STUDIA INFORMATICA 2000
Volume 21 Number 1 (39)

Henryk MAŁYSIAK, Rafał BAŁAGA
Politechnika Śląska, Instytut Informatyki

KONCEPCJA PŁATNOŚCI ELEKTRONICZNYCH W SIECI INTERNET

Streszczenie. W artykule przedstawiono podstawowe informacje o płatnościach elektronicznych w sieci Internet. Ponadto omówiono istniejące na świecie rozwiązania i standardy. Zaprezentowano także własną koncepcję rozwiązania problemu płatności w rozproszonym środowisku Internetu z uwzględnieniem specyfiki polskiego rynku.

THE CONCEPTION OF ELECTRONIC PAYMENT IN INTERNET

Summary. In this paper we present brief informations of electronic payment in Internet. Moreover, exisisting solution and standards in the world are shown. We also present own conception of solving payments in Internet distributed systems with special taken into consideration specificity of Polish market.

1. Wstęp

Dynamiczny rozwój Internetu daje ogromne możliwości i rodzi coraz to nowsze zastosowania. Wśród nich powstała idea biznesu internetowego, czyli zarabiania pieniędzy poprzez sieć. Stawia to przed różnego rodzaju korporacjami zupełnie nowe wyzwania. Daje im możliwość rozszerzenia swojej działalności i zaistnienia na odmiennym niż dotychczas bardzo obszernym rynku.

Zamieszczenie swojej oferty w sklepie internetowym pozwala dotrzeć firmom do milionów ludzi na całym świecie. Otwarcie sieci przed użytkownikiem, możliwość dokonywania zakupów bez wychodzenia z domu daje mu poczucie komfortu i czyni go potencjalnym klientem, który chętnie z tego udogodnienia będzie korzystał. Zatem handel elektroniczny to usługa internetowa stanowiąca z jednej strony źródło dochodów dla

sprzedawców, z drugiej zaś będącą kolejnym krokiem w kierunku zwiększania komfortu naszego życia. Handel elektroniczny to wszelkiego rodzaju procesy i aplikacje związane z zakupami internetowymi.

Ogólnodostępność Internetu sprawia, że potencjalnym klientem staje się tu każdy użytkownik Internetu, a liczba osób korzystających z sieci rośnie w Polsce w zawrotnym tempie. Obecnie szacuje się, że w naszym kraju jest ok. 3 miliony internautów. Większość użytkowników podchodzi jednak do robienia zakupów przez Internet z dużą rezerwą. W przeprowadzonej w tym roku przez Katedrę Marketingu Akademii Ekonomicznej w Krakowie ankiecie [1] na pytanie „dlaczego nie robimy zakupów przez Internet?", uzyskano następujące odpowiedzi:

Powody	Procent ankietowanych
Brak zaufania do tej formy nabywania produktów	34,8
Obawa, czy ktoś nie przejmie danych umożliwiających bezprawne korzystanie z mojej karty kredytowej	32,8
Konieczność zapłaty za pomocą karty kredytowej	32,6
Brak doświadczenia w robieniu zakupów w ten sposób	27,8
Mała liczba polskich firm oferujących swoje produkty w ten sposób	23,1
Konieczność ujawniania swoich danych osobowych	22,5
Niepewność, czy dostanę to, co zostało zamówione	22,3
Brak ofert zakupu interesujących mnie towarów w Internecie	19,4
Takie same ceny jak w sklepie	17,4
Konieczność oczekiwania na dostarczenie	15,5
Nieznajomość sprzedawcy (brak osobistego kontaktu)	13,2
Zbyt długi czas potrzebny na poszukiwanie produktu	10,6
Konieczność potwierdzania zamówienia telefonicznie	8,7
Inne	5,6

Niewątpliwie ankieta świadczy o braku zaufania użytkowników Internetu do tej formy zakupów. Przyczyn takiego stanu rzeczy można upatrywać w braku na polskim rynku bezpiecznych rozwiązań obsługi płatności – najbardziej newralgicznej części systemów biznesu elektronicznego. Bezpieczna obsługa płatności w Internecie musi zagwarantować ochronę numerów kart płatniczych oraz danych osobowych użytkowników przed wykradaniem ich przez komputerowych włamywaczy. Poza tym powinna ona zapewniać autoryzację użytkowników i sklepów, łatwość integracji sklepów z systemem, generować

wyciągi księgowe dla sklepów i użytkowników. Na drodze do stworzenia takiego systemu istnieje kilka barier, które spowalniają rozwój elektronicznego biznesu jako całości. Są to:

- brak zaufania do Internetu jako bezpiecznego środka przekazu danych,
- brak regulacji prawnych dotyczących elektronicznego dokumentu i elektronicznej transakcji,
- „anonimowość" protokołu TCP/IP, co oznacza, że nie posiada ona żadnych mechanizmów weryfikacji użytkowników.

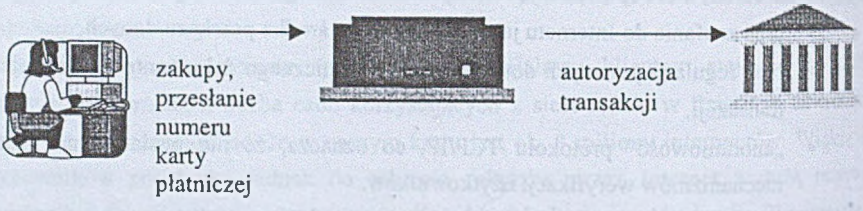
Biznes elektroniczny jest więc wciąż nowym obszarem, który rzuca wyzwanie informatykom. Stanowi ciekawe pole do tworzenia nowych rozwiązań i standardów.

1.1. Podstawowe informacje

Idea działania kart płatniczych wydaje się być dużo lepiej dopasowana do natury Internetu niż inne tradycyjne formy płatności. Większość kart płatniczych ma zasięg globalny: posiadacz takiej karty wydanej przez dowolny bank na świecie może zapłacić nią w dowolnej firmie, w dowolnym kraju, w dowolnej walucie: odpadają wszelkie problemy związane z wymianą walut i trudnościami międzynarodowych przekazów pieniężnych. Dodatkowo procedura dokonywania zapłaty kartami płatniczymi jest niezwykle prosta, bo aby dokonać zapłaty, należy po prostu podać sprzedawcy tajny szesnastocyfrowy numer swojej karty, oraz kilka innych danych, jak np. swoje nazwisko oraz datę ważności karty, a bank już sam obciąży należnością nasze konto. Każda taka transakcja jest na bieżąco autoryzowana (to znaczy sprzedawca sprawdza za pomocą specjalnego terminalu w bankowej bazie danych, czy taka karta faktycznie istnieje i czy np. nie została skradziona), a ponieważ numer karty jest tajny, domniemywa się, że osoba, która podała sprzedawcy prawidłowy numer, jest rzeczywistym posiadaczem danej karty.

Karty kredytowe stanowią zatem niemal gotowe rozwiązanie dla płatności Internetowych; zostały też do tego celu szybko wykorzystane i dziś zdecydowana większość sieciowych "sklepów" używa kart kredytowych.

Ogólny schemat funkcjonowania takiego sklepu przedstawia rysunek 1.



Rys.1. Ogólny schemat procesu dokonywania transakcji w Internecie
Fig. 1. General framework of process of making transaction in Internet

Podsumowując te rozważania, można podzielić funkcjonowanie systemu obsługi transakcji w Internecie na dwa etapy:

- wymiana informacji między klientem a sklepem,
- autoryzacja transakcji w centrum autoryzacyjnym.

1.2. Bezpieczeństwo transakcji internetowych

W założeniach protokołów TCP/IP brak jest jakichkolwiek mechanizmów identyfikowania użytkowników (mechanizmy takie będzie miał nowy protokół IPv6), a usługi informacyjne, takie jak np. WWW, są dostępne praktycznie anonimowo. Dokument umieszczony na serwerze może być przeczytany przez dowolną osobę na świecie posiadającą dostęp do komputera podłączonego do sieci; serwer nawet "nie wie", kto odczytuje z niego dokument (jeżeli pominąć "administracyjne" metody kontroli dostępu typu).

W takiej sytuacji, kiedy do dokonania zapłaty wystarcza znajomość danych wypisanych na karcie kredytowej, sprzedawca nie ma żadnej możliwości sprawdzenia tożsamości kupującego (a więc tego, czy w istocie jest on posiadaczem tej karty)! Otwiera się tu więc możliwość oszustw i nadużyć. Wystarczy posłużyć się danymi z cudzej karty (np. podglądniętymi u kogoś w zwykłym, "fizycznym" sklepie), aby dokonać - bez wiedzy właściciela karty - zakupu na jego rachunek.

Wspomniana powyżej niemożność zweryfikowania klienta przez sprzedawcę działa również w odwrotną stronę: także i klient nie może być pewny, że serwer, który pyta go o numer jego karty kredytowej, jest prawdziwym "sieciowym sklepem" uczciwego sprzedawcy, a nie fałszywym, "podstawionym" serwerem, umieszczonym przez kogoś w sieci specjalnie po to, aby w łatwy sposób zbierać numery kart kredytowych.

Ponadto oszust może "zbierać" numery kart kredytowych podglądając je w sklepach, jednak dużo efektywniejszą metodą jest przechwytywanie ich z samego Internetu, dlatego numery kart kredytowych lepiej przekazywać przez sieć w postaci zaszyfrowanej.

Wynika stąd, że przy transakcjach kartami kredytowymi w Internecie mamy do czynienia z trzema podstawowymi problemami:

- niemożliwością zweryfikowania klienta przez sprzedawcę - uwierzytelnianie i niezaprzeczalność,
- możliwością podsłuchu przesyłanego przez sieć numeru karty – poufność i nienaruszalność,
- niemożliwością zweryfikowania sprzedawcy przez klienta - uwierzytelnianie i niezaprzeczalność.

1.3. Autoryzacja transakcji

Zgodnie z zaproponowanym na początku tego rozdziału podziałem kolejnym etapem, po bezpiecznym przesłaniu danych, jest autoryzacja tej transakcji. Autoryzacja jest tu rozumiana jako sprawdzenie wiarygodności danych o karcie płatniczej oraz stanu samego konta powiązanego z tą kartą. Takie usługi są realizowane przez wyspecjalizowane firmy nazywane powszechnie centrami autoryzującymi. Samą usługę autoryzacji można podzielić na dwa rodzaje, przyjmując za kryterium stopień automatyzacji [4]:

- autoryzacje bez udziału człowieka (nazywana on-line order),
- autoryzacje z udziałem człowieka (nazywana phone/mail/fax order lub w skrócie off-line).

W przypadku autoryzacji on-line klient wpisuje numer karty płatniczej oraz inne dane (najczęściej datę ważności). Następnie dane te są przesyłane do serwera organizacji autoryzującej karty. Tam automat sprawdza poprawność danych, po czym odsyła potwierdzenie autoryzacji albo jej braku.

Inaczej jest w drugim przypadku – autoryzacji off-line, gdzie po wpisaniu danych o karcie przez klienta i po przesłaniu ich do serwera sklepu, sklep telefonicznie, faxem lub modemem przekazuje te dane do centrum autoryzującego, skąd tą samą drogą otrzymuje odpowiedź.

Istnieje wiele firm realizujących takie usługi, choć autoryzacja on-line nie jest dostępna jak na razie w Polsce. Zachodnie firmy zajmujące się autoryzacją to m.in.: Ibill, MultiCards. Za swoje usługi pobierają one poza prowizją, również zryczałtowane opłaty.

2. Przegląd rozwiązań

Z uwagi na wspomniane problemy przy dokonywaniu przez sieć transakcji kartami płatniczymi niezbędne okazuje się wykorzystanie różnorakich technik pozwalających, jeśli nie wyeliminować tych zagrożeń, to przynajmniej je zminimalizować.

Poniżej zostały omówione najczęściej stosowane techniki, także te, które nie rozwiązują problemów bezpieczeństwa, jak i pewne propozycje rozwiązań, które nie zostały jeszcze wdrożone (np. protokół SET jest wciąż jeszcze w fazie eksperymentów).

2.1. Metody „naiwne"

Ta technika nie przewiduje żadnych zabezpieczeń przy dokonywaniu transakcji. Schemat jej działania nie różni się praktycznie niczym od ogólnego schematu przedstawionego na rysunku w poprzednim rozdziale. Jest to metoda bardzo prosta, aczkolwiek nie dająca żadnych gwarancji bezpieczeństwa. Mimo tych wad jest ona wykorzystywana w niektórych sklepach internetowych ze względu na łatwość jej implementacji.

2.2. Szyfrowanie przysłanych informacji w WWW - SSL

Z uwagi na powyższe problemy przy dokonywaniu przez sieć transakcji kartami kredytowymi niezbędne okazuje się wykorzystanie technik kryptograficznych. Zastosowanie szyfrowania z kluczem publicznym pozwala zarówno na utajnienie przesyłanych przez sieć danych (a więc zabezpiecza przed przechwyceniem np. numeru karty kredytowej drogą podsłuchu), jak i - dzięki podpisowi elektronicznemu - wzajemne uwierzytelnienie uczestników transakcji. Wszystkie te cechy spełnia protokół SSL (Secure Socket Layer), który jest obecnie najpopularniejszą metodą zabezpieczania przesyłanych informacji w sieci Internet, szczególnie jeśli chodzi o WWW. Również zdecydowana większość sieciowych sklepów, w których używa się numeru karty kredytowej, korzysta aktualnie z SSL. Z reguły przeglądanie zawartości witryny i wybór towarów do zakupu odbywa się zwykłym (nieszyfrowanym) protokołem HTTP; dopiero końcowy formularz zamówienia, w którym trzeba wpisać dane karty kredytowej, przekazywany jest w sposób "bezpieczny".

System SSL rozwiązuje także niejako "przy okazji" problem weryfikacji sprzedawcy. Serwer stosujący protokół SSL nie tylko bowiem musi posiadać swój klucz publiczny, ale na dodatek klucz ten musi być certyfikowany przez jeden ze znanych przeglądarce tzw. urzędów certyfikacyjnych (*certification authorities*, CA).

Dzięki temu może zweryfikować poprawność certyfikatu, a tym samym fakt, że firma jest w istocie tym, za kogo się podaje. W przypadku gdy serwer nie posiada certyfikatu,

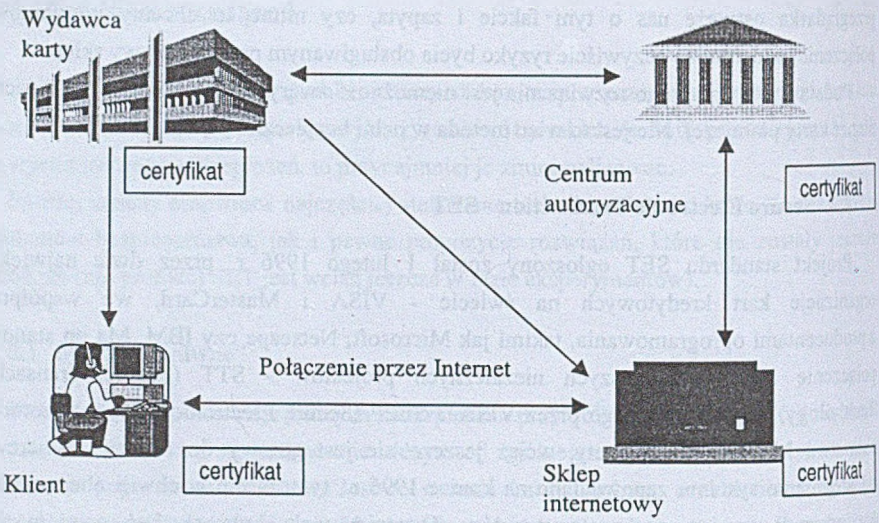
przeglądarka ostrzeże nas o tym fakcie i zapyta, czy mimo to chcemy kontynuować połączenie, podejmując oczywiście ryzyko bycia obsługiwanym przez fałszywy sklep.

Podstawową wadą tego rozwiązania jest niemożność zweryfikowania klienta podającego numer karty płatniczej. Nie jest to więc metoda w pełni bezpieczna [2].

2.3. Secure Electronic Transaction - SET

Projekt standardu SET ogłoszony został 1 lutego 1996 r. przez dwie największe organizacje kart kredytowych na świecie - VISA i MasterCard, we współpracy z producentami oprogramowania, takimi jak Microsoft, Netscape czy IBM. Ma on stanowić połączenie dwu wcześniejszych niezależnych projektów - STT (Secure Transaction Technology), opracowywanego przez VISA, i SEPP (Secure Electronic Payment Protocol), autorstwa MasterCard. Niestety, wciąż jeszcze nie jest gotowy do użytku: komercyjne udostępnienie systemu zapowiadano na koniec 1996 r., tymczasem w chwili obecnej nadal nie wyszedł on jeszcze z etapu testów. Ostatnio wiele było słychać o pierwszych eksperymentalnych transakcjach przeprowadzonych z użyciem SET. Wciąż jednak są to tylko realizacje pilotażowe: nie ma gotowego, ogólnie dostępnego oprogramowania, które obsługiwałoby ten protokół, nie została też jeszcze stworzona niezbędna do działania systemu infrastruktura (np. urzędy certyfikacyjne).

Podobnie jak SSL, system SET również opierać się ma na certyfikatach – w przeciwieństwie jednak do SSL, gdzie certyfikat jest "ogólnym" potwierdzeniem tożsamości serwera bądź użytkownika, certyfikaty stosowane w SET przeznaczone będą tylko i wyłącznie do celów transakcji kartami płatniczymi. Certyfikaty wystawiane będą w sposób automatyczny przez specjalne serwery, zarządzane przez firmy zajmujące się rozliczaniem kart płatniczych. Po połączeniu się z takim serwerem (oczywiście połączenie będzie szyfrowane, np. przez SSL) musimy podać dane naszej karty kredytowej oraz nasze dane osobowe, pozwalające na zweryfikowanie tożsamości (np. numer prawa jazdy, adres zamieszkania itp.). Po sprawdzeniu tych danych w naszym banku (czynność ta odbywa się poza Internetem, poprzez istniejące prywatne sieci międzybankowe służące do autoryzacji kart kredytowych) serwer przesyła do naszego komputera gotowy certyfikat, który zostaje zapamiętany na naszym dysku. Analogicznej procedury - dla uzyskania swojego certyfikatu - musi dopełnić również sprzedawca, który chce przyjmować płatności kartami w systemie SET. Po dopełnieniu tych wstępnych czynności podczas każdej transakcji oprogramowanie sprzedawcy i klienta sprawdza nawzajem swoje certyfikaty, eliminując tym samym z obu stron przypadki oszustwa. Schemat działania protokołu SET przedstawia rysunek 2.



Rys. 2. Ogólny schemat funkcjonowania systemu SET
Fig. 2. General framework of working SET system

System SET nie jest jeszcze ogólnie dostępny. Poza tym jego wdrożenie jest bardzo drogie i wymaga zaangażowania zarówno banków, jak i powstania urzędów certyfikacyjnych [3].

2.4. Rozwiązanie firmy Cyber Cash

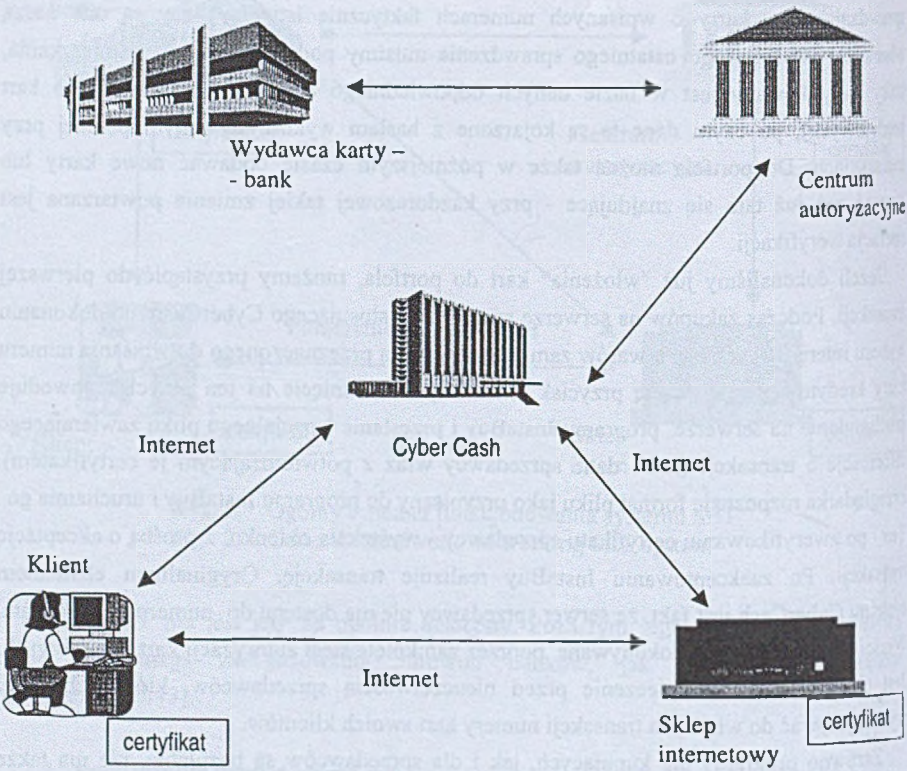
System opracowany przez firmę CyberCash opiera się na założeniach bardzo zbliżonych do SET: wzajemnym sprawdzaniu tożsamości klienta i sprzedawcy w oparciu o certyfikaty (oprogramowanie CyberCash ma być zresztą kompatybilne ze standardem SET, gdy tylko ten zostanie ostatecznie oddany do użytku). W systemie tym po obu stronach używane są specjalizowane programy, współpracujące z przeglądarką lub serwerem WWW: po stronie kupującego - InstaBuy, po stronie sprzedawcy - Cash Register. Do działania systemu niezbędny jest jeszcze obsługujący całość specjalny serwer firmy CyberCash, wykonujący wszelkie czynności związane z bezpośrednią obsługą kart kredytowych. Program InstaBuy instalowany jest jako "helper application" w przeglądarce WWW. Po zainstalowaniu programu użytkownik musi najpierw utworzyć swój "elektroniczny portfel", rejestrując się na serwerze firmy CyberCash. Następnie do utworzonego w ten sposób "portfela" trzeba "włożyć" karty kredytowe, którymi będziemy chcieli się posługiwać w sieciowych transakcjach (może ich być więcej niż jedna: podczas każdej transakcji program będzie oferował nam możliwość wyboru, którą z "włożonych" do portfela kart chcemy zapłacić).

Podczas tej operacji serwer CyberCash dokonuje weryfikacji podanych przez nas danych, sprawdzając, czy karty o wpisanych numerach faktycznie istnieją i czy są one naszą własnością (w celu tego ostatniego sprawdzenia musimy podać nasz adres zamieszkania, który weryfikowany jest w bazie danych odpowiedniego centrum rozliczeniowego kart kredytowych), po czym dane te są kojarzone z hasłem wykorzystywanym później przy transakcjach. Do portfela można także w późniejszym czasie dodawać nowe karty lub usuwać zeń już tam się znajdujące - przy każdorazowej takiej zmianie powtarzana jest operacja weryfikacji.

Jeżeli dokonaliśmy już "włożenia" kart do portfela, możemy przystąpić do pierwszej transakcji. Podczas zakupów na serwerze sprzedawcy stosującego CyberCash, po dokonaniu wyboru interesujących nas towarów zamiast formularza przeznaczonego do wpisania numeru karty kredytowej pojawia się przycisk "InstaBuy" . Kliknięcie na ten przycisk powoduje uruchomienie na serwerze programu InstaBuy i przesłanie specjalnego pliku zawierającego informacje o transakcji (m.in. dane sprzedawcy wraz z potwierdzającym je certyfikatem). Przeglądarka rozpoznaje format pliku jako przypisany do programu InstaBuy i uruchamia go. Ten - po zweryfikowaniu certyfikatu sprzedawcy - wyświetla okienko z prośbą o akceptację transakcji. Po zaakceptowaniu InstaBuy realizuje transakcję. Oryginalnym elementem systemu CyberCash jest fakt, że serwer sprzedawcy nie ma dostępu do numeru karty klienta. Właściwa transakcja jest dokonywana poprzez zamknięte sieci autoryzacji kart kredytowych. Jest to skuteczne zabezpieczenie przed nieuczciwością sprzedawców, którzy chcieliby wykorzystywać do własnych transakcji numery kart swoich klientów.

Zarówno programy dla kupujących, jak i dla sprzedawców są bezpłatne, nie ma także żadnych opłat (wyjąwszy normalne opłaty związane z kartami pobierane przez centra autoryzacyjne) za obsługę kart kredytowych za pomocą systemu.

Ze względu na szerokie rozpowszechnienie, swoją uniwersalność (różne metody płatności) oraz zapowiadaną zgodność z protokołem SET CyberCash wydaje się być dobrym kandydatem na przyszły standard w zakresie internetowych płatności. O tym, że firma poważnie myśli o swoim programie w tym kontekście, świadczy fakt, iż specyfikacja protokołu używanego przez CyberCash została przedstawiona IETF w postaci draftu internetowego - otwarta została zatem droga prowadząca do ewentualnego dokumentu RFC na ten temat [3].



Rys. 3. Ogólny schemat funkcjonowania systemu CyberCash
Fig. 3. General framework of working CyberCash system

2.5. Polski rynek a płatności w Internecie

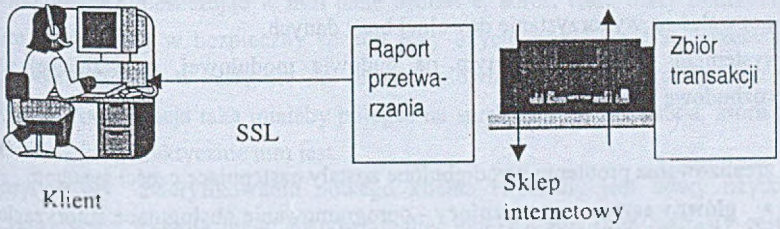
W Polsce znakomita większość sklepów internetowych nie stosuje żadnych systemów zwiększających bezpieczeństwo transakcji internetowych, lub co najwyżej stosuje protokół SSL. Z tych powodów zakupy w Internecie nie cieszą się w Polsce zbyt dużą popularnością. Przyczynia się również do tego w znacznym stopniu postawa rodzimych centrów autoryzujących takie transakcji, których usługi jak na razie ograniczają się tylko do autoryzacji off-line.

Niekwestionowanym liderem na polskim rynku w dziedzinie obsługi kart płatniczych jest firma PolCard. Wszystkie zakupy dokonywane przez Internet traktowane są przez Polcard jako transakcje typu MOTO *(Mail Order, Telephone Order)*, czyli zamówienie składane

listownie lub telefoniczne (rys 4). Są one obarczone większym ryzykiem i dlatego istnieje obowiązek ich autoryzacji (jeśli sprzedający chce mieć gwarancję otrzymania zapłaty) [5].

Sklep internetowy pragnący umożliwić klientom płatności przez Internet musi podpisać z PolCardem umowę wraz z aneksem na zamówienia pocztowe (także telefoniczne), co wiąże się ze spełnieniem określonych przez PolCard wymogów. Dlatego niektóre mniejsze czy mniej znane sklepy internetowe wymagają potwierdzania płatności faksem (co sprawia, że ich oferta jest mniej atrakcyjna dla użytkowników Internetu, dla których taka forma sprzedaży staje się kłopotliwa). Zwyczajowa prowizja wynosi ok. 3-4%.

Nie ma standardowej procedury postępowania. Duża znana firma może od razu zostać zwolniona z obowiązku takiego potwierdzania transakcji. Wiele zależy od oceny konkretnego przypadku, w tym poziomu sprzedaży. Przedstawiciele PolCardu wizytują siedzibę sklepu internetowego i na miejscu oceniają poziom zabezpieczeń (istotną sprawą jest bowiem poufność numerów kart zgromadzonych na serwerze, na którym prowadzony jest wirtualny sklep).



Rys. 4. Schemat transakcji typu MOTO *(Mail Order, Telephone Order)*
Fig. 4. Framework of MOTO trasactions

Właściciele sklepów internetowych narzekają, że są traktowani przez PolCard „po macoszemu", ale z perspektywy tej firmy sprzedaż w sieci na obecnym poziomie przysparza więcej kłopotów niż pożytku. Dla PolCardu obecna wartość transakcji zawieranych na polskim rynku w Internecie stanowi marginalną, wręcz ułamkową część procenta obrotów.

Prowadzone przez PolCard autoryzacje transakcji w sklepach internetowych odbywa się na drodze elektronicznej, lecz nigdy w trybie on-line. Zgromadzone dane są przesyłane do PolCardu (prostym nie szyfrowanym plikiem tekstowym zawierającym podstawowe informacje o autoryzowanych transakcjach poprzez połączenie komutowane do serwera FTP). Stąd są one pobierane (z opóźnieniem nie dłuższym niż doba). Dla domów wysyłkowych taka zwłoka nie stanowi większego problemu, natomiast może utrudniać prowadzenie sprzedaży oprogramowania czy dokumentów, które użytkownik chciałby natychmiast ściągnąć na swój komputer. Zakładane opóźnienie pozbawia możliwości praktycznego działania automatyczne generatory numerów kart kredytowych, które mogłyby przesyłać ko-

lejne numery kart aż do otrzymania pozytywnej odpowiedzi. Dlatego PolCard nie zrezygnuje z autoryzacji w trybie sesyjnym, dopóki kupujący pozostaje anonimowy.

PolCard pracuje obecnie nad rozwiązaniem problemu autoryzacji on-line, w którym numery kart kredytowych nie trafiałyby do internetowego sklepu. Otrzymywałby on jedynie informację o autoryzacji transakcji. Rozwiązanie to niestety jest wciąż w fazie opracowań.

3. Koncepcja rozwiązania problemu

W czasie opracowywania koncepcji systemu przyjęto, że powinien on być:

- dopasowany do warunków, jakie istnieją na polskim rynku. nie powinno to jednak wykluczać go z grona systemów, które mają zastosowanie na rynkach zagranicznych,
- w maksymalnym stopniu elastyczny, pozwalając konfigurować różne stopnie bezpieczeństwa i autoryzacji,
- przenośny, czyli pracować na wielu środowiskach sprzętowych i programowych oraz pozwalać na wykorzystanie dowolnej bazy danych,
- systemem otwartym, opartym na budowie modułowej, pozwalającej na prostą rozbudowę i udoskonalanie.

Do zrealizowania problemu wyodrębnione zostały następujące części systemu:

- **główny serwer autoryzujący** - oprogramowanie obsługujące autoryzacje klienta, sklepu i dokonujące transakcji. Kontakt z tym serwerem jest możliwy tylko dla serwera pośredniczącego i dla centrum autoryzującego płatności CA,
- **serwer pośredniczący** obsługuje bezpośrednio klienta , kontroluje cały proces interakcji z klientem, generuje strony WWW,
- **serwer bazy danych** gromadzi i udostępnia dane z bazy sql-owej,
- **serwer WWW**, którego zadaniem jest zbieranie z sieci komunikatów od klientów i sklepów,
- **serwer sklepu** - oprogramowanie pracujące w środowisku serwera internetowego generuje ofertę towarów w postaci stron WWW, zbiera i realizuje zamówienia oraz obsługuje bazę danych,
- **moduł administracyjny** pozwalający konfigurować system, w szczególności poziomy bezpieczeństwa i formy autoryzacji, a ponadto monitorować aktualnie wykonywane zadania w systemie i udostępniać statystyki takich zadań. Moduł ten działa niezależnie od systemu, co oznacza, że nie musi być on uruchomiony, by system funkcjonował,

- **oprogramowanie klienta** - oprogramowanie uruchamiane na przeglądarce klienta, odpowiedzialne za bezpieczną autoryzację klienta,
- **moduł do kontaktu z centrum autoryzacyjnym CA** - oprogramowanie oparte na zdefiniowanym wcześniej API odpowiedzialne za kontakt i realizacje transakcji z CA,
- **centrum autoryzujący płatności – CA** - organizacja zajmująca się realizacją i autoryzacją transakcji kartami płatniczymi w sieci Internet.

Proces funkcjonowania tak zaprojektowanego rozproszonego systemu obsługi płatności wyglądałby następująco (rys.5).

Użytkownik sieci zestawia połączenie z Internetem, uruchamia przeglądarkę, łączy się z wybranym przez siebie sklepem internetowym, wybiera towary i ostatecznie dokonuje zapłaty kartą płatniczą poprzez system obsługi transakcji elektronicznych.

Pierwsze wejście klienta wiąże się z jego rejestracją w systemie. W tym celu musi wypełnić formularz, umieszczając w nim dane osobowe, adres, dane karty płatniczej oraz swoje hasło. Dane te są w bezpieczny sposób przy użyciu protokołu SSL przesyłane do serwera pośredniczącego, a następnie do serwera głównego, który dokonuje autoryzacji nowego klienta. Autoryzacja taka miałaby polegać na sprawdzeniu, czy osoba, która podaje się za właściciela karty, faktycznie nim jest.

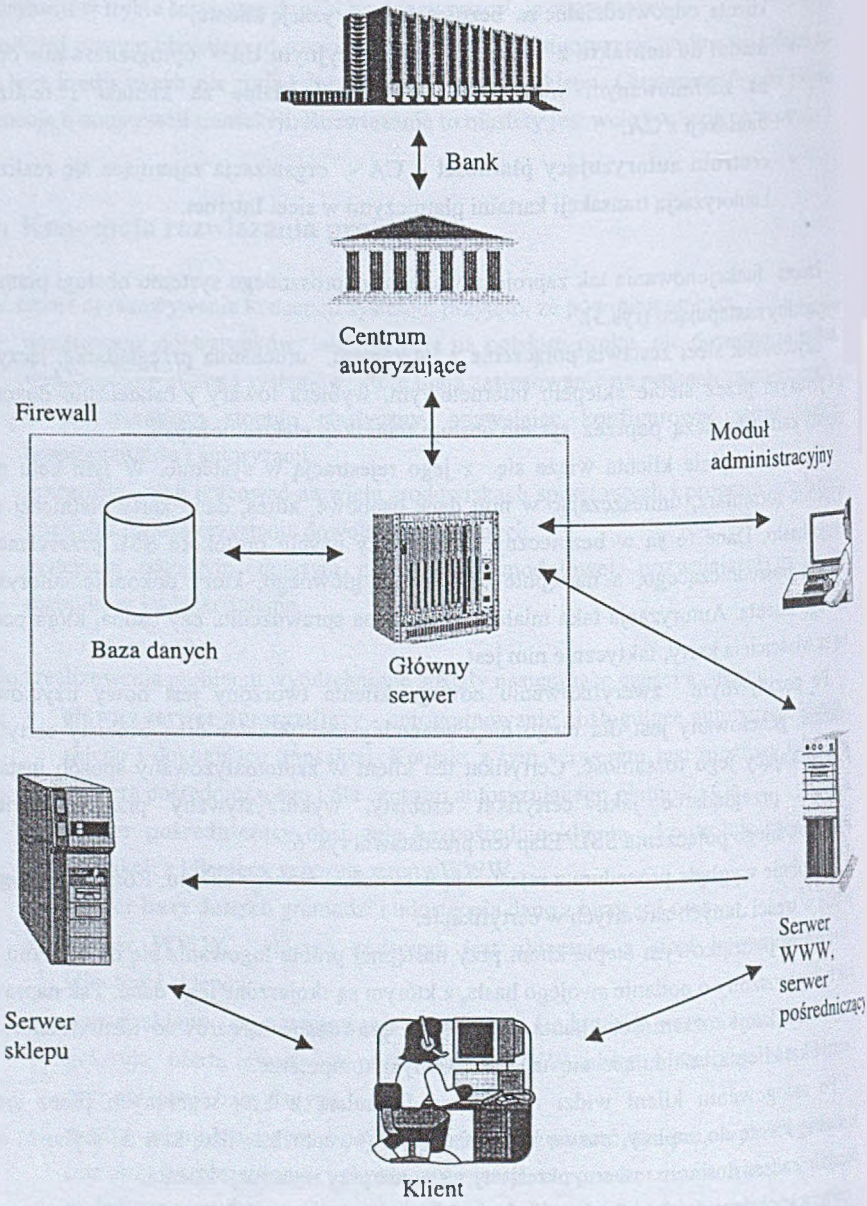
Po pozytywnym zweryfikowaniu nowego klienta tworzony jest nowy użytkownik systemu, generowany jest dla niego niepowtarzalny identyfikator oraz osobisty certyfikat potwierdzający jego tożsamość. Certyfikat ten klient w zautomatyzowany sposób instaluje w swojej przeglądarce jako certyfikat osobisty, wykorzystywany przy zestawieniu autoryzowanego połączenia SSL. Etap ten przedstawia rys. 6.

Podobnie wygląda procedura z rejestracją w systemie nowego sklepu. Różnica występuje jednie w treści danych zawartych w certyfikacie.

Po tym początkowym etapie klient przy następnej próbie logowania się do systemu jest już tylko proszony o podanie swojego hasła, z którym są skojarzone jego dane. Tak naprawdę przy weryfikacji tożsamości klienta dodatkowo sprawdzane są zarówno identyfikator, jak i certyfikat klienta, znajdujące się na jego lokalnym komputerze.

Po zalogowaniu klient widzi na ekranie formularz z listą wybranych przez siebie towarów, kwotę do zapłaty, nazwę karty płatniczej (ewentualnie listę kart do wyboru) oraz domyślny adres dostawy towaru, określony wstępnie przy rejestracji klienta.

Po wypełnieniu wszystkich pól formularza następuje przesłanie danych do serwera pośredniczącego, dalej do serwera głównego i w końcu dokonywana jest właściwa transakcja w centrum autoryzującym płatności. Wszystkie przesyły są szyfrowane w celu zapewniania poufności danych.

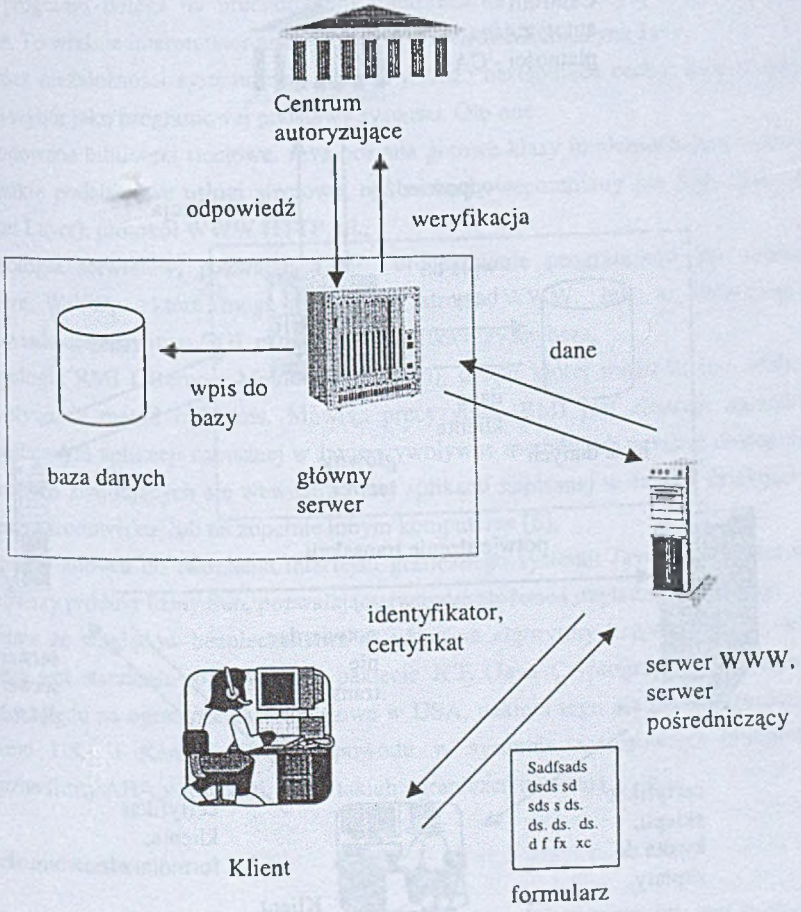


Rys. 5. Schemat projektowanego systemu obsługi transakcji w Internecie
Fig. 5. Framework of project transaction service system in internet

Centrum autoryzujące po zweryfikowaniu konta klienta zwraca odpowiedź pozytywnej bądź negatywnej autoryzacji. Informacja o odpowiedzi do klienta jest generowana przez serwer pośredniczący w postaci strony WWW, natomiast serwer sklepu jest informowany przez wywołanie określonych wcześniej skryptów (np. CGI) lub programów (np. serwlety).

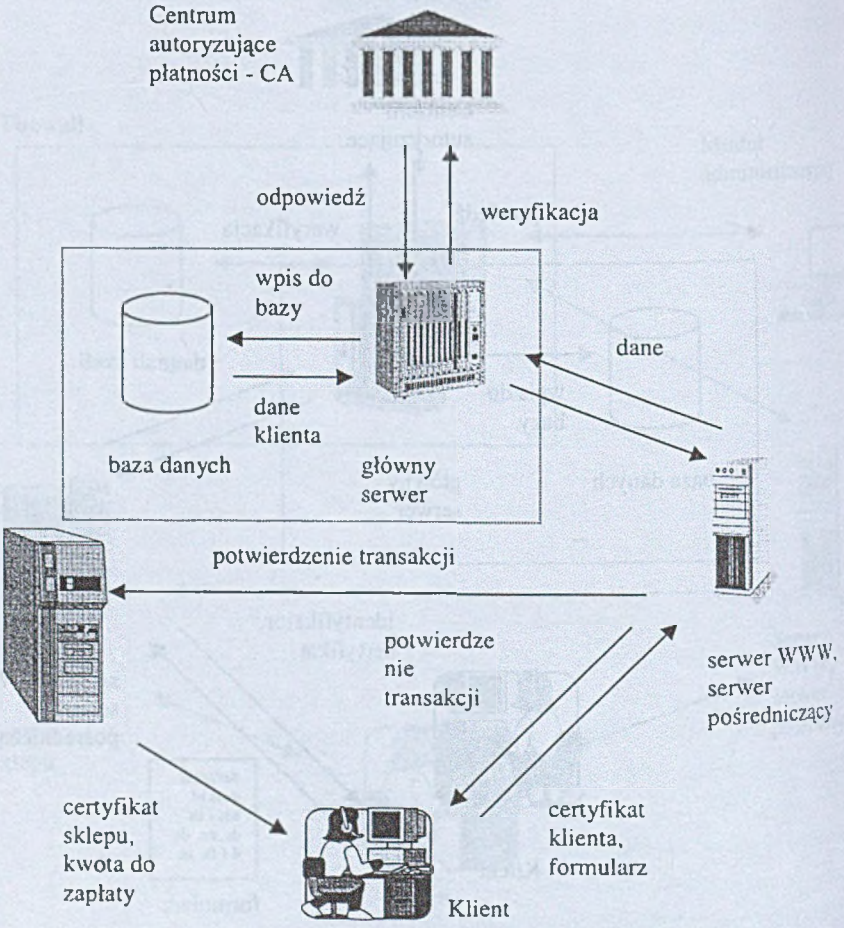
Na podstawie tej odpowiedzi sklep realizuje bądź odmawia sprzedaży towaru.

Wszelkie transakcje są zapisywane w systemie i w każdej chwili możliwe jest przejrzenie historii dokonanych transakcji. Zapisy te mogą również stanowić dowody przy ewentualnych nieporozumieniach stron biorących udział w transakcji.



Rys.6. Schemat rejestracji użytkownika w systemie
Fig. 6. Framework of registration user in system

Jak pokazano na rys. 5, w systemie występuje moduł administratora, którego podstawową funkcją jest monitorowanie systemu, pozwalające sprawdzić, w jakim stanie jest każda transakcja aktualnie realizowana w systemie. Poza tym udostępnia statystyki i informacje związane z każdym z klientów. Ponieważ wszystkie te dane są tajne, dostęp do nich powinien być ściśle chroniony, co jest realizowane przez wymóg znajomości hasła w chwili rozpoczęcia pracy z modułem. Poza tym program może być uruchomiony tylko z określonego wcześniej komputera, by mógł zostać przepuszczony przez „mur" bezpieczeństwa, jaki „stawia" firewall. Etap realizacji transakcji przedstawia rys 7.



Rys. 7. Schemat etapu dokonania transakcji w systemie
Fig. 7. Framework of accomplishment stage of transaction in system

3.1. Wybór narzędzi

System został zbudowany w oparciu o język programowania Java, który dzięki swym cechom pozwolił zrealizować założenie o przenoszalności sytemu pomiędzy różne platformy systemowe. Java to język niezależny systemowo, co oznacza, że programy pisane w tym języku mogą działać na każdym komputerze, dla którego stworzona została wirtualna maszyna Javy. Środowisko Javy składa się z dwóch części: kompilatora i interpretatora. Kompilator tłumaczy kod źródłowy i generuje tzw. kod bajtowy. Są to instrukcje przypominające kod maszynowy, jednak nie są one charakterystyczne dla żadnego procesora. Wykonanie programu polega na uruchomieniu interpretatora, który czyta kody bajtowe i wykonuje je. To właśnie interpretator nazywa się często wirtualną maszyną Javy.

Java oprócz niezależności systemowej posiada jeszcze następujące cechy, które miały wpływ na jej wybór jako programowej podstawy systemu. Oto one:

- rozbudowane biblioteki sieciowe. Java posiada gotowe klasy implementujące niemal wszystkie podstawowe usługi sieciowe, np. sockety, wspomniany już SSL (Secure Socket Layer), protokół WWW HTTP itd.,
- technologia serwletów, pozwalająca na uruchamianie programików po stronie serwera WWW, które mogą generować strony WWW. Jest to technologia odpowiadająca skryptom CGI, przy czym jest kilka razy szybsza,
- technologia RMI (Remote Method Invocation), dzięki której możliwe jest zdalne wywoływanie metod obiektów. Mówiąc precyzyjnie, RMI jest zbiorem narzędzi pozwalającym aplikacji napisanej w Javie wywoływać metody lub uzyskać dostęp do zmiennych znajdujących się wewnątrz innej aplikacji napisanej w Javie i działającej w innym środowisku, lub na zupełnie innym komputerze [6],
- biblioteka służąca do tworzenia interfejsu graficznego systemu Java Swing. Jest to najnowszy produkt firmy Sun, pozwalający tworzyć złożone i użyteczne interfejsy.

W systemie ze względów bezpieczeństwa są używane algorytmy kryptograficzne. Ich implementacja jest standardowo zawarta w pakiecie JCE (Java Cryptography Extension), jednakże ze względu na ograniczenia eksportowe w USA, pakietu tego nie można stosować poza terenami USA i Kanady. Z tego powodu w systemie zastosowano biblioteki kryptograficzne firmy ABA z Australii, które takich ograniczeń nie mają.

3.2. Podsumowanie

Przedstawiona tu koncepcja rozwiązania problemu płatności w sieci Internet posiada następujące cechy:

Podział systemu na kilka wyodrębnionych części, tj. serwer pośredniczący, serwer autoryzujący i część administracyjną czyni system elastycznym, a jednocześnie bezpiecznym,

dzięki ograniczeniu liczby komputerów mających dostęp do serwera autoryzującego i znajdujących się tam danych. Jednocześnie serwer pośredniczący może oferować dodatkowe funkcje, dzięki czemu możliwa jest hierarchiczna rozbudowa systemu.

Bezpieczeństwo dokonywanych transakcji, oparte na tajnym haśle, certyfikatach osobistych i szyfrowaniu, jest skutecznym rozwiązaniem, które jednocześnie nie obciąża zbytnio użytkownika systemu dodatkowymi czynnościami, które by musiał wykonać dla zachowania odpowiedniego poziomu bezpieczeństwa

Wykorzystanie języka programowania Java pozwoliło osiągnąć dużą elastyczność systemu, jeśli chodzi o działanie na różnych platformach systemowych. Jednocześnie język ten zawiera wiele technologii, które okazały się niezwykle pomocne przy realizacji projektu, tj. Serwlety i RMI. Należy tu jeszcze zaznaczyć, że pojawiają się wciąż nowe technologie w obrębie języka, jak np. JSSA.

LITERATURA

1. Adamczyk M.: E-biznes w małej i średniej firmie. PC Kurier nr 19/99.
2. Problematyka płatności w Internecie – materiały z konferencji 18.05.99, Warszawa.
3. Rafa J.: Internet i pieniądze. Internet 12/97.
4. Garfinkiel S., Spafford G.: Web Security & Commerce.
5. Gamdzyk P.: Ryzyko wygody. ComputerWorld nr 24/99.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 7 kwietnia 2000 r.

Abstract

This article describes problem of electronic payments in internet distributed systems with special taken into consideration specificity of Polish market.

In the first chapter were described general information about payments, security and authorizetion of transactions.

In the second chapter we have present existing solutions in the world. We have chosen only very popular ones like: SSL (Secure Socket Layer), SET (Secure Electronic Transaction) , CyberCash. We have also present solution, which existing on Polish market - MOTO (*Mail Order, Telephone Order)* created by PolCard.

In the last chapter we have described conception of electronic payments, which focuses on a problem of security and openness of system. This conception makes use of advantages of certification mechanism and flexibility of Java language.