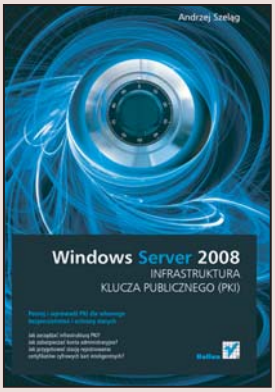
Windows Server 2008. Infrastruktura klucza publicznego (PKI)

Autor: Andrzej Szeląg
ISBN: 83-246-1914-3
Stron: 300



Poznaj i wprowadź PKI dla własnego bezpieczeństwa i ochrony danych

- Jak zarządzać infrastrukturą PKI?
- Jak zabezpieczać konta administracyjne?
- Jak przygotować stację rejestrowania certyfikatów cyfrowych kart inteligentnych?

Infrastruktura klucza publicznego PKI (skrót od ang. Public Key Infrastructure) stanowi zbiór sprzętu, oprogramowania, reguł oraz procedur koniecznych do tworzenia, zarządzania, przechowywania i dystrybucji certyfikatów opartych na kryptografii z kluczem publicznym. Dzięki tej infrastrukturze można tworzyć bezpieczne kanały do wymiany informacji oraz przesyłania ważnych danych przy użyciu Internetu. Najczęściej infrastruktura PKI wykorzystywana jest w handlu elektronicznym, ponieważ pozwala na wzajemną weryfikację sprzedawcy i kupującego oraz zapewnia bezpieczny kanał podczas obustronnej komunikacji sieciowej.

Książka „Windows Server 2008. Infrastruktura klucza publicznego (PKI)" zawiera wszystkie niezbędne informacje, związane z infrastrukturą klucza publicznego. Dzięki temu podręcznikowi poznasz zasady tworzenia PKI w przedsiębiorstwach dowolnej wielkości, a także wszystkie zagadnienia dotyczące szczegółowego procesu instalacji oraz konfiguracji nadrzędnego i podrzędnego urzędu certyfikacji. Dowiesz się, na czym polega konfigurowanie zasad grupy, związanych z infrastrukturą klucza publicznego – w szczególności tych dotyczących kart inteligentnych i usług, które są z nimi związane – na komputerze pracującym pod kontrolą serwerowego systemu operacyjnego Windows Server 2008 Standard.

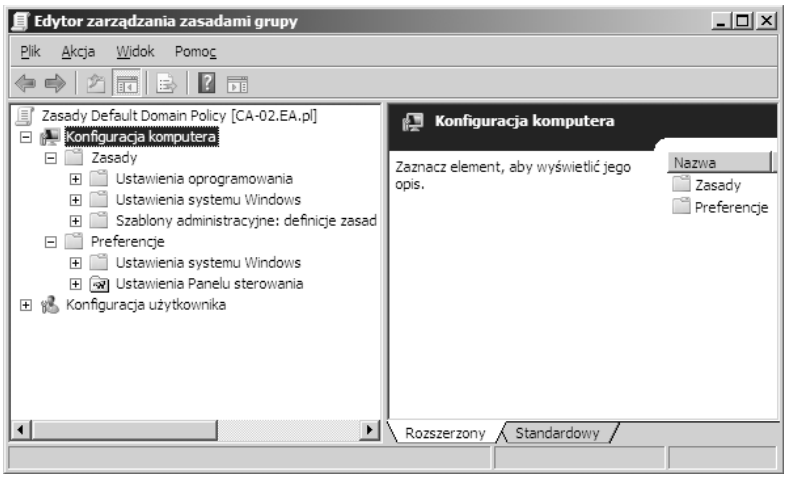
- Infrastruktura klucza publicznego
- Architektura PKI w Windows Server 2008
- PKI a szyfrowanie informacji
- Zastosowania PKI
- Tworzenie infrastruktury PKI
- Nadrzędny i podrzędny urząd certyfikacji
- Szablony certyfikatów cyfrowych
- Zasady grupy i usługi związane z PKI
- Konfigurowanie IIS 7, SSL i IE 7 na potrzeby PKI
- Uwierzytelnianie za pomocą kart inteligentnych w Windows Server 2008 i Windows Vista
- Zdalny dostęp w Windows Server 2008 i Windows Vista

Bezpieczeństwo to podstawa.
Profesjonalnie ochroń wartościowe dane firmy

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

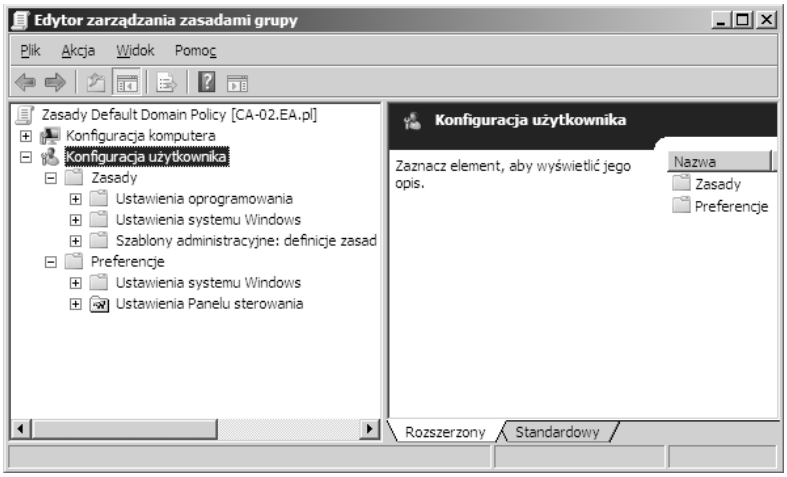
Spis treści

Rysunek 6.1. *Zasady grupy dotyczące komputera*



2. *Zasady grupy dotyczące użytkownika*, które przedstawiono na rysunku 6.2. Są one stosowane do tych użytkowników, którzy logują się do systemu na danym komputerze. Na ogół zasady te są aktywowane natychmiast po uwierzytelnieniu tożsamości użytkownika, ale przed przyznaniem mu dostępu do systemu Windows.

Rysunek 6.2. *Zasady grupy dotyczące użytkownika*

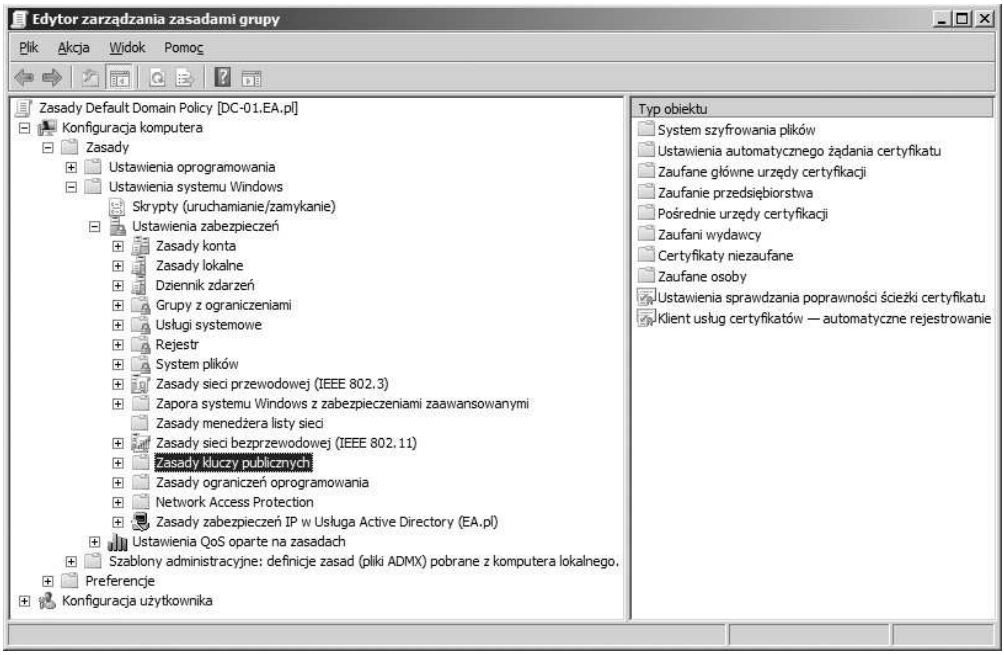


Zasady grupy nie powodują trwałych zmian w rejestrze systemu Windows. Można je więc bardzo łatwo dodawać i usuwać bez „zaśmiecania" rejestru czy konieczności ponownego uruchamiania systemu operacyjnego.

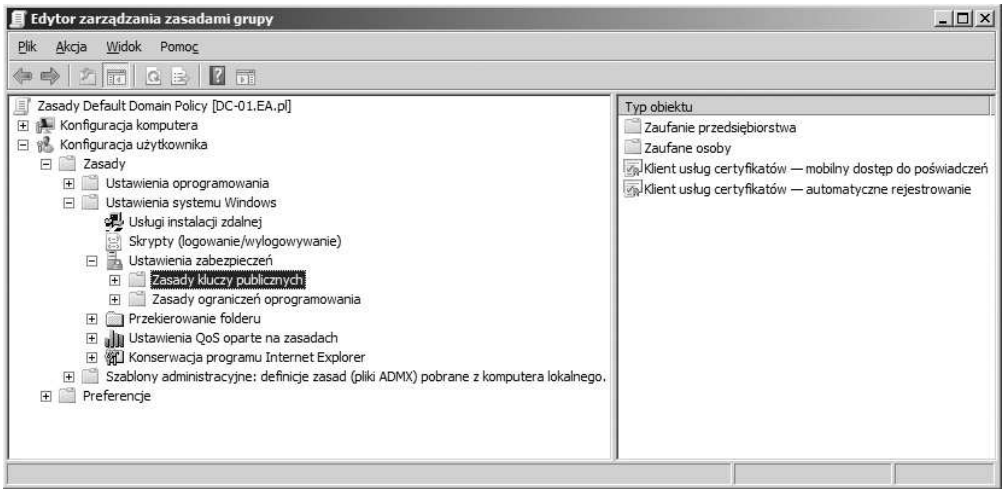
6.2. Zasady kluczy publicznych

W tej części książki zostaną przedstawione zasady grupy związane z infrastrukturą klucza publicznego (PKI), a w szczególności zawartość kontenera o nazwie *Zasady kluczy publicznych*. Obiekty i opcje dostępne w tym kontenerze umożliwiają zarządzanie

ustawieniami infrastruktury klucza publicznego, które znajdują się w sekcji dotyczącej komputera (rysunek 6.3) i użytkownika (rysunek 6.4) w dowolnej wielkości przedsiębiorstwie lub organizacji.



Rysunek 6.3. *Zasady kluczy publicznych dotyczące komputera*



Rysunek 6.4. *Zasady kluczy publicznych dotyczące użytkownika*

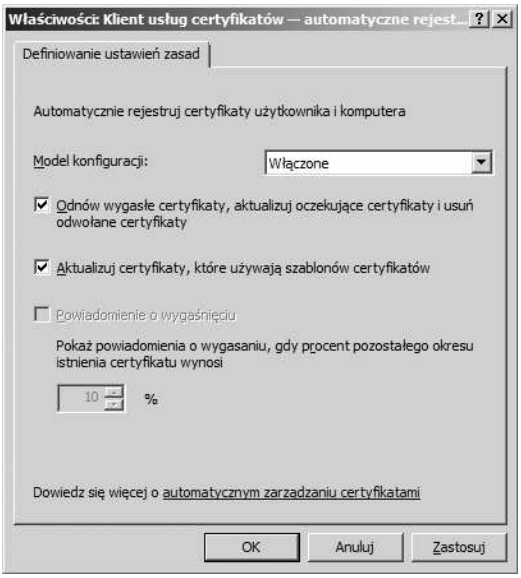
Co można skonfigurować za pomocą obiektów oraz opcji dostępnych w kontenerze *Zasady kluczy publicznych*? Najważniejsze ustawienia zostały przedstawione poniżej w punktach.

1. Automatyczne rejestrowanie certyfikatów cyfrowych użytkownika i komputera

Automatyczne rejestrowanie certyfikatów cyfrowych użytkownika i komputera pozwala w niezwykle prosty sposób zautomatyzować:

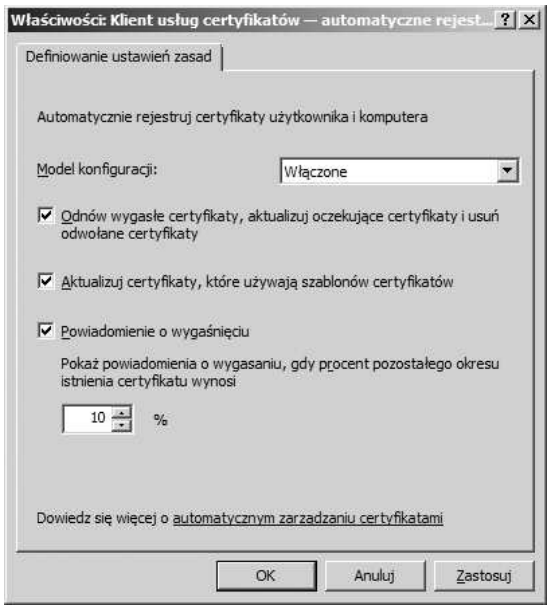
- proces odnawiania wygasłych certyfikatów cyfrowych,
- aktualizowanie oczekujących certyfikatów cyfrowych (również tych, które używają opisanych wcześniej szablonów certyfikatów cyfrowych),
- usuwanie odwołanych certyfikatów cyfrowych,
- powiadamianie o wygasaniu danego certyfikatu cyfrowego, zanim skończy się jego okres ważności.

Powyższe cele można osiągnąć, edytując właściwości obiektu *Klient usług certyfikatów — automatyczne rejestrowanie* z poziomu kontenera *Zasady kluczy publicznych*, co przedstawiono na rysunku 6.5.



Rysunek 6.5. *Klient usług certyfikatów — automatyczne rejestrowanie dla komputera*

Zgodnie z rysunkiem 6.5, na zakładce *Definiowanie ustawień zasad* można skonfigurować automatyczne rejestrowanie certyfikatów cyfrowych użytkowników oraz komputerów. W tym odnawianie wygasłych certyfikatów cyfrowych, aktualizację oczekujących czy usunięcie odwołanych certyfikatów cyfrowych. Poza tym można zaktualizować certyfikaty cyfrowe, które zostały utworzone na podstawie szablonów certyfikatów cyfrowych. W przypadku skonfigurowania automatycznego rejestrowania dla użytkowników dodatkowo pojawi się (rysunek 6.6) opcja *Powiadomienie o wygaśnięciu*. Jej włączenie spowoduje wyświetlanie powiadomienia o wygasaniu certyfikatu cyfrowego, gdy procent pozostałego okresu ważności tego certyfikatu wyniesie 10%. Tę domyślną wartość można oczywiście zmieniać w zależności od wymagań danego przedsiębiorstwa lub innej organizacji.



Rysunek 6.6. *Klient usług certyfikatów — automatyczne rejestrowanie dla użytkownika*

2. Konfigurowanie ustawień sprawdzania poprawności ścieżki certyfikatu

Użytkownicy przedsiębiorstwa lub innej organizacji mogą w dowolnym stopniu korzystać z certyfikatów cyfrowych. W najnowszych serwerowych systemach operacyjnych Microsoft Windows Server 2008 Standard administrator domeny ma możliwość kontrolowania (dzięki obiektowi o nazwie *Ustawienia sprawdzania poprawności ścieżki certyfikatu*, który jest dostępny w kontenerze *Zasady kluczy publicznych*) stopień zużytkowania tych certyfikatów. Po wybraniu właściwości obiektu *Ustawienia sprawdzania poprawności ścieżki certyfikatu* można przejść do konfigurowania ustawień sprawdzania poprawności ścieżki certyfikatu cyfrowego. Służą do tego opcje, które są dostępne na czterech zakładkach (*Magazyny*, *Zaufani wydawcy*, *Pobieranie z sieci* i *Odwoływanie*), oraz zasady *Sprawdzanie poprawności ścieżki certyfikatu*. Na potrzeby tej książki zostanie omówiona jedynie zakładka *Magazyny*, gdyż pozostałe nie są tak istotne.

Jak ogólnie wiadomo, przedsiębiorstwa i inne organizacje chcą jednoznacznie identyfikować oraz rozprowadzać w sieci komputerowej tylko zaufane certyfikaty cyfrowe nadrzędnych urzędów certyfikacji. Umożliwiają to opcje dostępne na zakładce o nazwie *Magazyny*, przedstawionej na rysunku 6.7. Z poziomu tej zakładki można określać m.in. reguły zaufania użytkownika do certyfikatu cyfrowego nadrzędnego CA, który funkcjonuje w danym przedsiębiorstwie lub organizacji.

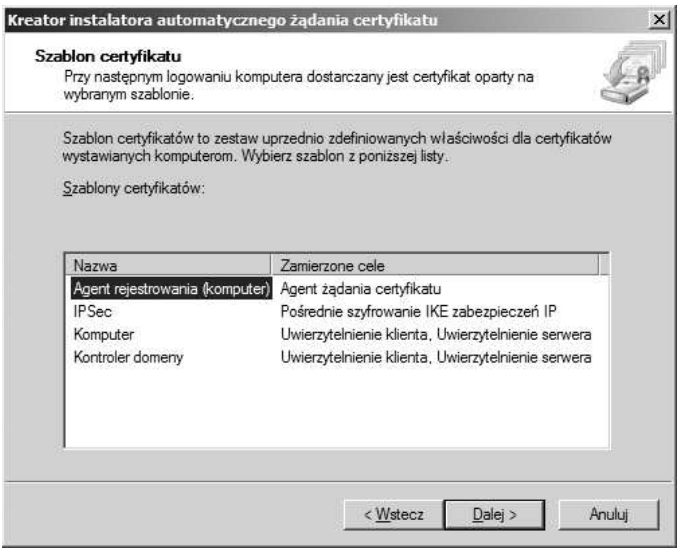
3. Konfigurowanie ustawienia automatycznego żądania certyfikatu dla komputerów

Jak już wspomniano na początku tego rozdziału, zarządzanie każdym certyfikatem cyfrowym z osobna jest czasochłonne. W kontenerze o nazwie *Ustawienia automatycznego żądania certyfikatu* administrator domeny może

Rysunek 6.7. *Zakładka „Magazyny”*

zdefiniować, których typów certyfikatów cyfrowych komputer może zażądać automatycznie. W przypadku tworzenia nowego żądania certyfikatu cyfrowego zostanie uruchomione narzędzie *Kreator instalatora automatycznego żądania certyfikatu*, co przedstawia rysunek 6.8.

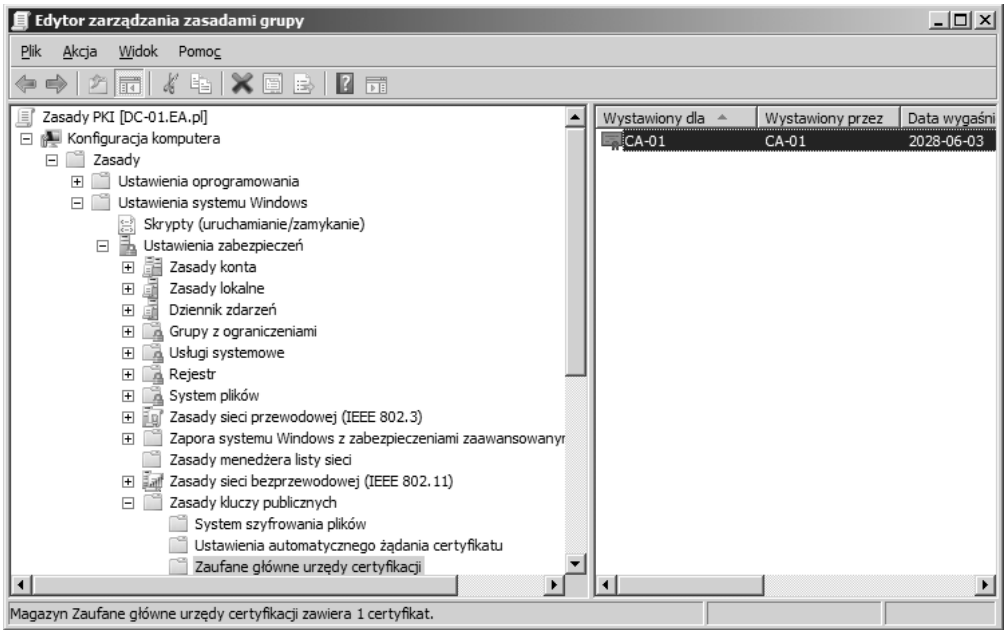
Rysunek 6.8. *„Kreator instalatora automatycznego żądania certyfikatu”*



4. Importowanie certyfikatu nadrzędnego CA do magazynu „Zaufane główne urzędy certyfikacji"

Po zainstalowaniu w przedsiębiorstwie lub innej organizacji nadrzędnego CA należy dodać (zaimportować) jego certyfikat cyfrowy do magazynu *Zaufane główne urzędy certyfikacji*, co pozwoli przenieść go automatycznie (za pomocą zasad grupy) na różne komputery (komputery klienckie, serwery członkowski itp.).

Certyfikat cyfrowy nadrzędnego CA można dodać do magazynu *Zaufane główne urzędy certyfikacji* po zaznaczeniu obiektu o nazwie *Zaufane główne urzędy certyfikacji*. Następnie trzeba wybrać z menu *Akcja* opcję *Importuj*... Zostanie wówczas uruchomiony dobrze znany z poprzednich rozdziałów kreator o nazwie *Kreator importu certyfikatów* — za jego pomocą można zaimportować certyfikat cyfrowy nadrzędnego CA (rysunek 6.9).

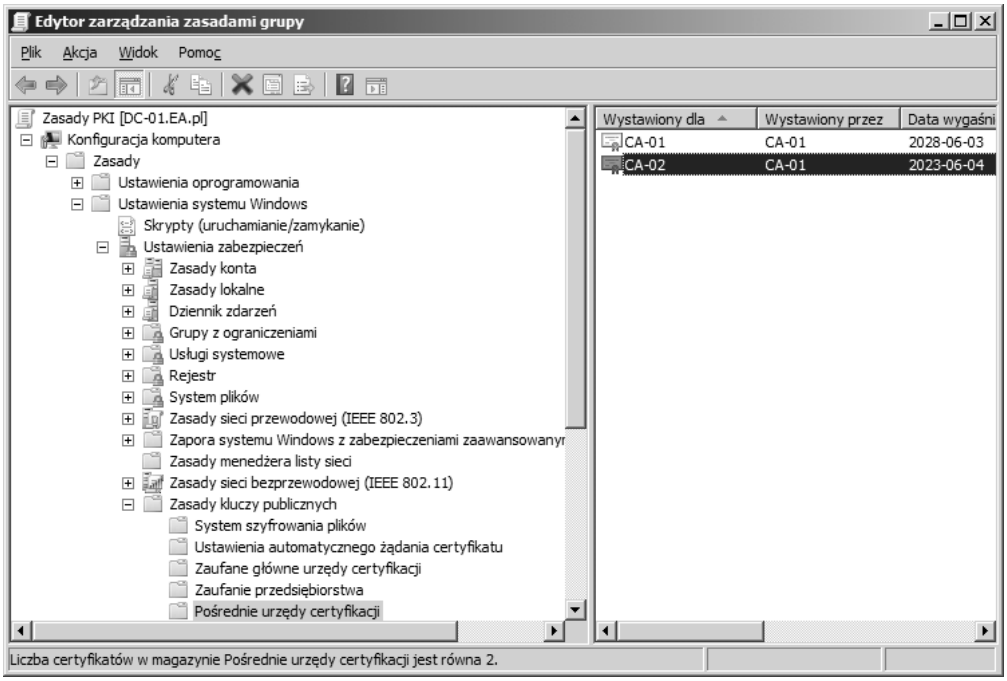


Rysunek 6.9. *Certyfikat cyfrowy nadrzędnego CA zaimportowany do magazynu „Zaufane główne urzędy certyfikacji"*

5. Importowanie certyfikatu podrzędnego CA do magazynu „Pośrednie urzędy certyfikacji"

Po zainstalowaniu w przedsiębiorstwie lub innej organizacji podrzędnego CA należy (podobnie jak w przypadku certyfikatu nadrzędnego CA) zaimportować jego certyfikat cyfrowy do magazynu *Pośrednie urzędy certyfikacji*.

Po zaimportowaniu certyfikatu cyfrowego podrzędnego CA do magazynu *Pośrednie urzędy certyfikacji* w prawym oknie konsoli powinien pojawić się certyfikat *CA-02*, jak na rysunku 6.10. Zostaje dodany również certyfikat cyfrowy nadrzędnego CA (*CA-01*), co także obrazuje ten sam rysunek. Jak pamiętamy z rozdziału 4., podczas eksportu certyfikatu cyfrowego



Rysunek 6.10. *Certyfikat podrzędnego CA zaimportowany do magazynu „Pośrednie urzędy certyfikacji"*

podrzędnego CA został wybrany format *PKCS #7 (.P7B)* wraz z opcją *Jeżeli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji*. Ponieważ certyfikat cyfrowy nadrzędnego CA należy do tej ścieżki, jest dodawany wszędzie tam, gdzie wprowadzono certyfikat cyfrowy podrzędnego CA.

Po wykonaniu powyższych kroków należy odświeżyć zasady grupy (użytkownika oraz komputera) za pomocą komendy `gpupdate /force`. Wykonanie tej komendy wymusza natychmiastową aktualizację zasad grupy użytkownika i komputera.

6.3. Konfigurowanie zasad grupy dotyczących kart inteligentnych

Najnowsze serwerowe systemy operacyjne Windows Server 2008 Standard zawierają kilka zasad, które dotyczą kart inteligentnych. W tej części książki zaprezentowane zostaną dwie najczęściej wykorzystywane, czyli:

1. **Logowanie interakcyjne: wymagaj karty inteligentnej**. To ustawienie zabezpieczeń określa, że użytkownicy domeny mogą się zalogować się do komputera tylko przy użyciu karty inteligentnej z właściwym certyfikatem cyfrowym.

2. **Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej**. To ustawienie zabezpieczeń określa, co się stanie, jeśli karta inteligentna aktualnie zalogowanego do komputera użytkownika zostanie wyjęta z czytnika kart inteligentnych.

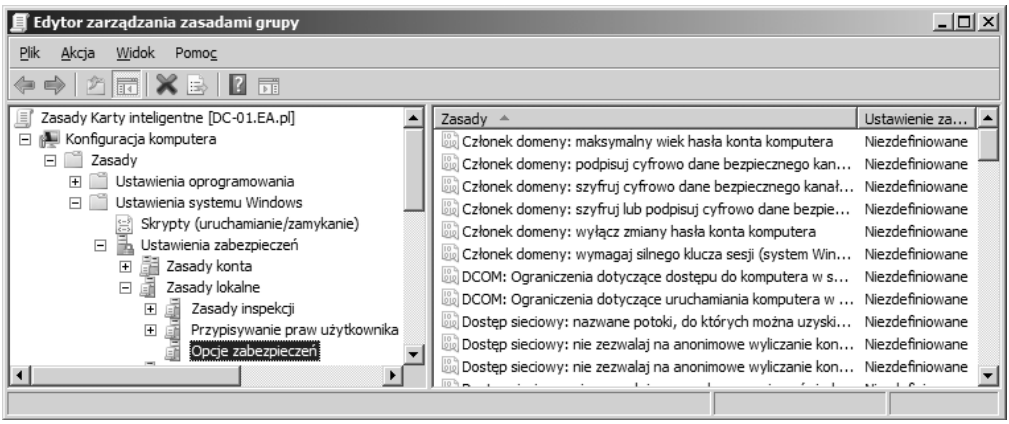
Powyższe zasady, których włączenie podnosi poziom bezpieczeństwa w przedsiębiorstwie lub innej organizacji wykorzystujących infrastrukturę klucza publicznego (PKI), są dostępne z poziomu konsoli *Zarządzanie zasadami grupy* na kontrolerze domeny.

Najczęściej zasady grupy dotyczące kart inteligentnych można definiować dla całej domeny sieciowej lub dla wybranej jednostki organizacyjnej (ang. *Organizational Unit*). Na potrzeby tej książki zdefiniowane zostaną zasady dla jednostki organizacyjnej o nazwie *PKI*. W tym celu Administrator domeny (użytkownik *EA.pl\Administrator*) na kontrolerze domeny o nazwie *DC-01* musi:

1. Uruchomić konsolę *Zarządzanie zasadami grupy* (np. za pomocą komendy `gpmc.msc`).
2. Przejść do obiektu o nazwie *PKI* i utworzyć w nim nowy obiekt zasad grupy o nazwie *Karty inteligentne*, jak na rysunku 6.11.

Rysunek 6.11. *Nowy obiekt zasad grupy o nazwie „Karty inteligentne”*

3. Rozwinąć węzeł *Obiekty zasad grupy* i zaznaczyć zasadę *Karty inteligentne*.
4. Z menu *Akcja* wybrać opcję *Edytuj...*
5. Przejść do węzła *Opcje zabezpieczeń*, przedstawionego na rysunku 6.12.



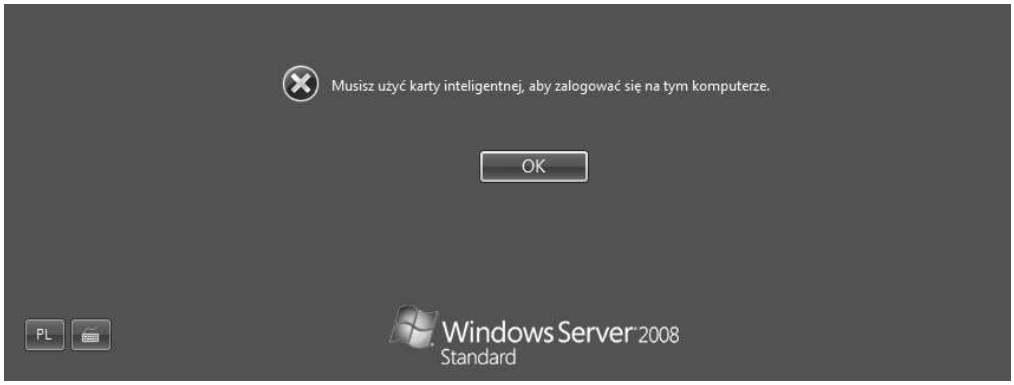
Rysunek 6.12. *Węzeł „Opcje zabezpieczeń” wraz z domyślnymi zasadami grypy*

Z poziomu węzła *Opcje zabezpieczeń* zostaną skonfigurowane dwie wspomniane wcześniej zasady grupy dotyczące kart inteligentnych, czyli:

- *Logowanie interakcyjne: wymagaj karty inteligentnej*,
- *Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej*.

6.3.1. Logowanie interakcyjne: wymagaj karty inteligentnej

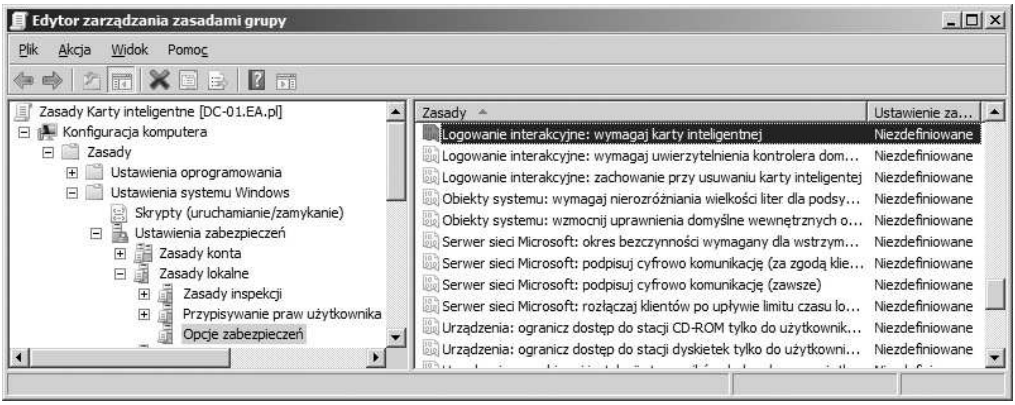
Jeżeli przedsiębiorstwo lub inna organizacja zechce umożliwić dostęp do jakiegoś serwera członkowskiego, np. o nazwie *CA-02* (podrzędnego CA), jedynie z wykorzystaniem kart inteligentnych, musi włączyć zasadę o nazwie *Logowanie interakcyjne: wymagaj karty inteligentnej*. Dzięki tej zasadzie podczas logowania za pomocą hasła dostępowego do tego serwera pojawi się komunikat przedstawiony na rysunku 6.13. Oczywiście po wcześniejszym wykonaniu omawianych w tym podrozdziale kroków i po przeniesieniu konta serwera członkowskiego o nazwie *CA-02* do jednostki organizacyjnej *PKI*, dla której została ustawiona powyższa zasada. Trzeba pamiętać o tym, aby przed przeniesieniem konta komputera do wspomnianej jednostki organizacyjnej zaimportować do odpowiednich magazynów certyfikaty cyfrowe nadrzędnego i podrzędnego CA oraz listy CRL.



Rysunek 6.13. *Wynik działania zasady „Logowanie interakcyjne: wymagaj karty inteligentnej”*

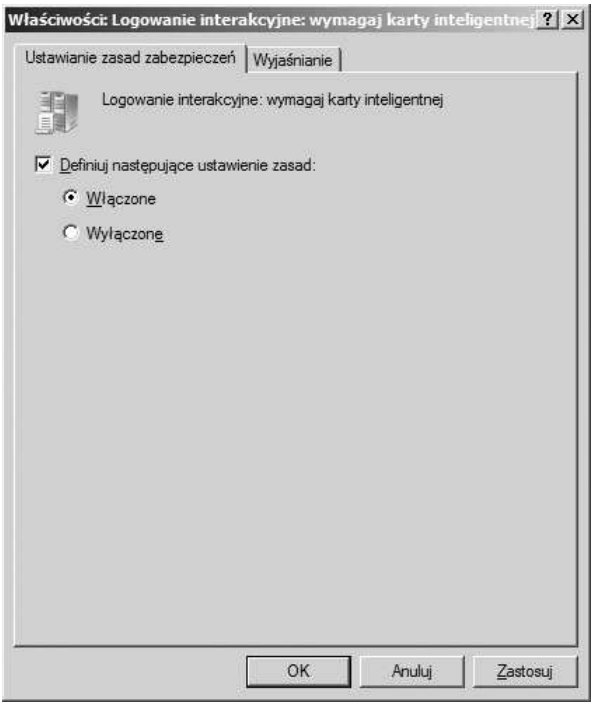
Aby włączyć zasadę o nazwie *Logowanie interakcyjne: wymagaj karty inteligentnej*, Administrator domeny (użytkownik *EA.pl\Administrator*) musi wykonać wymieniane poniżej działania na kontrolerze domeny.

1. Zaznaczyć w prawym oknie zasadę *Logowanie interakcyjne: wymagaj karty inteligentnej*, jak na rysunku 6.14.
2. Z menu *Akcja* wybrać opcję *Właściwości*.
3. Na zakładce *Ustawianie zasad zabezpieczeń* zaznaczyć pole wyboru *Definiuj następujące ustawienie zasad*, a następnie wybrać opcję *Włączone*, jak na rysunku 6.15.



Rysunek 6.14. *Zasada „Logowanie interakcyjne: wymagaj karty inteligentnej”*

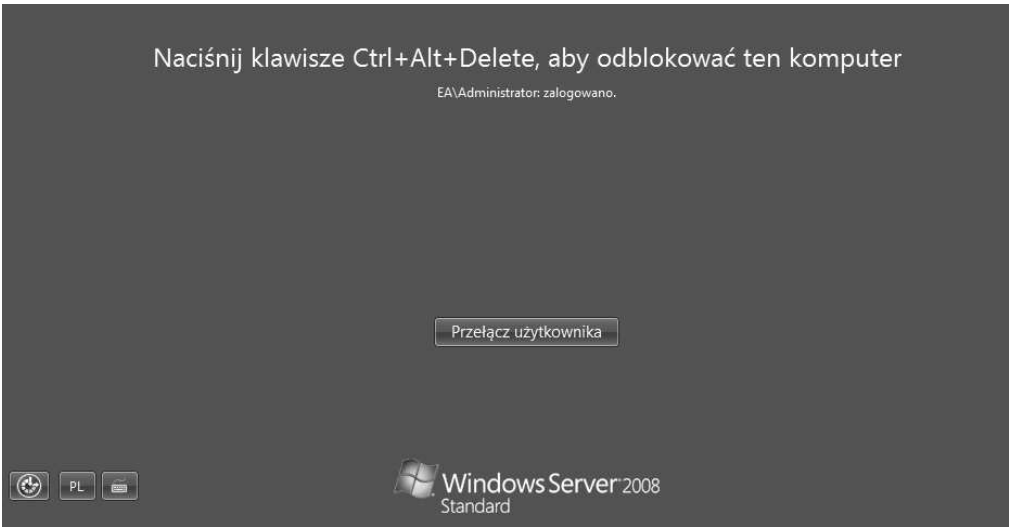
Rysunek 6.15. *Zakładka „Ustawianie zasad zabezpieczeń” dla „Logowanie interakcyjne: wymagaj karty inteligentnej”*



4. Kliknąć na przycisk *OK*, aby zamknąć okno *Właściwości: Logowanie interakcyjne: wymagaj karty inteligentnej*. Nie należy zamykać konsoli *Zarządzanie zasadami grupy*, gdyż będzie ona potrzebna do ustawienia kolejnej zasady o nazwie „Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej”.

6.3.2. Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej

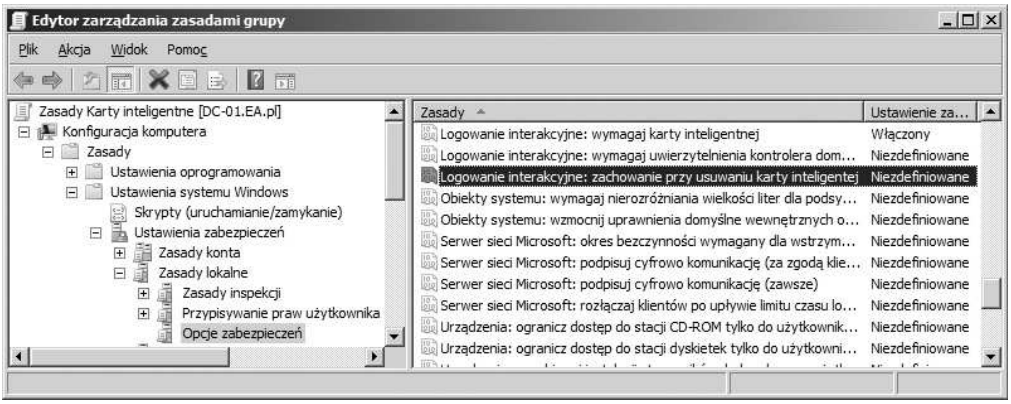
Jeżeli chcemy, aby dostęp do jakiegoś serwera członkowskiego, np. o nazwie *CA-02* (podrzędnego CA), był blokowany po wyjęciu karty inteligentnej z czytnika kart inteligentnych (rysunek 6.16), trzeba włączyć zasadę o nazwie *Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej*. Oczywiście po wcześniejszym wykonaniu przedstawionych w tym podrozdziale (i w dwóch kolejnych) kroków, a następnie po przeniesieniu konta serwera członkowskiego o nazwie *CA-02* do jednostki organizacyjnej *PKI*, dla której została ustawiona ta zasada grupy.



Rysunek 6.16. *Wynik działania zasady „Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej"*

Aby skonfigurować zasadę dotyczącą zachowania się komputera podczas usuwania karty inteligentnej z czytnika kart inteligentnych, Administrator domeny (użytkownik *EA.pl\Administrator*) musi wykonać wymieniane poniżej działania.

1. Zaznaczyć w prawym oknie konsoli *Zarządzanie zasadami grupy* zasadę *Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej*, jak na rysunku 6.17.
2. Z menu *Akcja* wybrać opcję *Właściwości*.
3. Na zakładce *Ustawianie zasad zabezpieczeń* zaznaczyć pole wyboru *Definiuj następujące ustawienie zasad*, a następnie z listy rozwijalnej wybrać akcję *Zablokuj stację roboczą*, jak na rysunku 6.18. Poza tą akcją są dostępne inne opcje:
   - *Brak akcji*,
   - *Wymuszaj wylogowanie*,
   - *Rozłącz w przypadku zdalnej sesji usług terminalowych*.



Rysunek 6.17. *Zasada „Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej”*

Rysunek 6.18. *Zakładka „Ustawianie zasad zabezpieczeń dla Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej”*

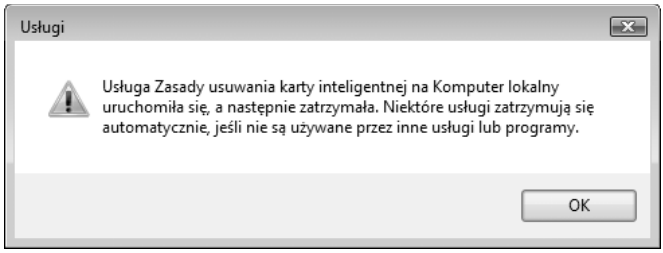
4. Kliknąć na przycisk *OK*.
5. Zamknąć konsolę *Edytor zarządzania zasadami grupy*.

Po wykonaniu powyższych działań należy odświeżyć zasady grupy (użytkownika oraz komputera) za pomocą komendy `gpupdate /force`. Komenda ta wymusza natychmiastową aktualizację zasad grupy użytkownika i komputera.

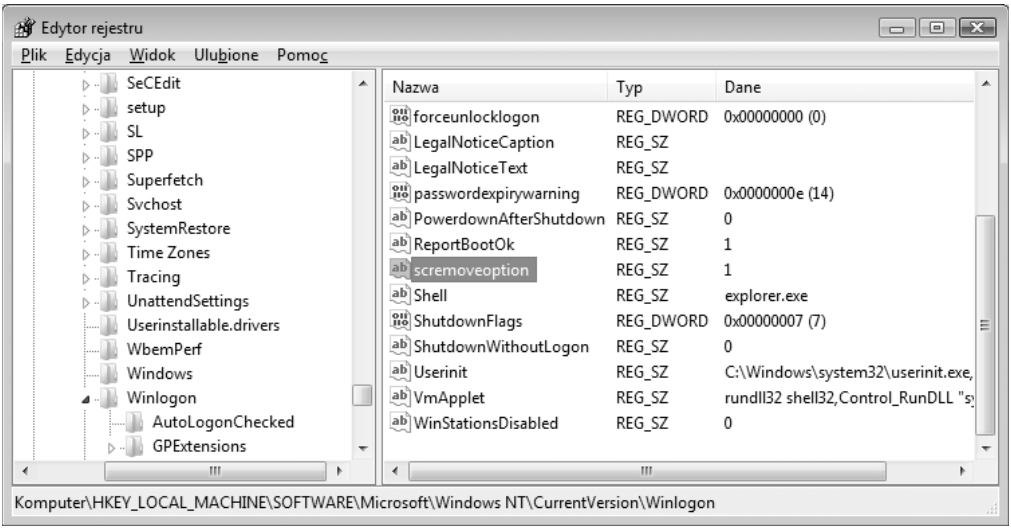
W przypadku zasady *Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej* warto pamiętać o jeszcze jednym. Zasada ta działa dopiero po włączeniu na komputerze wyposażonym w czytnik kart inteligentnych i kartę inteligentną (za pomocą

którego realizowane jest uwierzytelnianie z wykorzystaniem certyfikatu cyfrowego karty inteligentnej) usługi o nazwie *Zasady usuwania karty inteligentnej*. Jest to nowa usługa w systemach operacyjnych Windows Server 2008 Standard i Windows Vista Business, uruchamiana ręcznie lub automatycznie. Druga metoda zostanie przedstawiona w dalszej części tego rozdziału. W przypadku ręcznego uruchamiania powyższej usługi można ją włączyć poprzez ustawienie trybu uruchomienia na *Automatyczny*. Próba zmiany stanu usługi z domyślnej wartości *Zatrzymano* na *Uruchom* wygeneruje komunikat, który przedstawia rysunek 6.19.

Rysunek 6.19. *Okno „Usługi”*

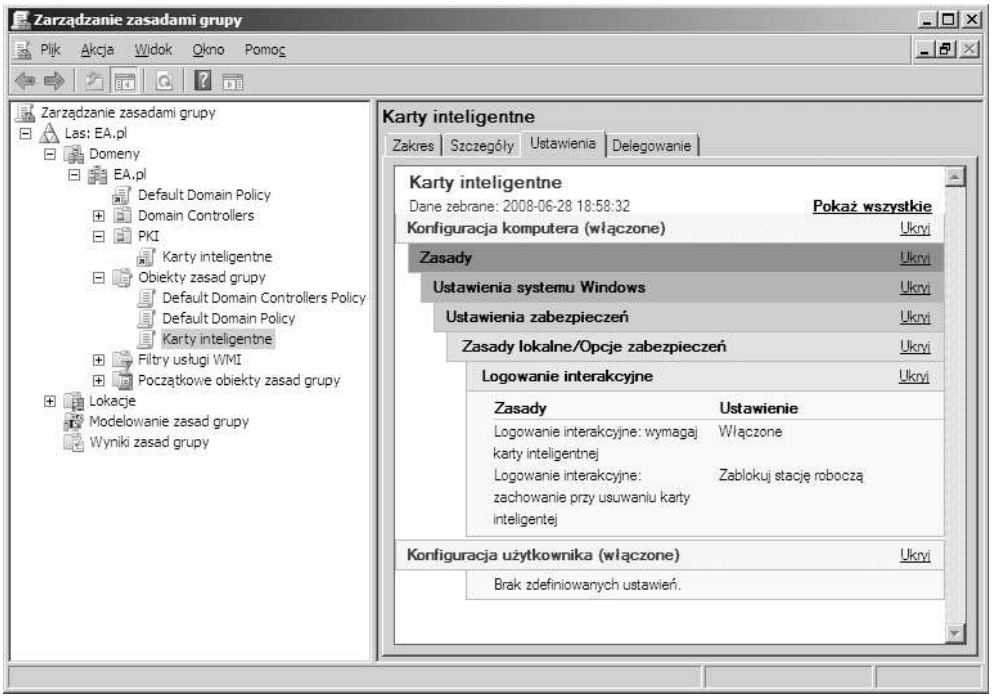


Zgodnie z komunikatem przedstawionym na rysunku 6.19, usługa *Zasady usuwania karty inteligentnej* została uruchomiona, a następnie z powrotem zatrzymana. Dlaczego tak się dzieje? Ponieważ jest ona zależna od innych usług. Można jednak wymusić włączenie powyższej usługi (bez komunikatu z rysunku 6.19) z poziomu okna *Edytor rejestru* poprzez zmianę wartości ciągu binarnego o nazwie *scremoveoption* z *0* na *1*. Wartość ta znajduje się w kluczu o nazwie *HKEY_LOCAL_MACHINE\SOFTWARE*
↪Microsoft\Windows NT\CurrentVersion\Winlogon, co przedstawia rysunek 6.20. Na potrzeby niniejszej książki usługa ta zostanie włączona za pomocą zasad grupy. Ręczne modyfikacje rejestru są niebezpieczne i należy się ich wystrzegać.



Rysunek 6.20. *Okno „Edytor rejestru”*

Wszystkie omówione w tym rozdziale ustawienia zasad grupy *Karty inteligentne* dla obiektu *PKI* (jednostki organizacyjnej o nazwie *PKI*) można sprawdzić na zakładce *Ustawienia*, przedstawionej na rysunku 6.21.



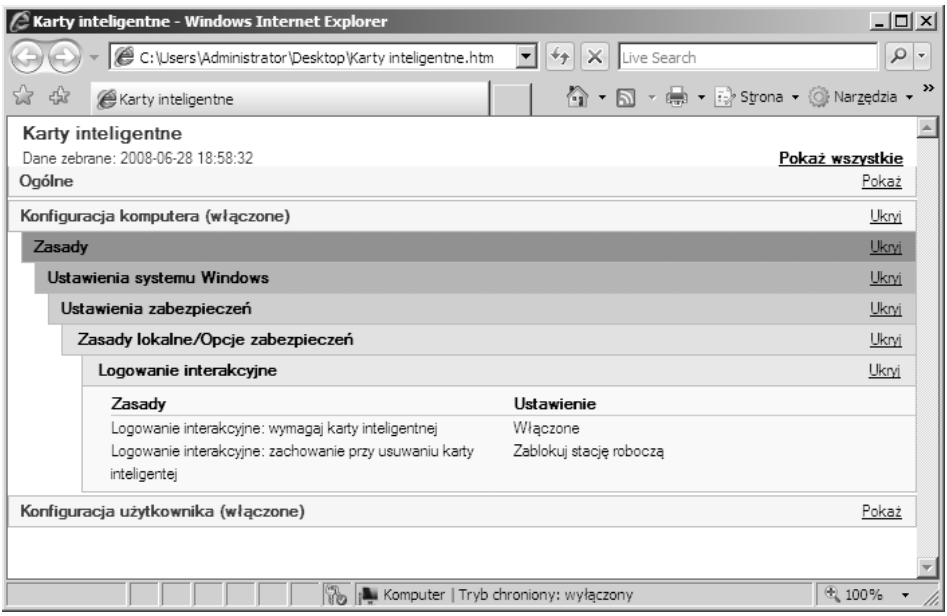
Rysunek 6.21. *Ustawienia zasad grupy „Karty inteligentne" dla obiektu PKI*

Ustawienia zasad grupy *Karty inteligentne* dla obiektu *PKI* można wyeksportować do formatu HTML (jako raport), a następnie przeglądać je za pomocą przeglądarki internetowej Internet Explorer 7, co przedstawia rysunek 6.22.

6.4. Usługi związane z kartami inteligentnymi

Najnowsze systemy operacyjne firmy Microsoft: Windows Server 2008 Standard oraz Windows Vista Business, zawierają kilka usług, które są związane z infrastrukturą klucza publicznego (PKI). Najważniejsze zostały przedstawione w tabeli 6.1 wraz z ich domyślnymi trybami uruchomienia i stanami.

Domyślny tryb uruchomienia i stany poszczególnych usług związanych z infrastruktura klucza publicznego (PKI) mogą się zmienić w zależności od potrzeb przedsiębiorstwa lub innej organizacji, o czym będzie mowa w następnych rozdziałach. Ogólnie rzecz ujmując, np. usługa o nazwie *Karta inteligentna* po zainstalowaniu sterownika



Rysunek 6.22. *Raport dla obiektu zasad grupy „Karty inteligentne”*

Tabela 6.1. *Domyślne ustawienia wybranych usług związanych z PKI*

Nazwa usługi	Opis usługi	Domyślny tryb uruchomienia	Stan usługi
Karta inteligentna (SCardSvr)	Zarządza dostępem do kart inteligentnych czytanych przez ten komputer.	Ręczny	Zatrzymano
Propagacja certyfikatu (CertPropSvc)	Propaguje certyfikaty z kart inteligentnych.	Ręczny	Zatrzymano
Zasady usuwania karty inteligentnej (SCPolicySvc)	Umożliwia skonfigurowanie systemu w taki sposób, aby po usunięciu karty inteligentnej był blokowany pulpit użytkownika.	Ręczny	Zatrzymano

czytnika kart inteligentnych na danym komputerze klienckim, serwerze członkowskim czy kontrolerze domeny zmienia automatycznie domyślny tryb uruchomienia na *Automatyczny* oraz stan na *Uruchomiono*.

6.5. Uruchamianie usługi Zasady usuwania karty inteligentnej

Jeżeli w sieci komputerowej przedsiębiorstwa lub innej organizacji korzystającej z najnowszych systemów operacyjnych firmy Microsoft: Windows Server 2008 Standard i Windows Vista Business z dodatkiem Service Pack 1, do uwierzytelniania się w domenie będą wykorzystywane karty inteligentne, na komputerach należących do sieci

trzeba uruchomić usługę o nazwie *Zasady usuwania karty inteligentnej*, o której była już wcześniej mowa. Dopóki ta usługa nie będzie uruchomiona, komputer po wyjęciu karty inteligentnej z czytnika kart inteligentnych będzie blokowany. Samo ustawienie zasady *Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej* nie wystarcza.

Usługa *Zasady usuwania karty inteligentnej* (SCPolicySvc) umożliwia skonfigurowanie najnowszych systemów operacyjnych firmy Microsoft w taki sposób, aby po usunięciu karty inteligentnej z czytnika kart inteligentnych był blokowany pulpit aktualnie zalogowanego użytkownika. W przypadku systemów operacyjnych Windows Server 2003 z dodatkiem Service Pack 2 czy Windows XP Professional z dodatkiem Service Pack 3 nie jest wymagane uruchamianie usługi *Zasady usuwania karty inteligentnej*, gdyż usługa taka nie jest w nich dostępna. Systemy automatycznie blokują komputer po wyjęciu karty inteligentnej z czytnika kart inteligentnych. Nie trzeba więc wykonywać omawianych w tym podrozdziale czynności. Wystarczy tylko dokonać ustawień zasad grupy dotyczących kart inteligentnych, które zostały przedstawione w poprzednich podrozdziałach. Odpowiednio skonfigurowane muszą być tylko najnowsze systemy operacyjne firmy Microsoft.

Jak już wcześniej wspomniano, istnieje kilka metod uruchamiania usługi *Zasady usuwania karty inteligentnej*. Można to wykonać ręcznie (na każdym komputerze wyposażonym w czytnik kart inteligentnych) z poziomu konsoli MMC o nazwie *Usługi* (ang. *Services*), którą włącza się za pomocą komendy `services.msc`. Można również skorzystać z metody automatycznej, tj. z wykorzystaniem zasad grupy, co będzie omówione dalej. To rozwiązanie jest znacznie mniej pracochłonne, co ma niebagatelne znaczenie w przypadku konfigurowania setek czy tysięcy komputerów. Wystarczy jedynie skonfigurować jedną zasadę i za pomocą usługi katalogowej Active Directory rozprowadzić ją do komputerów znajdujących się w określonej jednostce organizacyjnej.

Aby uruchomić usługi *Zasady usuwania karty inteligentnej* za pomocą zasad grupy, Administrator domeny (użytkownik *EA.pl\Andministrator*) musi wykonać następujące czynności.

1. Uruchomić konsolę *Zarządzanie zasadami grupy* (np. za pomocą komendy `gpmc.msc`), a następnie wyedytować wcześniej utworzoną zasadę grupy o nazwie *Karty inteligentne*.
2. Przejść do węzła *Usługi systemowe* i zaznaczyć w prawym oknie usługę *Zasady usuwania karty inteligentnej*, jak na rysunku 6.23.
3. Z menu *Akcja* wybrać opcję *Właściwości*.
4. Na zakładce *Ustawianie zasad zabezpieczeń* dokonać takich ustawień, jakie zostały przedstawione na rysunku 6.24, a następnie kliknąć na przycisk *OK*.
5. Zamknąć konsolę *Zarządzanie zasadami grupy*.
6. Odświeżyć zasady grupy (użytkownika i komputera) za pomocą komendy `gpupdate /force`. Komenda ta wymusza natychmiastową aktualizację zasad grupy użytkownika i komputera.