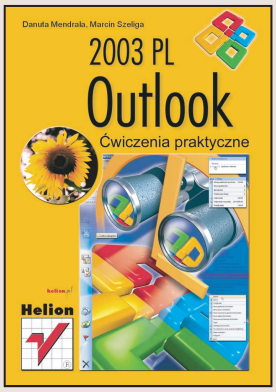
Outlook 2003 PL. Ćwiczenia praktyczne



Autorzy: Danuta Mendrala, Marcin Szeliga
ISBN: 83-7361-473-7
Format: B5, stron: 116

Outlook 2003 (składnik pakietu Office) to rozbudowany klient poczty elektronicznej z dodatkowymi funkcjami, takimi jak kalendarz, dziennik i notatki. Outlook pozwala na efektywne zarządzanie pocztą elektroniczną, jej ochronę przed wirusami i osobami niepowołanymi. Doskonale zastępuje tradycyjny kalendarz, listę spraw do załatwienia i karteczki z notatkami, którymi zwykle zarzucamy całe biurko. Dokładne poznanie wszystkich możliwości tego programu to poważne wyzwanie, ale nawet najdłuższa podróż rozpoczyna się od pierwszego kroku.

Takim pierwszym krokiem w poznawaniu Outlooka 2003 jest lektura tej książki. W krótkich, ilustrowanych ćwiczeniach znajdziesz podstawowe informacje dotyczące korzystania z poczty elektronicznej za pomocą Outlooka, korzystania z funkcji kalendarza i dziennika oraz tworzenia i odczytywania notatek.

- Instalacja i konfiguracja Outlooka
- Foldery, widoki i typy plików
- Tworzenie kont poczty elektronicznej
- Odbieranie i wysyłanie wiadomości
- Zabezpieczanie poczty elektronicznej
- Korzystanie z funkcji kalendarza i dziennika
- Notatki

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 4.

Zabezpieczenie poczty elektronicznej

Samo podłączenie komputera do sieci związane jest ze sporym zagrożeniem bezpieczeństwa, jednak na największą liczbę ataków (zwłaszcza tych automatycznie przeprowadzanych przez wirusy) narażasz się, uruchamiając program klienta pocztowego. Szczególnie duże ryzyko związane jest z uruchomieniem niezwykle popularnego (a więc choćby statystycznie częściej atakowanego) programu Microsoft Outlook.

Wykonując zawarte w tym rozdziale ćwiczenia, poznasz sposoby zapewnienia **poufności przesyłanych wiadomości** i **bezpieczeństwa wykorzystywanego w tym celu komputera**.

Podstawowe zabezpieczenia

Nie istnieje całkowicie bezpieczny, podłączony do sieci komputer. Jednak poprzez poprawną konfigurację, uruchomienie dodatkowych programów chroniących komputer i przestrzeganie podstawowych zasad zabezpieczeń możesz znacząco zmniejszyć ryzyko udanego ataku. **Wykonanie opisanych w tym podrozdziale ćwiczeń powinno uchronić Cię przed 3/4 przeprowadzanych ataków**.

Ochrona komputera

Zanim zabezpieczysz program Outlook, powinieneś zabezpieczyć sam komputer, a dokładniej — zainstalowany na nim system operacyjny.

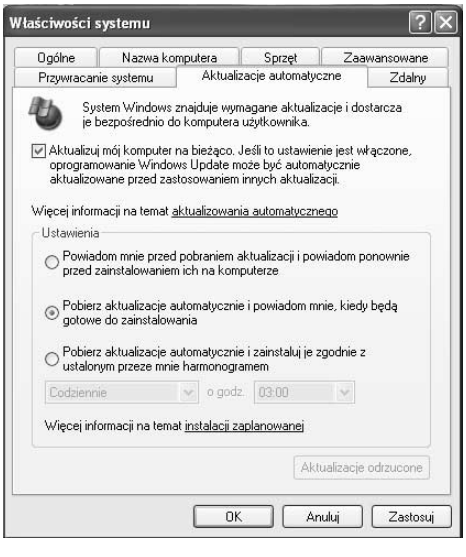
Przedstawienie technik zabezpieczenia systemów Windows wykracza poza zakres ćwiczeń. Zainteresowani Czytelnicy powinni przeczytać wydaną przez Helion książkę *Bezpieczeństwo w sieciach Windows*.

Ćwiczenie 4.1.

Aby zapewnić podstawowe bezpieczeństwo komputera:

1. **Nie używaj przestarzałych** (wcześniejszych od Windows 2000) **wersji systemu Windows**. Jeżeli wciąż używasz którejś z wcześniejszych wersji, jak najszybciej uaktualnij ją.
2. Systematycznie **aktualizuj system** poprzez instalowanie aktualizacji zabezpieczeń. W systemach Windows 2000 SP3 lub nowszych wykorzystaj do tego celu mechanizm Windows Update:
   a) Zaloguj się do systemu jako jego administrator.
   b) Kliknij prawym przyciskiem myszy ikonę *Mój komputer* i wybierz opcje *Właściwości*.
   c) Przejdź do zakładki *Aktualizacje automatyczne* i zaznacz pole wyboru *Aktualizuj mój komputer na bieżąco*.
   d) Zaznacz pole wyboru *Pobierz aktualizacje automatycznie i powiadom mnie, kiedy będą gotowe do zainstalowania* (rysunek 4.1).

Rysunek 4.1. *Jedynym sposobem na uchronienie się przed atakiem wykorzystującym odkryte słabe punkty systemu jest wcześniejsze zainstalowanie aktualizacji zabezpieczeń*



   e) Kliknij przycisk *OK* i zamknij wszystkie otwarte okna dialogowe. Od teraz po opublikowaniu nowych aktualizacji Twój komputer pobierze je i zgłosi gotowość ich zainstalowania.
3. **Zainstaluj program antywirusowy**. Samo jego zainstalowanie nie uchroni Cię jednak przed atakami:

Istnieje wiele firm produkujących oprogramowanie antywirusowe — z łatwością znajdziesz je w internecie. Niektóre z nich udostępniają klientom indywidualnym swoje produkty za darmo, a większość umożliwia ich bezpłatne testowanie przez okres np. jednego miesiąca.

a) Upewnij się, że monitor antywirusowy jest automatycznie uruchamiany podczas startu systemu.

b) **Codziennie aktualizuj sygnatury wirusów**.

c) Systematycznie (np. raz w tygodniu) skanuj wszystkie zapisane na lokalnych dyskach twardych pliki.

4. **Chroń komputer poprzez zaporę połączenia internetowego**. W systemach Windows XP i nowszych wbudowana jest prosta zapora, która powinna być włączona dla połączenia wykorzystywanego do komunikacji z internetem:

Istnieje wiele firm produkujących programowe zapory połączenia internetowego — z łatwością znajdziesz je w internecie. Niektóre z nich udostępniają klientom indywidualnym swoje produkty za darmo, a większość umożliwia ich bezpłatne testowanie przez okres np. jednego miesiąca.

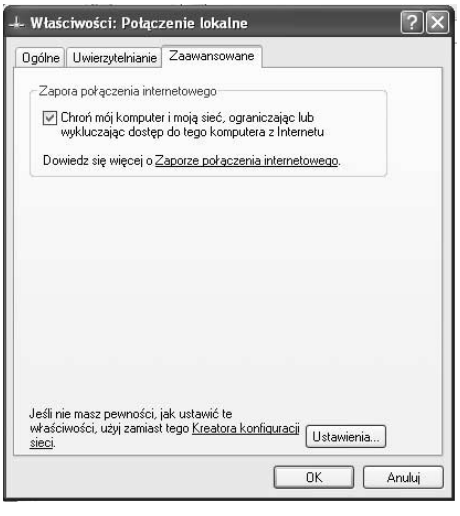
a) Zaloguj się do systemu jako jego administrator.

b) Kliknij prawym przyciskiem myszy ikonę *Moje miejsca sieciowe* i wybierz opcję *Właściwości*. Wyświetlone zostanie okno dialogowe *Połączenia sieciowe*.

c) Kliknij prawym przyciskiem myszy połączenie z internetem i z menu kontekstowego wybierz opcję *Właściwości*.

d) Przejdź do zakładki *Zaawansowane* i zaznacz pole wyboru *Chroń mój komputer*... (rysunek 4.2).

Rysunek 4.2. *Włączenie zapory dla połączenia z siecią lokalną będzie wymagało jej skonfigurowania — w innym przypadku przeglądanie zasobów sieci i korzystanie z nich będzie znacznie utrudnione*



e) Kliknij przycisk *OK* i zamknij wszystkie otwarte okna dialogowe.

Konfiguracja uwierzytelniania przez serwer pocztowy

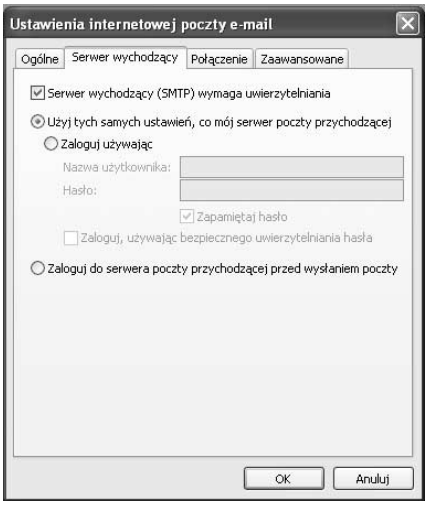
Łącząc się w celu odebrania wiadomości z serwerem pocztowym, należy podać poprawną nazwę użytkownika i hasło — sprawdzając te dane, serwer jest w stanie zweryfikować Twoją tożsamości i umożliwić odebranie wiadomości. Coraz częściej również **przed wysłaniem wiadomości należy podać hasło** — zapobiega to przesyłaniu wiadomości w Twoim imieniu przez nieuprawnione osoby. Niestety domyślnie **oba hasła** (w przypadku darmowych kont jest to z reguły takie same hasło) **przesyłane są przez sieć „otwartym tekstem"**, czyli każdy może w prosty sposób je poznać — nie wymaga to od niego żadnej fachowej wiedzy czy to z dziedziny sieci komputerowych, czy kryptografii. Rozwiązaniem jest szyfrowanie przesyłanych haseł.

Ćwiczenie 4.2.

Aby skonfigurować uwierzytelnienie przez serwer poczty wychodzącej:

Niektóre źle skonfigurowane serwery pocztowe nie umożliwiają uwierzytelniania podczas wysyłania wiadomości. **W takim przypadku po wykonaniu tego ćwiczenia nie będziesz mógł wysłać wiadomości**.

1. Wybierz *Narzędzia/Konta e-mail…*.
2. Upewnij się, czy zaznaczone jest pole *Wyświetl* lub zmień istniejące konta e-mail i kliknij przycisk *Dalej*.
3. Zaznacz konfigurowane konto i kliknij przycisk *Zmień…*.
4. Kliknij przycisk *Więcej ustawień…*.
5. Przejdź do zakładki *Serwer wychodzący* i zaznacz pole wyboru *Serwer wychodzący (SMTP) wymaga uwierzytelniania* (rysunek 4.3).



Rysunek 4.3. *Prawie wszystkie serwery pocztowe wymagają potwierdzenia tożsamości nie tylko przy odbieraniu wiadomości, lecz również przy ich wysyłaniu przez użytkownika*

6. Jeżeli administrator serwera nie poinformował Cię o haśle do serwera SMTP, kliknij przycisk *OK*; w przeciwnym razie wybierz opcję *Zaloguj używając*, wpisz poprawną nazwę użytkownika i hasło, a następnie kliknij przycisk *OK*.
7. Zamknij okno *Konta e-mail* i przetestuj nowe ustawienia konta, wysyłając **wiadomość do samego siebie**.

Szyfrowanie przesyłanych danych

Jeżeli serwer pocztowy, na którym masz założone konto, umożliwia nawiązywanie bezpiecznych połączeń, będziesz mógł zaszyfrować przesyłane do niego (w tym nazwę użytkownika i hasło) dane.

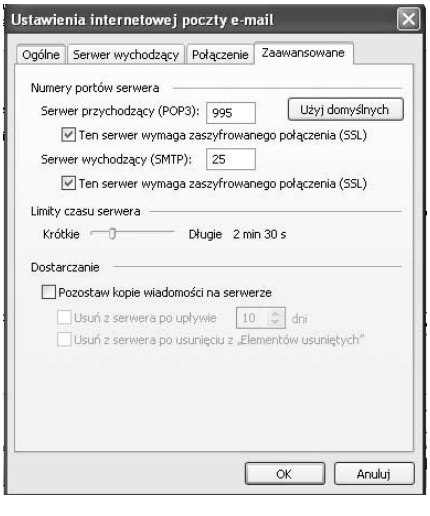
Ćwiczenie 4.3.

Aby zaszyfrować dane przesyłane pomiędzy serwerem pocztowym a Twoim komputerem:

Niektóre źle skonfigurowane serwery pocztowe nie umożliwiają nawiązywania bezpiecznych połączeń. W takim przypadku po wykonaniu tego ćwiczenia nie będziesz mógł odbierać i wysłać wiadomości. W każdym przypadku szyfrowanie przesyłanych danych spowoduje wydłużenie czasu potrzebnego na ich wysłanie i odebranie.

1. Kliknij przycisk *Więcej ustawień…*.
2. Przejdź do zakładki *Zaawansowane*.
3. Zaznacz oba pola wyboru *Ten serwer wymaga zaszyfrowanego połączenia (SSL)* (rysunek 4.4).

Rysunek 4.4. *Skuteczną obroną przed przechwyceniem przesyłanych danych jest ich zaszyfrowanie*



4. Kliknij przycisk *OK*.
5. Zamknij okno *Konta e-mail* i przetestuj nowe ustawienia konta, wysyłając **wiadomość do samego siebie**.

Blokowanie załączników

Przesyłane wraz z wiadomościami załączniki mogą być (jak to udowodniły epidemie wirusów Melisssa czy I Love You) wyjątkowo niebezpieczne. Zagrożeniem są pliki, które mogą zostać (automatycznie lub ręcznie) uruchomione — jeżeli zawierają one szkodliwy kod, zostanie on uruchomiony tak, jak każdy inny uruchamiany przez Ciebie program. Walcząc z tym zagrożeniem, firma Microsoft na **trwale zablokowała możliwość wysyłania i odbierania niektórych załączników** (tabela 4.1).

Tabela 4.1. *Lista rozszerzeń automatycznie blokowanych załączników*

Rozszerzenie pliku	Typ pliku
.ade	Rozszerzenie projektu programu Microsoft Access
.adp	Projekt programu Microsoft Access
.app	Aplikacja utworzona przez program FoxPro
.bas	Moduł klas języka Microsoft Visual Basic
.bat	Plik wsadowy
.chm	Skompilowany plik Pomocy w formacie HTML
.cmd	Skrypt polecenia systemu Microsoft Windows NT
.com	Program systemu Microsoft MS-DOS
.cpl	Rozszerzenie Panelu sterowania
.crt	Certyfikat zabezpieczeń
.csh	Skrypt powłoki systemu Unix
.exe	Program
.fxp	Plik programu FoxPro
.hlp	Plik Pomocy
.hta	Program w języku HTML
.inf	Informacje Instalatora
.ins	Usługa nazewnictwa internetowego
.isp	Ustawienia Komunikacji internetowej
.js	Plik języka JScript
.jse	Zakodowany plik języka Jscript
.ksh	Skrypt powłoki systemu Unix
.lnk	Skrót
.mda	Program-dodatek Microsoft Access
.mdb	Baza danych programu Microsoft Access
.mde	Baza danych programu Microsoft Access MDE

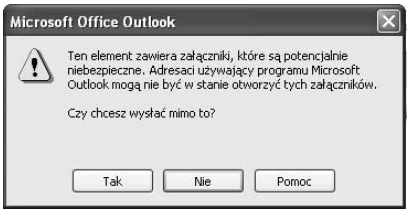
Tabela 4.1. *Lista rozszerzeń automatycznie blokowanych załączników — ciąg dalszy*

Rozszerzenie pliku	Typ pliku
.mdt	Dane programu-dodatku Microsoft Access
.mdw	Plik informacyjny grupy roboczej programu Microsoft Access
.mdz	Program Kreatora Microsoft Access
.msc	Dokument wspólnej konsoli firmy Microsoft
.msi	Pakiet Instalatora systemu Microsoft Windows
.msp	Poprawka Instalatora systemu Windows
.mst	Plik źródłowy Visual Test
.ops	Plik programu FoxPro
.pcd	Skompilowany skrypt Microsoft Visual Test lub obraz w formacie Photo CD
.pif	Skrót do programu systemu MS-DOS
.prf	Informacje o profilu programu Outlook (*msrating.dll*)
.prg	Plik źródłowy programu FoxPro
.reg	Wpisy rejestru
.scf	Polecenie programu Microsoft Windows Explorer
.scr	Wygaszacz ekranu
.sct	Składnik skryptów systemu Windows
.shb	Skrót do dokumentu
.shs	Obiekt Shell Scrap
.url	Skrót internetowy
.vb	Plik VBScript
.vbe	Zakodowany plik skryptów języka VBScript
.vbs	Plik VBScript
.wsc	Składnik skryptów systemu Windows
.wsf	Plik skryptów systemu Windows
.wsh	Plik z ustawieniami Hosta skryptów systemu Windows
.xsl	Plik XML, który może zawierać skrypt

Ćwiczenie 4.4.

Aby przekonać się, jak skończy się próba wysłania wiadomości z dołączonym załącznikiem jednego z blokowanych typów:

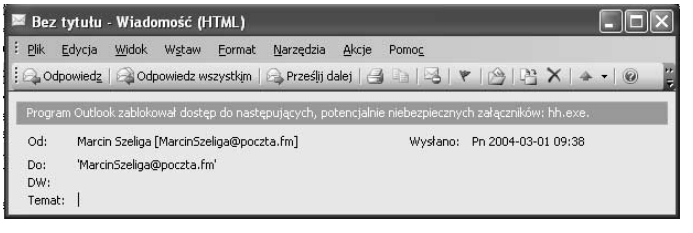
1. Otwórz formularz nowej wiadomości i zaadresuj ją do siebie.
2. Dołącz do wiadomości dowolny, krótki plik z rozszerzeniem *.exe*.
3. Kliknij przycisk *Wyślij*. Wyświetlone zostanie pokazane na rysunku 4.5 ostrzeżenie.



Rysunek 4.5.
Potencjalnie niebezpieczne załączniki i tak nie będą mogły zostać odebrane przez adresata wiadomości, nawet jeżeli korzysta on z innego programu pocztowego — prawdopodobnie taka wiadomość zostanie zablokowana na serwerze pocztowym

4. Kliknij przycisk *Tak*.

5. Po odebraniu tej wiadomości otwórz ją w okienku formularza wiadomości (rysunek 4.6).

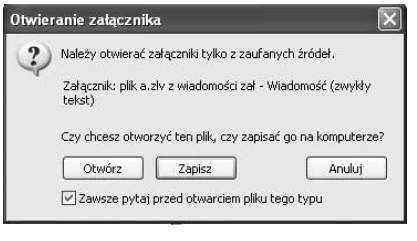


Rysunek 4.6.
Nawet jeżeli serwer pocztowy nie zablokuje wiadomości z potencjalnie niebezpiecznym załącznikiem, jej odbiorca nie będzie w stanie nie tylko uruchomić, ale nawet skopiować załącznika

6. Jeżeli musisz wysłać komuś plik blokowanego typu, albo **zmień jego rozszerzenie** (np. na *.bak*) **i w treści wiadomości poinformuj odbiorcę o prawidłowym rozszerzeniu pliku**, albo **skompresuj plik którymś z programów** do archiwizacji plików (np. programem *FreeZip*).

7. Raz jeszcze wyślij do siebie ten sam załącznik, ale tym razem zmień jego rozszerzenie albo skompresuj plik.

8. Odbierz wiadomość i dwukrotnie kliknij załącznik — wyświetlone zostanie okno dialogowe umożliwiające jego uruchomienie lub zapisanie (rysunek 4.7).



Rysunek 4.7.
Po zmianie rozszerzenia plik załącznika może zostać skopiowany na lokalny komputer

9. Zapisz plik i albo przywróć jego oryginalne rozszerzenie, albo rozpakuj archiwum.

Przetwarzanie wiadomości w formacie HTML

Odbieranie wiadomości zapisanych w formacie HTML może być zagrożeniem nie tylko Twojej prywatności, ale nawet bezpieczeństwa komputera. Zagrożenie polega na tym, że jeżeli w treści wiadomości znajdują się odnośniki do zapisanych na zdalnym komputerze (np. serwerze WWW) plików, z reguły plików graficznych, to w trakcie jej wyświetlania automatycznie nawiązane zostanie połączenie z tym komputerem i pobrane zostaną te pliki. Zagrożeniem bezpieczeństwa jest domyślne w systemie Windows przesłanie

do zdalnego serwera zaszyfrowanego (co nie znaczy, że bezpiecznego) hasła użytkownika, a zagrożeniem Twojej prywatności — uzyskanie przez wrogą osobę pewności, że Twój adres jest prawidłowy. Po uzyskaniu takiego potwierdzenia nadal będzie ona wysłała Ci niechciane wiadomości.

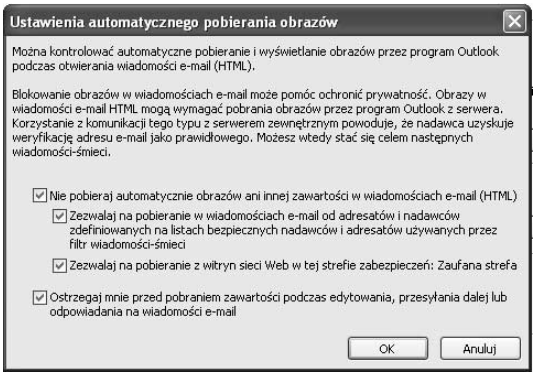
Jeżeli odebrałeś niechcianą wiadomość zawierającą odnośnik, którego kliknięcie ma usunąć Cię z listy adresatów tych śmieci, nie klikaj go. Znacznie częściej ma on służyć zweryfikowaniu istnienia konta — jeżeli potwierdzisz istnienie konta (bo przecież odebrałeś wysłaną na ten adres wiadomość), nie pozbędziesz się już wysyłanych na ten adres śmieci.

Ćwiczenie 4.5.

Aby skonfigurować automatyczne przetwarzanie wiadomości:

1. Wybierz *Narzędzia/Opcje…*.
2. Przejdź do zakładki *Zabezpieczenie* i kliknij przycisk *Zmień ustawienia automatycznego pobierania…*.
3. Domyślnie pobrane będą wyłącznie pliki, do których odnośniki znajdować się będą w wiadomościach przysłanych od zaufanych nadawców albo zapisane na uznanych za bezpieczne witrynach (rysunek 4.8).

Rysunek 4.8. *Domyślne ustawienia zabezpieczeń automatycznego pobierania plików*



4. Jeżeli nie będzie się to wiązało z utrudnieniami w korzystaniu z poczty, usuń zaznaczenie obu pól wyboru *Zezwalaj na pobieranie…*.
5. Kliknij przycisk *OK* i zamknij okno opcji.

Certyfikaty

Urzędy certyfikacji wystawiają certyfikaty, które służą do potwierdzania tożsamości użytkowników lub komputerów. Ponieważ każdy certyfikat jest podpisany przez wystawiający go urząd certyfikacji, treść certyfikatu umożliwia nie tylko zidentyfikowanie użytkownika posługującego się danym certyfikatem, lecz również urzędu certyfikacji, który go wystawił. Zapisany w certyfikacie klucz umożliwia również szyfrowanie przesyłanych plików, w tym wiadomości.

Tylko szyfrowanie i podpisywanie przy użyciu certyfikatu wiadomości zagwarantuje Ci, że: odbiorca wiadomości będzie w stanie jednoznacznie stwierdzić, czy odebrana przez niego wiadomość jest autentyczna (tj. czy rzeczywiście została wysłana przez Ciebie i czy po jej wysłaniu ktokolwiek jej nie zmodyfikował) i że wiadomość zostanie odczytana wyłącznie przez odbiorcę.

Pobieranie certyfikatu

Zanim będziesz mógł zaszyfrować czy podpisać wysyłane wiadomości, musisz pobrać i zainstalować wykorzystywany do zabezpieczenia poczty elektronicznej certyfikat. Proces instalowania certyfikatu opiszemy na przykładzie instalacji **darmowego na okres jednego miesiąca** certyfikatu wystawianego przez centrum certyfikacji Signet — w przypadku korzystania z usługi innych firm jego przebieg może nieco się różnić.

Ważność testowego certyfikatu może zostać odpłatnie przedłużona.

Ćwiczenie 4.6.

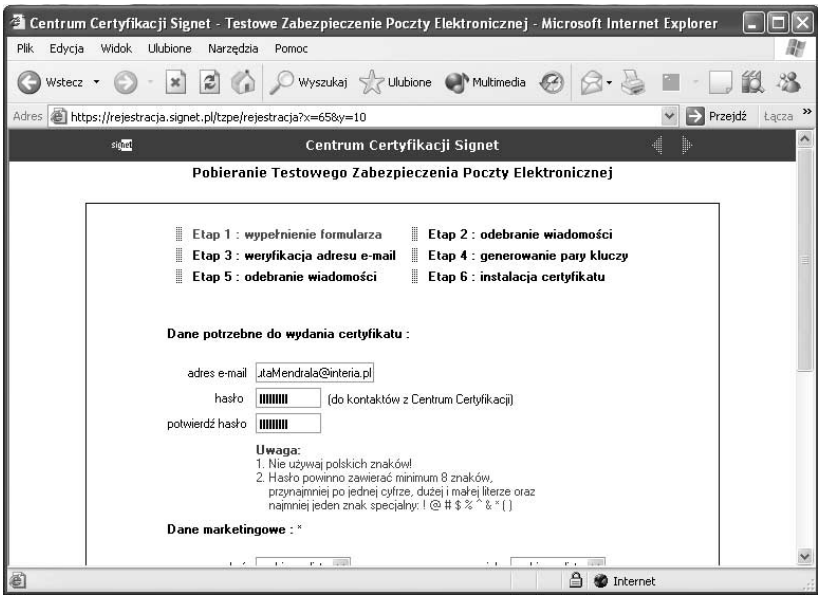
Aby otrzymać certyfikat:

1. Połącz się z witryną *http://www.signet.pl*.
2. Rozwiń znajdującą się w sekcji *Szybki start* listę wyboru *Pobierz certyfikat*.
3. Wybierz pozycje *Testowe Zabezpieczenie Poczty Elektronicznej*.
4. Aby ważność certyfikatu mogła być sprawdzana, należy pobrać i zainstalować certyfikat centrum certyfikacji, które go wystawiło — kliknij przycisk *CC Signet — Root CA*.
5. Zapisz certyfikat na dysku.
6. Zminimalizuj okno przeglądarki internetowej i uruchom pobrany plik. Wyświetlone zostanie okno dialogowe pokazane na rysunku 4.9.

Rysunek 4.9.
Instalacja certyfikatu centrum certyfikacji (CA) spowoduje dodanie go do listy zaufanych wydawców certyfikatów

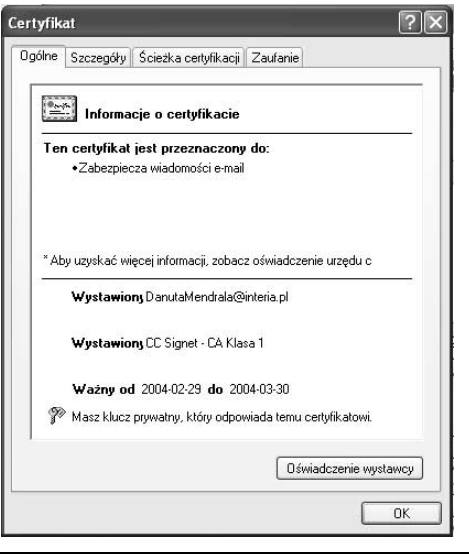
7. Kliknij przycisk *Zainstaluj certyfikat…*. Uruchomiony zostanie *Kreator importu certyfikatów*.
8. Kolejno kliknij przyciski *Dalej*, *Dalej* i *Zakończ*. Przy prawidłowo skonfigurowanym systemie wyświetlone zostanie ostrzeżenie o próbie dodania nowego centrum certyfikacji do listy zaufanych wydawców certyfikatów. Kliknij *Tak*.
9. Zamknij okno właściwości certyfikatu i przywróć okno przeglądarki internetowej.
10. Kliknij przycisk *Pobierz*. **Nawiązane zostanie bezpieczne połączenie** z serwerem WWW firmy Signet. Dwukrotnie kliknij znajdującą się na pasku stanu przeglądarki internetowej ikonę kłódki i wyświetl ścieżkę certyfikacji — po zainstalowaniu certyfikatu RootCA wszystkie wystawione przez ten urząd certyfikaty mogą być sprawdzane. Zamknij okno *Certyfikat*.
11. Wypełnij pola formularza i kliknij przycisk *Przejdź do etapu 2* (rysunek 4.10).

Rysunek 4.10. *Wysyłanie żądania wystawienia certyfikatu*



12. Zamknij okno przeglądarki internetowej. Po kilku minutach na podany adres przysłana zostanie wiadomość zawierająca długi odnośnik — kliknij go.
13. Wyświetlony zostanie formularz z pytaniem o podane w punkcie 11 hasło. Wpisz je i kliknij przycisk *Wyślij*.
14. Sprawdź, czy wyświetlony został poprawy adres e-mail i przejdź do kolejnego etapu.
15. Kliknij przycisk *Generuj klucze*. Ponownie, przy prawidłowo skonfigurowanym systemie, wyświetlone zostanie ostrzeżenie. Kliknij *Tak*.
16. Jeżeli wyświetlone zostanie okno dialogowe *Tworzenie nowego klucza RSA*, kliknij przyciski *OK*.
17. Zamknij okno przeglądarki internetowej. Po kilku minutach na podany adres przysłana zostanie wiadomość zawierająca kolejny długi odnośnik — kliknij go.

18. Kliknij przycisk *Instaluj certyfikat*. Ponownie powinno zostać wyświetlone ostrzeżenie o próbie zainstalowania dwóch nowych certyfikatów. Kliknij przycisk *Tak*.
19. Zamknij okno przeglądarki internetowej i wyświetl obszar roboczy programu Outlook.
20. Wybierz *Narzędzia/Opcje…* i przejdź do zakładki *Zabezpieczenia*.
21. Kliknij przycisk *Ustawienia…*. W polach *Certyfikat podpisujący:* i *Certyfikat szyfrujący:* widoczny będzie adres Twojego konta. Kliknij dowolny przycisk *Wybierz…*.
22. Jeżeli jest to Twój jedyny certyfikat, kliknij przycisk *Wyświetl certyfikat*; w innym przypadku najpierw zaznacz zainstalowany certyfikat.
23. Przejrzyj informacje o certyfikacie i zamknij wszystkie otwarte okna dialogowe (rysunek 4.11).



Rysunek 4.11. *Do podpisywania i szyfrowania wiadomości wymagany jest certyfikat i związany z nim klucz prywatny*

Eksport certyfikatu

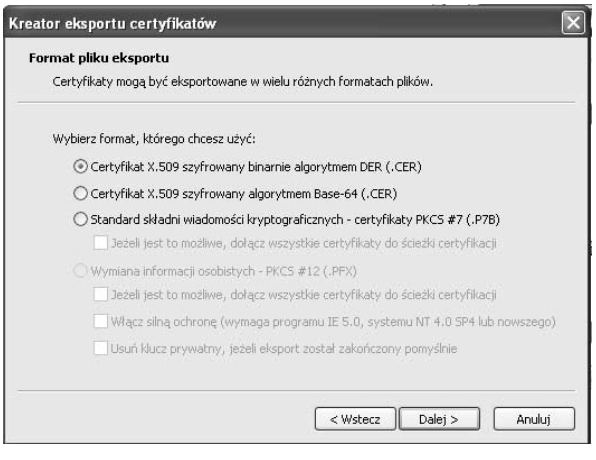
Po zainstalowaniu certyfikatu możesz już podpisywać cyfrowo wysłane przez Ciebie wiadomości. Jednak zanim będziesz mógł je zaszyfrować, powinieneś zainstalować certyfikaty wszystkich osób, do których planujesz wysłać zaszyfrowane wiadomości i udostępnić tym osobom własny certyfikat. Możesz to zrobić albo **przesyłając im plik certyfikatu**, albo **podpisaną cyfrowo wiadomość**.

Szyfrowanie wiadomości wymaga zapisanego w certyfikacie użytkownika klucza publicznego odbiorcy wiadomości i klucza prywatnego nadawcy. Własny klucz prywatny zainstalowałeś, wykonując poprzednie ćwiczenie.

Ćwiczenie 4.7.

Aby zapisać w pliku zainstalowany certyfikat:

1. Wybierz *Narzędzia/Opcje…/Zabezpieczenia*.
2. Kliknij przycisk *Ustawienia…*.
3. Kliknij znajdujący się obok pola *Certyfikat szyfrowania* przycisk *Wybierz…*.
4. Wybierz swój certyfikat i kliknij przycisk *Wyświetl certyfikat*.
5. Przejdź do zakładki *Szczegóły* i kliknij przycisk *Kopiuj do pliku…*. Zostanie uruchomiony *Kreator eksportu certyfikatów*.
6. Kliknij *Dalej*, **upewnij się, czy zaznaczone jest pole** *Nie eksportuj klucza prywatnego* i kliknij przycisk *Dalej*.
7. Wybierz format pliku (*.CER*) i kliknij przycisk *Dalej* (rysunek 4.12).



Rysunek 4.12. *Program Outlook umożliwia import certyfikatów zapisanych w formacie CER*

8. Kliknij *Dalej* i podaj nazwę oraz lokalizację pliku certyfikatu.
9. Zakończ pracę kreatora i zamknij wszystkie otwarte okna dialogowe.

Podpisywanie wiadomości

Podpis cyfrowy gwarantuje odbiorcy wiadomości, że jej nadawcą jest określona osoba (wysłanie wiadomości z cudzego konta nie jest specjalnie trudne) i że sama wiadomość po wysłaniu nie została przez nikogo zmieniona. Ponieważ jedynym warunkiem podpisywania wiadomości jest zainstalowanie własnego certyfikatu, po podpisaniu cyfrowo wiadomości zostanie do niej dołączony Twój certyfikat. **Osoby, które mają własny certyfikat i otrzymają tę wiadomość, będą mogły szyfrować wysyłane do Ciebie wiadomości**.

Ćwiczenie 4.8.

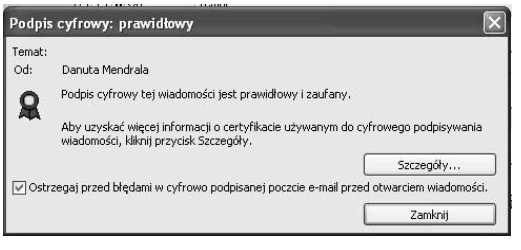
Aby cyfrowo podpisać wiadomość:

1. Zaadresuj wiadomość do osób, które powinny otrzymać Twój certyfikat.
2. Napisz treść wiadomości.
3. Kliknij znajdującą się na pasku narzędzi ikonę *Podpisz cyfrowo* albo kliknij *Opcje…/Ustawienia zabezpieczeń…/Dodaj podpis cyfrowy do wiadomości*, a następnie *OK* i *Zamknij*.

Aby automatycznie podpisywać wszystkie wysyłane wiadomości, wybierz *Narzędzia/Opcje… /Zabezpieczenia* i zaznacz pole wyboru *Dodaj podpis cyfrowy do wysyłanych wiadomości*.

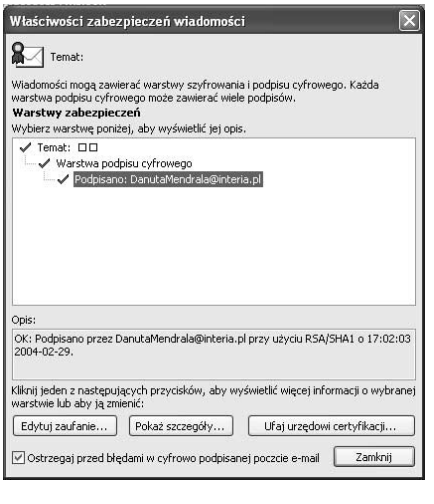
4. Wyślij wiadomość. Jej odbiorcy po otrzymaniu będą mogli sprawdzić autentyczność wiadomości:
   a) Po otrzymaniu podpisanej wiadomości kliknij znajdującą się w prawej części nagłówka ikonę podpisu. Wyświetlone zostanie okno dialogowe pokazane na rysunku 4.13.

Rysunek 4.13.
Podpisana cyfrowo, autentyczna wiadomość



5. Aby zapisać w pliku wykorzystany do podpisu certyfikat:
   a) Kliknij przycisk *Szczegóły*….
   b) Zaznacz wykorzystany do podpisania wiadomości certyfikat i kliknij przycisk *Pokaż szczegóły*… (rysunek 4.14).

Rysunek 4.14.
Podpisane wiadomości zawierają plik certyfikatu ich nadawcy



c) Kliknij przycisk *Wyświetl certyfikat…*.

d) Przejdź do zakładki *Szczegóły* i kliknij przycisk *Kopiuj do pliku…*.

e) Opis dalszych czynności związanych z zapisaniem certyfikatu w pliku znajduje się w poprzednim ćwiczeniu.

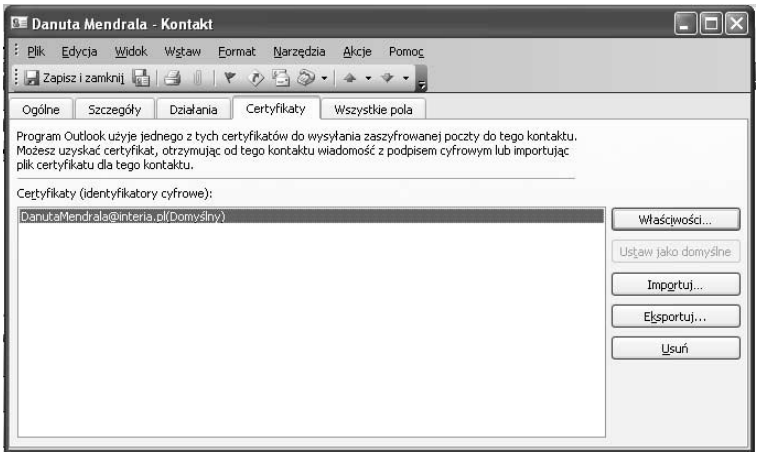
Importowanie cudzego certyfikatu

Otrzymany od znajomej osoby certyfikat należy zaimportować. Pozwoli to na szyfrowanie wysyłanych do tej osoby wiadomości.

Ćwiczenie 4.9.

Aby zainstalować certyfikat znajomej osoby:

1. Kliknij przycisk *Kontakty*.
2. Wyświetl formularz *Kontakt* nadawcy wiadomości (osoby, której certyfikat planujesz zainstalować).
3. Przejdź do zakładki *Certyfikaty* i kliknij przycisk *Importuj…*.
4. Wskaż lokalizację pliku z certyfikatem i kliknij przycisk *Otwórz*. Certyfikat zostanie zaimportowany (rysunek 4.15).



Rysunek 4.15. *Osoby, których certyfikaty zaimportowałeś, będą mogły otrzymywać zaszyfrowane wiadomości*

5. Zamknij okno kontaktu.

Szyfrowanie wiadomości

Uwieńczeniem ćwiczeń z bieżącego podrozdziału będzie wysłanie znajomej osobie zaszyfrowanej wiadomości.

Ćwiczenie 4.10.

Aby zaszyfrować wysyłaną wiadomość:

1. Otwórz formularz nowej wiadomości.
2. Zaadresuj wiadomość do osoby, której certyfikat cyfrowy zaimportowałeś w poprzednim ćwiczeniu.

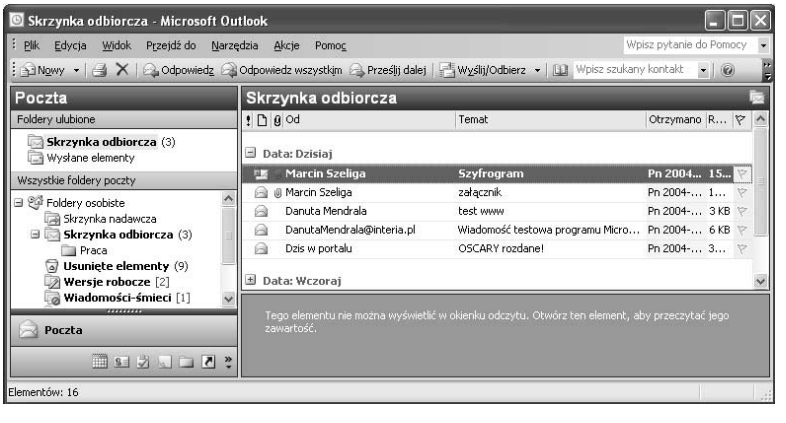
Próba zaszyfrowania wiadomości wysyłanej do osób, których certyfikatów nie zaimportowałeś, skończy się wyświetleniem ostrzeżenia, że niektórzy odbiorcy nie będą w stanie jej odczytać.

3. Kliknij znajdującą się na pasku narzędzi ikonę *Zaszyfruj wiadomość* albo kliknij *Opcje…/Ustawienia zabezpieczeń…/Szyfruj treść i załączniki wiadomości*, a następnie *OK* i *Zamknij*.

Aby automatycznie szyfrować wszystkie wysyłane wiadomości, wybierz *Narzędzia/Opcje… /Zabezpieczenia* i zaznacz pole wyboru *Szyfruj treść i załączniki wysyłanych wiadomości*.

4. Wpisz treść wiadomości i kliknij przycisk *Wyślij*.
5. Po odebraniu zaszyfrowanej wiadomości zaznacz ją (rysunek 4.16).

Rysunek 4.16. *Treść zaszyfrowanych wiadomości nie jest wyświetlana w okienku odczytu*



6. Dwukrotnie kliknij zaszyfrowaną wiadomość. Po ewentualnym pozwoleniu na dostęp do funkcji kryptograficznych systemu zostanie ona odszyfrowana i wyświetlona w formularzu wiadomości. Natomiast osoby, które nie mają zainstalowanego certyfikatu z kluczem prywatnym odpowiadającym kluczowi publicznemu wykorzystanemu do jej zaszyfrowania (a więc teoretycznie wszyscy poza odbiorcą wiadomości), a które przechwyciły wiadomość (co nie jest specjalnie trudne), zamiast jej treści zobaczą jedynie chaotyczny zbiór znaków.

Jeżeli haker zdobędzie klucz prywatny, będzie w stanie odczytać wszystkie zaszyfrowane za jego pomocą wiadomości. Ponieważ wystawienie nowego certyfikatu wiąże się z kosztami i kłopotami (będziesz zmuszony do wysłania nowego certyfikatu wszystkim znajomym), należy chronić plik z certyfikatem — przede wszystkim nie należy instalować i zapisywać go na komputerze, do którego dostęp mają inne osoby.