Jak otrzymać certyfikat SSL na przykładzie Thawte

Jacek Piechota
Centrum Bezpieczeństwa Sieciowego SA
ul. Gizów 6, 01-249 Warszawa
e–mail: jp@cbs.pl

Abstrakt. Certyfikaty SSL firmy Thawte potwierdzają tożsamość właściciela serwera WWW udostępniającego usługi wymagające zabezpieczenia poprzez szyfrowanie transmisji pomiędzy serwerem WWW, a użytkownikiem końcowym. Stosowanie protokołu SSL zabezpiecza cały proces komunikacji z odbiorcami informacji przesyłanych za pośrednictwem serwera WWW, a więc umożliwia składanie zamówień płatnych kartą kredytową, zabezpiecza ważne dane osobowe klientów i zapewnia zwiększenie odporności systemu informatycznego firmy na działania hackerów. Obecnie, stosowanie SSL z kluczem 128 bitowym w zasadzie całkowicie zabezpiecza przed „podsłuchem" ruchu przechodzącego przez serwer WWW firmy.

1. Wprowadzenie

Przeglądarki internetowe mogą działać w trybie normalnym lub bezpiecznym. To, w jakim trybie pracuje przeglądarka można określić np. na podstawie paska stanu w przeglądarce. Jeżeli pojawia się tam symbol złamanego klucza lub też otwartej kłódki, przeglądarka pracuje w trybie normalnym. Jeżeli pojawia się symbol klucza umieszczonego w dziurce lub zamkniętej kłódki[1], przeglądarka działa w trybie bezpiecznym.

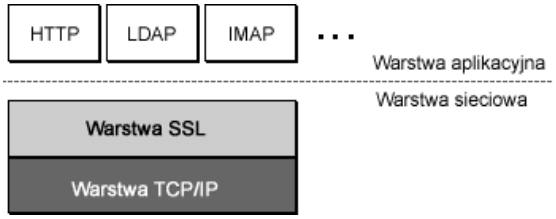
Gdy przeglądamy zasoby Internetu w trybie normalnym przeglądarki, informacje wysyłane i otrzymywane przez przeglądarkę są jawne dla potencjalnych podglądaczy. Natomiast kiedy przeglądarka jest w trybie bezpiecznym, wszelkie informacje pomiędzy nią a serwerem są szyfrowane – „podglądacze" zobaczą tylko bezładny ciąg znaków, tzw. „krzaki". To właśnie jest jednym z elementów bezpieczeństwa przy przesyłaniu informacji.

Szyfrowanie informacji odbywa się w oparciu o certyfikaty cyfrowe, zwane również paszportami cyfrowymi. Certyfikat cyfrowy zawiera nazwę firmy, serwera WWW lub dane personalne, razem z kluczem kryptograficznym używanym do szyfrowania przesyłanej informacji. Kiedy przeglądarka przełącza się na tryb bezpieczny, żąda od serwera WWW przedstawienia jego certyfikatu. Następnie przeglądarka na podstawie informacji o wydawcy certyfikatu decyduje, czy ma zaufać certyfikatowi, czy też nie. Jeśli decyzja jest na „tak", jak to ma miejsce w przypadku certyfikatów wydawanych przez Thawte, wszelka informacja przesyłana pomiędzy przeglądarką a serwerem zostanie zaszyfrowana przy użyciu klucza kryptograficznego zawartego w certyfikacie.

Certyfikatów cyfrowych można również używać do uruchamiania serwerów sieciowych w trybie bezpiecznym. Można ich również używać do podpisywania i szyfrowania wiadomości w poczcie elektronicznej oraz do cyfrowego podpisywania oprogramowania, dzięki czemu zostanie zagwarantowana jego „nienaruszalność".

Podpisywaniem i wydawaniem certyfikatów cyfrowych zajmują się instytucje certyfikujące (*Certificate Authority* lub w skrócie CA). Instytucji takich jest wiele, ale szczególnie popularne są

[1] W przeglądarce Internet Explorer, w prawej części paska stanu jest wyświetlana kłódka. Co więcej, wybierając z menu „Plik" polecenie „Właściwości" na karcie Zabezpieczenie - zobaczymy certyfikat autentyczności (podpis cyfrowy) danej strony. Natomiast w przeglądarce Netscape Communicator kłódka pokazuje się na pasku nawigacji (Navigation Toolbar). Wybierając opcję Security (Toolbar) możemy obejrzeć (View Certificate) certyfikat autentyczności danej strony.



firmy Verisign i Thawte (od lutego 2000 r. Thawte należy do Verisign). Thawte posiada swoje przedstawicielstwa w ponad 20 krajach.

2. Połączenia w trybie normalnym i bezpiecznym

Cała wymiana informacji w sieci Internet odbywa się za pośrednictwem protokołu TCP/IP (*Transmission Control Protocol/Internet Protocol*). Protokół TCP/IP umożliwia przesłanie danych z jednego komputera na dowolny inny znajdujący się w Internecie za pośrednictwem innych komputerów oraz podsieci tworzących Internet. TCP/IP zarządza przesyłaniem i rozdzielaniem danych w Internecie. Inne protokoły w warstwie aplikacyjnej, takie jak HTTP (*HyperText Transport Protocol*), LDAP (*Lightweight Directory Access Protocol*) czy też IMAP (*Internet Messaging Access Protocol*) wykorzystują TCP/IP do wykonywania swoich standardowych zadań, to znaczy wyświetlanie stron WWW czy też obsługa serwera poczty elektronicznej.

Połączenie między naszym komputerem i dowolnym węzłem w Internecie może nastąpić za pośrednictwem dziesiątków innych podsieci i komputerów, z których każdy może być w prosty sposób monitorowany. Internet nie jest jednolitym tworem, lecz konglomeratem tysięcy mniejszych i większych sieci: firmowych, uczelnianych, miejskich, regionalnych, krajowych i międzynarodowych. Aby użyć obrazowego porównania, korzystanie z usług Internetowych w trybie normalnym (nieszyfrowanym) można uznać za rozmowę pomiędzy dwoma osobami w zatłoczonym pomieszczeniu. Liczba osób mających dostęp do łącz i urządzeń sieciowych na drodze przesyłanych danych może być rzędu setek, przy czym każda z tych osób ma możliwość techniczną przechwycenia („podglądnięcia") przesyłanej informacji. Co więcej, do łącz sieciowych (podobnie jak i do innych łącz telekomunikacyjnych) mogą zyskać dostęp osoby nieupoważnione.

Jest zatem oczywiste, że zaszyfrowanie danych do postaci niezrozumiałej dla osób niepowołanych zabezpiecza te dane przed „kradzieżą". W pewnym stopniu, zabezpiecza je również przed sfałszowaniem: fałszerz wprowadzający modyfikacje do danych zaszyfrowanych nie wie, jaki będzie rezultat modyfikacji - po rozszyfrowaniu zazwyczaj otrzymane zostaną dane nonsensowne; tym samym nie jest w stanie sfałszować ich zgodnie ze swoim zamierzeniem. Zagadnienie szyfrowania jest kluczowe w handlu elektronicznym, gdzie typową formą płatności w takich transakcjach jest podanie numeru karty kredytowej.

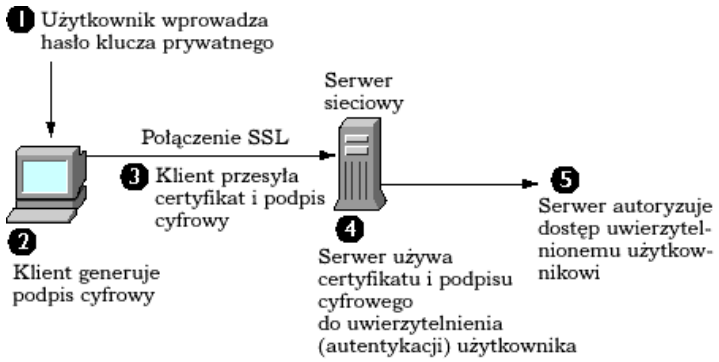
Jeśli chodzi o szyfrowanie przesyłanych danych największą popularność zdobyły dwa standardy: SSL (Secure Socket Layer) opracowany przez firmę Netscape i SSH (Secure Shell) firmy SSH Communications. Zdecydowanie bardziej rozpowszechniony jest ten pierwszy standard, ze względu na fakt jego zaimplementowania w najpopularniejszych przeglądarkach WWW (Netscape Communicator, Microsoft Internet Explorer, Lynx etc.) i serwerach WWW (ApacheSSL, Stronghold, Microsoft Internet Information Server). SSL korzysta z algorytmów RSA lub D-H, oraz z szyfrów symetrycznych DES, 3DES, RC2, RC4, IDEA i Fortezza. Szyfrem symetrycznym jest szyfrowane połączenie/sesja, zaś klucz szyfru jest na potrzeby każdej sesji generowany losowo i przekazywany z użyciem szyfru z kluczem publicznym. Dodatkowo, klucz publiczny RSA serwera i/lub klienta może być certyfikowany przez CA (w standardzie X.509) - pozwala to klientowi upewnić się, że połączył się z właściwym serwerem, a serwerowi zweryfikować tożsamość klienta. Istnieje obecnie kilka firm odpłatnie wydających takie certyfikaty, np. Verisign czy Thawte, których certyfikaty są automatycznie rozpoznawane przez większość przeglądarek WWW, np. Netscape.

Rys. 1. Umiejscowienie protokołu SSL w warstwach

Protokół SSL działa (rysunek 1) pomiędzy warstwą TCP/IP a protokołami wyższego rzędu (aplikacyjnymi), takimi jak IMAP czy też HTTP (a w zasadzie HTTPS - port 443 TCP, który jest zgodny z HTTP, ale posiada rozszerzenia umożliwiające przesyłanie informacji niezbędnych do szyfrowania, potwierdzania certyfikatów itd.). SSL pośredniczy w komunikacji pomiędzy TCP/IP a protokołami warstwy aplikacyjnej, umożliwiając uwierzytelnienie (autentykację) serwera, na którym jest zainstalowany, wobec oczekującego klienta i vice versa, ustanawiając w ten sposób połączenie szyfrowane (rysunek 2).

Rys. 2. Schemat procesu autentykacji z wykorzystaniem protokołu SSL i certyfikatu

Można zatem zadać uzasadnione pytanie, czy nie powinno się szyfrować wszystkich danych wymienianych pomiędzy serwerem a klientem? Gdyby dane te były zawsze szyfrowane (zamiast przesyłania przynajmniej części z nich w postaci jawnej), na skutek uruchomienia procedur szyfrujących połączenie zostałoby znacząco spowolnione. Przy przesyłaniu jednej formatki WWW może to nie zostać zauważone, natomiast w momencie szyfrowania całej wymiany informacji wydajność znacząco się pogorszy.



3. Co to jest certyfikat cyfrowy?

Certyfikat cyfrowy jest po prostu poświadczeniem podpisanym przez niezależną i wiarygodną instytucję (trzecią stronę). Postać poświadczenia jest zwykle określona standardem X.509, ale nie jest to niezbędne.

Certyfikat cyfrowy zawiera trzy elementy:

- **Nazwa oraz informacje dodatkowe** - jest to wszelka informacja dotycząca certyfikowanego podmiotu. W przypadku osoby fizycznej może się tu znaleźć nazwisko, narodowość, adres poczty elektronicznej, miejsce pracy, departament itd. Można również umieścić swoje zdjęcie, odciski palców, numer paszportu.
- **Informacja o Kluczu Publicznym** - jest to klucz publiczny certyfikowanego podmiotu. Certyfikat wiąże klucz publiczny z informacjami zawartymi powyżej. Klucz publiczny może być dowolnym kluczem asymetrycznym, ale zwykle jest to klucz RSA.
- **Podpis Instytucji Certyfikującej** - instytucja certyfikująca podpisuje powyższe dwa elementy i nadaje wiarygodność certyfikatowi. Ci, którzy otrzymają certyfikat sprawdzają podpis i mogą zaufać zawartym w certyfikacie informacjom o podmiocie i kluczowi publicznemu, jeśli oczywiście zaufają instytucji certyfikującej.

Certyfikat jest więc uwierzytelnieniem dokumentu elektronicznego zawierającego informację o właścicielu i klucz publiczny, autoryzowanego przez instytucję autoryzującą. Certyfikat taki może mieć wiele postaci, ale zwykle ich format jest określony standardem X.509, istniejącym od wielu lat i należącym do grupy standardów OSI. Certyfikaty w formacie X.509 są bardzo przejrzyście

definiowane przy użyciu notacji zwanej ASN.1 (*Abstract Syntax Notation 1*), która precyzyjnie specyfikuje typy danych binarnych wchodzących w skład certyfikatu.

ASN.1 może być zaszyfrowany na wiele sposobów, ale coraz powszechniejszym standardem staje się enkrypcja zwana DER (*Distinguished Encoding Rules*), której wynikiem jest zwarty certyfikat binarny. W przypadku wiadomości poczty elektronicznej certyfikat binarny będzie zakodowany w oparciu o standard Base64, a w efekcie końcowym będzie wyglądał jak dokument tekstowy ASCII:

```
-----BEGIN CERTIFICATE-----
MIICWDCCAgICAQAwDQYJKoZIhvcNAQEEBQAwgbYxCzAJBgNVBAYTAlpBMRUwEYDjabfHSkbdNvbTAe
VQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNVBAcTCUNhcGUgVG93bjEdMBsGA1UEChMUjVaFw05NjEyMTQ
VGhhd3RlIENvbnN1bHRpbmcgY2MxHzAdBgNVBAsTFkNlcnRpZmljYXRpb24gU2VymljZXMxFzAVBgN
dmljZXMxFzAVBgNVBAMTDnd3dy50aGF3dGUuY29tMSMwIQYJKoZIhvcNAQkBFhR3vcNAQkBFhRjkTR
ZWJtYXN0ZXJAdGhhd3RlLmNvbTAeFw05NjExMTQxNzE1MjVaFw05NjEyMTQxNzE1GNjMR8wAQkTRE4
MjVaMIG2MQswCQYDVQQGEwJaQTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRIwEAYD98JkjhgKL8FDrY
VQQHEwlDYXBlIFRvd24xHTAbBgNVBAoTFFRoYXd0ZSBDb25zdWx0aW5nIGNjMR8wAQkBFhR3vcNAgf
e5L4y3c/ViKdlou5BcQYAbxA7rwO/vz4m51w4w==
-----END CERTIFICATE-----
```

Jeśli odkodować taki certyfikat np. przy użyciu oprogramowania SSLeay ujrzymy certyfikat w postaci jawnej:

```
Certificate:
    Data:
        Version: 0 (0x0)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5withRSAEncryption
        Issuer: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services, CN=www.thawte.com,
                Email=webmaster@thawte.com
        Validity
            Not Before: Nov 14 17:15:25 1996 GMT
            Not After : Dec 14 17:15:25 1996 GMT
        Subject: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                 OU=Certification Services, CN=www.thawte.com,
                 Email=webmaster@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Modulus:
                    00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:
                    55:32:bb:26:de:0a:48:d8:fc:c8:c0:c8:77:f6:5d:
                    61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c2:6e:
                    45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:
                    a5:94:ac:8a:67
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5withRSAEncryption
        7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:a4:
        54:39:80:7b:b9:d9:49:b3:b2:2a:fe:8a:52:f4:c2:89:0e:5c:
        7b:92:f8:cb:77:3f:56:22:9d:96:8b:b9:05:c4:18:01:bc:40:
        ee:bc:0e:fe:fc:f8:9b:9d:70:e3
```

Zauważmy, że w tym przypadku klucz publiczny jest kluczem RSA i zawiera dwa parametry: wykładnik i modulo.

Otrzymany certyfikat powinien być jak najszerzej rozpowszechniony. Powinien być dostępny dla każdego, kto chce przysyłać do nas zaszyfrowane wiadomości. Nasza przeglądarka automatycznie wysyła nasz certyfikat kiedykolwiek podpisujemy swoje wiadomości w poczcie

elektronicznej. Natomiast dla swojego bezpieczeństwa należy utajnić dla osób postronnych wszelkie informacje o kluczu prywatnym, który odkodowuje przychodzące wiadomości.

W rzeczywistości certyfikat nie zawiera żadnych tajnych informacji. W każdym przypadku, w którym łączymy się z zabezpieczonym serwerem żądającym potwierdzenia tożsamości, przekazujemy swój certyfikat jako część procesu autentykacji.

Ważne jest, którą instytucję certyfikującą wybierzemy na wystawcę certyfikatu dla swojego serwera. Decydującym kryterium powinno być to, czy zamierzamy komunikować się z innymi użytkownikami sieci. Dla przykładu, jeśli certyfikat jest przeznaczony dla serwera sieci wewnętrznej i wszyscy użytkownicy sieci łączący się z nim będą wykorzystywali przeglądarki wskazane przez nas, najlepiej byłoby, gdybyśmy sami utworzyli „instytucję certyfikującą" wystawiającą certyfikaty, oraz skonfigurowali standardowe oprogramowanie tak, by akceptowało te certyfikaty. Jeśli natomiast mamy zamiar współpracować z klientami z całego świata, należy wybrać instytucję certyfikującą, której certyfikaty będą akceptowane przez zdecydowaną większość dostępnych na rynku przeglądarek.

Jeśli budujemy intranet i chcemy, aby serwer identyfikował każdego z naszych pracowników poprzez certyfikaty osobiste, wtedy najlepszym rozwiązaniem jest zakupienie oprogramowania w rodzaju Netscape Certificate Server i wydawanie tych certyfikatów samemu. Jeśli natomiast oferujemy usługi dostępowe w założeniu bez ograniczania ich dostępności i chcemy weryfikować użytkowników na podstawie certyfikatów osobistych, należy wybrać certyfikaty oferowane przez kilka sprawdzonych instytucji certyfikujących.

Certyfikaty osobiste i certyfikaty serwera używają dokładnie tych samych formatów. Różnica polega na tym, że zawierają odmienną informację na temat certyfikowanego podmiotu. Dla przykładu, parametr „Common Name" w certyfikacie serwera jest zwykle ustalony jako nazwa hosta, powiedzmy bilbo.thawte.com, gdy tymczasem w certyfikatach osobistych w tym miejscu występuje imię i nazwisko właściciela certyfikatu.

4. Dlaczego warto otrzymać certyfikat od Thawte?

Badania przeprowadzone przez firmę Netcraft wykazały, że certyfikaty wystawione przez Thawte znajdują się obecnie na 40% aktywnych serwerów obsługujących handel elektroniczny w Internecie. Ponad 90% firm znajdujących się w „Fortune 500" używa rozwiązań opartych o SSL w celu ochrony swoich ważnych danych.

Certyfikaty SSL Thawte są kompatybilne ze wszystkimi najnowszymi modelami przeglądarek internetowych, włączając w to oczywiście produkty Microsoft Internet Explorer oraz Netscape Communicator. Ponad 90% wszystkich wykorzystywanych dziś na świecie przeglądarek internetowych zaakceptuje certyfikaty wystawione przez Thawte jako wiarygodne potwierdzenie autentyczności serwera WWW. Certyfikaty Thawte są kompatybilne również ze wszystkimi obecnymi wersjami komercyjnych i darmowych serwerów WWW obsługujących SSL. Wśród obsługiwanych serwerów znajdują się: Oracle Application Server, Apache-SSL, Microsoft IIS, Netscape Enterprise i FastTrack, O'Reilly WebSite Pro, serwery C2 Net Stronghold, GoSite i Hockey, wszystkie obecne wersje bezpiecznych serwerów IBM, Lotus Domino Go!, OpenMarket Secure Serwer, serwery Apache w dystrybucjach RedHat i Raven sytemu operacyjnego Linux, serwery Roxen, WebSTAR/SSL, Tenon WebTen, WN oraz Zeus.

Certyfikaty SSL Thawte będą akceptowane przez zdecydowaną większość dostępnych na rynku przeglądarek. Lista przeglądarek, które akceptują certyfikaty SSL Thawte dla serwerów sieciowych przedstawia Tabela 1 i Tabela 2. Natomiast Tabela 3 wymienia przeglądarki, które certyfikatów Thawte nie akceptują.

Tabela 1. Lista przeglądarek akceptujących certyfikaty SSL Thawte

Przeglądarka	Platforma
Internet Explorer 5.x	Mac OS 8.x/9.x Mac OS X Windows 95/98 Windows NT 4.0
Navigator 4.x Communicator 4.x	Wszystkie obsługiwane systemy
Internet Explorer 4.x	Windows 95/98, Windows NT 4.0 Windows 3.1x, Windows NT 3.51
Internet Explorer 3.02	Windows 95/98, Windows NT 4.0 SP3 Windows 3.1x (IE 3.02a.2916), Windows NT 3.51
AOL 4.0 z Internet Explorer 4.x	Windows 95/98, Windows NT 4.0 Windows 3.1x, Windows NT 3.51
AOL 3.0 z Internet Explorer 3.02	Windows 95/98, Windows NT 4.0 SP3 Windows 3.1x (IE 3.02a.2916), Windows NT 3.51
WebTV Classic i Plus	TV
Opera 3.x i późniejsze	Windows 95/98 Windows 3.1x
FrontPage 2000	Wszystkie obsługiwane platformy
Internet Explorer 3.01	Windows 95/98 Windows NT 4.0 SP 3

Tabela 2. Lista przeglądarek, które po wprowadzeniu drobnych zmian w konfiguracji będą akceptowały certyfikaty SSL Thawte

Przeglądarka	Platforma
Internet Explorer 4.x	Mac
Navigator 3.x	Wszystkie obsługiwane systemy
Navigator 2.x	Wszystkie obsługiwane systemy
Internet Explorer 3.0	Windows 95/98

Tabela 3. Lista przeglądarek nie akceptujących certyfikatów SSL Thawte

Przeglądarka	Platforma
Navigator 1.x	Wszystkie obsługiwane systemy
Internet Explorer 3.0	Mac, Windows 3.1x
Internet Explorer 2.0	Wszystkie obsługiwane systemy
FrontPage 98	Wszystkie obsługiwane systemy

5. Procedura uzyskania certyfikatu Thawte

5.1. Zebranie niezbędnej dokumentacji

Przed wydaniem certyfikatu serwera, Thawte musi mieć całkowitą pewność, że wydaje go „właściwej" firmie. Pod pojęciem „właściwej" rozumiemy tutaj, że firma ta jest właścicielem domeny internetowej, która jest przedmiotem certyfikatu, że firma jest zarejestrowana w danym kraju, i że zarejestrowana nazwa jest taka sama jak ta, która znajdzie się na certyfikacie. Dlatego też Thawte wymaga nadesłania zestawu dokumentów identyfikujących firmę.

Dokumentacja ta oczywiście różni się w szczegółach w zależności od kraju, w którym jest zarejestrowana firma, oraz od charakteru działalności firmy. Najważniejsze jest, aby przesłana dokumentacja była potwierdzona przez administrację państwową lub lokalną, ponieważ na jej podstawie zostanie ustalona dokładna nazwa firmy, którą będzie zawierał certyfikat. W warunkach polskich wymaganymi dokumentami są:

- aktualny wyciąg z Sądu Rejestrowego
- zaświadczenie z Urzędu Skarbowego o nie zaleganiu z podatkami

5.2. Wygenerowanie klucza oraz wniosku o wydanie certyfikatu

5.2.1. Jeśli firma posiada serwer i zarządza nim.

Proszę postępować zgodnie z instrukcjami dostarczonymi wraz z bezpiecznym serwerem SSL oraz wygenerować klucz prywatny i wniosek o wydanie certyfikatu. (*Certificate Signing Request - CSR*). Aby otrzymać od Thawte *SupertCert* umożliwiający stosowanie szyfrowania 128 bitowego należy wygenerować 1024 bitowy klucz prywatny. Na stronie http://www.thawte.com/certs/server/keygen/contents.html dla ponad 30 najpopularniejszych bezpiecznych serwerów SSL (w tym *Oracle Application Server - OAS*) znajdują się instrukcje w jaki sposób można wygenerować klucz prywatny oraz wniosek o wydanie certyfikatu. Należy przy tym zwrócić uwagę, że możliwe jest uzyskanie certyfikatu Thawte dla OAS w wersji 4.0.8. Wersja 4.0.7.x nie akceptuje certyfikatów Thawte pomimo, że OAS w wersji 4.0.7.1 na platformę Linux nie wykazywał żadnych problemów w czasie testów.

5.2.2. Serwery utrzymywane przez pośredników, np. dostawców Internetu

Jeśli serwer firmy jest utrzymywany przez pośrednika należy zwrócić się do niego z prośbą o wygenerowanie klucza prywatnego oraz wniosku o wydanie certyfikatu. Proszę zwrócić uwagę na to, że wszystkie informacje o firmie zawarte we wniosku o wydanie certyfikatu muszą dotyczyć właściciela domeny a nie pośrednika utrzymującego tę domenę.

5.3. Przesłanie wniosku o wydanie certyfikatu przez Internet

Aby przesłać Internetem do Thawte przygotowany wniosek o wydanie certyfikatu należy umieścić go w specjalnej formatce. W celu dokończenia procesu ubiegania się o certyfikat należy również podać szczegóły dotyczące firmy oraz dane osób odpowiedzialnych za zgłoszenie. Jeśli firma lub pośrednik utrzymujący serwer firmy należy do programu partnerskiego, należy umieścić na formatce wpisać identyfikator przyznany w ramach udziału w programie partnerskim. Formatka do przesłania wniosku o wydanie certyfikatu znajduje się na stronie https://www.thawte.com/cgi/server/step1.exe

5.4. Przyznanie identyfikatora zamówienia

Po przesłaniu wniosku o wydanie certyfikatu do Thawte jako potwierdzenie otrzymania wniosku otrzymamy identyfikator zamówienia. Typowy identyfikator będzie miał postać w rodzaju:

USMISS25. Identyfikator należy użyć w celu sprawdzenia stanu realizacji zamówienia, wygenerowania umowy o wydanie certyfikatu (zwanego również listem autoryzującym) oraz odebrania ze stron WWW Thawte przyznanego certyfikatu.

5.5. Umowa o wydanie certyfikatu

Należy zapoznać się z wygenerowaną umową o wydanie certyfikatu. Jeśli jej treść nie budzi zastrzeżeń, umowę należy wydrukować na papierze firmowym i podpisaną przez osoby prawomocnie występujące w imieniu firmy przesłać na adres Thawte.

Przyznanie certyfikatu przez Thawte jest uwarunkowane podpisaniem umowy o wydanie certyfikatu. Przykładowa treść umowy znajduje się na stronach: http://www.thawte.com/certs/server/agreement.html .

5.6. Przesłanie dokumentacji firmy

Wszystkie dokumenty zebrane w punkcie 4.1. należy przesłać listem poleconym (firmą kurierską) lub faksem na adres Thawte.

5.7. Monitorowanie stanu zamówienia

Po prawidłowym wykonaniu etapów wymienionych powyżej zostały dopełnione wszystkie formalności wymagane przez Thawte. Rozpoczyna się etap generowania certyfikatu. Aktualny stan realizacji wniosku (zamówienia) można śledzić na stronie https://www.thawte.com/cgi/server/status.exe, oczywiście po wpisaniu przyznanego identyfikatora wniosku. W przypadku dodatkowych pytań w każdej chwili można skontaktować się z Thawte.

Po przygotowaniu certyfikatu Thawte przesyła wiadomość pocztą elektroniczna wraz z adresem URL, z którego można odebrać certyfikat. Odebrany certyfikat można zainstalować na bezpiecznym serwerze firmy. Jeśli serwer WWW firmy jest utrzymywany przez pośrednika, instalacja zostanie dokonana przez niego.

5.8.Instalacja certyfikatu.

I wreszcie finał – instalacja certyfikatu. Jeśli został on zainstalowany poprawnie, należy również odpowiednio skonfigurować SSL na swoim serwerze. Szczegóły konfiguracji powinna zawierać dokumentacja dostarczona wraz z oprogramowaniem. Należy pamiętać, że certyfikaty są ważne przez okres jednego roku od chwili wystawienia.

Aby zainstalować certyfikat należy użyć również klucza prywatnego użytego do wygenerowania wniosku o wydanie certyfikatu. Jeśli klucz został zgubiony lub nie można go użyć z innych powodów, nie można również używać otrzymanego certyfikatu. A to oznacza, że całą procedurę należy rozpocząć od nowa.

6. Inne certyfikaty Thawte

Thawte oferuje całą gamę certyfikatów, z których w tym artykule omówiono zaledwie jeden rodzaj: certyfikaty serwera SSL. Wydaje się, że w czasach gwałtownego wzrostu zainteresowania wykorzystaniem Internetu właśnie ten rodzaj certyfikatu powinien być najbardziej interesujący dla firmy z perspektywy jej działalności komercyjnej. Oprócz tego można wystąpić do Thawte o wydanie następujących certyfikatów:

- osobistego, przeznaczonego dla osób fizycznych, umożliwiającego szyfrowanie wiadomości poczty elektronicznej oraz autoryzację przez serwery sieciowe.
- programistycznego, do zabezpieczania oprogramowania przesyłanego przez Internet; z jednej strony certyfikat taki potwierdza tożsamość twórcy oprogramowania, z drugiej zabezpiecza

przed zmianami w kodzie źródłowym, które mogą powstać przy przesyłaniu oprogramowania w sieci lub zostać wprowadzone przez inne osoby.

Thawte oferuje również usługę delegowania autoryzacji na certyfikaty wydawane przez inne instytucje certyfikujące powodując, że certyfikaty wystawiane przez te instytucje stają się w Internecie równie wiarygodne, jak certyfikaty Thawte.

7. Zakończenie

Coraz więcej przedsiębiorstw decyduje się na poważne inwestycje mające na celu szersze wykorzystanie w swojej działalności Internetu. Jak przewidują analitycy Deloitte Consulting (http://www.dc.com), do końca 2001 r. aż 91% przedsiębiorstw w USA będzie dokonywać transakcji właśnie poprzez Internet. Również w Polsce Internet zyskuje coraz większą popularność - lawinowo wzrasta liczba osób wykorzystujących Internet do pracy, nauki i rozrywki. Różnorakie badania pokazują, że liczba polskich Internautów waha się od 2 do 4,5 mln. osób.

Internet zatem już niedługo może stać się fundamentem działalności gospodarczej. Ale Internet to również zagrożenia związane z nieograniczonym dostępem do sieci. Media co rusz publikują informacje o kolejnych atakach sieciowych włamywaczy – hackerów – do systemów informatycznych. Tymczasem, według zachodnich specjalistów zajmujących się bezpieczeństwem systemów informatycznych, ponad 68% zagrożeń pochodzi ze strony legalnych użytkowników sieci.

Coraz istotniejsze stają się zatem zagadnienia dotyczące ochrony danych. Obawy związane z tym problemem zgłasza coraz więcej firm w Polsce, które zdają sobie sprawę z rozmiaru zagrożenia i konieczności podjęcia konkretnych działań w celu uniknięcia katastrofy. W tej sytuacji szczególnego znaczenia nabiera kwestia ochrony danych. Jednym z elementów kompleksowego systemu ochrony danych korporacyjnych jest instalacja certyfikatów cyfrowych, zabezpieczających cały proces komunikacji w Internecie.