LABORATORIUM PROGRAMOWANIA KART ELEKTRONICZNYCH

Standard EMV – plugin do SCSuite

POLITECHNIKA POZNAŃSKA, LUTY 2013

1. Standard EMV

EMV jest standardem dla kart elektronicznych wykorzystywanych w systemach płatności bezgotówkowej. Nazwa EMV pochodzi od nazw organizacji, które stworzyły pierwotnie tą specyfikację (**E**uropay, **M**asterCard, **V**isa). Pierwsza wersja specyfikacji została opublikowana w 1996 roku. Obecnie pieczę nad utrzymaniem i rozwojem tego standardu sprawuje organizacja EMVCo.

Celem wprowadzenia standardu EMV było ujednolicenie sposobu wymiany informacji między chipami znajdującymi się na kartach płatniczych, a terminalami do obsługi płatności. Bardzo ważną kwestią było bezpieczeństwo danych, gdyż dotychczas karty wyposażone tylko w pasek magnetyczny można było dość w prosty sposób sfałszować poprzez skimming, czyli skopiowanie danych z katy. Ponadto karty z paskiem magnetycznym nie były dość elastyczne do coraz większej liczby zastosowań kart i ich zabezpieczania. Aktualnie na świecie znajduje się około 1 miliarda kard chipowych oraz ponad 15 milionów terminali zgodnych ze specyfikacją EMV.

Chip zgodny z EMV bardzo często jest umieszony w plastikowej karcie (karty płatnicze) oraz w takich urządzeniach osobistych jak np. telefon komórkowy (smartfon). Chip musi zapewniać 3 kluczowe elementy:

- Trwałe przechowywanie informacji
- Możliwość przeprowadzania obliczeń
- Bezpieczne przechowywanie informacji wraz z możliwością obliczeń związanych z szyfrowaniem (kryptografią)

2. Zalety standardu EMV

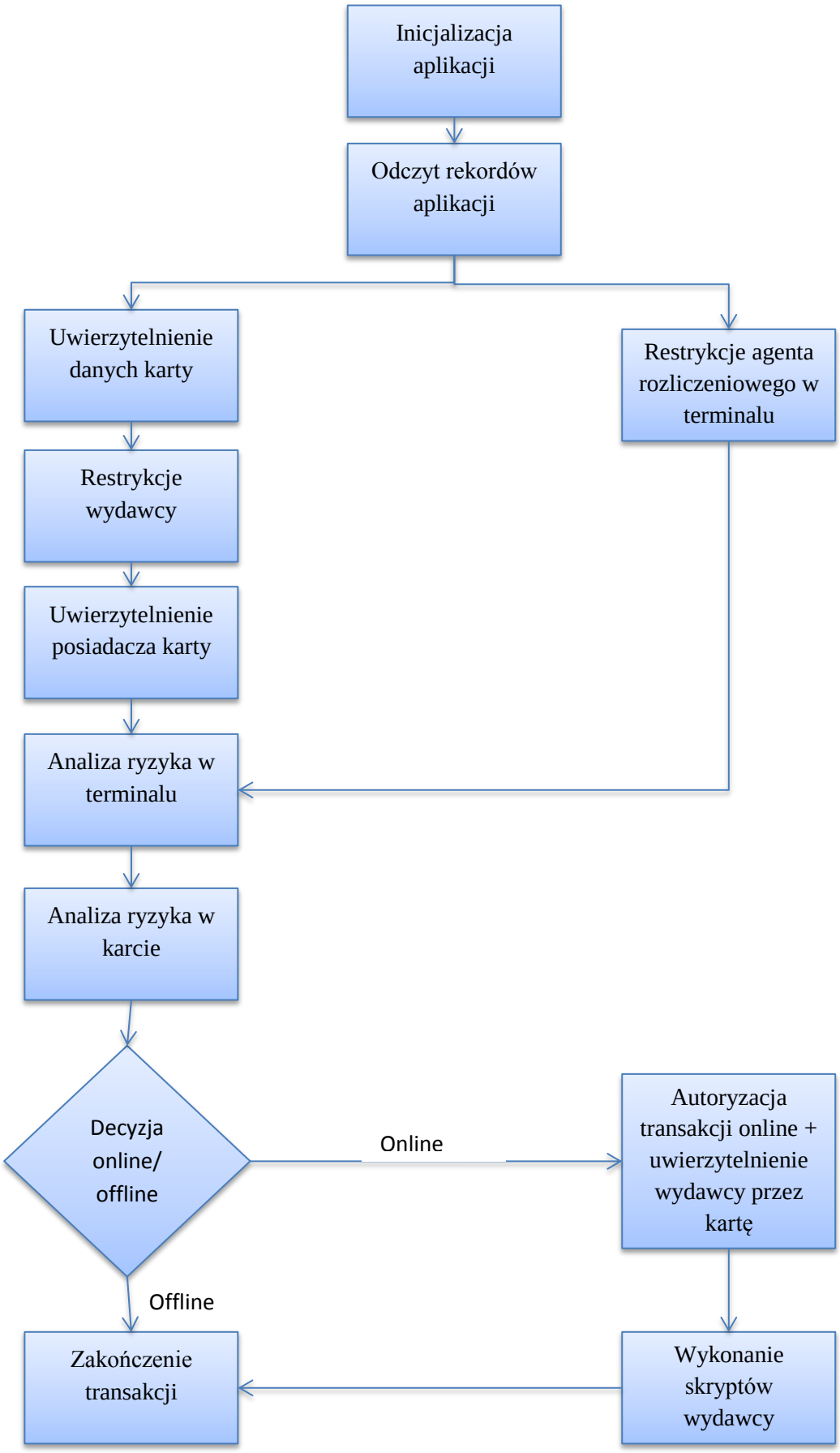
Standard EMV wnosi szereg udoskonaleń w stosunku do kart z paskiem magnetycznym. Przede wszystkim znacznie zwiększone zostało bezpieczeństwo transakcji bezgotówkowych. Do najważniejszych zalet standardu EMV należą:

- Zarządzanie ryzykiem w karcie
- Uwierzytelnienia karty. Może być to wykonane z użyciem różnych technik uwierzytelniania:
    - SDA (Static Data Authentication)
    - DDA (Dynamic Data Authentication)
    - CDA (Combined Dynamic Data Authentication/Cryptogram Generation)
- Weryfikacja PINu offline
- Wzajemne uwierzytelnienie w przypadku transakcji online z zastosowaniem szyfrów symetrycznych

2.1 Porównanie transakcji tradycyjnej, a EMV

Poniższe rysunki prezentują ogólny schemat transakcji płatniczej przy użyciu karty z paskiem magnetycznym (rysunek 1) oraz karty w standardzie EMV (rysunek 2). Jak widać transakcja EMV jest znacznie bardziej złożona. Gwarantuje jednak dużo większą kontrolę nad transakcją przez wydawcę karty oraz większe bezpieczeństwo dzięki mechanizmom analizy ryzyka i wielostopniowemu uwierzytelnianiu.

Rysunek 1 - transakcja z użyciem tradycyjnej karty



Rysunek 2 - transakcja z użyciem karty EMV

3. Płatności kontaktowe, a bezkontaktowe

Podstawową różnicą między płatnościami kontaktowymi a bezkontaktowymi jest inna specyfikacja opisująca dany format. Karty stykowe opisuje standard ISO/IEC 7816, natomiast bezstykowe ISO/IEC 14443. Abstrahując od szczegółów implementacji zawartej w standardach, największa różnica poleca na tym, że w przypadku płatności stykowych karta w ciągu całej transakcji musi być dostępna w czytniku, natomiast przy płatności bezstykowej wszystkie dane pobierane są na początku transakcji i dalej może się ona toczyć bez karty w zasięgu czytnika.

4. Struktura plików na karcie EMV

Aplikacja na karcie elektronicznej zawiera zestaw informacji, często przechowywanych we wnętrzu plików. Informacje te mogą być dostępne dla terminala po pomyślnym wyborze aplikacji (patrz rozdział 4.1). Pojedyncza informacja nazywana jest elementem danych. Jest to najmniejszy fragment informacji, który może być identyfikowany przez nazwę, opis zawartości logicznej, format i kodowanie. Zapewnienie poprawnego formatu danych na karcie jest zadaniem jej wystawcy.

Organizacja plików na karcie EMV jest zgodna z normą ISO/IEC 7816-4. Pliki na karcie widziane są przez terminal jako struktura drzewiasta. Każda z gałęzi drzewa jest typu ADF (Application Definition File) lub DDF (Directory Definition File). Plik ADF zawiera jeden bądź więcej plików AEF (Application Elementary Files), które zawierają dane. Plik ADF i powiązane z nim pliki danych widziane są jako jedna gałąź w strukturze drzewa. Plik DDF może zawierać pliki AEF, ADF lub inne pliki DDF. Struktura i zastosowanie plików AEF są zależne od aplikacji.

4.1 Wybór aplikacji

Norma ISO/IEC 7816 definiuje proces wyboru aplikacji. Miało to na celu umożliwienie wykorzystywania jednej karty do różnych zastosowań, np. przez wgranie aplikacji EMV i GSM. Jednakże standard EMV potraktował wybór aplikacji jako metodę identyfikacji typu produktu. Co za tym idzie wszyscy wystawcy kart (Visa, MasterCard itd.) posiadają własne aplikacje.

Wybór aplikacji możliwy jest za pomocą identyfikatora aplikacji (application identifier, AID). AID składa się z zarejestrowanego (zgodnie z normą ISO/IEC 7816-5) identyfikatora dostawcy aplikacji (RID) o długości pięciu bajtów oraz zastrzeżonego rozszerzenia identyfikatora aplikacji (PIX). PIX pozwala rozróżniać aplikacje oferowane przez jednego dostawcę. Zestawienie kart płatniczych i identyfikatorów wykorzystywanych w nich aplikacji przedstawia poniższa tabela.

Tabela 1 - zestawienie numerów AID

Wystawca karty	RID	Karta	PIX	AID
Visa	A000000003	Visa credit or debit	1010	A0000000031010
		Visa Electron	2010	A0000000032010
		V PAY	2020	A0000000032020
		Plus	8010	A0000000038010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
		MasterCard[4]	9999	A0000000049999
		Maestro (debit card)	3060	A0000000043060

		Cirrus (interbank network)	6000	A0000000046000
UK Domestic Maestro - Switch (karta debetowa)	A000000005	Maestro UK	0001	A0000000050001
American Express	A000000025	American Express	01	A00000002501
Verve (Nigeria)	A000000371	Verve	0001	A0000003710001
Diners Club	A000000152	Diners Club	3010	A0000001523010
LINK (UK) ATM network	A000000029	ATM card	1010	A0000000291010
CB card (Francja)	A000000042	CB card	1010	A0000000421010
JCB	A000000065	Japan Credit Bureau	1010	A0000000651010
Dankort (Dania)	A000000121	Debit card	1010	A0000001211010
CoGeBan (Włochy)	A000000141	PagoBANCOMAT	0001	A0000001410001
Discover	A000000152	Discover	3010	A0000001523010
Banrisul (Brazylia)	A000000154	Banricompras Debito	4442	A0000001544442
SPAN2 (Arabia Saudyjska)	A000000228	SPAN	1010	A00000022820101010
Interac (Kanada)	A000000277	Debit card	1010	A0000002771010
ZKA (Niemcy)	A000000359	Girocard	1010028001	A00000035910100280001
RuPay (Indie)	A000000524	RuPay	1010	A0000005241010
China Union Pay	A000000333	Debit	010101	A000000333010101
		Credit	010102	A000000333010102
		Quasi Credit	010103	A000000333010103
EAPS BANCOMAT	A000000359		10100380	A00000035910100380

5. Plugin do SCSuite

W ramach niniejszego projektu stworzony został plugin do oprogramowania SCSuite umożliwiający odczyt i prezentację plików z karty płatniczej. Został on napisany w języku C# z wykorzystaniem środowiska Microsoft Visual Studio 2012.

Jak zostało wspomniane w punkcie czwartym, struktura i wykorzystanie plików AEF są zależne od aplikacji. Oznacza to, że dla każdego typu karty zawartość i format pliku z danymi może być różna. Ponadto wystawcy kart nie publikują szczegółowej specyfikacji dotyczącej struktury danych w poszczególnych typach kart. Z tego względu postanowiono skupić się na kartach Visa Electron, z których dane pobrane zostały metodą Brute Force. Aplikacja została też przystosowana do obsługi innych typów kart, jednak nie została przetestowana pod tym kątem, gdyż autorzy dysponowali jedynie kartami Visa Electron. Po wykryciu karty i odpowiedniego dla niej AID aplikacja odczytuje wskazany plik. Plik jest czytany w całości i jeśli blok zawiera jakieś niepuste informacje, jest on ukazywany w formie zarówno heksadecymalnej jak i skonwertowanej do typu string. Następnie, dzięki poznaniu zawartości karty, możliwe jest odczytanie podstawowych danych jak np. typ karty oraz imię i nazwisko właściciela. Z powodu braku usystematyzowania danych (nawet na tych samych kartach) nie było możliwe stworzenie parsera działającego dla każdej karty.

6. Bibliografia

- EMV Integrated Circuit Card Specifications for Payment Systems Book 1, version 4.3
- EMV Integrated Circuit Card Specifications for Payment Systems Book 2, version 4.3
- EMV Integrated Circuit Card Specifications for Payment Systems Book 3, version 4.3
- EMV Integrated Circuit Card Specifications for Payment Systems Book 4, version 4.3
- EMVCo, A Guide to EMV, version 1.0
- http://en.wikipedia.org/wiki/EMV