php echo  $_POST['TRTYPE']; ?>
</td></tr>

<tr><td>MERCHANT</td>
<td><?php echo $_POST['MERCHANT']; ?>
</td></tr>

<tr><td>TERMINAL</td>
<td><?php echo $_POST['TERMINAL']; ?>
</td></tr>

<tr><td>AMOUNT</td>
<td><?php echo $_POST['AMOUNT']; ?>
</td></tr>

<tr><td>CURRENCY</td>
<td><?php echo $_POST['CURRENCY']; ?>
</td></tr>

<tr><td>ORDER</td>
<td><?php echo $_POST['ORDER']; ?>
</td></tr>

<tr><td>DESC</td>
<td><?php echo $_POST['DESC']; ?>
</td></tr>

<tr><td>CARDMAIL</td>
<td><?php echo $_POST['CARDMAIL']; ?>
</td></tr>

<tr><td>ADDSTR1</td>
<td><?php echo $_POST['ADDSTR1']; ?>
</td></tr>
<tr><td>ADDSTR2</td>
<td><?php echo $_POST['ADDSTR2']; ?>
</td></tr>
<tr><td>ADDSTR3</td>
<td><?php echo $_POST['ADDSTR3']; ?>
</td></tr>

<tr><td>COUNTRY</td>
<td><?php echo $_POST['COUNTRY']; ?>
</td></tr>

<tr><td>MERCH_GMT</td>
<td><?php echo $_POST['MERCH_GMT']; ?>
</td></tr>

<tr><td>MERCH_NAME</td>
<td><?php echo  $_POST['MERCH_NAME']; ?>
</td></tr>

<tr><td>MERCH_URL</td>
<td><?php echo  $_POST['MERCH_URL']; ?>
</td></tr>

<tr><td>EMAIL</td>
<td><?php echo  $_POST['EMAIL']; ?>
</td></tr>

<tr><td>BACKREF</td>
<td><?php echo  $_POST['BACKREF']; ?>
</td></tr>

<tr><td>TIMESTAMP</td>
```

```
<td><?php echo  $_POST['TIME']; ?>
</td></tr>

<tr><td>NONCE</td>
<td><?php echo  $_POST['NONCE']; ?>
</td></tr>

<input TYPE='HIDDEN' NAME='TRTYPE' VALUE='<?php echo $_POST['TRTYPE']; ?>' MAXLENGTH='1'></input>
<input type='hidden'  name='AMOUNT' type='text' size='25' readonly value='<?php echo
$_POST['AMOUNT']; ?>'>
<input type='hidden'  name='CURRENCY' type='text' size='25' readonly value='<?php echo
$_POST['CURRENCY']; ?>'>
<input type='hidden'  name='ORDER' type='text' size='25' readonly value='<?php echo
$_POST['ORDER']; ?>'>
<input type='hidden'  name='DESC' type='text' readonly value='<?php echo $_POST['DESC']; ?>'>
<input type='hidden'  name='MERCH_NAME' type='text' readonly value='<?php echo
$_POST['MERCH_NAME']; ?>'>
<input type='hidden'  name='MERCH_URL' type='text' readonly value='<?php echo $_POST['MERCH_URL'];
?>'>
<input type='hidden'  name='MERCHANT' type='text' readonly value='<?php echo $_POST['MERCHANT'];
?>'>
<input type='hidden'  name='TERMINAL' type='text' readonly value='<?php echo $_POST['TERMINAL'];
?>'>
<input type='hidden'  name='EMAIL' type='text' readonly value='<?php echo  $_POST['EMAIL']; ?>'>
<input type='hidden'  name='CARDMAIL' type='text' readonly value='<?php echo  $_POST['CARDMAIL'];
?>'>
<input type='hidden'  name='ADDSTR1' type='text' readonly value='<?php echo  $_POST['ADDSTR1'];
?>'>
<input type='hidden'  name='ADDSTR2' type='text' readonly value='<?php echo  $_POST['ADDSTR2'];
?>'>
<input type='hidden'  name='ADDSTR3' type='text' readonly value='<?php echo  $_POST['ADDSTR3'];
?>'>
<input type='hidden'  name='LANG' type='text' readonly value='<?php echo  $_POST['LANG']; ?>'>
<input type='hidden'  name='BACKREF' type='text' readonly value='<?php echo  $_POST['BACKREF'];
?>'>
<input TYPE='hidden'  name='NONCE' value='<?php echo $_POST['NONCE']; ?>' MAXLENGTH='64'></input>


<!-УВАГА! В даному прикладі при складанні мак-рядка не проводиться аналіз полів COUNTRY і
MERCH_GMT, а також не проводиться аналіз відсутності значень інших полів -->

<input TYPE='HIDDEN' NAME='P_SIGN' SIZE='256' VALUE='<?php echo hash_hmac('sha1',
$amount.$_POST['AMOUNT'].$cur.$_POST['CURRENCY'].$order.$_POST['ORDER'].$desc.$_POST['DESC']
.$m_name.$_POST['MERCH_NAME'].$m_url.$_POST['MERCH_URL'].$merchant.$_POST['MERCHANT'].$terminal.$_P
OST['TERMINAL'].$email.$_POST['EMAIL'].$trtype.$_POST['TRTYPE'].
"--".$time.$_POST['TIME'].$nonce.$_POST['NONCE'].$backref.$_POST['BACKREF'], $key); ?>'
MAXLENGTH='256'></input> <!-- MAC-підпис Торговця в шістнадцятковому форматі. Функція hash_hmac
підтримується по замовчуванню починаючи тільки з PHP версії 5 (http://ua2.php.net/hash) -->

<?php
}
?>

<input TYPE='HIDDEN' NAME='TIMESTAMP' VALUE='<?php echo $_POST['TIME']; ?>' MAXLENGTH='14'></input>
<!-- Часовий штамп покупки у форматі РРРРММДДГГХХСС -->

<tr><td colspan='2' align='center'><br><input size='25' TYPE='SUBMIT' VALUE='Відправити дані'
NAME='SEND_BUTTON'></input>
</form></td></tr>

</table>

</td></tr>
</table>

</body>
</html>
```

20. Коди відповіді Системи

Таблиця 10 "Значення кодів відповіді Системи (поле RC) при ACTION=3, 7"

RC	Опис коду
-1	У запиті не заповнене обов'язкове поле
-2	Запит не пройшов CGI-перевірку
-3	Хост екваєра не відповідає або невірний формат відповіді Системи
-4	Немає з'єднання з хостом екваєра
-5	Помилка з'єднання з хостом екваєра під час обробки транзакції
-6	Помилка налаштування Системи
-7	Некоректна відповідь хоста екваєра
-8	Помилка в полі "CARD" запиту
-9	Помилка в полі "EXP" або в полі "EXP_YEAR" запиту
-10	Помилка в полі "AMOUNT" запиту
-11	Помилка в полі "CURRENCY" запиту
-12	Помилка в полі "MERCHANT" запиту
-13	IP-адреса джерела транзакції не відповідає очікуваному
-14	Немає з'єднання з PIN-клавіатурою Інтернет-терміналу або програма-агент на комп'ютері/робочій станції Інтернет-терміналу не запущено
-15	Помилка в полі "RRN" запиту
-16	На терміналі виконується інша транзакція
-17	Терміналу відмовлено в доступі до Системи
-18	Помилка в поле "CVC2" або "CVC2 Description" запиту
-19	Помилка в запиті на аутентифікаційну інформацію або аутентифікація неуспішна
-20	Перевищено допустимий часовий інтервал (500 секунд) між значенням поля "Time Stamp" запиту і часом Системи
-21	Транзакція вже виконана (повторна транзакція)
-22	Транзакція містить помилкову аутентифікаційні інформацію
-23	Помилка в контексті транзакції
-24	Невідповідність в контексті транзакції
-25	Транзакція перервана користувачем
-26	Невірний BIN карти
-27	Помилка в імені продавця
-28	Помилка в додаткових даних
-29	Помилка в посиланні аутентифікації (пошкоджена або дублюється)
-30	Транзакція відхилена як шахрайська
-31	Транзакція в процесі виконання
-32	Повторна відхилена транзакція
-33	Транзакція в процесі аутентифікації клієнта за допомогою авторизації випадкової суми або одноразового випадкового коду
-34	MasterCard Installment транзакція в процесі вибору користувачем способу оплати
-35	MasterCard Installment транзакція в процесі вибору користувачем способу оплати була відхилена автоматично після перевищення ліміту часу на цю операцію
-36	MasterCard Installment транзакція в процесі вибору користувачем способу оплати була відхилена самим користувачем

Таблиця 11 "Значення кодів відповіді по транзакції (поле RC) при ACTION=0, 1, 2, 6"

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 CVC	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

Таблиця 12 "Деякі значення розширених кодів діагностики відповіді Системи (поле EXTCODE)"

EXTCODE	**Опис коду**
NONE	No errors
AS_FAIL	Картотримач не пройшов аутентифікацію на сторінці свого банку.
UNAVAIL	Directory Server платіжної системи не може отримати доступ до ACS-системи банка-емітента (див. *Загальна схема проведення авторизаційного запиту по технології 3-D Secure*) для того, щоб дати відповідь на питання як обслуговувати картку – як 3D Secure або як e-commerce (Directory Server дає відповідь "UNAVAIL"). Банк-емітент не може проводити аутентифікацію.
AS_ERROR	Технічний збій в ході проведення 3D аутентифікації, або запит від інтернет-магазину не відповідає параметрам конфігурування Торговця в Системі.
NS_ATTEMPT	No authentication is performed
BIN_ERROR	Cannot get BIN parameters
DESC_ERROR	Transaction description is empty
MPI_COMM_ERROR	MPI communication error
DS_ERROR	The error has occurred on ACS or Directory Server
ENROLL	Client is not enrolled

21. Реквізити

Адреса сервера **тестової** Системи**:**
https://3ds.eximb.com/cgi-bin/cgi_test

Адреса сервера **промислової** Системи**:**
https://3ds.eximb.com/cgi-bin/cgi_link

E-mail адміністратора Системи: egateway@hq.eximb.com

Остання редакція Специфікації знаходиться за адресою:
http://www.eximb.com/ia/spec/

22. Історія внесення змін

Таблиця 13 "Історія внесення змін до Специфікації"

Дата внесення змін	*Короткий опис змін*
06.08.2008	Виправлена помилка в описі поля ORDER.
21.03.2011	Додано опис поля CARDBIN.
01.04.2011	Додано доповнення.
12.04.2011	Додано опис поля EXTCODE.
16.06.2011	Внесено зміни в структуру Специфікації.
26.08.2011	Додано приклад перевірки MAC-ключа.
12.09.2011	Додано web-адресу розміщення Специфікації.
01.11.2012	Внесено зміни в структуру Специфікації та додаткові пояснення в деякі розділи. Додано опис поля PAN у відповідь на авторизаційний запит.
12.06.2013	Додано опис авторизаційного запиту при якому не вимагається виконання запиту 'Sales Completion Request'. Додано опис поля DESC у відповідь на авторизаційний запит.
25.07.2013	Додано опис поля IP у відповідь на авторизаційний запит.
11.09.2013	Додано опис галузевих доповнень.
15.10.2013	Додано опис поля CARDCOUNTRY у відповідь на авторизаційний запит.
20.12.2013	Змінено реквізити тестових карток.
27.07.2014	Відкориговано схеми взаємодії. Додано опис поля DELIVERY до авторизаційного запиту.
13.11.2014	Додано опис полів ADDSTR1, ADDSTR2, ADDSTR3 запиту. Внесено зміни до розділу «Підключення до промислової Системи».
13.01.2015	Відкориговано опис галузевих доповнень.
27.03.2015	Доповнено умови повторного надсилання HTTPS-нотифікації.
22.04.2015	Виправлено неточності, внесено доповнення.
05.05.2015	Додано опис полів CARDMAIL та CARDNAME.
14.05.2015	Додано опис поля AUTHTYPE у відповідь на авторизаційний запит.
12.04.2016	Додано опис процедури контролю унікальності запитів. Додано опис додаткових значень поля ACTION.
01.12.2016	Змінено реквізити тестових карток.
06.01.2017	Додано опис кодів відповіді Системи.