Windows Server 2003. Bezpieczeństwo sieci

Autorzy: Neil Ruston, Chris Peiris, Laura Hunter
Tłumaczenie: Adam Jarczyk (wstęp, rozdz. 1–7, 9, 10), Grzegorz Kowalczyk (rozdz. 8)
ISBN: 978-83-246-0498-2
Tytuł oryginału: How to Cheat at Designing Security for a Windows Server 2003 Network
Format: B5, stron: 584

Pomyśl o bezpieczeństwie już na etapie projektowania, a unikniesz późniejszych problemów

- Naucz się analizować wymogi biznesowe i techniczne
- Poznaj techniki sprawnego projektowania systemów
- Twórz bezpieczne sieci

Windows Server 2003 to niezwykle funkcjonalna, wydajna i skalowalna platforma wspomagająca zarządzanie sieciami komputerowymi. Jednak utworzenie na jej bazie bezpiecznego systemu w dużym przedsiębiorstwie może być bardzo skomplikowanym zadaniem. Dlatego warto, a nawet trzeba poświęcić odpowiednią ilość czasu na poprawne zaprojektowanie sieci. Pozwoli to uniknąć wielu problemów na dalszych etapach pracy.

Książka „Windows Server 2003. Bezpieczeństwo sieci" to zbiór praktycznych rozwiązań, które pomogą Ci szybko zaprojektować bezpieczną sieć. Nauczysz się gromadzić i analizować wymogi biznesowe oraz techniczne, które musi spełniać system. Dowiesz się, jak przygotować logiczny, a później fizyczny plan zabezpieczeń infrastruktury sieciowej. Przeczytasz także o tym, jak kontrolować dostęp do danych i tworzyć grupy służące do przyznawania uprawnień oraz jak zaprojektować fizyczne zabezpieczenia infrastruktury klienckiej.

- Analizowanie wymogów i ograniczeń
- Projektowanie architektury sieci
- Zarządzanie serwerami
- Projektowanie struktury kluczy publicznych i zarządzanie nią
- Proces zarządzania siecią
- Zabezpieczanie usług, protokołów sieciowych i dostępu zdalnego
- Korzystanie z usługi Active Directory
- Zabezpieczanie zasobów
- Komunikacja z komputerami klienckimi

Nie lekceważ zagrożeń — skorzystaj z praktycznych wskazówek i buduj bezpieczne sieci

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Współautorzy **9**

Redaktor merytoryczny **11**

Rozdział 1. Projektowanie architektury bezpiecznej sieci **13**

Wprowadzenie 13
Analiza wymogów firmy względem projektu bezpieczeństwa 14
Analiza istniejących zasad i procedur bezpieczeństwa 15
Ustalanie wymogów bezpieczeństwa danych 18
Analiza aktualnego stanu bezpieczeństwa 19
Projekt architektury dla implementacji zabezpieczeń 24
Przewidywanie zagrożeń dla sieci 24
Reagowanie na incydenty związane z bezpieczeństwem 35
Analiza ograniczeń technicznych projektu zabezpieczeń 39
Ustalenie możliwości istniejącej infrastruktury 40
Analiza ograniczeń interoperatywności 42
Podsumowanie 44
Rozwiązania w skrócie 45
Pytania i odpowiedzi 46

Rozdział 2. Zabezpieczanie serwerów na podstawie ich funkcji **49**

Wprowadzenie 49
Definiowanie wzorcowego szablonu zabezpieczeń 50
Szablony zabezpieczeń — dobre praktyki 52
Wstępnie zdefiniowane szablony zabezpieczeń w systemie Windows Server 2003 53
Ponowne stosowanie domyślnych ustawień zabezpieczeń 56
Konfiguracja szablonów zabezpieczeń 64
Konfiguracja zabezpieczeń dla starszych typów klientów 71
Wdrażanie szablonów zabezpieczeń 73
Projektowanie zabezpieczeń serwerów o określonych rolach 91
Typowe role serwerów 91
Konfiguracja zabezpieczeń kontrolerów domen 96
Zabezpieczanie roli IIS (Internet Information Server) 102
Konfiguracja zabezpieczeń serwerów poczty POP3 105
Zabezpieczanie innych ról w sieci 107
Modyfikacje wzorcowych szablonów zabezpieczeń według ról serwerów 117

Podsumowanie ... 123
Rozwiązania w skrócie ... 125
Pytania i odpowiedzi ... 127

Rozdział 3. Projektowanie bezpiecznej infrastruktury klucza publicznego ... 129
Wprowadzenie ... 129
Projektowanie infrastruktury klucza publicznego ... 130
Wprowadzenie do PKI ... 133
Projekt implementacji CA ... 135
Projektowanie logicznej strategii uwierzytelniania ... 141
Projektowanie zabezpieczeń serwerów CA ... 143
Projektowanie dystrybucji certyfikatów ... 147
Projektowanie zgłaszania żądań i dystrybucji ... 151
Aprobowanie certyfikatów przez administratora CA ... 153
Odwoływanie certyfikatów przez administratora CA ... 153
Konfiguracja odnawiania i inspekcji ... 154
Podsumowanie ... 157
Rozwiązania w skrócie ... 158
Pytania i odpowiedzi ... 159

Rozdział 4. Zabezpieczanie procesu zarządzania siecią ... 161
Wprowadzenie ... 161
Zabezpieczanie procesu zarządzania siecią ... 162
Zarządzanie ryzykiem w administrowaniu siecią ... 163
Zabezpieczanie najczęściej używanych narzędzi administracyjnych ... 166
Projektowanie zabezpieczeń dla Usług zarządzania awaryjnego ... 173
Projektowanie infrastruktury aktualizacji zabezpieczeń ... 174
Projekt infrastruktury Software Update Services ... 175
Wykorzystanie zasad grupy do wdrażania aktualizacji oprogramowania ... 177
Strategia identyfikacji komputerów, które nie mają aktualnego poziomu poprawek ... 179
Projektowanie relacji zaufania pomiędzy domenami i lasami ... 180
Projektowanie modeli zaufania pomiędzy lasami i domenami ... 183
Projektowanie zabezpieczeń w interoperacyjności ... 187
Podsumowanie ... 189
Rozwiązania w skrócie ... 191
Pytania i odpowiedzi ... 192

Rozdział 5. Zabezpieczanie usług i protokołów sieciowych ... 195
Wprowadzenie ... 195
Projektowanie zabezpieczeń infrastruktury sieciowej ... 196
IPSec — wprowadzenie ... 204
Skojarzenia zabezpieczeń ... 205
Tryby IPSec ... 208
Protokoły IPSec ... 208
Proces IPSec ... 213
Przegląd zasad IPSec ... 214
Domyślne zasady IPSec ... 214
Jak są aplikowane zasady IPSec? ... 222
Projektowanie zasad IPSec ... 231
Zabezpieczanie usługi DNS ... 239
Przestrzeń nazw DNS ... 240
Usługa Serwer DNS ... 242
Strefy DNS ... 245
Rekordy zasobów DNS ... 246
Klienty DNS ... 247

Projektowanie zabezpieczeń transmisji danych ... 248
Zabezpieczenia sieci bezprzewodowych ... 257
Krótka historia sieci bezprzewodowych ... 258
Zagrożenia sieci bezprzewodowych ... 260
Krótki przegląd technologii PKI i RADIUS/RAS ... 262
Projektowanie bezprzewodowych sieci lokalnych ... 264
Projektowanie infrastruktury WLAN ... 264
Projektowanie uwierzytelniania w sieciach bezprzewodowych ... 270
Projektowanie i testowanie infrastruktury dostępu bezprzewodowego ... 277
Podsumowanie ... 279
Rozwiązania w skrócie ... 280
Pytania i odpowiedzi ... 282

Rozdział 6. Zabezpieczanie usługi IIS ... 285
Wprowadzenie ... 285
Projektowanie uwierzytelniania użytkowników w IIS ... 286
Uwierzytelnianie za pomocą certyfikatów ... 289
Zintegrowane uwierzytelnianie systemu Windows ... 294
Uwierzytelnianie RADIUS ... 299
Projektowanie zabezpieczeń IIS ... 305
Zabezpieczanie IIS ... 306
Projektowanie strategii monitorowania IIS ... 317
Strategia zarządzania treścią WWW w serwerach IIS ... 325
Podsumowanie ... 326
Rozwiązania w skrócie ... 327
Pytania i odpowiedzi ... 329

Rozdział 7. Zabezpieczanie VPN i komunikacji ekstranetowej ... 331
Wprowadzenie ... 331
Projektowanie zabezpieczeń dla komunikacji pomiędzy sieciami ... 332
Windows Server 2003 jako router ... 333
Projektowanie połączeń VPN ... 343
Wybór protokołów dla dostępu VPN ... 345
Korzystanie z zasad dostępu zdalnego ... 357
Projektowanie routingu pomiędzy sieciami wewnętrznymi ... 360
Projektowanie infrastruktury ekstranetów ... 360
Podsumowanie ... 361
Rozwiązania w skrócie ... 362
Pytania i odpowiedzi ... 363

Rozdział 8. Zabezpieczanie usługi Active Directory ... 365
Wprowadzenie ... 365
Projektowanie strategii kontroli dostępu dla usług katalogowych ... 366
Analiza zagrożeń dla usług katalogowych ... 370
Tworzenie zasad zabezpieczeń konta ... 375
Tworzenie bezpiecznych haseł ... 387
Inspekcje aktywności konta użytkownika ... 394
Tworzenie strategii delegowania ... 401
Projektowanie strategii grup dla dostępu do zasobów ... 405
Tworzenie struktury uprawnień dla danych ... 407
Podsumowanie ... 411
Rozwiązania w skrócie ... 415
Pytania i odpowiedzi ... 416

Rozdział 9. Zabezpieczanie zasobów sieciowych 419
Wprowadzenie 419
Projektowanie strategii kontroli dostępu do plików i folderów 420
Analiza zagrożeń danych 421
Przegląd kontroli dostępu i list ACL 422
Dostęp do zasobów 427
Praca z grupami zabezpieczeń 430
Analiza wymogów inspekcji 440
Strategia kontroli dostępu do rejestru 446
System szyfrowania plików 456
Tworzenie strategii szyfrowania i odszyfrowywania plików i folderów 470
Bezpieczeństwo strategii wykonywania kopii zapasowych i przywracania danych 485
Zabezpieczanie procesu wykonywania kopii zapasowych i przywracania danych 486
Zabezpieczanie Usług zarządzania awaryjnego 496
Podsumowanie 507
Rozwiązania w skrócie 509
Pytania i odpowiedzi 511

Rozdział 10. Zabezpieczanie klientów sieciowych 515
Wprowadzenie 515
Zabezpieczanie komputerów klienckich 516
Utwardzanie klienckich systemów operacyjnych 516
Ograniczenie dostępu użytkownika do funkcji systemu operacyjnego 523
Projektowanie strategii uwierzytelniania klientów 524
Analiza wymogów uwierzytelniania 525
Wybór protokołu uwierzytelniania 531
Projektowanie planu bezpiecznego dostępu zdalnego 535
Wybór metody dostępu zdalnego 535
Wybór protokołu dostępu zdalnego 536
Projektowanie zasad dostępu zdalnego 538
Usługa uwierzytelniania internetowego 544
Podsumowanie 550
Rozwiązania w skrócie 551
Pytania i odpowiedzi 552

Skorowidz 555

Rozdział 3.

Projektowanie bezpiecznej infrastruktury klucza publicznego

W tym rozdziale:

- Projektowanie infrastruktury klucza publicznego
- Projektowanie dystrybucji certyfikatów

Wprowadzenie

Jednym z największych wyzwań w naszym świecie pełnym najróżniejszych połączeń są kwestie: jak zweryfikować tożsamość osób, których nigdy nie spotkaliśmy, aby prowadzić z nimi interesy, i jak przesyłać poufne informacje przez sieć publiczną, taką jak Internet? Wprawdzie istnieje wiele rozwiązań obu tych problemów, lecz jedno z nich jest obecnie stosowane powszechnie, z uwagi na stosunkowo niskie koszty i łatwość wdrożenia — **infrastruktura klucza publicznego**, w skrócie PKI (*public key infrastructure*). Spotkamy się z PKI zaimplementowaną z wielu powodów, lecz najczęstszym zastosowaniem jest zabezpieczenie transakcji e-handlu. PKI pozwala sprzedawcy zidentyfikować kupującego a klientom daje pewność, że przesyłają dane swoich kart kredytowych do właściwego odbiorcy.

Do tego celu służy szereg urzędów certyfikacji — CA (*Certificate Authority*), odgrywających rolę bezstronnego zewnętrznego pośrednika, ustalającego i weryfikującego tożsamość organizacji, które prowadzą interesy w Internecie. Cały system PKI opiera się na idei *zaufania*. Firma zajmująca się e-handlem ufa zewnętrznemu urzędowi certyfikacji (np. VeriSign) w kwestii wydana certyfikatu, którego będzie używać. Klient z kolei ufa, że certyfikat wydany przez firmę VeriSign jest autentyczny, to znaczy, że VeriSign

z należytą troską zweryfikowała, iż wydaje certyfikat pełnoprawnej firmie. Klienci ufają firmie VeriSign i certyfikatowi wydanemu przez VeriSign dla firmy internetowej, więc mogą bezpiecznie prowadzić interesy z danym sprzedawcą.

PKI może mieć też szereg zastosowań wewnątrz sieci korporacji. Implementacja PKI obecna w systemie Windows Server 2003 — *Usługi certyfikatów* — pozwala na użycie IPSec do zabezpieczania transmisji TCP/IP, komunikacji SSL z serwerem WWW oraz zaszyfrowanego systemu plików (EFS) do zabezpieczania plików i folderów znajdujących się w udostępnianych zasobach sieciowych. Teorie matematyczne, na których opiera się PKI, mogą zniechęcać Czytelnika, lecz znajomość zagadnienia (zarówno teoretyczna, jak i praktyczna) jest niezbędna, by odpowiednio zabezpieczyć sieć przedsiębiorstwa. Z tego powodu niniejszy rozdział zaczynamy od szczegółowego wyjaśnienia podstawowych idei, na których opiera się PKI, po czym omówimy praktyczne implementacje PKI w systemie Windows Server 2003. Przed przejściem do dalszej lektury książki zalecamy Czytelnikowi dokładne zapoznanie się z tematami omówionymi w niniejszym rozdziale, ponieważ wiele innych mechanizmów zabezpieczeń w systemie Windows Server 2003 wymaga do działania PKI i Usług certyfikatów.

Projektowanie infrastruktury klucza publicznego

Zanim zagłębimy się w temat CA w systemie Windows Server 2003, musimy zrozumieć podstawowe pojęcia PKI. W sieciach publicznych, takich jak Internet, codziennie wędrują miliony wiadomości. Jak uwierzytelniać te wiadomości? Jak poznać, że ktoś manipulował wiadomością, zanim dotarła do odbiorcy? Handel elektroniczny nie byłby możliwy w Internecie, gdyby na te pytania nie udało się skutecznie odpowiedzieć. Każda transakcja w e-handlu musi spełnić trzy podstawowe wymogi, by była bezpieczna i kompletna:

- **Nadawca jest upoważniony do wysłania wymaganej wiadomości.** Nadawca zostaje uwierzytelniony, by wysłać informację do odbiorcy.
- **Wiadomość jest autentyczna.** Treść wiadomości nie została zmieniona po drodze do odbiorcy. Haker może ją zdobyć, podłączając się do trasy transmisji, a następnie zmodyfikować treść, podszywając się pod oryginalnego nadawcę.
- **Nadawca nie może fałszywie zaprzeczyć wysłaniu wiadomości ani jej zawartości.** Ta funkcja jest powszechnie nazywana *niezaprzeczalnością* (*nonrepudiation*).

Oznacza to, że musimy chronić dane podczas procesu transmisji. W tym celu treść wiadomości jest szyfrowana za pomocą matematycznych algorytmów. Istnieje kilka metod szyfrowania wiadomości, lecz wszystkie można podzielić na dwie kategorie: algorytmy *symetryczne* i *asymetryczne*. Model symetryczny opiera się na wspólnym kluczu i dobrze sprawdza się w środowiskach „chronionych". Przykładem wymiany z kluczem symetrycznym jest transakcja w bankomacie. Klient i bank dysponują

tym samym numerem PIN (*Personal Identification Number*) w środowisku zamkniętym. Klient musi dobrze chronić swój klucz i nie ujawniać go nikomu. Im więcej osób zna numer PIN, tym bardziej maleje „skalowalność" bezpieczeństwa (więcej osób może podawać się za klienta). Bank i klient wstępnie uzgadniają ze sobą numer PIN. Takie rozwiązanie staje się jednak o wiele mniej bezpieczne, gdy inne osoby poznają ten numer.

Druga technologia szyfrowania nosi nazwę *kryptografii asymetrycznej* lub *kryptografii z kluczem publicznym*. Ta technika opiera się na parach dwóch asymetrycznych kluczy, które nie działają tak jak numer PIN. Klucz banku i klucz klienta są różne. Każda para składa się z klucza *prywatnego* i *publicznego*. Klucz publiczny może być udostępniony innym użytkownikom, lecz klucz prywatny jest unikatowy dla użytkownika lub zasobu i musi być utajniony. Autentyczność nadawcy i niezaprzeczalność opiera się na podpisaniu cyfrowego dokumentu jego kluczem prywatnym. Klucze prywatny i publiczny są ze sobą matematycznie powiązane, lecz poznanie klucza prywatnego przez złamanie klucza publicznego jest niemożliwe. Poza tym oba klucze mają odwrotne role (dane zaszyfrowane jednym kluczem mogą być odszyfrowane za pomocą drugiego).

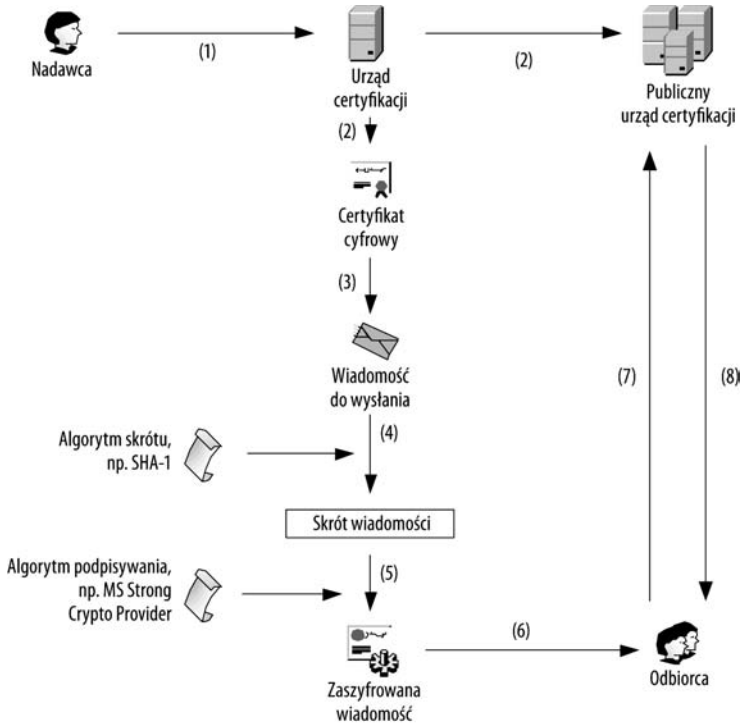
Certyfikaty cyfrowe opierają się na kryptografii z kluczem publicznym. Certyfikat jest tworzony poprzez zastosowanie do wiadomości dwóch poziomów kryptografii: algorytmów mieszających (skrótu) i algorytmów podpisywania:

- Algorytm mieszający, inaczej algorytm skrótu lub funkcja skrótu (*hashing algorithm*), jest bardzo skomplikowanym algorytmem matematycznym, stosowanym do oryginalnej wiadomości. Jego wynikiem jest 160-bitowy łańcuch, unikatowy dla każdej wiadomości. Łańcuch ten jest nazywany *skrótem wiadomości* (*message digest*). W platformach Microsoftu używanych jest kilka popularnych funkcji skrótu: MD2, MD4, MD5 i SHA-1.
- Po wygenerowaniu skrótu jest do niego stosowany algorytm podpisu. W procesie podpisywania używany jest klucz prywatny nadawcy. Wynikiem jest unikatowy ciąg znaków, nazywany *certyfikatem cyfrowym*. Domyślnym algorytmem podpisywania w systemie Windows Server 2003 jest *Microsoft strong cryptographic provider*.

Każdy użytkownik może zdobyć oprogramowanie do generowania certyfikatów cyfrowych i wygenerować własne klucze prywatne i publiczne. Narzędzia służące do tego są ogólnie dostępne w Internecie. Jak wobec tego możemy zaufać dokumentowi, który został cyfrowo podpisany? Złośliwy napastnik może wygenerować oprogramowanie podpisane cyfrowo równie łatwo, jak dobrze znany producent, a cyfrowy podpis może nas zwieść i przekonać do zainstalowania w naszej sieci złośliwego oprogramowania. Na szczęście istnieje rozwiązanie tego problemu: będziemy akceptować tylko użytkowników, którzy podpisują swoje dokumenty za pomocą certyfikatu wydanego przez dobrze znaną firmę lub zaufaną stronę. Takie zaufane strony noszą nazwę **urzędów certyfikacji**, czyli CA (*Certificate Authorities*). Certyfikaty na potrzeby transakcji e-handlu wydaje kilka liczących się CA; najlepiej znane z nich to VeriSign i RSA. W takim przypadku typowy użytkownik będzie miał większą pewność, że jego transakcje są chronione przez CA o dobrej reputacji.

Certyfikaty mogą też być potrzebne wewnątrz organizacji. Możemy za ich pomocą ograniczać dostęp do cennych zasobów. Infrastruktura klucza publicznego może być używana razem z takimi technologiami jak System szyfrowania plików EFS (*Encrypted File System*) i IPSec do ochrony zasobów przedsiębiorstwa; te zagadnienia zostaną omówione bardziej szczegółowo w dalszych rozdziałach. Możemy użyć usługi CA w systemie Windows Server 2003, by włączyć tę funkcjonalność.

Spróbujmy zastosować całą tę teorię w praktyce. Rysunek 3.1 przedstawia kompletny proces PKI, w którym wysyłamy wiadomość e-mail do odbiorcy.



Rysunek 3.1. *Sposób funkcjonowania PKI*

1. Proces zaczyna się od zażądania przez nadawcę certyfikatu z CA (1). Certyfikat cyfrowy jest nam potrzebny, by chronić wiadomość e-mail.
2. CA sprawdza poświadczenia użytkownika i wydaje certyfikat cyfrowy. Urząd certyfikacji może użyć Active Directory i danych logowania użytkownika w systemie Windows, by wspomóc generowanie certyfikatu. Dodatkowo CA publikuje certyfikat w publicznym repozytorium certyfikatów (dzięki temu odbiorca wiadomości będzie mógł zweryfikować tożsamość nadawcy). Ten krok jest reprezentowany jako (2).
3. Próbujemy podpisać wiadomość e-mail kluczem (3). Proces podpisywania składa się z dwóch faz.
4. Pierwszą fazą jest zastosowanie algorytmu skrótu (4). W jej wyniku otrzymujemy skrót wiadomości.

5. W drugiej fazie stosujemy do skrótu wiadomości algorytm podpisywania z kluczem prywatnym (5). Algorytm skrótu i dane podpisu są zawarte w certyfikacie, by wspomóc kroki (4) i (5). Wynikiem jest zaszyfrowana wiadomość.
6. Zaszyfrowana wiadomość zostaje wysłana do odbiorcy (6).
7. Odbiorca łączy się z publicznym repozytorium certyfikatów, by sprawdzić autentyczność informacji zawartych w certyfikacie (7).
8. Publiczne repozytorium certyfikatów odpowiada znacznikiem wskazującym autentyczność wiadomości (8). Odbiorca będzie mógł odszyfrować wiadomość zależnie od tej odpowiedzi.

Tak wygląda pełna implementacja PKI. Spróbujmy teraz przeanalizować proces PKI bardziej szczegółowo.

Wprowadzenie do PKI

PKI można opisać jako zbiór standardów, zasad, przepisów i procedur, które zapewniają bezpieczeństwo przy użyciu par kluczy prywatnych i publicznych. PKI wspomaga transakcje elektroniczne za pomocą certyfikatów cyfrowych i CA, pozwalając weryfikować i sprawdzać autentyczność potencjalnych użytkowników naszych aplikacji.

PKI w systemie Windows Server 2003 opiera się na standardzie infrastruktury klucza publicznego X.509 (PKIX) oraz standardach IETF (*Internet Engineering Task Force*), by zapewnić zgodność z innymi implementacjami PKI. IETF zaleca też stosowanie kilku innych standardów zabezpieczeń, które ściśle współpracują z architekturą PKI: TLS (*Transport Layer Security*), S/MIME (*Secure Multipurpose Internet Mail Extensions*) oraz IPSec.

Przyjrzyjmy się teraz dokładniej architekturze PKI. Jest ona kombinacją kilku kluczowych elementów, od samych certyfikatów aż po listy autoryzujące lub odmawiające użytkownikowi dostępu do zasobów przedsiębiorstwa.

- **Certyfikaty cyfrowe.** Certyfikaty są rdzeniem technologii PKI i zawierają klucze publiczne, służące do walidacji użytkownika. Klucz publiczny jest podpisem cyfrowym, służącym do podpisywania i szyfrowania danych, które użytkownicy wymieniają w sieci przedsiębiorstwa. Certyfikat cyfrowy zawiera wersję, numer seryjny, podpis wydawcy, datę ważności, nazwę podmiotu i klucz publiczny podmiotu oraz wystawia unikatowy identyfikator, unikatowy identyfikator podmiotu i informacje o rozszerzeniach. Pozwala to stronom trzecim ustalić tożsamość użytkownika i wydawcy certyfikatu.
- **Urzędy certyfikacji (CA).** CA wydają zaufane certyfikaty. Użytkownik musi otrzymać certyfikat z CA, by mieć podpis cyfrowy. W obrębie przedsiębiorstwa może istnieć kilka CA, które będą zorganizowane w logiczny sposób, aby wykonywać specjalne zadania. Niektóre mogą służyć do wydawania certyfikatów dla podległych urzędów certyfikacji, a inne do wydawania wewnętrznych lub zewnętrznych certyfikatów.

Rady niezależnego specjalisty

TLS, S/MIME i IPSec

Przyjrzyjmy się trochę dokładniej tym trzem protokołom. Są one używane razem z PKI, by poprawić bezpieczeństwo aplikacji klasy enterprise. Protokoły te są niezależne od procesu uwierzytelniania certyfikatów PKI, lecz współpracują z nim, pozwalając uniknąć naruszenia zabezpieczeń przez napastników.

- **Protokół Transport Layer Security (TLS)** — standard branżowy, zapewniający bezpieczną komunikację z serwerami WWW (w sieciach wewnętrznych i w Internecie). Udostępnia bezpieczny zaszyfrowany kanał do przesyłania danych i pomaga uwierzytelniać użytkowników. TLS jest zaawansowaną wersją protokołu SSL.
- **Secure Multipurpose Internet Mail Extensions (S/MIME)** — ulepszenie standardu MIME, zapewniające bezpieczną wymianę poczty elektronicznej dzięki podpisom cyfrowym, które udowadniają pochodzenie wiadomości. S/MIME pozwala również szyfrować treść wiadomości, zapewniając poufność danych.
- **Internet Security Protocol (IPSec)** — zestaw protokołów, które udostępniają będące standardem branżowym mechanizmy kryptograficzne w wymianie danych. IPSec implementuje algorytmy dla wszystkich protokołów stosu TCP/IP z wyjątkiem ARP (*Address Resolution Protocol*). Standard IPSec jest używany razem z protokołem L2TP (*Layer 2 Tunneling Protocol*) w wirtualnych sieciach prywatnych (VPN).

- **Repozytoria certyfikatów.** Po wydaniu przez CA certyfikaty muszą być gdzieś przechowywane. Repozytorium jest „kontenerem" służącym do tego celu. Preferowaną lokalizacją repozytorium certyfikatów w systemie Windows Server 2003 jest Active Directory. Usługa Active Directory udostępnia użytkownikom certyfikaty na żądanie. Same certyfikaty są fizycznie przechowywane na dyskach twardych urzędów certyfikacji. Active Directory zawiera odnośniki, pozwalające zlokalizować na żądanie odpowiedni certyfikat.
- **Odzyskiwanie kluczy.** Ten proces odzyskuje w sytuacji awaryjnej klucz prywatny z pary kluczy publiczny-prywatny (użytkownik mógł utracić klucz lub administrator musi przyjąć tożsamość użytkownika). Ten proces nie przywraca żadnych danych ani wiadomości przesyłanych pomiędzy użytkownikiem i serwerem przedsiębiorstwa, a jedynie poświadczenia klucza prywatnego.

To są główne składniki PKI. Jak jednak zarządzać procesem wydawania certyfikatów? Czy możemy zapobiec uzyskaniu certyfikatu przez złośliwego użytkownika? Potrzebne są nam pewne zasady i narzędzia do zarządzania procesem wydawania certyfikatów. Do tego celu służą następujące elementy:

- **Zasady certyfikatów i reguły postępowania**, które udokumentują sposób użycia certyfikatów w przedsiębiorstwie. W dokumentach tych są opisane szczegóły sposobów użycia certyfikatów, relacje zaufania pomiędzy certyfikatami i zasobami oraz konsekwencje nadużycia zaufania.

- **Lista certyfikatów unieważnionych** (*Certificate Revocation List* — CRL) wskazuje, które certyfikaty zostały unieważnione przed upłynięciem czasu ważności. Użytkownicy znajdujący się na tej liście tracą dostęp do zasobów zabezpieczanych przez certyfikaty.

CRL może być długą listą, której przesyłanie zajmuje dużą część pasma sieci. Serwer certyfikatów w systemie Windows Server 2003 wprowadza nową ideę o nazwie Delta CRL (przyrostowa lista certyfikatów unieważnionych). Delta CRL publikuje tylko ostatnio unieważnione certyfikaty, by zużyć mniej zasobów sieci. Wyświetlana jest tylko część listy, a nie pełna CRL.

- **Lista zaufanych certyfikatów (CTL)** dokumentuje zaufane certyfikaty w przedsiębiorstwie. Ta podpisana lista jest publikowana przez CA. Zarządzanie CTL w systemie Windows Server 2003 odbywa się przez obiekty zasad grupy (GPO).

PKI może pełnić wiele funkcji zabezpieczających przedsiębiorstwo, w tym:

- Cyfrowe podpisywanie wiadomości e-mail, aplikacji i ważnych dokumentów.
- Ochrona dostępu zdalnego do komputerów przez Internet.
- Użycie kart inteligentnych do uwierzytelniania i jednokrotnego logowania w całym przedsiębiorstwie.

Pierwszym krokiem w implementacji PKI jest zaprojektowanie CA, obejmujące identyfikację wymagań organizacji dla certyfikatów. Możemy zmodernizować CA z istniejącej implementacji Windows (NT 4.0 lub Windows 2000) lub innego producenta i skorzystać z nowych funkcji dostępnych w systemie Windows Server 2003. Po ukończeniu fazy projektowania możemy wdrożyć PKI na potrzeby wewnętrznych zabezpieczeń i bezpiecznej wymiany danych z partnerami firmy. Zobaczmy, jak wygląda projektowanie implementacji CA.

Projekt implementacji CA

Projektowanie urzędu certyfikacji jest bardzo ważnym krokiem. Poprawny projekt CA zapewni świadczenie użytkownikom niezawodnych usług i jednolitą strukturę do usuwania i dodawania użytkowników, a zarazem zmniejszy koszty utrzymania. Przy implementowaniu CA należy rozważyć kilka czynników:

- **Projekt głównego urzędu certyfikacji.** Duże przedsiębiorstwo może mieć szereg CA, które będą wydawać certyfikaty użytkownikom. Wszystkie te CA muszą być kontrolowane z jednego, centralnego miejsca, które nosi nazwę **głównego urzędu certyfikacji** (*root CA*). Ten CA musi zostać zaimplementowany i poprawnie skonfigurowany, zanim zaczniemy tworzyć hierarchię urzędów certyfikacji. Ważne jest też, kto będzie właścicielem CA. Kto ma sprawować kontrolę i zarządzać CA (na przykład, naczelne kierownictwo czy też dział informatyki)? Kolejną ważną kwestią jest funkcjonalność

głównego urzędu certyfikacji. Czy będzie tylko delegować do innych CA w hierarchii? Czy ma wydawać certyfikaty dla użytkowników? Omówimy to w następnym punkcie.

Projektowanie i planowanie

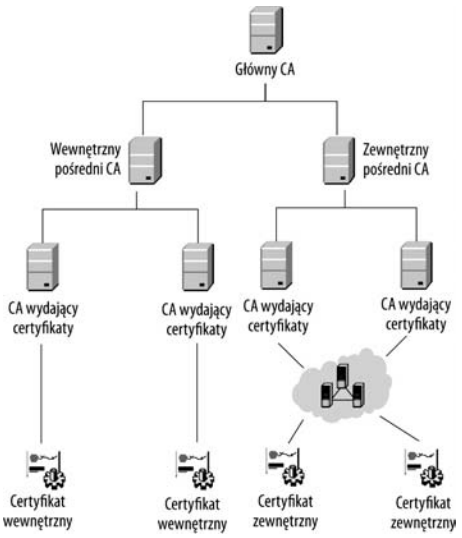
Różnice pomiędzy głównym i podrzędnymi CA

Główny CA znajduje się na szczycie hierarchii urzędów certyfikacji i musi zawsze być zaufany. Na głównym CA kończy się łańcuch certyfikatów. Przedsiębiorstwo może mieć główny CA **przedsiębiorstwa** (*enterprise*) lub **autonomiczny** (*stand-alone*) — różnice zostaną omówione w dalszej części rozdziału. Główny CA jest jedyną jednostką, która może *sama podpisywać* (wydawać) własne certyfikaty w przedsiębiorstwie. Windows Server 2003 pozwala tylko jednemu komputerowi pełnić rolę głównego CA. Jest to najważniejszy urząd certyfikacji i dobrą praktyką jest odłączenie go od sieci i używanie podrzędnych CA do wydawania certyfikatów użytkownikom.

Wszystkie urzędy certyfikacji poza głównym są zaklasyfikowane jako podrzędne. Pierwszy poziom podrzędnych CA otrzymuje własne certyfikaty z głównego urzędu certyfikacji. Serwery te są często określane terminem **pośrednich CA** i przekazują informacje certyfikacji dalej w dół łańcucha CA. Nazywa się je „pośrednimi" CA, ponieważ *pośredniczą* pomiędzy głównym CA i CA wydającymi certyfikaty. Pośrednie CA instruują CA wydające certyfikaty poprzez certyfikaty dostosowane dla przedsiębiorstwa. Informacje te dalej są używane do generowania certyfikatów dla użytkowników. Powszechne jest stosowanie w przedsiębiorstwach osobnych CA wydających certyfikaty dla kontroli dostępu wewnętrznego oraz osobnych dla dostępu z zewnątrz.

Rysunek 3.2 ilustruje typową hierarchię CA w przedsiębiorstwie.

Rysunek 3.2. *Typowa struktura hierarchii CA przedsiębiorstwa*



- **Definiowanie typów i ról CA.** W systemie Windows Server 2003 zdefiniowane są dwa typy CA: *przedsiębiorstwa* i *autonomiczne*. Każdy z nich można skonfigurować jako główny lub podrzędny urząd certyfikacji. Podrzędny CA można dodatkowo skonfigurować jako urząd certyfikacji pośredni lub wydający certyfikaty.

Rady niezależnego specjalisty

Urzędy certyfikacji przedsiębiorstwa i autonomiczne

Urzędy certyfikacji przedsiębiorstwa (*enterprise CA*) publikują certyfikaty i listy CRL w Active Directory. Usługa Active Directory zawiera informacje o kontach użytkowników, użytkownikach i zasadach decydujących, czy zaaprobować wydanie certyfikatu, czy nie. CA przedsiębiorstwa wykorzystują szablony certyfikatów, które służą do generowania certyfikatów dla użytkowników. Możemy więc użyć CA przedsiębiorstwa do automatycznego wydawania i aprobowania certyfikatów. Certyfikaty kart inteligentnych są automatycznie mapowane na ustawienia Active Directory, umożliwiając w ten sposób uwierzytelnianie w Active Directory za pomocą kart inteligentnych.

Urzędy certyfikacji przedsiębiorstwa są ściśle powiązane ze strukturą Active Directory przedsiębiorstwa. Oznacza to, że CA przedsiębiorstwa może jedynie wydawać certyfikaty dla użytkowników z Active Directory. Po zainstalowaniu usługi CA w komputerze niemożliwa staje się zmiana nazwy serwera CA, ponieważ unieważniłoby to certyfikaty. Komputer urzędu certyfikacji przedsiębiorstwa nie może też zostać usunięty ze struktury domen przedsiębiorstwa. Musimy więc rozważyć strukturę Active Directory przed zaplanowaniem implementacji PKI. Obecność w przedsiębiorstwie więcej niż jednego lasu Active Directory może skomplikować sprawę. Konieczne jest w takiej strukturze przydzielenie osobnego CA przedsiębiorstwa dla każdego lasu. Urzędy certyfikacji przedsiębiorstwa są też zależne od obecności schematu Active Directory. Może zajść konieczność aktualizacji tego schematu z wersji Windows 2000 do Windows Server 2003 (niektóre funkcje, np. szablon certyfikatów w wersji 2, są obsługiwane tylko przez schemat AD z systemu Windows Server 2003).

Autonomiczne CA (*stand-alone CA*) nie wykorzystują Active Directory ani szablonów certyfikatów. W przypadku autonomicznego CA certyfikat musi zawierać wszystkie dane użytkownika (w środowisku CA przedsiębiorstwa dane te mogą być wspólnie używane przez certyfikaty i Active Directory). Z tego powodu certyfikaty wydawane przez autonomiczne CA mają większe rozmiary niż w CA przedsiębiorstwa. Poza tym certyfikaty wydane przez autonomiczny urząd certyfikacji muszą być aprobowane przez administratora — oczekują w kolejce, dopóki nie zostaną zaakceptowane. Można skonfigurować autonomiczny CA tak, że będzie wydawać certyfikaty automatycznie, lecz nie jest to zalecane, ponieważ brak wtedy autoryzacji w Active Directory. Autonomiczne urzędy certyfikacji są konfigurowane jako należące do grup roboczych (w przeciwieństwie do kontrolerów domeny). Możemy więc zmienić nazwę serwera CA, co nie będzie miało negatywnego wpływu na proces generowania certyfikatów.

Zaleca się używanie CA przedsiębiorstwa w organizacjach, gdzie użytkownicy posiadają konta w systemie Windows i ustawienia Active Directory. Pozwala to automatycznie wydawać certyfikaty takim użytkownikom. Autonomiczne CA są częściej stosowane w sieciach zewnętrznych i internetowych zastosowaniach PKI. Certyfikaty takie muszą być aprobowane przez administratora, ponieważ nie są związane z kontami Windows w przedsiębiorstwie.

- **Czy chcemy utrzymywać wewnętrzne CA, czy oddelegować zadanie do CA zewnętrznego dostawcy usługi?** Odpowiedź na to pytanie zależy od struktury i budżetu PKI. Jeśli firma prowadzi dużo wewnętrznych działań biznesowych, korzystne jest posiadanie własnego, wewnętrznego urzędu certyfikacji. Jeśli większość interesów firma prowadzi z zewnętrznymi partnerami, zewnętrzny urząd certyfikacji może być lepszy. Zewnętrzny urząd certyfikacji może też zwiększyć zaufanie klientów. Oprócz tego eksperci od inspekcji zabezpieczeń wolą mieć do czynienia z zewnętrznymi dostawcami usługi, cieszącymi się dobrą reputacją, np. VeriSign.

- **Jaki będzie optymalny poziom pojemności CA?** Osoby podejmujące decyzje w przedsiębiorstwie powinny uzgodnić wydajność i skalowalność serwerów CA. Zależy to od liczby certyfikatów wydawanych przez CA, rodzaju sprzętu serwera CA i rozmiaru samych certyfikatów. Należy też wziąć pod uwagę jakość zasobów sieciowych i liczbę klientów, które trzeba będzie skonfigurować.

Projektowanie i planowanie

Skalowalność PKI opartej na systemie Windows Server 2003

Autonomiczny urząd certyfikacji w systemie Windows Server 2003 może pomieścić 35 milionów certyfikatów o standardowych rozmiarach. Wielkość certyfikatu jest czynnikiem decydującym. System Windows Server 2003 uruchomiony w komputerze z dwoma procesorami i 512 MB pamięci może wydawać do 2 milionów certyfikatów dziennie. W wielu implementacjach CA przepustowość sieci i jakość zasobów sieciowych mają podstawowe znaczenie i decydują o liczbie CA w organizacji. Wymiana informacji w sieci dla 2 milionów certyfikatów może generować znaczące obciążenie sieci. Wprawdzie z łatwością możemy podłączyć lub odłączyć CA od sieci, lecz modernizacja samej sieci jest przedsięwzięciem kosztownym i czasochłonnym. Inne czynniki, które należy brać pod uwagę w serwerach CA, to:

- **Liczba procesorów** — im więcej procesorów, tym większa wydajność.
- **Wydajność dysków** — zależy od liczby wydawanych certyfikatów i ich rozmiarów. Jeśli certyfikaty są większe lub ich liczba przekracza 2 miliony dziennie, potrzebny będzie kontroler dysków o wyższej wydajności.
- **Pojemność dysków twardych** — średnia wielkość certyfikatu wynosi około 17 kB. Wpisy w dzienniku związane z certyfikatem mają około 15 kB. Rozmiary bazy danych certyfikatów rosną wraz z liczbą wydawanych certyfikatów, co musimy wziąć pod uwagę.
- **Liczba administratorów CA** — w niektórych organizacjach stosowany jest rozproszony model administracyjny, rozciągający się na większą liczbę biur i działów informatyki. Zwykle dobrze jest scentralizować kontrolę w małym zespole, aby zaoszczędzić pasma sieci i zmniejszyć koszty administracyjne.

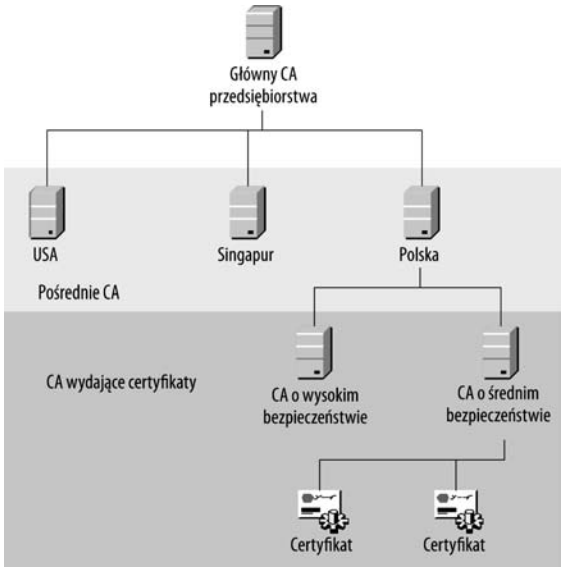
To są czynniki, które należy brać pod uwagę przy projektowaniu CA. Musimy teraz zająć się sposobem rozmieszczenia tych urzędów certyfikacji tak, by wydawać certyfikaty dla użytkowników. Istnieje kilka modeli grupowania (organizowania) CA na potrzeby implementacji PKI, powszechnie nazywanych *hierarchiami zaufania*.

Model PKI w systemie Windows Server 2003 składa się z dobrze zdefiniowanych relacji nadrzędny-podrzędny pomiędzy serwerami CA. Podrzędny CA jest certyfikowany przez nadrzędny CA i otrzymuje upoważnienie do wydawania certyfikatów dla następnego poziomu serwerów CA. Zaleca się zorganizowanie serwerów urzędów certyfikacji w model trzypoziomowy. Kolejne poziomy w tym modelu to główny urząd certyfikacji, pośrednie CA i CA wydające certyfikaty. Prześledźmy te hierarchie zaufania na przykładzie fikcyjnej firmy IronClad Security, mającej filie w USA, Singapurze i Polsce. Jest to duża firma, mająca wielu partnerów biznesowych. Zatrudnia w filiach 10 000 pracowników, z czego część etatowych, a część kontraktowych.

Hierarchia geograficzna

CA w hierarchii geograficznej są zorganizowane zgodnie z filiami przedsiębiorstwa. Model taki pozwala regionalnym administratorom bardziej wydajnie zarządzać swoimi domenami. Firma ma filie w USA, Singapurze i Polsce, więc trzypoziomowa hierarchia zaufania firmy, oparta na geografii, może wyglądać jak na rysunku 3.3.

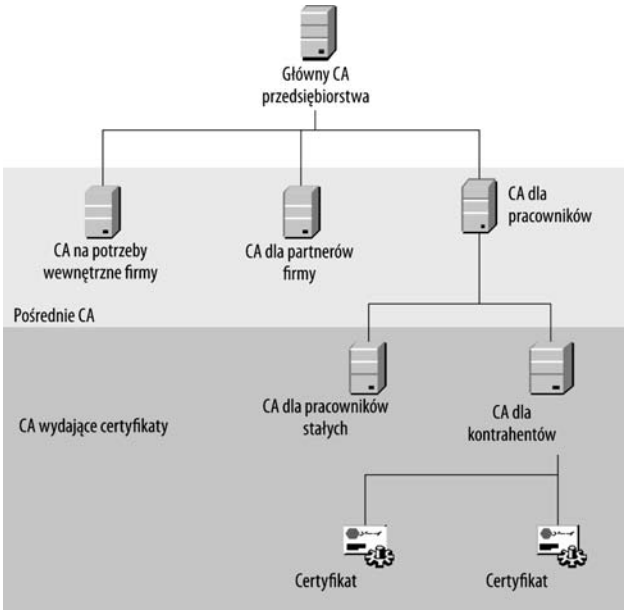
Rysunek 3.3.
Przykład hierarchii geograficznej



Firma ma jeden główny urząd certyfikacji, który może mieścić się w USA, Singapurze lub Polsce. Stanowi on pierwszy poziom hierarchii CA. Drugim poziomem są pośrednie CA, przydzielone na podstawie lokalizacji. Oznacza to, że filie w USA, Singapurze i Polsce będą miały własne CA. Trzecim poziomem są CA wydające certyfikaty. Na rysunku 3.3 zostały przedstawione CA w polskiej filii. Muszą tu być wydawane dwa typy certyfikatów: o wysokim poziomie bezpieczeństwa (dla poufnych informacji; będą one bardzo szczegółowe i kosztowne) oraz o średnim poziomie bezpieczeństwa (które nie mają aż tak wysokich wymogów). Certyfikaty o średnim poziomie bezpieczeństwa są mniej opisowe i mniej kosztowne. Wyznaczyliśmy osobne serwery CA dla użytkowników o wysokim i średnim poziomie bezpieczeństwa.

Hierarchia organizacyjna

Hierarchia zaufania może też być zaprojektowana pod kątem struktury organizacyjnej przedsiębiorstwa. Firma IronClad Security zatrudnia zarówno stałych pracowników, jak i kontrahentów. Ma też wielu partnerów biznesowych. Partner firmy może nie życzyć sobie, by korzystać ze wspólnego certyfikatu z innymi partnerami. Certyfikaty dla wewnętrznych pracowników to osobna sprawa. Takie wymogi uzasadniają zbudowanie hierarchii zaufania na podstawie struktury organizacyjnej, mogącej wyglądać jak na rysunku 3.4.



Rysunek 3.4. *Przykład organizacyjnej hierarchii zaufania*

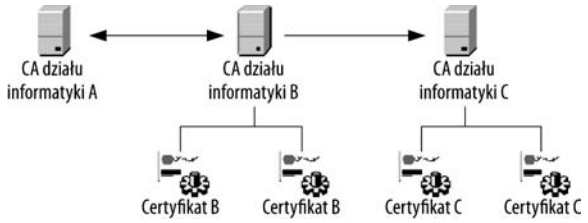
Hierarchia zaufania firmy IronClad Security oparta na strukturze organizacyjnej jest również zgodna z trzypoziomowym modelem CA. Zawiera jeden główny urząd certyfikacji. Pośrednie CA odzwierciedlają strukturę organizacyjną firmy. Jeden serwer CA został przeznaczony na wewnętrzne potrzeby firmy. Drugi służy do wydawania certyfikatów dla partnerów biznesowych. Trzeci służy do wydawania certyfikatów dla pracowników. Firma IronClad Security ma zarówno kontrahentów, jak i stałych pracowników, więc dobrze jest przeznaczyć osobne CA dla obu typów pracowników.

Sieciowa hierarchia zaufania

Niektóre organizacje mają rozproszone i niezależne działy informatyki. W takiej sytuacji wyznaczenie i zaimplementowanie jednego głównego urzędu certyfikacji może być trudne, a komunikacja pomiędzy filiami może być ograniczona, ponieważ wszystkie działają niezależnie we własnych domenach. Projekt z pojedynczym głównym CA może nie być rozwiązaniem odpowiednim dla takiego scenariusza.

Możemy uporać się z tym problemem, projektując sieciowy model zaufania. W modelu tym nie istnieje jeden główny urząd certyfikacji; rolę tę przejmuje kilka CA. Pomiędzy tymi CA występują „relacje zaufania", uzyskane poprzez wydanie przez CA dla siebie nawzajem *certyfikatów wzajemnych* (*cross certificate*). Certyfikaty wzajemne mogą być jednostronne lub dwustronne. Spróbujmy wyjaśnić ten scenariusz na przykładzie firmy IronClad Security. Firma ta przyznała swoim różnym działom informatyki uprawnienia do zaimplementowania sieciowego modelu zaufania. Każdy dział informatyki ma własny serwer CA. Poszczególne działy nawiązują ze sobą relacje zaufania za pomocą certyfikatów wzajemnych. Ilustruje to rysunek 3.5.

Rysunek 3.5.
Przykład sieciowej hierarchii zaufania



Firma IronClad Security ma trzy działy informatyki i żadnego głównego CA. Każdy dział używa własnego CA do wydawania certyfikatów. Pomiędzy nimi istnieją certyfikaty wzajemne, umożliwiające dostęp z jednego działu do drugiego. Te relacje mogą być jednostronne lub dwustronne. Na przykład, pomiędzy działami A i B istnieje relacja dwustronna, więc pracownicy z A i B mogą korzystać z zasobów obu działów (inaczej mówiąc, pracownik działu A ma dostęp do zasobów działu B i vice versa). Pomiędzy działem B i C istnieje jednak tylko jednostronna relacja zaufania. Z tego powodu dział C nie będzie mógł uzyskać żadnych certyfikatów z działu B, więc jego pracownicy nie będą mieli dostępu do zasobów działu B. Dział B ma jednostronny dostęp do C, więc użytkownicy z B mogą uzyskać dostęp do zasobów działu C.

Sieciowy model zaufania jest trudniejszy w utrzymaniu niż model z głównym urzędem certyfikacji. Trudność utrzymania rośnie wraz z liczbą CA w przedsiębiorstwie. Model ten może też mieć ujemny wpływ na przepustowość sieci. Zalecany jest, gdy pomiędzy działami występuje minimalna komunikacja.

Dodatkowym problemem w modelu sieciowym jest brak głównego CA. Oznacza to, że w przedsiębiorstwie trzeba zainstalować globalną usługę katalogową (np. Active Directory). Jest ona jedyną metodą, która pozwoli znaleźć CA innych działów.

Projektowanie logicznej strategii uwierzytelniania

Logiczna strategia uwierzytelniania dla przedsiębiorstwa może być bardzo złożona. Musimy zapewnić bezpieczne środowisko do komunikacji z partnerami biznesowymi. Przedsiębiorstwo może mieć wielu pracowników w wielu lokalizacjach. Pracownicy ci mogą pracować na terenie firmy lub zdalnie (łącząc się zdalnie z domu), mogą też odbywać podróże służbowe. Najważniejszym elementem strategii uwierzytelniania jest uniemożliwienie napastnikom dostępu do poufnych danych. Wszystkie te czynniki musimy wziąć pod uwagę, aby stworzyć logiczną strategię uwierzytelniania dla firmy.

System Windows Server 2003 udostępnia bezpieczną architekturę dla użytkowników, komputerów i usług w przedsiębiorstwie. Dla wszystkich zasobów, które mają być w firmie udostępniane, tworzone są konta w Active Directory. Pierwszym krokiem będzie przegląd istniejącej strategii uwierzytelniania. Powinniśmy zidentyfikować zasoby, które nie są z nią zgodne. Następnie należy utworzyć w Active Directory konta dla użytkowników tych zasobów. Tworzenie kont użytkowników powinno odbywać się za pomocą *planu zarządzania kontami użytkowników*. Plan ten będzie dokumentować użytkowników, ich prawa dostępu i przyczyny, dla których powinni otrzymać dostęp do zasobów. Następnie należy skonfigurować konta komputerów

i usług. Informacje o tych kontach powinny zostać zawarte w planie zarządzania kontami komputerów. Kolejnym krokiem będzie zabezpieczenie procesu uwierzytelniania w przedsiębiorstwie. Możemy to osiągnąć na szereg sposobów:

- **Tworzenie zasad silnych haseł dla użytkowników i kont usług w przedsiębiorstwie.** Hasła powinny być kombinacją liter i cyfr i mieć długość przynajmniej ośmiu znaków.
- **Konfiguracja zasad blokady kont.** Intruzi używają zautomatyzowanych, wyrafinowanych algorytmów do odkrywania haseł do kont użytkowników. Musimy więc skonfigurować system Windows Server 2003 tak, że będzie reagował na powtarzające się niepowodzenia uwierzytelnienia hasła. Konto powinno zostać zablokowane, jeśli użytkownik nie będzie w stanie podać poprawnego hasła w określonej liczbie prób (często stosuje się blokadę po trzech nieudanych próbach).
- **Ograniczenie dostępu do określonych godzin.** Konta można skonfigurować tak, że będą dostępne według harmonogramu (na przykład, od godziny 9:00 do 18:00 od poniedziałku do piątku). Pomoże to powstrzymać hakerów, którzy próbują spenetrować system w innych godzinach.
- **Monitorowanie czasu wygasania certyfikatów PKI.** Musimy ustawić czas ważności wszystkich certyfikatów wydawanych przez przedsiębiorstwo. Okres ważności certyfikatów jest różny w różnych organizacjach. Należy rewidować regularnie ten parametr, aby ustalić najlepszy czas ważności certyfikatu na potrzeby firmy. Pomoże to zapobiec próbom włamania do systemu przez niezadowolonych byłych pracowników.

Możemy używać certyfikatów PKI do uwierzytelniania wielu użytkowników i zasobów. Możemy zaimplementować usługę Obsługa rejestrowania w sieci Web usług certyfikatów (omówioną w dalszej części rozdziału), aby wydawać certyfikaty dla stron aplikacji WWW. Strony (aplikacje) te za pomocą certyfikatów będą mogły z łatwością uwierzytelniać się w innych zasobach przedsiębiorstwa. Możemy za pomocą architektury PKI używać zabezpieczeń opartych na rolach. Certyfikat zawiera wszystkie niezbędne informacje o użytkownikach i ich prawach dostępu, więc możemy zaimportować informacje zabezpieczeń do dowolnego zasobu w sieci przedsiębiorstwa. Zasób może zezwalać na dostęp lub odmawiać, zależnie od informacji znajdujących się w certyfikacie. Możemy umieścić wszystkie niezbędne role użytkownika w Active Directory. Serwer CA sprawdzi wpisy w Active Directory (używając API logowania do systemu Windows), aby wygenerować certyfikat dla danego użytkownika. Informacje o rolach będą osadzone w certyfikacie użytkownika i sprawdzane przez zasoby (za pomocą Active Directory) za każdym razem, gdy użytkownik będzie próbował zyskać dostęp do zasobu. Po zmodyfikowaniu ról wydamy nowy certyfikat dla użytkownika.

Możemy też użyć kart inteligentnych, by rozszerzyć infrastrukturę PKI. Pracownicy będą musieli włożyć taką kartę do każdego urządzenia, do którego będą chcieli uzyskać dostęp. Karty inteligentne „zmuszają" pracownika do użycia klucza asymetrycznego i numeru PIN do uwierzytelnienia (zostanie to omówione w dalszej części rozdziału). Omówimy też w jednym z dalszych rozdziałów użycie certyfikatów 802.1x do uwierzytelniania w urządzeniach bezprzewodowych.

Musimy też podjąć odpowiednie kroki, by zabezpieczyć CA przedsiębiorstwa i autonomiczne. CA przedsiębiorstwa regularnie komunikuje się z Active Directory, więc zaleca się, by ten urząd certyfikacji znajdował się w tej samej podsieci co serwery Active Directory. Zminimalizuje to ruch w sieci i opóźnienia. W większości dużych przedsiębiorstw można spotkać farmę serwerów o wysokim bezpieczeństwie, chronioną zaawansowanymi metodami: uzbrojeni strażnicy, bezpieczne drzwi i środki techniczne takie jak uwierzytelnianie za pomocą kart inteligentnych. Serwer CA przedsiębiorstwa będzie podłączony do takiej farmy. CA przedsiębiorstwa musi uwierzytelniać się w kontrolerze domeny, by uzyskać dostęp do Active Directory, więc trudno jest odłączyć ten serwer od sieci. Z tego powodu musimy rozważnie zaplanować dodanie CA do sieci (po ustawieniu nazwy CA przedsiębiorstwa trudno będzie zmienić nazwę komputera bez narażenia istniejących certyfikatów). Implementacja autonomicznych urzędów certyfikacji została omówiona w podpunkcie „Zabezpieczanie autonomicznego CA".

Projektowanie zabezpieczeń serwerów CA

Zabezpieczenie serwerów CA przedsiębiorstwa jest bardzo ważnym krokiem w implementacji PKI. Włamanie do CA pozwala hakerom przeprowadzić mnóstwo różnych ataków na poufne dane przedsiębiorstwa. Mogą oni modyfikować certyfikaty lub zmieniać konfigurację serwerów CA, wpływając w ten sposób na wszystkie systemy w zasobach informatycznych przedsiębiorstwa. Powinniśmy podjąć odpowiednie kroki w stronę zabezpieczenia serwerów CA. Omówimy ten temat bardziej szczegółowo. Zacznijmy od typowych zagrożeń urzędów certyfikacji.

Typowe zagrożenia usług certyfikatów

Główny urząd certyfikacji jest najważniejszym CA w przedsiębiorstwie. Włamanie do niego naraża całą implementację PKI, ponieważ główny CA dostarcza wszystkie informacje o certyfikatach poprzez pośrednie urzędy certyfikacji do wydających certyfikaty w organizacji. Włamanie do głównego CA pozwala napastnikom manipulować danymi certyfikatów i wydawać fałszywe certyfikaty przez nadużycie CA wydających certyfikaty, które będą bezbronne, ponieważ są podległe głównemu CA.

Jak zabezpieczyć główny CA przed włamaniem? Najczęściej stosowanym przez napastników sposobem włamania do CA jest atak przez sieć. Sieci przedsiębiorstw mogą być bardzo złożone, więc bardzo trudno je utrzymywać i przeprowadzać inspekcje. Może to pozwolić inteligentnemu hakerowi na penetrację systemów poprzez niezałatane lub niewykryte luki w zabezpieczeniach. Luką taką może być choćby skradziona karta dostępu należąca do administratora systemów albo wyrafinowane algorytmy oprogramowania, które skanuje otwarte porty w zaporze sieciowej przedsiębiorstwa. Udany atak może pozwolić na zdobycie klucza prywatnego głównego CA i zniszczenie zasobów przedsiębiorstwa lub manipulowanie nimi. Ważne jest, by ochronić CA, *zanim* napastnik zaatakuje.

Najlepszą metodą ochrony głównego urzędu certyfikacji jest odłączenie go od sieci. W ten sposób, nawet jeśli sieć zostanie zinfiltrowana, napastnik nie uzyska dostępu do głównego CA. Ten sam krok można podjąć w przypadku pośrednich CA; w środowiskach o wysokim bezpieczeństwie systemy te powinny być odłączone od sieci. Uniemożliwi to przechwycenie ich kluczy prywatnych przez napastników. Odłączenie CA od sieci może odbyć się na jeden z poniższych sposobów:

- **Instalacja autonomicznego serwera Windows Server 2003 jako głównego CA.** System ten powinien być fizycznie odłączony od sieci.

Zaleca się nie instalować serwera CA jako członka domeny. Sprawi to problemy, gdy administrator CA podłączy serwer do sieci w celu konserwacji lub wykonania kopii zapasowej. Hasła dla kont w domenie domyślnie wygasają po 30 dniach, więc hasła serwera CA po 30-dniowym okresie staną się nieważne. Rozwiązaniem problemu jest skonfigurowanie odłączonego od sieci serwera CA jako członka grupy roboczej.

Nie należy konfigurować CA przedsiębiorstwa jako głównego urzędu certyfikacji. CA przedsiębiorstwa komunikuje się z globalnym katalogiem (Active Directory). Odłączenie od sieci głównego CA, na którym jest również zainstalowany CA przedsiębiorstwa, spowoduje problemy z aktualizacjami Active Directory, więc główny CA powinien być skonfigurowany jako autonomiczny.

- **Wyłączenie usługi CA.** Serwer CA może być podłączony do sieci, możemy jednak wyłączyć lub zatrzymać usługę CA w komputerze. Taki krok ograniczy proces generowania certyfikatów i zatrzyma działania z tym związane. CA przestanie wydawać, blokować, aktualizować i odczytywać dane certyfikatów, a automatyczne wydawanie certyfikatów zostanie wyłączone. Jednakże serwer CA pozostanie podatny na ataki hakerów skanujących system plików, by uzyskać dane certyfikatów.
- **Fizyczne wyłączenie serwera CA.** Ta metoda jest powszechnie stosowana dla głównych CA wymagających najwyższych zabezpieczeń. Serwer głównego CA pozostaje fizycznie wyłączony, dopóki nie zajdzie potrzeba wydania nowych certyfikatów dla pośrednich CA. Uniemożliwia to jednak inspekcje serwera CA.

Rady niezależnego specjalisty

Skutki odłączenia CA od sieci

Odłączenie urzędu certyfikacji od sieci nie ma wpływu na certyfikację po stronie klienta. Klient potrzebuje danych CRL i AIA do weryfikacji poświadczeń certyfikatu. Klient taki sprawdza łańcuch certyfikacji i upewnia się, że wpis nie znajduje się na liście CRL. Informacje CRL i AIA są udostępniane przez inne, podrzędne CA, dostępne w sieci. Te urzędy certyfikacji wydają informacje zgodnie z instrukcjami otrzymanymi z nadrzędnych CA, odłączonych od sieci. Urząd certyfikacji odłączony od sieci przetwarza bardzo niewielką liczbę żądań z podrzędnych CA, wydających certyfikaty. Oznacza to, że koszty administracyjne są pomijalne. Spróbujmy to wyjaśnić na przykładzie firmy IronClad Security z poprzedniego punktu.

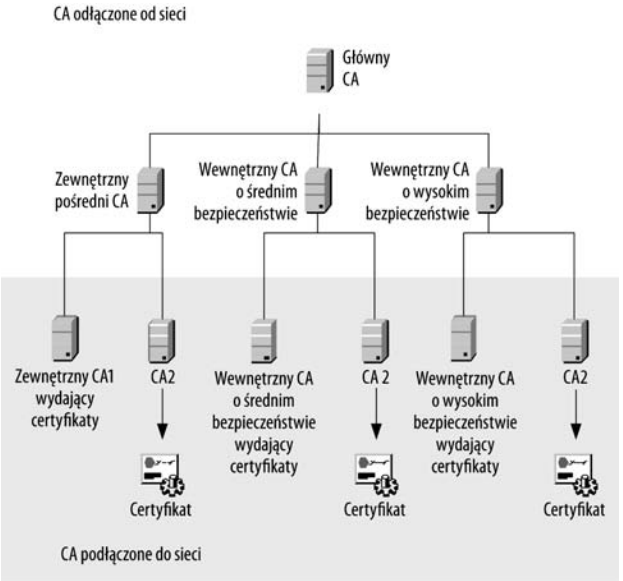
Firma IronClad Security ma geograficzną strukturę hierarchii CA. Jej główny urząd certyfikacji znajduje się w filii w USA. Pośrednie CA znajdują się w USA, Singapurze i Polsce. W każdej geograficznej lokalizacji obecne są też CA wydające certyfikaty. Główny CA w Stanach Zjednoczonych zostanie odłączony od sieci korporacji i będzie podłączany tylko w celu aktualizacji lub wydania nowych certyfikatów dla pośrednich CA w USA, Singapurze i Polsce. Te pośrednie urzędy certyfikacji również przez większość czasu są odłączone od sieci. Zostają włączone tylko po to, by wydać certyfikaty dla CA wydających certyfikaty. Tylko te ostatnie urzędy certyfikacji znajdujące się w sieciach lokalnych firmy są „widoczne" cały czas. Główny i pośrednie CA są włączane do sieci tylko w określonych porach w celu utrzymania (na przykład do zaktualizowania informacji Active Directory) i aktualizacji certyfikatów.

Spróbujmy wykorzystać wszystkie te informacje w praktyce. Będziemy projektować przykładową implementację PKI w systemie Windows Server 2003, opartą na zalecanych rozwiązaniach, dla fikcyjnej firmy. Zaczniemy od hierarchii serwerów CA przedsiębiorstwa, a następnie omówimy kroki niezbędne, by zabezpieczyć autonomiczny serwer CA.

Zabezpieczanie hierarchii CA przedsiębiorstwa

Hierarchia przedsiębiorstwa może składać się z wielu urzędów certyfikacji. Musimy zorganizować je w logiczną strukturę. Firma może mieć tylko jeden główny urząd certyfikacji, który nie powinien być zależny od żadnych innych zasobów przedsiębiorstwa (np. Active Directory). Główny CA nie może więc być urzędem certyfikacji przedsiębiorstwa. Interakcja z Active Directory może powodować pewne problemy (aktualizacje nie będą odzwierciedlane w czasie rzeczywistym, ponieważ CA będzie odłączony od sieci). Właściwym rozwiązaniem będzie więc zaimplementowanie głównego CA jako autonomicznego.

Na potrzeby firmy posłużymy się trzypoziomowym modelem CA. Będzie on na najwyższym poziomie zawierał jeden główny urząd certyfikacji. Główny CA będzie delegować zadania do pośrednich CA. Rozkład pośrednich CA zależy od struktury organizacyjnej lub modelu biznesu. W naszej fikcyjnej firmie zidentyfikowaliśmy trzy główne obszary dystrybucji certyfikatów. Zachodzi potrzeba wydawania certyfikatów na zewnątrz dla partnerów biznesowych. Wewnętrzne bezpieczeństwo firmy wymaga stosowania dwóch typów certyfikatów. Certyfikaty wydawane przez wewnętrzny CA o wysokim bezpieczeństwie będą chronić poufne dane. Certyfikaty o średnim poziomie bezpieczeństwa będą wydawane przez osobny wewnętrzny CA. Architekturę CA ilustruje rysunek 3.6.



Rysunek 3.6. *Przykład trzypoziomowej hierarchii CA przedsiębiorstwa*

Struktura ta daje nam bezpieczny i elastyczny mechanizm wydawania certyfikatów w przedsiębiorstwie. Jest też skalowalna, więc pozwala dodawać i usuwać serwery CA. Urzędy certyfikacji pośrednie i wydające certyfikaty możemy dodawać i usuwać zależnie od potrzeb. Zobaczmy, jak możemy zabezpieczyć autonomiczne CA i dostawców usług kryptograficznych — CSP (*Cryptographic Service Provider*).

Zabezpieczanie autonomicznego CA

Autonomiczny CA można zabezpieczyć na kilka sposobów. Zaleca się implementować główne i pośrednie CA jako autonomiczne. Możemy takie serwery odłączyć od sieci, co zostało omówione w podpunkcie „Typowe zagrożenia usług certyfikatów". Certyfikaty wydawane przez CA muszą być przechowywane w bezpiecznym środowisku, zwykle nazywanym dostawcą usług kryptograficznych (CSP). Oto kilka innych metod zabezpieczenia:

- **Użycie sprzętowego CSP.** Dostępne są sprzętowe CSP, zdolne do obsługi złożonej kryptografii i magazynów kluczy. Sprzętowy magazyn kluczy CSP jest bezpieczniejszy od programowego. Trudno w nim manipulować, w przeciwieństwie do programowego CSP, gdzie klucze mogą być przechowywane na dyskach twardych. Pozwala to administratorom CA, używającym sprzętowych CSP, przedłużyć okres ważności certyfikatów.

Niektórzy hakerzy są zdolni do uzyskania zrzutu pamięci w programowych CSP. Może to doprowadzić do zdobycia przez nich kluczy prywatnych organizacji. Sprzętowe CSP nie sprawiają tego problemu. Nie przechowują danych kluczy w pamięci, lecz w dedykowanych urządzeniach. Utrudnia to hakerom zdobycie danych o kluczach prywatnych.

Należy też wziąć pod uwagę fizyczny dostęp do sprzętowych CSP. Urządzenia powinny być przechowywane w bezpiecznych strefach budynku o ograniczonym dostępie. Należy też utrzymywać kopie zapasowe danych kont dostępu i kluczy prywatnych.

- **Sprzętowe CSP mogą być kosztowne w zakupie i utrzymaniu.** Alternatywą dla nich mogą być karty inteligentne, w których będą zapisane klucze.

Implementacja kart inteligentnych dodaje kolejny poziom zabezpieczeń przedsiębiorstwa. Klucz kryptograficzny jest zapisany w karcie. Dostęp do karty wymaga podania odpowiedniego numeru PIN, więc do dostępu lub odwołania danych certyfikatu niezbędne są zarówno karta, jak i numer PIN. Eliminuje to ryzyko wykorzystania skradzionej karty do nielegalnych celów. Wydanie kart inteligentnych wszystkim pracownikom może być przedsięwzięciem kosztownym. Zaleca się jednak, by przynajmniej administratorzy urzędów certyfikacji dysponowali kartami inteligentnymi do zarządzania serwerami CA. Karty inteligentne pozwalają też wdrożyć w przedsiębiorstwie implementację jednokrotnego logowania (*single sign-on*), ponieważ użytkownik przenosi własny certyfikat na karcie z jednego miejsca i komputera do drugiego.

- Należy też wziąć pod uwagę fizyczny dostęp do CA i CSP. Powinny być one przechowywane w bezpiecznym środowisku i dostępne tylko dla małego zespołu administratorów. Zdecydowanie zaleca się prowadzenie inspekcji

tych serwerów, co pozwoli wyśledzić wszelkich napastników lub próby nadużycia przez złośliwych pracowników. Zaleca się też regularnie wykonywać kopie zapasowe tych informacji.

Projektowanie dystrybucji certyfikatów

Zapoznaliśmy się już ze szczegółami implementacji PKI, więc pora zastosować teorię w praktyce. Pokażemy, jak zaimplementować rozwiązanie PKI od podstaw. Pierwszym krokiem będzie zainstalowanie w systemie Windows Server 2003 serwera certyfikatów, który domyślnie nie jest instalowany.

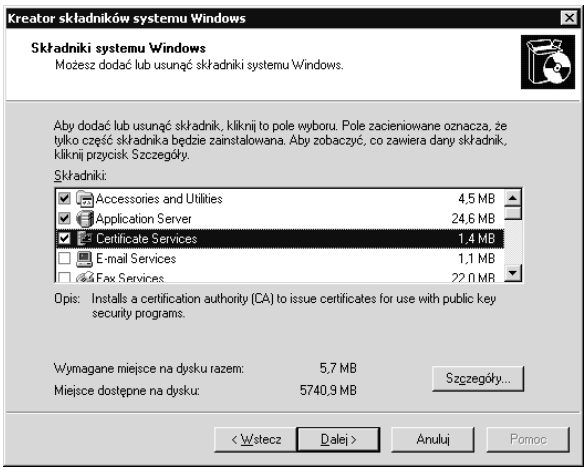
Nie należy instalować CA w systemie plików FAT. System FAT nie wspiera zabezpieczeń domenowych. Zalecanym rozwiązaniem jest instalacja CA w systemie NTFS. System plików NTFS pozwala na bezproblemową interakcję z Active Directory i współużytkowanie danych kont użytkowników.

Konfiguracja i implementacja

Instalowanie CA w systemie Windows Server 2003

1. Przejdź do *Start/Panel sterowania/Dodaj lub usuń programy*.
2. W lewym panelu kliknij *Dodaj/usuń składniki systemu Windows*.
3. Otworzy się okno kreatora składników systemu Windows. Z dostępnych opcji wybierz *Certificate Services*. Okno powinno wyglądać jak na rysunku 3.7.

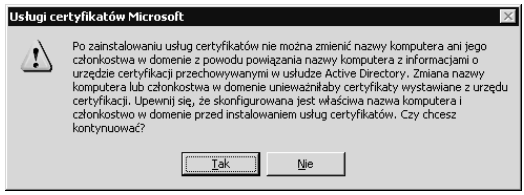
Rysunek 3.7. *Wybór usług certyfikatów do zainstalowania*



Natychmiast po kliknięciu pola wyboru *Certificate Services* pojawi się okienko komunikatu, ostrzegające użytkownika o konsekwencjach zmiany nazwy komputera lub domeny, do której należy serwer. Po zmianie nazwy komputera certyfikaty staną się nieważne (ponieważ certyfikaty generowane w tym serwerze będą powiązane z danymi serwera — jego nazwą). W razie zmiany nazwy komputera

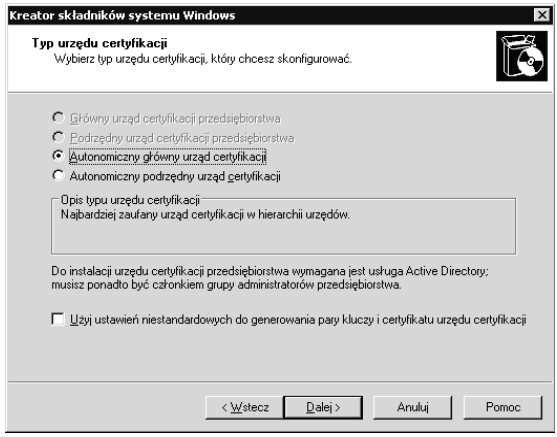
lub przynależności do domeny usługa Active Directory również utraci dostęp do informacji CA. Ostrzeżenie wygląda podobnie jak na rysunku 3.8. Kliknij *Tak*, by przejść do następnego okna.

Rysunek 3.8. *Ostrzeżenie przed zainstalowaniem usług certyfikatów*



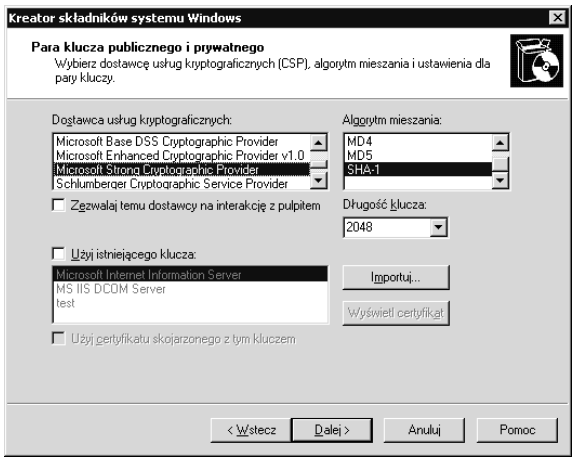
4. Następne okno pozwoli wybrać typ CA. Opcji jest kilka: główny CA przedsiębiorstwa, podrzędny CA przedsiębiorstwa, autonomiczny główny CA i autonomiczny podrzędny CA. Serwer w tym kroku sprawdza też, czy w sieci obecna jest usługa Active Directory. CA przedsiębiorstwa, główny lub podrzędny, można zainstalować tylko wtedy, gdy Active Directory jest dostępna. W przeciwnym razie można zainstalować tylko autonomiczny CA, a opcje CA przedsiębiorstwa będą w oknie niedostępne. Taki scenariusz ilustruje rysunek 3.9. Na potrzeby przykładu utworzymy główny CA. Wybierz *Autonomiczny główny urząd certyfikacji* i kliknij *Dalej*.

Rysunek 3.9. *Wybór typu CA*



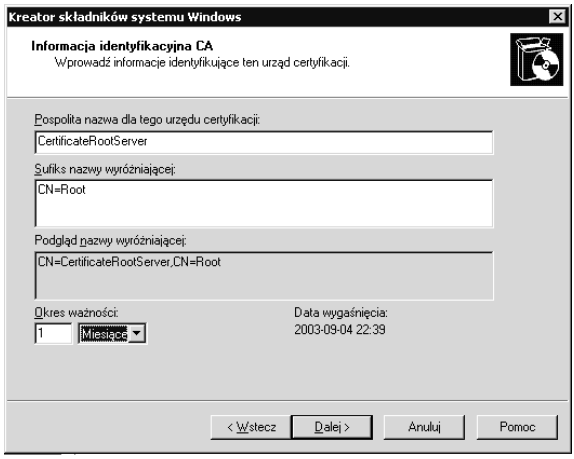
5. W przypadku zaznaczenia w poprzednim oknie opcji *Użyj ustawień niestandardowych do generowania pary kluczy i certyfikatu urzędu certyfikacji* następne okno pozwoli wybrać parę kluczy, publiczny i prywatny. Rysunek 3.10 przedstawia dostępne opcje. Z listy CSP można wybrać dostawcę usług kryptograficznych i skojarzyć z nim funkcję skrótu. System Windows Server 2003 udostępnia kilka CSP: MS Base DSS Cryptographic Provider, MS Enhanced Cryptographic Provider i MS Strong Cryptographic Provider (domyślny). W systemie dostępnych jest kilka wbudowanych funkcji skrótu: MD2, MD3, MD5 i SHA-1 (domyślny), które są zaawansowanymi algorytmami mieszającymi, używanymi do szyfrowania danych. Możemy też wybrać długość klucza: 512, 1024, 2048 lub 4096 bitów, domyślnie 2048. Im dłuższy klucz, tym bezpieczniejsze transakcje, jednak wydajność serwera może się pogorszyć z uwagi na większą złożoność obliczeń. Można też zaimportować parę kluczy, klikając przycisk *Importuj*, albo użyć istniejącej pary (przez wybór opcji *Użyj istniejącego klucza*). Na potrzeby demonstracji pozostawiliśmy wartości domyślne. Kliknij *Dalej*, by przejść do następnego okna.

Rysunek 3.10. *Wybór pary kluczy prywatnego i publicznego*



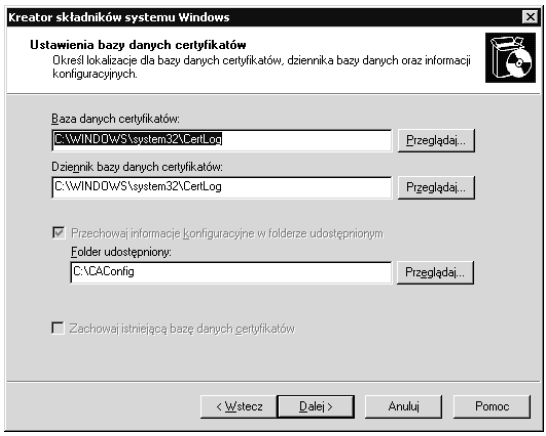
6. Następne okno, jak na rysunku 3.11, pozwala skonfigurować nazwy CA w przedsiębiorstwie. *Pospolita nazwa dla tego urzędu certyfikacji* jest tożsamością CA w sieci. Jako nazwę podamy *CertificateRootServer*. Nazwa ta powinna mieć nie więcej niż 64 znaki. To ograniczenie nakłada protokół LDAP używany przez Active Directory — nazwy o długości przekraczającej 64 znaki są skracane. Musimy też podać sufiks nazwy wyróżniającej. To również jest wymóg LDAP przy tworzeniu nowych obiektów Active Directory. Ten wpis będzie odróżniać obiekt głównego CA od reszty obiektów Active Directory. Na koniec wybierzemy czas ważności certyfikatu. Na potrzeby przykładu wybraliśmy dla certyfikatów generowanych przez ten główny CA czas ważności wynoszący 1 miesiąc (domyślnym standardem branżowym jest jeden rok, a domyślną wartością w Windows 2003 5 lat). Kliknij *Dalej*, by przejść do kolejnego ekranu.

Rysunek 3.11. *Dane tożsamości CA*



7. Kolejny ekran pozwala skonfigurować położenie baz danych i dzienników certyfikatów. Certyfikaty są przechowywane lokalnie w serwerze CA, domyślnie w katalogu *%systemroot%\system32\certlog*. Zaleca się przechowywanie certyfikatów na osobnym dysku fizycznym, co powinno poprawić wydajność serwera. Okno powinno wyglądać jak na rysunku 3.12. Kliknij *Dalej*, by przejść do następnego ekranu.

Rysunek 3.12. *Konfiguracja ustawień bazy danych*



Active Directory nie służy jako baza danych dla serwera autonomicznego CA. Proces instalacji automatycznie wprowadzi informacje CA do Active Directory, jeśli ta usługa jest obecna w sieci. Certyfikaty są przechowywane lokalnie w serwerze CA, a w Active Directory zostają zapisane informacje o ich położeniu. W implementacji CA przedsiębiorstwa certyfikaty są przechowywane w kontenerach obiektów użytkowników.

8. Następny krok zainstaluje CA w serwerze. Pojawi się też okno żądające zatrzymania serwera IIS, jeśli jest uruchomiony. Na koniec pojawi się ekran informujący o końcu procesu instalacji.

Rady niezależnego specjalisty

Obsługa rejestrowania w sieci Web usług certyfikatów

Podczas instalacji CA w systemie Windows Server 2003 urzędu certyfikacji udostępniany jest fronton WWW oparty na technologii ASP, który pozwala zgłaszać żądania i zarządzać certyfikatami. Jest on instalowany domyślnie i nazywany *Obsługa rejestrowania w sieci Web usług certyfikatów* (*Certificate Services Web Enrollment Support*). Można go odinstalować lub zainstalować ponownie, wybierając *Start/Panel sterowania/Dodaj lub usuń programy/Dodaj/usuń składniki systemu Windows*. Należy wybrać *Usługi certyfikatów* i kliknąć przycisk *Szczegóły*. W dostępnych opcjach można zaznaczyć *Obsługa rejestrowania w sieci Web usług certyfikatów* lub usunąć zaznaczenie, by odpowiednio zainstalować lub odinstalować tę usługę. Może ona służyć jako alternatywa dla konsoli MMC CA. Niektóre opcje nie są jednak dostępne w narzędziu *Obsługa rejestrowania w sieci Web usług certyfikatów* (na przykład, nie można w tym interfejsie WWW włączyć inspekcji CA). Interfejs ten pomoże administratorom CA w bezpieczniejszym zarządzaniu certyfikatami z różnych komputerów (aby połączyć się z CA, nie trzeba instalować konsoli MMC CA w innych komputerach).

Obsługa rejestrowania w sieci Web usług certyfikatów udostępnia administratorom CA szereg usług: na przykład, mogą za pomocą tego narzędzia zgłosić żądanie certyfikatu. Administratorzy CA mogą też poprzez te strony WWW sprawdzać status oczekujących certyfikatów i pobierać certyfikaty i CRL. Narzędzie dodaje do serwisu IIS komputera wirtualny katalog *certsrv*, do którego lokalna ścieżka to *http://*`<nazwa_serwera>`*/certsrv/*. Obsługa rejestrowania w sieci Web usług certyfikatów jest powszechnie stosowana do wydawania certyfikatów dla aplikacji WWW, pozwalających uwierzytelniać użytkowników.

Przyjrzyjmy się kilku zadaniom administracyjnym związanym z serwerem CA Windows Server 2003. Omówimy żądanie, odnawianie i odwoływanie certyfikatów oraz konfigurację inspekcji serwerów CA. Posłużymy się narzędziem Obsługa rejestrowania w sieci Web usług certyfikatów do zażądania certyfikatu, a za pomocą MMC CA przejdziemy cały cykl życia certyfikatu.

Projektowanie zgłaszania żądań i dystrybucji

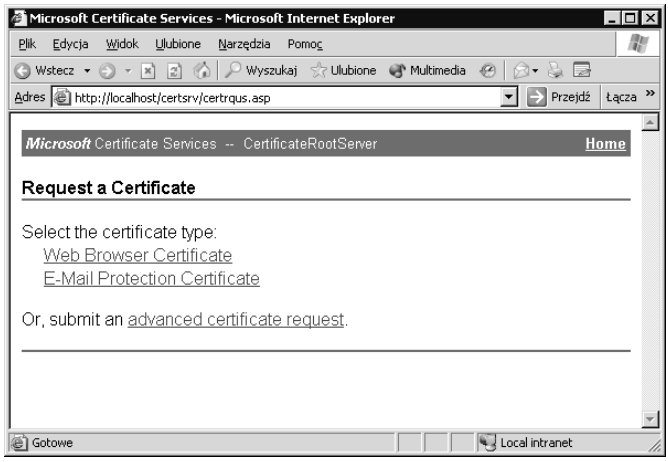
Pierwszym krokiem będzie żądanie certyfikatu w CA. Możemy do tego celu użyć narzędzia *Obsługa rejestrowania w sieci Web usług certyfikatów*. Jego interfejs wygeneruje certyfikat i doda go do kolejki oczekujących żądań w CA. Administrator CA musi otworzyć konsolę MMC i zaakceptować żądanie.

Konfiguracja i implementacja

Żądanie certyfikatu poprzez interfejs Obsługa rejestrowania w sieci Web usług certyfikatów

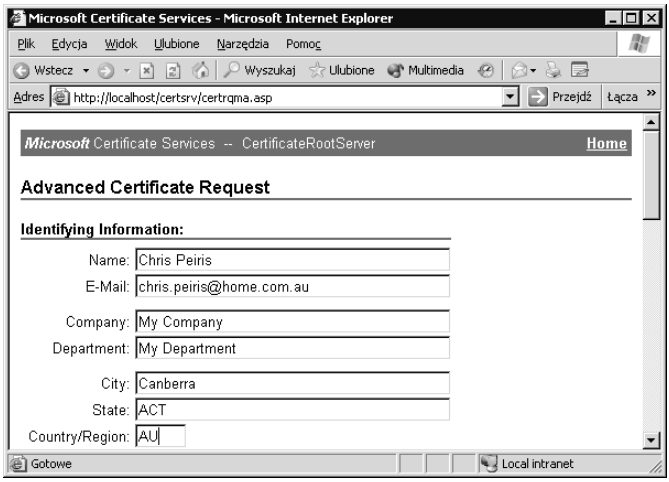
1. Otwórz okno programu Internet Explorer i wpisz adres `http://<nazwa_serwera>/certsrv/` (lub `http://localhost/certsrv/`, gdy CA znajduje się w lokalnym komputerze).
2. Kliknij łącze *Żądanie certyfikatu*. Pojawi się okno podobne do tego z rysunku 3.13. Próbujemy utworzyć certyfikat dla przeglądarek WWW, więc kliknij łącze *Certyfikat przeglądarki sieci Web*. Można też wygenerować certyfikat do uwierzytelniania wiadomości e-mail przez kliknięcie łącza *Certyfikat ochrony poczty e-mail*. Zaawansowane żądanie certyfikatu (*advanced certificate request*) udostępnia więcej opcji tworzenia zaawansowanych certyfikatów, na przykład przez wybór innego algorytmu skrótu lub długości kluczy niż w domyślnych ustawieniach serwera CA.

Rysunek 3.13. *Wybór typu certyfikatu*



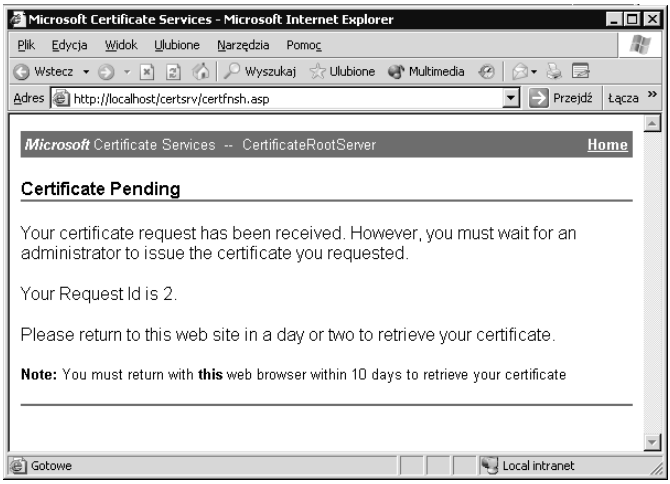
3. Rysunek 3.14 ilustruje kolejny ekran. Wpisz odpowiednie dane użytkownika. Można tu też zmienić domyślny CSP przez kliknięcie łącza *Więcej opcji*.

Rysunek 3.14. *Informacje o użytkowniku do wydania certyfikatu*



4. Kliknij *Prześlij*, by wysłać żądanie do serwera CA. Czynność ta wstawi certyfikat do kolejki żądań oczekujących w CA. Administrator CA może zaaprobować lub odmówić wydania certyfikatu, w zależności od zasad obowiązujących w organizacji. Ekran potwierdzenia wygląda jak na rysunku 3.15. Należy zapamiętać identyfikator żądania (*Request ID*) — może być potrzebny podczas akceptacji w kolejce. Identyfikator ten jest automatycznie generowany przez serwer CA, więc najprawdopodobniej będzie miał inną wartość niż w naszym przykładzie.

Rysunek 3.15. *Ekran potwierdzenia żądania certyfikatu*



Każdy użytkownik w przedsiębiorstwie może zalogować się do tego publicznego serwisu WWW i zgłosić za jego pomocą żądanie certyfikatu.

Aprobowanie certyfikatów przez administratora CA

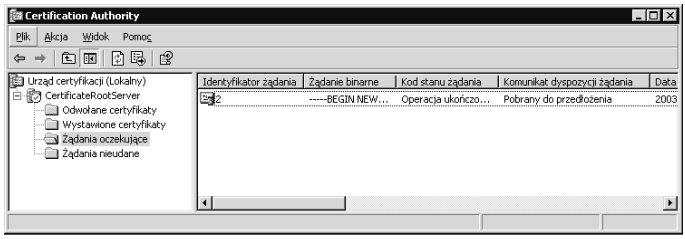
Zobaczmy, jak wygląda rola administratora w wystawianiu i odwoływaniu certyfikatów. Aby wykonać opisane poniżej żądania, musimy zmienić rolę z użytkownika na administratora CA.

Konfiguracja i implementacja

Wystawianie i odmawianie certyfikatów z kolejki żądań oczekujących

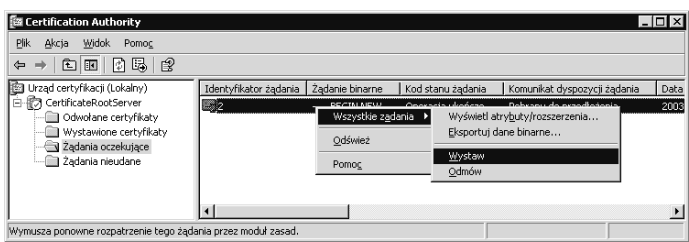
1. Przejdź do *Start/Programy/Narzędzia administracyjne/Urząd certyfikacji*.
2. Otworzy się konsola zarządzania urzędem certyfikacji. Przejdź do *Urząd certyfikacji/<nazwa serwera>/Żądania oczekujące*. W naszym przykładzie jest to *Urząd certyfikacji (Lokalny)/CertificateRootServer/Żądania oczekujące*. Ekran powinien wyglądać podobnie jak na rysunku 3.16.

Rysunek 3.16. *Żądania oczekujące w CA*



3. Kliknij prawym przyciskiem myszy odpowiedni certyfikat. Będzie to w naszym przykładzie certyfikat o identyfikatorze 2 (zobacz poprzednia ramka). Otworzy się menu kontekstowe. Wybierz *Wszystkie zadania/Wystaw*. Kliknięcie opcji *Odmów* pozwala odmówić wydania certyfikatu. Ekran będzie wyglądać podobnie jak na rysunku 3.17. Certyfikat zostanie usunięty z folderu *Żądania oczekujące* i przeniesiony do *Wystawione certyfikaty*.

Rysunek 3.17. *Zaaprobowanie certyfikatu z kolejki żądań oczekujących*



4. Przejdź do folderu *Wystawione certyfikaty*. Powinien pojawić się w nim wydany właśnie certyfikat (o identyfikatorze żądania 2). Dwukrotne kliknięcie certyfikatu pozwoli go wyświetlić.

Odwoływanie certyfikatów przez administratora CA

Administrator CA może odwołać certyfikat, zanim jeszcze upłynie jego ważność. Do tego również służy przystawka MMC Urząd certyfikacji. Poniższa ramka opisuje procedurę odwołania certyfikatu.

Konfiguracja i implementacja

Odwołanie certyfikatu

1. Przejdź do *Start/Programy/Narzędzia administracyjne/Urząd certyfikacji*.
2. Otworzy się konsola zarządzania urzędem certyfikacji. Przejdź do *Urząd certyfikacji/<nazwa serwera>*. W naszym przykładzie jest to *Urząd certyfikacji (Lokalny)/CertificateRootServer*.
3. Przejdź do folderu *Wystawione certyfikaty* i kliknij prawym przyciskiem myszy certyfikat, który chcesz odwołać.
4. Wybierz *Wszystkie zadania/Odwołaj certyfikat*. Certyfikat zostanie przeniesiony z folderu *Wystawione certyfikaty* do folderu *Odwołane certyfikaty*.

Konfiguracja odnawiania i inspekcji

Pary kluczy, prywatnych i publicznych, przedsiębiorstwa muszą być chronione. Ich ujawnienie poważnie naraziłoby bezpieczeństwo całego przedsiębiorstwa. Napastnicy mogliby wyrządzać szkody w zasobach, zyskując nieupoważniony dostęp do nich. Niezadowolony pracownik mógłby zadziałać jak intruz i sabotować systemy informatyczne. Intruz taki mógłby zalogować się do serwera CA i wydawać fałszywe certyfikaty nieupoważnionym użytkownikom. Co może zrobić administrator CA, by uniknąć takiego scenariusza?

Zaleca się włączyć inspekcje działań serwera CA. Pozwolą one sprawdzić, czy ktoś próbuje się do niego włamać. Inspekcje są nową funkcją systemu Windows Server 2003. Możemy je włączyć dla wielu czynności związanych z wydawaniem certyfikatów.

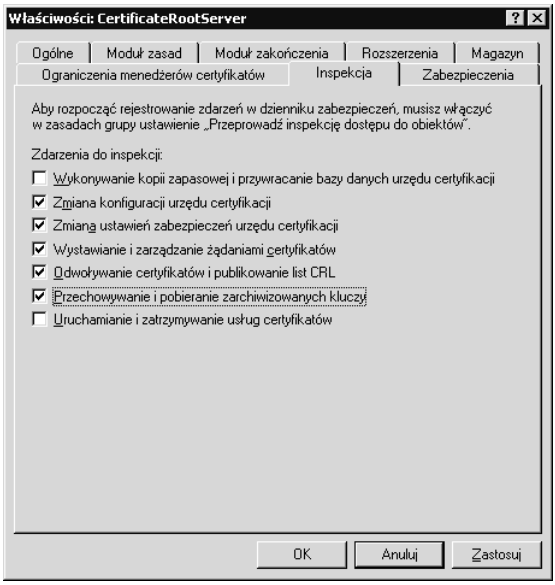
Włączenie inspekcji w systemie Windows Server 2003 jest łatwe. Zobaczmy, jak można to zrobić. Inspekcje pozwolą nam monitorować działania w serwerze, by identyfikować potencjalne problemy.

Konfiguracja i implementacja

Włączenie inspekcji serwera CA

1. Przejdź do *Start/Programy/Narzędzia administracyjne/Urząd certyfikacji*.
2. Otworzy się konsola zarządzania urzędem certyfikacji. Przejdź do *Urząd certyfikacji/<nazwa serwera>*. W naszym przykładzie jest to *Urząd certyfikacji (Lokalny)/CertificateRootServer*.
3. Kliknij nazwę serwera prawym przyciskiem myszy i wybierz *Właściwości* z menu podręcznego. Pojawi się okno *Właściwości: CertificateRootServer*. Przejdź do zakładki *Inspekcja*. Okno powinno wyglądać podobnie do tego z rysunku 3.18. Może zajść potrzeba śledzenia działań CA — intruz zmienia konfigurację CA i wydaje fałszywe certyfikaty. Zaznaczymy więc opcje jak na poniższym rysunku.

Rysunek 3.18. *Inspekcje CA*



4. Kliknij *Zastosuj*, by wprowadzić nowe zasady inspekcji CA. Wynik inspekcji będzie dodawany do dziennika *Zabezpieczenia*, dostępnego w narzędziu *Podgląd zdarzeń*.
5. Teraz możemy monitorować dziennik zdarzeń *Zabezpieczenia* i wyśledzić intruza (każda zmiana konfiguracji i ustawień CA, itp. będzie w naszym przykładzie rejestrowana w dzienniku zabezpieczeń). Narzędzie *Podgląd zdarzeń* jest dostępne w menu *Start/Programy/Narzędzia administracyjne*.

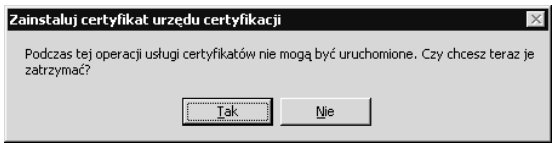
Po wyśledzeniu intruza możemy być zmuszeni do podjęcia dodatkowych kroków. Intruzowi udało się dostać do serwera CA i wydać certyfikaty. Oznacza to, że te pary kluczy publicznych i prywatnych przestały być wiarygodne. Z tego powodu musimy zmienić pary kluczy: publicznych i prywatnych, aby stare nie dawały już dostępu do systemu. Proces ten nosi nazwę odnawiania kluczy. Odnawianie kluczy jest również niezbędne po upłynięciu okresu ich ważności. Zobaczmy, jak odnowić klucze.

Konfiguracja i implementacja

Włączenie inspekcji serwera CA

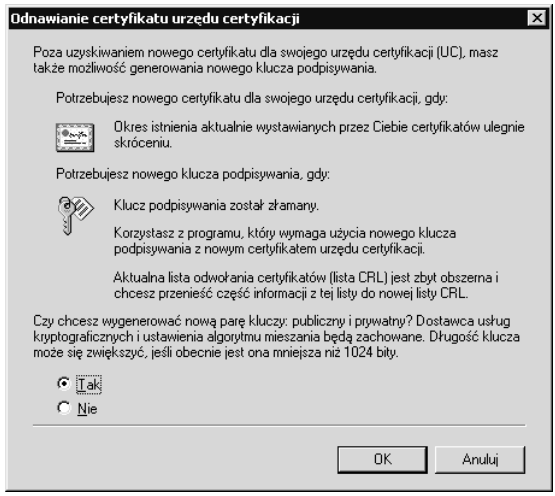
1. Przejdź do *Start/Programy/Narzędzia administracyjne/Urząd certyfikacji*.
2. Otworzy się konsola zarządzania urzędem certyfikacji. Przejdź do *Urząd certyfikacji/<nazwa serwera>*. W naszym przykładzie jest to *Urząd certyfikacji (Lokalny)/CertificateRootServer*.
3. Kliknij pozycję menu *Akcja* i wybierz *Wszystkie zadania/Odnów certyfikat urzędu certyfikacji*.
4. Pojawi się okno dialogowe z rysunku 3.19, z pytaniem, czy zatrzymać serwer certyfikatów. Kliknij *Tak*.

Rysunek 3.19. *Potwierdzenie zatrzymania usługi certyfikatów*



5. Nowy certyfikat można otrzymać, używając starej pary kluczy. Niestety, nie jest to w naszym przypadku bezpieczne, ponieważ klucze zostały narażone przez intruza. Musimy więc wygenerować zarówno certyfikat, jak i parę kluczy. Pojawi się okno z pytaniem o potwierdzenie zmiany kluczy, podobne jak na rysunku 3.20. Wybierz *Tak*, by wygenerować nową parę kluczy. Czynność ta utworzy nową parę kluczy i uruchomi ponownie serwer certyfikatów. Taki scenariusz może być dla firmy kosztownym przedsięwzięciem. Łatwo jest wygenerować nową parę kluczy w serwerze, lecz rozprowadzenie kluczy prywatnych do wszystkich pracowników i partnerów biznesu wymaga pieniędzy i czasu. Należy więc jak najlepiej chronić dane certyfikatu CA.

Rysunek 3.20. *Potwierdzenie wygenerowania nowych kluczy*



Wszystkie opisane funkcje konsoli MMC można wykonać za pomocą narzędzia wiersza poleceń *certutil.exe*. Było ono już obecne w systemie Windows 2000, lecz w systemie Windows Server 2003 są w nim dostępne nowe opcje, głównie do interakcji z Active Directory. W serwerze CA systemu Windows Server 2003 certyfikaty i listy CRL można publikować bezpośrednio w Active Directory. Służy do tego polecenie o składni:

```
certutil -dspublish [cert|crl]
```

Podsumowanie

Niniejszy rozdział poświęcony był infrastrukturze klucza publicznego (PKI) w systemie Windows Server 2003. Zaczęliśmy od omówienia podstaw implementacji PKI. Infrastruktura klucza publicznego jest mechanizmem kryptografii asymetrycznej, służącym do zabezpieczania informacji. W PKI istnieją pary kluczy — publiczny i prywatny. Nadawca podpisuje dokumenty swoim kluczem prywatnym i wysyła do odbiorcy. Proces podpisywania wiadomości składa się z dwóch kroków. Pierwszym jest zastosowanie do wiadomości funkcji skrótu. Uzyskany skrót (*digest message*) jest szyfrowany kluczem prywatnym nadawcy i dołączany do wiadomości jako podpis. Odbiorca uwierzytelnia klucz nadawcy za pomocą zewnętrznego urzędu certyfikacji (np. VeriSign).

W systemie Windows Server 2003 istnieją dwa typy urzędów certyfikacji: CA przedsiębiorstwa oraz autonomiczne. CA przedsiębiorstwa do wydawania certyfikatów używa informacji z Active Directory. Autonomiczny CA nie komunikuje się z Active Directory. W przedsiębiorstwach zaleca się stosowanie trzypoziomowego modelu CA. Pierwszym poziomem jest pojedynczy główny urząd certyfikacji, który zarządza wszystkimi pozostałymi w sieci przedsiębiorstwa, bezpośrednio zarządzając drugim poziomem. Drugi poziom zawiera tzw. *pośrednie* CA, których liczba może być różna w zależności od organizacji. Pośrednie CA wydają instrukcje urzędom certyfikacji wydającym certyfikaty. Te CA, na najniższym poziomie, wydają certyfikaty dla klientów.

Główny i pośrednie CA powinny być odłączone od sieci. CA wydające certyfikaty powinny być dostępne w sieci, by wykonywać swoje zadanie. Takie rozwiązanie jest ważnym środkiem bezpieczeństwa, chroniącym strukturę CA. Organizacja powinna w określonych oknach czasowych podłączać główny i pośrednie CA do sieci w celu aktualizacji (należy aktualizować CRL, aby odzwierciedlały nowe środki bezpieczeństwa).

Trzypoziomowy model CA może być zorganizowany na szereg sposobów, na przykład, odzwierciedlając strukturę geograficzną międzynarodowej organizacji lub wewnętrzną strukturę firmy. W pewnych przypadkach potrzebne są CA niezależne od wyższego poziomu (nie pod kontrolą głównego CA). Na potrzeby takich scenariuszy dostępna jest struktura sieciowa CA.

Istnieje kilka zagrożeń dla serwerów CA. Należy szczególnie chronić główny urząd certyfikacji. Włamanie do niego naraziłaby całość zabezpieczeń przedsiębiorstwa. Należy podjąć odpowiednie kroki, by poprawić fizyczne bezpieczeństwo tego serwera i używać do uwierzytelniania kart inteligentnych. Karty te poprawiają bezpieczeństwo dzięki stosowaniu numeru PIN oprócz klucza prywatnego. Bezpieczeństwo można też zwiększyć, stosując sprzętowy CSP.

Na koniec przyjrzeliśmy się konfiguracji serwerów CA w systemie Windows Server 2003. W tym systemie operacyjnym dostępny jest system rejestrowania żądań certyfikatów przez WWW oraz automatyczne zgłaszanie żądań i automatyczne odnawianie certyfikatów. Poza tym Windows Server 2003 obsługuje przyrostowe listy CRL. Do zarządzania serwerem CA może służyć przystawka MMC lub narzędzie wiersza poleceń *certutil.exe*.

Rozwiązania w skrócie

Projektowanie infrastruktury klucza publicznego używającej CA

- Pierwszym krokiem w implementacji PKI jest zaprojektowanie głównego urzędu certyfikacji. Główny CA zawiera certyfikat podpisany przez siebie, dlatego jego bezpieczeństwo jest nie do przecenienia. W środowisku Windows Server 2003 może działać tylko jeden główny CA.
- Główny CA powinien komunikować się z przynajmniej dwoma pośrednimi CA (jednym dla certyfikatów wewnętrznych, i jednym do zewnętrznych). Pośrednie CA powinny kontrolować CA wydające certyfikaty dla użytkowników.
- W systemie Windows Server 2003 istnieją dwa typy CA. CA przedsiębiorstwa komunikuje się z Active Directory i wydaje automatycznie certyfikaty. Informacje do certyfikatów mogą być pobierane z danych konta Windows i z Active Directory.
- Autonomiczne CA nie komunikują się z Active Directory i wydają certyfikaty tylko za zgodą administratora CA. Można je konfigurować tak, by wydawały certyfikaty automatycznie, lecz nie jest to zalecane.
- Firma może zaprojektować strukturę CA zgodną z rozmieszczeniem geograficznym lub strukturą organizacyjną. Oba rozwiązania opierają się na trzypoziomowym modelu CA. Można też zastosować sieciowy model zaufania, w którym certyfikaty wzajemne pozwalają na dostęp do niezależnych CA w niezależnych działach informatyki.
- Główny i pośrednie CA nie powinny być stale dostępne w sieci. Można w tym celu wyłączyć komputer lub usługę CA, albo skonfigurować system Windows Server 2003 jako serwer autonomiczny, odłączony od domeny.
- W celu zwiększenia bezpieczeństwa CA w przedsiębiorstwie można posłużyć się też sprzętowymi CSP i kartami inteligentnymi. Karta inteligentna będzie zawierać klucz użytkownika i będzie wymagała wprowadzenia numeru PIN, by potwierdzić tożsamość właściciela.

Projektowanie logicznej strategii uwierzytelniania

- Usługi certyfikatów w systemie Windows Server 2003 należy instalować w systemie plików NTFS, a nie w systemie FAT. Pozwoli to używać danych uwierzytelniania Windows i ułatwi dostęp do Active Directory.
- W systemie Windows Server 2003 dostępne jest narzędzie *Obsługa rejestrowania w sieci Web usług certyfikatów*, które pozwala wydawać certyfikaty dla stron aplikacji WWW i zarządzać nimi.
- Do wydawania, odmawiania i odwoływania certyfikatów można użyć przystawki MMC lub narzędzia wiersza poleceń *certutil.exe*.

- Każdy użytkownik może zażądać certyfikatu poprzez narzędzie *Obsługa rejestrowania w sieci Web usług certyfikatów*. Żądanie będzie oczekiwać w kolejce, dopóki nie zaaprobuje go administrator CA, który do wydawania i odmawiania certyfikatów używa konsoli MMC. W zależności od decyzji, certyfikat zostaje przeniesiony do folderu *Wystawione certyfikaty* lub *Odwołane certyfikaty*.
- Zaleca się włączyć inspekcje serwera CA, co umożliwi monitorowanie aktywności w serwerze. Wyniki inspekcji można przeglądać w dzienniku zdarzeń *Zabezpieczenia*.
- W razie wykrycia nieupoważnionych działań może zajść potrzeba odwołania certyfikatów i odnowienia pary kluczy. Takie nieupoważnione działania można monitorować za pomocą wyników inspekcji.
- Windows Server 2003 obsługuje również nowe funkcje automatycznego żądania i odnawiania certyfikatów.

Pytania i odpowiedzi

Poniższe pytania, na które odpowiadają autorzy niniejszej książki, mają w założeniach zarówno pomóc Czytelnikowi w zrozumieniu pojęć przedstawionych w rozdziale, jak i wspomóc praktyczną implementację tych pojęć. Aby znaleźć więcej pytań i odpowiedzi, należy otworzyć stronę *www.syngress.com/solutions* (wymagane jest założenie konta użytkownika do logowania w serwisie www.syngress.com).

P: Ile głównych urzędów certyfikacji może mieć przedsiębiorstwo?

O: W przedsiębiorstwie może być tylko jeden główny CA, który będzie zarządzać innymi urzędami certyfikacji.

P: Czy główny CA może wydawać certyfikaty?

O: Tak, lecz nie jest to zalecane. Główny CA powinien być chroniony za pomocą pośrednich CA i odłączony od sieci.

P: Czy możemy mieć więcej niż dwa pośrednie CA?

O: Tak. Dobrą praktyką jest użycie wewnętrznego i zewnętrznego pośredniego CA (wymóg minimalny). W architekturze PKI możemy jednak przydzielić więcej CA na inne cele. Załóżmy, że firma prowadzi 60% interesów z jednym, dużym klientem — możemy specjalnie dla niego zastosować osobny CA.

P: Czy architektura PKI może istnieć bez głównego urzędu certyfikacji?

O: Tak. Model hierarchii sieciowej nie zawiera głównego CA. Jednakże globalna usługa katalogowa (np. Active Directory) musi zawierać odpowiednie informacje, by znaleźć inne „równorzędne” CA przedsiębiorstwa.

P: Czy można stosować szablon certyfikatów w autonomicznym CA?

O: Tak. Szablony certyfikatów są dostępne zarówno w CA przedsiębiorstwa, jak i autonomicznych.

P: Czy usługa Active Directory jest niezbędna w organizacji do tworzenia szablonów certyfikatów?

O: Tak. Szablony certyfikatów będą niedostępne, jeśli usługa Active Directory nie będzie obecna.