Ćwiczenie 04b Implementacja infrastruktury klucza publicznego

Celem ćwiczenia jest zapoznanie studentów z wybranymi funkcjami realizowanymi przez urzędy certyfikacyjne w ramach infrastruktury klucza publicznego. Ćwiczenie jest realizowane na dwóch komputerach, z których jeden (oznaczony w niniejszej instrukcji jako X) pełni rolę urzędu głównego a drugi (oznaczony jako Y) pełni rolę urzędu podrzędnego. Na obu komputerach należy zainstalować serwer WWW, który umożliwi klientom komunikację z urzędem certyfikacyjnym. Na komputerze X, na którym zainstalowano urząd główny należy zrealizować zadania 1, 4. Na komputerze Y, na którym zainstalowano urząd podrzędny należy zrealizować zadania 2, 3, 5÷12. Zadania 1÷5 dotyczą instalowania i podstawowych czynności konfiguracyjnych urzędów certyfikacyjnych. W zadaniach 6÷11, 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. 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.

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

Poniższe, zaznaczone zielonym kolorem czynności zrealizować na obu systemach wykorzystywanych w ćwiczeniu, tylko w przypadku jeżeli nie jest na nich zainstalowany IIS.

1. Uruchomić program menedżera serwera (*Server Manager*) i w panelu ról oraz funkcji serwera lokalnego (*Roles and features*) wybrać zadanie dodawania roli.
2. W uruchomionym kreatorze należy przejść przez kolejne strony (bez zmiany jakichkolwiek ustawień) do strony wyboru ról (*Select server roles*).
3. W wykazie ról wybrać rolę serwera „webowego” (*Web Server (IIS)*).
4. W oknie wyboru usług ról (*Select role services*) zaznaczyć (dodatkowo w stosunku do tych, które już są zaznaczone) dostępne wersje ASP.NET i rozszerzenia .NET. Można je znaleźć w gałęzi dotyczącej tworzenia aplikacji (*Application Development)*.
5. Zatwierdzić wybór i przez kolejne strony przejść bez zmieniania jakichkolwiek ustawień.

Zadanie 1. Tworzenie wydzielonego, korzeniowego CA (*Stand-Alone Root CA*)

TO ZADANIE NALEŻY WYKONAĆ TYLKO NA JEDNYM KOMPUTERZE (KOMPUTER X).

1. Zalogować się jako administrator.
2. Utworzyć konsolę ***mmc*** poprzez uruchomienie programu ***mmc,*** w oknie programu ***Windows PowerShell***, a następnie dodać do niej przystawkę certyfikatów (*Certificates*) – menu plików (*File*). W czasie pracy kreatora, zaznaczyć opcje odnoszącą się do konta komputera lokalnego (*Computer account*). Do tej samej konsoli dodać kolejną przystawkę certyfikatów ale odnoszącą się do konta użytkownika (*User account*). Zapisać plik konsoli na pulpicie pod nazwą CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta).
3. W oknie konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta) w obu przystawkach rozwinąć kontener osobisty (*Personal*). Czy są w nim widoczne jakieś certyfikaty?

4. Uruchomić program menedżera serwera (*Server Manager*) i dodać rolę usługi certyfikatów (*Active Directory Certificate Services).* W oknie usług roli, które pojawi się podczas instalacji usługi certyfikatów, zaznaczyć usługę urzędu certyfikacyjnego (*Certification Authority*) oraz interfejs dostępu z wykorzystaniem protokołu HTTP (*Certificate Authority Web Enrollment*).
5. Po zakończeniu instalacji, przejść do procedury konfiguracji ADCS (łącze ADCS w oknie menedżera serwera. Podczas konfiguracji urzędu certyfikacyjnego należy określić następujące parametry (pozostałe zostawić bez zmian):
   - konfiguracja obu wymienionych wyżej usług,
   - autonomiczny urząd certyfikacji (*Standalone CA),*
   - urząd główny (*Root CA*),
   - tworzenie nowego klucza prywatnego (*Create a new private key*).
6. Po zakończeniu instalacji sprawdzić zawartość kontenera osobistego (*Personal*) w konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta). Zapoznać się z zawartością wygenerowanego certyfikatu. Zwrócić uwagę na identyfikator wystawcy i identyfikator właściciela (żądającego wystawienia) certyfikatu.
7. Sprawdzić zawartość kontenera zaufanych główne urzędy certyfikacji (*Trusted Root Certification Authorities*) w konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta). Odszukać wygenerowany przed chwilą certyfikat. Zapoznać się z zawartością tego certyfikatu.
8. Otworzyć konsolę urzędu 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.

Zadanie 2. Rejestrowanie dodatkowego zaufanego CA

TO ZADANIE NALEŻY WYKONAĆ TYLKO NA KOMPUTERZE Y.

1. Zalogować się jako administrator.
2. Utworzyć konsolę ***mmc*** poprzez uruchomienie programu ***mmc,*** w oknie programu ***Windows PowerShell***, a następnie dodać do niej przystawkę certyfikatów (*Certificates*) – menu plików (*File*). W czasie pracy kreatora, zaznaczyć opcje odnoszącą się do konta komputera lokalnego (*Computer account*). Do tej samej konsoli dodać kolejną przystawkę certyfikatów ale odnoszącą się do konta użytkownika (*User account*). Zapisać plik konsoli na pulpicie pod nazwą CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta).
3. W oknie konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta), w obu przystawkach rozwinąć kontener osobisty (*Personal*). Czy są w nim widoczne jakieś certyfikaty?
4. Uruchomić przeglądarkę ***Internet Explorer*** i w polu adresu wpisać:
   http://*nazwa_komputera_X* ***/certsrv***
5. Na stronie powitalnej *(Welcome)* wybrać opcję pobierania certyfikatu urzędu certyfikacyjnego.
6. Na kolejnej stronie wybrać łącze pobierania certyfikatu urzędu certyfikacyjnego (*CA cerificate*). Pobrać certyfikat i zapisać go na pulpicie. Zamknąć okno przeglądarki.
7. W menu podręcznym zapisanego pliku, zawierającego pobrany certyfikat, wybrać funkcję instalowania certyfikatu (*Install Certificate*). Certyfikat umieścić w magazynie zaufanych głównych urzędów certyfikacyjnych (*Trusted Root Certification Authorities*) komputera lokalnego.
8. W konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta), odszukać pobrany przed chwilą certyfikat komputera X. Zapoznać się z zawartością tego

certyfikatu. Porównać tą zawartość z zawartością certyfikatu wygenerowanego podczas realizacji zadania 1.

Zadanie 3. Tworzenie wydzielonego, podrzędnego CA (*Stand-Alone Subordinate CA*)

TO ZADANIE NALEŻY WYKONAĆ TYLKO NA KOMPUTERZE Y.

1. Uruchomić program menedżera serwera (*Server Manager*) i dodać rolę usługi certyfikatów (*Active Directory Certificate Services).* W oknie usług roli (*role services*), które pojawi się podczas instalacji usługi certyfikatów, zaznaczyć usługę urzędu certyfikacyjnego (*Certification Authority*) oraz interfejs dostępu z wykorzystaniem protokołu HTTP (*Certificate Authority Web Enrollment*).
2. Po zakończeniu instalacji, przejść do procedury konfiguracji ADCS (łącze ADCS w oknie menedżera serwera). Podczas konfiguracji urzędu certyfikacyjnego należy określić następujące parametry (pozostałe zostawić bez zmian):
   - konfiguracja obu wymienionych wyżej usług,
   - autonomiczny urząd certyfikacji (*Standalone CA),*
   - urząd podrzędny (*Subordinate CA*),
   - tworzenie nowego klucza prywatnego (*Create a new private key*),
   - wysłanie żądania do urzędu nadrzędnego (*parent*), którym jest komputer X. Po naciśnięciu przycisku wyboru (Select), wpisać nazwę komputera X.

   Dokończyć instalację.

Zadanie 4. Emitowanie certyfikatu dla podrzędnego CA

TO ZADANIE NALEŻY WYKONAĆ TYLKO NA KOMPUTERZE X.

1. Na komputerze pełniącym funkcję korzeniowego CA (komputer X), w grupie narzędzi administracyjnych otworzyć konsolę urzędu certyfikacyjnego (*Certification Authority).*
2. Rozwinąć pozycję swojego komputera i wybrać kontener żądań oczekujących (*Pending Requests)*.
3. W panelu szczegółów, w menu podręcznym pozycji zgłoszonego żądania wybrać pozycję wszystkich zadań (*All Tasks)* a potem funkcję wystawiania certyfikatu (*Issue).*
4. W drzewie konsoli wybrać otworzyć kontener wystawionych certyfikatów (*Issued Certificates)* i sprawdzić czy certyfikat został wyemitowany. Zapoznać się z treścią wygenerowanego certyfikatu. Zwrócić uwagę na pole identyfikacji zamawiającego certyfikat.
5. Zminimalizować konsolę urzędu certyfikacyjnego (*Certification Authority)*.

Zadanie 5. Instalowanie certyfikatu dla podrzędnego CA

TO ZADANIE NALEŻY WYKONAĆ TYLKO NA KOMPUTERZE Y.

1. Na komputerze pełniącym rolę podrzędnego CA (komputer Y), w grupie narzędzi administracyjnych otworzyć konsolę urzędu certyfikacyjnego (*Certification Authority)*. W drzewie konsoli w menu podręcznym pozycji swojego komputera wybrać pozycję wszystkich zadań (*All Tasks),* a potem funkcję instalowania certyfikatu urzędu certyfikacyjnego (*Install CA Certificate).*

2. W oknie dialogowym wybierania pliku *(Select file to complete CA installation)* wybrać przycisk anulowania (*Cancel).*
3. W oknie dialogowym żądania certyfikatu urzędu certyfikacyjnego (*CA Certificate Request),* powinny pojawić się nazwa komputera X i identyfikator dostępnego na nim urzędu certyfikacyjnego. Zatwierdzić (przycisk OK).
4. Odświeżyć obraz konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta). W przystawce dotyczącej komputera lokalnego, sprawdzić zawartość kontenera osobistego (*Personal)*. Zapoznać się z zawartością wygenerowanego certyfikatu. Porównać zawartość z zawartością certyfikatu wygenerowanego podczas realizacji zadania 4. Zwrócić uwagę na identyfikator wystawcy i identyfikator właściciela (żądającego wystawienia) certyfikatu.
5. W oknie programu ***Windows PowerShell***, wprowadzić polecenie :
   `certutil -setreg CA\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE`
6. W konsoli urzędu certyfikacyjnego (*Certification Authority)*, w menu podręcznym pozycji swojego komputera wybrać pozycję uruchomienia usługi (*Start service*) – o ile usługa nie jest jeszcze uruchomiona.
7. Zminimalizować konsolę urzędu certyfikacyjnego (*Certification Authority)*.

KOLEJNE ZADANIA MOŻNA WYKONAĆ NIEZALEŻNIE NA OBU KOMPUTERACH
STUDENCI STUDIÓW INTERNETOWYCH POWINNI JE WYKONAĆ NA KOMPUTERZE Y (PODRZĘDNYM URZĘDZIE CERTYFIKACYJNYM)

Zadanie 6. Żądanie certyfikatu IPSec

1. Uruchomić przeglądarkę ***Internet Explorer*** i w polu adresu wpisać: **http:*//serwer /certsrv*** (gdzie *serwer* jest nazwą własnego komputera).
2. Na stronie powitalnej (*Welcome*) wybrać link żądania certyfikatu (*Request a certificate*).
3. Na stronie żądania certyfikatu (*Request a certificate*) wybrać link zaawansowanego żądania certyfikatu (*advanced certificate request*).
4. Na stronie zaawansowanego żądania certyfikatu (*Advanced Certificate Request*) wybrać link utworzenia i przesłania żądanie do urzędu certyfikacji (*Create and submit a certificate request to this CA*).
5. Na kolejnej stronie zaawansowanego żądania certyfikatu (*Advanced Certificate Request*) wpisać swoje dane personalne.
6. W sekcji typu potrzebnego certyfikatu (*Type of Certificate Needed)*), wybrać certyfikat zabezpieczeń IP (IPSec) (*IPSec Certificate*). Zapoznać się z innymi dostępnymi pozycjami.
7. W sekcji opcji klucza (*Key Options*), wybrać opcję oznaczenia kluczy jako eksportowalnych (*Mark keys as exportable*).
8. W sekcji opcji dodatkowych, w polu przyjaznej nazwy (*Friendly Name*) wpisać IPSEC. Pozostałe pola pozostawić bez zmian i nacisnąć przycisk wysłania żądania (*Submit*).
9. Po pojawieniu się strony oczekiwania na certyfikat (*Certificate Pending*)**,** zamknąć okno programu ***Internet Explorer***.
10. Sprawdzić zawartość kontenera ***żądań wydania certyfikatu*** (*Certificate Enrollment Requests*) w konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta). Zapoznać się z zawartością wygenerowanego żądania. Zwrócić uwagę na pola identyfikatora wystawcy i podmiotu, wartości klucza publicznego, przyjaznej nazwy.

Zdanie 7. Emitowanie i instalowanie żądanego certyfikatu

1. Przywrócić konsolę urzędu certyfikacyjnego (*Certification Authority*).
2. W drzewie konsoli rozwinąć kontener swojego serwera i wybrać kontener oczekujących żądań (*Pending Requests*).
3. Odświeżyć obraz wybierając w menu akcji (*Action*) funkcję odświeżania (*Refresh*).
4. Korzystając z menu definiowania widoku (*View*), skonfigurować okno w ten sposób aby dla każdego certyfikatu wyświetlały się jedynie kolumny: identyfikatora żądania, nazwy żądającego, kodu stanu żądania, binarnego klucza publicznego.
5. W panelu szczegółów, w menu podręcznym pozycji zgłoszonego żądania wybrać pozycję wszystkich zadań (*All Tasks*) a potem funkcję wystawiania certyfikatu (*Issue*).
6. W drzewie konsoli wybrać kontener wystawionych certyfikatów (*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 urzędu certyfikacyjnego (*Certification Authority*).
8. Otworzyć okno przeglądarki ***Internet Explorer***.
9. W polu adresu wpisać **http://***serwer***/certsrv** (gdzie *serwer* jest nazwą własnego komputera).
10. Na stronie powitalnej (*Welcome*) wybrać link umożliwiający zapoznanie się ze stanem oczekującego żądania certyfikatu (*View the status of a pending certificate request*).
11. Na kolejnej stronie sprawdzić, czy wysłane żądanie zostało obsłużone, tzn. czy żądany certyfikat został przygotowany. Jeżeli tak to uaktywnić łącze prowadzące do niego.
12. Na stronie wystawionego certyfikatu (*Certificate Issued*) wybrać funkcję instalowania certyfikatu (*Install this certificate*).
13. Zamknąć okno programu ***Internet Explorer***.
14. Odświeżyć obraz konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta). Sprawdzić zawartość kontenera osobistego (*Personal*) w przystawce użytkownika. Zapoznać się z zawartością nowego certyfikatu. Porównać z zawartością wygenerowanego uprzednio żądania oraz certyfikatu wygenerowanego podczas realizacji zadań 6 i 7.

Zadanie 8. Eksportowanie i importowanie certyfikatów

1. Przywrócić konsolę CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta).
2. W przystawce użytkownika otworzyć kontener osobisty (*Personal*) a nim podkontener certyfikatów (*Certificates*).
3. Widoczny tam certyfikat wyeksportować do pliku na pulpicie. Wymusić również eksport klucza prywatnego (*private key*). Tworzony w ten sposób plik zabezpieczyć dowolnym hasłem.
4. W menu podręcznym podkontenera certyfikatów (*Certificates*), kontenera osobistego (*Personal*) przystawki komputera wybrać funkcję importowania. Jako importowany, wskazać utworzony przed chwilą plik. Wymusić oznaczenie klucza jako eksportowalnego (*exportable*) oraz włączyć wszystkie rozszerzenia (*extended properties*).
5. Odświeżyć obraz konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta). Sprawdzić zawartość kontenera osobistego (*Personal*) w przystawce komputera. Zapoznać się z zawartością nowego certyfikatu. Porównać z zawartością certyfikatu wygenerowanego podczas realizacji zadania 7.

Zadanie 9. Żądanie, emitowanie i instalowanie dodatkowych certyfikatów dla komputera

1. W sposób opisany w zadaniu 6 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 7 wyemitować certyfikaty, realizując żądania wygenerowane w punkcie 1. Następnie zainstalować te certyfikaty.
3. Dokonać exportu i importu certyfikatów w celu umieszczenia ich w magazynie komputera.

Zadanie 10. Unieważnianie certyfikatów i publikowanie CRL

1. W konsoli urzędu certyfikacyjnego (*Certification Authority*) otworzyć kontener wystawionych certyfikatów (*Issued Certificates*).
2. Wybrać dowolny z certyfikatów wygenerowanych podczas realizacji zadania 9.
3. W jego menu podręcznym wybrać pozycję wszystkich zadań (*All Tasks*) a następnie funkcję odwołania certyfikatu (*Revoke Certificate*). Jako przyczynę odwołania podać złamanie klucza (*Key Compromise*).
4. Podobnie unieważnić jeszcze jeden certyfikat spośród wygenerowanych w zadaniu 9. Jako przyczynę unieważnienia podać zaprzestanie działania (*Change of Affiliation*).
5. W konsoli urzędu certyfikacyjnego (*Certification Authority*) otworzyć kontener odwołanych certyfikatów (*Revoked Certificates*) i sprawdzić czy zostały tam umieszczone unieważnione certyfikaty.
6. Aby opublikować CRL, w menu podręcznym kontenera odwołanych certyfikatów (*Revoked Certificates*) wybrać pozycję wszystkich zadań (*All Tasks*) a następnie funkcję publikowania (*Publish*). Na ewentualne pytanie dotyczące „nadpisania” poprzednio opublikowanych odpowiedzieć twierdząco, tzn., opublikować nową, pełną listę odwołanych certyfikatów.

Zadanie 11. Pobieranie opublikowanych CRL

1. Otworzyć okno przeglądarki ***Internet Explorer***.
2. W polu adresu wpisać **http://***serwer***/certsrv** (gdzie *serwer* jest nazwą własnego komputera).
3. Na stronie powitalnej (*Welcome*) wybrać opcję pobrania certyfikatu urzędu certyfikacji, łańcucha certyfikatów lub listy CRL (*Donload a CA certificate, certificate chain or CRL*).
4. Na kolejnej stronie (*Download a CA Certificate, Certificate Chain or CRL*) wybrać link umożliwiający pobranie najnowszej podstawowej CRL (*Download latest base CRL*).
5. Zapisać plik CRL na pulpicie i amknąć okno programu ***Internet Explorer***.
6. Na pulpicie, w menu podręcznym ikony utworzonego przed chwilą pliku, wybrać polecenie zainstalowania CRL (*Install CRL*).
7. Gdy zostanie otwarty kreator importu certyfikatów, wybrać opcję automatycznego wybierania magazynu certyfikatów na podstawie typu certyfikatu.
8. W konsoli CERTYFIKATY_XX.MSC (gdzie XX jest numerycznym identyfikatorem studenta) otworzyć kontener pośrednich urzędów certyfikacyjnych (*Intermediate Certification Authorities*), a w nim kontener list odwołanych certyfikatów (*Certificate Revocation List*). W panelu szczegółów otworzyć (dwuklik) pozycję odpowiadającą własnemu komputerowi i pod

zakładką listy odwołań (*Revocation List*) zapoznać się z zainstalowaną listą unieważnionych certyfikatów. Sprawdzić, czy są to rzeczywiście certyfikaty unieważnione podczas realizacji zadania 10.

Zadanie 12. Usuwanie usług

1. Korzystając z programu menedżera serwera (*Server Manager*) usunąć rolę ADCS oraz *Web Server (IIS)*).
2. Usunąć z pulpitu wszystkie pliki utworzone podczas realizacji niniejszego ćwiczenia.
3. Zamknąć system.