Ćwiczenie 9 Implementacja infrastruktury klucza publicznego

Celem ćwiczenia jest zapoznanie studentów z wybranymi funkcjami realizowanymi przez urzędy certyfikacyjne w ramach infrastruktury klucza publicznego. Ćwiczenie jest realizowane w zespołach, w których jeden komputer pełni funkcje urzędu głównego a jeden lub dwa pozostałe pełnia funkcje urzędu podrzędnego. Na obu komputerach należy zainstalować serwer WWW, który umożliwi klientom komunikację z urzędem certyfikacyjnym. Na komputerze, na którym zainstalowano urząd główny należy zrealizować zadania A, D, F÷K. Na komputerze, na którym zainstalowano urząd podrzędny należy zrealizować zadania B, C, E÷K. Zadania A÷E dotyczą instalowania i podstawowych czynności konfiguracyjnych urzędów certyfikacyjnych. W zadaniach F÷K, przy pomocy przeglądarki Internet Explorer realizuje się wybrane działania klientów, których obsługuje urząd certyfikacyjny. Należy zwrócić uwagę, że w czasie realizacji ćwiczenia klient i serwer (urząd certyfikacyjny) osadzone są na tym samym komputerze. W rzeczywistości najczęściej klient i serwer funkcjonują na różnych komputerach.

W ramach przygotowania do ćwiczenia należy zapoznać się z udostępnionymi materiałami wykładowymi (prezentacja BSI-04). W zależności od wersji używanego systemu operacyjnego, format formularzy umożliwiających klientowi komunikowanie się z urzędem certyfikacyjnym może się nieco różnić od tych, które są opisane w scenariuszu ćwiczenia. W takim przypadku studenci powinni samodzielnie wybierać i właściwie wypełniać pola takich formularzy.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań. *Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.*

PRZED PRZYSTĄPIENIEM DO ĆWICZENIA ZSYNCHRONIZOWAĆ ZEGARY OBU KOMPUTERÓW PARTNERSKICH. WYKORZYSTAĆ POLECENIE NET TIME.

Poniższe 4 punkty zrealizować tylko w przypadku jeżeli w systemie nie jest zainstalowany IIS.

1. Otworzyć panel sterowania, i uruchomić program ***Dodaj lub usuń programy*** (*Add/Remove Programs*) , a w jego oknie przycisk ***Dodaj/Usuń składniki systemu Windows*** (*Add/Remove Windows Components*).
2. W oknie kreatora wybrać pozycję ***Serwer aplikacji*** (*Application Server*) i nacisnąć przycisk ***Szczegóły*** *(Details).*
3. Zaznaczyć pozycję ***Internetowe usługi informacyjne*** (IIS) i nacisnąć przycisk ***Szczegóły*** *(Details).*
4. Zaznaczyć opcję ***Usługa World Wide Web*** i kolejno zatwierdzać dokonane wybory.

A. Tworzenie wydzielonego, korzeniowego CA (*Stand-Alone Root CA*)

TO ĆWICZENIE NALEŻY WYKONAĆ NA JEDNYM KOMPUTERZE W PARZE. NALEŻY WYBRAĆ KOMPUTER O WYŻSZYM NUMERZE.

1. Zalogować się jako administrator.
2. Uruchomić program MMC i w utworzonej konsoli, umieścić przystawkę (*Snap in*) ***Certyfikaty*** (*Certificates*). W czasie pracy kreatora, w oknie ***Przystawka certyfikatów*** (*Certificates snap-in*), zaznaczyć opcję ***Konto komputera*** (*Computer account*). Zapisać plik konsoli na pulpicie pod nazwą CERTYFIKATY_KOMPUTERA.MSC.
3. W oknie konsoli CERTYFIKATY_KOMPUTERA rozwinąć kontener ***Osobisty*** (*Personal*). Czy są w nim widoczne jakieś certyfikaty?

4. Otworzyć panel sterowania, i uruchomić program ***Dodaj lub usuń programy*** (*Add/Remove Programs*) , a w jego oknie przycisk ***Dodaj/Usuń składniki systemu Windows*** (*Add/Remove Windows Components*).

5. W oknie kreatora zaznaczyć opcję ***Usługi Certyfikatów*** (*Certificate Services*).
6. Na stronie ***Typ urzędu certyfikacji*** (*Certification Authority Type*), kreatora wybrać opcję ***Autonomiczny główny urząd certyfikacji*** (*Stand-alone root CA*).
7. Na stronie ***Informacja identyfikacyjna CA*** (*CA Identifying Information*) kreatora, w polu nazwy urzędu wpisać nazwę swojego komputera. Pozostałe pola zostawić bez zmian.
8. Pozostałe strony kreatora pozostawić bez zmian.
9. Po zakończeniu instalacji sprawdzić zawartość kontenera ***Osobisty*** (*Personal*) w konsoli CERTYFIKATY_KOMPUTERA. Zapoznać się z zawartością wygenerowanego certyfikatu. Zwrócić uwagę na identyfikator wystawcy i identyfikator właściciela (żądającego wystawienia) certyfikatu.
10. Sprawdzić zawartość kontenera ***Zaufane główne urzędy certyfikacji*** (*Trusted Root Certification Authorities*) w konsoli CERTYFIKATY_KOMPUTERA. Odszukać wygenerowany przed chwilą certyfikat. Zapoznać się z zawartością tego certyfikatu.
11. Otworzyć konsolę ***Urząd certyfikacji*** (*Certification Authority)*, z grupy narzędzi administracyjnych. Zapoznać się z zawartością tej konsoli. Jeżeli usługa nie jest włączona, to należy ją włączyć poprzez użycie stosownej funkcji w menu podręcznym pozycji swojego komputera.

B. Rejestrowanie dodatkowego zaufanego CA

TO ĆWICZENIE NALEŻY WYKONAĆ NA JEDNYM KOMPUTERZE W PARZE. NALEŻY WYBRAĆ KOMPUTER O NIŻSZYM NUMERZE.

1. Zalogować się jako administrator.
2. Uruchomić program MMC i w utworzonej konsoli umieścić przystawkę (*Snap in*) ***Certificates*** (*Certificates*). W czasie pracy kreatora, w oknie ***Przystawka certyfikatów*** (*Certificates snap-in*), zaznaczyć opcję ***Konto komputera*** (*Computer account*). Zapisać plik konsoli na pulpicie pod nazwą CERTYFIKATY_KOMPUTERA.MSC.
3. W oknie konsoli rozwinąć kontener ***Osobisty*** (*Personal*). Czy są w nim widoczne jakieś certyfikaty?
4. Wybrać przycisk ***Start*** a następnie ***Uruchom*** *(Run)*.
5. Wpisać: **http:*//serwer_partnera*certsrv** (gdzie *serwer_partnera* jest nazwą komputera partnera wykorzystanego w ćwiczeniu poprzednim).
6. Na stronie ***Zapraszamy*** *(Welcome)* wybrać opcję ***Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL*** (*Retrieve the CA certificate or certificate revocation list)*.
7. Na stronie ***Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL*** (*Retrieve the CA certificate or certificate revocation list)*, wybrać ***Zainstaluj jego łańcuch certyfikatów*** (*Install this CA certification path)*. Następnie zaakceptować proponowany certyfikat.
8. Gdy rozwinie się strona ***Instalacja certyfikatu urzędu certyfikacji*** (*CA Certificate Installed)*, zamknąć okno ***Internet Explorera***.
9. Po zakończeniu instalacji sprawdzić zawartość kontenera ***Zaufane główne urzędy certyfikacji*** (*Trusted Root Certification Authorities*) w konsoli CERTYFIKATY_KOMPUTERA. Odszukać certyfikat komputera partnera. Zapoznać się z zawartością tego certyfikatu. Porównać tą zawartość z zawartością certyfikatu wygenerowanego podczas realizacji zadania A. Jeżeli w tym kontenerze nie ma certyfikatu komputera partnera, to po upływie 30 minut należy ten punkt ćwiczenia powtórzyć i udokumentować.

C. Tworzenie wydzielonego, podrzędnego CA (*Stand-Alone Subordinate CA*)

TO ĆWICZENIE NALEŻY WYKONAĆ NA JEDNYM KOMPUTERZE W PARZE. NALEŻY WYBRAĆ KOMPUTER O NIŻSZYM NUMERZE, WYKORZYSTANY W POPRZEDNIM ĆWICZENIU.

1. Jeżeli nie jest zainstalowana usługa IIS, to zainstalować ją.
2. Otworzyć panel sterowania, następnie uruchomić program ***Dodaj lub usuń programy*** (*Add/Remove Programs*) , a w jego oknie przycisk ***Dodaj/Usuń składniki systemu Windows*** (*Add/Remove Windows Components*)..
3. W oknie kreatora zaznaczyć opcję ***Usługi Certyfikatów*** (*Certificate Services*).
4. Na stronie ***Typ urzędu certyfikacji*** (*Certification Authority Type*), kreatora wybrać opcję ***Autonomiczny podrzędny urząd certyfikacji*** *(Stand-alone subordinate CA)*.
5. Na stronie ***Informacja identyfikacyjna CA*** (*CA Identifying Information*) kreatora, w polu nazwy urzędu wpisać nazwę swojego komputera. Pozostałe pola wypełnić w identyczny sposób jak na komputerze partnera.
6. Na stronie ***Żądanie certyfikatu od urzędu certyfikcji*** *(CA Certificate Request****)***, w polu nazy komputera, wpisać nazwę komputera partnera i nacisnąć klawisz TAB.
7. Dokończyć instalację.

D. Emitowanie certyfikatu dla podrzędnego CA

1. Na komputerze pełniącym funkcję korzeniowego CA, otworzyć konsolę ***Urząd certyfikacji*** (*Certification Authority)*, z grupy narzędzi administracyjnych.
2. Rozwinąć pozycję swojego komputera i wybrać pozycję ***Żądania oczekujące*** (*Pending Requests)*.
3. W panelu szczegółów, w menu podręcznym pozycji zgłoszonego żądania wybrać pozycję ***Wszystkie zadania*** (*All Tasks)* a potem ***Wystaw*** (*Issue).*
4. W drzewie konsoli wybrać ***Wystawione certyfikaty*** (*Issued Certificates)* i sprawdzić czy certyfikat został wyemitowany. Zapoznać się z treścią wygenerowanego certyfikatu. Zwrócić uwagę na pole identyfikacji zamawiającego certyfikat.
5. Zminimalizować konsolę ***Urząd certyfikacji*** (*Certification Authority)*.

E. Instalowanie certyfikatu dla podrzędnego CA

1. Na komputerze pełniącym rolę podrzędnego CA, otworzyć konsolę ***Urząd certyfikacji*** (*Certification Authority)*, z grupy narzędzi administracyjnych. W drzewie konsoli w menu podręcznym pozycji swojego komputera wybrać pozycję ***Wszystkie zadania*** (*All Tasks),* a potem ***Zainstaluj certyfikat urzędu certyfikacji*** (*Install CA Certificate).*
2. W oknie dialogowym ***Wybierz plik, aby ukończyć instalację urzędu certyfikacji*** *(Select file to complete CA installation)* wybrać ***Anuluj*** (*Cancel).*
3. W oknie dialogowym ***Żądanie certyfikatu od urzędu certyfikacji*** (*CA Certificate Request),* w polu nazwy komputera powinna pojawić się nazwa komputera partnera.
4. W liście ***Nadrzędny urząd certyfikacji*** *(Parent CA)* wybrać pozycję komputera partnera i zatwierdzić dokonane wybory (przycisk OK).
5. Odświeżyć obraz konsoli CERTYFIKATY_KOMPUTERA. Sprawdzić zawartość kontenera ***Osobisty*** (*Personal)* w konsoli CERTYFIKATY_KOMPUTERA. Zapoznać się z zawartością wygenerowanego certyfikatu. Porównać zawartość z zawartością certyfikatu

wygenerowanego podczas realizacji zadania D. Zwrócić uwagę na identyfikator wystawcy i identyfikator właściciela (żądającego wystawienia) certyfikatu.

6. W konsoli ***Urząd certyfikacji*** (*Certification Authority)*, w menu podręcznym pozycji swojego komputera wybrać pozycję ***Uruchom usługę*** (*Start service*) – o ile usługa nie jest jeszcze włączona.
7. Zminimalizować konsolę ***Urząd certyfikacji*** (*Certification Authority)*.

KOLEJNE ĆWICZENIA NALEŻY WYKONAĆ NIEZALEŻNIE NA OBU KOMPUTERACH PARTNERSKICH

F. Żądanie certyfikatu IPSec dla komputera

1. Wybrać przycisk ***Start*** a następnie ***Uruchom*** (*Run*).
2. Wpisać: **http://***serwer***/certsrv** (gdzie *serwer* jest nazwą własnego komputera).
3. Na stronie ***Zapraszamy*** (*Welcome*) wybrać link ***Żądanie certyfikatu*** (*Request a certificate*).
4. Na stronie ***Żądaj certyfikatu*** (*Choose Request Type*) wybrać ***Zaawansowanie żądanie certyfikatu*** (*Advanced request*).
5. Na stronie ***Zaawansowanie żądanie certyfikatu*** (*Advanced Certificate Requests*) wybrać link ***Utwórz i prześlij żądanie do tego urzędu certyfikacji*** (*Submit a certificate request to this CA using a form*).
6. Na kolejnej stronie ***Zaawansowanie żądanie certyfikatu*** (*Advanced Certificate Requests*), w sekcji ***Informacje identyfikujące*** (*Identifying Information*) wpisać swoje dane personalne.
7. W sekcji ***Typ potrzebnego certyfikatu*** (*Intended Purpose*), wybrać ***Certyfikat zabezpieczeń IP (IPSec)*** (*IPSec Certificate*). Zapoznać się z innymi dostępnymi pozycjami.
8. W sekcji ***Opcje klucza*** (*Key Options*), wybrać ***Zachowaj certyfikat w magazynie certyfikatów komputera lokalnego*** (*Use local machine store*).
9. W sekcji ***Opcje dodatkowe***, w polu ***Przyjazna nazwa*** wpisać IPSEC. Pozostałe pola pozostawić bez zmian i nacisnąć przycisk ***Prześlij*** (*Submit*).
10. Po pojawieniu się strony ***Oczekiwanie na certyfikat*** (*Certificate Pending*)**,** zamknąć okno programu ***Internet Explorer***.
11. Sprawdzić zawartość kontenera ***Żądanie zarejestrowania certyfikatu*** w konsoli CERTYFIKATY_KOMPUTERA. Zapoznać się z zawartością wygenerowanego żądania. Zwrócić uwagę na pola identyfikatora wystawcy i podmiotu, wartości klucza publicznego, przyjaznej nazwy.

G. Emitowanie i instalowanie żądanego certyfikatu dla komputera

1. Przywrócić konsolę ***Urząd certyfikacji*** (*Certification Authority*).
2. W drzewie konsoli rozwinąć pozycję swojego serwera i wybrać pozycję ***Żądania oczekujące*** (*Pending Requests*).
3. Odświeżyć obraz wybierając w menu ***Akcja*** (*Action*) funkcję ***Odśwież*** (*Refresh*).
4. Korzystając z funkcji Dodaj/usuń kolumny w menu ***Widok*** (*View*), skonfigurować okno w ten sposób aby dla każdego certyfikatu wyświetlały się jedynie kolumny: ***identyfikator żądania, nazwa żądającego, kod stanu żądania, binarny klucz publiczny***.
5. W panelu szczegółów, w menu podręcznym pozycji zgłoszonego żądania wybrać pozycję ***Wszystkie zadania*** (*All Tasks*) a potem ***Wystaw*** (*Issue*).

6. W drzewie konsoli wybrać kontener ***Wystawione certyfikaty*** (*Issued Certificates*) i sprawdzić czy certyfikat został wyemitowany. Zapoznać się z jego treścią. Zwrócić uwagę na numer seryjny certyfikatu i klucz publiczny.
7. Zamknąć konsolę ***Urząd certyfikacji*** (*Certification Authority*).
8. Otworzyć okno programu ***Internet Explorer***.
9. W polu adresu wpisać **http:*//serwer/certsrv*** (gdzie *serwer* jest nazwą własnego komputera).
10. Na stronie ***Zapraszamy*** (*Welcome*) wybrać link ***Pokaż stan oczekującego żądania certyfikatu*** (*Check on a pending certificate*).
11. Na stronie ***Pokaż stan oczekującego żądania certyfikatu*** (*Check On A Pending Certificate Request*) sprawdzić, czy wysłane żądanie zostało obsłużone, tzn. czy żądany certyfikat został przygotowany.
12. Na stronie ***Certyfikat został wystawiony*** (*Certificate Issued*) wybrać ***Zainstaluj ten certyfikat*** (*Install this certificate*).
13. Po zakończeniu instalacji zamknąć okno programu ***Internet Explorer***.
14. Odświeżyć obraz konsoli CERTYFIKATY_KOMPUTERA. Sprawdzić zawartość kontenera ***Osobisty*** (*Personal*) w konsoli CERTYFIKATY_KOMPUTERA. Zapoznać się z zawartością nowego certyfikatu. Porównać z zawartością wygenerowanego uprzednio żądania oraz certyfikatu wygenerowanego podczas realizacji zadania F.

H. Żądanie, emitowanie i instalowanie dodatkowych certyfikatów dla komputera

1. W sposób opisany w zadaniu F wygenerować żądania wystawienia niżej wymienionych certyfikaty dla komputera:
   - ***Certyfikat ochrony poczty e-mail*** (*E-mail Protection Certificate*)
   - ***Certyfikat uwierzytelniania klienta*** (*Client Authentication Certificate*)
   - ***Certyfikat uwierzytelniania serwera*** (*Server Authentication Certificate*)

2. W sposób opisany w zadaniu G wyemitować certyfikaty, realizując żądania wygenerowane w punkcie 1. Następnie zainstalować te certyfikaty.

I. Unieważnianie certyfikatów i publikowanie CRL

1. W konsoli ***Urząd certyfikacji*** (*Certification Authority*).otworzyć kontener ***Wystawione certyfikaty*** (*Issued Certificates*).
2. Wybrać dowolny z certyfikatów wygenerowanych podczas realizacji zadania H.
3. W jego menu podręcznym wybrać pozycję ***Wszystkie zadania*** (*All Tasks*) a następnie ***Odwołaj certyfikat*** (*Revoke Certificate*). Jako przyczynę odwołania podać ***Złamanie klucza*** (*Key Compromise*).
4. Podobnie unieważnić jeszcze jeden certyfikat spośród wygenerowanych w zadaniu H. Jako przyczynę unieważnienia podać ***Zaprzestanie działania*** (*Change of Affiliation*).
5. W konsoli ***Urząd certyfikacji*** (*Certification Authority*) otworzyć kontener ***Odwołane certyfikaty*** (*Revoked Certificates*) i sprawdzić czy zostały tam umieszczone unieważnione certyfikaty.
6. Aby opublikować CRL, w menu podręcznym kontenera ***Odwołane certyfikaty*** (*Revoked Certificates*) wybrać funkcję ***Wszystkie zadania*** (*All Tasks*) a następnie ***Opublikuj*** (*Publish*). Na ewentualne pytanie dotyczące „nadpisania” poprzednio opublikowanych odpowiedzieć twierdząco, tzn., opublikować nową, pełną listę odwołanych certyfikatów.

J. Pobieranie opublikowanych CRL

1. Otworzyć okno programu ***Internet Explorer***.
2. W polu adresu wpisać **http:*//serwer/certsrv*** (gdzie *serwer* jest nazwą własnego komputera).
3. Na stronie ***Zapraszamy*** (*Welcome*) wybrać opcję ***Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL*** (*Retrieve the CA certificate or certificate revocation list*).
4. Na stronie ***Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL*** (*Retrieve The CA Certificate or Certificate Revocation List*) wybrać opcję ***Pobierz najnowszą podstawową listę CRL*** (*Download latest certificate revocation list*).
5. W oknie dialogowym ***Pobieranie pliku*** (*File download*), wybrać opcję zapisania pliku na dysku i zapisać plik na pulpicie.
6. Otworzyć okno programu ***Windows Eksplorer*** i zlokalizować właśnie zapisany plik .crl. W menu podręcznym ikony zlokalizowanego pliku wybrać polecenie ***Zainstaluj CRL*** (*Install CRL*).
7. Gdy zostanie otwarty kreator importu certyfikatów, wybrać opcję automatycznego wybierania magazynu certyfikatów na podstawie typu certyfikatu.
8. W konsoli CERTYFIKATY_KOMPUTERA.MSC otworzyć kontener ***Pośrednie urzędy certyfikacji*** (*Intermediate Certification Authorities*), a w nim kontener ***Lista odwołania certyfikatów*** (*Certificate Revocation List*). W panelu szczegółów otworzyć (dwuklik) pozycję odpowiadającą własnemu komputerowi i pod zakładką ***Lista odwołania*** (*Revocation List*) zapoznać się z zainstalowaną listą unieważnionych certyfikatów. Sprawdzić, czy są to rzeczywiście certyfikaty unieważnione w ćwiczeniu I.

K. Usuwanie usługi

1. Korzystając z programu ***Dodaj lub usuń programy*** (*Add/Remove Programs*) usunąć z systemu ***Usługę Certyfikatów*** (*Certificate Services*).
2. Zamknąć system.