STUDIA INFORMATICA 2000
Volume 21 Number 1 (39)

Tomasz FRANEK
Sotel, sp. z o. o.

PROGRAMOWA OCHRONA POCZTY ELEKTRONICZNEJ Z WYKORZYSTANIEM KONCEPCJI URZĘDÓW CERTYFIKATÓW NA PRZYKŁADZIE ROZWIĄZAŃ FIRMY SOTEL

Streszczenie. Artykuł porusza zagadnienia dotyczące obecnie stosowanych technik zabezpieczania wiadomości poczty elektronicznej. Zabezpieczenia wiadomości opierają się na szyfrowaniu z zastosowaniem kryptografii wykorzystującej klucze prywatne i publiczne autoryzowane w urzędach certyfikacji. Artykuł przedstawia również metody generacji i zarządzania certyfikatami umieszczonymi na serwerze certyfikatów.

PROGRAMMING E-MAIL PROTECTION USING CONCEPTION OF CERTIFICATE AUTHORITY IN SOTEL SOLUTION EXAMPLE

Summary. The paper presents basic information about e-mail security technology using public key cryptography. There are also presents conception of generating and managing users certificates in Certification Authority.

1. Wprowadzenie

W obecnej kryptografii wykorzystującej do szyfrowania klucze bezpieczeństwo informacji opiera się na bezpieczeństwie klucza. Zarządzanie kluczami jest równie ważnym zadaniem jak sam proces szyfrowania. Wybór bezpiecznego algorytmu szyfrującego wykorzystywanego do ochrony przesyłanych wiadomości i jego późniejsza implementacja jest w miarę prosta. Problemem staje się jednak identyfikacja osoby szyfrującej wiadomość. Kiedy otrzymujemy wiadomość zaszyfrowaną przy pomocy kluczy przesłaną pocztą elektroniczną, nie mamy pewności, czy pochodzi ona od osoby, która tę wiadomość przesłała. Coraz częściej można spotkać się z podszywaniem się jednych osób pod inne. Konieczne staje się więc tworzenie

urzędów, których zadaniem jest pilnowanie bezpieczeństwa kluczy publicznych podpisując je własnym certyfikatem. Podpisy cyfrowe zapewniają nam autentyczność otrzymywanych wiadomości.

1.1. Podstawowe pojęcia

Certyfikat to wiadomość specjalnego rodzaju [1] zawierająca czyjeś nazwisko, adres poczty elektronicznej i klucz publiczny osoby. Dodatkowo certyfikat zawiera nazwisko osoby godnej zaufania, która wydała i podpisała certyfikat.

Urząd certyfikacji jest organizacją świadczącą usługi wydawania certyfikatów. Jej głównym celem jest wydawanie, przechowywanie i zarządzanie certyfikatami. Zaufanie do urzędu sprawia, że ufamy certyfikatom podpisywanym przez urząd.

Klucze są to ciągi bitów, które wraz z algorytmem służą do zabezpieczania przesyłanych wiadomości. W kryptografii asymetrycznej wykorzystuje się klucze publiczne i prywatne. Z danym użytkownikiem związana jest więc para kluczy. Jawny klucz może być użyty przez wielu użytkowników do zaszyfrowania informacji skierowanej do właściciela klucza. Tajny klucz należy wyłącznie do właściciela i używa on go do odszyfrowania przychodzących wiadomości. Jest on również wykorzystywany do podpisywania poczty wychodzącej od właściciela klucza.

2. Zalecenia dotyczące projektowania urzędów certyfikatów

Przy tworzeniu urzędów certyfikatów konieczne jest spełnienie podstawowych założeń. Urząd certyfikatów powinien posiadać parę kluczy publiczny i prywatny, przy pomocy których podpisuje certyfikaty. Może on posiadać więcej niż jedną taką parę, ale do certyfikacji danego klucza wykorzystuje się tylko jedną. Informacja o kluczach używanych do certyfikacji powinna jednoznacznie identyfikować parę aktualnie używanych kluczy. Podpis cyfrowy powinien zawsze towarzyszyć wystawianiu certyfikatów wiarygodności, przesyłaniu kluczy, publikowaniu listy certyfikatów unieważnionych, oraz wszystkich innych informacji na temat pracy urzędu.

Urząd certyfikacji powinien wystawiać cyklicznie listy certyfikatów unieważnionych. Głównymi powodami, dla których został unieważniony jakiś klucz, jest albo podejrzenie przez osobę niepowołaną (kompromitacja klucza), bądź też przeniesienie, czy zwolnienie użytkownika posiadającego obecnie klucz z ciążących na nim obowiązków. Oprócz nazwy kluczy, których certyfikaty zostały unieważnione w takiej liście, powinny znaleźć się również informacje dotyczące daty, kiedy lista ta została opublikowana, oraz datę następnego

przewidywanego wydania listy. Data wydania wyznacza moment, od którego wiadomości podpisywane kluczami umieszczonymi na liście mogą być traktowane jako niewiarygodne. Przewidywana data wydania następnej listy certyfikatów unieważnionych nie oznacza, że taka lista nie może zostać wydana wcześniej. Na podstawie zgłoszeń do urzędu informacji o istniejących przypuszczeniach kompromitacji klucza może wcześniej nastąpić wydanie nowej listy. Data ta mówi również, czy dana lista jest nadal obowiązująca, a jeżeli okres ten minął, to serwer wystawił już nową listę certyfikatów unieważnionych. W skład listy mogą wchodzić również listy certyfikatów unieważnionych tworzonych przez inne urzędy certyfikacji .

Urzędy certyfikatów tworzone są w oparciu o różne koncepcje. Najbardziej rozpowszechnione jest tworzenie urzędów działających w standardzie rozproszonego potwierdzania komunikatów [1]. Taki model działania wykorzystywany jest w pakiecie PGP (*Pretty Good Privacy*). Certyfikaty mogą być poświadczane przez więcej niż jeden urząd certyfikatów, co jest niewątpliwie zaletą, gdyż można mieć większe zaufanie dla klucza certyfikowanego przez wiele urzędów. Ten model urzędu certyfikacji ma bardzo dobre zastosowanie w grupach osób, które mogły się nigdy nie spotkać, lub nie tworzą organizacji o ściśle określonej hierarchii. Z powodu poświadczania certyfikatu przez więcej niż jeden urząd certyfikacji konieczna staje się wymiana listy certyfikatów odwołanych pomiędzy urzędami.

Gdy struktura urzędu powinna być hierarchiczna, to można do niej zastosować inny model działający według standardu PEM (*Privacy Enhanced Mail*). Ufamy certyfikatowi, który jest wyżej w hierarchii, natomiast nam ufają ludzie znajdujący się niżej w hierarchii. Na samym szczycie hierarchii znajduje się zaufany urząd upoważniający wszystkich do wystawiania certyfikatów. Droga sprawdzania poprawności polega na sprawdzaniu ciągów podpisów zwierzchników, doprowadzające do jednego zwierzchnika wspólnego dla certyfikatu sprawdzanego i dla naszego certyfikatu. Struktura urzędu certyfikatu działającego hierarchicznie nadaje się do zastosowania w instytucjach, w których istnieje hierarchiczna struktura organizacji, czyli urzędy, wojsko, firmy, banki itd.

3. Odniesienie do serwera certyfikatów Sotel

Przy projektowaniu serwera certyfikatów położono nacisk na zachowanie zgodności z podstawowymi zaleceniami dotyczącymi tworzenia urzędów certyfikatów. Serwer ten został oparty na zasadzie rozproszonego systemu potwierdzania certyfikatów PGP, gdzie klucz może dostać poświadczenie certyfikatu od różnych urzędów certyfikatów. Serwer posiada własną parę kluczy wykorzystywaną do poświadczania autentyczności certyfikatów. Ich poprawność

jest sprawdzana w czasie komunikacji z nim przez program pobierający certyfikaty, a w przypadku wystąpienia nieścisłości informuje o nich użytkownika. Na serwerze urzędu certyfikatów została zaimplementowana również funkcja wystawiająca listę certyfikatów unieważnionych. Dla każdego unieważnionego certyfikatu można dodać informację, z jakiego powodu nastąpiło unieważnienie.

Program serwera certyfikatów posiada dwie niezależne części, z których jedna przyjmuje żądania przychodzące do serwera, natomiast druga służy do zarządzania pracą i administracją. Komunikacja z serwerem odbywa się przez sieć z wykorzystaniem protokołu TCP/IP według specjalnych schematów wymiany informacji. Serwer certyfikatów bardzo ściśle współpracuje z programem SecMail firmy Sotel szyfrującym pocztę elektroniczną z wykorzystaniem kluczy publicznych. W program został wbudowany moduł komunikacyjny wymieniający certyfikaty pomiędzy serwerem a lokalną bazą danych.

Rozdzielenie serwera na dwie części ma za zadanie umożliwić pracę serwera niezależnie od pracy konsoli zarządzającej. Serwer może tworzyć plik z wykazem wszystkich operacji, jakie były na nim wykonywane. Zawierają one wykazy kluczy, które zostały z niego pobrane, informację o nadawaniu i usuwaniu certyfikatów, zawierają adresy IP komputerów, z których dokonywano logowania się na serwer. Mogą być dzielone na wykazy dzienne, tygodniowe lub miesięczne. Dodatkową opcją programu jest zabezpieczenie przez blokowanie numerów IP komputerów, które nie mają dostępu do serwera.

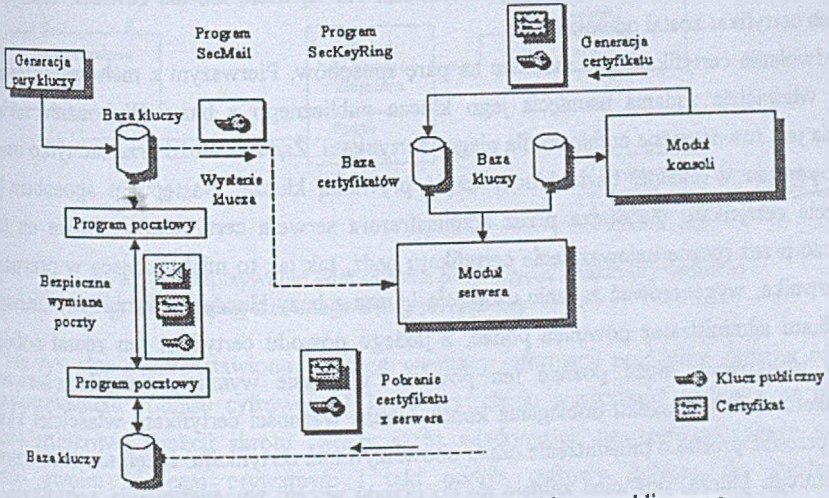
W certyfikacie występują więc następujące pola:

- numer seryjny certyfikatu – jest on unikalny w ramach danego urzędu certyfikacji i przypisany przez niego każdemu z wydawanych certyfikatów,
- data ważności certyfikatu – okres ważności certyfikatu, określa przedział czasu, w trakcie którego urząd gwarantuje, iż będzie on zarządzał informacją określającą status certyfikatu. Jest to pole składające się z dwóch dat, z czego pierwsza określa początek trwania okresu, a druga jego koniec. Przedział czasu jest jednocześnie okresem ważności klucza publicznego,
- identyfikator wystawcy certyfikatu – jest to nazwa urzędu certyfikacji wydającego certyfikat. Pole to pozwala zidentyfikować urząd i musi zawierać nazwę urzędu,
- nazwisko osoby, do której należy ten klucz,
- nazwa instytucji (firmy), w której pracuje dana osoba,
- adres poczty elektronicznej – pole to identyfikuje adres elektroniczny odbiorcy wiadomości i określa, na jaki adres mają być przesyłane szyfrowane dane,

Zamieszczenie tych informacji powoduje, że certyfikat generowany przez serwer jest zgodny ze standardem X.509 wersja 3 [2].

3.1. Droga certyfikacji klucza

Urząd certyfikacji ma określoną drogę postępowania w celu nadania kluczowi certyfikatu (rys. 1). Na samym początku użytkownik generuje swój własny klucz. Operacje wykonuje się w programie pocztowym SecMail, wykorzystującym klucze do szyfrowania lub podpisywania poczty elektronicznej. Po generacji klucz prywatny zostaje umieszczony w lokalnej bazie danych kluczy prywatnych. Część publiczną klucza można eksportować do pliku bądź bezpośrednio przez moduł komunikujący się z serwerem kluczy wysłać klucz do serwera certyfikatów.



Rys. 1. Schemat uzyskiwania certyfikatu dla klucza publicznego
Fig. 1. Public key certification schema

Żądanie wydania certyfikatu powinno zawierać następujące pola [4]:

- nazwa wyróżniona klucza publicznego,
- klucz publiczny,
- opcjonalnie atrybuty związane z kluczem – nazwisko osoby, do której należy klucz, adres jej poczty elektronicznej, nazwa firmy, z której pochodzi,
- całość pola powinna zostać podpisana kluczem prywatnym – zapobiega to możliwości podszycia się ze swoim kluczem publicznym pod inną osobę,
- wersja – określa wersję żądania przesłaną do urzędu, w przypadku gdy urząd certyfikacji obsługuje kilka wersji żądań certyfikatów.

Osoba tworząca klucz zazwyczaj wysyła zgłoszenie do certyfikacji klucza po wygenerowaniu klucza, ale może to również zrobić po zmianie nazwy wyróżnionej dla klucza, adresu poczty elektronicznej itd.

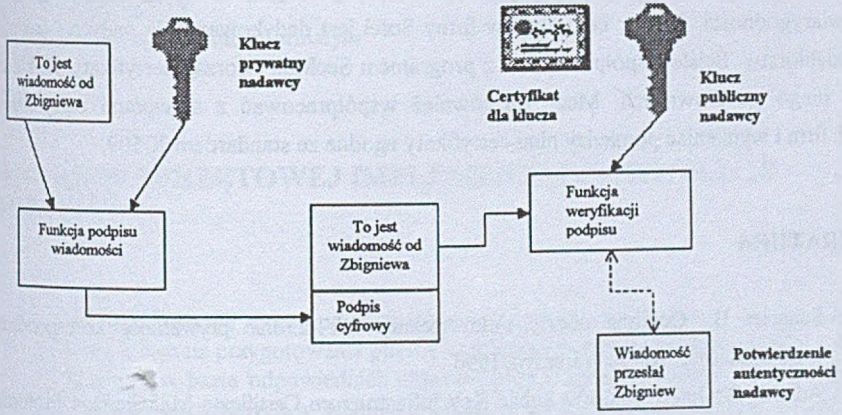
Wysłaniu klucza na serwer odpowiada jednocześnie wygenerowanie dla niego na serwerze żądania certyfikacji i umieszczenie zgłoszenia w kolejce zgłoszeń certyfikacji. Administrator serwera, posiadający prawa tworzenia certyfikatu dla klucza, może dla żądań stworzyć certyfikat bądź go odrzucić. W przypadku odrzucenia przez administratora żądania możliwe jest przesłanie informacji osobie wystawiającej to żądanie, z jakiego powodu nie zostało ono zrealizowane. Klucz przesłany do serwera certyfikatów, a którego żądanie certyfikacji znajduje się w kolejce żądań, nie jest umieszczany na liście kluczy serwera. Mogą się na niej znajdować tylko klucze certyfikowane. Ogranicza się w ten sposób dystrybucję kluczy publicznych przed wydaniem dla nich certyfikatu. Na tej liście nie ma również kluczy, dla których certyfikat został odwołany.

Odwołanie certyfikatu jest możliwe na parę sposobów. Pierwszym z nich jest przesłanie przez właściciela żądania usunięcia jego klucza publicznego z bazy. Wykonanie takiego żądania jest równoważne cofnięciu dla niego certyfikatu. Żądanie może przesłać tylko osoba, która posiada w lokalnej bazie kluczy część prywatną klucza. Następnym sposobem jest cofnięcie certyfikatu dla klucza przez administratora serwera certyfikatów. Może on tego dokonać przez ręczne unieważnienie certyfikatu bądź, tak jak to miało miejsce w przypadku użytkownika, wygenerować żądanie usunięcia klucza z bazy kluczy serwera. Przy usuwaniu certyfikatu administrator powinien podać, z jakiego powodu certyfikat ten został cofnięty. Każdy użytkownik może poznać ten powód w czasie wymiany danych z serwerem certyfikatów. W przypadku dobiegania końca okresu ważności certyfikatu właściciel klucza może przesłać prośbę o przedłużenie czasu obowiązywania certyfikatu. Jeżeli nie chce używać dalej starego klucza, powinien zgłosić się do urzędu w celu wygenerowania certyfikatu dla swojego nowego klucza.

Użytkownik programu SecMail podczas komunikacji z serwerem certyfikatów może z niego pobrać certyfikaty, oraz sprawdzić, czy wszystkie klucze znajdujące się w lokalnej bazie kluczy posiadają ważny certyfikat. Możliwa jest również synchronizacja całej bazy lokalnej i wtedy serwer przesyła wszystkie klucze i informacje o certyfikatach do bazy programu SecMail.

Administrator serwera może ręcznie wprowadzić klucz do bazy w module zarządzającym pracą serwera. Sposób zarządzania żądaniami certyfikacji zależy głównie od administratora urzędu certyfikatów. W przypadku serwera działającego niezależnie od określonych struktur, oraz na serwerach certyfikatów o niższym poziomie identyfikacji, wystawianie certyfikatów może odbywać się bez sprawdzenia wiarygodności osoby. Dla zamkniętej instytucji lub przy wysokim poziomie identyfikacji wystawieniu certyfikatu może towarzyszyć dodatkowa weryfikacja danych zawartych w polach klucza (imienia i nazwiska właściciela, jego adresu pocztowego, nazwy instytucji, z której pochodzi i adresu poczty elektronicznej).

4. Weryfikacja podpisu nadawcy wiadomości z wykorzystaniem certyfikatu



Rys. 2. Podpisywanie wiadomości przy użyciu klucza prywatnego
Fig. 2. Signing a message using private key

Na rysunku 2 przedstawiono przebieg wymiany informacji pomiędzy dwiema osobami z zastosowaniem podpisu cyfrowego [3]. Po stworzeniu wiadomości nadawca za pomocą jednokierunkowej funkcji skrótu tworzy skrót wiadomości, następnie podpisuje wartość skrótu swoim kluczem prywatnym i taki podpis cyfrowy dołącza do wiadomości. Po przesłaniu wiadomości odbiorca oddziela od treści wiadomości jej podpis i za pomocą jednokierunkowej funkcji skrótu oblicza wartość skrótu wiadomości. Odbiorca odbiera klucz jawny z lokalnej bazy danych albo z serwera certyfikatów. Jeżeli klucz nadawcy nie posiada certyfikatu w bazie serwera certyfikatów, oraz w lokalnej bazie danych, to odbiorca powinien odrzucić wiadomość Przy pomocy klucza jawnego następuje odszyfrowanie podpisu dołączonego do wiadomości. Na samym końcu odbiorca porównuje odszyfrowany podpis cyfrowy z obliczoną przez niego wartością skrótu wiadomości. Jeżeli są one takie same, to wiadomość jest akceptowana, jeżeli jednak różnią się pomiędzy sobą, to odbiorca odrzuca wiadomość.

5. Podsumowanie

Profesjonalne zarządzanie kluczami szyfrowania jest równie ważne, jak posiadane algorytmy szyfrujące. W czasach, gdy coraz częściej drogą elektroniczną przesyła się

informacje o dużym znaczeniu, tylko certyfikaty mogą zapewnić pełną weryfikację autentyczności nadawcy. Przy tworzeniu urzędów certyfikatów koniecznie jest nie tylko zadbanie o dostarczenie do urzędu informacji jednoznacznie identyfikującej właściciela klucza, ale również opracowanie polityki bezpieczeństwa pracy urzędu, co wpływa na zwiększenie jego wiarygodności. Serwer certyfikatów firmy Sotel jest dedykowany dla małych i średnich przedsiębiorstw. Ściśle współpracuje on z programem SecMail tworząc certyfikaty dla kluczy przez niego generowanych. Może on również współpracować z serwerami certyfikatów innych firm i wymieniać pomiędzy nimi certyfikaty zgodne ze standardem X.509.

LITERATURA

1. Schneier B.: Ochrona poczty elektronicznej. Jak chronić prywatność korespondencji w sieci Internet. WNT, Warszawa 1996.
2. Adams. C.: Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, Entrust Technologies, marzec 1999.
3. Viasec – Technical White Paper – Consus – Secure E-mail Gateway WP270999, Viasec, 1999.
4. PKCS #7 RSA Laboratories. PKCS #7: Cryptographic Message Syntax Standard. Wersja 1.5, listopad 1993.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 28 kwietnia 2000 r.

Abstract

This article describes problem of sending e-mails across global network. Main part of article presents solution for protecting the confidentiality, integrity and authenticity of any private message. There are described conception of asymmetric cryptography using public and private keys, and Certificate Authority, which generates and manages certificates for users keys. There are also presented standard X.509 that defines Digital Certificates. Next part show certification path and the reason for which the certificate is revoked. Last part presents an example how to send a signed message using a public key.