Izabela Sękowska

Dr kom., adiunkt, Wydział Administracji i Nauk Społecznych, Akademia Medycznych i Społecznych Nauk Stosowanych w Elblągu

Znaczenie systemu EMV w zwalczaniu skimmingu bankomatowego

W opracowaniu poruszono kwestię zastosowania standardu technicznej kompatybilności dla kart płatniczych EMV (skrót od European, MasterCard i VISA). Wskazano, że utworzenie tego systemu było niezbędne do ujednolicenia i zapewnienia bezpieczeństwa transakcji płatniczych przy użyciu kart, w szczególności w odniesieniu do skimmingu bankomatowego. Skupiono się na wskazaniu elementów mających wpływ na poszczególne etapy bezpiecznych płatności, poprzez uwierzytelnienie karty, weryfikację jej użytkownika oraz autoryzację transakcji. Wskazano także typy i uwierzytelnienia kart, tj. CDA (*Combined Dynamic Data Authentication*), DDA (*Dynamic Data Authentication*), SDA (*Static Data Authentication*), i krótko je scharakteryzowano. Całość opracowania została zamknięta autorskim podsumowaniem wpływu systemu EMV na zjawisko skimmingu bankomatowego jako istotnego czynnika determinującego bezpieczeństwo finansowe każdego człowieka.

Słowa kluczowe: skimming, bankomat, karty płatnicze, system EMV, bezpieczeństwo finansowe, uwierzytelnienie karty, weryfikacja użytkownika, autoryzacja transakcji, bezpieczne płatności.

Abstract

The paper deals with the application of a technical compatibility standard for payment cards EMV (acronym for European, MasterCard and VISA). It was indicated that the creation of this system was necessary to standardize and ensure and ensuring security of payment transactions using cards,

in particular with regard to ATM skimming. The focus was on identifying the elements that affect the various stages of secure payments through card authentication, cardholder verification and transaction authorization. The types and card authentication i.e. CDA (Combined Dynamic Data Authentication), DDA (Dynamic Data Authentication), SDA (Static Data Authentication) were also indicated and briefly characterized. The whole study was closed with the author's summary of the EMV system's influence on the ATM skimming phenomenon as an important factor determining everyone's financial security.

Keywords: skimming, ATM, payment cards, EMV system, financial security, card authentication, user verification, transaction authorization, secure payments.

Wprowadzenie

Instytucje finansowe uczestniczące w obrocie bezgotówkowym (banki, centra rozliczeniowe), jak również producenci bankomatów oraz instytucje kartowe (pionierzy – Visa, Mastercard, Europay), starają się na różne sposoby przeciwdziałać nadużyciom w systemie płatniczym. Generalnie globalna budowa narzędzi wykrywania oszukańczych transakcji kartowych skupia się na zaawansowanych, ciągle unowocześnianych, systemach wykrywania oszustw, które oceniają transakcje w czasie niemal rzeczywistym. Instytucje te wraz z pojawieniem się nowych technologii oraz usług bankowych działają dwupłaszczyznowo – biorą pod uwagę wygodę klienta, ale jednocześnie jego bezpieczeństwo finansowe. Dlatego za każdą nową usługą podąża rozwój narzędzi zapewniających minimalizowanie mogących wystąpić działań przestępczych. Wdrożone systemy bezpieczeństwa często opierają się na samouczących się modułach, których działanie polega na automatycznie obliczonych profilach bazujących na historii danych danego użytkownika. W przypadku „podejrzanych" transakcji aplikacja wytwarza ostrzeżenie, dające podstawę do uwierzytelnienia i zweryfikowania informacji. Opisywane systemy bezpieczeństwa mogą w takich wypadkach także odmówić zgody na wykonanie transakcji bezpośrednio w trakcie jej dokonywania. Równie ważni są w takich przypadkach pracownicy banków zajmujących się przetwarzaniem przepływu informacji, obejmujących np. system reklamacji transakcji kartowych, gdyż na podstawie odpowiednich danych uzyskanych od klientów

bank jest w stanie ustalić miejsce „wycieku" wrażliwych informacji, np. konkretny bankomat, w którym doszło do skimmingu bankomatowego[1]. Z uwagi na powyższe, tak istotne wydaje się znaczenie systemu EMV w zwalczaniu skimmingu bankomatowego.

Pojęcie skimmingu bankomatowego

Jedna z definicji skimmingu definiuje to pojęcie jako użycie nakładki skimmingowej, która jest najczęściej przyklejana lub instalowana w oryginalnym czytniku kart, aby nielegalnie pozyskiwać dane z kart płatniczych. Tak pozyskane informacje sprawcy kopiują na inne karty (biały plastik) i używają do wypłat gotówki w krajach nieobsługujących standardu EMV[2].

Można wyróżnić skimming w wąskim i szerokim znaczeniu. Skimming w wąskim znaczeniu obejmuje nielegalne skopiowanie paska magnetycznego oryginalnej karty płatniczej bez poznania treści zapisu. Karta płatnicza zawiera trzy ścieżki magnetyczne, z których kopiowana jest druga, z uwagi na fakt, że jest dla sprawców najważniejsza, bo zawiera dane wykorzystywane podczas transakcji bezgotówkowych, takich jak: numer karty, data jej ważności, informacja czy karta posiada mikroprocesor, jak również kod serwisowy niezbędny do prawidłowej realizacji transakcji. Z kolei szersze znaczenie skimmingu obejmuje wiele działań, których ostatecznym efektem jest uzyskanie fałszywej karty płatniczej (tzw. białego plastiku) i przypisanego do niej numeru PIN (na pasku magnetycznym karty płatniczej są umieszczone dane, które pozwalają zweryfikować poprawność użytego kodu)[3]. Tak stworzoną fałszywą kartę przestępcy wykorzystują do nielegalnej wypłaty pieniędzy z bankomatu lub nielegalnych zakupów towarów (usług). W tym przypadku skimming w szerszym znaczeniu identyfikuje cały proceder przestępczy, polegający – po pierwsze – na przygotowaniu urządzeń kopiujących, a po drugie – ich wykorzystaniu do uzyskania zapisu danych z paska karty magnetycznej

[1] P. Opitek, *Przestępstwo skimmingu*, „Prokuratura i Prawo" 2015, nr 11, s. 76.

[2] T. Kielich, Euronet SA (arch. własne autorki).

[3] P. Opitek, *Przestępstwo skimmingu*, s. 66–81.

oraz numeru PIN. Opisany proces odbywa się poprzez umieszczenie tego urządzenia na bankomacie czy terminalu POS (*Point Of Sale* – elektroniczny terminal służący do autoryzacji kart płatniczych), a po stworzeniu „karty-klonu" dokonanie przy jej użyciu przestępczych transakcji. Natomiast najszerzej pojmowane znaczenie skimmingu coraz częściej odpowiada działaniu zorganizowanych grup przestępczych i polega na skopiowaniu karty płatniczej w każdym z możliwych miejsc jej użycia, a następnie wykorzystaniu tych danych do operacji już nie tylko za pomocą „białego plastiku", ale także do nielegalnych transakcji kartowych w tzw. środowisku *card not present* (np. w Internecie czy do transakcji typu „moto")[4]. Reasumując – skimming polega na założeniu specjalnego urządzenia elektronicznego, umieszczonego zazwyczaj na elementach obudowy bankomatu lub włożonego do wejścia czytnika kart, które ma za zadanie sczytać, a następnie skopiować drugą ścieżkę paska magnetycznego, jednocześnie nagrywając sekwencję kodu PIN przy pomocy kamerki lub specjalnej nakładki na klawiaturę. Pozyskane w ten sposób dane są umieszczane na tzw. białym plastiku, a następnie wypłacane w bankomatach, które pozwalają na wypłaty gotówki z kart bankomatowych bez uwierzytelnienia EMV.

System EMV

Standard EMV – to standard technicznej kompatybilności dla kart płatniczych, wypracowany w latach 90. minionego wieku przez trzy organizacje systemów płatniczych: Europay, MasterCard i VISA (stąd skrót EMV)"[5]. Opiera się on na wykorzystywaniu w kartach elektronicznych z tzw. chipem ustalonych współczynników i współpracujących ze sobą aplikacji. Stworzenie tego systemu było niezbędne do ujednolicenia i zapewnienia bezpieczeństwa transakcji płatniczych przy użyciu kart. Bowiem to właśnie karty płatnicze są najważniejszym determinantem migracji EMV i należy je jak najszybciej wymienić z tradycyjnych kart zawierających jedynie pasek magnetyczny

[4] Tamże, s. 69.

[5] *Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne*, Forum Technologii Bankowych, Związek Banków Polskich, styczeń 2005, s. 3.

na karty elektroniczne, które spełniają wymogi EMV. Personalizacja kart EMV jest niezwykle ważna, gdyż wymaga dość dużych zmian w kontekście umieszczenia na nich modułu odpowiedzialnego za kodowanie układu elektronicznego karty EMV. Migracja na EMV wymusza także zmiany generacji, gdyż obok tradycyjnych informacji związanych z kodowaniem I i II ścieżki paska magnetycznego, jak również danych wytłaczanych na karcie, należy wziąć pod uwagę dodatkowy zbiór danych związanych z systemem EMV, np. kryptogramy, które są generowane nie przez terminal, ale właśnie przez kartę. W okresie przejściowym standard EMV pozwala na umieszczenie na kartach mikroprocesora i paska magnetycznego. Jak twierdzą specjaliści ze Związku Banków Polskich, „zapis na pasku magnetycznym ma umożliwiać akceptację kart EMV w środowiskach jeszcze niedostosowanych do EMV. W urządzeniach zdolnych do przeprowadzenia transakcji EMV użycie paska magnetycznego winno skutkować natychmiastowym rozpoczęciem wymiany danych z procesorem, lub przynajmniej żądaniem włożenia karty do czytnika kart procesorowych"[6].

Jak już wspomniano wcześniej, standard EMV stworzyły trzy instytucje kartowe – Europay, Mastercard i VISA – i to od pierwszych liter ich nazw powstała nazwa systemu[7]. Podczas jednego z kongresów naukowych Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond z University of Cambridge zwrócili uwagę na lukę w systemie EMV, które nazwali *Chip and PIN is Broken* (chip i PIN są zepsute)[8]. Zaznaczyli, że EMV jest dominującym protokołem używanym do kart inteligentnych płatności na całym świecie z ponad 730 milionami kart w obiegu. System ten wprowadzono m.in. w Europie i Kanadzie. Zobligowano w tej sprawie również USA, które ociągały się z pełnym wprowadzeniem systemu EMV.

Banki krajów, w których zastosowano opisywany standard tak duży nacisk kładły na wdrożenie go w USA, ponieważ – kiedy wiele państw przeszło

---

[6] Tamże, s. 28.

[7] https://www.google.com/search?q=emv+co+to&oq=emv+&aqs=chrome.1.69i57j0i512l3j46i175i199i512j0i512l5.7626j0j15&sourceid=chrome&ie=UTF-8 [dostęp: 30.05.2022].

[8] S.J. Murdoch, S. Drimer, R. Anderson, M. Bond, *Chip and PIN is Broken*, IEEE Symposium on Security and Privacy, Cambridge 2010, s. 433–437,443.

na uwierzytelnianie wypłat w systemie EMV – Stany Zjednoczone stały się łatwym celem oszustów. Aby takiej sytuacji uniknąć, USA rozpoczęły migrację do EMV w latach 2014–2015. Wraz ze wzrostem eksploracji na rynku technologii EMV na całym świecie, prawie w 100% nawet w niektórych krajach, technologia kart zawierających jedynie paski magnetyczne stała się coraz bardziej archaiczna[9]. Użytkownicy kart bez mikroprocesora mieli w ciągu ostatnich lat kłopoty za granicą, gdyż wiele bankomatów dostosowanych do nowego standardu zwyczajnie nie obsługiwało takich kart. Dzięki nowym kartom EMV, które są zgodne ze światowymi standardami, takie sytuacje zostały wyeliminowane. Stało się to możliwe, gdyż wydane w USA karty chipowe we wszystkich krajach na całym świecie spełniają normy standardu EMV. Zabezpieczenie to ma zadanie chronić transakcje kartami kredytowymi i debetowymi przez uwierzytelnienie obu transakcji (karta i klient), przedstawiając ją przez połączenie kryptograficzne kodów uwierzytelniających, podpisy cyfrowe i wprowadzenie kodu PIN[10].

W systemie EMV użytkownicy kart autoryzują transakcję kartą płatniczą po jej włożeniu do czytnika bankomatu i wprowadzeniu kodu PIN. PIN jest zwykle weryfikowany przez mikroprocesor inteligentnej karty, który z kolei jest uwierzytelniony w terminalu za pomocą cyfrowego certyfikatu. Szczegóły transakcji są także weryfikowane przez kod uwierzytelniania wiadomości kryptograficznych (MAC) za pomocą symetrycznego klucza współdzielonego między kartą płatniczą a bankiem, który wydał kartę klientowi (wystawcy). Tłumacząc tą dość skomplikowaną operację, po włożeniu karty do czytnika następuje weryfikacja dwuetapowa – dane z drugiej ścieżki paska magnetycznego zawierają ten sam klucz, który umieszczony jest w mikroprocesorze. Bank, uwierzytelniając transakcję, oczekuje tego klucza z paska oraz z chipa. Jeśli otrzyma odpowiedź tylko z jednego źródła, transakcja nie powinna dojść do skutku, gdyż istnieje podejrzenie, że karta jest fałszywa. W starym systemie bank weryfikował tylko drugą ścieżkę paska magnetycznego i na podstawie zawartego w niej klucza weryfikował operację. EMV był mocno

[9] https://www-thalesgroup-com.translate.goog/en/americas/united-states/digital-identity-and-security/emv?_x_tr_sl=en&_x_tr_tl=pl&_x_tr_hl=pl&_x_tr_pto=sc, dostęp: 2022-05-30.

[10] S.J. Murdoch, S. Drimer, R. Anderson, M. Bond, *Chip and PIN is Broken*, s. 433–437, 443.

promowany w ramach Chip i PIN podczas krajowego wdrożenia w Wielkiej Brytanii. Technologia ta była przedstawiana jako rozwiązanie problemu zmniejszenia liczby skimmingu bankomatowego, aby zapobiec podrabianiu kart oraz kodów PIN, czyli nadużyciom skradzionych kart. Ale niestety, EMV wprawdzie ograniczyło oszustwo, jednak go nie wyeliminowało, ponieważ oszuści znaleźli lukę, którą wykorzystywali do kontynuowania działalności przestępczej.

W praktyce wykorzystanie systemu EMV działa następująco: Bank, który emituje karty typuje podzestaw protokołów EMV. Ich wybór musi być zgodny z zasadami systemu kart, jak również architekturą EMV. Tymczasem kupcy i banki nabywające (którzy otrzymują płatności w imieniu handlowców) zamawiają sprzęt i oprogramowanie zgodne z EMV i łączą się do sieci płatniczych (obsługiwanych przez systemy kart płatniczych)[11].

Protokół EMV można podzielić na trzy fazy:

1. Uwierzytelnianie karty – upewnia terminal, którego bank wydał kartę, że dane karty nie zostały zmodyfikowane. Karty inteligentne EMV mogą posiadać różne aplikacje zawierające odmienne klucze kryptograficzne, takie jak np. karta debetowa lub kredytowa do użytku w sklepach. Niebagatelną rzeczą jest także funkcjonalność bankomatu i uwierzytelnianie mikroprocesorowe – po umieszczeniu karty w danym urządzeniu w punkcie sprzedaży terminal w pierwszej kolejności żąda listy obsługiwanych aplikacji i wybiera jedną z nich. Faktyczna transakcja jest kolejno inicjowana przez przekazanie komunikatu: uzyskaj opcje przetwarzania polecenia do karty. Następnie terminal weryfikuje dane użytkownika karty z pliku karty, wysyłając polecenie z odpowiednim identyfikatorem plików. Wspomniany identyfikator zawiera dane karty (np. główny numer konta, data rozpoczęcia i data ważności), dane kompatybilności (np. kopia paska magnetycznego) oraz parametry kontrolne dla protokołu (np. posiadacza karty, listę metod weryfikacji i inne listy obiektów danych karty). Zapisy zawierają też cyfrowy podpis RSA na stronie i podzbiór rekordów wraz z powiązaniem łańcucha certyfikatów oraz klucz podpisu do klucza głównego schematu karty znanego terminalu[12].

[11] Tamże, s. 434.

[12] Tamże, s. 435.

2. **Weryfikacja posiadacza karty** – zapewnia terminalowi, że PIN wprowadzony przez klienta pasuje do tej karty. Weryfikacja rozpoczyna się od negocjacji mechanizmu wykonywanego między kartą a terminalem, aby ustalić, którą metodę uwierzytelniania posiadacza karty mogą (lub muszą) użyć. Lista CVM określa zasady dotyczące karty, kiedy do uwierzytelniania użyć kodu PIN lub podpisu albo obyć się bez nich. EMV określa kompleks algorytmu negocjacji, za pomocą którego terminal może wybrać odpowiednią metodę w zależności od wartości transakcji, jej typ (np. gotówka, zakup) i terminal możliwości. Lista CVM określa również, jakie działania powinny być podejmowane, jeśli weryfikacja posiadacza karty nie powiedzie się, tzn. czy powinna zostać wypróbowana następna metoda lub czy transakcja ma zostać odrzucona[13].

3. **Autoryzacja transakcji** – zapewnia terminal, że bank, który wydał kartę autoryzuje transakcję. Na tym etapie terminal oczekuje wygenerowania z karty kryptograficznego MAC (*message authentication code* – kody uwierzytelnienia wiadomości wykorzystywane do uwierzytelnienia danych i zapewnienia ich integralności), zawierającego szczegóły transakcji, które należy przesłać do banku, który wydał kartę. Terminal wywołuje polecenie, aby zażądać ARQC (*Authorization Request Cryptogram* – kryptogram żądania autoryzacji) z karty. Zazwyczaj sprawdza szczegóły, takie jak kwota transakcji, waluta, typ. Jeśli karta pozwala na transakcję, zwraca ARQC, w przeciwnym razie zwraca AAC (*Application Authentication Cryptogram* – uwierzytelnianie aplikacji kryptogram), który przerywa transakcję. ARQC jest następnie wysłane przez terminal do banku wydającego za pośrednictwem agenta rozliczeniowego i sieć płatniczą. Emitent w takim przypadku przeprowadza różne kontrole, eliminujące oszustwa finansowe, jak na przykład: czy karta została wymieniona jako skradziona, czy istnieją odpowiednie fundusze i czy algorytm analizy ryzyka uważa, że transakcja jest akceptowalna. Jeśli kontrole się powiodą, wystawca zwraca dwubajtowe ARC (*Authorisation Response Code* – odpowiedź autoryzacyjna kodu), wskazując sposób postępowania transakcji, oraz ARPC (*Authorisation Response Cryptogram* – kryptogram odpowiedzi na autoryzację), który jest zazwyczaj MAC ponad ARQC. Oba elementy zostają przekazane przez terminal do karty. Karta sprawdza

[13] Tamże, s. 435–436.

poprawność MAC zawartego w ARPC, a jeśli się powiedzie, zaktualizuje swój stan wewnętrzny, aby zauważyć, że emitent autoryzował transakcję[14].

Powyżej pokazano, jak bardzo funkcja weryfikacji PIN w protokole EMV jest wadliwa. Brak uwierzytelnienia w systemie, odpowiedź weryfikacyjna PIN połączona z niejednoznacznością w kodowaniu wyniku weryfikacji posiadacza karty w TVR, pozwala atakującemu z *man-in-the-middle* na użycie karty bez poprawnego kodu PIN. Ta właśnie luka jest wykorzystywana m.in. przez przestępców zajmujących się nielegalnym kopiowaniem kart płatniczych. W zasadzie cały problem polega na wypłacie pieniędzy za pomocą „białego plastiku" w bankomatach obsługujących karty z samym paskiem magnetycznym albo wykorzystujących wyżej opisaną lukę, jak również pozytywnie weryfikujące rzekome uszkodzenie lub nieczytelność mikroprocesora umieszczonego na karcie płatniczej. Inaczej to zjawisko ujmując, jeśli bank podczas weryfikacji transakcji w bankomacie nie otrzyma np. informacji zwrotnej zawierającej klucz z mikroprocesora, a jedynie z paska magnetycznego, wówczas albo blokuje transakcje, albo może taką operację zautoryzować, zakładając, że gdzieś wystąpił błąd. Taki błąd może wynikać np. z uszkodzenia mechanicznego, które uniemożliwia prawidłowe odczytanie i porównanie klucza. Jednak, jeśli takie operacje powtórzą się, są obligatoryjnie blokowane. Reasumując, jeśli dane pozyskane w wyniku skimmingu są czytelne i uda się je powiązać z kodami PIN, przestępcy uzyskują idealną kopię karty płatniczej z przypisanym jej kodem PIN i mogą realizować wypłaty z bankomatu nieobjętego systemem EMV.

Powyższe informacje pokrótce wyjaśniają, dlaczego obecnie skimming bankomatowy jest wymierzony w karty z paskiem magnetycznym i wbudowanym mikroprocesorem z układami niechronionej klasy.

W standardzie EMV wyróżnia się trzy typy uwierzytelnienia (czwarty typ to jego brak): 1. CDA (*Combined Dynamic Data Authentication*), 2. DDA (*Dynamic Data Authentication*), 3. SDA (*Static Data Authentication*).

Powyższe typy uwierzytelnienia usystematyzowano w kolejności stopnia ich zaawansowania i skomplikowania algorytmów. Typ CDA zdecydowanie zajmuje najwyższą klasyfikację. Specyfikacja EMV nie wymusza kolejności

[14] Tamże, s. 436.

uwierzytelnienia transakcji, tym niemniej wskazuje, że musi to z pewnością nastąpić po odczytaniu danych z karty, ale przed zakończeniem transakcji. Każdy z typów uwierzytelnienia ma wspólny cel – zabezpieczyć dany system płatniczy przed fałszerstwami. Typ uwierzytelnienie CDA w sposób dynamiczny i statyczny uwierzytelnia karty, jednak jest procesem niezależnym od decyzji karty dotyczącej rezultatu transakcji (co nie oznacza, że wyniki takiego uwierzytelnienia nie są brane pod uwagę). W związku z tym teoretycznie jest możliwa podmiana karty (trudne, ale możliwe) w taki sposób, aby uwierzytelnienie było wykonywane przez oryginalną kartę, natomiast decyzja (pozytywna) była podejmowana przez kartę sfałszowaną. Dlatego zakłada się dążenie do tego, aby decyzja transakcyjna i uwierzytelnienie karty odbywały się w sposób uniemożliwiający podmienienie karty pomiędzy tymi dwoma procesami. Schemat CDA ukazuje rys. 1.

„Uwierzytelnienie karty w trybie SDA jest realizowane w dwóch krokach: – pierwszy krok zmierza do wyliczenia klucza publicznego wydawcy karty. Po uzyskaniu klucza publicznego wydawcy urządzenie przystępuje do właściwego uwierzytelnienia danych z karty[15]. Chociaż SDA uwierzytelnia dane pochodzące z karty, to metoda ta nie zabezpiecza wydawców kart przed oszustwami w 100 procentach, bowiem zachowania prawdziwej karty w środowisku offlineowym umożliwia realizację transakcji oszukańczych na kwoty poniżej floor-limitu terminala"[16]. Rys. 2 przedstawia proces SDA.

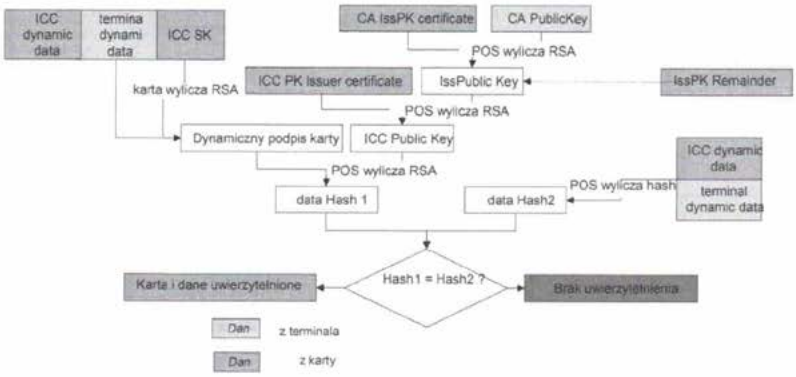
„DDA wymaga trzech kroków: – pierwszy krok, identyczny jak w SDA, ma na celu uzyskanie klucza publicznego wydawcy karty. Po uzyskaniu klucza publicznego wydawcy karty terminal przystępuje do dynamicznego uwierzytelnienia karty"[17]. Uwierzytelnienie potwierdza, że: dane umieszczone na karcie nie zostały zmienione od chwili wydania karty (hash jest zgodny); po drugie – karta nie została sklonowana, bo wydał ją uprawniony do tego bank. Rys. 3 przedstawia proces DDA.

---

[15] *Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne*, s. 32–33.

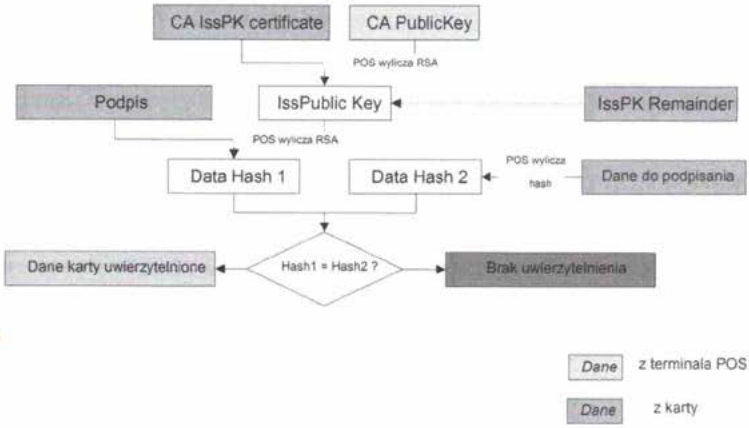
[16] Tamże, s. 32.

[17] *Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne*, s. 34.



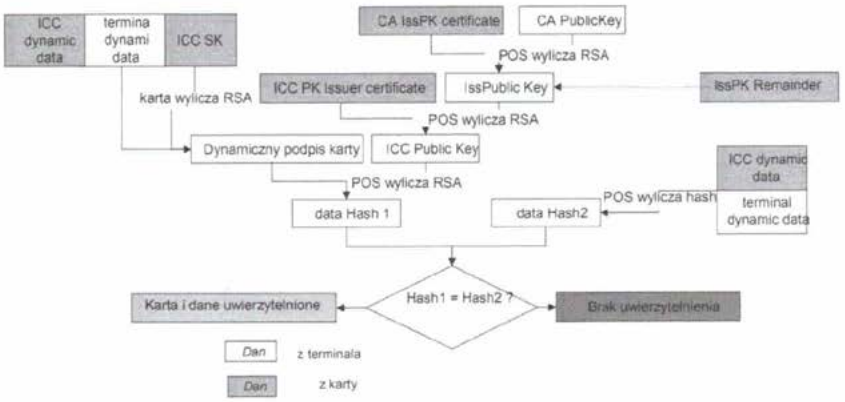
Rys. 1. Schemat CDA

Źródło: *Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne*, Forum Technologii Bankowych, Związek Banków Polskich – Typ uwierzytelnienia SDA obejmuje przede wszystkim weryfikację pod kątem nieautoryzowanej zmiany wartości istotnych dla bezpieczeństwa systemu płatniczego współczynników zapisanych na karcie w trakcie jej personalizacji. Ten typ stanowi najprostszą i przez to najmniej bezpieczną metodę uwierzytelnienia karty. Uwierzytelnia nie tyle samą kartę, co dane na niej zapisane.



Rys. 2. Proces SDA

Źródło: *Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne*. Typ uwierzytelnienia DDA ma zapewnić i potwierdzić autentyczność danych umieszczonych na karcie, wygenerowanych przez kartę oraz otrzymanych z terminala w trakcie transakcji EMV



Rys. 3. Schemat DDA

Źródło: *Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne*

Podsumowanie

Zebrane w opracowaniu informacje wskazują jak duże znaczenie dla zwalczania skimmingu bankomatowego ma system EMV. W znacznym stopniu ogranicza on kopiowanie danych z kart bankomatowych, gdyż możliwości zarówno samego kopiowania, jak również wypłat z „lewych" kart są zawężone. Przestępcy znacznie częściej wskazują, że najłatwiejsze do skopiowania i do wypłat są karty wyposażone jedynie w mechanizm SDA, występujące w krajach o niskim poziomie rozwoju (sam pasek magnetyczny). Wytworzenie takiej karty jest tańsze, gdyż nie wymaga stosowania koprocesora kryptograficznego, co wpływa na cenę ich wytworzenia i sprzedaży instytucjom bankowym. Sytuacja jest analogiczna w przypadku terminali *offline*, gdyż występują tam częściej z uwagi na niską dostępność infrastruktury sieciowej. Czy wprowadzenie systemu EMV w wersji podstawowej ma wpływ na skimming? Zdecydowanie tak, jednak wraz ze wzrostem technologii bankowych, wzrasta również poziom działania sprawców, dla których skimming to bardzo dochodowy biznes. Oszuści zajmujący się skimmingiem nie dopuszczają do znaczących spadków ich dochodów i szybko znajdują nowe metody

prowadzenia swojej działalności[18]. Ujawnili oni i wykorzystali błąd protokołu, który umożliwiał im korzystanie z autentycznej karty i wykonywanie transakcji finansowych bez znajomości kodu PIN karty. Pozostają anonimowi nawet wówczas, gdy sprzedawca ma połączenie internetowe i połączenie z siecią bankową. Oszuści dokonują ataku *man-in-the-middle*[19], by przekonać terminal, że sekwencja kodu PIN została poprawnie zweryfikowana, jednocześnie przekonując kartę, że nie posiada ona kodu PIN. Jak to jest możliwe? Przecież system EMV został wdrożony na szeroką skalę. Otóż wniosek nasuwa się sam – protokół EMV nie jest pozbawiony wad. Błąd systemu jest znaczący, gdyż przestępcy kartowi nagminnie go wykorzystują, a banki często odmawiają ofiarom takich oszustw zwrotu pieniędzy z tytułu reklamacji, argumentując, że karta nie może być używana bez poprawnego kodu PIN, więc zapewne klient zaniedbał zasady bezpieczeństwa przy realizacji płatności za pomocą karty. Mając na uwadze powyższe, zasadne jest prowadzenie dalszych badań i udoskonalenie technologii uwierzytelniania transakcji kartowych, w celu wypełnienia luki między teoretycznym i praktycznym bezpieczeństwem systemów płatności bankowych. Taka sytuacja wskazuje natomiast potrzebę udoskonalenia obecnej wersji EMV.

Specjaliści od polityki bezpieczeństwa banków zasygnalizowali, że w niedalekiej przyszłości zostanie wprowadzony nowy standard, będący częścią unijnej dyrektywy „w sprawie usług płatniczych (PSD2) – uaktualnionej regulacji dotyczącej handlu cyfrowego. EMV 3D Secure (lub EMV 3DS) to

[18] https://zaufanatrzeciastrona.pl/post/przestepcy-potrafia-juz-skopiowac-chipowe-karty-kredytowe [dostęp: 31.05.2022].

[19] Atak typu *man-in-the-middle* [MITM] jest rodzajem cyberataku, w którym złośliwy „aktor" włącza się w rozmowę między dwiema stronami, podszywa się pod obie strony i uzyskuje dostęp do informacji, które dwie strony próbowały wysłać sobie nawzajem. Atak typu *man-in-the-middle* pozwala złośliwemu „aktorowi" przechwytywać, wysyłać i odbierać dane przeznaczone dla kogoś innego lub uniemożliwić ich wysyłkę. *Man-in-the-middle* jest rodzajem ataku-podsłuchu, który pojawia się, gdy złośliwy „aktor" umieszcza się jako przekaźnik/serwer proxy w sesji komunikacyjnej między ludźmi lub systemami. Atak MITM wykorzystuje przetwarzanie transakcji, konwersacji lub przesyłania innych danych w czasie rzeczywistym. Ataki typu *man-in-the-middle* umożliwiają atakującym przechwytywanie, wysyłanie i odbieranie danych, które nigdy nie były przeznaczone dla nich, bez wiedzy właściwych osób uczestniczących w przekazie.

globalny standard branży kartowej, zaprojektowany z myślą o ułatwieniu sklepom detalicznym i wystawcom kart płatniczych uwierzytelnianie transakcji cyfrowych. Krótko mówiąc, pomaga on w lepszym zabezpieczeniu płatności online kartą. Regulacja ta wspiera nowe technologie, takie jak uwierzytelnianie biometryczne, dzięki którym zakupy internetowe są mniej uciążliwe dla klientów, co przekłada się na wyniki sprzedaży"[20].

Obecne czasy niejako wymuszają korzystanie z pieniądza elektronicznego. Banki wychodzą naprzeciw dostarczając atrakcyjny produkt, czerpiąc z tego ogromne zyski. Jednocześnie z ofertą produktu są zobligowane do zapewnienia bezpieczeństwa zarówno oferowanych kart, jak również wykonywanych przy ich użyciu transakcji finansowych.

Literatura

Kielich T., Euronet SA (arch własne autorki).

Murdoch S.J., Drimer S., Anderson R., Bond M., *Chip and PIN is Broken*, IEEE Symposium on Security and Privacy, Cambridge 2010.

Opitek P., *Przestępstwo skimmingu*, „Prokuratura i Prawo" 2015, nr 11.

Migracja na standard EMV w Polsce – aspekty organizacyjno-techniczne, Forum Technologii Bankowych, Związek Banków Polskich, styczeń 2005.

https://www.google.com/search?q=emv+co+to&oq=emv+&aqs=chrome.1.69i57j0i512l3j46i175i199i512j0i512l5.7626j0j15&sourceid=chrome&ie=UTF-8

https://zaufanatrzeciastrona.pl/post/przestepcy-potrafia-juz-skopiowac-chipowe-karty-kredytowe/

https://www.mastercard.com/news/europe/pl-pl/centrum-prasowe/aktualnosci/pl-pl/2019/czerwiec/dlaczego-standard-platnosci-emv-3d-secure-jest-wazny-dla-sklepow-internetowych.

[20] https://www.mastercard.com/news/europe/pl-pl/centrum-prasowe/aktualnosci/pl-pl/2019/czerwiec/dlaczego-standard-platnosci-emv-3d-secure-jest-wazny-dla-sklepow-internetowych [dostęp: 31.05.2022].