

Sprawozdanie z odczytu logów transakcji z kart płatniczych EMV

Projekt

9 czerwca 2026

1 Cel ćwiczenia

W ćwiczeniu przygotowano sposób odczytu publicznego logu transakcji z kart płatniczych EMV przez czytnik PC/SC. Nie wystarczył jeden prosty wariant odczytu. Karty zachowują się różnie: część podaje położenie logu wprost, część pokazuje tylko format rekordu, a część wymaga przejścia przez pełniejszą sekwencję EMV.

Ten opis można odtworzyć na dowolnym komputerze z agentem IDE, terminalem, Pythonem i czytnikiem PC/SC. Nie zależy od prywatnego katalogu ani od gotowych plików. Ważna jest kolejność komend APDU, interpretacja statusów i dodatkowe ścieżki dla kart, które nie odpowiadają w najprostszym trybie.

2 Założenia i bezpieczeństwo

Odczyt obejmował tylko publicznie dostępne dane EMV. Nie używano PIN-u, nie wykonywano transakcji i nie obchodzono zabezpieczeń karty.

Przyjęto następujące zasady ochrony danych:

- nie zapisywać pełnego PAN,
- nie zapisywać Track 2,
- nie zapisywać danych posiadacza karty,
- w raporcie umieszczać tylko pola potrzebne do potwierdzenia logu: datę, kwotę, walutę, ATC i status APDU,
- surowe APDU traktować jako dane diagnostyczne, a nie jako część zwykłego raportu.

3 Przebieg wykonania

3.1 Sprawdzenie czytnika i obecności karty

Najpierw sprawdzono, czy system widzi czytnik i kartę. Na macOS służą do tego informacje systemowe o kartach inteligentnych, na Linuksie np. `pcsc_scan`, a na Windows narzędzia PC/SC albo biblioteki systemowe. Ten krok oddziela problem sprzętowy od problemu w samej sekwencji EMV.

Poprawny stan to widoczny czytnik PC/SC i ATR karty. ATR nie oznacza jeszcze, że uda się wybrać aplikację płatniczą. Potwierdza tylko, że karta jest dostępna dla warstwy PC/SC.

3.2 Łączenie z kartą przez PC/SC

Dla wszystkich kart użyto tej samej strategii łączenia. Najpierw próbowano trybu współdzielonego z maską protokołów T=0 | T=1. Jeżeli karta albo sterownik odrzucały taką negocjację, kolejne próby szły już z pojedynczym protokołem:

Kolejność	Protokół
1	T=0 T=1
2	T=0
3	T=1

Ten wariant awaryjny usuwa prostą pułapkę: karta może być prawidłowo włożona i nadal zwracać błąd PC/SC przy negocjacji T=0 | T=1. Wymuszenie T=0 albo T=1 pozwala wtedy przejść dalej.

3.3 Wyszukiwanie aplikacji EMV

Po połączeniu z kartą szukano aplikacji płatniczej dwiema metodami.

1. Najpierw wybierano katalogi płatnicze 1PAY.SYS.DDF01 i 2PAY.SYS.DDF01. Jeśli karta zwracała rekordy katalogu, odczytywano z nich AID aplikacji.
2. Jeżeli katalog PSE/PPSE nie był dostępny albo nie zwracał aplikacji, sprawdzano bezpośrednio popularne AID, np. Visa, Visa Electron, V PAY, Mastercard, Maestro, American Express, JCB i UnionPay.

Obie metody są potrzebne, bo brak PSE nie oznacza braku aplikacji płatniczej. Niektóre karty dają się wybrać dopiero przez bezpośredni SELECT AID.

3.4 Standardowe znaczniki logu transakcji

Dla każdej wybranej aplikacji próbowano odczytać dwa znaczniki związane z logiem:

Tag	Nazwa	Znaczenie
9F4D	Log Entry	SFI pliku logu i maksymalna liczba rekordów
9F4F	Log Format	Format pojedynczego rekordu logu jako DOL

Najprościej jest wtedy, gdy karta zwraca oba znaczniki. 9F4D wskazuje SFI i liczbę rekordów, a 9F4F opisuje, jak rozłożyć bajty pojedynczego rekordu.

3.5 Parser TLV i DOL

Odpowiedzi EMV są zwykle kodowane jako TLV. Parser musi rozpoznać tag, długość i wartość. Dla tagów konstruowanych musi też wejść w elementy zagnieżdżone.

Osobno obsłużono DOL. 9F4F nie przechowuje wartości, tylko pary tag, długość. Parser nie może być zbyt sztywny, bo karty potrafią używać tagów prywatnych albo specyficznych dla danej organizacji płatniczej. W takim przypadku zbyt ścisła interpretacja BER może przesunąć granicę tagu i zepsuć dekodowanie poprawnego rekordu.

3.6 Pełny przepływ EMV: SELECT, GPO i AFL

Jeżeli odpowiedź po SELECT nie wystarczała, wykonywano pełniejszą sekwencję EMV:

1. odczyt FCI po SELECT AID,
2. odczyt PDOL z FCI,
3. zbudowanie danych terminala wymaganych przez PDOL,
4. wysłanie komendy GET PROCESSING OPTIONS,
5. odczyt AFL,
6. odczyt rekordów wskazanych przez AFL,
7. sprawdzenie odczytanych rekordów pod kątem 9F4D, 9F4F i innych znaczników diagnostycznych.

Ten etap sprawdza, czy karta faktycznie nie udostępnia logu, czy tylko nie pokazuje jego położenia w najprostszej odpowiedzi po SELECT.

3.7 Ścieżka awaryjna dla kart bez 9F4D

Osobny przypadek to karty, które zwracają 9F4F, ale nie zwracają 9F4D. Taka karta podaje format rekordu, ale nie podaje wprost miejsca, z którego trzeba czytać log.

Dla takich kart zastosowano pasywny skan:

1. z 9F4F obliczano oczekiwaną długość rekordu logu,
2. wykonywano READ RECORD dla SFI od 1 do 30 i rekordów od 1 do 32,
3. odrzucano odpowiedzi inne niż 9000,
4. odrzucano rekordy o długości niezgodnej z 9F4F,
5. pozostałe rekordy dekodowano według DOL,
6. za kandydatów logu uznawano rekordy zawierające sensowne pola, np. datę 9A, kwotę 9F02, walutę 5F2A lub ATC 9F36.

Ta ścieżka znalazła log także wtedy, gdy GET DATA 9F4D zwracało 6A88, czyli brak żądanego obiektu danych.

4 Zaobserwowane warianty kart

Podczas pracy pojawiły się trzy zachowania kart:

Wariant	Objaw	Sposób obsługi
Karta standardowa	Dostępne 9F4D i 9F4F	Odczyt SFI i liczby rekordów z 9F4D, dekodowanie rekordów według 9F4F.
Karta bez PSE	Brak katalogu płatniczego, ale działa bezpośredni SELECT AID	Sprawdzenie listy znanych AID organizacji płatniczych.
Karta z ukrytym położeniem logu	Dostępne 9F4F, ale brak 9F4D	Pasywny skan READ RECORD i dopasowanie rekordów po formacie 9F4F.

Brak jednego znacznika nie powinien kończyć analizy. Dla kart EMV trzeba sprawdzić kilka ścieżek, bo banki i organizacje płatnicze różnią się szczegółami implementacji.

5 Dekodowanie wyników

Po znalezieniu rekordów logu dekodowano je według formatu DOL. W raporcie zostawiano przede wszystkim te pola:

Tag	Znaczenie	Sposób interpretacji
9A	data transakcji	BCD jako YYMMDD
9F02	kwota autoryzowana	BCD, zwykle z dwiema cyframi groszy
5F2A	waluta	kod numeryczny ISO 4217, np. 985 = PLN
9F36	ATC	licznik transakcji aplikacji
9C	typ transakcji	kod rodzaju operacji, jeśli występuje w logu

Nie każda karta zapisuje w logu ten sam zestaw danych. Jeśli w formacie logu nie ma 9C, nie raportuje się typu transakcji. Jeśli nie ma nazwy akceptanta, nie zgaduje się jej.

6 Wnioski

Odczyt logów transakcji z kart EMV wymaga procedury, która nie zakłada jednego zachowania karty. W praktyce sprawdza się następujący zestaw kroków:

- sprawdzenie warstwy PC/SC i ATR przed analizą APDU,
- awaryjna kolejność protokołów T=0 | T=1, T=0, T=1,
- wyszukiwanie aplikacji zarówno przez PSE/PPSE, jak i przez znane AID,
- próba standardowego odczytu 9F4D i 9F4F,

- wykonanie GPO i odczyt AFL, gdy prosta ścieżka nie wystarcza,
- pasywny skan READ RECORD, gdy istnieje 9F4F, ale nie ma 9F4D,
- filtrowanie rekordów po długości i sensownych polach logu,
- ochrona danych wrażliwych przez pomijanie PAN, Track 2 i danych posiadacza.

Ta sama metoda obejmuje karty standardowe, karty bez katalogu PSE oraz karty, które mają log, ale nie publikują jego położenia przez 9F4D.

7 Prompt do odtworzenia zadania

Poniższy prompt nie zakłada konkretnego katalogu roboczego. Można go uruchomić w agentic IDE z dostępem do terminala, Pythona i czytnika PC/SC.

Masz do dyspozycji komputer z agentic IDE, terminalem, Pythonem oraz czytnikiem kart PC/SC. Do czytnika jest włożona karta płatnicza EMV, która może udostępnić publiczny log transakcji. Twoim zadaniem jest odtworzyć procedurę odczytu logu dla dowolnej takiej karty.

Wymagania:

1. Nie zakładaj istnienia żadnych konkretnych plików ani katalogów. Jeśli potrzebujesz kodu, utwórz go w bieżącym katalogu roboczym.
2. Sprawdź, czy system widzi czytnik i kartę przez PC/SC oraz czy dostępny jest ATR karty.
3. Połącz się z kartą przez PC/SC. Najpierw próbuj T=0|T=1, a jeśli to zawiedzie, próbuj osobno T=0 oraz T=1.
4. Znajdź aplikację płatniczą EMV przez PSE/PPSE: 1PAY.SYS.DDF01 i 2PAY.SYS.DDF01. Jeśli PSE/PPSE nie działa, sprawdź znane AID, m.in. Visa, Visa Electron, V PAY, Mastercard, Maestro, American Express, JCB i UnionPay.
5. Po SELECT AID sparsuj FCI jako TLV. Spróbuj odczytać GET DATA 9F4D oraz GET DATA 9F4F.
6. Jeśli dostępne są 9F4D i 9F4F, odczytaj wskazane rekordy READ RECORD i dekoduj je według formatu DOL z 9F4F.
7. Jeśli 9F4F jest dostępne, ale 9F4D nie jest dostępne, nie kończ pracy. Oblicz długość rekordu z 9F4F i wykonaj pasywny skan READ RECORD dla SFI od 1 do 30 oraz rekordów od 1 do 32. Za rekordy logu uznaj te, które mają zgodną długość i po dekodowaniu zawierają sensowne pola, takie jak data 9A, kwota 9F02, waluta 5F2A lub ATC 9F36.
8. Jeśli prosta ścieżka nie wystarcza, wykonaj GET PROCESSING OPTIONS, odczytaj AFL i sprawdź rekordy aplikacji pod kątem znaczników związanych z logiem.
9. W raporcie nie zapisuj pełnego PAN, Track 2 ani danych posiadacza karty. Pokaż tylko bezpieczne pola: datę, kwotę, walutę, ATC, AID aplikacji i statusy APDU potrzebne do uzasadnienia wyniku.
10. Na koniec opisz, która ścieżka zadziałała dla danej karty i dlaczego prosty odczyt mógł nie wystarczyć.