

SET (Secure Electronic Transaction)

Krzysztof Maćkowiak

Wprowadzenie

SET (*Secure Electronic Transaction*) [1] to protokół bezpiecznych transakcji elektronicznych. Jest standardem umożliwiającym bezpieczne przeprowadzanie transakcji z wykluczeniem bezpośredniego kontaktu przez Internet, z użyciem kart kredytowych. Projekt ten został ogłoszony 1 lutego 1996 roku. Popierany jest przez dwie największe organizacje związane z kartami płatniczymi – VISA i MasterCard oraz wspierany przez firmę IBM. Protokół ten posiada cechy następujących technologii: SSL (*Secure Socket Layer*) [2], STT (*Secure Transaction Technology*), SEPP (*Secure Electronic Payment Protocol*) oraz S-HTTP (*Secure Hypertext Transfer Protocol*). SET rozszerza możliwości SSL przez wprowadzenie identyfikacji drugiej strony - klienta. Protokół zawiera, więc mechanizmy identyfikacji obu stron. Została wyeliminowana możliwość podejrzenia numeru karty przez sprzedawcę – zakodowane numery kart przesyłane są wprost do firmy zajmującej się ich obsługą.

Do przeprowadzenia transakcji wymagane są:

- po stronie klienta – przeglądarka internetowa Netscape Navigator lub Internet Explorer w wersji od 4.0 wzwyż, system operacyjny posiadający mechanizmy służące do obsługi certyfikatów (np. repozytorium).
- po stronie sprzedawcy – serwer obsługujący protokół SET.

Certyfikaty, w przeciwieństwie do SSL, stosowane są jedynie do transakcji z udziałem kart płatniczych. Firmy, zajmujące się rozliczaniem kart kredytowych, zarządzają specjalnymi serwerami, które w sposób automatyczny wystawiają certyfikaty. Osoba, chcąc uzyskać certyfikat, łączy się z takim serwerem szyfrowanym połączeniem i podaje swoje dane osobowe oraz dane związane z posiadaną kartą kredytową. Dane te następnie sprawdzane są przez prywatne sieci międzybankowe, które służą do autoryzacji kart kredytowych. W przypadku, gdy weryfikacja jest poprawna zostaje wydany certyfikat.

Zapewnienie dwóch stron o wiarygodności partnera podczas przeprowadzania każdej transakcji, jest uzyskiwane poprzez sprawdzanie certyfikatów po obu stronach.

Strony wyróżniane w protokole SET:

- **kupujący** (klient) zamawiający towary u sprzedawcy i dokonujący zapłaty,
- **sprzedawca** oferujący towary, usługi oraz zapewniający przeprowadzenie transakcji,
- **bank** będący instytucją finansową, która założyła konto klientowi i wydała mu kartę kredytową,
- **centrum autoryzacji** dokonujące autoryzacji kart płatniczych oraz płatności,
- **brama autoryzacji** przetwarzająca komunikaty sprzedawcy w czasie realizacji płatności elektronicznych,
- **system płatniczy** np. VISA, MasterCard ustalający mechanizmy obsługi i akceptacji kart płatniczych.

Zanim klient i sprzedawca będą mogli korzystać z protokołu SET muszą się zarejestrować. Rejestracja klienta i sprzedawcy polega na wystawieniu certyfikatu przez centrum autoryzacyjne (CA).

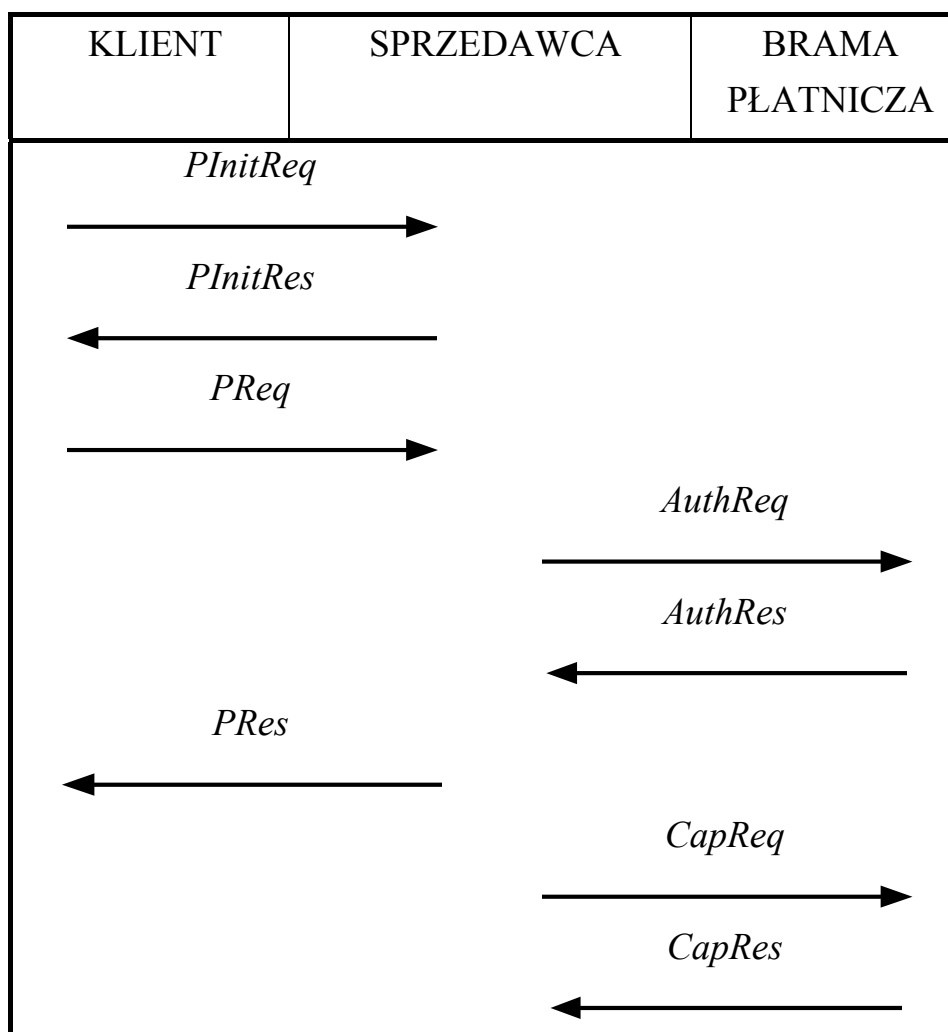
Przebieg transakcji elektronicznej:

- przeglądanie i zakupy,
- wybór sprzedawcy i towaru,
- negocjacje i zamówienie,
- wybór sposobu płatności,
- żądanie przeprowadzenia transakcji (SET),
- uwierzytelnianie płatności (SET),
- dostarczenie towaru,
- przeprowadzenie płatności (SET).

Tylko trzy zaznaczone procesy są wykonywane z wykorzystaniem protokołu SET.

Protokół SET jest wykorzystywany, gdy klient jako sposób płatności wybierze kartę kredytową.

Transakcja SET:



Rys.1. Komunikaty podstawowej transakcji.

Komunikaty transakcji SET opisane są poniżej.

PlnitReq – żądanie rozpoczęcia transakcji, zawiera informację o systemie płatniczym.

PlnitRes – identyfikator transakcji podpisany kluczem prywatnym sprzedawcy oraz zawierający certyfikaty: sprzedawcy i bramy płatniczej.

PReq – złożenie zamówienia.

AuthReq – żądanie uwierzytelnienia płatności.

AuthRes – odpowiedź potwierdzająca weryfikację klienta, sprzedawcy i transakcji w banku.

PRes – w przypadku poprawnej weryfikacji, sklep potwierdza przeprowadzenie transakcji.

CapReq, CapRes – realizacja płatności.

Wszystkie te komunikaty są obowiązkowe i występują w każdym procesie transakcji. Dodatkowo mogą występować jeszcze opcjonalne komunikaty m.in. AuthRevReq, AuthRevRes – stosowane do zmiany lub anulowania procesu uwierzytelniania.

Etap uwierzytelnienia (AuthReq/AuthRes)

Ze względu na bezpieczeństwo transakcji najważniejszym etapem jest etap uwierzytelnienia. Uwierzytelnienie służy zapewnieniu, że otrzymane dane zostały wysłane przez określoną osobę. Na podstawie otrzymanych danych odbiorca może zidentyfikować nadawcę tych danych. Proces ten jest dokonywany z użyciem podpisu cyfrowego oraz certyfikatów wystawianych przez CA. W protokole SET uwierzytelnieniu podlegają: kupujący, sprzedawca oraz brama płatnicza.

Proces uwierzytelniania składa się z dwóch wiadomości: prośby uwierzytelnienia (AuthReq) generowanej przez sprzedawcę i wysyłanej do bramy płatniczej oraz odpowiedzi generowanej przez bramę płatniczą i przesyłanej do sprzedawcy. Wiadomości te używane są zarówno w transakcjach uwierzytelniania jak i w transakcjach sprzedaży.

Para komunikatów dostarcza sprzedawcy mechanizm do dokonania uwierzytelnienia związanego z realizacją zakupów.

Sprzedawca generując prośbę o uwierzytelnienie wysyła dane związane z realizacją zakupów, które są podpisane i zaszyfrowane oraz dodatkowe informacje (PI) otrzymane od osoby dokonującej zakupu. Przesłane informacje zawarte są w komunikacie AuthReq i służą do dokonania uwierzytelnienia, które wykonuje brama płatnicza z wykorzystaniem sieci międzybankowych.

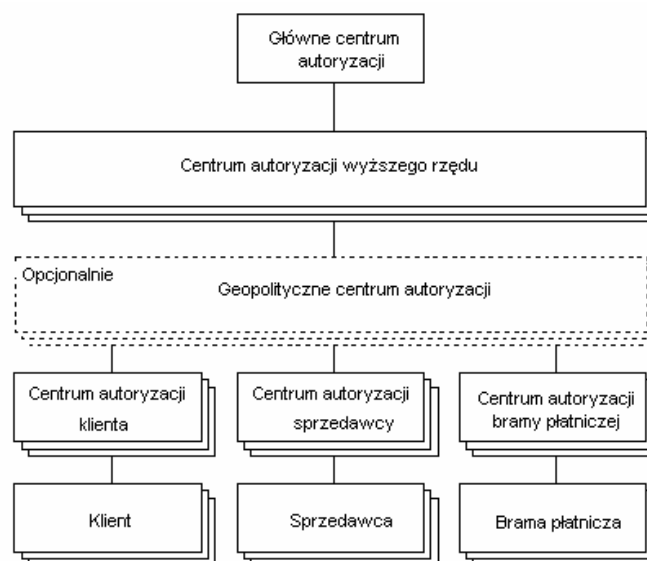
Brama płatnicza korzystając z sieci międzybankowych przeprowadza proces uwierzytelnienia, w wyniku czego generowany jest komunikat i przesyłany do sprzedawcy, który zwracał się z prośbą o uwierzytelnienie.

Algorytmy używane w protokole SET:

- Certyfikaty – X.509v3
- Szyfrowanie symetryczne – DES CBC, CDMF.
- Szyfrowanie asymetryczne – RSA z kluczami o długości 1024 i 2048 bitów.
- Podpis cyfrowy – RSA.
- Funkcja skrótu – SHA-1 generująca skrót o długości 160 bitów.

System certyfikatów występujący w protokole SET:

- certyfikat klienta (*Cardholder*),
- certyfikat sprzedawcy (*Merchant*),
- certyfikat bramy płatniczej (*Payment Gateway*),
- certyfikat centrum autoryzacji klienta (banku) (*Cardholder CA*),
- certyfikat centrum autoryzacji sprzedawcy (*Merchant CA*),
- certyfikat centrum autoryzacji bramy płatniczej (*Payment Gateway CA*),
- certyfikat geopolitycznego centrum autoryzacji (*Geo-Political CA*),
- certyfikat wyższego rzędu (*Brand CA*),
- certyfikat główny (*Root CA*).



Największym problemem związanym z wprowadzeniem protokołu SET w życie jest problem z masowym generowaniem certyfikatów dla każdego klienta i jednoczesnym zapewnieniu ich wiarygodności oraz pełnej identyfikacji użytkowników. Jednym z możliwych rozwiązań może być wydawanie certyfikatu wraz z kartą kredytową w banku.

Literatura

1. <http://www.setco.org>, Maj 2003.
2. <http://www.openssl.org>, Maj 2003.