

CERTYFIKATY SSL

Działaj zgodnie z prawem



IIS 7.5

Instalacja certyfikatów pośrednich na serwerze

Windows 2008/2012

wersja 1.0

Spis treści

1. WSTĘP	3
2. INSTALACJA CERTYFIKATÓW POŚREDNICH NA SERWERZE	3
2.1. INSTALACJA CERTYFIKATÓW POŚREDNICH DLA TEST SSL	4
2.2. INSTALACJA CERTYFIKATÓW POŚREDNICH DLA COMMERCIAL SSL.....	6
2.3. INSTALACJA CERTYFIKATÓW POŚREDNICH DLA TRUSTED SSL.....	8
2.4. INSTALACJA CERTYFIKATÓW POŚREDNICH DLA PREMIUM EV SSL	10

1. Wstęp

Certyfikat Test SSL posiada pełną funkcjonalność opcji Commercial SSL – podstawowe potwierdzenie tożsamości oraz szyfrowanie 128 bitowe. Podobnie jak komercyjne certyfikaty, jest akceptowany przez większość popularnych przeglądarek internetowych. Pozwala również na zachowanie pełnej poufności połączenia pomiędzy użytkownikiem a serwerem. W efekcie nie istnieje obawa, że wrażliwe dane zostaną przechwycone przez nieuprawnioną osobę. Test SSL jest w pełni darmowy przez okres 30 dni. Pozwala na bliższe zapoznanie się z elementami podnoszącymi bezpieczeństwo witryny i jej użytkowników, a następnie dokonanie wyboru jednej z możliwych opcji pełnego zabezpieczenia.

Commercial SSL jest najprostszym dostępnym rozwiązaniem, które pozwala stosować w pełni szyfrowane połączenia pomiędzy użytkownikiem a serwerem do 256 bitów i jest akceptowany przez wszystkie najpopularniejsze przeglądarki internetowe. W związku z zastosowaniem uproszczonej weryfikacji kupującego (tylko w formie sprawdzenia prawa do domeny) procedura została znacząco uproszczona. Dzięki temu Commercial SSL jest możliwy do zainstalowania natychmiast po dokonaniu płatności i zweryfikowaniu domeny. Stanowi on najlepszy wybór dla witryn niekomercyjnych, forów internetowych, portali społecznościowych, małych sklepów internetowych oraz serwerów pocztowych.

Trusted SSL jest przeznaczony dla banków i instytucji finansowych. W związku ze szczególnymi wymaganiami procedura wydawania certyfikatu zawiera wnikliwą weryfikację tożsamości kupującego. W efekcie, stosując Trusted SSL, ma się pewność korzystania z najlepszych możliwych zabezpieczeń. Trusted SSL jest wydawany na 1,2 lub 3 lata, oraz posiada najwyższą gwarancję w wysokości 750 000 PLN. Ponadto certyfikat posiada możliwość szyfrowania transmisji pomiędzy użytkownikiem a serwerem do 256 bitów i jest akceptowany przez wszystkie najpopularniejsze przeglądarki internetowe.

Premium EV SSL to certyfikat z typu Extended Validation gwarantujący najwyższy poziom bezpieczeństwa i zaufania. Przeznaczony jest do zabezpieczenia stron WWW oraz danych przekazywanych przez sieć Internet. Wszystkie dane zawarte w certyfikacie tj. nazwa domeny, dane jej właściciela podlegają szczegółowej weryfikacji zgodnie z międzynarodowym standardem WebTrustSM/TM Extended Validation. Certyfikat Premium EV SSL przeznaczony jest dla firm, organizacji i administracji publicznej.

Strony WWW zabezpieczone certyfikatem Premium EV SSL wyświetlane są z zielonym paskiem adresu WWW w przeglądarce. Dodatkowo widoczne są także dane właściciela strony internetowej. Dzięki temu użytkownik ma pewność, że znajduje się na właściwej stronie, którą może obdarzyć pełnym zaufaniem.



Certyfikaty Premium EV SSL CERTUM wydawane są na 1 lub 2 lata zgodnie ze standardami Guidelines For The Issuance And Management Of Extended Validation Certificates - co oznacza, że osoby odwiedzające zabezpieczone nimi serwisy WWW nie otrzymują komunikatu "niezaufany certyfikat - zabierz mnie stąd!".

2. Instalacja certyfikatów pośrednich na serwerze

Uwaga! Czynności opisane w niniejszym rozdziale należy wykonać tylko w przypadku braku zaświadczeń certyfikacyjnych w systemie Windows 2008/2012 server.

Bardzo ważnym elementem są certyfikaty urzędów pośrednich. Należy je zainstalować na serwerze WWW aby przeglądarka internetowa poprawnie zweryfikowała wystawcę certyfikatu.

2.1. Instalacja certyfikatów pośrednich dla certyfikatów SSL

Proszę wejść na stronę certum.pl i z górnego menu wybrać „Obsługa certyfikatów a następnie **Zaświadczenia i klucze**. Proszę zapisać certyfikaty urzędów **Certum CA**, **Certum Level I CA**, . Proszę wybrać certyfikaty dla serwerów SSL/TLS:

- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum%20CA
- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#lev1

W przypadku certyfikatów wspierających algorytm SHA-2 należy pobrać poniższe zaświadczenia certyfikacyjne:

- https://certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum CTNA
- <https://repository.certum.pl/bundles/Class1Chain-SHA2.crt>

Zalecaną metodą jest dystrybucja zaświadczeń certyfikacyjnych w domenie. Czynności te należy wykonać na kontrolerze domeny.

W pierwszym kroku uruchom linię poleceń. Wpisz i uruchom poniższe polecenia

```
certutil -f -dspublish CertumCA.cer NTAAuthCA lub certutil -f -dspublish CertumCTNCA.cer NTAAuthCA
```

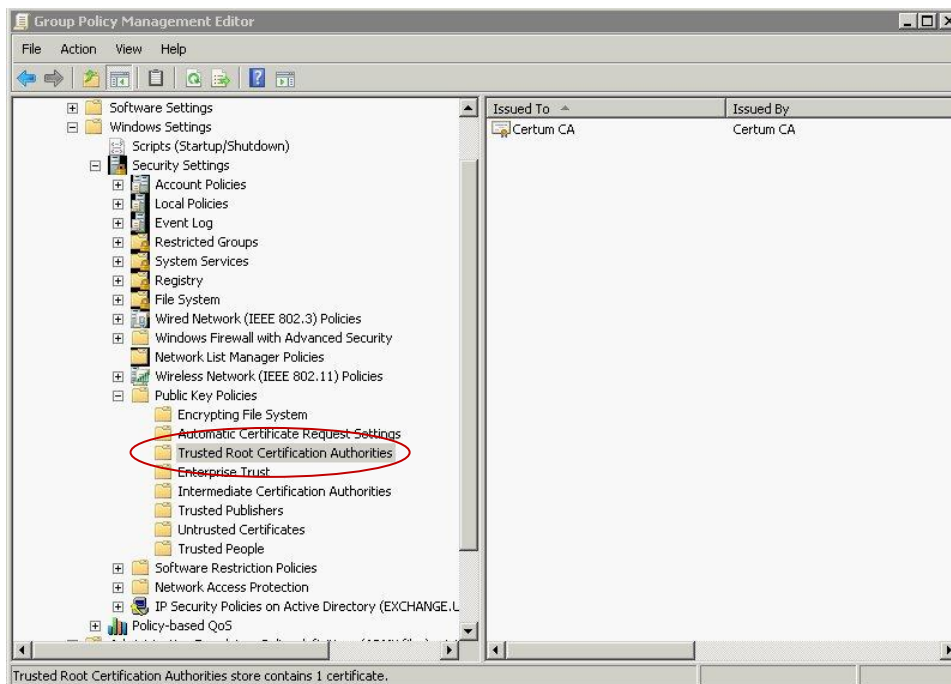
```
certutil -f -dspublish LevelIVCA.cer NTAAuthCA lub certutil -f -dspublish Class1Chain-SHA2.cer NTAAuthCA
```

```
certutil -f -dspublish CertumCA.cer RootCA lub certutil -f -dspublish CertumCTNCA.cer RootCA
```

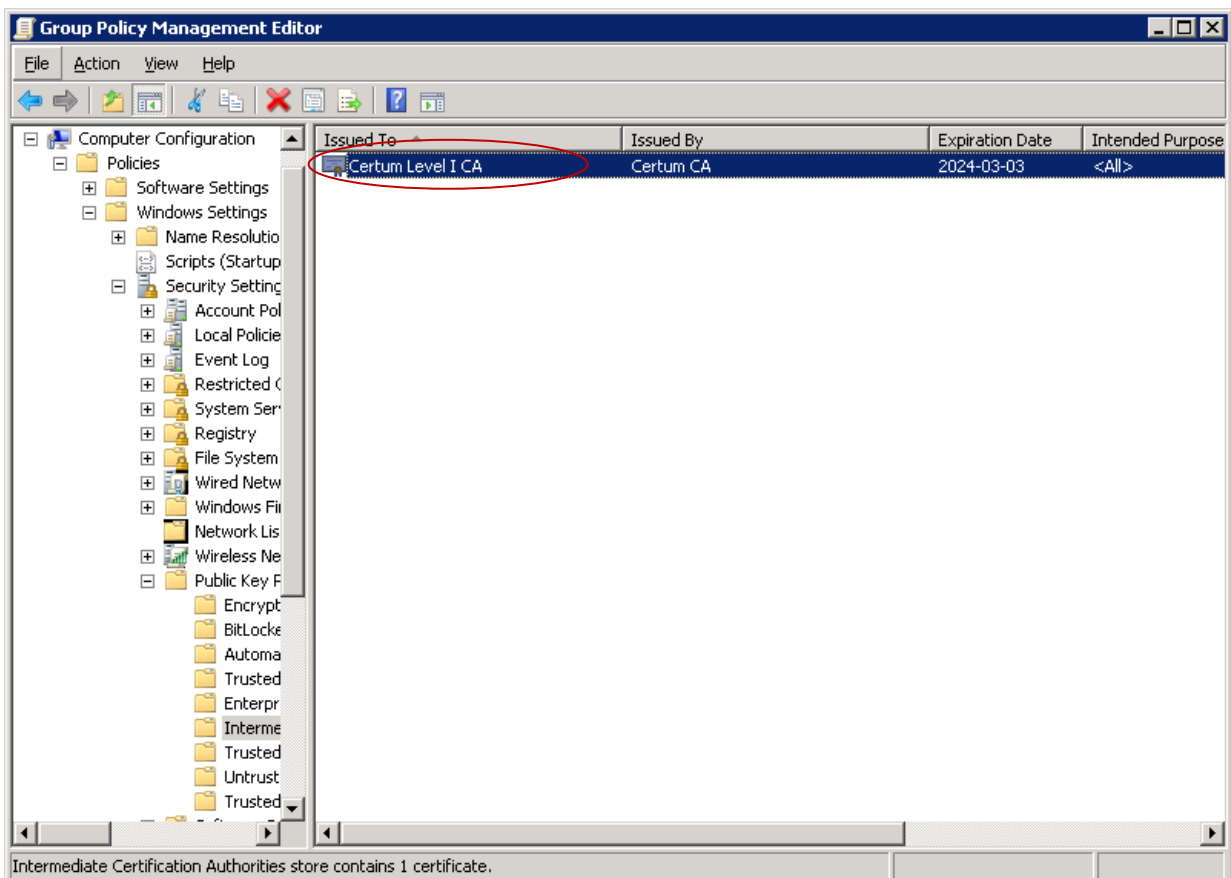
W celu instalacji certyfikatów roota oraz pośrednich należy z menu **Start-Programs-Administrative Tools** wybrać **Group Policy Management**.

UWAGA: W celu instalacji konsoli **Group Policy Management** wykonaj czynności opisane pod adresem: <http://technet.microsoft.com/en-us/library/cc754841.aspx>

Po uruchomieniu konsoli **Group Policy Management** należy zaimportować zapisane wcześniej certyfikaty **Certum CA** lub **Certum CTNA** do **Trusted Root Certification Authorities**



oraz Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA, Certum Class I CA SHA2, do **Intermediate Certification Authorities**.



Odświeżenie zasad grup GPO spowoduje automatyczną dystrybucję certyfikatów w domenę.

2.2. Instalacja certyfikatów pośrednich dla Commercial SSL

Proszę wejść na stronę certum.pl i z górnego menu wybrać „Obsługa certyfikatów a następnie **Zaświadczenia i klucze**. Proszę zapisać certyfikaty urzędów **Certum CA**, **Certum Level II CA**, Proszę wybrać certyfikaty dla serwerów SSL/TLS:

- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum%20CA
- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#lev2

W przypadku certyfikatów wspierających algorytm SHA-2 należy pobrać poniższe zaświadczenia certyfikacyjne:

- https://certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum CTNA
- <https://repository.certum.pl/bundles/DVSSLChain-SHA2.crt>

Zalecaną metodą jest dystrybucja zaświadczeń certyfikacyjnych w domenę. Czynności te należy wykonać na kontrolerze domeny.

W pierwszym kroku uruchom linię poleceń. Wpisz i uruchom poniższe polecenia

```
certutil -f -dspublish CertumCA.cer NTAAuthCA lub certutil -f -dspublish CertumCTNCA.cer NTAAuthCA
```

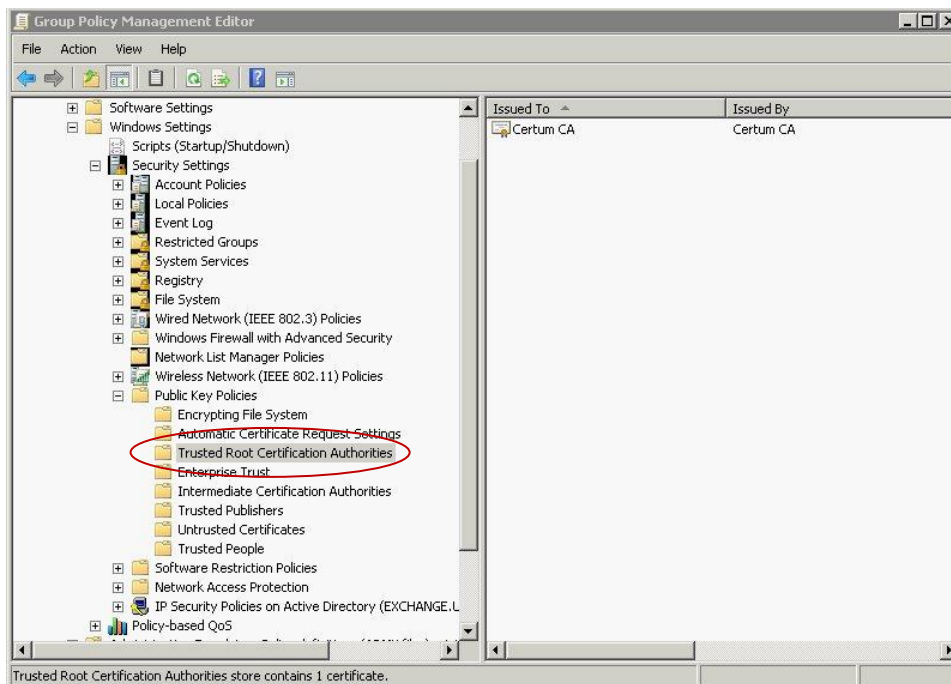
```
certutil -f -dspublish LevelIIICA.cer NTAAuthCA lub certutil -f -dspublish DVSSLChain-SHA2.cer NTAAuthCA
```

```
certutil -f -dspublish CertumCA.cer RootCA lub certutil -f -dspublish CertumCTNCA.cer RootCA
```

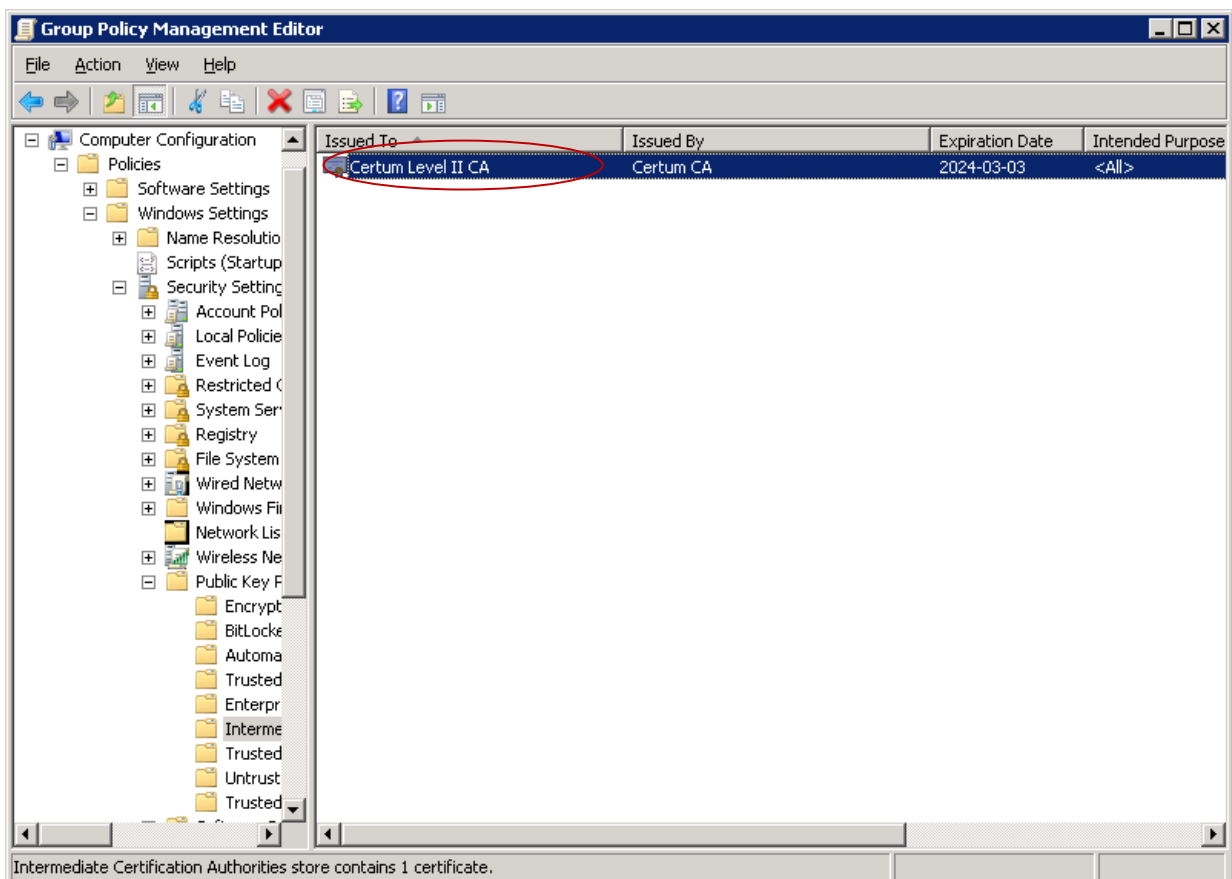
W celu instalacji certyfikatów roota oraz pośrednich należy z menu **Start-Programs-Administrative Tools** wybrać **Group Policy Management**.

UWAGA: W celu instalacji konsoli **Group Policy Management** wykonaj czynności opisane pod adresem: <http://technet.microsoft.com/en-us/library/cc754841.aspx>

Po uruchomieniu konsoli **Group Policy Management** należy zaimportować zapisane wcześniej certyfikaty Certum CA lub Certum CTNA do **Trusted Root Certification Authorities**



oraz Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA oraz Certum Domain Validation CA SHA2 do **Intermediate Certification Authorities**.



Odświeżenie zasad grup GPO spowoduje automatyczną dystrybucję certyfikatów w domenę.

2.3. Instalacja certyfikatów pośrednich dla Trusted SSL

Proszę wejść na stronę certum.pl i z górnego menu wybrać „Obsługa certyfikatów a następnie **Zaświadczenia i klucze**. Proszę zapisać certyfikaty urzędów **Certum CA, Certum Level III CA**. Proszę wybrać certyfikaty dla serwerów SSL/TLS:

- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum%20CA
- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#lev3

W przypadku certyfikatów wspierających algorytm SHA-2 należy pobrać poniższe zaświadczenia certyfikacyjne:

- https://certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum CTNA
- <https://repository.certum.pl/bundles/OVSSLChain-SHA2.crt>

Zalecaną metodą jest dystrybucja zaświadczeń certyfikacyjnych w domenę. Czynności te należy wykonać na kontrolerze domeny.

W pierwszym kroku uruchom linię poleceń. Wpisz i uruchom poniższe polecenia

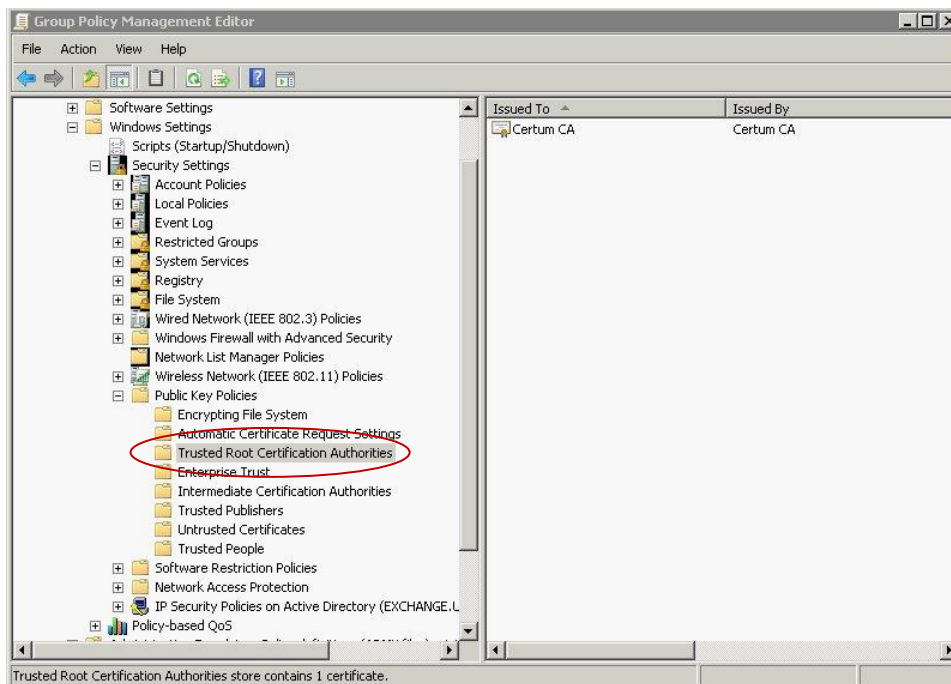
certutil -f -dspublish CertumCA.cer NTAAuthCA lub certutil -f -dspublish CertumCTNCA.cer NTAAuthCA

certutil -f -dspublish LevelIVCA.cer NTAAuthCA lub certutil -f -dspublish OVSSLChain-SHA2.cer NTAAuthCA certutil -f -dspublish CertumCA.cer RootCA lub certutil -f -dspublish CertumCTNCA.cer RootCA

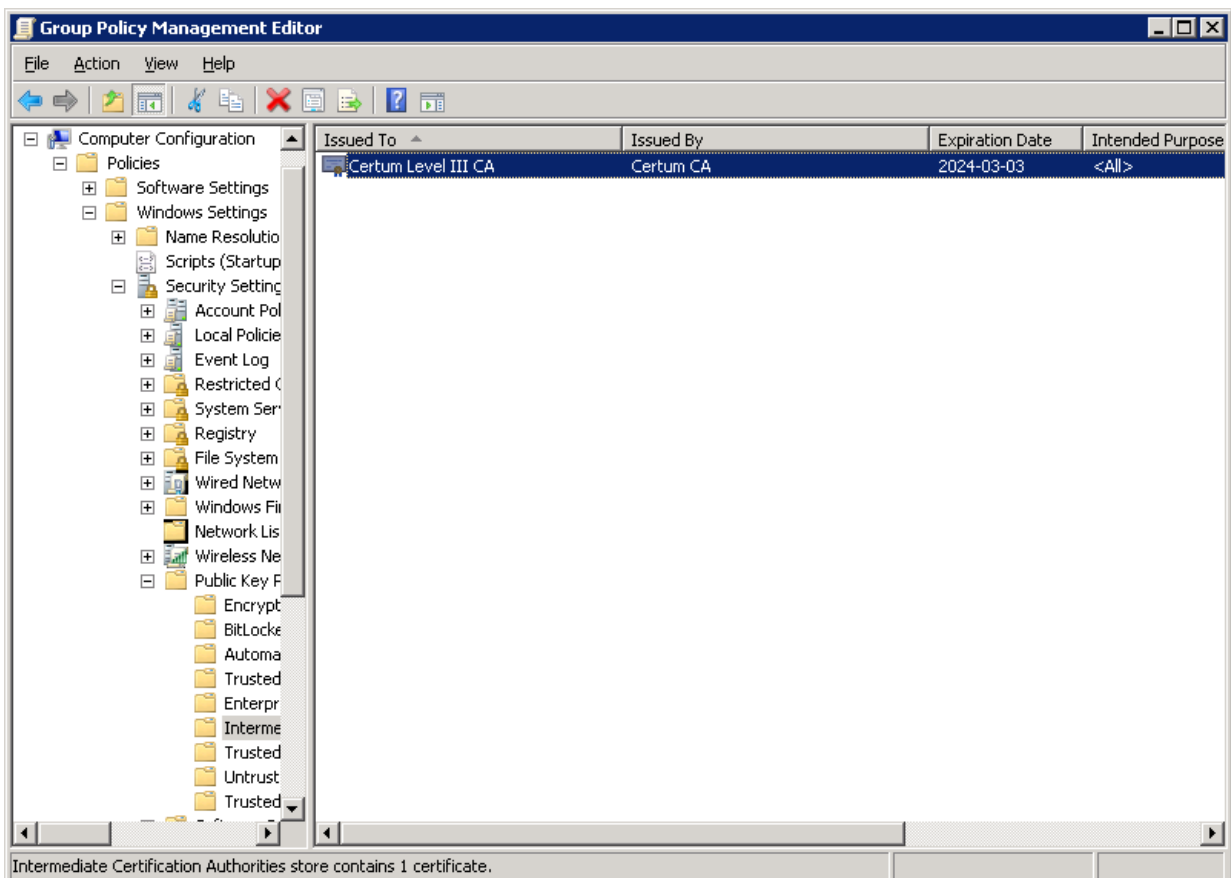
W celu instalacji certyfikatów roota oraz pośrednich należy z menu **Start-Programs-Administrative Tools** wybrać **Group Policy Management**.

UWAGA: W celu instalacji konsoli **Group Policy Management** wykonaj czynności opisane pod adresem: <http://technet.microsoft.com/en-us/library/cc754841.aspx>

Po uruchomieniu konsoli **Group Policy Management** należy zaimportować zapisane wcześniej certyfikaty **Certum CA** lub **Certum CTNA** do **Trusted Root Certification Authorities**



Certum Level III CA oraz Certum Organization Validation CA do Intermediate Certification Authorities.



Odświeżenie zasad grup GPO spowoduje automatyczną dystrybucję certyfikatów w domenę.

2.4. Instalacja certyfikatów pośrednich dla Premium EV SSL

Proszę wejść na stronę certum.pl i z górnego menu wybrać „Obsługa certyfikatów a następnie **Zaświadczenia i klucze**. Proszę zapisać certyfikaty urzędów **Certum CA, Certum Level IV CA**. Proszę wybrać certyfikaty dla serwerów SSL/TLS:

- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum%20CA
- http://www.certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#lev4

W przypadku certyfikatów wspierających algorytm SHA-2 należy pobrać poniższe zaświadczenia certyfikacyjne:

- https://certum.pl/certum/cert,wiedza_zaswiadczenia_klucze_certum.xml#Certum CTNA
- <https://repository.certum.pl/bundles/EVSSLChain-SHA2.crt>

Zalecaną metodą jest dystrybucja zaświadczeń certyfikacyjnych w domenę. Czynności te należy wykonać na kontrolerze domeny.

W pierwszym kroku uruchom linię poleceń. Wpisz i uruchom poniższe polecenia

certutil -f -dspublish CertumCA.cer NTAAuthCA lub certutil -f -dspublish CertumCTNCA.cer NTAAuthCA

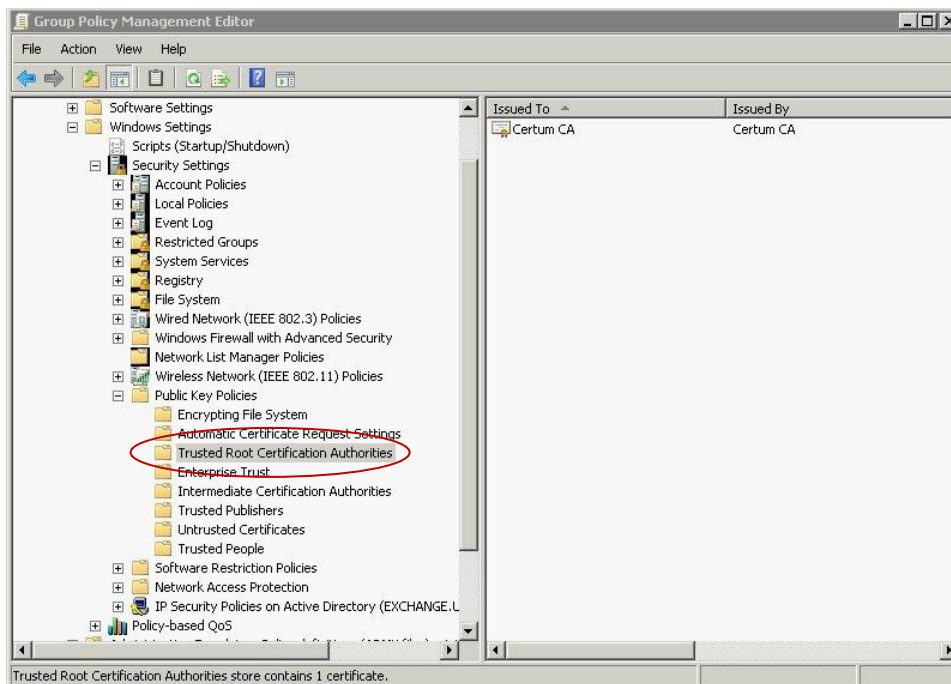
certutil -f -dspublish LevelIVCA.cer NTAAuthCA lub certutil -f -dspublish EVSSLChain-SHA2.cer NTAAuthCA

certutil -f -dspublish CertumCA.cer RootCA lub certutil -f -dspublish CertumCTNCA.cer RootCA

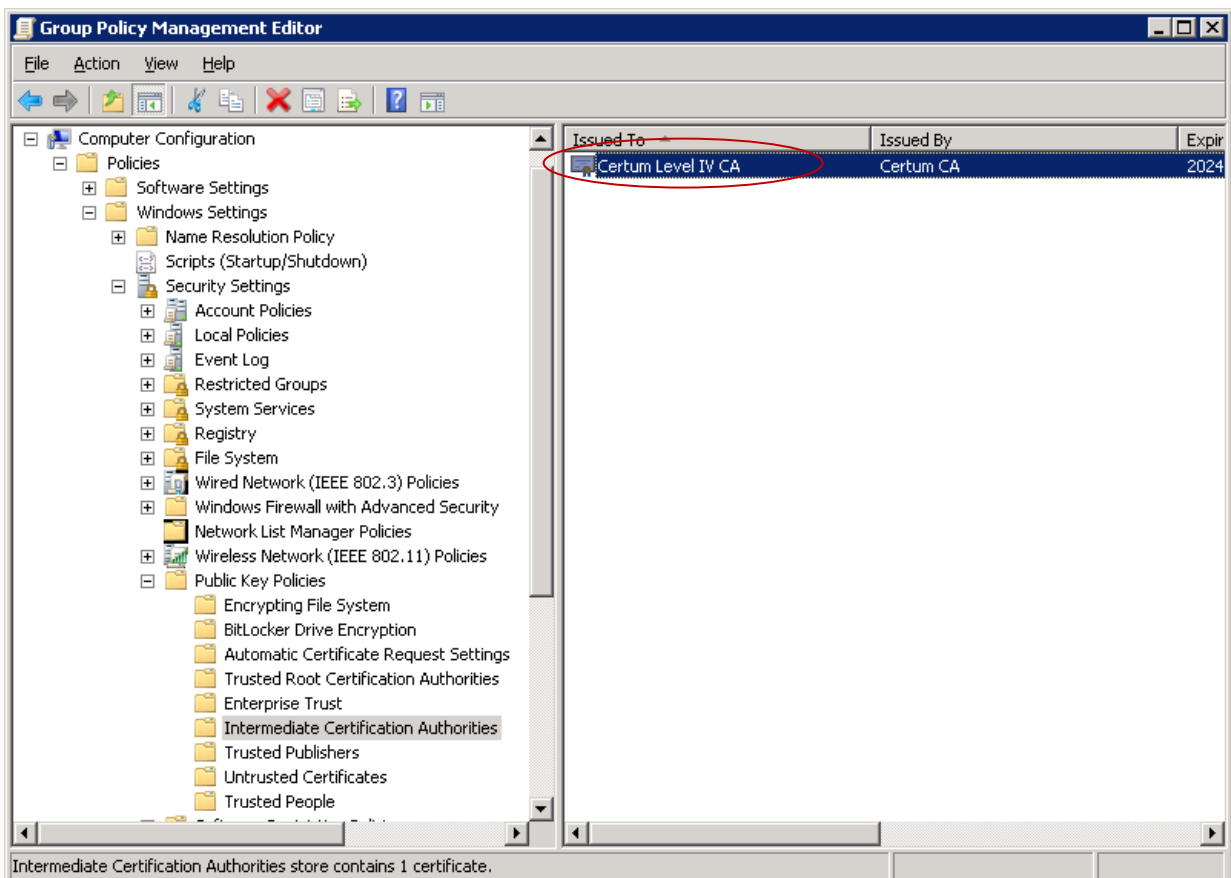
W celu instalacji certyfikatów roota oraz pośrednich należy z menu **Start-Programs-Administrative Tools** wybrać **Group Policy Management**.

UWAGA: W celu instalacji konsoli **Group Policy Management** wykonaj czynności opisane pod adresem: <http://technet.microsoft.com/en-us/library/cc754841.aspx>

Po uruchomieniu konsoli **Group Policy Management** należy zaimportować zapisane wcześniej certyfikaty **Certum CA Certum CTNA** do **Trusted Root Certification Authorities**



oraz Certum Level IV CA oraz **Certum Extended Validation CA SHA2** do **Intermediate Certification Authorities**.



Odświeżenie zasad grup GPO spowoduje automatyczną dystrybucję certyfikatów w domenie.