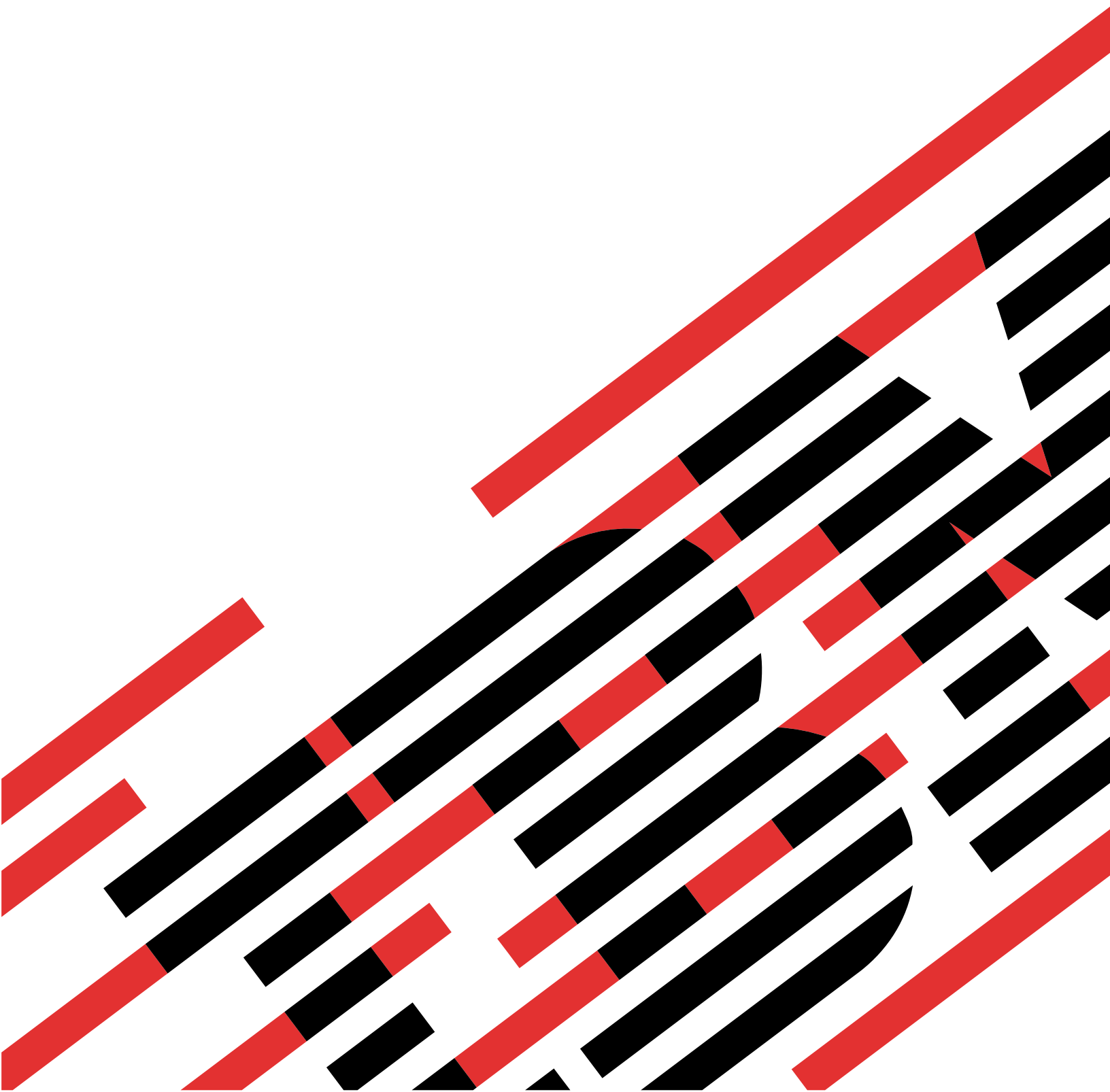


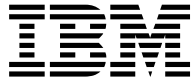
IBM

@server

iSeries

Menedżer certyfikatów cyfrowych





@server

iSeries

Menedżer certyfikatów cyfrowych

Spis treści

| | |
|--|-----------|
| Część 1. Menedżer certyfikatów cyfrowych (DCM). | 1 |
| Rozdział 1. Co nowego w wersji V5R2. | 3 |
| Rozdział 2. Drukowanie tego dokumentu | 5 |
| Rozdział 3. Migracja z wcześniejszych wersji programu DCM. | 7 |
| Rozdział 4. Scenariusze programu DCM | 9 |
| Scenariusz: korzystanie z certyfikatów w celu zabezpieczenia dostępu do aplikacji i zasobów publicznych | 9 |
| Szczegóły konfigurowania | 12 |
| Scenariusz: korzystanie z certyfikatów w celu zabezpieczenia dostępu do aplikacji i zasobów wewnętrznych | 15 |
| Szczegóły konfigurowania | 19 |
| Rozdział 5. Koncepcje dotyczące certyfikatów cyfrowych | 23 |
| Nazwa wyróżniająca | 23 |
| Podpisy cyfrowe | 24 |
| Para kluczy publiczny-prywatny | 25 |
| Zadania dotyczące ośrodka certyfikacji. | 25 |
| Położenie listy odwołań certyfikatów (CRL) | 26 |
| Bazy certyfikatów | 26 |
| Kryptografia | 27 |
| Protokół Secure Sockets Layer | 28 |
| Rozdział 6. Planowanie DCM | 29 |
| Wymagania dotyczące korzystania z programu DCM | 29 |
| Typy certyfikatów cyfrowych. | 30 |
| Certyfikaty publiczne a certyfikaty prywatne | 31 |
| Certyfikaty cyfrowe w bezpiecznej komunikacji SSL | 32 |
| Certyfikaty cyfrowe jako uwierzytelnienie użytkowników. | 33 |
| Certyfikaty cyfrowe w połączeniach VPN | 34 |
| Podpisywanie obiektów za pomocą certyfikatów cyfrowych | 35 |
| Certyfikaty cyfrowe do weryfikowania podpisów obiektów | 35 |
| Rozdział 7. Konfigurowanie programu DCM | 37 |
| Uruchomienie Menedżera certyfikatów cyfrowych (DCM) | 37 |
| Pierwsze konfigurowanie certyfikatów | 38 |
| Tworzenie i prowadzenie lokalnego ośrodka certyfikacji. | 39 |
| Zarządzanie certyfikatami użytkowników | 40 |
| Tworzenie certyfikatu użytkownika | 41 |
| Przypisanie certyfikatu użytkownika | 42 |
| Używanie funkcji API do programowego wydawania certyfikatów użytkownikom innych systemów niż iSeries | 43 |
| Uzyskanie kopii certyfikatu prywatnego ośrodka certyfikacji | 43 |
| Zarządzanie certyfikatami z publicznego internetowego ośrodka certyfikacji | 44 |
| Zarządzanie certyfikatami publicznymi dla sesji komunikacyjnych SSL | 45 |
| Zarządzanie certyfikatami publicznymi cyfrowego podpisywania obiektów | 46 |
| Zarządzanie certyfikatami publicznymi do weryfikowania podpisów obiektów | 48 |
| Rozdział 8. Zarządzanie programem DCM | 51 |
| Wykorzystanie lokalnego ośrodka certyfikacji do wystawiania certyfikatów innym systemom iSeries. | 51 |
| Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V5R2 | 54 |

| | |
|---|-----------|
| Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V5R1 | 58 |
| Wykorzystanie prywatnych certyfikatów do podpisywania obiektów w systemie docelowym V5R2 lub V5R1 | 62 |
| Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V4R5 lub V4R4 | 65 |
| Zarządzanie aplikacjami w programie DCM | 69 |
| Tworzenie definicji aplikacji | 69 |
| Zarządzanie przypisywaniem certyfikatów aplikacjom | 70 |
| Definiowanie listy zaufanych ośrodków certyfikacji dla aplikacji | 71 |
| Sprawdzanie poprawności certyfikatów i aplikacji | 72 |
| Przypisanie certyfikatu do aplikacji | 72 |
| Zarządzanie informacjami o położeniu listy CRL | 73 |
| Przechowywanie kluczy certyfikatów za pomocą koprocesora szyfrującego IBM 4758 | 74 |
| Przechowywanie klucza prywatnego certyfikatu bezpośrednio w koprocesorze | 74 |
| Korzystanie z klucza głównego koprocesora do szyfrowania klucza prywatnego certyfikatu | 75 |
| Zarządzanie miejscem położenia ośrodków certyfikacji PKIX | 75 |
| Podpisywanie obiektów | 76 |
| Weryfikowanie podpisów obiektów | 77 |
| Rozdział 9. Rozwiązywanie problemów związanych z programem DCM | 81 |
| Rozwiązywanie problemów związanych z hasłami i problemów ogólnych | 81 |
| Rozwiązywanie problemów związanych z bazami certyfikatów i bazami kluczy | 83 |
| Rozwiązywanie problemów związanych z przeglądarką | 84 |
| Rozwiązywanie problemów związanych z serwerem HTTP Server for iSeries | 85 |
| Błędy migracji i procedury odtwarzania | 87 |
| Rozwiązywanie problemów związanych z przypisywaniem certyfikatów użytkowników | 89 |
| Rozdział 10. Informacje pokrewne tematowi DCM. | 91 |

Część 1. Menedżer certyfikatów cyfrowych (DCM)

Certyfikat cyfrowy to elektroniczne świadectwo tożsamości, którego można używać w transakcjach elektronicznych. Certyfikaty cyfrowe zapewniające rozszerzone środki ochrony w sieci, znajdują coraz więcej zastosowań. Mają one na przykład podstawowe znaczenie podczas konfigurowania i korzystania z warstwy SSL (Secure Sockets Layer). Warstwa SSL umożliwia utworzenie bezpiecznego połączenia pomiędzy użytkownikami a aplikacjami serwera poprzez sieć niechronioną, na przykład Internet. Jest to jedno z najlepszych rozwiązań ochrony prywatności cennych danych, takich jak nazwy i hasła użytkowników Internetu. Usługi i aplikacje serwera iSeries, takie jak na przykład FTP, Telnet, HTTP Server for iSeries i wiele innych, obsługują warstwę SSL w celu ochrony prywatności danych.

Serwer iSeries oferuje rozbudowaną obsługę certyfikatów cyfrowych, umożliwiającą wykorzystywanie ich w roli dowodów tożsamości w wielu aplikacjach ochrony. Oprócz zastosowania certyfikatów przy konfigurowaniu SSL, można ich również użyć jako dowody tożsamości, wobec umożliwiającego identyfikację klienta w transakcjach SSL i w sieci VPN. Certyfikatów cyfrowych oraz przypisanych im kluczy blokad można użyć do oznaczania obiektów. Podpisanie obiektów oraz weryfikacja podpisów w celu sprawdzenia integralności obiektu umożliwia wykrywanie zmian lub możliwych manipulacji zawartością obiektu.

Zastosowanie Menedżera certyfikatów cyfrowych (DCM), bezpłatnej funkcji systemu iSeries do centralnego zarządzania certyfikatami na potrzeby lokalnych aplikacji, pozwala w pełni wykorzystać zalety obsługi tych certyfikatów w systemie iSeries. Program DCM służy do zarządzania certyfikatami cyfrowymi uzyskanymi z dowolnego ośrodka certyfikacji (CA). Programu można również używać do prowadzenia lokalnego ośrodka certyfikacji, w celu wystawiania prywatnych certyfikatów systemom i użytkownikom.

Podstawą skutecznego wykorzystania dodatkowych korzyści związanych z ochroną oferowaną przez certyfikaty cyfrowe jest odpowiednie planowanie i ocena. Aby dowiedzieć się więcej o działaniu certyfikatów cyfrowych i sposobach wykorzystania programu DCM do zarządzania nimi, należy przeczytać następujące sekcje:

Co nowego w wersji V5R2

Sekcja zawiera informacje o zmianach wprowadzonych w tej wersji Menedżera certyfikatów cyfrowych oraz o modyfikacjach w tematach informacyjnych.

Drukowanie tego dokumentu

Sekcja zawiera informacje o drukowaniu tego dokumentu w formacie pliku PDF.

Migracja z wcześniejszych wersji programu DCM

Sekcja zawiera informacje o czynnościach, jakie należy wykonać oraz koncepcjach, które należy zrozumieć przez przystąpieniem do migracji z używanej wersji programu DCM do wersji aktualnej.

Scenariusze programu DCM

Sekcja zawiera opis dwóch scenariuszy ilustrujących typowe schematy implementacji certyfikatów, które to scenariusze mogą pomóc w planowaniu indywidualnego wdrożenia, jako elementu strategii ochrony systemu iSeries. Każdy scenariusz zawiera wszystkie niezbędne zadania, które należy wykonać podczas konfigurowania, aby zastosować scenariusz.

Koncepcje dotyczące certyfikatów cyfrowych

Przedstawione w sekcji koncepcje i informacje pokrewne pozwalają lepiej zrozumieć, czym są certyfikaty cyfrowe i w jaki sposób działają. Sekcja zawiera również charakterystykę różnych typów certyfikatów oraz opis sposobu użycia ich jako elementu strategii ochrony.

Planowanie DCM

Informacje przedstawione w tej sekcji pomogą zdecydować, kiedy i w jaki sposób użyć certyfikatów cyfrowych, aby osiągnąć założone cele ochrony. Sekcja zawiera informacje dotyczące oprogramowania, które należy zainstalować, oraz wymagań, jakie należy spełnić przed przystąpieniem do korzystania z programu DCM.

Konfigurowanie programu DCM

Sekcja zawiera informacje o czynnościach konfigurowania, które należy wykonać, aby można było używać programu DCM do zarządzania certyfikatami i ich kluczami.

Zarządzanie programem DCM

Z sekcji można dowiedzieć się, w jaki sposób używać programu DCM do zarządzania certyfikatami i wykorzystującymi je aplikacjami. Można również dowiedzieć się, w jaki sposób cyfrowo podpisywać obiekty i jak utworzyć i prowadzić własny ośrodek certyfikacji.

Rozwiązywanie problemów związanych z programem DCM

Przedstawione informacje pozwalają nauczyć się rozwiązywać niektóre powszechne błędy, na które można się natknąć podczas korzystania z programu DCM.

Informacje pokrewne tematowi DCM

Sekcja zawiera odsyłacze do innych zasobów opisujących certyfikaty cyfrowe, strukturę kluczy publicznych, Menedżera certyfikatów cyfrowych oraz inne informacje pokrewne.


Rozdział 1. Co nowego w wersji V5R2

Do Menedżera certyfikatów cyfrowych (DCM) V5R2 oraz certyfikatów cyfrowych iSeries wprowadzone zostały następujące rozszerzenia:


- **Funkcja przypisania certyfikatu**
Jest to nowe zadanie programu DCM, umożliwiające szybsze i prostsze przypisanie certyfikatu jednej lub kilku aplikacjom. Zadanie to dostępne jest z listy zadań **Zarządzanie certyfikatami** lub z szybkiej ścieżki po wywołaniu stron **Praca z serwerem i certyfikatami** lub **Praca z certyfikatami podpisującymi obiekty**. Funkcja ta jest dostępna tylko dla bazy certyfikatów *SYSTEM oraz *OBJECTSIGNING.
- **Podpisywanie obiektów typu (*CMD)**
Programu DCM można użyć do tworzenia podpisów cyfrowych dla obiektów komend (*CMD), które to podpisy będą pełnić rolę narzędzia do sprawdzania integralności komend. Program stwarza również możliwości wyboru zakresu podpisywania obiektów *CMD. Użytkownik może za pomocą tego programu podpisać cały obiekt *CMD lub tylko kluczowe komponenty tego obiektu. Program DCM udostępnia informacje na temat zakresu podpisu podczas podglądu podpisu obiektu *CMD.
- **Funkcje API do tworzenia certyfikatu użytkownika podpisanego przez lokalny ośrodek certyfikacji bez użycia programu DCM**
Wprowadzono dwie nowe funkcje API, które można wykorzystać do programistycznego wystawiania certyfikatów - podpisanych przez lokalny ośrodek certyfikacji (CA) - użytkownikom innych systemów niż iSeries. Funkcje API umożliwiają wystawianie certyfikatów użytkownikom nieposiadającym profilu użytkownika w systemie iSeries bez konieczności uruchamiania programu DCM, który indywidualnie dla każdego użytkownika uzyskuje certyfikat uwierzytelniania klienta.

Nowości informacyjne to:

- Dwa nowe scenariusze, które mogą pomóc przy określaniu sposobu zastosowania certyfikatów do własnych, przyjętych celów ochrony.
- Przeorganizowanie informacji, dzięki czemu łatwiejsze staje się ich szybkie odszukanie podczas korzystania z programu DCM.


Informacje o tym, co zostało w tej wersji dodane lub rozszerzone można znaleźć w dokumencie *Informacje dla użytkowników* .

Rozdział 2. Drukowanie tego dokumentu

Aby wyświetlić lub pobrać wersję PDF, należy wybrać Menedżer certyfikatów cyfrowych  (plik wielkości 468 KB lub około 110 stron).

Aby zapisać plik PDF na stacji roboczej do przeglądania lub wydruku:

1. Otwórz plik PDF w przeglądarce (kliknij odsyłacz powyżej).
2. W menu przeglądarki kliknij **Plik**.
3. Kliknij **Zapisz jako...**
4. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
5. Kliknij **Zapisz**.

Jeśli do przeglądania lub drukowania wymaga się programu Adobe Acrobat, można go pobrać z serwisu WWW firmy Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Rozdział 3. Migracja z wcześniejszych wersji programu DCM

Podczas migracji z wersji V4R3 programu Menedżer certyfikatów cyfrowych (DCM) do wersji V5R2 program DCM automatycznie aktualizuje istniejący lokalny ośrodek certyfikacji (CA) i pliki kluczy certyfikatów systemu. Program DCM aktualizuje pliki, które noszą nazwę default.kyr, przekształcając je na odpowiednie pliki bazy certyfikatów o nazwie default.kdb. Ponadto program DCM dokonuje migracji wszystkich prawidłowych certyfikatów z plików kluczy powiązanych z serwerami Hypertext Transfer Protocol (HTTP) i Lightweight Directory Access Protocol (LDAP). Kierunkiem tej migracji jest baza certyfikatów *SYSTEM (default.kdb).

Uwaga: W przypadku migracji z wersji V4R4, V4R5 lub V5R1 programu DCM nie ma potrzeby wykonywania żadnych czynności związanych z migracją, ponieważ pliki certyfikatów z tych wersji są zgodne z wersją V5R2 programu DCM.

Migracja pliku kluczy do bazy certyfikatów – migracja z wersji V4R3

Podczas instalacji programu DCM w wersji V5R2 system dokonuje migracji następujących plików kluczy:

- domyślnego pliku kluczy programu DCM,
- pliku kluczy używanego przez pliki konfiguracyjne serwera HTTP,
- pliku kluczy używanego przez pliki konfiguracyjne serwera LDAP.

Jeśli przy pierwszym uruchomieniu programu DCM skorzysta się z pliku .kyr, który nie został automatycznie zaktualizowany, program zamieni go w plik kyr.kdb. Jeśli na przykład, po raz pierwszy poda się nazwę pliku secure.kyr w interfejsie użytkownika programu DCM, program dokona konwersji tego pliku na nową bazę certyfikatów, której plik będzie nosił nazwę secure.kyr.kdb.

Uwaga: Pliki kluczy różnią się od baz certyfikatów, dlatego te pliki, których program DCM nie zaktualizował automatycznie, należy przekształcić, korzystając z interfejsu użytkownika w programie DCM. Ręczna zmiana rozszerzenia nazw plików na .kdb spowoduje błędy przy próbie pracy z tymi plikami w programie DCM.

Przy próbie usunięcia pliku secure.kyr program DCM archiwizuje go, usuwając w rzeczywistości plik secure.kyr.kdb.

Hasło domyślnej bazy certyfikatów

Jeśli plik /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR istnieje, system migruje ten plik kluczy i pozostaje do bazy certyfikatów *SYSTEM. Oryginalne hasło powiązane z plikiem /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR staje się hasłem do bazy certyfikatów *SYSTEM.

Jeśli plik /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR nie istnieje, ale są inne pliki kluczy gotowe do migracji (na przykład pliki kluczy używane przez pliki konfiguracyjne serwera HTTP), system tworzy bazę *SYSTEM z hasłem DEFAULT (wielkie litery) i kończy migrację.

Informacje o błędach, które mogą wystąpić podczas procesu migracji plików, oraz o sposobach ich usuwania można znaleźć w sekcji Błędy migracji i procedury odtwarzania.

Rozdział 4. Scenariusze programu DCM

Menedżer certyfikatów cyfrowych oraz obsługa certyfikatów cyfrowych w systemie iSeries udostępniają wiele sposobów wykorzystania certyfikatów do udoskonalenia strategii ochrony. Sposób wykorzystania certyfikatów zależy od rodzaju prowadzonej działalności oraz wymagań ochrony.

Zastosowanie certyfikatów cyfrowych poprawia ochronę na wiele sposobów. Umożliwiają one stosowanie protokołu Secure Sockets Layer (SSL) do chronionego dostępu do serwerów WWW i innych usług internetowych. Można ich użyć do skonfigurowania połączeń w wirtualnych sieciach prywatnych (VPN). Można również użyć kluczy certyfikatów do cyfrowego podpisywania obiektów lub do sprawdzania cyfrowych podpisów obiektów w celu ustalenia ich autentyczności. Takie podpisy cyfrowe zapewniają wiarygodność pochodzenia obiektów i chronią ich integralność.

Jeśli używa się certyfikatów cyfrowych (zamiast nazw użytkowników i haseł), ochronę systemu można rozszerzyć o uwierzytelnianie i autoryzowanie sesji pomiędzy serwerem a użytkownikami. Można także użyć programu DCM do powiązania certyfikatu użytkownika z profilem tego użytkownika w systemie iSeries. W rezultacie, certyfikat otrzymuje te same uprawnienia i prawa dostępu, co profil, do którego został przypisany.

Wybór certyfikatów może być skomplikowany i uzależniony od wielu czynników. Opisane w tej sekcji scenariusze opisują kilka celów ochrony z wykorzystaniem certyfikatów cyfrowych w typowych sytuacjach biznesowych. Scenariusze zawierają wszystkie szczegóły dotyczące niezbędnego sprzętu i oprogramowania, które należy posiadać, aby zastosować dany scenariusz. Przejrzenie poniższych scenariuszy pomoże w określeniu sposobu wykorzystania certyfikatów do poprawy bezpieczeństwa:

Scenariusz: korzystanie z certyfikatów w celu zabezpieczenia dostępu do aplikacji i zasobów publicznych

Scenariusz ten opisuje, kiedy i w jaki sposób należy wykorzystać certyfikaty w celu zabezpieczenia i ograniczenia dostępu użytkownikom publicznym do aplikacji i zasobów publicznych i ekstranetowych.

Scenariusz: korzystanie z certyfikatów w celu zabezpieczenia dostępu do aplikacji i zasobów internetowych

Scenariusz ten opisuje, kiedy i w jaki sposób należy wykorzystać certyfikaty w celu zabezpieczenia i ograniczenia dostępu użytkownikom wewnętrznym do aplikacji i zasobów na serwerze wewnętrznym.

Scenariusz: korzystanie z certyfikatów w celu zabezpieczenia dostępu do aplikacji i zasobów publicznych

Opis sytuacji

Administrator w firmie ubezpieczeniowej jest odpowiedzialny za obsługę różnych aplikacji na firmowych serwerach intranetowych i ekstranetowych. Jedną z aplikacji, za którą odpowiada, jest aplikacja do obliczania składek, której dowolna liczba agentów ubezpieczeniowych może używać do przedstawiania odpowiednich kwot swoim klientom. Informacje, które udostępnia ta aplikacja, są dość istotne, dlatego też administrator chce mieć pewność, że mogą z niej korzystać tylko zarejestrowani agenci. Administrator chce również udostępnić bezpieczniejszą, niż metoda podawania nazwy użytkownika i hasła, metodę dostępu użytkowników do aplikacji. Przy aktualnej strategii ochrony istnieje niebezpieczeństwo nieuprawnionego dostępu do informacji podczas przesyłania ich przez sieć, która nie jest traktowana jako zaufana. Również agenci mogą udzielać sobie na wzajem informacji bez przeprowadzania autoryzacji.

Po przeanalizowaniu sytuacji zdecydowano, że korzystanie z certyfikatów cyfrowych może zapewnić odpowiednią ochronę. Korzystanie z certyfikatów umożliwia zastosowanie protokołu SSL w celu zabezpieczenia przesyłania danych dotyczących składek. Zarówno przedsiębiorstwo, jak i agenci będą potrzebowali czasu, zanim wszystkie cele dotyczące bezpieczeństwa zostaną zrealizowane. W tym okresie,

w dalszym ciągu stosować się będzie metodę uwierzytelniania poprzez podawanie nazwy użytkownika oraz hasła, co pozwoli protokołowi SSL zabezpieczyć dane podczas ich przesyłania.

Ze względu na rodzaj aplikacji, jej użytkowników oraz przyszły cel uwierzytelniania certyfikatów użytkowników, administrator zdecydował się na korzystanie z certyfikatu publicznego otrzymanego ze znanego ośrodka certyfikacji (CA) w celu skonfigurowania dla aplikacji połączeń SSL.

Zalety rozwiązania opisanego w scenariuszu

Można wymienić następujące zalety:

- Korzystanie z certyfikatów cyfrowych w celu skonfigurowania dostępu SSL do aplikacji wyliczającej składki daje pewność, że informacje przesyłane pomiędzy serwerem a klientem są zabezpieczone i nie zostaną upublicznione.
- Korzystanie zawsze kiedy to tylko możliwe z certyfikatów cyfrowych do uwierzytelniania klientów jest najbezpieczniejszą metodą identyfikacji autoryzowanych użytkowników. Jeśli korzystanie z tych certyfikatów nie jest możliwe, uwierzytelnianie klienta następuje tylko przez nazwę użytkownika i hasło, a sesja SSL zapewnia bezpieczeństwo i zachowanie prywatności ID i hasła użytkownika, co czyni wymianę istotnych informacji w dalszym ciągu bezpieczną.
- Korzystanie z *publicznych* certyfikatów cyfrowych w celu umożliwienia dostępu do aplikacji i danych jest rozwiązaniem praktycznym, o ile spełnione są wymienione poniżej lub zbliżone do nich warunki:
 - dane i aplikacje wymagające różnych poziomów ochrony,
 - występowanie dużej fluktuacji kadr wśród zaufanych użytkowników,
 - aplikacje i dane, na przykład internetowy serwis WWW lub aplikacja ekstranetowa, są udostępniane publicznie,
 - nie zamierza się prowadzić własnego ośrodka certyfikacji (CA) ze względu na dużą liczbę użytkowników, którzy mają dostęp do aplikacji lub zasobów, lub ze względu na inne przyczyny natury administracyjnej.
- Korzystanie z certyfikatów publicznych w celu skonfigurowania aplikacji przeliczającej składki do korzystania z połączenia SSL zmniejsza liczbę czynności konfiguracyjnych, które będą musieli wykonać użytkownicy, aby uzyskać dostęp do tej aplikacji. Większość oprogramowania typu klient zawiera certyfikaty powszechnie znanych ośrodków certyfikacji (CA).

Cele

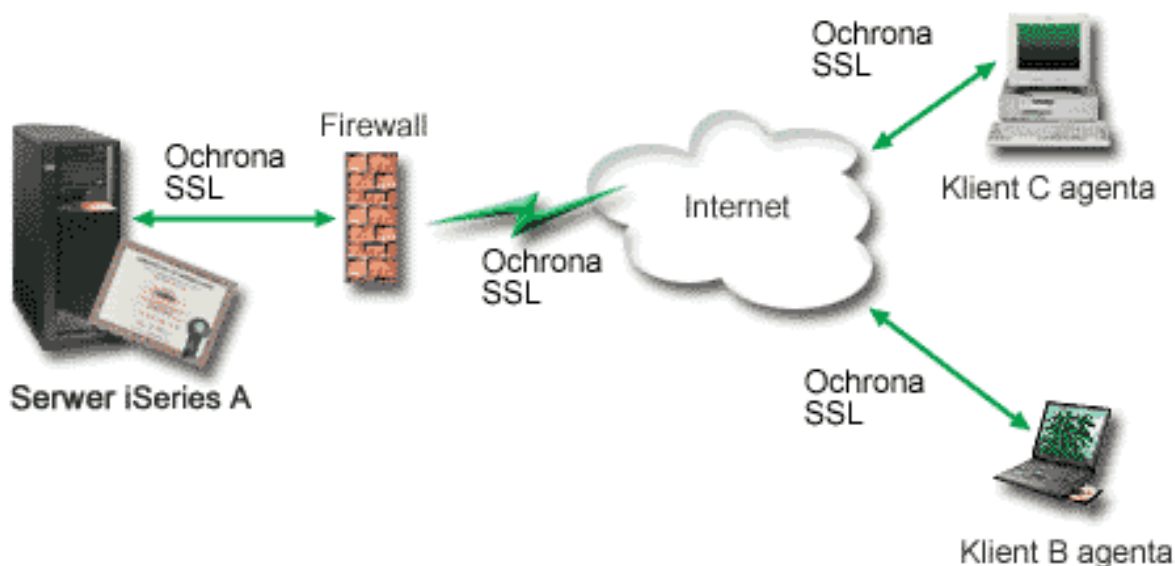
Firma ubezpieczeniowa będzie używała certyfikatów cyfrowych w celu zabezpieczenia zgromadzonych w aplikacji informacji dotyczących przeliczanych składek, które to informacje dostępne są autoryzowanym publicznym użytkownikom. Przedsiębiorstwo chce zapewnić wyższy poziom bezpieczeństwa przez zastosowanie metody uwierzytelniania użytkowników, którzy mają dostęp do aplikacji.

Wymagania związane z wprowadzeniem metody zaproponowanej w scenariuszu:

- Wykorzystywana w przedsiębiorstwie aplikacja przeliczania składek musi używać protokołu SSL w celu zabezpieczenia prywatności danych udostępnianych użytkownikom.
- Konfigurację SSL należy zrealizować, wykorzystując certyfikaty z powszechnie znanego, publicznego, internetowego ośrodka certyfikacji (CA).
- Aby uzyskać dostęp do aplikacji w trybie SSL, autoryzowani użytkownicy muszą podać poprawną nazwę użytkownika oraz hasło. Użytkownicy ci muszą również korzystać z jednej z dwóch metod bezpiecznego uwierzytelniania. Agenci muszą przedstawić albo publiczny certyfikat cyfrowy powszechnie znanego ośrodka certyfikacji (CA) albo poprawną nazwę użytkownika i hasło.

Szczegóły

Rysunek przedstawia konfigurację sieci zastosowaną w tym scenariuszu:



Na rysunek składają się następujące elementy:

Serwer publiczny przedsiębiorstwa – serwer iSeries A

- Serwer iSeries A udostępnia aplikację przeliczania składek stosowaną w przedsiębiorstwie.
- Na serwerze iSeries A działa system OS/400 wersja 5 wydanie 2 (V5R2).
- Na serwerze iSeries A jest zainstalowany program szyfrujący (5722-AC3).
- Na serwerze iSeries A jest zainstalowany i skonfigurowany Menedżer certyfikatów cyfrowych (opcja 34 systemu OS/400) oraz serwer IBM HTTP Server for iSeries (5722-DG1).
- Na serwerze iSeries A działa aplikacja wyliczająca składki, która:
 - wymaga trybu SSL,
 - do konfigurowania SSL korzysta z certyfikatu publicznego powszechnie znanego ośrodka certyfikacji (CA),
 - wymaga uwierzytelniania za pomocą nazwy użytkownika i hasła.
- Gdy klienci B i C chcą uzyskać dostęp do aplikacji, serwer iSeries A przedstawia swój certyfikat w celu rozpoczęcia sesji SSL.
- Po zainicjowaniu sesji SSL a przed umożliwieniem dostępu do aplikacji wyliczającej składki, serwer iSeries A wysyła zapytanie do klientów B i C, aby podali poprawne nazwy użytkowników i hasła.

Systemy klienckie agenta – klient B i klient C

- Klienci B i C są niezależnymi agentami, którzy mają dostęp do aplikacji przeliczającej składki.
- Klienci B i C mają kopię powszechnie znanego ośrodka certyfikacji (CA), który dla aplikacji wystawił certyfikat zainstalowany z oprogramowaniem klienckim.
- Klienci B i C uzyskują dostęp do aplikacji przeliczającej składki na serwerze iSeries A, który przedstawia swój certyfikat oprogramowaniu klienckiemu agentów w celu zweryfikowania swojej tożsamości i nawiązania sesji SSL.
- Oprogramowanie klienckie w systemach klientów B i C jest skonfigurowane tak, aby akceptować certyfikat przekazany z serwera iSeries A oraz rozpocząć sesję SSL.
- Po rozpoczęciu sesji SSL, aby serwer iSeries A umożliwił dostęp do aplikacji wyliczającej składki, klienci B i C muszą podać poprawne nazwy użytkowników i hasła.

Wymagania wstępne i założenia

Można wymienić następujące wymagania wstępne i założenia:

1. Aplikacja przeliczania składek na serwerze iSeries A jest dowolną aplikacją, która może korzystać z protokołu SSL. Większość aplikacji, w tym wiele aplikacji iSeries, udostępnia obsługę SSL. Kroki, które

należy wykonać, aby skonfigurować połączenie SSL, różnią się w zależności od aplikacji. Dlatego też, przedstawiony scenariusz nie zawiera konkretnych instrukcji, jakie należy zrealizować podczas konfigurowania połączenia SSL dla aplikacji przeliczania składek. Zamieszczone są natomiast instrukcje, które należy wykonać podczas konfigurowania i zarządzania certyfikatami, które są niezbędne, aby aplikacja mogła używać połączenia SSL.

2. *Opcjonalnie*, aplikacja przeliczania składek udostępnia możliwość uwierzytelniania klienta po podaniu certyfikatu. Scenariusz ten zawiera również instrukcje, w jaki sposób użyć Menedżera certyfikatów cyfrowych (DCM) do takiego ustawienia uwierzytelniania, aby serwer akceptował certyfikaty przydzielone aplikacjom. Kroki, które należy wykonać, aby skonfigurować uwierzytelnianie klienta, różnią się w zależności od aplikacji. Z tego powodu przedstawiony scenariusz nie zawiera konkretnych instrukcji, jakie należy wykonać podczas konfigurowania uwierzytelniania w celu akceptacji certyfikatu klienta dla aplikacji przeliczania składek.
3. Serwer iSeries A spełnia wszystkie wymagania niezbędne do zainstalowania i używania Menedżera certyfikatów cyfrowych (DCM).
4. Na serwerze iSeries A nie był wcześniej konfigurowany ani używany program DCM.
5. Aby użytkownicy mogli zrealizować zadania przewidziane w scenariuszu, ich profile związane z programem DCM muszą posiadać uprawnienia specjalne *SECADM i *ALLOBJ.
6. W serwerze iSeries A nie jest zamontowany koprocesor szyfrujący IBM 4758-023 PCI.

Kroki zadania

Na serwerze iSeries A należy wykonać następujące zadania:

1. Aby zainstalować i skonfigurować wszystkie niezbędne produkty iSeries, zrealizuj wszystkie kroki niezbędne, aby spełnić wymagania wstępne.
2. Aby utworzyć zgłoszenie certyfikatu serwera, użyj Menedżera certyfikatów cyfrowych (DCM).
3. Skonfiguruj aplikację, aby korzystała z protokołu Secure Sockets Layer (SSL).
4. Użyj programu DCM, aby zaimportować podpisany certyfikat serwera lub klienta a następnie przypisać go do ID aplikacji.
5. Jeśli jest to konieczne, uruchom aplikację w trybie SSL.
6. *Zadanie opcjonalne*: za pomocą programu DCM zdefiniuj listę zaufanych ośrodków certyfikacji, w celu umożliwienia uwierzytelniania klienta w oparciu o certyfikaty aplikacji udostępniającej taką obsługę.

Uwaga: Scenariusz nie wymaga, aby aplikacja przeliczania składek korzystała z certyfikatów do uwierzytelniania klienta. Wiele aplikacji obsługuje uwierzytelnianie klienta za pomocą certyfikatu; sposób skonfigurowania tej usługi jest różny dla różnych aplikacji. Przedstawione zadanie opcjonalne pomaga zrozumieć sposób wykorzystania programu DCM do okazania zaufania certyfikatowi podczas uwierzytelniania klienta, jako podstawy konfigurowania aplikacji do obsługi uwierzytelniania klienta za pomocą certyfikatu.

Szczegóły konfigurowania

Aby użyć certyfikatów do skonfigurowania zabezpieczonego, publicznego dostępu do aplikacji i zasobów, wykonaj opisane zadania:

Krok 1: Aby zainstalować wszystkie niezbędne produkty iSeries, należy zakończyć zadania dotyczące wymagań wstępnych

Aby zainstalować i skonfigurować wszystkie niezbędne produkty iSeries, zanim będzie możliwe wykonanie specyficznych zadań konfigurowania w celu zastosowania scenariusza, zrealizuj wszystkie kroki niezbędne, aby spełnić wymagania wstępne.

Krok 2: Utworzenie zgłoszenia certyfikatu serwera lub klienta

Aby można było używać protokołu Secure Sockets Layer (SSL) w celu zabezpieczenia danych aplikacji, należy najpierw uzyskać certyfikat cyfrowy publicznego ośrodka certyfikacji (CA). Zgłoszenie zawierające informacje wymagane przez publiczny ośrodek certyfikacji (CA) do wystawienia certyfikatu można utworzyć przy użyciu Menedżera certyfikatów cyfrowych (DCM).

Aby rozpocząć procedurę uzyskania certyfikatu, wykonaj następujące kroki:

1. Uruchom program DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie nowej bazy certyfikatów**, aby rozpocząć procedurę i wypełnić szereg formularzy. Formularze te prowadzą przez proces tworzenia bazy certyfikatów i certyfikatu, którego aplikacje będą mogły używać podczas sesji SSL.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

3. Zaznacz ***SYSTEM** jako bazę certyfikatów, która ma zostać utworzona, i kliknij **Kontynuuj**.
4. Wybierz **Tak**, aby utworzyć certyfikat jako część bazy certyfikatów, i kliknij **Kontynuuj**.
5. Jako ośrodek podpisujący nowy certyfikat wybierz **VeriSign lub inny internetowy ośrodek certyfikacji** i kliknij **Kontynuuj**, aby wyświetlić formularz pozwalający podać informacje identyfikujące dla nowego certyfikatu.
6. Wypełnij formularz i kliknij **Kontynuuj**, aby wyświetlić stronę potwierdzenia. Na stronie tej wyświetlane są dane do wniosku, który należy dostarczyć do ośrodka certyfikacji (CA) wystawiającego certyfikat. Dane Certificate Signing Request (CSR) zawierają klucz publiczny i inne informacje podane w certyfikacie.
7. Uważnie skopiuuj dane CSR i wklej je do formularza wniosku o certyfikat lub do osobnego pliku wymaganego przez ośrodek publiczny przy występowaniu o certyfikat. Należy użyć wszystkich danych CSR, w tym również wierszy Początek wniosku o nowy certyfikat i Koniec wniosku o nowy certyfikat. Po zamknięciu tej strony dane zostaną utracone i nie będzie można ich odtworzyć.
8. Formularz wniosku lub plik należy wysłać do wybranego ośrodka certyfikacji (CA), który ma wystawić i podpisać certyfikat.
9. Następny krok zadania można rozpocząć dopiero po odesłaniu przez ośrodek podpisanego, wypełnionego certyfikatu.

Po odesłaniu przez ośrodek podpisanego, wypełnionego certyfikatu można rozpocząć: konfigurowanie aplikacji do korzystania z połączenia SSL, import certyfikatu do bazy certyfikatów *SYSTEM oraz przypisanie certyfikatu do aplikacji, aby używała połączenia SSL.

Krok 3: Konfigurowanie aplikacji do korzystania z połączenia SSL

Po otrzymaniu z publicznego ośrodka certyfikacji (CA) podpisanego, wypełnionego certyfikatu można kontynuować czynności związane z uruchamianiem komunikacji Secure Sockets Layer (SSL) dla aplikacji. Przed rozpoczęciem pracy z podpisanym certyfikatem należy skonfigurować aplikację, aby używała połączenia SSL. Podczas konfigurowania niektóre programy jak np. serwer HTTP Server for iSeries generują unikalne ID aplikacji i rejestrują je korzystając z Menedżera certyfikatów cyfrowych. Aby przypisać podpisany certyfikat aplikacji i zakończyć proces konfigurowania SSL, należy znać ID aplikacji przed uruchomieniem programu DCM.

Sposób konfigurowania aplikacji do korzystania z połączenia SSL zależy od aplikacji. W scenariuszu nie zakładano, że aplikacja do przeliczania składek, będzie pochodziła z jakiegoś konkretnego źródła, ponieważ firma ubezpieczeniowa może dostarczyć taką aplikację swoim agentom w różny sposób.

Aby skonfigurować aplikację do korzystania z połączenia SSL, należy postępować zgodnie z instrukcjami zamieszczonymi w dokumentacji aplikacji. Więcej informacji na temat konfigurowania połączenia SSL dla aplikacji IBM zawiera temat Ochrona aplikacji przy użyciu połączenia SSL w Centrum informacyjnym.

Krok 4: Import i przypisanie podpisanego certyfikatu publicznego

Po skonfigurowaniu aplikacji, tak aby używała połączenia SSL, można użyć programu DCM do importu podpisanego certyfikatu oraz przypisania certyfikatu do aplikacji.

Aby zaimportować certyfikat oraz przypisać go do aplikacji, co zakończy konfigurowanie SSL, wykonaj następujące kroki:

1. Uruchom program DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
4. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Import certyfikatu**, aby rozpocząć proces importowania podpisanego certyfikatu do bazy certyfikatów *SYSTEM.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

6. Na liście zadań **Zarządzanie certyfikatami** zaznacz **Przypisanie certyfikatu**, aby wyświetlić listę certyfikatów w bieżącej bazie certyfikatów.
7. Zaznacz certyfikat na liście i kliknij **Przypisanie do aplikacji**, aby wyświetlić listę definicji aplikacji dla bieżącej bazy certyfikatów.
8. Zaznacz aplikację na liście i kliknij **Kontynuuj**. Wyświetlony zostanie komunikat potwierdzający wybranie przypisania lub komunikat o błędzie, jeśli pojawią się problemy.

Jeśli zadanie zostało zakończone, można uruchomić aplikację w trybie SSL i rozpocząć ochronę prywatności dostarczanych przez nią danych.

Krok 5: Uruchomienie aplikacji w trybie SSL

Po zakończeniu importu i przypisaniu certyfikatu do aplikacji, może być konieczne zamknięcie aplikacji i uruchomienie jej ponownie w trybie SSL. Wykonanie tych czynności jest konieczne w niektórych przypadkach, ponieważ gdy aplikacja jest uruchomiona, może nie być w stanie sprawdzić, czy istnieje przypisanie certyfikatu. Informacje o tym, czy konieczne jest ponowne uruchomienie aplikacji, oraz inne informacje dotyczące uruchamiania aplikacji w trybie SSL zawiera dokumentacja aplikacji.

Opcjonalny krok 6: Definiowanie listy zaufanych ośrodków certyfikacji (CA) dla aplikacji wymagającej certyfikatu do uwierzytelniania klienta

Aplikacje obsługujące certyfikaty do uwierzytelniania klienta podczas sesji Secure Sockets Layer (SSL) muszą określić, czy zaakceptować certyfikat jako prawidłowy dowód tożsamości. Jednym z kryteriów stosowanych przez aplikację jest ocena, czy uwierzytelniany certyfikat został wystawiony przez zaufany ośrodek certyfikacji (CA).

Scenariusz nie wymaga, aby aplikacja do przeliczania składek korzystała z certyfikatów do uwierzytelniania klienta. Wiele aplikacji obsługuje uwierzytelnianie klienta za pomocą certyfikatu; sposób skonfigurowania tej usługi jest różny dla różnych aplikacji. Przedstawione zadanie opcjonalne pomaga zrozumieć sposób wykorzystania programu DCM do okazania zaufania certyfikatowi używanemu podczas uwierzytelniania klienta, jako podstawy w trakcie konfigurowania aplikacji do korzystania z certyfikatu podczas uwierzytelniania klienta.

Przed zdefiniowaniem listy zaufanych ośrodków certyfikacji (CA) należy spełnić kilka warunków:

- aplikacja musi obsługiwać uwierzytelnianie klienta,
- w programie DCM, w definicji aplikacji należy podać, że aplikacja korzysta z listy zaufanych ośrodków certyfikacji (CA).

Jeśli w definicji aplikacji podano, że aplikacja używa listy zaufanych ośrodków certyfikacji (CA), aplikacja będzie mogła pomyślnie uwierzytelnić klienta dopiero po zdefiniowaniu tej listy. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Aby dla aplikacji zdefiniować listę zaufanych ośrodków certyfikacji (CA) wykorzystując program DCM, wykonaj następujące czynności:

1. Uruchom program DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
4. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
5. Na liście zadań zaznacz **Ustawianie statusu ośrodka certyfikacji**, aby wyświetlić listę certyfikatów ośrodka certyfikacji (CA).

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

6. Na liście zaznacz certyfikat ośrodka certyfikacji (CA), któremu powinna ufać aplikacja, i kliknij **Aktywuj**, aby wyświetlić listę aplikacji, które korzystają z listy zaufania ośrodków certyfikacji (CA).
7. Na liście zaznacz aplikację, do której należy dodać zaznaczony ośrodek certyfikacji (CA) do listy zaufania, i kliknij **OK**. W górnej części strony wyświetlony zostanie komunikat informujący, że zaznaczona aplikacja będzie ufać ośrodkowi certyfikacji (CA) oraz wydanym przez ten ośrodek certyfikatom.

Teraz można rozpocząć konfigurowanie aplikacji do uwierzytelniania klienta przez sprawdzanie certyfikatów. Informacje na ten temat zawiera dokumentacja aplikacji.

Scenariusz: korzystanie z certyfikatów w celu zabezpieczenia dostępu do aplikacji i zasobów wewnętrznych

Opis sytuacji

Administrator sieci troszczy się zwykle o takie sprawy, jak zgodność z prawem i zachowanie prywatności danych. Pracownicy przedsiębiorstwa zgłosili, że chcą mieć dostęp online do informacji dotyczących wynagrodzenia i ochrony zdrowia. Przedsiębiorstwo odpowiedziało pozytywnie na te prośby i utworzono wewnętrzny serwis WWW udostępniający te informacje. Za zarządzanie tym serwisem odpowiedzialny jest administrator sieci.

Pracownicy pracują w dwóch oddalonych biurach, a część z nich często podróżuje, dlatego też konieczne jest zachowanie prywatności informacji przesyłanych siecią Internet. Ograniczenie dostępu do danych przedsiębiorstwa uzyskuje się na podstawie uwierzytelniania przez podanie nazwy użytkownika i hasła. Jednak tego rodzaju ograniczenie dostępu może być niewystarczające. Pracownicy mogą przecież zapomnieć hasła, przekazać je innemu pracownikowi czy nawet je ukraść.

Po przeanalizowaniu sytuacji zdecydowano, że korzystanie z certyfikatów cyfrowych może zapewnić odpowiednią ochronę. Korzystanie z certyfikatów umożliwi zastosowanie protokołu SSL w celu zabezpieczenia przesyłania danych. Dodatkowo, aby bezpieczniej uwierzytelnić użytkowników oraz ograniczyć dostęp do danych osobowych, można zastosować certyfikaty zamiast haseł.

Z tego powodu należy podjąć decyzję o utworzeniu prywatnego, lokalnego ośrodka certyfikacji (CA) i wystawieniu certyfikatów wszystkim pracownikom. Ten typ implementacji certyfikatów prywatnych umożliwia bardziej rygorystyczną kontrolę dostępu do istotnych informacji, a także kontrolę prywatności danych za

pomocą protokołu SSL. Z pewnością samodzielne wystawianie certyfikatów zwiększa szanse, że dane pozostaną bezpieczne i będą dostępne tylko konkretnym osobom.

Zalety rozwiązania opisanego w scenariuszu

Można wymienić następujące zalety:

- Korzystanie z certyfikatów cyfrowych w celu skonfigurowania dostępu SSL do serwera WWW obsługującego dane osobowe daje pewność, że informacje przesyłane pomiędzy serwerem a klientem są zabezpieczone i nie zostaną upublicznione.
- Korzystanie z certyfikatów cyfrowych do uwierzytelniania klientów jest najbezpieczniejszą metodą identyfikacji autoryzowanych użytkowników.
- Korzystanie z *prywatnych* certyfikatów cyfrowych w celu umożliwienia dostępu do aplikacji i danych jest rozwiązaniem praktycznym, o ile spełnione są wymienione poniżej lub zbliżone do nich warunki:
 - wysoki poziom ochrony, szczególnie w odniesieniu do uwierzytelniania użytkowników,
 - certyfikaty otrzymują tylko zaufane osoby,
 - użytkownicy mają już profile użytkowników, umożliwiające kontrolowanie ich dostępu do aplikacji i danych,
 - zamierza się poprowadzić własny ośrodek certyfikacji.
- Korzystanie z certyfikatów prywatnych do uwierzytelniania klienta ułatwia powiązanie certyfikatu z profilem autoryzowanego użytkownika w systemie iSeries. Powiązanie certyfikatu z profilem użytkownika podczas uwierzytelniania umożliwia serwerowi HTTP określenie profilu użytkownika właściciela certyfikatu. Serwer HTTP może przełączyć się do tego profilu i działać lub wykonać akcje na podstawie informacji w nim zgromadzonych.

Cele

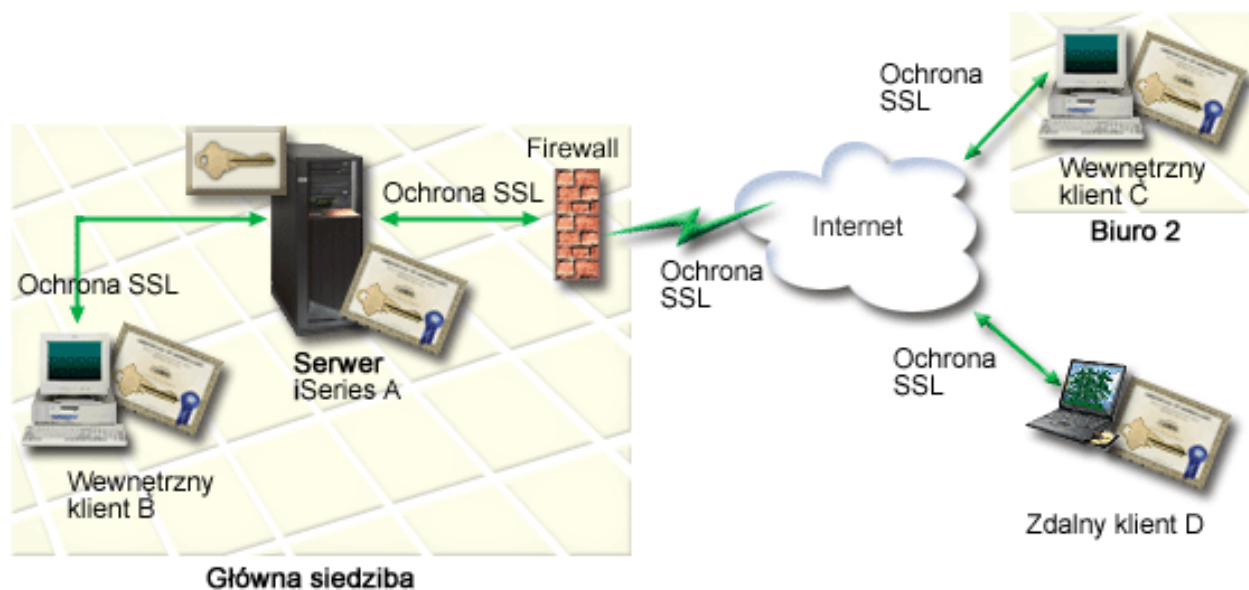
Firma ubezpieczeniowa będzie używała certyfikatów cyfrowych w celu zabezpieczenia zgromadzonych danych osobowych, które dostępne są w serwisie WWW danych osobowych dla pracowników przedsiębiorstwa. Przedsiębiorstwo chce zapewnić wyższy poziom bezpieczeństwa, stosując metodę uwierzytelniania użytkowników, którzy mają dostęp do serwisu WWW.

Wymagania związane z wprowadzeniem metody zaproponowanej w scenariuszu:

- Wykorzystywany w przedsiębiorstwie wewnętrzny serwis WWW danych osobowych musi używać protokołu SSL w celu zabezpieczenia prywatności danych udostępnianych użytkownikom.
- Konfigurację SSL należy zrealizować, wykorzystując prywatne certyfikaty z wewnętrznego, lokalnego ośrodka certyfikacji (CA).
- Aby uzyskać dostęp do serwisu WWW w trybie SSL, autoryzowani użytkownicy muszą podać poprawny certyfikat.

Szczegóły

Rysunek przedstawia konfigurację sieci zastosowaną w tym scenariuszu:



Na rysunek składają się następujące elementy:

Serwer WWW obsługujący dane osobowe pracowników przedsiębiorstwa – serwer iSeries A

- Serwer iSeries A udostępnia sieciową aplikację obsługującą dane osobowe pracowników przedsiębiorstwa.
- Na serwerze iSeries A działa system OS/400 wersja 5 wydanie 2 (V5R2).
- Na serwerze iSeries A jest zainstalowany program szyfrujący (5722-AC3).
- Na serwerze iSeries A jest zainstalowany i skonfigurowany Menedżer certyfikatów cyfrowych (opcja 34 systemu OS/400) oraz serwer IBM HTTP Server for iSeries (5722-DG1).
- Na serwerze iSeries A działa aplikacja obsługująca dane osobowe, która:
 - wymaga trybu SSL,
 - do konfigurowania SSL korzysta z certyfikatu prywatnego lokalnego ośrodka certyfikacji (CA),
 - wymaga certyfikatu podczas uwierzytelniania klienta.
- Gdy klienci B, C i D chcą uzyskać dostęp do aplikacji, serwer iSeries A przedstawia swój certyfikat w celu rozpoczęcia sesji SSL.
- Po zainicjowaniu sesji SSL, przed umożliwieniem dostępu do aplikacji obsługującej dane osobowe, serwer iSeries A wysyła zapytanie do klientów B, C i D, aby podali poprawne certyfikaty. Wymiana certyfikatów jest niewidoczna dla użytkowników klientów B, C i D.

Systemy klienckie pracowników – klient B, C i D

- Klient B jest pracownikiem pracującym w głównej siedzibie przedsiębiorstwa, gdzie znajduje się serwer iSeries A.
- Klient C jest pracownikiem pracującym w oddziale przedsiębiorstwa oddalonym od siedziby głównej.
- Klient D jest pracownikiem przemieszczającym się pomiędzy dwoma siedzibami i często podróżującym służbowo; musi on mieć możliwość bezpiecznego dostępu do serwisu WWW danych osobowych, niezależnie od miejsca przebywania.
- Klienci B, C i D są pracownikami przedsiębiorstwa, którzy korzystają z aplikacji obsługującej dane osobowe.
- Klienci B, C i D mają kopie certyfikatu wydanego przez lokalny ośrodek certyfikacji (CA), który wystawił dla aplikacji certyfikat zainstalowany z oprogramowaniem klienckim.
- Klienci B, C i D uzyskują dostęp do aplikacji obsługującej dane osobowe na serwerze iSeries A, który przedstawia swój certyfikat oprogramowaniu klienckiemu agentów w celu zweryfikowania swojej tożsamości i nawiązania sesji SSL.
- Oprogramowanie klienckie w systemach klientów B, C i D jest skonfigurowane tak, aby akceptować certyfikat przekazany z serwera iSeries A oraz rozpocząć sesję SSL.

- Po rozpoczęciu sesji SSL, klienci B, C i D muszą udostępnić poprawny certyfikat, aby serwer iSeries A umożliwił im dostęp do aplikacji i jej zasobów.

Wymagania wstępne i założenia

Można wymienić następujące wymagania wstępne i założenia:

1. Na serwerze iSeries A, na którym jest uruchomiony IBM HTTP Server for iSeries, działa aplikacja obsługująca dane osobowe. Są dwa typy serwerów HTTP Server for iSeries (oryginalny i oparty na platformie Apache), a najnowsza, znacznie zmieniona, wersja serwera HTTP będzie dostępna po ukazaniu się tej publikacji. Dlatego przedstawiony scenariusz nie zawiera *konkretnych instrukcji*, które należy zrealizować podczas konfigurowania serwera HTTP dla połączenia SSL. Zamieszczone są natomiast instrukcje, które należy wykonać podczas konfigurowania i zarządzania certyfikatami, i które są niezbędne, aby aplikacja mogła używać połączenia SSL.
2. Serwer HTTP udostępnia możliwość uwierzytelniania klienta po podaniu certyfikatu. Scenariusz ten zawiera również instrukcje używania Menedżera certyfikatów cyfrowych (DCM) do skonfigurowania wymagań dotyczących zarządzania certyfikatami. Jednak przedstawiony scenariusz nie zawiera *konkretnych* kroków konfiguracji, które należy zrealizować podczas konfigurowania uwierzytelniania klientów za pomocą certyfikatu dla serwera HTTP.
3. Na serwerze HTTP obsługującym dane osobowe w systemie iSeries A stosuje się ochronę za pomocą hasła.
4. Serwer iSeries A spełnia wszystkie wymagania niezbędne do zainstalowania i używania Menedżera certyfikatów cyfrowych (DCM).
5. Na serwerze iSeries A nie był wcześniej konfigurowany ani używany program DCM.
6. Aby użytkownicy mogli zrealizować zadania przewidziane w scenariuszu, ich profile związane z programem DCM muszą posiadać uprawnienia specjalne *SECADM i *ALLOBJ.
7. W serwerze iSeries A nie jest zamontowany koprocesor szyfrujący IBM 4758-023 PCI.

Kroki zadania

Są dwa zestawy zadań, które należy wykonać; pierwszy zestaw zadań opisuje kolejne etapy takiego konfigurowania aplikacji obsługującej dane osobowe na serwerze iSeries A, aby używała połączenia SSL i certyfikatów podczas uwierzytelniania użytkowników. Drugi zestaw zadań opisuje tok postępowania umożliwiającego klientom B, C i D partycypowanie w sesji SSL z aplikacją obsługującą dane osobowe oraz umożliwiającego uzyskanie certyfikatu uwierzytelniania użytkownika.

Zadania dotyczące aplikacji serwera WWW obsługującej dane osobowe

Na serwerze iSeries A należy wykonać następujące zadania:

1. Aby zainstalować i skonfigurować wszystkie niezbędne produkty iSeries, zrealizuj wszystkie kroki opisane jako wymagania wstępne.
2. Skonfiguruj połączenie SSL na serwerze HTTP obsługującym dane osobowe i zanotuj ID aplikacji dla instancji serwera.
3. Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można utworzyć i prowadzić lokalny ośrodek certyfikacji oraz wystawiać certyfikaty dla serwera HTTP obsługującego dane osobowe. Podczas realizowania kolejnych zadań przypiszesz certyfikat do aplikacji serwera oraz dodasz ośrodek certyfikacji (CA) do listy ośrodków, którym ufa aplikacja.
4. Teraz można rozpocząć konfigurowanie na serwerze WWW uwierzytelniania klienta przez sprawdzanie certyfikatów.
5. Uruchom serwer HTTP w trybie SSL.

Zadania związane z konfigurowaniem klienta

Zadania dla użytkowników (klient B, C i D), którzy mają dostęp do serwera WWW obsługującego dane osobowe w systemie iSeries A:

6. Zainstaluj kopię certyfikatu lokalnego ośrodka certyfikacji w przeglądarce.

7. Zażądaj certyfikatu z lokalnego ośrodka certyfikacji (CA).

Szczegóły konfigurowania

Aby użyć certyfikatów do skonfigurowania bezpiecznego dostępu do aplikacji i zasobów wewnętrznych, wykonaj opisane zadania.

Krok 1: Aby zainstalować wszystkie niezbędne produkty iSeries, należy zakończyć zadania dotyczące wymagań wstępnych

Zanim będzie możliwe wykonanie specyficznych zadań konfigurowania w celu zastosowania scenariusza, zrealizuj wszystkie kroki opisane jako wymagania wstępne, aby zainstalować i skonfigurować wszystkie niezbędne produkty iSeries.

Krok 2: Konfigurowanie połączenia SSL dla serwera HTTP obsługującego dane osobowe

Kroki konfigurowania protokołu Secure Sockets Layer (SSL) dla serwera HTTP obsługującego dane osobowe w systemie iSeries A są różne w zależności od tego, czy używa się oryginalnej wersji serwera HTTP, czy wersji opartej na serwerze Apache.

Więcej informacji o konfigurowaniu połączenia SSL na oryginalnym serwerze HTTP zawiera sekcja Konfigurowanie serwera chronionego na serwerze HTTP.

Więcej informacji o konfigurowaniu połączenia SSL na serwerze HTTP opartym na serwerze Apache zawiera sekcja Scenariusz: Aktywacja w firmie JKL ochrony Secure Sockets Layer (SSL) na serwerze HTTP (opartym na serwerze Apache). Przedstawiono w niej wszystkie kroki zadania niezbędne do utworzenia wirtualnego hosta oraz skonfigurowania dla niego połączenia SSL. Więcej informacji zawiera sekcja "Aktywacja połączenia SSL dla wirtualnego hosta".

Więcej informacji o konfigurowaniu bieżącej i przyszłych wersji serwera HTTP Server for iSeries (oryginalnych i opartych na serwerze Apache) zawiera temat Usługi sieciowe.

Krok 3: Tworzenie i prowadzenie lokalnego ośrodka certyfikacji

Po skonfigurowaniu protokołu Secure Sockets Layer (SSL) dla serwera HTTP obsługującego dane osobowe, należy skonfigurować dla serwera certyfikat, wykorzystywany podczas inicjowania połączenia SSL. W oparciu o przyjęte cele, aby wystawiać certyfikaty dla serwera wybrano rozwiązanie polegające na tworzeniu i prowadzeniu lokalnego ośrodka certyfikacji (CA).

Jeśli lokalny ośrodek certyfikacji (CA) będzie tworzony przy użyciu programu DCM, użytkownik zostanie przeprowadzony przez proces tworzenia ośrodka w sposób zapewniający, że zostaną skonfigurowane wszystkie elementy niezbędne do aktywowania połączenia SSL dla aplikacji. Proces ten obejmuje przypisanie do aplikacji serwera WWW certyfikatu wystawionego przez lokalny ośrodek certyfikacji (CA) oraz dodanie lokalnego ośrodka certyfikacji (CA) do listy zaufanych ośrodków dla aplikacji serwera WWW. Jeśli lokalny ośrodek znajduje się na liście ośrodków, którym ufa aplikacja, aplikacja rozpoznaje i uwierzytelnia użytkowników prezentujących certyfikaty wystawione przez ten lokalny ośrodek certyfikacji (CA).

Aby utworzyć i prowadzić lokalny ośrodek certyfikacji (CA) za pomocą programu Menedżer certyfikatów cyfrowych (DCM) oraz wystawiać certyfikaty dla aplikacji serwera obsługującego dane osobowe, wykonaj następujące czynności:

1. Uruchom program DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić szereg formularzy. Formularze te prowadzą przez proces tworzenia lokalnego ośrodka certyfikacji (CA),

podpisywania obiektów, weryfikowania podpisów i wykonywania innych zadań niezbędnych do rozpoczęcia korzystania z certyfikatów cyfrowych dla potrzeb protokołu SSL.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

3. Wypełnij wszystkie formularze zadań. Jeśli korzystasz z tych formularzy podczas wykonywania wszystkich zadań niezbędnych do utworzenia lokalnego ośrodka certyfikacji (CA):
 - a. Wprowadź informacje identyfikujące lokalny ośrodek certyfikacji (CA).
 - b. Zainstaluj certyfikat lokalnego ośrodka na komputerze PC lub w przeglądarce, tak aby oprogramowanie mogło rozpoznać ten ośrodek i sprawdzać poprawność wystawianych przez niego certyfikatów.
 - c. Wybierz strategię dla lokalnego ośrodka certyfikacji (CA).

Uwaga: Należy pamiętać o zaznaczeniu, że lokalny ośrodek certyfikacji (CA) może wystawiać certyfikaty użytkownikom.

- d. Użyj nowego, lokalnego ośrodka do wystawienia serwerowi lub klientowi certyfikatu, którego będą używać aplikacje podczas połączeń SSL.
- e. Wybierz aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL.

Uwaga: Należy pamiętać o zaznaczeniu ID aplikacji dla serwera HTTP obsługującego dane osobowe.

- f. Użyj nowego, lokalnego ośrodka certyfikacji (CA) do wystawienia certyfikatu, którego aplikacje będą używać do podpisywania obiektów. W tym podzadaniu tworzy się bazę certyfikatów *OBJECTSIGNING; jest to baza służąca zarządzaniu certyfikatami do podpisywania obiektów.

Uwaga: Poniższy krok należy wykonać, pomimo że w scenariuszu nie wykorzystuje się certyfikatów do podpisywania obiektów. Jeśli w tym miejscu przerwane zostanie wykonywanie zadania, należy wykonać inne zadania, które umożliwią zakończenie konfigurowania certyfikatów SSL.

- g. Wybierz aplikacje, które powinny ufać lokalnemu ośrodkowi.

Uwaga: Należy pamiętać o zaznaczeniu ID aplikacji dla serwera HTTP obsługującego dane osobowe, jako jedną z aplikacji, które ufają lokalnemu ośrodkowi certyfikacji (CA).

Konfigurowanie certyfikatów wymaganych przez aplikację serwera WWW podczas połączenia SSL zostało zakończone. Teraz można rozpocząć takie konfigurowanie aplikacji serwera WWW, aby podczas uwierzytelniania użytkownika żądała ona certyfikatu.

Krok 4: Konfigurowanie serwera WWW obsługującego dane osobowe, pod kątem uwierzytelniania klienta jedynie po okazaniu certyfikatu

Kroki konfigurowania protokołu Secure Sockets Layer (SSL) podjęte w celu uwierzytelniania klienta poprzez podawanie certyfikatu dla serwera HTTP obsługującego dane osobowe w systemie iSeries A są różne w zależności od tego, czy używa się wersji oryginalnej serwera HTTP, czy wersji opartej na serwerze Apache.

Więcej informacji o konfigurowaniu uwierzytelniania klienta poprzez żądanie certyfikatów na oryginalnym serwerze HTTP zawiera sekcja Tworzenie bezpiecznych instalacji na oryginalnym serwerze HTTP.

Więcej informacji o konfigurowaniu połączenia SSL na serwerze HTTP opartym na serwerze Apache, aby do uwierzytelniania klientów używać certyfikatów, zawiera sekcja Scenariusz: Aktywacja w firmie JKL ochrony Secure Sockets Layer (SSL) na serwerze HTTP (opartym na serwerze Apache). Przedstawiony dla serwera HTTP scenariusz zawiera wszystkich kroki zadania niezbędne do utworzenia wirtualnego hosta oraz skonfigurowania dla niego połączenia SSL i certyfikatów do uwierzytelniania klientów. Więcej informacji zawiera sekcja "Aktywacja połączenia SSL dla wirtualnego hosta".

Więcej informacji o konfigurowaniu bieżącej i przyszłych wersji serwera HTTP Server for iSeries (oryginalnych i opartych na serwerze Apache) zawiera temat Usługi sieciowe.

Krok 5: Uruchomienie serwera WWW obsługującego dane osobowe w trybie SSL

Aby serwer HTTP mógł wykryć certyfikat i wykorzystać go do rozpoczęcia sesji SSL, należy serwer zatrzymać i ponownie uruchomić.

Aby zatrzymać i uruchomić serwer HTTP (oryginalny), użyj formularzy Konfigurowanie i Administrowanie, oraz wykonaj następujące czynności:

1. Kliknij **Administrowanie**.
2. Kliknij **Zarządzanie serwerami HTTP**.
3. Zaznacz serwer.
4. W polu dostępnym na formularzu, wprowadź opcjonalne parametry uruchamiania.
5. Kliknij **Uruchom**.

Uwaga: Jeśli podczas przypisywania certyfikatu serwer był uruchomiony, należy wykonać polecenie Zatrzymaj serwer, a następnie Uruchom serwer. Klikanie **Restart** nie zawsze powoduje wykrycie przez serwer zmian certyfikatów, jakie zostały wprowadzone podczas działania serwera.

Aby zatrzymać i uruchomić serwer HTTP (oparty na serwerze Apache), użyj formularzy Konfigurowanie i Administrowanie, oraz wykonaj następujące kroki:

1. Kliknij **Administrowanie**.
2. W menu znajdującym się po lewej stronie, w opcji **Ogólne Administrowanie serwerami** kliknij **Zarządzanie serwerami HTTP**.
3. Zaznacz serwer i kliknij **Uruchom** lub **Zatrzymaj**. Więcej informacji na temat parametrów uruchamiania znajduje się w pomocy elektronicznej.

Więcej informacji o zarządzaniu oryginalnymi lub opartymi na serwerze Apache bieżącymi i przyszłymi wersjami serwera HTTP Server for iSeries zawiera temat Usługi sieciowe.

Jeśli zadanie zostało zakończone można uruchomić aplikację obsługującą dane osobowe w trybie SSL i rozpocząć ochronę prywatności danych dostarczanych przez tę aplikację.

Krok 6: Instalowanie przez użytkowników kopii certyfikatu lokalnego ośrodka certyfikacji w przeglądarce

Serwer dostępny poprzez połączenie Secure Sockets Layer (SSL) przedstawia oprogramowaniu klienta użytkownika certyfikat jako dowód swojej tożsamości. Oprogramowanie klienta musi następnie sprawdzić certyfikat serwera, aby mógł on nawiązać połączenie. Aby sprawdzić certyfikat serwera, oprogramowanie klienta musi mieć dostęp do lokalnie przechowywanej kopii certyfikatu ośrodka certyfikacji (CA), który wystawił certyfikat serwera. Jeśli serwer przedstawia certyfikat z publicznego ośrodka certyfikacji (CA), używana przeglądarka użytkownika lub inne oprogramowanie klienta powinno już mieć kopię certyfikatu tego ośrodka. Jeśli jak w scenariuszu, serwer przedstawia certyfikat z prywatnego lokalnego ośrodka certyfikacji (CA), należy użyć Menedżera certyfikatów cyfrowych (DCM) do zainstalowania kopii certyfikatu tego ośrodka.

Zadania dla użytkowników (klienci B, C i D), którzy chcą otrzymać kopię lokalnego ośrodka certyfikacji:

1. Uruchom program DCM.
2. W ramce nawigacji wybierz **Instalowanie certyfikatu lokalnego ośrodka CA na komputerze PC**, aby wyświetlić stronę umożliwiającą pobranie certyfikatu lokalnego ośrodka do przeglądarki lub zapisanie go w pliku w systemie lokalnym.
3. Zaznacz opcję Instalowanie certyfikatu. Zaznaczenie tej opcji spowoduje pobranie certyfikatu lokalnego ośrodka certyfikacji do przeglądarki jako użytkownika zaufanego. Dzięki temu przeglądarka będzie

- mogła nawiązywać bezpieczne sesje komunikacyjne z serwerami WWW używającymi certyfikatów z tego ośrodka. Przeglądarka będzie wyświetlać kolejne okna, aby pomóc w procesie instalacji.
4. Kliknij **OK**, aby powrócić do strony głównej programu Menedżer certyfikatów cyfrowych.

Krok 7: Żądanie użytkownika przedstawienia certyfikatu lokalnego ośrodka certyfikacji

Wykonane wcześniej kroki doprowadziły do takiego skonfigurowania serwera WWW obsługującego dane osobowe, aby podczas uwierzytelniania klienta kierował do niego żądanie certyfikatu. Teraz użytkownicy muszą przedstawić poprawny certyfikat lokalnego ośrodka certyfikacji (CA) przed otrzymaniem pozwolenia na dostęp do serwera WWW. Każdy użytkownik musi skorzystać z Menedżera certyfikatów cyfrowych DCM, aby używając zadania **Tworzenie certyfikatu** uzyskać certyfikat. Aby jednak było to możliwe, strategia lokalnego ośrodka certyfikacji (CA) musi zezwalać na wystawianie certyfikatów użytkownikom.

Zadania dla użytkowników (klienci B, C i D), którzy chcą otrzymać certyfikat:

1. Uruchom program DCM.
2. W ramce nawigacji wybierz **Tworzenie certyfikatu**.
3. Jako typ tworzonego certyfikatu wybierz **Certyfikat użytkownika**. Zostanie wyświetlony formularz, w którym należy wpisać informacje identyfikacyjne dla certyfikatu.
4. Wypełnij formularz i kliknij **Kontynuuj**.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

5. W tym momencie program DCM współpracuje z przeglądarką w celu utworzenia prywatnego i publicznego klucza dla certyfikatu. Przeglądarka może w tym celu wyświetlić wiele okien. Postępuj zgodnie z instrukcjami wyświetlanymi przez przeglądarkę. Po wygenerowaniu kluczy przez przeglądarkę wyświetla się strona potwierdzająca utworzenie certyfikatu przez program DCM.
6. Zainstaluj w przeglądarce nowy certyfikat. Przeglądarka może w tym celu wyświetlić wiele okien. Wykonaj polecenia podawane przez przeglądarkę w celu zakończenia tego zadania.
7. Kliknij **OK**, aby zakończyć.

Podczas przetwarzania Menedżer certyfikatów cyfrowych automatycznie przypisuje certyfikat do profilu użytkownika iSeries.

Rozdział 5. Koncepcje dotyczące certyfikatów cyfrowych

Stosowanie certyfikatów cyfrowych jako elementu strategii ochrony systemu i sieci wymaga wiedzy na temat tego, czym są certyfikaty cyfrowe i jakie korzyści związane z bezpieczeństwem przynosi ich wykorzystanie.

Certyfikat cyfrowy jest cyfrowym świadectwem tożsamości, które identyfikuje właściciela certyfikatu, podobnie jak paszport. Zaufany podmiot, zwany ośrodkiem certyfikacji (CA), wystawia certyfikaty cyfrowe użytkownikom oraz aplikacjom serwera i klienta. Zaufanie do ośrodka certyfikacji stanowi fundament zaufania do certyfikatu jako dokumentu uwierzytelniającego.

Więcej informacji na temat koncepcji dotyczących certyfikatów zawierają sekcje:

Nazwa wyróżniająca

Sekcja zawiera informacje o parametrach identyfikacyjnych certyfikatów cyfrowych.

Podpisy cyfrowe

Sekcja zawiera informacje o podpisach cyfrowych oraz ich zastosowaniu do zapewnienia integralności obiektów.

Para kluczy publiczny-prywatny

Sekcja zawiera informacje o kluczach ochrony powiązanych w certyfikatami cyfrowymi.

Zadania dotyczące ośrodka certyfikacji

Sekcja zawiera informacje o ośrodkach certyfikacji (CA) i jednostkach wystawiających certyfikaty cyfrowe.

Położenie list CRL

W sekcji opisano listy odwołań certyfikatów (CRL) oraz sposób korzystania z nich w procesie sprawdzania i uwierzytelniania certyfikatów.

Bazy certyfikatów

Sekcja opisuje bazy certyfikatów i sposób wykorzystania programu DCM do pracy z nimi oraz z zawartymi w nich certyfikatami.

Kryptografia

Informacje zawarte w tej sekcji pozwalają dowiedzieć się, czym jest kryptografia i jak wykorzystać funkcje kryptograficzne do zwiększenia bezpieczeństwa.

Protokół Secure Sockets Layer

W sekcji przedstawiono krótki opis protokołu SSL.

Nazwa wyróżniająca

Każdy ośrodek certyfikacji (CA) ma własną strategię określającą, jakie dane identyfikacyjne są konieczne do wystawienia certyfikatu. Niektóre publiczne ośrodki certyfikacji (CA) w Internecie do wystawienia certyfikatu wymagają jedynie podstawowych informacji, na przykład nazwy i adresu poczty elektronicznej. Inne ośrodki publiczne mogą wymagać więcej informacji i dowodów na ich autentyczność. Na przykład ośrodki zgodne ze standardami Public Key Infrastructure Exchange (PKIX) mogą wymagać, aby informacje podane przez wnioskodawcę zostały przed wystawieniem certyfikatu potwierdzone przez ośrodek rejestracyjny (RA). Dlatego planując akceptowanie certyfikatów i używanie ich w charakterze świadectwa tożsamości, należy zapoznać się z wymaganiami identyfikacyjnymi dla danego ośrodka i sprawdzić, czy odpowiadają one przyjętym wymogom bezpieczeństwa.

Nazwa wyróżniająca (DN) to termin określający informacje identyfikujące posiadacza certyfikatu, będące częścią samego certyfikatu. W zależności od strategii identyfikacyjnej ośrodka certyfikacji (CA) wydającego certyfikat, nazwa wyróżniająca może zawierać różne informacje. Program Menedżer certyfikatów cyfrowych (DCM) umożliwia tworzenie prywatnego ośrodka certyfikacji (CA) i wystawianie prywatnych certyfikatów. Programu tego można również używać do generowania nazw wyróżniających i par kluczy na podstawie certyfikatów uzyskanych z publicznego, internetowego ośrodka certyfikacji (CA). Informacje o nazwie wyróżniającej, które należy dostarczyć dla każdego typu certyfikatów, obejmują:

- nazwę posiadacza certyfikatu,
- organizację,

- jednostkę organizacyjną,
- miasto,
- województwo,
- kraj.

Korzystając z programu DCM do wystawiania prywatnych certyfikatów, można podać dodatkowe informacje o nazwie wyróżniającej obejmujące:

- adres IP w wersji 4,
- pełną nazwę domeny,
- adres poczty elektronicznej.

Te dodatkowe informacje są użyteczne, jeśli planuje się wykorzystanie certyfikatów do skonfigurowania połączeń sieci VPN (virtual private network).

Podpisy cyfrowe

Podpis cyfrowy na dokumencie elektronicznym lub innym obiekcie jest tworzony za pomocą metod stosowanych w kryptografii i odpowiada osobistemu podpisowi na zwykłym dokumencie. Podpis cyfrowy stanowi świadectwo pochodzenia i umożliwia zweryfikowanie integralności obiektu. Właściciel certyfikatu cyfrowego "podpisuje" obiekt, używając klucza prywatnego certyfikatu. Odbiorca obiektu korzysta z klucza publicznego tego samego certyfikatu w celu deszyfrowania podpisu, weryfikując w ten sposób integralność podpisanego obiektu z jego nadawcą.

Ośrodek certyfikacji podpisuje wystawiane przez siebie certyfikaty. Podpis taki jest łańcuchem danych zaszyfrowanym przez prywatny klucz ośrodka certyfikacji (CA). Każdy użytkownik może zweryfikować podpis na certyfikacie, używając klucza publicznego ośrodka certyfikacji (CA) do deszyfrowania podpisu.

Podpis cyfrowy jest podpisem elektronicznym, tworzonym dla obiektu przez użytkownika lub aplikację, za pomocą klucza prywatnego certyfikatu. Podpis cyfrowy obiektu tworzy unikalne, elektroniczne połączenie dowodu tożsamości podpisującego (właściciela klucza podpisującego) z miejscem pochodzenia obiektu. Po uzyskaniu dostępu do obiektu z podpisem elektronicznym można zweryfikować źródło pochodzenia obiektu (na przykład, sprawdzić, czy pobierana aplikacja rzeczywiście pochodzi z autoryzowanego źródła, jak firma IBM). Proces weryfikacji umożliwia również sprawdzenie, czy po podpisaniu obiektu dokonano w nim jakichś nieautoryzowanych zmian.

Przykład zastosowania podpisu cyfrowego

Producent oprogramowania napisał aplikację iSeries, która ma być dystrybuowana poprzez sieć Internet, ze względu na jej ekonomiczność oraz łatwy dostęp dla klientów. Producent oprogramowania zdaje sobie jednak sprawę, że użytkownicy obawiają się pobierania programów poprzez sieć Internet, ze względu na rosnące zagrożenie pobrania obiektu, który podszywa się pod prawdziwy program, a jest w rzeczywistości szkodliwym programem wirusowym.

W efekcie producent decyduje się na podpisanie aplikacji podpisem cyfrowym, aby klienci mieli możliwość zweryfikowania, czy miejsce, z którego pobierany jest program, jest prawdziwym miejscem pochodzenia aplikacji. Do podpisania aplikacji wykorzystywany jest klucz publiczny, który producent oprogramowania otrzymuje z publicznego ośrodka certyfikacji (CA). Klucz ten udostępnia się klientom. Pobierany pakiet zawiera między innymi kopię certyfikatu cyfrowego, którego użyto do podpisania obiektu. Po pobraniu pakietu aplikacji, klient może użyć klucza publicznego certyfikatu do zweryfikowania podpisu aplikacji. W ten sposób klient może dokonać identyfikacji oraz weryfikacji aplikacji, jak również upewnić się, czy od czasu podpisania aplikacji nie zmieniono zawartości obiektu aplikacji.

Para kluczy publiczny-prywatny

Każdy certyfikat cyfrowy jest powiązany z parą kluczy szyfrujących. Ta para kluczy składa się z klucza prywatnego i klucza publicznego. (Certyfikaty do weryfikacji podpisu stanowią wyjątek od tej reguły i są powiązane tylko z kluczem publicznym.)

Klucz publiczny jest częścią certyfikatu cyfrowego jego właściciela i mogą go używać wszyscy zainteresowani. Jednakże klucz prywatny jest chroniony przez właściciela klucza i tylko on może się nim posłużyć. Ograniczony dostęp do klucza zapewnia ochronę komunikacji prowadzonej za jego pomocą.

Właściciel certyfikatu może korzystać z zalet oferowanych przez klucze funkcji zabezpieczeń szyfrujących. Właściciel certyfikatu może na przykład używać klucza prywatnego certyfikatu do "podpisywania" i szyfrowania danych przesyłanych pomiędzy użytkownikami a serwerami, takich jak wiadomości, dokumenty i kod. Odbiorca podpisanego obiektu używa klucza publicznego, znajdującego się w certyfikacie podpisującego, do deszyfrowania podpisu. Podpisy cyfrowe zapewniają wiarygodność pochodzenia obiektów i umożliwiają sprawdzenie integralności obiektu.

Zadania dotyczące ośrodka certyfikacji

Ośrodek certyfikacji (CA) jest zaufaną centralną jednostką administracyjną, która może wystawiać cyfrowe certyfikaty użytkownikom i serwerom. Zaufanie do ośrodka certyfikacji (CA) stanowi fundament zaufania do certyfikatu jako dokumentu uwierzytelniającego. Ośrodek certyfikacji stosuje swój klucz prywatny do wykonania podpisu cyfrowego na wystawianym certyfikacie, co stanowi gwarancję pochodzenia certyfikatu. Klucza publicznego certyfikatu ośrodka certyfikacji (CA) używa się do weryfikowania autentyczności certyfikatów wystawianych i podpisywanych przez ten ośrodek.

Ośrodek certyfikacji (CA) może być publiczną jednostką komercyjną, jak na przykład VeriSign, lub jednostką operacyjną utworzoną w ramach organizacji na potrzeby wewnętrzne. Komercyjne usługi ośrodków certyfikacji dla użytkowników sieci Internet oferuje kilka firm. Menedżer certyfikatów cyfrowych (DCM) pozwala zarządzać zarówno certyfikatami z ośrodków publicznych, jak i z prywatnych.

Programu można również używać do prowadzenia własnego ośrodka certyfikacji (CA), w celu wystawiania prywatnych certyfikatów systemom i użytkownikom. Gdy ośrodek certyfikacji (CA) wystawia certyfikat użytkownika, program DCM automatycznie przypisuje ten certyfikat odpowiedniemu profilowi użytkownika systemu iSeries. Dzięki temu przywileje dostępu i uprawnienia związane z certyfikatem są takie same, jak dla profilu użytkownika właściciela certyfikatu.

Status użytkownika zaufanego

Termin użytkownik zaufany odnosi się do specjalnej roli, jaką pełni certyfikat ośrodka certyfikacji. Miano użytkownika zaufanego pozwala przeglądarce lub innej aplikacji uwierzytelniać i akceptować certyfikaty wystawiane przez ten ośrodek certyfikacji (CA).

Po pobraniu certyfikatu ośrodka certyfikacji do przeglądarki uznaje ona ten ośrodek za użytkownika zaufanego. Także inne aplikacje obsługujące certyfikaty muszą być odpowiednio skonfigurowane, aby uznać ośrodek certyfikacji (CA) za zaufany, zanim będą mogły uwierzytelniać i ufać certyfikatом wystawianym przez ten ośrodek.

Za pomocą programu DCM można włączyć lub wyłączyć status zaufania dla certyfikatu ośrodka certyfikacji (CA) w bazie certyfikatów. Po włączeniu tego statusu dla certyfikatu ośrodka certyfikacji (CA) można skonfigurować aplikacje, tak aby używały go do uwierzytelniania i akceptowania certyfikatów wystawionych przez ten ośrodek. Nie można tego zrobić, jeśli status zaufania dla certyfikatu ośrodka certyfikacji (CA) zostanie wyłączony.

Strategia ośrodka certyfikacji

Tworząc ośrodek certyfikacji (CA) za pomocą programu Menedżer certyfikatów cyfrowych można zdefiniować strategię tego ośrodka. Strategia ośrodka certyfikacji (CA) opisuje uprawnienia do podpisywania, które ten ośrodek posiada. Strategia określa:

- czy ośrodek może wystawiać i podpisywać certyfikaty użytkowników,
- jak długo są ważne certyfikaty wystawiane przez ośrodek.

Położenie listy odwołań certyfikatów (CRL)

Lista odwołań certyfikatów (CRL) jest plikiem zawierającym wszystkie niepoprawne i unieważnione certyfikaty wystawione przez określony ośrodek certyfikacji (CA). Ośrodki okresowo aktualizują swoje listy CRL i udostępniają je innym w celu opublikowania w katalogach protokołu Lightweight Directory Access Protocol (LDAP). Kilka ośrodków certyfikacji (CA), na przykład SSH z Finlandii, samodzielnie publikuje listę CRL w katalogach LDAP, do których użytkownicy mają bezpośredni dostęp. Jeśli ośrodek samodzielnie publikuje listę CRL, jego certyfikat zawiadamia o tym poprzez informację o punkcie dystrybucji CRL w formie adresu URI (Uniform Resource Identifier).

Menedżer certyfikatów cyfrowych (DCM) umożliwia definiowanie informacji o położeniu list CRL i zarządzanie nimi w celu zapewnienia bardziej rygorystycznego uwierzytelniania akceptowanych certyfikatów. Definicja położenia listy CRL zawiera informacje o położeniu i o dostępie do serwera Lightweight Directory Access Protocol (LDAP), na którym znajduje się lista CRL.

Aby sprawdzić, czy ośrodek nie unieważnił określonego certyfikatu, aplikacje uwierzytelniające certyfikat przeszukują miejsce położenia listy CRL dla danego ośrodka, o ile zostało ono zdefiniowane. Program DCM umożliwia definiowanie informacji o położeniu listy DCM, potrzebnych aplikacjom do przetwarzania listy CRL podczas uwierzytelniania certyfikatu, oraz zarządzanie tymi informacjami. Przykłady aplikacji i procesów, które mogą przetwarzać listę CRL podczas uwierzytelniania certyfikatu, to: wirtualne sieci prywatne (VPN), serwer Internet Key Exchange (IKE), aplikacje obsługujące protokół Secure Sockets Layer (SSL) oraz procesy podpisywania obiektów. Ponadto podczas definiowania położenia listy CRL i wiązania jej z certyfikatem ośrodka program DCM przetwarza listę CRL jako element procesu sprawdzania certyfikatów wystawianych przez dany ośrodek certyfikacji (CA).

Bazy certyfikatów

Baza certyfikatów to specjalny plik bazy danych kluczy używany przez Menedżer certyfikatów cyfrowych (DCM) do przechowywania certyfikatów cyfrowych. Baza certyfikatów zawiera również klucze prywatnego certyfikatu, chyba że do przechowywania kluczy używany jest koprocessor szyfrujący 4758. Program DCM pozwala utworzyć i zarządzać kilkoma typami baz certyfikatów. Program DCM kontroluje dostęp do bazy certyfikatów poprzez hasła oraz przez sterowanie dostępem do katalogu i plików IFS tworzących bazę.

Bazy te są klasyfikowane na podstawie rodzaju przechowywanych w nich certyfikatów. Również zadania administracyjne dla każdej bazy certyfikatów zależą od typu przechowywanych w niej certyfikatów. W programie DCM można utworzyć i poprzez niego zarządzać następującymi predefiniowanymi bazami certyfikatów:

Lokalny ośrodek certyfikacji (CA)

Jeśli został utworzony lokalny ośrodek certyfikacji (CA), program DCM używa tej bazy do przechowywania certyfikatu ośrodka i jego klucza prywatnego. Certyfikatu z tej bazy można używać do podpisywania certyfikatów wystawianych przez lokalny ośrodek certyfikacji (CA). Kiedy lokalny ośrodek certyfikacji (CA) wystawia certyfikat, program DCM umieszcza kopię certyfikatu ośrodka w odpowiedniej bazie certyfikatów (na przykład *SYSTEM) w celu uwierzytelnienia. Aplikacje używają certyfikatów ośrodków do potwierdzenia pochodzenia certyfikatów, które muszą uwierzytelnić w procesie negocjacji SSL, aby nadać uprawnienia do zasobów.

Baza *SYSTEM

Program DCM udostępnia tę bazę w celu zarządzania zarówno certyfikatami serwera, jak i klienta, używanymi przez aplikacje w celu uczestniczenia w sesji komunikacyjnej Secure Sockets Layer (SSL). Aplikacje IBM iSeries (i aplikacje wielu dostawców oprogramowania) są napisane w taki sposób, aby korzystały wyłącznie z certyfikatów przechowywanych w bazie *SYSTEM. Program DCM utworzy tę bazę certyfikatów, gdy lokalny ośrodek certyfikacji (CA) tworzono przy użyciu programu DCM. Bazę tę należy utworzyć, gdy certyfikaty, wykorzystywane przez aplikacje serwera i klienta, uzyskiwane będą z publicznego ośrodka certyfikacji (CA), jak np. ośrodek VeriSign.

Baza *OBJECTSIGNING

Ta baza certyfikatów służy do zarządzania certyfikatami używanymi do podpisywania obiektów. Zadania dostępne w tej bazie umożliwiają również tworzenie cyfrowych podpisów obiektów oraz przeglądanie i weryfikowanie tych podpisów. Program DCM utworzy tę bazę certyfikatów, gdy lokalny ośrodek certyfikacji (CA) tworzony jest przy użyciu programu DCM. Bazę tę należy utworzyć, gdy certyfikaty do podpisywania obiektów uzyskiwane będą z publicznego ośrodka certyfikacji (CA), jak np. ośrodek VeriSign.

Baza *SIGNATUREVERIFICATION

Jest to baza do zarządzania certyfikatami używanymi do uwierzytelniania cyfrowych podpisów obiektów. Aby uwierzytelnić certyfikat cyfrowy, baza ta musi zawierać kopię certyfikatu, którym podpisano obiekt. Baza musi zawierać również kopię certyfikatu ośrodka certyfikacji (CA) dla ośrodka certyfikacji, z którego pochodzi certyfikat użyty do podpisania obiektów. Certyfikat ten można uzyskać eksportując certyfikaty podpisujące obiekt w aktualnym systemie do bazy lub importując certyfikaty otrzymane od podpisującego obiekt.

Inne bazy certyfikatów systemu

Te bazy stanowią alternatywne miejsce przechowywania certyfikatów serwerów i klientów używanych podczas sesji SSL. Inne bazy certyfikatów systemu to definiowane przez użytkowników zapasowe bazy certyfikatów SSL. Opcja Inna baza certyfikatów systemu pozwala zarządzać certyfikatami dla aplikacji używających funkcji API SSL_Init w celu programowego dostępu do certyfikatów i wykorzystania ich do nawiązania sesji SSL. Funkcja ta umożliwia aplikacji użycie domyślnego certyfikatu z bazy certyfikatów zamiast certyfikatu specjalnego. Najczęściej tego rodzaju baz certyfikatów używa się podczas migracji certyfikatów z wcześniejszych wersji programu DCM lub w celu utworzenia specjalnego podzbioru certyfikatów na użytek protokołu SSL.

Uwaga: Jeśli na serwerze iSeries zainstalowany jest koprocesor szyfrujący IBM 4758 PCI, można wybrać inne opcje przechowywania kluczy prywatnych dla używanych certyfikatów (z wyjątkiem certyfikatów do podpisywania obiektów). Można również użyć koprocesora do zaszyfrowania klucza prywatnego i przechowywać go w specjalnym pliku klucza, a nie w bazie certyfikatów.

Program DCM kontroluje dostęp do baz certyfikatów za pomocą haseł. Program ten obsługuje również kontrolę dostępu do katalogów i plików zintegrowanego systemu plików, składających się na bazę certyfikatów. Bazy certyfikatów lokalnego ośrodka certyfikacji, *SYSTEM, *OBJECTSIGNING i *SIGNATUREVERIFICATION muszą znajdować się w określonych ścieżkach wewnątrz zintegrowanego systemu plików. Inne bazy certyfikatów systemu mogą znajdować się gdziekolwiek w zintegrowanym systemie plików.

Kryptografia

Kryptografia jest nauką o ochronie danych. Kryptografia umożliwia przechowywanie informacji oraz ich przesyłanie w taki sposób, aby osoby postronne nie były w stanie odczytać przechowywanych lub przesyłanych informacji. Szyfrowanie przekształca zrozumiały tekst w niezrozumiały ciąg danych (tekst zaszyfrowany). Deszyfrowanie odtwarza zrozumiały tekst z niezrozumiałych danych. Oba procesy wymagają matematycznych wzorów lub algorytmów i tajnej sekwencji danych (klucza).

Istnieją dwa rodzaje kryptografii:

- W kryptografii z **kluczem wspólnym lub tajnym (symetrycznej)** dwie komunikujące się strony używają wspólnego klucza. Do szyfrowania i deszyfrowania służy ten sam klucz.
- W kryptografii z **kluczem publicznym (asymetrycznej)** do szyfrowania i deszyfrowania obie strony używają różnych kluczy. Każda strona posiada parę kluczy składającą się z klucza publicznego i klucza prywatnego. Klucz publiczny jest rozpowszechniany bez ograniczeń, zwykle jako część certyfikatu cyfrowego, podczas gdy klucz prywatny jest bezpiecznie przechowywany przez właściciela. Oba klucze

są matematycznie powiązane, jednak uzyskanie klucza prywatnego z klucza publicznego jest praktycznie niemożliwe. Obiekt zaszyfrowany za pomocą czyjegoś klucza publicznego może zostać deszyfrowany tylko za pomocą odpowiedniego klucza prywatnego. I odwrotnie, serwer lub użytkownik może użyć prywatnego klucza do "podpisania" obiektu, a odbiorca może użyć odpowiedniego klucza publicznego do deszyfrowania podpisu cyfrowego w celu sprawdzenia pochodzenia i integralności obiektu.

Protokół Secure Sockets Layer

Protokół Secure Sockets Layer (SSL), opracowany przez firmę Netscape, jest obecnie standardem szyfrowania sesji pomiędzy klientem a serwerem. SSL wykorzystuje metody kryptografii asymetrycznej (kryptografii klucza prywatnego) do szyfrowania sesji pomiędzy serwerem a klientem. Klient i aplikacje serwera negocjują klucz sesji podczas wymiany certyfikatów cyfrowych. Ważność klucza wygasa automatycznie po 24 godzinach, a dla każdego połączenia klienta i serwera tworzony jest inny klucz. Wynika z tego, że nawet jeśli nieuprawniony użytkownik przechwyci i odszyfruje klucz sesji (co jest nieprawdopodobne), to nie będzie mógł go użyć do podsłuchiwania kolejnych sesji.

Rozdział 6. Planowanie DCM

Aby efektywnie wykorzystać program Menedżer certyfikatów cyfrowych do zarządzania certyfikatami cyfrowymi w firmie, należy sporządzić ogólny plan wykorzystywania tych certyfikatów jako elementu strategii ochrony.

Poniższe sekcje instruuja w jaki sposób zaplanować wykorzystywanie programu DCM oraz jak włączyć certyfikaty cyfrowe do własnej strategii ochrony.

Wymagania dotyczące korzystania z programu DCM

Sekcja zawiera informacje o oprogramowaniu, jakie należy zainstalować, oraz inne informacje potrzebne do skonfigurowania systemu w celu używania programu DCM.

Typy certyfikatów cyfrowych

Sekcja zawiera informacje o różnych typach certyfikatów, którymi można zarządzać przy użyciu programu DCM.

Certyfikaty publiczne, a certyfikaty prywatne

Dzięki informacjom przedstawionym w tej sekcji można dowiedzieć się, jaki rodzaj certyfikatu najbardziej odpowiada konkretnym potrzebom, jeśli została już podjęta decyzja o sposobie używania certyfikatów w celu zapewnienia dodatkowej ochrony. Można posługiwać się certyfikatami pochodzącymi z publicznych ośrodków certyfikacji (CA) lub utworzyć i poprowadzić, w celu wystawiania certyfikatów, prywatny ośrodek certyfikacji (CA). Sposób uzyskania certyfikatów zależy od ich planowanego wykorzystania.

Certyfikaty cyfrowe w bezpiecznej komunikacji SSL

W sekcji opisano, w jaki sposób użyć certyfikatów cyfrowych, aby aplikacje mogły nawiązywać bezpieczne sesje komunikacyjne.

Certyfikaty cyfrowe jako uwierzytelnienie użytkowników

W sekcji opisano sposób użycia certyfikatów jako środków pewniejszego uwierzytelniania użytkowników korzystających z zasobów serwera iSeries.

Certyfikaty cyfrowe w połączeniach VPN

W sekcji opisano sposób użycia certyfikatów w procesie konfigurowania połączeń sieci VPN.

Podpisywanie obiektów za pomocą certyfikatów cyfrowych

Sekcja zawiera informacje o wykorzystaniu certyfikatów do zapewnienia integralności obiektów i do weryfikacji cyfrowych podpisów obiektów w celu ustalenia ich autentyczności.

Certyfikaty cyfrowe do weryfikowania podpisów obiektów

Sekcja zawiera informacje o wykorzystaniu certyfikatów do weryfikacji cyfrowych podpisów obiektów w celu ustalenia ich autentyczności.

Wymagania dotyczące korzystania z programu DCM

Menedżer certyfikatów cyfrowych (DCM) jest bezpłatnie dostarczaną opcją systemu iSeries, dzięki której można centralnie zarządzać certyfikatami cyfrowymi aplikacji. Aby bez problemów korzystać z programu, wykonaj następujące czynności (lub sprawdź, czy zostały one wykonane już wcześniej):

- Zainstaluj program licencjonowany Cryptographic Access Provider (5722–AC3). Maksymalna długość klucza dla algorytmów szyfrujących w tym programie jest ustalana w oparciu o regulacje prawne dotyczące eksportu i importu. Aby można było tworzyć certyfikaty, ten program musi być zainstalowany.
- Zainstaluj opcję 34 systemu OS/400. Jest to oparta na przeglądarce opcja DCM.
- Zainstaluj IBM HTTP Server for iSeries (5722–DG1) i uruchom instancję serwera *ADMIN.
- Sprawdź, czy w systemie został skonfigurowany protokół TCP, tak aby można było korzystać z przeglądarki WWW i instancji *ADMIN serwera HTTP w celu dostępu do opcji DCM.

Uwaga: Dopóki nie zostaną zainstalowane wszystkie wymagane produkty, nie będzie można tworzyć certyfikatów. Jeśli wymagany produkt nie zostanie zainstalowany, program DCM wyświetli komunikat o błędzie informujący o konieczności zainstalowania brakującego komponentu.

Typy certyfikatów cyfrowych

Istnieje kilka klasyfikacji certyfikatów cyfrowych. Opisują one sposób użycia certyfikatów. Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można zarządzać certyfikatami następujących typów:

Certyfikaty ośrodków certyfikacji (CA)

Certyfikaty ośrodków certyfikacji są świadectwami tożsamości potwierdzającymi tożsamość ośrodka certyfikacji, który jest właścicielem takiego certyfikatu. Certyfikaty te zawierają informacje identyfikujące ośrodek oraz jego klucz publiczny. Klucza publicznego certyfikatu ośrodka certyfikacji (CA) używa się do weryfikowania autentyczności certyfikatów wystawianych i podpisywanych przez ten ośrodek. Certyfikaty ośrodków certyfikacji (CA) mogą być podpisane przez inny ośrodek, na przykład przez VeriSign, lub przez właściciela certyfikatu w przypadku jednostek niezależnych. Ośrodek certyfikacji (CA) tworzony za pomocą programu Digital Certificate Manager jest jednostką niezależną. Klucza publicznego certyfikatu ośrodka certyfikacji (CA) używa się do weryfikowania autentyczności certyfikatów wystawianych i podpisywanych przez ten ośrodek. Aby użyć certyfikatu do nawiązania sesji SSL, do podpisania obiektów lub weryfikacji podpisu obiektu należy mieć kopię certyfikatu ośrodka certyfikacji (CA), który wystawił certyfikat.

Certyfikaty serwerów lub klientów

Certyfikat serwera lub klienta to cyfrowe świadectwo tożsamości identyfikujące aplikację serwera lub klienta używającą tego certyfikatu w celu bezpiecznej komunikacji. Certyfikaty tego rodzaju zawierają informacje identyfikujące organizację, która jest właścicielem aplikacji, na przykład nazwę wyróżniającą systemu. Certyfikat zawiera także klucz publiczny systemu. Serwer musi mieć certyfikat cyfrowy, aby używać protokołu Secure Sockets Layer do komunikacji chronionej. Aplikacje, które obsługują certyfikaty cyfrowe, mogą sprawdzać certyfikat serwera, aby potwierdzić jego tożsamość w momencie, gdy klient uzyskuje do niego dostęp. Aplikacja może następnie użyć uwierzytelnienia certyfikatu jako podstawy do zainicjowania sesji szyfrowanej poprzez SSL pomiędzy klientem a serwerem. Jedynie baza certyfikatów *SYSTEM umożliwia zarządzanie tymi typami certyfikatów.

Certyfikaty do podpisywania obiektów

Certyfikaty te są używane do cyfrowego "podpisywania" obiektów. Dzięki podpisaniu obiektu można potwierdzić integralność obiektu, źródło pochodzenia obiektu lub prawo własności do tego obiektu. Jednego certyfikatu można użyć do podpisania różnych obiektów, w tym większości obiektów zintegrowanego systemu plików IFS oraz obiektów *CMD. Pełna lista tych obiektów znajduje się w sekcjach: Podpisywanie obiektów oraz Weryfikacja podpisu obiektów. Aby zweryfikować autentyczność podpisu obiektu złożonego za pomocą klucza prywatnego certyfikatu do podpisywania obiektów, odbiorca obiektu musi mieć dostęp do kopii odpowiedniego certyfikatu do weryfikowania podpisów. Jedynie baza certyfikatów *OBJECTSIGNING umożliwia zarządzanie tymi typami certyfikatów.

Certyfikaty do weryfikowania podpisów

Certyfikat do weryfikowania podpisu jest kopią certyfikatu do podpisywania obiektu pozbawioną klucza prywatnego tego certyfikatu. Za pomocą klucza publicznego certyfikatu do weryfikowania podpisów można uwierzytelnić podpis cyfrowy utworzony za pomocą certyfikatu do podpisywania obiektów. Weryfikacja podpisu umożliwia określenie miejsca, skąd pochodzi obiekt oraz sprawdzenie, czy po podpisaniu obiekt nie został zmieniony. Jedynie baza certyfikatów *SIGNATUREVERIFICATION umożliwia zarządzanie tymi typami certyfikatów.

Certyfikaty użytkownika

Certyfikaty użytkowników to cyfrowe świadectwa potwierdzające tożsamość klienta lub użytkownika, który jest właścicielem certyfikatu. Obecnie wiele aplikacji obsługuje certyfikaty, zamiast nazw użytkowników i haseł, w celu uwierzytelniania użytkowników żądających określonych zasobów. Program Menedżer certyfikatów cyfrowych (DCM) automatycznie przypisuje certyfikat użytkownika, wystawiony przez prywatny ośrodek certyfikacji (CA), do profilu tego użytkownika w systemie iSeries. Programu tego można również użyć do powiązania profilu użytkownika w systemie iSeries z certyfikatami użytkownika wystawionymi przez inne ośrodki.

Menedżer certyfikatów cyfrowych (DCM) organizuje certyfikaty według powyższej klasyfikacji i umieszcza je wraz z powiązanimi z nimi kluczami prywatnymi w bazie certyfikatów.

Uwaga: Jeśli w serwerze iSeries zainstalowany jest koprocesor szyfrujący IBM 4758 PCI, można wybrać inne opcje przechowywania kluczy prywatnych dla używanych certyfikatów (z wyjątkiem certyfikatów do podpisywania obiektów). Klucze prywatne można przechowywać w samym koprocesorze. Można również użyć koprocesora do zaszyfrowania klucza prywatnego i

przechowywać go w specjalnym pliku klucza, a nie w bazie certyfikatów. Same certyfikaty użytkowników i ich klucze prywatne są przechowywane w systemie użytkownika albo w oprogramowaniu przeglądarki, albo w pakiecie oprogramowania klienckiego.

Certyfikaty publiczne a certyfikaty prywatne

Gdy zostanie podjęta decyzja o używaniu certyfikatów, należy wybrać implementację certyfikatu, która najlepiej pasuje do danych wymogów bezpieczeństwa. Możliwe opcje uzyskania certyfikatów obejmują:

- zakupienie certyfikatów w publicznym, internetowym ośrodku certyfikacji (CA),
- stworzenie własnego ośrodka certyfikacji (CA) w celu wystawiania prywatnych certyfikatów na potrzeby lokalnych użytkowników i aplikacji,
- używanie kombinacji certyfikatów z publicznego ośrodka internetowego i z własnego ośrodka.

Wybór jednej z powyższych opcji zależy od wielu czynników, wśród których jednym z najważniejszych jest środowisko, w którym używane są certyfikaty. Poniżej przedstawiono pewne informacje mogące pomóc w określeniu, które opcje implementacyjne są najlepsze do określonych wymagań dotyczących firmy i ochrony.

Korzystanie z certyfikatów publicznych

Publiczne internetowe ośrodki certyfikacji (CA) wystawiają certyfikaty każdemu, kto wnieśli odpowiednią opłatę. Jednak ośrodki te przed wystawieniem certyfikatu wymagają potwierdzenia tożsamości. Poziom wymaganych świadectw może być różny, zależnie od strategii identyfikacji stosowanej przez dany ośrodek. Przed podjęciem decyzji o uzyskaniu certyfikatu z danego ośrodka lub zaliczeniu go do ośrodków zaufanych należy ocenić, czy rygorystyczność strategii identyfikacji stosowanej przez ten ośrodek spełnia przyjęte wymogi bezpieczeństwa. W miarę ewolucji standardów infrastruktury klucza publicznego dla protokołu X.509 (PKIX) niektóre nowe publiczne ośrodki certyfikacji (CA) oferują coraz bardziej rygorystyczne procedury identyfikacji przy wystawianiu certyfikatów. Proces uzyskiwania certyfikatów z takich ośrodków jest bardziej złożony, jednak wydawane przez nie certyfikaty zapewniają lepszą ochronę dostępu do aplikacji przez niepowołanymi użytkownikami. Menedżer certyfikatów cyfrowych pozwala na korzystanie i zarządzanie certyfikatami wystawionymi przez ośrodki stosujące te nowe standardy certyfikacji.

Należy również wziąć pod uwagę koszty wystawienia certyfikatu przez ośrodek publiczny. Jeśli certyfikaty są potrzebne ograniczonej liczbie aplikacji serwerów lub klientów i użytkowników, koszt może nie być czynnikiem decydującym. Jednak w przypadku dużej liczby użytkowników *prywatnych* wymagających publicznego certyfikatu do uwierzytelniania klienta, koszt może nabrać szczególnego znaczenia. W takim przypadku należy również rozważyć kroki administracyjne i programistyczne w celu skonfigurowania aplikacji serwera do akceptowania tylko określonego podzbioru certyfikatów wystawianych przez publiczny ośrodek certyfikacji (CA).

Korzystanie z certyfikatów wystawionych przez ośrodki publiczne może przyczynić się do oszczędności czasu i zasobów, ponieważ wiele aplikacji serwerów, klientów i użytkowników rozpoznaje większość powszechnie znanych publicznych ośrodków certyfikacji (CA). Ponadto inne firmy i inni użytkownicy mogą uznawać te certyfikaty i ufać tym z nich wystawianym przez znane ośrodki publiczne bardziej niż certyfikatom wystawianym przez ośrodek prywatny.

Korzystanie z certyfikatów prywatnych

Utworzenie własnego ośrodka certyfikacji (CA) pozwala na wystawianie certyfikatów systemom i użytkownikom w bardziej ograniczonym zakresie, takim jak firma bądź organizacja. Utworzenie i obsługa własnego ośrodka CA umożliwia wystawianie certyfikatów tylko zaufanym członkom grupy, co zwiększa bezpieczeństwo sieci. Dzięki temu, że możliwa jest dokładniejsza kontrola jednostek, które mają certyfikaty, jak również osób, które mają dostęp do zasobów, zwiększa się bezpieczeństwo. Wadą utrzymywania własnego, lokalnego ośrodka certyfikacji jest nakład czasu i zasoby, które trzeba zainwestować. Jednak Menedżer certyfikatów cyfrowych znacznie ułatwia realizację tych czynności.

W przypadku lokalnego ośrodka certyfikacji (CA) wydającego użytkownikom certyfikaty w celu uwierzytelniania programów klienckich, należy podjąć decyzję, czy certyfikaty użytkowników mają być powiązane z profilami użytkownika systemu iSeries. Jeśli certyfikaty użytkowników mają być powiązane profilami użytkownika iSeries, użytkownicy mogą uzyskać certyfikat lokalnego ośrodka certyfikacji (CA) korzystając z programu DCM. Od wersji V5R2, można używać funkcji API do programowego wystawiania certyfikatów użytkownikom systemów innych niż iSeries. Tego typu użytkownicy mogą używać certyfikatu prywatnego do uwierzytelniania programów klienckich, ale nie muszą mieć profilu użytkownika iSeries.

Uwaga: Bez względu na to, który ośrodek CA zostanie wybrany do wystawiania certyfikatów, administrator systemu sprawuje kontrolę nad tym, który ośrodek CA ma być zaufanym dla danego systemu. Jeśli w przeglądarce znajduje się kopia certyfikatu ogólnie znanego ośrodka CA, przeglądarkę tę można skonfigurować tak, aby przyjmowała certyfikaty serwera wysłane przez ten ośrodek CA. Jeśli jednak certyfikatu danego ośrodka nie ma w bazie certyfikatów *SYSTEM, serwer nie może ufać certyfikatom klienta lub użytkownika wystawionym przez ten ośrodek. Aby certyfikaty wydane przez ośrodek CA były uznawane, należy uzyskać kopię certyfikatu CA z tego ośrodka. Kopia ta musi mieć odpowiedni format pliku i musi być dodana do bazy certyfikatów programu DCM.

Podczas rozstrzygnięcia zagadnienia, które certyfikaty, prywatne czy publiczne, lepiej pasują do przyjętych wymogów dotyczących firmy i bezpieczeństwa, pomocne mogą okazać się scenariusze typowych zastosowań certyfikatów.

Zadania pokrewne

Po przyjęciu określonego sposobu używania certyfikatów oraz określeniu typu używanych certyfikatów, w celu wprowadzenia planu w życie, należy zapoznać się procedurami opisanymi w poniższych sekcjach:

- Tworzenie i prowadzenie prywatnego ośrodka certyfikacji, gdzie opisano zadania, które trzeba wykonać, jeśli zdecydowano się na stworzenie ośrodka w celu wystawiania certyfikatów prywatnych.
- Zarządzanie certyfikatami z publicznego internetowego ośrodka certyfikacji, gdzie opisano zadania, które trzeba wykonać, aby móc korzystać z certyfikatów wystawionych przez powszechnie znane ośrodki, w tym również ośrodki działające zgodnie ze standardami PKIX.
- Korzystanie z lokalnych ośrodków certyfikacji na innych serwerach iSeries, gdzie opisano zadania, które trzeba wykonać, jeśli zamierza się używać certyfikatów z prywatnych ośrodków działających w kilku systemach.

Certyfikaty cyfrowe w bezpiecznej komunikacji SSL

Za pomocą certyfikatów cyfrowych można skonfigurować aplikacje do korzystania z protokołu Secure Sockets Layer (SSL) w celu ochrony sesji komunikacyjnych. Aby nawiązać sesję SSL serwer zawsze okazuje do sprawdzenia klientowi żądającemu połączenia kopię swojego certyfikatu. Korzystanie z połączenia SSL:

- zapewnia klienta lub użytkownika o autentyczności serwera,
- udostępnia szyfrowaną sesję komunikacyjną, gwarantującą zachowanie prywatności przesyłanych danych.

W celu zapewnienia bezpieczeństwa danych aplikacje klienta i serwera współpracują ze sobą w następujący sposób:

1. Aplikacja serwera przedstawia certyfikat aplikacji klienta (użytkownika) jako dowód tożsamości serwera.
2. Aplikacja klienta sprawdza tożsamość serwera na podstawie kopii certyfikatu ośrodka certyfikacji (CA), który wystawił certyfikat. (Aplikacja klienta musi mieć dostęp do przechowywanej lokalnie kopii odpowiedniego certyfikatu ośrodka certyfikacji (CA)).
3. Aplikacje serwera i klienta porozumiewają się co do symetrycznego klucza szyfrującego i używają go do szyfrowania sesji komunikacyjnej.

4. Opcjonalnie serwer może wymagać teraz, aby klient okazał swój dowód tożsamości, zanim udostępni mu żądane zasoby. Aby używać certyfikatów jako dowodów tożsamości, komunikujące się ze sobą aplikacje muszą obsługiwać uwierzytelnianie użytkowników za pomocą certyfikatów.

W trakcie uzgadniania sesji protokołu SSL używa algorytmów klucza asymetrycznego (publicznego) do negocjowania klucza symetrycznego, który następnie używany jest do szyfrowania i deszyfrowania danych aplikacji w aktualnej sesji SSL. Oznacza to, że serwer i klient używają różnych kluczy dla każdego połączenia, a ponadto klucze te tracą ważność automatycznie po określonym czasie. Przechwycenie i rozszyfrowanie przez kogoś klucza danej sesji jest nieprawdopodobne, co więcej, nie da się na podstawie danego klucza przewidzieć żadnego przyszłego klucza.

Certyfikaty cyfrowe jako uwierzytelnienie użytkowników

Tradycyjnie użytkownik otrzymuje dostęp do aplikacji lub systemu na podstawie nazwy i hasła użytkownika. Gdy używa się certyfikatów cyfrowych (zamiast nazw użytkowników i haseł), ochronę systemu można rozszerzyć o uwierzytelnianie i autoryzowanie sesji pomiędzy serwerem a użytkownikami. Programu DCM można użyć także do powiązania certyfikatu użytkownika z profilem tego użytkownika w systemie iSeries. W rezultacie, certyfikat otrzymuje te same uprawnienia i prawa dostępu, co profil, do którego został przypisany. Od wersji V5R2, można używać funkcji API, aby programowo wykorzystać prywatny lokalny ośrodek certyfikacji (CA) do wydawania certyfikatów użytkownikom innych systemów niż iSeries. Funkcje API udostępniają możliwość wydawania certyfikatów prywatnych użytkownikom, którzy nie mają profili iSeries.

Certyfikat cyfrowy działa jak elektroniczne uwierzytelnienie i potwierdza, że dana osoba jest rzeczywiście tą, za którą się podaje. Pod tym względem certyfikat jest podobny do paszportu. Oba ustalają tożsamość osoby, zawierają unikalny numer do celów identyfikacyjnych i oba są wystawione przez uznaną władzę potwierdzającą autentyczność uwierzytelnienia. W przypadku certyfikatu ośrodek certyfikacji (CA) działa jako zaufana trzecia strona, która potwierdza autentyczność uwierzytelnienia.

Do celów uwierzytelniania certyfikaty korzystają z klucza publicznego i związanego z nim klucza prywatnego. Do celów identyfikacyjnych ośrodek certyfikacji (CA) wiąże te klucze wraz z informacjami o właścicielu certyfikatu w samym certyfikacie.

Obecnie coraz więcej aplikacji obsługuje certyfikaty do uwierzytelniania klienta podczas sesji SSL. Aktualnie uwierzytelnianie klienta za pomocą certyfikatu obsługują następujące aplikacje iSeries:

- serwer Telnet,
- IBM HTTP Server (oryginalny i oparty na serwerze Apache),
- serwer usług katalogowych (LDAP),
- Centrum Zarządzania,
- Client Access Express (w tym również iSeries Navigator),
- serwer FTP.

W przyszłości, także inne aplikacje będą udostępniały obsługę certyfikatów do uwierzytelniania klientów; dokumentacja poszczególnych aplikacji zawiera informacje, czy taka obsługa jest dostępna.

Certyfikaty zapewniają pewniejsze środki uwierzytelniania klientów z kilku powodów:

- Może zdarzyć się, że użytkownik zapomni hasła. Aby tego uniknąć, należy nauczyć się go na pamięć lub zapisać swoją nazwę użytkownika i hasło. Zapisane dane mogą jednak zostać przejęte przez osoby nieuprawnione. Ponieważ certyfikaty są przechowywane w pliku w formie elektronicznej, obsługą dostępu do certyfikatu i jego prezentacją w celu uwierzytelnienia zajmują się aplikacje typu klient (a nie użytkownicy). Zmniejsza to prawdopodobieństwo przechwycenia certyfikatu przez nieuprawnionych użytkowników, chyba że mają oni dostęp do systemu. Certyfikaty mogą być również instalowane na kartach elektronicznych, co stanowi ich dodatkową ochronę przed nieuprawnionym użyciem.
- Certyfikat obejmuje również klucz prywatny, który jednak nigdy nie jest wysyłany z certyfikatem w celu identyfikacji. System używa tego klucza podczas szyfrowania i deszyfrowania danych. Inni użytkownicy mogą używać odpowiadającego certyfikatu klucza publicznego w celu potwierdzenia tożsamości nadawcy obiektów podpisanych kluczem prywatnym.

- W wielu systemach wymaga się hasła nie dłuższego niż osiem znaków, co sprawia, że hasła takie są bardziej narażone na odgadnięcie. Klucze szyfrujące certyfikatów mają długość setek znaków. Ta długość w połączeniu z losowym charakterem kluczy kryptograficznych sprawia, że klucze te są znacznie trudniejsze do złamania niż hasła.
- Certyfikaty cyfrowe oferują kilka potencjalnych zastosowań, do których nie nadają się hasła, na przykład zapewnienie integralności i prywatności danych. Certyfikatów i powiązanych z nimi kluczy można użyć do:
 - Zapewnienia integralności danych przez wykrywanie w nich zmian.
 - Wykazania, że określone działanie zostało naprawdę wykonane. Określa się to mianem nieodrzucania.
 - Zapewnienia prywatności przesyłanych danych za pomocą protokołu Secure Sockets Layer do szyfrowania sesji.

Więcej informacji o konfigurowaniu aplikacji serwera iSeries w celu korzystania z certyfikatów do uwierzytelniania klientów podczas sesji SSL można znaleźć w publikacji *Securing applications with SSL*.

Certyfikaty cyfrowe w połączeniach VPN

Certyfikaty cyfrowe mogą służyć do utworzenia połączenia VPN dla systemu iSeries. Aby dynamiczne połączenie VPN mogło być aktywowane, obydwa punkty końcowe powinny być w stanie przeprowadzić wzajemne uwierzytelnienie. Uwierzytelnianie punktów końcowych jest realizowane przez serwer protokołu Internet Key Exchange (IKE) na obu końcach łącza. Po pomyślnym uwierzytelnieniu serwery IKE negocjują metodologię i algorytmy szyfrowania, które zostaną użyte w celu zabezpieczenia połączenia VPN.

W wersjach wcześniejszych niż V5R1 serwery IKE mogły się wzajemnie uwierzytelić tylko za pomocą klucza współużytkowanego. Zastosowanie klucza współużytkowanego jest mniej bezpieczne, ponieważ należy go wcześniej przekazać administratorowi drugiego punktu końcowego łącza VPN. Powoduje to niebezpieczeństwo przechwycenia klucza podczas procesu przekazywania.

Ryzyka tego można uniknąć, używając do uwierzytelniania punktów końcowych certyfikatów cyfrowych. Serwer IKE może uwierzytelić certyfikat innego serwera, nawiązać połączenie i negocjować metodologię i algorytmy szyfrowania, które zostaną użyte w celu zabezpieczenia połączenia.

Do zarządzania certyfikatami używanymi przez serwery IKE w celu nawiązywania dynamicznych połączeń VPN można użyć programu Menedżer certyfikatów cyfrowych (DCM). Najpierw jednak należy zdecydować, czy serwer IKE ma korzystać z certyfikatów publicznych, czy wystawić mu certyfikaty prywatne.

Niektóre implementacje sieci VPN wymagają, aby certyfikat zawierał alternatywną nazwę podmiotu, na przykład nazwę domeny lub adres poczty elektronicznej, oprócz standardowej nazwy wyróżniającej. Informacje te można podać w certyfikacie wystawionym przez prywatny ośrodek certyfikacji (CA), utworzonym za pomocą programu DCM. Dzięki tym informacjom, połączenie VPN dla systemu iSeries jest zgodne z innymi implementacjami sieci VPN, które mogą wymagać tych danych do przeprowadzenia uwierzytelnienia.

Aby dowiedzieć się więcej o tym, jak zarządzać certyfikatami dla połączeń VPN, należy zapoznać się z informacjami zawartymi w poniższych źródłach:

- Przy całkowitym braku doświadczeń z wykorzystaniem programu DCM do zarządzania certyfikatami pomocne będą następujące sekcje:
 - Tworzenie i korzystanie z lokalnego prywatnego ośrodka certyfikacji, gdzie opisano, w jaki sposób używać programu DCM do wystawiania dla aplikacji certyfikatów prywatnych.
 - Zarządzanie certyfikatami z publicznego internetowego ośrodka certyfikacji, gdzie opisano, w jaki sposób używać programu DCM do zarządzania certyfikatami uzyskanymi z publicznego ośrodka certyfikacji (CA).
- Użytkownicy korzystający obecnie z programu DCM do zarządzania certyfikatami dla innych aplikacji powinni przejrzeć wymienione poniżej zasoby, aby dowiedzieć się, jak określić, że aplikacja korzysta z istniejącego certyfikatu i które certyfikaty dana aplikacja może zaakceptować i uwierzytelić:

- Zarządzanie przypisaniem certyfikatu aplikacji, gdzie opisano, jak używać programu DCM do przypisania istniejącego certyfikatu aplikacji, na przykład serwerowi IKE.
- Definiowanie listy zaufanych ośrodków certyfikacji dla aplikacji, gdzie opisano, jak określić ośrodki certyfikacji (CA), którym aplikacja może ufać przy akceptacji certyfikatu w celu uwierzytelnienia klienta (lub połączenia VPN).

Podpisywanie obiektów za pomocą certyfikatów cyfrowych

Począwszy od wersji V5R1 system OS/400 obsługuje certyfikaty, które służą do cyfrowego "podpisywania" obiektów. Cyfrowe podpisywanie obiektów jest metodą weryfikowania integralności zawartości obiektu, a także potwierdzenia autentyczności jego źródła pochodzenia. Obsługa podpisywania obiektów wspomaga tradycyjne narzędzia systemu iSeries, służące do kontroli uprawnień użytkowników do zmiany obiektów. Tradycyjne narzędzia nie mogą jednak ochronić obiektów przed nieuprawnioną modyfikacją podczas ich przesyłania poprzez Internet i inne sieci niechronione lub wtedy, gdy są przechowywane w systemie innym niż iSeries. Jednak tradycyjne narzędzia nie zawsze pozwalają stwierdzić, w obiekcie dokonano nieuprawnionych zmian lub manipulacji. Używanie podpisów cyfrowych dla obiektów pozwala wykryć, czy dokonano jakichś zmian w podpisanym obiekcie.

Umieszczenie podpisu cyfrowego na obiekcie polega na zastosowaniu klucza prywatnego certyfikatu do obliczenia zaszyfrowanej sumy danych w obiekcie. Taki podpis chroni dane przed nieuprawnionymi zmianami. Obiekt i jego zawartość nie są zaszyfrowane przez podpis cyfrowy; zaszyfrowana jest tylko suma kontrolna, aby uniemożliwić nieuprawnione zmiany obiektu. Chcąc się upewnić, że obiekt nie został zmieniony podczas przesyłania i że pochodzi z akceptowanego, legalnego źródła, należy użyć klucza publicznego certyfikatu wykorzystanego do podpisu, aby sprawdzić autentyczność podpisu cyfrowego. Jeśli podpis nie będzie zgodny, może to oznaczać, że dane zostały zmienione. W takim przypadku odbiorca nie powinien używać obiektu, tylko skontaktować się z nadawcą, aby przesłał kopię podpisanego obiektu.

Jeśli użycie certyfikatów cyfrowych mieści się w ramach zidentyfikowanych potrzeb i przyjętych strategii bezpieczeństwa, należy jeszcze rozstrzygnąć, czy powinno się używać certyfikatów publicznych, czy wystawiać certyfikaty prywatne. W przypadku dystrybucji obiektów do użytkowników publicznych, należy rozważyć zastosowanie do podpisania obiektów certyfikatów z ogólnie znanego publicznego ośrodka certyfikacji (CA). Certyfikaty publiczne pozwalają innym łatwo i tanio zweryfikować podpisy złożone na wysyłanych im obiektach. Jeśli jednak zamierza się rozpowszechniać obiekty wyłącznie w ramach własnej organizacji, wygodniejsze może być użycie Menedżera certyfikatów cyfrowych (DCM) w celu utworzenia prywatnego, lokalnego ośrodka certyfikacji (CA) i wystawiania prywatnych certyfikatów do podpisywania obiektów. Wystawianie prywatnych certyfikatów lokalnego ośrodka certyfikacji (CA) jest mniej kosztowne niż kupowanie ich w zewnętrznych publicznych ośrodkach certyfikacji (CA).

Podpis na obiekcie reprezentuje system, który podpisał ten obiekt, a nie konkretnego użytkownika tego systemu (choć użytkownik musi mieć odpowiednie uprawnienia, aby użyć certyfikatu do podpisania obiektu). Menedżer certyfikatów cyfrowych (DCM) umożliwia zarządzanie certyfikatami używanymi do podpisywania obiektów oraz do weryfikowania podpisów obiektów. Menedżer certyfikatów cyfrowych (DCM) umożliwia również podpisywanie obiektów oraz weryfikowanie podpisów obiektów.

Certyfikaty cyfrowe do weryfikowania podpisów obiektów

Począwszy od wersji V5R1 serwery iSeries obsługują certyfikaty do weryfikacji podpisów cyfrowych obiektów. Chcąc się upewnić, że podpisany obiekt nie został zmieniony podczas przesyłania i że pochodzi z akceptowanego, legalnego źródła, należy użyć klucza publicznego certyfikatu wykorzystanego do podpisu, aby sprawdzić autentyczność podpisu cyfrowego. Jeśli podpis nie będzie zgodny, może to oznaczać, że dane zostały zmienione. W takim przypadku odbiorca nie powinien używać obiektu, tylko skontaktować się z nadawcą, aby przesłał kopię podpisanego obiektu.

Podpis na obiekcie reprezentuje system, który podpisał ten obiekt, a nie konkretnego użytkownika tego systemu. Elementem procesu weryfikacji podpisów cyfrowych musi być decyzja o tym, które ośrodki certyfikacji (CA) uznaje się za zaufane i które certyfikaty uznaje się za zaufane przy podpisywaniu obiektów.

Po wyborze zaufanych ośrodków certyfikacji (CA) można zdecydować, czy uznaje się za zaufane podpisy utworzone przez innych za pomocą certyfikatu wystawionego przez te ośrodki. Uznanie ośrodka certyfikacji (CA) za niewiarygodny oznacza jednocześnie uznanie za niewiarygodne certyfikatów wystawionych przez ten ośrodek i utworzonych za pomocą tych certyfikatów podpisów.

Wartość systemowa Weryfikacja odtwarzania obiektu (Verify object restore - QVfyOBJRST)

Decydując się na stosowanie weryfikacji podpisów, należy najpierw określić, jak ważne są te podpisy dla obiektów odtwarzanych w systemie. Służy do tego wartość systemowa o nazwie QVfyOBJRST. Domyślne ustawienie tej wartości systemowej umożliwia odtwarzanie niepodpisanych obiektów, ale zapewnia jednocześnie, że obiekty podpisane mogą być odtworzone tylko wtedy, gdy ich podpis jest prawidłowy. System określa obiekt jako podpisany tylko wtedy, gdy ma on podpis elektroniczny ośrodka certyfikacji (CA), któremu system ufa; system ignoruje inne "niewiarygodne" podpisy obiektów i traktuje te obiekty jako niepodpisane.

Istnieje kilka opcji ustawień, których można użyć dla wartości systemowej QVfyOBJRST, począwszy od ignorowania wszystkich podpisów, aż do wymagania prawidłowych podpisów od wszystkich obiektów odtwarzanych w systemie. Wartość ta dotyczy jedynie odtwarzanych obiektów wykonywalnych, a nie zbiorów składowania czy plików systemu IFS. Więcej informacji na temat tej i innych wartości systemowych można znaleźć w sekcji System Value Finder w Centrum informacyjnym.

Menedżer certyfikatów cyfrowych (DCM) umożliwia implementację decyzji o zaufanych ośrodkach certyfikacji (CA) i certyfikatach, a także zarządzanie certyfikatami używanymi do weryfikowania podpisów obiektów. Menedżer certyfikatów cyfrowych (DCM) umożliwia również podpisywanie obiektów oraz weryfikowanie podpisów obiektów.

Rozdział 7. Konfigurowanie programu DCM

Menedżer certyfikatów cyfrowych (DCM) posiada, wzorowany na przeglądarce, interfejs użytkownika, za pomocą którego można zarządzać certyfikatami cyfrowymi aplikacji i użytkowników. Interfejs użytkownika dzieli się na dwie ramki: ramkę nawigacji i ramkę zadań.

Ramka nawigacji służy do wyboru zadań związanych z zarządzaniem certyfikatami lub używającymi ich aplikacjami. Mimo że niektóre indywidualne zadania są wyświetlane bezpośrednio w ramce nawigacji, większość z nich jest tam pogrupowana w kategorie. Na przykład **Zarządzanie certyfikatami** jest kategorią zadań obejmującą różne indywidualne zadania, takie jak wyświetlenie certyfikatu, odnowienie certyfikatu, import certyfikatu i tym podobne. Jeśli pozycja w ramce nawigacji jest kategorią zawierającą więcej niż jedno zadanie, po jej lewej stronie jest wyświetlana strzałka. Strzałka ta informuje, że wybór odsyłacza kategorii spowoduje wyświetlenie rozszerzonej listy zadań, z której można wybrać konkretne zadanie do wykonania.

Wszystkie zadania w ramce nawigacji, z wyjątkiem zadań w kategorii **Krótką ścieżką**, to zadania wykonywane w kilku etapach. Kategoria Krótka ścieżka obejmuje szereg funkcji zarządzających certyfikatami i aplikacjami, które umożliwiają doświadczonym użytkownikom programu DCM szybki dostęp do zadań pokrewnych z centralnego zestawu stron.

To, które zadania są dostępne w ramce nawigacji, zależy od bazy certyfikatów, w której się pracuje. Ponadto, kategoria i liczba zadań dostępnych w ramce nawigacji zależy od uprawnień profilu użytkownika iSeries. Wszystkie zadania dotyczące prowadzenia ośrodka certyfikacji (CA), zarządzania certyfikatami używanymi przez aplikacje i zadania systemowe są dostępne tylko szefom ochrony i administratorom systemu iSeries. Aby przeglądać i wykonywać te działania, szef ochrony lub administrator muszą mieć uprawnienia specjalne *SECADM i *ALLOBJ. Użytkownicy nieposiadający odpowiednich uprawnień mają jedynie dostęp do funkcji dotyczących certyfikatów użytkownika.

Aby dowiedzieć się, w jaki sposób skonfigurować program DCM oraz używać go do zarządzania certyfikatami, należy zapoznać się z poniższymi tematami:

Uruchomienie DCM

Sekcja zawiera informacje o sposobie dostępu do funkcji zarządzania certyfikatami cyfrowymi w systemie iSeries.

Pierwsze konfigurowanie certyfikatów

Sekcja zawiera informacje, jak rozpocząć korzystanie z programu DCM i jak skonfigurować ustawienia niezbędne do korzystania z certyfikatów po raz pierwszy. Ponadto w sekcji opisano, jak rozpocząć zarządzanie certyfikatami otrzymanymi z publicznego, internetowego ośrodka certyfikacji oraz jak utworzyć i poprowadzić lokalny ośrodek w celu wystawiania certyfikatów.

Doskonałym źródłem dokładniejszych informacji o korzystaniu z certyfikatów cyfrowych w środowisku internetowym, w celu zwiększenia bezpieczeństwa systemu i sieci, jest serwis WWW VeriSign. Zawiera on bogatą bibliotekę publikacji poświęconych certyfikatom cyfrowym, a także innym zagadnieniom związanym z bezpieczeństwem w Internecie. Do biblioteki tej można uzyskać dostęp przez odsyłacz VeriSign Help Desk



Uruchomienie Menedżera certyfikatów cyfrowych (DCM)

Przed użyciem dowolnej funkcji programu DCM, należy go najpierw uruchomić. Aby pomyślnie uruchomić program DCM, wykonaj następujące czynności:

1. Zainstaluj opcję 34 5722 SS1. Jest to Menedżer certyfikatów cyfrowych (DCM).
Zainstaluj serwer 5722 DG1. Jest to serwer IBM HTTP Server for iSeries.

Zainstaluj produkt 5722 AC3. Jest to produkt szyfrujący, którego program DCM V5R2 używa do generowania dla certyfikatów par kluczy publiczny-prywatny, do szyfrowania eksportowanych plików certyfikatów i do deszyfrowania importowanych plików certyfikatów.

2. Za pomocą programu iSeries Navigator uruchom instancję *ADMIN serwera HTTP:
 - a. Uruchom program **iSeries Navigator**.
 - b. Dwukrotnie kliknij ikonę lokalnego serwera iSeries w widoku głównego drzewa.
 - c. Dwukrotnie kliknij **Sieć**.
 - d. Dwukrotnie kliknij **Serwery**.
 - e. Dwukrotnie kliknij **TCP/IP**.
 - f. Prawym przyciskiem myszy kliknij **Administrowanie HTTP**.
 - g. Kliknij **Uruchom**.
3. Uruchom przeglądarkę WWW.
4. Za pomocą przeglądarki przejdź do strony Zadania iSeries w systemie pod adresem `http://nazwa_twojego_systemu:2001`.
5. Z listy produktów na stronie Zadania iSeries wybierz **Menedżer certyfikatów cyfrowych**, aby uruchomić opcję DCM.

W przypadku migracji z wcześniejszej wersji programu DCM, na tej stronie zostaną wyświetlone zadania wymagane do aktualizacji systemu.

Pierwsze konfigurowanie certyfikatów

Lewa część okna Menedżera certyfikatów cyfrowych (DCM) to ramka nawigacji. W ramce tej można wybrać jedno z wielu zadań zarządzania certyfikatami i używającymi ich aplikacjami. To, które zadania są dostępne, zależy od tego, która baza certyfikatów została otwarta (jeśli jakaś baza została otwarta) oraz od uprawnień profilu użytkownika. Większość zadań jest dostępna tylko użytkownikom posiadającym uprawnienia specjalne *ALLOBJ i *SECADM.

Przy pierwszym uruchomieniu Menedżera certyfikatów cyfrowych żadna baza certyfikatów nie istnieje (chyba że zaktualizowano poprzednią wersję programu DCM). Dlatego w ramce nawigacji wyświetlane są jedynie następujące zadania (pod warunkiem że użytkownik ma wystarczające uprawnienia):

- Zarządzanie certyfikatami użytkownika.
- Tworzenie nowej bazy certyfikatów.
- Tworzenie ośrodka certyfikacji (CA). (Uwaga: Po wykonaniu tego zadania i utworzeniu prywatnego ośrodka certyfikacji (CA) nie jest ono już wyświetlane na liście.)
- Zarządzanie położeniami list CRL.
- Zarządzanie położeniem żądań PKIX.

Nawet jeśli w systemie istnieją już bazy certyfikatów (na przykład w wyniku migracji z wcześniejszej wersji programu DCM), w lewej ramce nawigacji programu DCM wyświetla się ograniczona liczba zadań lub kategorii zadań. Aby rozpocząć wykonywanie większości zadań związanych z zarządzaniem certyfikatami i aplikacjami, należy najpierw otworzyć bazę certyfikatów. W tym celu należy kliknąć zadanie **Wybór bazy certyfikatów** w ramce nawigacji.

Ramka nawigacji programu DCM udostępnia również przycisk **Połączenie chronione**. Za pomocą tego przycisku można otworzyć drugie okno przeglądarki w celu zainicjowania bezpiecznego połączenia za pomocą protokołu Secure Sockets Layer (SSL). Funkcja ta będzie działała prawidłowo, jeśli wcześniej IBM HTTP Server for iSeries zostanie skonfigurowany do pracy w trybie chronionym z wykorzystaniem protokołu SSL. Następnie należy uruchomić serwer HTTP w trybie chronionym. Jeśli serwer HTTP nie zostanie odpowiednio skonfigurowany i uruchomiony w trybie SSL, wyświetli się komunikat o błędzie i przeglądarka nie będzie mogła uruchomić bezpiecznej sesji.

Wprowadzenie

Za pomocą certyfikatów można realizować wiele zadań związanych z bezpieczeństwem, jednak pierwsze kroki zależą od tego, jak zaplanowano uzyskanie certyfikatów. Gdy po raz pierwszy używa się programu DCM, można wybrać jedną z dwóch głównych ścieżek postępowania, zależnie od tego, czy zamierza się używać certyfikatów publicznych, czy wystawiać certyfikaty prywatne:

Tworzenie i prowadzenie lokalnego ośrodka certyfikacji w celu wystawiania certyfikatów aplikacjom.

Zarządzanie certyfikatami z publicznego internetowego ośrodka certyfikacji używanymi przez lokalne aplikacje.

Tworzenie i prowadzenie lokalnego ośrodka certyfikacji

Załóżmy, że po dokładnym przeanalizowaniu wymagań i strategii ochrony zdecydowano się na prowadzenie lokalnego ośrodka certyfikacji (CA) w celu wystawiania prywatnych certyfikatów używanym aplikacjom. Własny lokalny ośrodek można utworzyć i administrować nim za pomocą programu Menedżer certyfikatów cyfrowych (DCM). Program DCM udostępnia ścieżki zadań z instrukcjami, które pomagają w procesie tworzenia ośrodka i wykorzystywania go do wystawiania certyfikatów dla aplikacji. W ten sposób program zapewnia wszystkie elementy niezbędne do rozpoczęcia korzystania z certyfikatów cyfrowych, konfigurowania obsługi protokołu SSL przez aplikacje oraz do podpisywania obiektów i weryfikowania podpisów.

Uwaga: Aby używać certyfikatów na serwerze IBM HTTP Server for iSeries, należy przed uruchomieniem programu DCM utworzyć i skonfigurować serwer WWW. Podczas konfigurowania warstwy SSL na serwerze WWW, tworzony jest ID aplikacji dla tego serwera. Identyfikator ten należy zapisać, aby można było wskazać w programie DCM certyfikat, którego aplikacja ma używać dla tego ID.

Nie należy zatrzymywać ani restartować serwera, dopóki w programie DCM nie przypisze się temu serwerowi certyfikatu. Jeśli instancja *ADMIN serwera WWW zostanie zatrzymana przed przypisaniem certyfikatu, serwer nie uruchomi się i nie będzie można użyć programu DCM do przypisania certyfikatu serwerowi.

Aby utworzyć i skonfigurować lokalny ośrodek CA za pomocą programu DCM, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić szereg formularzy. Formularze te prowadzą przez proces tworzenia lokalnego ośrodka certyfikacji (CA), podpisywania obiektów, weryfikowania podpisów i wykonywania innych zadań niezbędnych do rozpoczęcia korzystania z certyfikatów cyfrowych dla potrzeb protokołu SSL.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

3. Wypełnij wszystkie formularze zadań. Jeśli korzystasz z tych formularzy podczas wykonywania wszystkich zadań niezbędnych do utworzenia lokalnego ośrodka certyfikacji (CA):
 - a. Wybierz sposób przechowywania klucza prywatnego dla certyfikatu lokalnego ośrodka certyfikacji (CA). (Czynność ta jest niezbędna tylko wtedy, gdy w systemie iSeries zainstalowano koprocesor szyfrujący IBM 4758–023 PCI. Jeśli w systemie nie ma koprocesora szyfrującego, program DCM automatycznie przechowuje certyfikat i jego klucz prywatny w bazie certyfikatów lokalnego ośrodka certyfikacji (CA).)
 - b. Wprowadź informacje identyfikujące lokalny ośrodek certyfikacji (CA).
 - c. Zainstaluj certyfikat lokalnego ośrodka na komputerze PC lub w przeglądarce, tak aby oprogramowanie mogło rozpoznać ten ośrodek i sprawdzać poprawność wystawianych przez niego certyfikatów.
 - d. Wybierz strategię dla lokalnego ośrodka certyfikacji (CA).
 - e. Użyj nowego, lokalnego ośrodka do wystawienia serwerowi lub klientowi certyfikatu, którego będą używać aplikacje podczas połączeń SSL. (Jeśli w serwerze iSeries zainstalowano koprocesor szyfrujący IBM 4758–023 PCI, krok stwarza możliwość określenia sposobu przechowywania klucza prywatnego certyfikatu serwera lub klienta. Jeśli w systemie nie ma tego koprocesora, program DCM

automatycznie umieszcza certyfikat i jego klucz prywatny w bazie certyfikatów *SYSTEM. Program DCM tworzy bazę certyfikatów *SYSTEM w ramach tego podzadania.)

- f. Wybierz aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL.

Uwaga: Jeśli baza certyfikatów *SYSTEM została już utworzona podczas zarządzania certyfikatami z publicznego, internetowego ośrodka rejestracji, nie należy wykonywać tej ani poprzedniej czynności.

- g. Użyj nowego, lokalnego ośrodka certyfikacji (CA) do wystawienia certyfikatu, którego aplikacje będą używać do podpisywania obiektów. W tym podzadaniu tworzy się bazę certyfikatów *OBJECTSIGNING; jest to baza służąca zarządzaniu certyfikatami do podpisywania obiektów.
- h. Wybierz aplikacje, które mogą używać tego certyfikatu do cyfrowego podpisywania obiektów.

Uwaga: Jeśli baza certyfikatów *OBJECTSIGNING została już utworzona podczas zarządzania certyfikatami do podpisywania obiektów z publicznego, internetowego ośrodka rejestracji, nie należy wykonywać tej ani poprzedniej czynności.

- i. Wybierz aplikacje, które powinny ufać utworzonemu lokalnemu ośrodkowi certyfikacji (CA).

Po zakończeniu całej procedury spełnione są wszelkie warunki konieczne do konfigurowania aplikacji do korzystania z protokołu SSL w celu bezpiecznej komunikacji.

Po skonfigurowaniu aplikacji użytkownicy korzystający z nich poprzez połączenia SSL muszą użyć programu DCM, aby uzyskać kopię certyfikatu lokalnego ośrodka certyfikacji (CA). Każdy użytkownik musi mieć kopię tego certyfikatu, tak aby używane przez niego oprogramowanie typu klient mogło uwierzytelnić tożsamość serwera w procesie negocjacji SSL. Użytkownicy mogą za pomocą programu DCM skopiować certyfikat lokalnego ośrodka do pliku lub pobrać go do przeglądarki. Sposób przechowywania certyfikatu lokalnego ośrodka zależy od oprogramowania typu klient używanego do nawiązywania połączeń SSL z aplikacją.

Lokalnego ośrodka certyfikacji (CA) można również używać do wystawiania certyfikatów aplikacjom w innych systemach iSeries.

Więcej informacji na temat wykorzystania programu DCM do zarządzania certyfikatami użytkownika oraz uzyskania kopii certyfikatu lokalnego ośrodka certyfikacji (CA) do uwierzytelniania certyfikatów wystawionych przez lokalny ośrodek certyfikacji zawierają sekcje:

Zarządzanie certyfikatami użytkowników

Sekcja zawiera informacje, w jaki sposób użytkownicy mogą uzyskać certyfikaty z programu DCM lub powiązać istniejące certyfikaty z posiadanymi profilami użytkowników systemu iSeries.

Używanie funkcji API do programowego wydawania certyfikatów użytkownikom innych systemów niż iSeries

Sekcja zawiera informacje, w jaki sposób wykorzystać lokalny ośrodek certyfikacji (CA) do wystawienia certyfikatów prywatnych użytkownikom bez wiązania ich z profilami użytkowników systemu iSeries.

Uzyskanie kopii certyfikatu prywatnego ośrodka certyfikacji

W sekcji opisano, jak uzyskać kopię certyfikatu ośrodka prywatnego i jak zainstalować ją na komputerze PC, aby można było uwierzytelnić dowolny certyfikat serwera wystawiony przez ten ośrodek.

Zarządzanie certyfikatami użytkowników

Użytkownicy systemu mogą korzystać z programu Menedżer certyfikatów cyfrowych (DCM) do zarządzania certyfikatami niezbędnymi do uczestniczenia w sesjach komunikacyjnych protokołu Secure Sockets Layer (SSL).

Jeśli użytkownicy mają dostęp do publicznych lub wewnętrznych serwerów poprzez połączenia SSL, muszą mieć kopię certyfikatu ośrodka certyfikacji, który wystawił certyfikat serwera. Jest ona niezbędna do tego, aby oprogramowanie klienta mogło sprawdzić autentyczność certyfikatu serwera i nawiązać połączenie. Jeśli serwer używa certyfikatu z publicznego ośrodka certyfikacji (CA), oprogramowanie użytkowników powinno już mieć kopię certyfikatu tego ośrodka. W rezultacie ani administrator programu DCM, ani

użytkownicy nie muszą podejmować żadnych dodatkowych działań w celu nawiązania połączeń SSL. Jeśli jednak serwer używa certyfikatu z lokalnego ośrodka prywatnego, użytkownicy muszą najpierw uzyskać kopie certyfikatu ośrodka lokalnego, aby móc nawiązywać połączenia SSL z serwerem.

Ponadto, jeśli aplikacja serwera obsługuje i wymaga uwierzytelnienia klienta za pomocą certyfikatu, użytkownicy muszą przedstawić akceptowalne certyfikaty użytkowników, aby uzyskać dostęp do zasobów serwera. W zależności od przyjętych wymogów bezpieczeństwa użytkownicy mogą przedstawiać certyfikaty z publicznych internetowych ośrodków certyfikacji (CA) lub certyfikaty uzyskane w ośrodku prowadzonym lokalnie. W przypadku aplikacji serwera udostępniającej zasoby użytkownikom wewnętrznym posiadającym profile użytkowników iSeries, programu DCM można użyć do dodania certyfikatów użytkowników do ich profili. Zapewni to taki sam poziom praw dostępu do zasobów podczas posługiwania się certyfikatem, jaki został przyznany profilom użytkowników.

Menedżer certyfikatów cyfrowych (DCM) umożliwia zarządzanie certyfikatami przypisanymi do profili użytkowników systemu iSeries. Profil użytkownika z uprawnieniami specjalnymi *ALLOBJ pozwala na zarządzanie przypisywaniem certyfikatów do profili wszystkich użytkowników. Odpowiednie zadania dostępne są w ramce nawigacji na stronie **Zarządzanie certyfikatami użytkownika**, o ile nie jest otwarta żadna baza certyfikatów lub jest otwarta baza certyfikatów lokalnego ośrodka certyfikacji. Jeśli otwarta jest inna baza certyfikatów, zadania dotyczące certyfikatów użytkowników są zintegrowane z zadaniami na stronie **Zarządzanie certyfikatami**.

Użytkownicy, których profile nie posiadają specjalnych uprawnień *SECADM i *ALLOBJ, mogą zarządzać jedynie przypisywaniem certyfikatów do własnego profilu użytkownika. Mogą oni użyć zadań na stronie **Zarządzanie certyfikatami użytkownika** w celu obejrzenia certyfikatów związanych ze swoim profilem użytkownika, usunięcia certyfikatu z profilu lub przypisania certyfikatu z innego ośrodka certyfikacji (CA) do swojego profilu użytkownika. Oprócz uprawnień specjalnych dla swojego profilu użytkownika, użytkownicy mogą uzyskać certyfikat użytkownika z lokalnego ośrodka certyfikacji (CA) po zaznaczeniu w głównej ramce nawigacji zadania **Tworzenie certyfikatu**.

Więcej informacji na temat korzystania z programu DCM do zarządzania i tworzenia certyfikatów użytkowników można znaleźć w sekcjach:

Tworzenie certyfikatu użytkownika

Sekcja ta zawiera informacje opisujące, w jaki sposób użytkownicy mogą uzyskać certyfikat do uwierzytelniania klienta z lokalnego ośrodka certyfikacji (CA).

Przypisanie certyfikatu użytkownika

W tej sekcji opisano, w jaki sposób powiązać posiadany certyfikat ze swoim profilem użytkownika. Certyfikat może pochodzić z prywatnego ośrodka lokalnego w innym systemie lub z ogólnie znanego ośrodka internetowego. Aby można było przypisać certyfikat do profilu użytkownika, ośrodek, który go wystawił, musi być uznawany przez serwer za zaufany i certyfikatu tego nie można przypisać profilowi użytkownika w systemie.

Tworzenie certyfikatu użytkownika: Jeśli do uwierzytelniania użytkowników mają służyć certyfikaty cyfrowe, wszyscy użytkownicy muszą posiadać takie certyfikaty. Jeśli za pomocą programu Menedżer certyfikatów cyfrowych (DCM) prowadzi się prywatny lokalny ośrodek certyfikacji, można używać tego ośrodka do wystawiania certyfikatów dla każdego użytkownika. Każdy użytkownik musi skorzystać z programu DCM, aby wykonując zadanie **Tworzenie certyfikatu** uzyskać certyfikat. Aby jednak było to możliwe, strategia lokalnego ośrodka certyfikacji (CA) musi zezwalać na wystawianie certyfikatów użytkowników.

Aby uzyskać certyfikat z lokalnego ośrodka certyfikacji (CA), wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji wybierz **Tworzenie certyfikatu**.
3. Jako typ tworzonego certyfikatu wybierz **Certyfikat użytkownika**. Zostanie wyświetlony formularz, w którym należy wpisać informacje identyfikacyjne dla certyfikatu.
4. Wypełnij formularz i kliknij **Kontynuuj**.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

5. W tym momencie program DCM współpracuje z przeglądarką w celu utworzenia prywatnego i publicznego klucza dla certyfikatu. Przeglądarka może w tym celu wyświetlić wiele okien. Postępuj zgodnie z instrukcjami wyświetlanymi przez przeglądarkę. Po wygenerowaniu kluczy przez przeglądarkę wyświetla się strona potwierdzająca utworzenie certyfikatu przez program DCM.
6. Zainstaluj w przeglądarce nowy certyfikat. Przeglądarka może w tym celu wyświetlić wiele okien. Wykonaj polecenia podawane przez przeglądarkę w celu zakończenia tego zadania.
7. Kliknij **OK**, aby zakończyć.

Podczas przetwarzania Menedżer certyfikatów cyfrowych (DCM) automatycznie przypisuje certyfikat do profilu użytkownika iSeries.

Aby używany do uwierzytelniania klienta certyfikat użytkownika wystawiony przez inny ośrodek certyfikacji (CA) miał takie same uprawnienia jak profil użytkownika, można użyć programu DCM w celu przypisania certyfikatu do profilu użytkownika.

Przypisanie certyfikatu użytkownika: Jeśli do uwierzytelniania użytkowników mają służyć certyfikaty cyfrowe, wszyscy użytkownicy muszą posiadać takie certyfikaty. Jeśli mają to być certyfikaty z publicznego internetowego ośrodka certyfikacji, użytkownicy mogą korzystać z programu Menedżer certyfikatów cyfrowych (DCM) celem przypisania tych certyfikatów do swoich profili użytkowników. Pozwala to użytkownikom na stosowanie programu DCM do zarządzania tymi certyfikatami.

Do skorzystania z zadania **Przypisanie certyfikatu użytkownika** potrzebna jest bezpieczna sesja komunikacyjna z serwerem HTTP, poprzez którą uzyskuje się dostęp do programu Menedżer certyfikatów cyfrowych (DCM). To, czy sesja jest bezpieczna, zależy od numeru portu w adresie URL używanym do połączenia z programem DCM. Jeśli został użyty port 2001, który jest domyślnym portem do połączeń z programem DCM, sesja nie jest bezpieczna. Przed przejściem w tryb bezpiecznej sesji, konieczne jest również skonfigurowanie serwera HTTP do korzystania z protokołu SSL.

Po wybraniu tego zadania zostanie wyświetlone nowe okno przeglądarki. Jeśli bezpieczna sesja nie została uruchomiona, program DCM zażąda wybrania zadania **Przypisanie certyfikatu użytkownika**, aby ją uruchomić. Następnie program DCM zainicjuje negocjacje protokołu Secure Sockets Layer (SSL) z przeglądarką.

Podczas tych negocjacji przeglądarka może zapytać o to, czy ma ufać ośrodkowi certyfikacji, który wystawił certyfikat identyfikujący serwer HTTP. Może również zapytać, czy zaakceptować sam certyfikat serwera.

Po zezwoleniu przeglądarce na uznanie ośrodka certyfikacji (CA) za zaufany i na akceptację certyfikatu serwera serwer może zażądać okazania certyfikatu w celu uwierzytelnienia klienta. Zależnie od ustawień konfiguracyjnych przeglądarki może ona zapytać o wybór certyfikatu do okazania w celu uwierzytelnienia. Jeśli przeglądarka okaże certyfikat z ośrodka uznanego przez system za zaufany, program DCM wyświetli informację o certyfikacie w osobnym oknie. Jeśli okazany certyfikat nie zostanie zaakceptowany, zamiast niego serwer może zażądać podania nazwy użytkownika i hasła w celu uwierzytelnienia przed przydzieleniem dostępu.

Po nawiązaniu bezpiecznej sesji program DCM próbuje wczytać odpowiedni certyfikat z przeglądarki w celu powiązania go z profilem użytkownika. Jeśli próba ta powiedzie się, będzie można przejrzeć wczytane certyfikaty i wybrać ten, który ma zostać powiązany z profilem użytkownika.

Jeśli program DCM nie wyświetli informacji z certyfikatu, powiązanie certyfikatu z profilem użytkownika nie będzie możliwe. Przyczyną tego może być problem z certyfikatem użytkownika. Na przykład znajdujący się w przeglądarce certyfikat może już być powiązany z profilem użytkownika.

Jeśli preferuje się wykorzystanie lokalnego ośrodka certyfikacji (CA) do wystawiania certyfikatów, użytkownicy, zamiast przypisywać certyfikaty do profili, muszą utworzyć certyfikaty użytkowników.

Używanie funkcji API do programowego wydawania certyfikatów użytkownikom innych systemów niż iSeries

Począwszy od wersji V5R2, dostępne są dwie nowe funkcje API, których można użyć do programowego wydawania certyfikatów użytkownikom systemów innych niż iSeries. We wcześniejszych wersjach, gdy do wydawania użytkownikom certyfikatów używany był lokalny ośrodek certyfikacji (CA), wydane certyfikaty były automatycznie wiązane z profilami użytkownika systemu iSeries. W efekcie, aby wykorzystywać lokalny ośrodek certyfikacji (CA) do wydawania certyfikatów użytkownikom w celu przeprowadzania uwierzytelniania klienta, każdy użytkownik musiał mieć profil użytkownika w systemie iSeries. Każdy użytkownik, który chciał uzyskać z lokalnego ośrodka certyfikacji (CA) certyfikat do uwierzytelniania klientów, musiał używać programu DCM, a więc musiał mieć własny profil użytkownika w systemie iSeries, który umożliwia dostęp do programu DCM oraz poprawne wpisanie się do tego systemu iSeries.

Powiązanie certyfikatu z profilem użytkownika ma wiele zalet, szczególnie gdy obsługiwani są wewnętrzni użytkownicy systemu. Jednak wymienione ograniczenia i wymagania czynią to rozwiązanie mniej praktycznym, gdy lokalny ośrodek certyfikacji (CA) używany jest do wystawiania certyfikatów wielu użytkownikom, a szczególnie gdy nie przewiduje się tworzenia profili dla wszystkich tych użytkowników w systemie iSeries. Jeśli profile nie zostaną udostępnione tym użytkownikom, to w przypadku stosowania uwierzytelniania użytkowników za pomocą certyfikatów będą oni zmuszeni do płacenia za certyfikaty znanego, publicznego ośrodka certyfikacji (CA).

Dwie nowe funkcje API udostępniają interfejs do tworzenia, dla dowolnej nazwy użytkownika, certyfikatów użytkownika podpisanych przez certyfikat lokalnego ośrodka certyfikacji (CA). Certyfikat ten nie będzie powiązany z profilem użytkownika. Dlatego użytkownik nie musi posiadać profilu na serwerze iSeries, który udostępnia program DCM oraz program ten nie musi być używany do tworzenia certyfikatu.

Dwie funkcje API, dla obu głównych przeglądarek, można wywołać, używając narzędzia Net.Data, do tworzenia programu wystawiającego certyfikaty użytkownikom. Aby tworzona aplikacja mogła używać lokalnego ośrodka certyfikacji (CA) do podpisywania certyfikatów, musi udostępniać kod interfejsu GUI niezbędny do tworzenia certyfikatu użytkownika oraz wywołania odpowiedniej funkcji API.

Więcej informacji na temat używania funkcji API zawierają sekcje:

- Generate and Sign User Certificate Request (QYUGSUC) API.
- Sign User Certificate Request (QYCUSUC) API.

Uzyskanie kopii certyfikatu prywatnego ośrodka certyfikacji

Podczas dostępu do serwera poprzez połączenie Secure Sockets Layer (SSL) serwer przedstawia oprogramowaniu klienta certyfikat jako dowód swojej tożsamości. Oprogramowanie klienta musi następnie sprawdzić certyfikat serwera, aby mógł on nawiązać połączenie. Aby sprawdzić certyfikat serwera, oprogramowanie klienta musi mieć dostęp do lokalnie przechowywanej kopii certyfikatu ośrodka certyfikacji (CA), który wystawił certyfikat serwera. Jeśli serwer przedstawia certyfikat z publicznego ośrodka certyfikacji (CA), używana przeglądarka lub inne oprogramowanie klienta powinno już mieć kopię certyfikatu tego ośrodka. Jeśli jednak serwer przedstawia certyfikat z prywatnego lokalnego ośrodka certyfikacji (CA), należy użyć Menedżera certyfikatów cyfrowych (DCM) do uzyskania kopii certyfikatu tego ośrodka.

Za pomocą programu DCM można pobrać certyfikat lokalnego ośrodka certyfikacji (CA) bezpośrednio do przeglądarki lub skopiować go do pliku, aby inne programy klienta również miały do niego dostęp i mogły z niego korzystać. Jeśli używa się zarówno przeglądarki, jak i innych aplikacji do bezpiecznych połączeń, może być konieczne zastosowanie obydwu metod instalacji certyfikatu lokalnego ośrodka. W takim przypadku należy najpierw zainstalować certyfikat w przeglądarce, a dopiero potem skopiować go i wkleić do pliku.

Jeśli aplikacja serwera wymaga, aby użytkownik uwierzytelił się, przedstawiając certyfikat lokalnego ośrodka certyfikacji (CA), należy pobrać certyfikat tego ośrodka do przeglądarki przed wystąpieniem o certyfikat użytkownika z lokalnego ośrodka.

Aby za pomocą programu DCM uzyskać kopię certyfikatu lokalnego ośrodka certyfikacji (CA), wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji wybierz **Instalowanie certyfikatu lokalnego ośrodka CA na komputerze PC**, aby wyświetlić stronę umożliwiającą pobranie certyfikatu lokalnego ośrodka do przeglądarki lub zapisanie go w pliku w systemie lokalnym.
3. Zaznacz metodę uzyskania certyfikatu lokalnego ośrodka.
 - a. Zaznacz **Instalowanie certyfikatu**, aby pobrać certyfikat lokalnego ośrodka certyfikacji (CA) do przeglądarki jako użytkownika zaufanego. Dzięki temu przeglądarka będzie mogła nawiązywać bezpieczne sesje komunikacyjne z serwerami używającymi certyfikatów z tego ośrodka. Przeglądarka będzie wyświetlać kolejne okna, aby pomóc w procesie instalacji.
 - b. Zaznacz **Kopiowanie certyfikatu**, aby wyświetlić stronę, na której znajduje się specjalnie zakodowana kopia certyfikatu lokalnego ośrodka certyfikacji (CA). Skopiuj do schowka obiekt tekstowy widoczny na stronie. Informacje te trzeba będzie później wkleić do pliku. Plik ten jest wykorzystywany przez programy narzędziowe komputerów osobistych (takie jak MKKF lub KEYMAN) do przechowywania certyfikatów dla programów klienckich w komputerze osobistym. Aplikacje klienta będą mogły rozpoznać i użyć certyfikatu lokalnego ośrodka do uwierzytelniania dopiero wtedy, gdy skonfiguruje się je tak, aby rozpoznawały certyfikat jako użytkownika zaufanego. W tym celu należy skorzystać z instrukcji dostępnych w tych aplikacjach.
4. Kliknij **OK**, aby powrócić do strony głównej programu Menedżer certyfikatów cyfrowych.

Zarządzanie certyfikatami z publicznego internetowego ośrodka certyfikacji

Po dokładnym przeanalizowaniu wymagań i strategii ochrony zdecydowano się używać certyfikatów z publicznego internetowego ośrodka certyfikacji (CA), takiego jak VeriSign. Podejście takie jest wskazane na przykład przy obsłudze publicznego serwisu WWW, gdy chce się używać protokołu Secure Sockets Layer (SSL) do bezpiecznej komunikacji w celu zapewnienia prywatności informacji o transakcjach. Ponieważ serwis jest dostępny publicznie, najlepiej będzie używać certyfikatów, które zostaną rozpoznane przez większość przeglądarek WWW.

Także w przypadku opracowywania aplikacji dla zewnętrznych klientów wskazane jest korzystanie z publicznych certyfikatów do cyfrowego podpisywania pakietów aplikacji. Dzięki podpisaniu pakietów klienci mogą być pewni, że pochodzą one z danej firmy i nie zostały zmienione podczas przesyłania przez osoby nieupoważnione. Zastosowanie certyfikatów publicznych umożliwi klientom łatwe i tanie zweryfikowanie cyfrowego podpisu na pakiecie. Certyfikatu tego można również użyć do zweryfikowania podpisu przed wysłaniem pakietu do klientów.

Ścieżki zadań w programie Menedżer certyfikatów cyfrowych (DCM) pozwalają centralnie zarządzać certyfikatami publicznymi i aplikacjami używającymi ich do nawiązywania połączeń SSL, podpisywania obiektów lub weryfikowania podpisów na obiektach.

Zarządzanie certyfikatami publicznymi

Aby używać programu DCM do zarządzania certyfikatami z publicznego internetowego ośrodka certyfikacji (CA), należy najpierw utworzyć bazę certyfikatów. Baza certyfikatów to specjalny plik bazy danych kluczy używany przez Menedżera certyfikatów cyfrowych (DCM) do przechowywania certyfikatów cyfrowych i powiązanych z nimi kluczy prywatnych. Program DCM pozwala utworzyć i zarządzać kilkoma typami baz certyfikatów, zależnie od typów przechowywanych w nich certyfikatów.

Typ utworzonej bazy certyfikatów oraz kolejne zadania, które należy wykonać w celu zarządzania certyfikatami i używającymi ich aplikacjami, zależy od planu wykorzystania certyfikatów. Aby dowiedzieć się więcej o tym, jak korzystać z programu DCM, w celu utworzenia odpowiedniej bazy certyfikatów i zarządzania publicznymi certyfikatami internetowymi dla lokalnych aplikacji, należy zapoznać się z następującymi sekcjami:

- Zarządzanie certyfikatami publicznymi dla sesji komunikacyjnych SSL

- Zarządzanie certyfikatami publicznymi cyfrowego podpisywania obiektów
- Zarządzanie internetowymi certyfikatami publicznymi do weryfikowania podpisów obiektów

Program DCM umożliwia zarządzanie certyfikatami uzyskanymi z ośrodka certyfikacji (CA) zarządzającego infrastrukturą kluczy publicznych dla X.509 (PKIX).

Zarządzanie certyfikatami publicznymi dla sesji komunikacyjnych SSL

Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można zarządzać certyfikatami publicznymi dla aplikacji w celu nawiązywania bezpiecznych sesji komunikacyjnych z wykorzystaniem protokołu Secure Sockets Layer (SSL). Jeśli nie używa się programu DCM do prowadzenia własnego lokalnego ośrodka certyfikacji, należy najpierw utworzyć bazę certyfikatów publicznych używanych dla sesji SSL. Jest to baza certyfikatów *SYSTEM. Podczas tworzenia bazy certyfikatów program DCM prowadzi użytkownika poprzez proces tworzenia wniosku o certyfikat, który należy złożyć w publicznym ośrodku certyfikacji (CA) w celu uzyskania certyfikatu.

Aby za pomocą programu DCM korzystać z certyfikatów publicznych w celu umożliwienia aplikacjom nawiązywania sesji komunikacyjnych SSL, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie nowej bazy certyfikatów**, aby rozpocząć procedurę i wypełnić szereg formularzy. Formularze te prowadzą przez proces tworzenia bazy certyfikatów i certyfikatu, którego aplikacje będą mogły używać podczas sesji SSL.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

3. Zaznacz ***SYSTEM** jako bazę certyfikatów, która ma zostać utworzona, i kliknij **Kontynuuj**.
4. Wybierz **Tak**, aby utworzyć certyfikat jako część bazy certyfikatów, i kliknij **Kontynuuj**.
5. Jako ośrodek podpisujący nowy certyfikat wybierz **VeriSign lub inny internetowy ośrodek certyfikacji** i kliknij **Kontynuuj**, aby wyświetlić formularz pozwalający podać informacje identyfikujące dla nowego certyfikatu.

Uwaga: Jeśli w serwerze iSeries jest zainstalowany koprocesor szyfrujący IBM 4758–023 PCI, program DCM umożliwia określenie w następnym kroku sposobu przechowywania klucza prywatnego certyfikatu. Jeśli w systemie nie ma tego koprocesora, program DCM automatycznie umieszcza klucz prywatny w bazie certyfikatów *SYSTEM. W przypadku pojawienia się pytań dotyczących sposobu przechowywania klucza prywatnego należy skorzystać z systemu pomocy programu DCM.

6. Wypełnij formularz i kliknij **Kontynuuj**, aby wyświetlić stronę potwierdzenia. Na stronie tej wyświetlane są dane do wniosku, który należy dostarczyć do ośrodka certyfikacji (CA) wystawiającego certyfikat. Dane Certificate Signing Request (CSR) zawierają klucz publiczny i inne informacje podane w certyfikacie.
7. Uważnie skopiuj dane CSR i wklej je do formularza wniosku o certyfikat lub do osobnego pliku wymaganego przez ośrodek publiczny przy występowaniu o certyfikat. Należy użyć wszystkich danych CSR, w tym również wierszy Początek wniosku o nowy certyfikat i Koniec wniosku o nowy certyfikat. Po zamknięciu tej strony dane zostaną utracone i nie będzie można ich odtworzyć. Formularz wniosku lub plik należy wysłać do wybranego ośrodka certyfikacji (CA), który ma wystawić i podpisać certyfikat.

Uwaga: Procedurę można zakończyć dopiero po odesłaniu przez ośrodek podpisanego, wypełnionego certyfikatu.

Uwaga: Aby używać certyfikatów na serwerze HTTP Server for iSeries, należy przed uruchomieniem programu DCM utworzyć i skonfigurować serwer WWW. Podczas konfigurowania warstwy SSL w serwerze WWW, tworzony jest ID aplikacji dla tego serwera. Identyfikator ten należy zapisać, aby można było wskazać w programie DCM certyfikat, którego aplikacja ma używać dla tego ID.

Nie należy zatrzymywać ani restartować serwera, dopóki program DCM nie przypisze serwerowi podpisanego, wypełnionego certyfikatu. Jeśli instancja *ADMIN serwera WWW zostanie zatrzymana przed przypisaniem certyfikatu, serwer nie uruchomi się i nie będzie można użyć programu DCM do przypisania certyfikatu serwera.

- Po odesłaniu podpisanego certyfikatu przez ośrodek certyfikacji (CA) uruchom program DCM.
- W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
- Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
- Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
- Z listy zadań wybierz **Import certyfikatu**, aby rozpocząć proces importowania podpisanego certyfikatu do bazy certyfikatów *SYSTEM. Po zakończeniu importowania można określić aplikacje, które powinny korzystać z certyfikatu dla celów komunikacji SSL.
- W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
- Z listy zadań wybierz **Aktualizacja przypisania certyfikatu**, aby wyświetlić listę aplikacji obsługujących SSL, do których można przypisać certyfikat.
- Wybierz aplikację z listy i kliknij **Aktualizacja przypisania certyfikatu**.
- Wybierz zaimportowany certyfikat i kliknij **Przypisanie nowego certyfikatu**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru certyfikatu dla aplikacji.

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Aby mogły one uwierzytelniać certyfikaty, zanim udzielą dostępu do zasobów, należy dla nich zdefiniować listę zaufanych ośrodków certyfikacji (CA). Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Po zakończeniu całej procedury spełnione są wszelkie warunki konieczne do konfigurowania aplikacji do korzystania z protokołu SSL w celu bezpiecznej komunikacji. Zanim jednak użytkownicy będą mieli dostęp do tych aplikacji poprzez połączenia SSL, muszą otrzymać kopię certyfikatu ośrodka, który wystawił certyfikat serwera. Jeśli certyfikat ten pochodzi z powszechnie znanego ośrodka, użytkownicy oprogramowania klienta mogą już mieć kopię certyfikatu tego ośrodka. Jeśli jej nie mają, powinni połączyć się z serwisem WWW tego ośrodka i postąpić zgodnie ze wskazówkami w celu pobrania kopii certyfikatu ośrodka.

Zarządzanie certyfikatami publicznymi cyfrowego podpisywania obiektów

Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można zarządzać certyfikatami publicznymi do cyfrowego podpisywania obiektów. Jeśli do prowadzenia własnego lokalnego ośrodka certyfikacji nie wykorzystuje się programu DCM, należy najpierw utworzyć bazę certyfikatów publicznych używanych do podpisywania obiektów. Jest to baza certyfikatów *OBJECTSIGNING. Podczas tworzenia bazy certyfikatów, program DCM prowadzi użytkownika poprzez proces tworzenia wniosku o certyfikat, który należy złożyć w publicznym internetowym ośrodku certyfikacji (CA) w celu uzyskania certyfikatu.

Ponadto, aby używać certyfikatu do podpisywania obiektów, należy zdefiniować ID aplikacji. ID aplikacji kontroluje poziom uprawnień użytkownika wymagany do podpisywania obiektów za pomocą określonego certyfikatu i stanowi dodatkowy poziom kontroli dostępu, niezależny od kontroli dostępu realizowanej w programie DCM. Domyślna definicja aplikacji wymaga, aby w celu używania certyfikatu dla aplikacji do podpisywania obiektów użytkownik miał specjalne uprawnienia *ALLOBJ. (W programie iSeries Navigator można jednak zmienić poziom uprawnień wymagany przez ID aplikacji.)

Aby za pomocą programu DCM używać certyfikatów publicznych do podpisywania obiektów, wykonaj następujące czynności:

- Uruchom sesję DCM.

2. W ramce nawigacji programu DCM wybierz **Tworzenie nowej bazy certyfikatów**, aby rozpocząć procedurę i wypełnić szereg formularzy. Formularze te prowadzą przez proces tworzenia bazy certyfikatów i certyfikatu, którego można będzie używać do podpisywania obiektów.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

3. Zaznacz ***OBJECTSIGNING** jako bazę certyfikatów, która ma zostać utworzona, i kliknij **Kontynuuj**.
4. Wybierz **Tak**, aby utworzyć certyfikat jako część bazy certyfikatów, i kliknij **Kontynuuj**.
5. Jako ośrodek podpisujący nowy certyfikat wybierz **VeriSign lub inny internetowy ośrodek certyfikacji** i kliknij **Kontynuuj**. Zostanie wyświetlony formularz do podania informacji identyfikacyjnych dla nowego certyfikatu.
6. Wypełnij formularz i kliknij **Kontynuuj**, aby wyświetlić stronę potwierdzenia. Na stronie tej wyświetlane są dane do wniosku, który należy dostarczyć do ośrodka certyfikacji (CA) wystawiającego certyfikat. Dane Certificate Signing Request (CSR) zawierają klucz publiczny i inne informacje podane w certyfikacie.
7. Uważnie skopiuj dane CSR i wklej je do formularza wniosku o certyfikat lub do osobnego pliku wymaganego przez ośrodek publiczny przy występowaniu o certyfikat. Należy użyć wszystkich danych CSR, w tym również wierszy Początek wniosku o nowy certyfikat i Koniec wniosku o nowy certyfikat. Po zamknięciu tej strony dane zostaną utracone i nie będzie można ich odtworzyć. Formularz wniosku lub plik należy wysłać do wybranego ośrodka certyfikacji (CA), który ma wystawić i podpisać certyfikat.

Uwaga: Procedurę można zakończyć dopiero po odesłaniu przez ośrodek podpisanego, wypełnionego certyfikatu.

8. Po odesłaniu podpisanego certyfikatu przez ośrodek certyfikacji (CA) uruchom program DCM.
9. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
10. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
11. W ramce nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
12. Z listy zadań wybierz **Import certyfikatu**, aby rozpocząć proces importowania podpisanego certyfikatu do bazy certyfikatów *OBJECTSIGNING. Po zakończeniu importowania można zdefiniować aplikacje, które mogą korzystać z certyfikatu do podpisywania obiektów.
13. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
14. Z listy zadań wybierz **Dodaj aplikację**, aby rozpocząć proces tworzenia definicji aplikacji podpisujących obiekty za pomocą danego certyfikatu.
15. Wypełnij formularz, aby zdefiniować aplikację podpisującą obiekty, i kliknij **Dodaj**. Ta definicja aplikacji nie opisuje rzeczywistej aplikacji, tylko typy obiektów, które mają być podpisywane za pomocą konkretnego certyfikatu. W przypadku niejasności przy wypełnianiu formularza należy skorzystać z systemu pomocy.
16. Kliknij **OK**, aby zaakceptować komunikat potwierdzenia definicji aplikacji i wyświetlić listę zadań Zarządzanie aplikacjami.
17. Z listy zadań wybierz **Aktualizacja przypisania certyfikatu**, a następnie kliknij **Kontynuuj**, aby wyświetlić listę ID aplikacji podpisujących obiekty, do których można przypisać certyfikat.
18. Wybierz ID aplikacji z listy i kliknij **Aktualizacja przypisania certyfikatu**.
19. Wybierz zaimportowany certyfikat i kliknij **Przypisanie nowego certyfikatu**.

Po zakończeniu tych czynności spełnione są wszelkie warunki, aby rozpocząć podpisywanie obiektów w celu zapewnienia ich integralności.

Aby odbiorcy dystrybuowanych podpisanych obiektów mogli sprawdzić poprawność podpisu na obiekcie i upewnić się, że nie został on zmieniony i pochodzi od znanego nadawcy, muszą dysponować programem

DCM w wersji V5R1 lub nowszej. W celu sprawdzenia podpisu odbiorca musi mieć kopię certyfikatu do weryfikacji podpisów. Kopię tego certyfikatu należy dołączyć do pakietu z podpisanymi obiektami.

Ponadto odbiorca musi mieć kopię certyfikatu ośrodka certyfikacji (CA), który wystawił certyfikat użyty do podpisania obiektu. Jeśli do podpisania obiektów został użyty certyfikat z powszechnie znanego ośrodka certyfikacji (CA), w programie DCM odbiorcy powinna znajdować się kopia certyfikatu tego ośrodka. Jednak na wypadek gdyby odbiorca nie miał kopii certyfikatu ośrodka, powinno się ją dołączyć do przesyłanych podpisanymi obiektów. Kopię certyfikatu lokalnego ośrodka należy na przykład przesłać do odbiorcy, jeśli obiekty zostały podpisane certyfikatem wystawionym przez prywatny lokalny ośrodek. Ze względów bezpieczeństwa certyfikat ośrodka należy dostarczyć w odrębnym pakiecie lub udostępnić go publicznie wszystkim, którzy go potrzebują.

Zarządzanie certyfikatami publicznymi do weryfikowania podpisów obiektów

Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można zarządzać certyfikatami używanymi do sprawdzania podpisów cyfrowych na obiektach. Aby podpisać obiekt, używa się prywatnego klucza certyfikatu do utworzenia podpisu. Wysyłając podpisany obiekt do innych osób, należy dołączyć do niego kopię certyfikatu, którym podpisano ten obiekt. W tym celu używa się programu DCM do wyeksportowania certyfikatu podpisującego obiekt (bez klucza prywatnego certyfikatu) jako certyfikatu do weryfikacji podpisu. Certyfikat taki można wyeksportować do pliku, który następnie można przesłać innym. Jeśli natomiast zamierza się samodzielnie zweryfikować utworzone podpisy, można wyeksportować certyfikat do weryfikacji podpisu do bazy certyfikatów *SIGNATUREVERIFICATION.

Aby sprawdzić podpis obiektu, potrzebna jest kopia certyfikatu, którym podpisano obiekt. Do weryfikacji podpisu utworzonego za pomocą klucza prywatnego używa się odpowiadającego mu klucza publicznego certyfikatu podpisującego. Dlatego, aby zweryfikować podpis na obiekcie, należy uzyskać kopię certyfikatu podpisującego od nadawcy podpisanymi obiektów.

Potrzebna jest również kopia certyfikatu ośrodka certyfikacji, który wystawił certyfikat użyty do podpisania obiektów. Certyfikat ten służy do zweryfikowania autentyczności certyfikatu, którym podpisano obiekt. W programie DCM dostępne są kopie certyfikatów wielu powszechnie znanych ośrodków certyfikacji (CA). Jeśli jednak obiekt został podpisany certyfikatem z innego ośrodka publicznego lub prywatnego ośrodka lokalnego, przed zweryfikowaniem podpisu trzeba uzyskać kopię certyfikatu tego ośrodka.

Aby używać programu DCM do weryfikowania podpisów obiektów, należy najpierw utworzyć bazę certyfikatów używanych do tego celu, to jest bazę *SIGNATUREVERIFICATION. Po utworzeniu tej bazy program DCM automatycznie uzupełnia ją kopiami certyfikatów większości popularnych, publicznych ośrodków certyfikacji (CA).

Uwaga: Aby móc weryfikować własne podpisy, należy utworzyć bazę *SIGNATUREVERIFICATION i skopiować do niej certyfikaty z bazy *OBJECTSIGNING. Jest to konieczne nawet wtedy, gdy planuje się weryfikowanie podpisów za pomocą certyfikatów z bazy *OBJECTSIGNING.

Aby za pomocą programu DCM zarządzać certyfikatami do weryfikacji podpisów, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie nowej bazy certyfikatów**, aby rozpocząć procedurę i wypełnić szereg formularzy.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

3. Zaznacz ***SIGNATUREVERIFICATION** jako bazę certyfikatów, która ma zostać utworzona, i kliknij **Kontynuuj**.

Uwaga: Jeśli baza certyfikatów *OBJECTSIGNING już istnieje, program DCM zapyta o skopiowanie z niej certyfikatów podpisujących obiekty do nowej bazy jako certyfikatów weryfikujących podpisy.

Aby używać istniejących certyfikatów podpisujących obiekty do weryfikowania podpisów, wybierz **Tak** i kliknij **Kontynuuj**. Aby skopiować certyfikaty z bazy *OBJECTSIGNING, musisz znać jej hasło.

4. Podaj hasło nowej bazy certyfikatów i kliknij **Kontynuuj**, aby ją utworzyć. Wyświetli się informacja z potwierdzeniem pomyślnego utworzenia bazy certyfikatów. Po wykonaniu tych czynności można już używać bazy do zarządzania certyfikatami weryfikującymi podpisy.

Uwaga: Jeśli baza została utworzona w celu weryfikacji własnych podpisów, można zakończyć tę procedurę. Należy jednak pamiętać, aby po utworzeniu nowych certyfikatów podpisujących obiekty wyeksportować je z bazy *OBJECTSIGNING do tej bazy certyfikatów. W przeciwnym razie nie będzie można weryfikować podpisów utworzonych za pomocą tych certyfikatów.

Uwaga: Jeśli baza została utworzona w celu weryfikacji podpisów na obiektach otrzymanych z innych źródeł, należy kontynuować procedurę i zaimportować niezbędne certyfikaty do bazy certyfikatów.

5. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SIGNATUREVERIFICATION**, aby utworzyć tę bazę certyfikatów.
6. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
7. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
8. Z listy zadań wybierz **Import certyfikatu**. Zadanie to prowadzi przez proces importowania do bazy certyfikatów koniecznych do weryfikowania podpisów na obiektach otrzymanych z innych źródeł.
9. Wybierz typ certyfikatu, który chcesz zaimportować. Wybierz **Sprawdzania podpisu**, aby zaimportować certyfikat otrzymany wraz z podpisanymi obiektami i zakończyć zadanie importu.

Uwaga: Jeśli w bazie certyfikatów nie ma kopii certyfikatu ośrodka, który wystawił certyfikat weryfikujący podpis, należy *najpierw* zaimportować certyfikat ośrodka. W przeciwnym razie, podczas importowania certyfikatu weryfikującego podpisy wystąpi błąd.

Po wykonaniu powyższych czynności można używać tych certyfikatów do weryfikowania podpisów obiektów.

Rozdział 8. Zarządzanie programem DCM

Po zakończeniu konfigurowania Menedżera certyfikatów cyfrowych (DCM), należy wykonać zadania związane z zarządzaniem certyfikatami. Aby dowiedzieć się w jaki sposób wykorzystać program DCM do zarządzania certyfikatami cyfrowymi, należy zapoznać się z następującymi sekcjami:

Wykorzystanie lokalnego ośrodka certyfikacji do wystawiania certyfikatów innym systemom iSeries

W sekcji opisano, jak używać prywatnego lokalnego ośrodka certyfikacji (CA) do wystawiania certyfikatów używanych w innych systemach iSeries.

Zarządzanie aplikacjami w programie DCM

W sekcji opisano wykorzystanie programu DCM do pracy z definicjami aplikacji obsługujących SSL lub aplikacji podpisujących obiekty. Sekcja zawiera informacje o tworzeniu definicji aplikacji i o przypisywaniu aplikacjom certyfikatów. Można dzięki niej również uzyskać informacje o listach zaufanych ośrodków, na podstawie których aplikacje akceptują certyfikaty w procesie uwierzytelniania klienta.

Sprawdzanie poprawności certyfikatów i aplikacji

W sekcji opisano, w jaki sposób zweryfikować autentyczność konkretnego certyfikatu, zanim aplikacja go użyje lub zaakceptuje.

Przypisanie certyfikatu

W sekcji opisano, w jaki sposób szybko przypisać certyfikat do jednej lub kilku aplikacji, aby aplikacje te używały funkcji ochrony.

Zarządzanie informacjami o położeniu listy CRL W sekcji opisano, jak definiować i wykorzystywać informacje o położeniu listy odwołań certyfikatów (CRL), której to listy aplikacje używają do sprawdzenia, czy akceptowane przez nie certyfikaty są ważne.

Przechowywanie kluczy certyfikatów za pomocą koprocesora szyfrującego IBM 4758

W sekcji opisano, w jaki sposób wykorzystać zainstalowany w systemie koprocesor do bezpieczniejszego przechowywania kluczy prywatnych certyfikatu.

Zarządzanie miejscem położenia ośrodków certyfikacji PKIX

W sekcji opisano, jak za pomocą programu DCM zarządzać certyfikatami uzyskanymi z publicznego internetowego ośrodka certyfikacji (CA), który wystawia certyfikaty zgodnie ze standardami Public Key Infrastructure for X.509 (PKIX).

Podpisywanie obiektów

W sekcji opisano, jak w programie DCM zarządzać certyfikatami, używanymi do podpisywania obiektów, w celu zapewnienia ich integralności.

Weryfikowanie podpisów obiektów

W sekcji opisano, jak używać programu DCM do sprawdzenia autentyczności cyfrowych podpisów obiektów.

Wykorzystanie lokalnego ośrodka certyfikacji do wystawiania certyfikatów innym systemom iSeries

Załóżmy, że w systemie iSeries w danej sieci działa już prywatny, lokalny ośrodek certyfikacji (CA). Istnieje okazja, by zasięgiem objąć także inne systemy iSeries w tej sieci. Można będzie wówczas użyć bieżącego ośrodka lokalnego na przykład do wystawienia certyfikatu serwera lub klienta aplikacji na innym systemie iSeries aby umożliwić jej nawiązywanie sesji komunikacyjnych SSL. Można również użyć do podpisywania obiektów przechowywanych w innym serwerze iSeries certyfikatów z tego lokalnego ośrodka.

Aby zrealizować to zadanie, należy użyć programu Menedżer certyfikatów cyfrowych (DCM). Część niezbędnych zadań wykonuje się w systemie iSeries, w którym działa lokalny ośrodek certyfikacji (CA), a pozostałe w dodatkowym systemie iSeries będącym hostem aplikacji, którym mają być wystawiane certyfikaty. Ten dodatkowy system nazywa się systemem docelowym. Zadania, przeznaczone do wykonania w systemie docelowym, zależą od wersji tego systemu.

Uwaga: Jeśli w systemie iSeries, w którym działa lokalny ośrodek certyfikacji (CA), są zainstalowane produkty szyfrujące, które oferują skuteczniejsze szyfrowanie niż system docelowy, mogą pojawić

się problemy. (Dla wersji V5R2 tylko produkt 5722–AC3 udostępnia możliwość szyfrowania; jest to najskuteczniejszy z dostępnych produktów. Jednak w wersjach wcześniejszych można zainstalować inny, mniej zaawansowany produkt (5722–AC1, lub 5722–AC2) o mniejszych możliwościach szyfrujących. Podczas eksportu certyfikatu (zawierającego klucz prywatny) system szyfruje go w celu zabezpieczenia jego zawartości. Jeśli użyje się do tej czynności bardziej zaawansowanego produktu szyfrującego niż zainstalowany w systemie docelowym, system docelowy nie będzie mógł odszyfrować pliku podczas procesu importowania. W rezultacie import może się nie powieść lub certyfikat nie będzie nadawał się do nawiązania sesji SSL. Dotyczy to także sytuacji, w której wielkość klucza nowego certyfikatu jest zgodna z produktem szyfrującym w systemie docelowym.

Lokalny ośrodek certyfikacji (CA) można wykorzystać do wystawiania certyfikatów innym systemom, a następnie używać tych certyfikatów do podpisywania obiektów lub do nawiązywania połączeń SSL. Wówczas pliki utworzone przez program DCM będą zawierały kopię certyfikatu ośrodka lokalnego, a także kopie certyfikatów wielu ośrodków publicznych.

Zadania, które należy wykonać w programie DCM, różnią się nieznacznie w zależności od typu certyfikatów wystawianych przez lokalny ośrodek certyfikacji (CA) oraz od numeru wersji i warunków w systemie docelowym.

Wystawianie certyfikatów prywatnych innemu systemowi iSeries V5R1 lub V5R2

Aby użyć lokalnego ośrodka certyfikacji (CA) do wystawiania certyfikatów innemu systemowi iSeries V5R2 lub V5R1, w systemie, w którym działa lokalny ośrodek, wykonaj następujące czynności:

1. Uruchom sesję DCM.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

2. W ramce nawigacji zaznacz **Tworzenie certyfikatu**, aby wyświetlić listę typów certyfikatów, jakie można utworzyć w lokalnym ośrodku certyfikacji (CA).

Do wykonania tego zadania nie trzeba otwierać bazy certyfikatów. W tej procedurze przyjmuje się, że żadna baza certyfikatów nie jest otwarta lub że otwarto bazę certyfikatów lokalnego ośrodka certyfikacji (CA). Aby można było wykonać opisane czynności, w systemie musi istnieć lokalny ośrodek certyfikacji (CA).

3. Zaznacz typ certyfikatu, jaki ma wystawić lokalny ośrodek certyfikacji (CA), i kliknij **Kontynuuj**, aby rozpocząć procedurę i wypełnić szereg formularzy. Zaznacz tworzenie **certyfikatu serwera lub klienta dla innego systemu iSeries** (dla sesji SSL) lub **certyfikatu podpisywania obiektów dla innego systemu iSeries** (do użycia w innym systemie).

Uwaga: Aby inny system, któremu wystawia się certyfikat podpisujący obiekty, mógł używać tego certyfikatu, musi na nim działać system OS/400 w wersji V5R1 lub nowszej. Dlatego w tym przypadku program DCM nie proponuje wyboru numeru wersji systemu docelowego.

4. W przypadku certyfikatu serwera lub klienta wybierz numer wersji systemu iSeries, dla którego wystawiasz ten certyfikat. Kliknij **Kontynuuj**, aby wyświetlić formularz do wprowadzenia informacji identyfikacyjnych dla nowego certyfikatu.

Uwaga: Podany numer wersji systemu docelowego określa format, w jakim program DCM wystawia nowy certyfikat. Także ilość i typ informacji identyfikacyjnych zależy od podanego numeru wersji. Dzięki temu pliki certyfikatów są zgodne z wersją systemu iSeries, który będzie używał tego certyfikatu.

5. Wypełnij formularz i kliknij **Kontynuuj**, aby wyświetlić stronę potwierdzenia.

Uwaga: Jeśli w systemie docelowym istnieją już bazy certyfikatów *OBJECTSIGNING lub *SYSTEM, należy podać unikalną etykietę i unikalną nazwę pliku certyfikatu. Pozwoli to bez problemów zaimportować certyfikat do bazy certyfikatów w systemie docelowym.

Na stronie potwierdzenia zostają wyświetlone nazwy plików utworzonych przez program DCM w celu przesłania do systemu docelowego. Program DCM tworzy te pliki na podstawie podanego numeru wersji systemu docelowego. Do plików tych automatycznie dołączana jest kopia certyfikatu lokalnego ośrodka certyfikacji (CA).

Uwaga: Program DCM tworzy nowy certyfikat we własnej bazie certyfikatów i generuje dwa pliki do przesłania: plik z bazy certyfikatów (rozszerzenie .KDB) i plik żądania (rozszerzenie .RDB).

6. W celu przesłania plików do systemu docelowego użyj klienta protokołu File Transfer Protocol (FTP) w trybie binarnym lub innej metody.

Wystawianie certyfikatów prywatnych systemowi iSeries V4R4 lub V4R5

Aby użyć lokalnego ośrodka certyfikacji (CA) do wystawienia certyfikatów systemowi iSeries V4R4 lub V4R5, w systemie, w którym działa lokalny ośrodek certyfikacji V5R2, wykonaj następujące czynności:

1. Uruchom sesję DCM.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

2. W ramce nawigacji zaznacz **Tworzenie certyfikatu**, aby wyświetlić listę typów certyfikatów, jakie można utworzyć w lokalnym ośrodku certyfikacji (CA).

Do wykonania tego zadania nie trzeba otwierać bazy certyfikatów. W tej procedurze przyjmuje się, że żadna baza certyfikatów nie jest otwarta lub że otwarto bazę certyfikatów lokalnego ośrodka certyfikacji (CA). Aby można było wykonać opisane czynności, w systemie musi istnieć lokalny ośrodek certyfikacji (CA).

3. Zaznacz typ certyfikatu, jaki ma wystawić lokalny ośrodek certyfikacji (CA), i kliknij **Kontynuuj**, aby rozpocząć procedurę i wypełnić szereg formularzy.

Uwaga: Ponieważ certyfikat jest wystawiany systemowi iSeries V4R4 lub V4R5, musisz wybrać **certyfikat serwera lub klienta dla innego systemu iSeries**. W systemach docelowych, w wersji wcześniejszej niż V5R1 nie można używać certyfikatów podpisujących obiekty.

4. Zaznacz numer wersji systemu iSeries, dla którego wystawiasz ten certyfikat. Kliknij **Kontynuuj**, aby wyświetlić formularz do wprowadzenia informacji identyfikacyjnych dla nowego certyfikatu.

Uwaga: Podany numer wersji systemu docelowego określa format, w jakim program DCM wystawia nowy certyfikat. Także ilość i typ informacji identyfikacyjnych zależy od podanego numeru wersji. Dzięki temu pliki certyfikatów są zgodne z wersją systemu iSeries, który będzie używał tego certyfikatu.

5. Wypełnij formularz i kliknij **Kontynuuj**, aby wyświetlić stronę potwierdzenia.

Uwaga: Jeśli w systemie docelowym istnieje już baza certyfikatów *SYSTEM, należy podać unikalną etykietę i unikalną nazwę pliku certyfikatu. Pozwoli to bez problemów zaimportować certyfikat do bazy certyfikatów w systemie docelowym.

Na stronie potwierdzenia zostają wyświetlone nazwy plików utworzonych przez program DCM w celu przesłania do systemu docelowego. Program DCM tworzy te pliki na podstawie podanego numeru wersji systemu docelowego. Do plików tych automatycznie dołączana jest kopia certyfikatu lokalnego ośrodka certyfikacji (CA).

Uwaga: Program DCM tworzy nowy certyfikat we własnej bazie certyfikatów i generuje dwa pliki do przesłania: plik bazy certyfikatów (rozszerzenie .KDB) i plik żądania (rozszerzenie .RDB).

Uwaga: Jeśli planuje się używanie certyfikatów z tych plików w istniejącej bazie certyfikatów *SYSTEM w systemie docelowym V4R4 lub V4R5, nie można zaimportować certyfikatu lokalnego ośrodka bezpośrednio z plików .KDB i .RDB. Jest to spowodowane tym, że certyfikat ośrodka nie jest zapisany w formacie rozpoznawanym przez funkcję importu programu DCM. W takiej sytuacji

należy na hoście wyeksportować kopię certyfikatu lokalnego ośrodka do osobnego pliku, zyskując gwarancję, że będzie ona w formacie czytelnym dla funkcji importu z wcześniejszych wersji.

6. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
7. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów na hoście i kliknij **Kontynuuj**.
8. W ramce nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
9. Z listy zadań wybierz **Eksport certyfikatu**.
10. Wybierz **Ośrodek certyfikacji** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodków certyfikacji (CA).
11. Z listy certyfikatów wybierz certyfikat lokalnego ośrodka certyfikacji (na przykład LOCAL_CERTIFICATE_AUTHORITY). Kliknij **Eksport**, aby wyświetlić formularz umożliwiający wybór miejsca docelowego dla certyfikatu ośrodka.
12. Wybierz **Plik** i kliknij **Kontynuuj**.
13. Podaj pełną ścieżkę i nazwę dla pliku eksportu i kliknij **Kontynuuj**. Wyświetli się strona potwierdzenia z informacją, że program DCM pomyślnie wyeksportował plik.

Uwaga: Należy sprawdzić, czy plikowi nadano unikalną nazwę i rozszerzenie. Plik można na przykład nazwać mycafile.exp. Nadając plikowi nazwę, nie należy korzystać z następujących rozszerzeń: .TXT, .KDB, .RDB lub .KYR. Używanie wymienionych typów rozszerzeń może spowodować problemy podczas importu plików w systemie docelowym.

14. Do przesłania plików utworzonej bazy certyfikatów (pliki o rozszerzeniach .KDB i .RDB) do systemu docelowego V4R4 lub V4R5 użyj klienta protokołu File Transfer Protocol (FTP) w trybie binarnym lub zastosuj inną metodę. Do przesyłania plików zawierających wyeksportowane certyfikaty lokalnego ośrodka certyfikacji (CA) należy użyć protokołu FTP w trybie ASCII.

Korzystanie z przesłanych plików w systemie docelowym

Do pracy z przesłanymi plikami certyfikatów należy użyć programu DCM w systemie docelowym. Zadania, które należy wykonać w programie DCM, zależą od numeru wersji systemu docelowego i od tego, jakie bazy certyfikatów istnieją w tym systemie. Także typ certyfikatów wystawionych na hoście ma wpływ na wybór zadania do wykonania w systemie docelowym. Aby dowiedzieć się, jak korzystać z programu DCM w systemie docelowym do pracy z przesłanymi plikami certyfikatów, należy zapoznać się z następującymi sekcjami:

- Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V5R2
- Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V5R1
- Wykorzystanie prywatnych certyfikatów do podpisywania obiektów w systemie docelowym V5R2 lub V5R1
- Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V4R5 lub V4R4

Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V5R2

Certyfikatami używanymi przez aplikacje podczas sesji SSL zarządza się z bazy certyfikatów *SYSTEM w programie Menedżer certyfikatów cyfrowych (DCM). Jeśli program DCM nie był nigdy używany w systemie docelowym V5R2 do zarządzania certyfikatami podczas sesji SSL, bazy tej nie powinno być w tym systemie. Zadania związane z korzystaniem z przesłanych plików certyfikatów utworzonych na hoście lokalnego ośrodka certyfikacji (CA) zależą od tego, czy baza certyfikatów *SYSTEM istnieje w systemie docelowym. Jeśli nie ma bazy certyfikatów *SYSTEM, jej rolę mogą pełnić przesłane pliki certyfikatów. Jeśli w systemie docelowym V5R2 istnieje baza certyfikatów *SYSTEM, przesłane pliki certyfikatów mogą być wykorzystane na dwa sposoby:

- Przesłane pliki można traktować jak Inną bazę certyfikatów systemu.
- Można wykonać import przesyłanych plików do istniejącej bazy certyfikatów *SYSTEM.

Baza certyfikatów *SYSTEM nie istnieje

Jeśli w systemie docelowym V5R2 nie ma bazy certyfikatów *SYSTEM, jej rolę mogą pełnić przesłane pliki certyfikatów. Aby w docelowym systemie V5R2 utworzyć bazę certyfikatów *SYSTEM oraz używać plików certyfikatów, wykonaj następujące czynności:

1. Sprawdź, czy pliki bazy certyfikatów (dwa pliki: jeden z rozszerzeniem .KDB i jeden z rozszerzeniem .RDB) utworzone na hoście lokalnego ośrodka certyfikacji (CA) znajdują się w katalogu /QIBM/USERDATA/ICSS/CERT/SERVER.
 2. W katalogu /QIBM/USERDATA/ICSS/CERT/SERVER, zmień nazwy przesłanych plików certyfikatów na DEFAULT.KDB oraz DEFAULT.RDB. Zmieniając nazwy tych plików w odpowiednim katalogu, tworzy się komponenty, które zawierają bazę certyfikatów *SYSTEM dla systemu docelowego. Pliki bazy certyfikatów zawierają już certyfikaty wielu publicznych ośrodków certyfikacji (CA). Podczas tworzenia plików bazy certyfikatów program DCM dodał do nich te certyfikaty, a także kopię certyfikatu ośrodka lokalnego.
- Uwaga:** Jeśli w systemie docelowym w katalogu /QIBM/USERDATA/ICSS/CERT/SERVER znajdują się już pliki DEFAULT.KDB i DEFAULT.RDB, oznacza to, że baza certyfikatów *SYSTEM już istnieje w tym systemie. W takim przypadku nie należy zmieniać nazw przesłanych plików. Nadpisanie plików domyślnych spowoduje problemy podczas korzystania z programu DCM, przesłanej bazy certyfikatów i jej zawartości. Należy wówczas sprawdzić, czy przesłane pliki bazy certyfikatów mają unikalne nazwy i użyć ich jako **Innej bazy certyfikatów systemu**. Jeśli jednak użyje się tych plików jako Innej bazy certyfikatów systemu, nie będzie można użyć programu DCM do określenia, które aplikacje powinny używać tych certyfikatów.
3. Uruchom sesję DCM. Należy teraz zmienić hasło do bazy certyfikatów *SYSTEM, którą utworzono przez zmianę nazwy przesłanych plików. Zmiana hasła umożliwi programowi DCM zapisanie nowego hasła, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej bazy certyfikatów.
 4. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
 5. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia w systemie *hosta* bazy certyfikatów dla docelowego systemu V5R2, i kliknij **Kontynuuj**.
 6. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów. Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć. Następnie należy określić aplikacje, które powinny używać certyfikatów w komunikacji SSL.
 7. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
 8. Na wyświetlonej stronie bazy certyfikatów wpisz nowe hasło i kliknij **Kontynuuj**.
 9. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
 10. Z listy zadań wybierz **Przypisanie certyfikatu**, aby wyświetlić listę certyfikatów w bieżącej bazie certyfikatów.
 11. Zaznacz certyfikat, który został utworzony w systemie *hosta*, i kliknij **Przypisanie do aplikacji**, aby wyświetlić listę aplikacji obsługujących protokół SSL, którym można przypisać certyfikat.
 12. Zaznacz aplikacje, które powinny używać certyfikatów w komunikacji SSL, i kliknij **Kontynuuj**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru certyfikatu dla aplikacji.

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Aplikacje te przed udostępnieniem zasobów muszą być w stanie uwierzytelniać certyfikaty. W tym celu należy dla nich zdefiniować listę zaufanych ośrodków certyfikacji (CA). Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Gdy zadania te zostaną wykonane, aplikacje mogą używać certyfikatów wydanych przez lokalny ośrodek CA w innym systemie iSeries. Zanim jednak można będzie rozpocząć używanie tych aplikacji, należy skonfigurować je do korzystania z protokołu SSL.

Aby uzyskać dostęp do wybranych aplikacji poprzez połączenie SSL, użytkownik musi użyć programu DCM do pobrania kopii certyfikatu lokalnego ośrodka certyfikacji działającego na hoście. Certyfikat ten musi być skopiowany do pliku w komputerze osobistym użytkownika lub pobrany do przeglądarki użytkownika, w zależności od wymagań aplikacji używającej SSL.

Baza certyfikatów *SYSTEM istnieje — korzystanie z Innej bazy certyfikatów systemu

Jeśli w systemie docelowym V5R2 baza certyfikatów *SYSTEM już istnieje, należy zdecydować, jak pracować z plikami certyfikatów. Z przesłanych plików można utworzyć **Inną bazę certyfikatów systemu**. Można też zaimportować certyfikat prywatny i odpowiadający mu certyfikat lokalnego ośrodka certyfikacji do istniejącej bazy certyfikatów *SYSTEM.

Inne bazy certyfikatów systemu są definiowanymi przez użytkowników zapasowymi bazami certyfikatów SSL. Mogą one służyć do udostępniania certyfikatów na potrzeby napisanych przez użytkowników aplikacji z obsługą SSL, które nie korzystają z funkcji API programu DCM w celu zarejestrowania ID aplikacji w tym programie. Opcja Inna baza certyfikatów systemu pozwala zarządzać certyfikatami dla aplikacji używających funkcji API SSL_Init w celu programowego dostępu do certyfikatów i wykorzystania ich do nawiązania sesji SSL. Funkcja ta umożliwia aplikacji użycie domyślnego certyfikatu z bazy certyfikatów zamiast certyfikatu specjalnego.

Aplikacje IBM iSeries (i aplikacje wielu dostawców oprogramowania) są napisane w taki sposób, aby korzystały wyłącznie z certyfikatów przechowywanych w bazie *SYSTEM. Jeśli użyje się przesłanych plików jako Innej bazy certyfikatów systemu, nie będzie można użyć programu DCM do określenia, które aplikacje powinny używać certyfikatów na potrzeby sesji SSL. W rezultacie nie będzie można skonfigurować standardowych aplikacji systemu iSeries z obsługą SSL, tak aby używały tego certyfikatu. Aby aplikacje systemu iSeries mogły używać tego certyfikatu, należy zaimportować go z przesłanej bazy certyfikatów do bazy certyfikatów *SYSTEM.

Aby użyć przesłanych plików certyfikatu jako Innej bazy certyfikatów systemu, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby utworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów (tego z rozszerzeniem .KDB) przesłanego z hosta ośrodka certyfikacji (CA). Podaj również hasło określone podczas tworzenia w systemie *hosta* bazy certyfikatów dla docelowego systemu V5R2, i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie utworzyć. Następnie można zaznaczyć, że certyfikaty z tej bazy mają być używane jako certyfikaty domyślne.

5. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby utworzyć tę bazę certyfikatów.
6. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów, nowe hasło i kliknij **Kontynuuj**.
7. Po odświeżeniu widoku ramki nawigacji zaznacz **Zarządzanie bazą certyfikatów** i z listy zadań wybierz **Ustawienie domyślnego certyfikatu**.

Po utworzeniu i skonfigurowaniu Innej bazy certyfikatów systemu dowolna aplikacja korzystająca z funkcji API SSL_Init będzie mogła używać certyfikatu z tej bazy do nawiązywania połączeń SSL.

Certyfikatów z przesłanych plików bazy certyfikatów można używać również w bazie certyfikatów *SYSTEM istniejącej w systemie docelowym V5R2. W tym celu należy zaimportować certyfikaty z plików bazy certyfikatów do istniejącej bazy *SYSTEM. Nie można jednak zaimportować certyfikatów bezpośrednio z plików .KDB i .RDB, ponieważ funkcja importu programu DCM nie obsługuje formatu tych plików. Aby wykorzystać przesłane certyfikaty w istniejącej bazie certyfikatów *SYSTEM, należy otworzyć pliki jako Inną bazę certyfikatów systemu, a następnie wyeksportować je do bazy certyfikatów *SYSTEM.

Aby wyeksportować certyfikaty z plików bazy certyfikatów do bazy certyfikatów *SYSTEM w systemie docelowym V5R2, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i zaznacz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów (tego z rozszerzeniem .KDB) przesłanego z hosta ośrodka certyfikacji (CA). Podaj również hasło określone podczas tworzenia w systemie *hosta* bazy certyfikatów dla docelowego systemu V5R2, i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy. Jeśli przed zaznaczeniem opcji Automatyczne logowanie nie zostanie zmienione hasło, mogą pojawić się błędy podczas eksportowania certyfikatów z tej bazy do bazy certyfikatów *SYSTEM.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć.

5. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
6. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów, nowe hasło i kliknij **Kontynuuj**.
7. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań, a następnie wybierz z tej listy **Eksport certyfikatu**.
8. Zaznacz **Ośrodek certyfikacji** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**.

Uwaga: Certyfikat lokalnego ośrodka certyfikacji (CA) należy wyeksportować do bazy certyfikatów przed wyeksportowaniem certyfikatu serwera lub klienta. W przeciwnym razie może wystąpić błąd, ponieważ w bazie nie będzie certyfikatu lokalnego ośrodka.

9. Wybierz certyfikat lokalnego ośrodka certyfikacji (CA) i kliknij **Eksportuj**.
10. Jako miejsce docelowe eksportowanego certyfikatu wybierz **Baza certyfikatów** i kliknij **Kontynuuj**.
11. Wpisz *SYSTEM jako docelową bazę certyfikatów, podaj hasło do bazy certyfikatów *SYSTEM i kliknij **Kontynuuj**. Wyświetli się komunikat informujący o pomyślnie zakończonym eksporcie certyfikatu lub komunikat o błędzie, jeśli proces eksportowania nie powiódł się.
12. Teraz można wyeksportować certyfikat klienta lub serwera do bazy certyfikatów *SYSTEM. Zaznacz ponownie zadanie **Eksport certyfikatu**.
13. Zaznacz **Serwer lub klient** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**.
14. Zaznacz certyfikat serwera lub klienta i kliknij **Eksport**.
15. Jako miejsce docelowe eksportowanego certyfikatu wybierz **Baza certyfikatów** i kliknij **Kontynuuj**.
16. Wpisz *SYSTEM jako docelową bazę certyfikatów, podaj hasło do bazy certyfikatów *SYSTEM i kliknij **Kontynuuj**. Wyświetli się komunikat informujący o pomyślnie zakończonym eksporcie certyfikatu lub komunikat o błędzie, jeśli proces eksportowania nie powiódł się.
17. Teraz można przypisać certyfikat do aplikacji, aby mogły korzystać z protokołu SSL. Kliknij **Wybór ośrodka certyfikacji** i zaznacz w ramce nawigacji ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
18. Na wyświetlonej stronie bazy certyfikatów wpisz hasło bazy certyfikatów *SYSTEM i kliknij **Kontynuuj**.

19. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
20. Z listy zadań wybierz **Przypisanie certyfikatu**, aby wyświetlić listę certyfikatów w bieżącej bazie certyfikatów.
21. Zaznacz certyfikat, który został utworzony w systemie *hosta*, i kliknij **Przypisanie do aplikacji**, aby wyświetlić listę aplikacji obsługujących protokół SSL, którym można przypisać certyfikat.
22. Zaznacz aplikacje, które powinny używać certyfikatów w komunikacji SSL, i kliknij **Kontynuuj**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru certyfikatu dla aplikacji.

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Aplikacje te przed udostępnieniem zasobów muszą być w stanie uwierzytelniać certyfikaty. W tym celu należy dla nich zdefiniować listę zaufanych ośrodków certyfikacji (CA). Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Gdy zadania te zostaną wykonane, aplikacje mogą używać certyfikatów wydanych przez lokalny ośrodek CA w innym systemie iSeries. Zanim jednak można będzie rozpocząć używanie tych aplikacji, należy skonfigurować je do korzystania z protokołu SSL.

Aby uzyskać dostęp do wybranych aplikacji poprzez połączenie SSL, użytkownik musi użyć programu DCM do pobrania kopii certyfikatu lokalnego ośrodka certyfikacji działającego na hoście. Certyfikat ten musi być skopiowany do pliku w komputerze osobistym użytkownika lub pobrany do przeglądarki użytkownika, w zależności od wymagań aplikacji używającej SSL.

Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V5R1

Certyfikatami używanymi przez aplikacje podczas sesji SSL zarządza się z bazy certyfikatów *SYSTEM w programie Menedżer certyfikatów cyfrowych (DCM). Jeśli program DCM nie był nigdy używany w systemie docelowym V5R1 do zarządzania certyfikatami podczas sesji SSL, bazy tej nie powinno być w tym systemie. Zadania związane z korzystaniem z przesłanych plików certyfikatów utworzonych na hoście lokalnego ośrodka certyfikacji (CA) zależą od istnienia bazy certyfikatów *SYSTEM w systemie docelowym. Jeśli nie ma bazy certyfikatów *SYSTEM, jej rolę mogą pełnić przesłane pliki certyfikatów. Jeśli w systemie docelowym V5R1 istnieje baza certyfikatów *SYSTEM, przesłane pliki certyfikatów mogą być wykorzystane na dwa sposoby:

- Przesłane pliki można traktować jak Inną bazę certyfikatów systemu
- Można wykonać import przesyłanych plików do istniejącej bazy certyfikatów *SYSTEM

Baza certyfikatów *SYSTEM nie istnieje

Jeśli w systemie docelowym V5R1 nie ma bazy certyfikatów *SYSTEM, jej rolę mogą pełnić przesłane pliki certyfikatów. Aby w docelowym systemie V5R1 używać plików certyfikatów, wykonaj następujące czynności:

1. Sprawdź, czy pliki bazy certyfikatów (dwa pliki: jeden z rozszerzeniem .KDB i jeden z rozszerzeniem .RDB) utworzone na hoście lokalnego ośrodka certyfikacji (CA) znajdują się w katalogu /QIBM/USERDATA/ICSS/CERT/SERVER.
2. W katalogu /QIBM/USERDATA/ICSS/CERT/SERVER, zmień nazwy przesłanych plików certyfikatów na DEFAULT.KDB oraz DEFAULT.RDB. Zmieniając nazwy tych plików w odpowiednim katalogu, tworzy się komponenty, które zawierają bazę certyfikatów *SYSTEM dla systemu docelowego. Pliki bazy certyfikatów zawierają już certyfikaty wielu publicznych ośrodków certyfikacji (CA). Podczas tworzenia plików bazy certyfikatów program DCM dodał do nich te certyfikaty, a także kopię certyfikatu ośrodka lokalnego.

Uwaga: Jeśli w systemie docelowym w katalogu /QIBM/USERDATA/ICSS/CERT/SERVER znajdują się już pliki DEFAULT.KDB i DEFAULT.RDB, oznacza to, że baza certyfikatów *SYSTEM już

istnieje w tym systemie. W takim przypadku nie należy zmieniać nazw przesłanych plików. Nadpisanie plików domyślnych spowoduje problemy podczas korzystania z programu DCM, przesłanej bazy certyfikatów i jej zawartości. Należy wówczas sprawdzić, czy przesłane pliki bazy certyfikatów mają unikalne nazwy i użyć ich jako **Innej bazy certyfikatów systemu**. Jeśli jednak użyje się tych plików jako Innej bazy certyfikatów systemu, nie będzie można użyć programu DCM do określenia, które aplikacje powinny używać tych certyfikatów.

3. Uruchom sesję DCM. Należy teraz zmienić hasło do bazy certyfikatów *SYSTEM, którą utworzono przez zmianę nazwy przesłanych plików. Zmiana hasła umożliwi programowi DCM zapisanie nowego hasła, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej bazy certyfikatów.
4. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
5. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia w systemie *hosta* bazy certyfikatów dla docelowego systemu V5R1, i kliknij **Kontynuuj**.
6. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów. Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć. Następnie należy określić aplikacje, które powinny używać certyfikatów w komunikacji SSL.
7. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
8. Na wyświetlonej stronie bazy certyfikatów wpisz nowe hasło i kliknij **Kontynuuj**.
9. Po odświeżeniu widoku ramki nawigacji zaznacz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
10. Z listy zadań wybierz **Aktualizacja przypisania certyfikatu**, aby wyświetlić listę aplikacji obsługujących SSL, do których można przypisać certyfikat.
11. Wybierz aplikację z listy i kliknij **Aktualizacja przypisania certyfikatu**.
12. Wybierz certyfikat wystawiony *na hoście* lokalnego ośrodka certyfikacji (CA) i kliknij **Przypisanie nowego certyfikatu**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru certyfikatu dla aplikacji.

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Aplikacje te przed udostępnieniem zasobów muszą być w stanie uwierzytelniać certyfikaty. W tym celu należy dla nich zdefiniować listę zaufanych ośrodków certyfikacji. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Gdy zadania te zostaną wykonane, aplikacje mogą używać certyfikatów wydanych przez lokalny ośrodek CA w innym systemie iSeries. Zanim jednak można będzie rozpocząć używanie tych aplikacji, należy skonfigurować je do korzystania z protokołu SSL.

Aby uzyskać dostęp do wybranych aplikacji poprzez połączenie SSL, użytkownik musi użyć programu DCM do pobrania kopii certyfikatu lokalnego ośrodka certyfikacji działającego na hoście. Certyfikat ten musi być skopiowany do pliku w komputerze osobistym użytkownika lub pobrany do przeglądarki użytkownika, w zależności od wymagań aplikacji używającej SSL.

Baza certyfikatów *SYSTEM istnieje — korzystanie z Innej bazy certyfikatów systemu

Jeśli w systemie docelowym V5R1 baza certyfikatów *SYSTEM już istnieje, należy zdecydować, jak pracować z plikami certyfikatów. Z przesłanych plików można utworzyć **Inną bazę certyfikatów systemu**. Można też zaimportować certyfikat prywatny i odpowiadający mu certyfikat lokalnego ośrodka certyfikacji do istniejącej bazy certyfikatów *SYSTEM.

Inne bazy certyfikatów systemu są definiowanymi przez użytkowników zapasowymi bazami certyfikatów SSL. Mogą one służyć do udostępniania certyfikatów na potrzeby napisanych przez użytkowników aplikacji

z obsługą SSL, które nie korzystają z funkcji API programu DCM w celu zarejestrowania ID aplikacji w tym programie. Opcja Inna baza certyfikatów systemu pozwala zarządzać certyfikatami dla aplikacji używających funkcji API SSL_Init w celu programowego dostępu do certyfikatów i wykorzystania ich do nawiązania sesji SSL. Funkcja ta umożliwia aplikacji użycie domyślnego certyfikatu z bazy certyfikatów zamiast certyfikatu specjalnego.

Aplikacje IBM iSeries (i aplikacje wielu dostawców oprogramowania) są napisane w taki sposób, aby korzystały wyłącznie z certyfikatów przechowywanych w bazie *SYSTEM. Jeśli użyje się przesłanych plików jako Innej bazy certyfikatów systemu, nie będzie można użyć programu DCM do określenia, które aplikacje powinny używać certyfikatów na potrzeby sesji SSL. W rezultacie nie będzie można skonfigurować standardowych aplikacji systemu iSeries z obsługą SSL, tak aby używały tego certyfikatu. Aby aplikacje systemu iSeries mogły używać tego certyfikatu, należy zaimportować go z przesłanej bazy certyfikatów do bazy certyfikatów *SYSTEM.

Aby użyć przesłanych plików certyfikatu jako Innej bazy certyfikatów systemu, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów (tego z rozszerzeniem .KDB) przesłanego z hosta ośrodka certyfikacji (CA). Podaj również hasło określone podczas tworzenia w systemie *hosta* bazy certyfikatów dla docelowego systemu V5R1, i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć. Następnie można zaznaczyć, że certyfikaty z tej bazy mają być używane jako certyfikaty domyślne.

5. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
6. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów, nowe hasło i kliknij **Kontynuuj**.
7. Po odświeżeniu widoku ramki nawigacji zaznacz **Zarządzanie bazą certyfikatów** i z listy zadań wybierz **Ustawienie domyślnego certyfikatu**.

Po utworzeniu i skonfigurowaniu Innej bazy certyfikatów systemu dowolna aplikacja korzystająca z funkcji API SSL_Init będzie mogła używać certyfikatu z tej bazy do nawiązywania połączeń SSL.

Baza certyfikatów *SYSTEM istnieje — korzystanie z certyfikatów w istniejącej bazie *SYSTEM

Certyfikatów z przesłanych plików bazy certyfikatów można używać również w bazie certyfikatów *SYSTEM istniejącej w systemie docelowym V5R1. W tym celu należy zaimportować certyfikaty z plików bazy certyfikatów do istniejącej bazy *SYSTEM. Nie można jednak zaimportować certyfikatów bezpośrednio z plików .KDB i .RDB, ponieważ funkcja importu programu DCM nie obsługuje formatu tych plików. Aby wykorzystać przesłane certyfikaty w istniejącej bazie certyfikatów *SYSTEM, należy otworzyć pliki jako Inną bazę certyfikatów systemu, a następnie wyeksportować je do bazy certyfikatów *SYSTEM.

Uwaga: W tej procedurze opisano, w jaki sposób w systemie docelowym wykorzystać Inną bazę certyfikatów systemu do wyeksportowania certyfikatów z oryginalnych plików bazy certyfikatów do bazy certyfikatów *SYSTEM. Procedura ta, użyta do dodania certyfikatów do bazy certyfikatów

*SYSTEM, pozwala uniknąć problemów w przypadku, gdyby system docelowy korzystał z mniej zaawansowanych produktów szyfrujących (5722–AC2) niż host.

Aby wyeksportować certyfikaty z plików bazy certyfikatów do bazy certyfikatów *SYSTEM w systemie docelowym V5R1, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i zaznacz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów (tego z rozszerzeniem .KDB) przesłanego z hosta ośrodka certyfikacji (CA). Podaj również hasło określone podczas tworzenia w systemie *hosta* bazy certyfikatów dla docelowego systemu V5R1 i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy. Jeśli przed zaznaczeniem opcji Automatyczne logowanie nie zostanie zmienione hasło, mogą pojawić się błędy podczas eksportowania certyfikatów z tej bazy do bazy certyfikatów *SYSTEM.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć.

5. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
6. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów, nowe hasło i kliknij **Kontynuuj**.
7. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań, a następnie wybierz z tej listy **Eksport certyfikatu**.
8. Zaznacz **Ośrodek certyfikacji** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**.

Uwaga: Certyfikat lokalnego ośrodka certyfikacji (CA) należy wyeksportować do bazy certyfikatów przed wyeksportowaniem certyfikatu serwera lub klienta. W przeciwnym razie może wystąpić błąd, ponieważ w bazie nie będzie certyfikatu lokalnego ośrodka.

9. Wybierz certyfikat lokalnego ośrodka certyfikacji (CA) i kliknij **Eksportuj**.
10. Jako miejsce docelowe eksportowanego certyfikatu wybierz **Baza certyfikatów** i kliknij **Kontynuuj**.
11. Wpisz *SYSTEM jako docelową bazę certyfikatów, podaj hasło do bazy certyfikatów *SYSTEM i kliknij **Kontynuuj**.
12. Teraz można wyeksportować certyfikat klienta lub serwera do bazy certyfikatów *SYSTEM. Zaznacz ponownie zadanie **Eksport certyfikatu**.
13. Zaznacz **Serwer lub klient** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**.
14. Zaznacz certyfikat serwera lub klienta i kliknij **Eksport**.
15. Jako miejsce docelowe eksportowanego certyfikatu wybierz **Baza certyfikatów** i kliknij **Kontynuuj**.
16. Wpisz *SYSTEM jako docelową bazę certyfikatów, podaj hasło do bazy certyfikatów *SYSTEM i kliknij **Kontynuuj**. Wyświetli się komunikat informujący o pomyślnie zakończonym eksporcie certyfikatu lub komunikat o błędzie, jeśli proces eksportowania nie powiódł się.
17. Teraz można przypisać certyfikat do aplikacji, aby mogły korzystać z protokołu SSL. Kliknij **Wybór ośrodka certyfikacji** i zaznacz w ramce nawigacji ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
18. Na wyświetlonej stronie bazy certyfikatów wpisz hasło bazy certyfikatów *SYSTEM i kliknij **Kontynuuj**.
19. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
20. Z listy zadań wybierz **Aktualizacja przypisania certyfikatu**, aby wyświetlić listę aplikacji obsługujących SSL, do których można przypisać certyfikat.
21. Wybierz aplikację z listy i kliknij **Aktualizacja przypisania certyfikatu**.
22. Wybierz certyfikat wystawiony *na hoście* lokalnego ośrodka certyfikacji (CA) i kliknij **Przypisanie nowego certyfikatu**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru certyfikatu dla aplikacji.

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Aplikacje te przed udostępnieniem zasobów muszą być w stanie uwierzytelniać certyfikaty. W tym celu należy dla nich zdefiniować listę zaufanych ośrodków certyfikacji. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Gdy zadania te zostaną wykonane, aplikacje mogą używać certyfikatów wydanych przez lokalny ośrodek CA w innym systemie iSeries. Zanim jednak można będzie rozpocząć używanie tych aplikacji, należy skonfigurować je do korzystania z protokołu SSL.

Aby uzyskać dostęp do wybranych aplikacji poprzez połączenie SSL, użytkownik musi użyć programu DCM do pobrania kopii certyfikatu lokalnego ośrodka certyfikacji działającego na hoście. Certyfikat ten musi być skopiowany do pliku w komputerze osobistym użytkownika lub pobrany do przeglądarki użytkownika, w zależności od wymagań aplikacji używającej SSL.

Wykorzystanie prywatnych certyfikatów do podpisywania obiektów w systemie docelowym V5R2 lub V5R1

Certyfikatami używanymi do podpisywania obiektów zarządza się z bazy certyfikatów *OBJECTSIGNING w programie Menedżer certyfikatów cyfrowych (DCM). Jeśli program DCM nie był nigdy używany w systemie docelowym V5R1 do zarządzania certyfikatami podpisującymi obiekty, bazy tej nie powinno być w tym systemie. Zadania związane z korzystaniem z przesłanych plików certyfikatów utworzonych na hoście lokalnego ośrodka certyfikacji (CA) zależą od tego, czy baza certyfikatów *OBJECTSIGNING istnieje w systemie docelowym. Jeśli nie ma bazy certyfikatów *OBJECTSIGNING, jej rolę mogą pełnić przesłane pliki certyfikatów. Jeśli w systemie docelowym istnieje baza certyfikatów *OBJECTSIGNING, przesłane certyfikaty należy zaimportować do tej bazy.

Baza certyfikatów *OBJECTSIGNING nie istnieje

Zadania, które trzeba wykonać, aby móc używać plików bazy certyfikatów utworzonych na hoście lokalnego ośrodka certyfikacji (CA), zależą od tego, czy program DCM był kiedykolwiek używany w systemie docelowym do zarządzania certyfikatami podpisującymi obiekty.

Jeśli w systemie docelowym V5R2 lub V5R1, w którym znajdują się przesłane pliki bazy certyfikatów, nie ma bazy certyfikatów *OBJECTSIGNING, wykonaj następujące czynności:

1. Sprawdź, czy pliki bazy certyfikatów (dwa pliki: jeden z rozszerzeniem .KDB i jeden z rozszerzeniem .RDB) utworzone na hoście lokalnego ośrodka certyfikacji (CA) znajdują się w katalogu /QIBM/USERDATA/ICSS/CERT/SIGNING.
2. Jeśli jest to konieczne, w katalogu /QIBM/USERDATA/ICSS/CERT/SIGNING zmień nazwy przesłanych plików certyfikatów na SGNOBJ.KDB oraz SGNOBJ.RDB. Zmieniając nazwę tych plików tworzy się komponenty, które zawierają bazę certyfikatów *OBJECTSIGNING dla systemu docelowego. Pliki bazy certyfikatów zawierają już certyfikaty wielu publicznych ośrodków certyfikacji (CA). Podczas tworzenia plików bazy certyfikatów program DCM dodał do nich te certyfikaty, a także kopię certyfikatu ośrodka lokalnego.

Uwaga: Jeśli w systemie docelowym w katalogu /QIBM/USERDATA/ICSS/CERT/SIGNING znajdują się już pliki SGNOBJ.KDB i SGNOBJ.RDB, oznacza to, że baza certyfikatów *OBJECTSIGNING już istnieje w tym systemie. W takim przypadku nie należy zmieniać nazw przesłanych plików. Nadpisanie domyślnych plików do podpisywania obiektów spowoduje problemy podczas korzystania z programu DCM, przesłanej bazy certyfikatów i jej zawartości. Istnieją dwa sposoby przeniesienia certyfikatów z tych plików do istniejącej bazy *OBJECTSIGNING. Można je wyeksportować do zestawu plików tekstowych, z których będzie je można zaimportować do bazy *OBJECTSIGNING. Można również otworzyć przesłane pliki jako Inną bazę certyfikatów systemu i wyeksportować certyfikaty bezpośrednio do bazy

*OBJECTSIGNING, tak jak to opisano w dalszej części tej dokumentacji. W każdym przypadku, aby móc zarządzać aplikacjami korzystającymi z tych certyfikatów, należy je przenieść do bazy *OBJECTSIGNING, zgodnie z opisaną procedurą.

3. Uruchom sesję DCM. Teraz należy zmienić hasło do bazy certyfikatów *OBJECTSIGNING. Zmiana hasła umożliwi programowi DCM zapisanie nowego hasła, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej bazy certyfikatów.
4. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
5. Na wyświetlonej stronie wpisz hasło określone podczas tworzenia bazy certyfikatów na hoście i kliknij **Kontynuuj**.
6. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów. Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć. Następnie można określić definicje aplikacji, które mogą korzystać z certyfikatu do podpisywania obiektów.
7. Po ponownym otwarciu bazy certyfikatów wybierz w ramce nawigacji **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
8. Z listy zadań wybierz **Dodaj aplikację**, aby rozpocząć proces tworzenia definicji aplikacji podpisujących obiekty za pomocą danego certyfikatu.
9. Wypełnij formularz, aby zdefiniować aplikację podpisującą obiekty, i kliknij **Dodaj**. Ta definicja aplikacji nie opisuje rzeczywistej aplikacji, tylko typy obiektów, które mają być podpisywane za pomocą konkretnego certyfikatu. W przypadku niejasności przy wypełnianiu formularza należy skorzystać z systemu pomocy.
10. Kliknij **OK**, aby zaakceptować komunikat potwierdzenia definicji aplikacji i wyświetlić listę zadań **Zarządzanie aplikacjami**.
11. Z listy zadań wybierz **Aktualizacja przypisania certyfikatu**, aby wyświetlić listę ID aplikacji podpisujących obiekty, do których można przypisać certyfikat.
12. Wybierz ID aplikacji z listy i kliknij **Aktualizacja przypisania certyfikatu**.
13. Wybierz certyfikat wystawiony na hoście lokalnego ośrodka certyfikacji (CA) i kliknij **Przypisanie nowego certyfikatu**.

Po zakończeniu tych czynności spełnione są wszelkie warunki, aby rozpocząć podpisywanie obiektów w celu zapewnienia ich integralności.

Aby odbiorcy dystrybuowanych podpisanych obiektów mogli zweryfikować podpis na obiekcie i upewnić się, że nie został on zmieniony oraz że pochodzi od znanego nadawcy, muszą dysponować programem DCM w wersji V5R1 lub V5R1. W celu sprawdzenia podpisu odbiorca musi mieć kopię certyfikatu do weryfikacji podpisów. Kopię tego certyfikatu należy dołączyć do pakietu z podpisanymi obiektami.

Ponadto odbiorca musi mieć kopię certyfikatu ośrodka certyfikacji (CA), który wystawił certyfikat użyty do podpisania obiektu. Jeśli do podpisania obiektów został użyty certyfikat z powszechnie znanego ośrodka certyfikacji (CA), w programie DCM odbiorcy powinna znajdować się kopia certyfikatu tego ośrodka. Jednak na wszelki wypadek należy ją dołączyć do przesyłanych podpisanych obiektów. Kopię certyfikatu lokalnego ośrodka należy na przykład przesłać do odbiorcy, jeśli obiekty zostały podpisane certyfikatem wystawionym przez lokalny ośrodek. Ze względów bezpieczeństwa certyfikat ośrodka należy dostarczyć w odrębnym pakiecie lub udostępnić go publicznie wszystkim, którzy go potrzebują.

Baza certyfikatów *OBJECTSIGNING istnieje

Certyfikatów z przesłanych plików bazy certyfikatów można używać również w bazie certyfikatów *OBJECTSIGNING istniejącej w systemie docelowym V5R2 lub V5R1. W tym celu należy zaimportować certyfikaty z plików bazy certyfikatów do istniejącej bazy *OBJECTSIGNING. Nie można jednak zaimportować certyfikatów bezpośrednio z plików .KDB i .RDB, ponieważ funkcja importu programu DCM nie obsługuje formatu tych plików. Certyfikaty te można dodać do bazy *OBJECTSIGNING, otwierając przesłane pliki w systemie docelowym V5R2 lub V5R1 jako Inną bazę certyfikatów systemu. Następnie

można wyeksportować certyfikaty z tej bazy bezpośrednio do bazy *OBJECTSIGNING. Z przesłanych plików należy wyeksportować zarówno certyfikat lokalny, jak i certyfikat lokalnego ośrodka certyfikacji (CA).

Aby wyeksportować certyfikaty z plików bazy certyfikatów bezpośrednio do bazy certyfikatów *OBJECTSIGNING w systemie docelowym V5R2 lub V5R1, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i zaznacz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
3. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów. Podaj również hasło określone podczas tworzenia tej bazy na hoście i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie bazą certyfikatów**, a następnie z listy zadań wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy. Jeśli przed zaznaczeniem opcji Automatyczne logowanie nie zostanie zmienione hasło, mogą pojawić się błędy podczas eksportowania certyfikatów z tej bazy do bazy certyfikatów *OBJECTSIGNING.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć.

5. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz **Inna baza certyfikatów systemu**, aby otworzyć tę bazę certyfikatów.
6. Na wyświetlonej stronie bazy certyfikatów oraz hasła podaj pełną ścieżkę i nazwę pliku bazy certyfikatów, nowe hasło i kliknij **Kontynuuj**.
7. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań, a następnie wybierz z tej listy **Eksport certyfikatu**.
8. Zaznacz **Ośrodek certyfikacji** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**.

Uwaga: W zadaniach założono, że korzystając z Innej bazy certyfikatów systemu, pracuje się z certyfikatami serwerów lub klientów. Założenie to bierze się stąd, że ten typ bazy certyfikatów przewidziano do spełnienia roli zapasowej bazy certyfikatów dla bazy certyfikatów *SYSTEM. Jednak skorzystanie z zadania eksportu w tej bazie certyfikatów jest najprostszym sposobem dodania certyfikatów z przesłanych plików do istniejącej bazy *OBJECTSIGNING.

9. Wybierz certyfikat lokalnego ośrodka certyfikacji (CA) i kliknij **Eksportuj**.

Uwaga: Certyfikat lokalnego ośrodka certyfikacji (CA) należy wyeksportować do bazy certyfikatów przed wyeksportowaniem certyfikatu podpisującego obiekty. W przeciwnym razie może wystąpić błąd, ponieważ w bazie nie będzie certyfikatu lokalnego ośrodka.

10. Jako miejsce docelowe eksportowanego certyfikatu wybierz **Baza certyfikatów** i kliknij **Kontynuuj**.
11. Wpisz *OBJECTSIGNING jako docelową bazę certyfikatów, podaj hasło do tej bazy i kliknij **Kontynuuj**.
12. Teraz można wyeksportować certyfikat podpisujący obiekty do bazy *OBJECTSIGNING. Zaznacz ponownie zadanie **Eksport certyfikatu**.
13. Zaznacz **Serwer lub klient** jako typ eksportowanego certyfikatu i kliknij **Kontynuuj**.
14. Wybierz właściwy certyfikat i kliknij **Eksport**.
15. Jako miejsce docelowe eksportowanego certyfikatu wybierz **Baza certyfikatów** i kliknij **Kontynuuj**.
16. Wpisz *OBJECTSIGNING jako docelową bazę certyfikatów, podaj hasło do bazy certyfikatów *OBJECTSIGNING i kliknij **Kontynuuj**. Wyświetli się komunikat informujący o pomyślnie zakończonym eksporcie certyfikatu lub komunikat o błędzie, jeśli proces eksportowania nie powiódł się.

Uwaga: Aby używać tego certyfikatu do podpisywania obiektów, należy w tym momencie przypisać certyfikat do aplikacji podpisującej obiekty.

Wykorzystanie prywatnych certyfikatów podczas sesji SSL w systemie docelowym V4R5 lub V4R4

Certyfikatami używanymi przez aplikacje podczas sesji SSL zarządza się z bazy certyfikatów *SYSTEM w programie Menedżer certyfikatów cyfrowych (DCM). Jeśli program DCM nie był nigdy używany w systemie docelowym V4R5 lub V4R4 do zarządzania certyfikatami dla sesji SSL, bazy tej nie powinno być w tym systemie. Przesłane pliki bazy certyfikatów, utworzone na hoście lokalnego ośrodka certyfikacji (CA), zawierają dwa certyfikaty. Pliki te to: utworzony certyfikat serwera lub klienta oraz (użyty do podpisania tego pierwszego certyfikatu) certyfikat prywatnego lokalnego ośrodka certyfikacji (CA).

Zadania związane z korzystaniem z przesłanych plików bazy certyfikatów zależą od tego, czy baza certyfikatów *SYSTEM istnieje w systemie docelowym. Jeśli nie ma bazy certyfikatów *SYSTEM, jej rolę mogą pełnić przesłane pliki certyfikatów. Jeśli w systemie docelowym istnieje baza certyfikatów *SYSTEM, przesłane pliki certyfikatów mogą być wykorzystane na dwa sposoby:

- Przesłane pliki można traktować jak Inną bazę certyfikatów systemu.
- Można wykonać import przesyłanych plików do istniejącej bazy certyfikatów *SYSTEM.

Baza certyfikatów *SYSTEM nie istnieje

Jeśli w systemie docelowym V4R5 lub V4R4 nie ma bazy certyfikatów *SYSTEM, wykonaj następujące czynności:

1. Sprawdź, czy pliki bazy certyfikatów (dwa pliki: jeden z rozszerzeniem .KDB i jeden z rozszerzeniem .RDB) utworzone na hoście lokalnego ośrodka certyfikacji (CA) znajdują się w katalogu /QIBM/USERDATA/ICSS/CERT/SERVER.
2. W katalogu /QIBM/USERDATA/ICSS/CERT/SERVER, zmień nazwy przesłanych plików certyfikatów na DEFAULT.KDB oraz DEFAULT.RDB. Zmieniając nazwy tych plików w odpowiednim katalogu, tworzy się komponenty, które zawierają bazę certyfikatów *SYSTEM dla systemu docelowego. Pliki bazy certyfikatów zawierają już certyfikaty wielu publicznych ośrodków certyfikacji (CA). Podczas tworzenia plików bazy certyfikatów program DCM dodał do nich te certyfikaty, a także kopię certyfikatu ośrodka lokalnego.

Uwaga: Jeśli w systemie docelowym w katalogu /QIBM/USERDATA/ICSS/CERT/SERVER znajdują się już pliki DEFAULT.KDB i DEFAULT.RDB, oznacza to, że baza certyfikatów *SYSTEM już istnieje w tym systemie. W takim przypadku nie należy zmieniać nazw przesłanych plików. Nadpisanie plików domyślnych spowoduje problemy podczas korzystania z programu DCM, przesłanej bazy certyfikatów i jej zawartości. Należy wówczas sprawdzić, czy przesłane pliki bazy certyfikatów mają unikalne nazwy i użyć ich jako **Innej bazy certyfikatów systemu**. Jeśli jednak użyje się tych plików jako Innej bazy certyfikatów systemu, nie będzie można użyć programu DCM do określenia, które aplikacje powinny używać tych certyfikatów.

3. Uruchom sesję DCM. Teraz należy zmienić hasło do bazy certyfikatów *SYSTEM. Zmiana hasła umożliwi programowi DCM zapisanie nowego hasła, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej bazy certyfikatów.
4. W ramce nawigacji sprawdź, czy baza *SYSTEM jest wymieniona na rozwijanej liście baz, i wybierz **Certyfikaty systemu**, aby wyświetlić listę dostępnych zadań. Wyświetli się okno **Baza certyfikatów i hasło**.
5. W odpowiednie pola wpisz *SYSTEM jako nazwę bazy, która ma być utworzona, i hasło określone podczas tworzenia plików na hoście lokalnego ośrodka certyfikacji (CA). Teraz należy zmienić hasło do bazy certyfikatów.
6. Z listy zadań w ramce nawigacji wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów. Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć.
7. Po ponownym otwarciu bazy *SYSTEM z listy zadań wybierz **Praca z aplikacjami chronionymi**, aby wyświetlić stronę pozwalającą zarządzać certyfikatami powiązanych z określonymi aplikacjami.
8. Z listy aplikacji wybierz aplikacje, które podczas sesji SSL powinny używać przesłanych certyfikatów prywatnych.

9. Kliknij **Praca z certyfikatami systemu** i zaznacz na hoście certyfikat wystawiony przez lokalny ośrodek certyfikacji (CA).
10. Kliknij **Przypisanie nowego certyfikatu**, aby używały go wybrane aplikacje.

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Użycie certyfikatów do uwierzytelniania klienta zapewnia, że aplikacje otrzymują poprawne certyfikaty, zanim udzielą dostępu do kontrolowanych przez siebie zasobów. Zanim jednak aplikacja będzie mogła uwierzytelniać certyfikaty wystawione przez dany ośrodek certyfikacji (CA), należy ją skonfigurować tak, aby uznawała ten ośrodek za zaufany. Aby sprawdzić, czy w bazie certyfikatów certyfikat ośrodka certyfikacji (CA) ma status zaufany, wyświetl stronę **Praca z ośrodkami certyfikacji**. Następnie, aby sprawdzić, czy aplikacja używająca certyfikatu ufa lokalnemu ośrodkowi, który ją wystawił, należy użyć strony **Praca z aplikacjami chronionymi**. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Gdy zadania te zostaną wykonane, aplikacje w docelowym systemie V4R5 lub V4R4 mogą używać certyfikatów wydanych przez lokalny ośrodek certyfikacji V4R5 w innym systemie iSeries. Zanim jednak można będzie rozpocząć używanie tych aplikacji, należy skonfigurować je do korzystania z protokołu SSL.

Aby uzyskać dostęp do wybranych aplikacji poprzez połączenie SSL, użytkownik musi użyć programu DCM do pobrania kopii certyfikatu lokalnego ośrodka certyfikacji działającego na hoście. Certyfikat ten musi być skopiowany do pliku w komputerze osobistym użytkownika lub pobrany do przeglądarki użytkownika, w zależności od wymagań aplikacji używającej SSL.

Baza certyfikatów *SYSTEM istnieje — korzystanie z Innej bazy certyfikatów systemu

Jeśli w systemie docelowym V4R5 lub V4R4 baza certyfikatów *SYSTEM już istnieje, należy określić sposób pracy z plikami certyfikatów. Przesłane pliki bazy certyfikatów zawierają dwa certyfikaty: utworzony certyfikat serwera lub klienta oraz (użyty do podpisania tego pierwszego certyfikatu) certyfikat prywatnego lokalnego ośrodka certyfikacji (CA). Z przesłanych plików można utworzyć **Inną bazę certyfikatów systemu**. Można też zaimportować certyfikat prywatny i odpowiadający mu certyfikat ośrodka certyfikacji (CA) do istniejącej bazy certyfikatów *SYSTEM.

Jeśli użyje się przesłanych plików jako **Innej bazy certyfikatów systemu**, nie będzie można użyć programu DCM do określenia, które aplikacje powinny używać certyfikatów na potrzeby sesji SSL. Można jednak ustawić certyfikaty z tej bazy jako certyfikaty domyślne. Opcja Inna baza certyfikatów systemu pozwala zarządzać certyfikatami dla aplikacji używających funkcji API SSL_Init, w celu programowego dostępu do certyfikatów i wykorzystania ich do nawiązania sesji SSL. Funkcja ta umożliwia aplikacji użycie domyślnego certyfikatu z bazy certyfikatów zamiast konkretnego innego certyfikatu.

Jeśli w systemie docelowym V4R5 lub V4R4, w którym mają zostać użyte przesłane pliki bazy certyfikatów, istnieje baza certyfikatów *SYSTEM, wykonaj następujące czynności:

1. Uruchom sesję DCM. Teraz należy zmienić hasło do przesłanej bazy certyfikatów. Zmiana hasła umożliwi programowi DCM zapisanie nowego hasła, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej bazy certyfikatów.
2. Sprawdź, czy na rozwijanej liście w ramce nawigacji znajduje się pozycja **INNE** i wybierz **Certyfikaty systemu**, aby wyświetlić listę dostępnych zadań. Wyświetli się okno **Baza certyfikatów i hasło**.
3. W odpowiednie pola wpisz pełną ścieżkę i nazwę pliku bazy certyfikatów (rozszerzenie KDB) przesłanej z hosta lokalnego ośrodka certyfikacji (CA). Wpisz hasło określone podczas tworzenia plików na *hoście*. Teraz należy zmienić hasło do bazy certyfikatów.
4. Z listy zadań **Certyfikaty systemu** w ramce nawigacji wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć.

Następnie można zaznaczyć, że certyfikaty z tej bazy mają być używane jako certyfikaty domyślne.

5. W ramce nawigacji wybierz **Praca z certyfikatami**, aby wyświetlić stronę umożliwiającą wykonanie wielu zadań administracyjnych.
6. Z listy certyfikatów wybierz ten, który ma być certyfikatem domyślnym dla bieżącej bazy, i kliknij **Ustaw wartości domyślne**.

Po utworzeniu i skonfigurowaniu Innej bazy certyfikatów systemu dowolna aplikacja korzystająca z funkcji API SSL_Init będzie mogła używać certyfikatu z tej bazy do nawiązywania połączeń SSL.

Baza certyfikatów *SYSTEM istnieje — importowanie plików do istniejącej bazy *SYSTEM

Przed zaimportowaniem certyfikatów do bazy *SYSTEM w systemie docelowym V4R5 lub V4R4 należy najpierw wyeksportować je z utworzonej bazy certyfikatów do plików o innym formacie. Następnie będzie można zaimportować z tych nowych plików certyfikaty do bazy *SYSTEM. Przesłane pliki bazy certyfikatów zawierają dwa certyfikaty: utworzony certyfikat serwera lub klienta oraz (użyty do podpisania tego pierwszego certyfikatu) certyfikat prywatnego lokalnego ośrodka certyfikacji (CA). Oba te certyfikaty należy zaimportować do bazy certyfikatów *SYSTEM.

Uwaga: Funkcje eksportu w wersji V4R5 i V4R4 programu DCM działają inaczej niż w wersji V5R2 i podczas eksportowania w systemie docelowym certyfikatu prywatnego lokalnego ośrodka certyfikacji (CA) mogą wystąpić problemy. Dlatego należy użyć hosta V5R2 do wyeksportowania *dodatkowej* kopii certyfikatu ośrodka lokalnego do odrębnego pliku, zamiast używać w tym celu systemu docelowego V4R4 lub V4R5. Po wyeksportowaniu certyfikatu lokalnego ośrodka w systemie V5R2 hosta można ręcznie przesłać plik wynikowy do systemu docelowego V4R4 lub V4R5 i wykonać kolejne czynności opisane w tej procedurze w celu zaimportowania certyfikatu lokalnego ośrodka do bazy certyfikatów *SYSTEM. Certyfikat lokalnego ośrodka certyfikacji (CA) należy zaimportować, *zanim* zaimportuje się utworzony przy jego użyciu certyfikat prywatny. Jeśli najpierw zostanie zaimportowany certyfikat prywatny, może wystąpić błąd, ponieważ w bazie nie będzie certyfikatu lokalnego ośrodka.

Aby wyeksportować certyfikat z plików bazy certyfikatu w systemie docelowym V4R4 lub V4R5, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. Sprawdź, czy na rozwijanej liście w ramce nawigacji znajduje się pozycja **INNE** i wybierz **Certyfikaty systemu**, aby wyświetlić listę dostępnych zadań. Wyświetli się okno **Baza certyfikatów i hasło**.
3. Wpisz pełną ścieżkę i nazwę przesłanych plików bazy certyfikatów oraz hasło określone podczas ich tworzenia na *hoście* i kliknij **OK**. Teraz należy zmienić hasło do bazy certyfikatów.
4. Z listy zadań Certyfikaty systemu w ramce nawigacji wybierz **Zmiana hasła**. Wypełnij formularz, aby zmienić hasło do bazy certyfikatów.

Uwaga: Podczas zmiany hasła do bazy certyfikatów należy wybrać opcję **Automatyczne logowanie**. Wybór tej opcji spowoduje, że program DCM zapisze nowe hasło, dzięki czemu będzie można korzystać z wszystkich funkcji zarządzania certyfikatami w programie DCM w odniesieniu do tej nowej bazy. Jeśli przed zaznaczeniem opcji Automatyczne logowanie nie zostanie zmienione hasło, mogą pojawić się błędy podczas eksportowania certyfikatów z tej bazy.

Aby można było pracować z certyfikatami w bazie, po zmianie hasła należy ją ponownie otworzyć.

5. W ramce nawigacji wybierz **Praca z certyfikatami**, aby wyświetlić listę certyfikatów.
6. Wybierz z listy certyfikat prywatny i kliknij **Eksportuj**, aby wyświetlić stronę Eksport certyfikatu.
7. Wypełnij formularz Eksport certyfikatu.

Uwaga: Należy sprawdzić, czy plikowi nadano unikalną nazwę i rozszerzenie. Plik można nazwać na przykład myfile.exp. Nadając plikowi nazwę, nie należy korzystać z następujących rozszerzeń: .TXT, .KDB, .RDB lub .KYR; używanie wymienionych rozszerzeń może spowodować błędy podczas importowania certyfikatu z pliku. Należy wybrać numer wersji systemu docelowego, w którym będzie używany ten certyfikat. Podany numer wersji ma wpływ na format wyeksportowanego certyfikatu.

8. Kliknij przycisk **OK**. U góry strony pojawi się komunikat, że program DCM wyeksportował certyfikat do wybranego pliku.

Należy teraz użyć programu DCM w systemie V5R2 hosta, aby wyeksportować dodatkową kopię certyfikatu ośrodka lokalnego, a następnie ręcznie przesłać go do docelowego systemu V4R4 lub V4R5. Należy także w tym systemie docelowym użyć programu DCM do wyeksportowania prywatnego certyfikatu serwera lub klienta do pliku. Po wykonaniu tych czynności można przystąpić do importowania certyfikatów do bazy certyfikatów *SYSTEM. Certyfikat lokalnego ośrodka certyfikacji (CA) należy zaimportować *przed* importem certyfikatu prywatnego utworzonego za pomocą certyfikatu tego ośrodka. Jeśli najpierw zostanie zaimportowany certyfikat prywatny, może wystąpić błąd, ponieważ w bazie nie będzie certyfikatu ośrodka lokalnego.

Aby zaimportować certyfikaty z tych plików i określić aplikacje z obsługą SSL, które będą ich używać, wykonaj następujące czynności w systemie docelowym V4R4 lub V4R5:

1. Uruchom sesję DCM.
2. W ramce nawigacji sprawdź, czy baza *SYSTEM jest wymieniona na rozwijanej liście baz, i wybierz **Certyfikaty systemu**, aby wyświetlić listę dostępnych zadań. Wyświetli się okno **Baza certyfikatów i hasło**.
3. Wybierz *SYSTEM jako bazę certyfikatów, która ma być otworzona, podaj hasło i kliknij **Kontynuuj**.
4. Zaimportuj certyfikat lokalnego ośrodka z pliku eksportu utworzonego na hoście V5R2. W ramce nawigacji wybierz **Odbiór certyfikatu ośrodka certyfikacji**, aby wyświetlić formularz.
5. Wypełnij formularz i kliknij **OK**, aby wyświetlić stronę Pomyślny odbiór certyfikatu. Podczas pracy z bazą *SYSTEM na tej stronie wyświetlane są aplikacje, spośród których można wybrać te, które mają ufać zaimportowanemu certyfikatowi ośrodka certyfikacji (CA).

Uwaga: Niektóre aplikacje z obsługą SSL obsługują również uwierzytelnianie klienta na podstawie certyfikatu. Dzięki użyciu certyfikatów do uwierzytelniania klienta aplikacje otrzymują poprawne certyfikaty, zanim udzielą dostępu do kontrolowanych przez siebie zasobów. Zanim jednak aplikacja będzie mogła uwierzytelniać certyfikaty wystawione przez dany ośrodek certyfikacji (CA), należy ją skonfigurować tak, aby uznawała ten ośrodek za zaufany. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

6. Wybierz aplikacje, które powinny ufać ośrodkowi CA wydającemu te certyfikaty, i kliknij **OK**. Pojawi się strona Status aplikacji chronionych potwierdzająca, że wybrane aplikacje ufają nowemu certyfikatowi.
7. Można teraz zaimportować certyfikat serwera. W ramce nawigacji wybierz **Praca z certyfikatami**, aby wyświetlić listę certyfikatów.
8. Kliknij przycisk **Import**, aby wyświetlić stronę Import certyfikatu.
9. Wypełnij formularz Import certyfikatu i kliknij przycisk **OK**, aby powrócić do strony Praca z certyfikatami. Sprawdź, czy podałeś nazwę pliku zawierającego wyeksportowany certyfikat serwera lub klienta oraz numer wersji systemu docelowego zgodne z podanymi wcześniej podczas eksportowania certyfikatu. U góry strony pojawi się komunikat, że program DCM dodał certyfikat do bieżącej bazy certyfikatów. Ponadto importowany certyfikat powinien pojawić się na liście certyfikatów.
10. Określ aplikacje, które powinny używać zaimportowanego certyfikatu w komunikacji SSL. W ramce nawigacji wybierz **Praca z aplikacjami chronionymi**, aby wyświetlić stronę, która pozwoli zarządzać certyfikatami powiązanymi z określonymi aplikacjami.
11. Wybierz aplikację z listy i kliknij **Praca z certyfikatem systemowym**, aby wyświetlić listę certyfikatów, które można powiązać z aplikacjami nawiązującymi połączenia SSL.

- Wybierz certyfikat z listy i kliknij **Przypisanie nowego certyfikatu**, aby przypisać wybrany certyfikat do określonej aplikacji. U góry strony zostanie wyświetlony komunikat potwierdzenia wyboru certyfikatu.

Po wykonaniu tych zadań aplikacje w systemie docelowym V4R4 lub V4R5 będą mogły używać certyfikatów wystawionych przez lokalny ośrodek certyfikacji (CA) w innym systemie iSeries. Zanim jednak można będzie rozpocząć używanie tych aplikacji, należy skonfigurować je do korzystania z protokołu SSL.

Aby uzyskać dostęp do wybranych aplikacji poprzez połączenie SSL, użytkownik musi użyć programu DCM do pobrania kopii certyfikatu lokalnego ośrodka certyfikacji działającego na hoście. Certyfikat ten musi być skopiowany do pliku w komputerze osobistym użytkownika lub pobrany do przeglądarki użytkownika, w zależności od wymagań aplikacji używającej SSL.

Zarządzanie aplikacjami w programie DCM

Program Menedżer certyfikatów cyfrowych (DCM) może być wykorzystywany do wykonywania wielu różnych zadań administracyjnych dotyczących aplikacji z obsługą SSL i aplikacji podpisujących obiekty. Przy jego użyciu można na przykład decydować, których certyfikatów będą używać aplikacje do nawiązywania sesji komunikacyjnych Secure Sockets Layer (SSL). Wykonywane zadania administracyjne zależą od typu aplikacji i bazy certyfikatów, z którą się pracuje. Zarządzanie aplikacjami jest możliwe tylko dla baz *SYSTEM lub *OBJECTSIGNING.

O ile większość zadań dostępnych w programie DCM i dotyczących aplikacji jest zrozumiała, kilka z nich może wymagać dodatkowych wiadomości. W tym celu należy zapoznać się z następującymi sekcjami:

Tworzenie definicji aplikacji, gdzie opisano typy aplikacji, które można zdefiniować i z którymi można pracować.

Zarządzanie przypisywaniem certyfikatów aplikacjom, gdzie opisano, jak przypisać aplikacji certyfikat używany do nawiązywania komunikacji SSL lub do podpisywania obiektów oraz jak zmienić to przypisanie.

Definiowanie listy zaufanych ośrodków certyfikacji (CA) dla aplikacji, gdzie opisano przypadki, w których można i powinno się zdefiniować ośrodki certyfikacji (CA), którym aplikacja może ufać przy sprawdzaniu i akceptowaniu certyfikatów.

Pozostałe zadania programu DCM opisane zostały w pomocy online.

Tworzenie definicji aplikacji

Istnieją dwa typy definicji aplikacji, z którymi można pracować w programie DCM: definicje aplikacji korzystających z SSL i definicje aplikacji używanych do podpisywania obiektów.

Aby używać programu DCM do pracy z aplikacjami SSL i ich certyfikatami, należy najpierw zarejestrować aplikacje w programie DCM jako definicje aplikacji posiadające unikalne ID aplikacji. Programiści aplikacji rejestrują aplikacje z obsługą SSL w programie DCM za pomocą funkcji API (QSYRGAP, QsyRegisterAppForCertUse) w celu automatycznego utworzenia ID aplikacji. Wszystkie aplikacje IBM iSeries z obsługą SSL są zarejestrowane w programie DCM, dzięki czemu można używać tego programu do przypisywania im certyfikatów w celu nawiązywania połączeń SSL. Również dla aplikacji napisanych samodzielnie lub zakupionych u innych dostawców można w programie DCM utworzyć definicję aplikacji i ID aplikacji. Utworzenie definicji aplikacji SSL dla aplikacji klienta lub serwera jest możliwe tylko podczas pracy z bazą certyfikatów *SYSTEM.

Aby używać certyfikatu do podpisywania obiektów, należy zdefiniować aplikację, która będzie używała tego certyfikatu. W przeciwieństwie do definicji aplikacji SSL definicje aplikacji podpisujących obiekty nie opisują faktycznej aplikacji. Zamiast tego, utworzone definicje aplikacji powinny opisywać typ lub grupę obiektów, które mają być podpisywane. Utworzenie definicji aplikacji podpisującej obiekty jest możliwe tylko podczas pracy z bazą certyfikatów *OBJECTSIGNING.

Aby utworzyć definicję aplikacji, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. Kliknij **Wybór ośrodka certyfikacji** i wybierz odpowiednią bazę. (Będzie to albo baza *SYSTEM, albo baza *OBJECTSIGNING, zależnie od typu tworzonej definicji aplikacji.)

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) znajdujący się w górnej części strony, aby otworzyć pomoc online.

3. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Dodaj aplikację**, aby wyświetlić formularz definiowania aplikacji.

Uwaga: W przypadku pracy z bazą certyfikatów *SYSTEM program DCM zapyta, czy ma to być definicja aplikacji klienta, czy definicja aplikacji serwera.

6. Wypełnij formularz i kliknij **Dodaj**. Informacje podane dla definicji aplikacji zależą od typu definiowanej aplikacji. Definiując aplikację serwera, można również określić, czy aplikacja może używać certyfikatów do uwierzytelniania klienta i czy uwierzytelnianie jest wymagane. Można również zdecydować, czy aplikacja ma używać listy zaufanych ośrodków certyfikacji (CA) do uwierzytelniania certyfikatów.

Zarządzanie przypisywaniem certyfikatów aplikacjom

Aby aplikacja mogła realizować bezpieczne funkcje, jak na przykład nawiązywanie połączeń Secure Sockets Layer (SSL) lub podpisywanie obiektów, należy wcześniej użyć programu Menedżer certyfikatów cyfrowych (DCM) do przypisania jej certyfikatu. Aby przypisać certyfikat aplikacji lub zmienić przypisanie certyfikatu, wykonaj poniższe czynności:

1. Uruchom sesję DCM.
2. Kliknij **Wybór ośrodka certyfikacji** i wybierz odpowiednią bazę. (Będzie to albo baza *SYSTEM, albo baza *OBJECTSIGNING, zależnie od typu aplikacji, której przypisuje się certyfikat.)

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) znajdujący się w górnej części strony, aby otworzyć pomoc online.

3. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
5. W bazie certyfikatów *SYSTEM, zaznacz typ aplikacji, którą będziesz zarządzać (zaznacz aplikację typu **serwer** lub **klient**).
6. Z listy zadań wybierz **Aktualizacja przypisania certyfikatu**, aby wyświetlić listę aplikacji, do których można przypisać certyfikat.
7. Wybierz aplikację z listy i kliknij **Aktualizacja przypisania certyfikatu**, aby wyświetlić listę certyfikatów, które można przypisać aplikacji.
8. Wybierz z listy certyfikat i kliknij **Przypisanie nowego certyfikatu**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru certyfikatu dla aplikacji.

Uwaga: Przypisując certyfikat aplikacji z obsługą SSL, obsługującej również wykorzystanie certyfikatów do uwierzytelniania klienta, należy zdefiniować listę zaufanych ośrodków certyfikacji dla tej aplikacji. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Przy zmianie lub usunięciu certyfikatu aplikacji podczas jej działania aplikacja może, ale nie musi rozpoznać wprowadzonej zmiany. Na przykład serwery Client Access Express automatycznie wprowadzą wszelkie

dokonane zmiany przypisanych im certyfikatów. Jednak w przypadku serwerów Telnet, serwera IBM HTTP Server for iSeries lub innych aplikacji może pojawić się konieczność ich restartowania, aby wprowadziły one dokonane zmiany certyfikatów.

Począwszy od wersji V5R2, aby przypisać ten sam certyfikat wielu aplikacjom jednocześnie, można wykorzystać zadanie Przypisanie certyfikatu.

Definiowanie listy zaufanych ośrodków certyfikacji dla aplikacji

Aplikacje obsługujące certyfikaty do uwierzytelniania klienta podczas sesji Secure Sockets Layer (SSL) muszą określić, czy zaakceptować certyfikat jako prawidłowy dowód tożsamości. Jednym z kryteriów stosowanych przez aplikację jest to, czy uwierzytelniany certyfikat został wystawiony przez zaufany ośrodek certyfikacji (CA).

Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można zdefiniować ośrodki certyfikacji (CA), którym aplikacje mogą ufać, przeprowadzając uwierzytelnianie klienta. Służy do tego lista zaufanych ośrodków certyfikacji (CA).

Przed zdefiniowaniem listy zaufanych ośrodków certyfikacji (CA) należy spełnić kilka warunków:

- aplikacja musi obsługiwać uwierzytelnianie klienta,
- w definicji aplikacji należy podać, że aplikacja korzysta z listy zaufanych ośrodków certyfikacji (CA).

Jeśli w definicji aplikacji podano, że aplikacja używa listy zaufanych ośrodków certyfikacji (CA), aplikacja będzie mogła pomyślnie uwierzytelniać klienta dopiero po zdefiniowaniu tej listy. Dzięki temu aplikacja będzie sprawdzała jedynie certyfikaty z ośrodków, które zostały uznane za zaufane. Jeśli użytkownik lub klient przedstawi certyfikat z ośrodka, który nie jest wymieniony na liście ośrodków zaufanych, aplikacja nie zaakceptuje go jako podstawy do pozytywnego uwierzytelnienia.

Po wpisaniu na listę ośrodka certyfikacji (CA) należy sprawdzić, czy ośrodek ten działa.

Aby zdefiniować listę zaufanych ośrodków certyfikacji (CA) dla aplikacji, wykonaj następujące czynności:

1. Uruchoom sesję DCM.
2. Kliknij **Wybór ośrodka certyfikacji** i wybierz *SYSTEM, aby otworzyć tę bazę certyfikatów.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) znajdujący się w górnej części strony, aby otworzyć pomoc online.

3. Na wyświetlonej stronie bazy certyfikatów wpisz hasło określone podczas tworzenia bazy certyfikatów i kliknij **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Definiowanie listy zaufanych ośrodków certyfikacji (CA)**.
6. Wybierz typ aplikacji, dla której chcesz zdefiniować listę, i kliknij **Kontynuuj**.
7. Wybierz aplikację z listy i kliknij **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodków, których można użyć do zdefiniowania listy ośrodków zaufanych.
8. Wybierz ośrodek, któremu aplikacja powinna ufać, i kliknij **OK**. Program DCM wyświetli komunikat w celu potwierdzenia wyboru zaufanych ośrodków.

Uwaga: Można wybrać pojedyncze ośrodki z listy lub zaznaczyć, że aplikacja albo powinna ufać każdemu ośrodkowi z listy, albo nie powinna ufać żadnemu. Ponadto, przed dodaniem ośrodka do listy można go wyświetlić lub sprawdzić.

Sprawdzanie poprawności certyfikatów i aplikacji

Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można sprawdzać poprawność poszczególnych certyfikatów lub aplikacji, które ich używają. Lista cech sprawdzanych przez program DCM zależy od tego, czy sprawdza się certyfikat, czy aplikację.

Sprawdzanie aplikacji

Korzystanie z programu DCM do sprawdzania definicji aplikacji pomaga zapobiec problemom pojawiającym się podczas wykonywania przez aplikację funkcji wymagających użycia certyfikatów. Takie problemy mogłyby uniemożliwić aplikacji pomyślne uczestniczenie w sesji Secure Sockets Layer (SSL) lub podpisywanie obiektów.

Podczas weryfikacji aplikacji program DCM sprawdza, czy tej aplikacji został przypisany certyfikat i czy certyfikat ten jest prawidłowy. Ponadto, dla aplikacji skonfigurowanych do korzystania z listy zaufanych ośrodków certyfikacji (CA) program DCM sprawdza, czy na liście znajduje się przynajmniej jeden certyfikat ośrodka. Następnie program DCM sprawdza, czy certyfikaty zaufanych ośrodków są prawidłowe. Także w przypadku, gdy w definicji aplikacji podano, że przetwarzana jest lista odwołań certyfikatów (CRL) i zdefiniowano położenie listy CRL dla danego ośrodka, program DCM sprawdza listę CRL w ramach procesu sprawdzania aplikacji.

Sprawdzanie poprawności certyfikatu

Podczas weryfikacji certyfikatu program DCM sprawdza wiele pozycji dotyczących tego certyfikatu, aby potwierdzić jego autentyczność i poprawność. Sprawdzenie certyfikatu zmniejsza prawdopodobieństwo wystąpienia problemów w pracy aplikacji używającej tego certyfikatu do nawiązywania połączeń SSL lub do podpisywania obiektów.

Elementem procesu sprawdzania certyfikatu jest upewnienie się za pomocą programu DCM, czy certyfikat nie jest przedawniony. Ponadto, program DCM sprawdza, czy certyfikat nie znajduje się na liście odwołań certyfikatów (CRL) jako certyfikat odwołany, o ile ośrodkowi, który wystawił ten certyfikat, znane jest położenie listy CRL. Dodatkowo program DCM sprawdza, czy certyfikat ośrodka, który wystawił dany certyfikat, znajduje się w bieżącej bazie certyfikatów i czy certyfikat tego ośrodka jest aktywny a tym samym zaufany. Jeśli certyfikat ma klucz prywatny (certyfikaty serwera, klienta i podpisujące obiekty), program DCM sprawdza również parę kluczy publiczny-prywatny, aby upewnić się, że są one zgodne. Polega to na zaszyfrowaniu danych kluczem publicznym i sprawdzeniu, czy mogą one być odszyfrowane kluczem prywatnym.

Przypisanie certyfikatu do aplikacji

Począwszy od wersji V5R2, nowe rozszerzenia Menedżera certyfikatów cyfrowych (DCM) umożliwiają szybkie i proste przypisanie certyfikatu do aplikacji. Przypisanie certyfikatu do wielu aplikacji jest możliwe tylko dla baz *SYSTEM lub *OBJECTSIGNING.

Aby przypisać certyfikat dla jednej lub kilku aplikacji, wykonaj poniższe kroki:

1. Uruchom sesję DCM.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza podczas korzystania z programu DCM należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING** lub ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
3. Wpisz hasło do bazy certyfikatów i kliknij **Kontynuuj**.
4. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Przypisanie certyfikatu**, aby wyświetlić listę certyfikatów dla bieżącej bazy certyfikatów.

6. Zaznacz certyfikat na liście i kliknij **Przypisanie do aplikacji**, aby wyświetlić listę definicji aplikacji dla bieżącej bazy certyfikatów.
7. Zaznacz jedną lub kilka aplikacji na liście i kliknij **Kontynuuj**. Wyświetli się komunikat potwierdzający wybranie przypisania lub komunikat o błędzie, jeśli pojawią się problemy.

Zarządzanie informacjami o położeniu listy CRL

Menedżer certyfikatów cyfrowych (DCM) umożliwi definiowanie informacji o miejscu położenia listy odwołań certyfikatów (CRL) dla określonych ośrodków certyfikacji (CA) oraz zarządzanie tymi informacjami w celu wykorzystania ich w procesie sprawdzania poprawności certyfikatu. Program DCM lub aplikacja, która przetwarza listy CRL, mogą używać tych list do określenia, czy ośrodek certyfikacji (CA), który wystawił dany certyfikat, nie unieważnił go. Po zdefiniowaniu miejsca położenia listy CRL dla danego ośrodka aplikacja obsługująca uwierzytelnianie klienta za pomocą certyfikatu ma dostęp do tej listy.

Aplikacje obsługujące uwierzytelnianie klientów za pomocą certyfikatów mogą skorzystać z listy CRL, aby zapewnić bardziej rygorystyczne uwierzytelnianie certyfikatów, które wymagają akceptacji jako dowody tożsamości. Aby aplikacja mogła używać określonej listy CRL w procesie weryfikacji certyfikatu, definicja aplikacji w programie DCM musi narzucać na tę aplikację taki obowiązek.

Przetwarzanie list CRL

Jeśli używa się programu DCM do weryfikacji certyfikatu lub aplikacji program ten domyślnie przetwarza listę CRL, jako element procesu weryfikacji. Jeśli dla ośrodka certyfikacji (CA), który wystawił sprawdzany certyfikat, nie określono miejsca położenia listy CRL, program DCM nie będzie mógł sprawdzić tej listy. Jednak program DCM może sprawdzić inne ważne informacje dotyczące certyfikatu, takie jak poprawność podpisu ośrodka certyfikacji (CA) na danym certyfikacie oraz przynależność ośrodka, który wystawił dany certyfikat do listy ośrodków zaufanych.

Definiowanie położenia CRL

Aby zdefiniować położenie listy CRL dla danego ośrodka, wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji wybierz **Zarządzanie położeniami CRL**, aby wyświetlić listę zadań.
3. Z listy zadań wybierz **Dodaj położenie CRL**, aby wyświetlić formularz pozwalający opisać położenie oraz sposób dostępu programu DCM lub aplikacji do tego miejsca.
4. Wypełnij formularz i kliknij **OK**. Następnie należy nadać unikalną nazwę miejscu położenia listy CRL, zidentyfikować serwer LDAP, na którym znajduje się lista, i podać informacje o połączeniu z serwerem LDAP.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza w tym zadaniu należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy. Można teraz powiązać definicje położenia CRL z danym ośrodkiem certyfikacji (CA).

5. W ramce nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
6. Na liście zadań zaznacz **Aktualizacja przypisania położenia CRL**, aby wyświetlić listę certyfikatów ośrodka certyfikacji (CA).
7. Z listy wybierz certyfikat ośrodka certyfikacji (CA), który chcesz przypisać do utworzonej definicji położenia CRL i kliknij **Aktualizacja przypisania położenia CRL**. Wyświetli się lista położen CRL.
8. Z listy wybierz położenie list CRL, które chcesz powiązać ośrodkiem certyfikacji (CA), i kliknij **Aktualizacja przypisania**. W górnej części strony wyświetlony zostanie komunikat informujący, że położenie list CRL przypisano do certyfikatu ośrodka certyfikacji (CA).

Po zdefiniowaniu miejsca położenia listy CRL dla określonego ośrodka certyfikacji (CA) program DCM i inne aplikacje będą mogły skorzystać z tych informacji podczas przetwarzania listy CRL. Aby jednak przetwarzanie listy CRL było możliwe, serwer usług katalogowych musi zawierać odpowiednią listę CRL. Ponadto należy skonfigurować aplikacje serwera i klienta usług katalogowych do korzystania z protokołu SSL i przypisać certyfikat do aplikacji za pomocą programu DCM.

Aby więcej się dowiedzieć o konfigurowaniu i korzystaniu z serwera usług katalogowych (LDAP) iSeries, należy zapoznać się z następującymi tematami w Centrum informacyjnym (CA):

- Usługi katalogowe (LDAP)
Pod tym hasłem można znaleźć wszystkie informacje niezbędne do poznania zagadnień związanych z konfigurowaniem i korzystaniem z serwera usług katalogowych (LDAP) iSeries.
- Korzystanie z ochrony Secure Sockets Layer (SSL) podczas pracy z serwerem usług katalogowych LDAP
Ten temat poświęcony jest opisowi czynności, które trzeba wykonać, aby skonfigurować serwer LDAP do korzystania z protokołu SSL w celu bezpiecznej komunikacji.

Przechowywanie kluczy certyfikatów za pomocą koprocesora szyfrującego IBM 4758

Jeśli w systemie iSeries zainstalowany jest koprocesor szyfrujący IBM 4758–023 PCI, można go użyć do bezpiecznego przechowywania klucza prywatnego certyfikatu. Koprocesor może służyć do przechowywania klucza prywatnego certyfikatu serwera, klienta lub lokalnego ośrodka certyfikacji (CA). Nie można go jednak użyć do przechowywania klucza prywatnego certyfikatu użytkownika, ponieważ klucz ten musi być przechowywany w systemie użytkownika. Na razie nie można również przechowywać za pomocą koprocesora klucza prywatnego certyfikatu podpisującego obiekty.

Koprocesora można używać do przechowywania certyfikatów na dwa sposoby:

- przechowywać klucz prywatny certyfikatu bezpośrednio w koprocesorze,
- użyć klucza głównego koprocesora do zaszyfrowania klucza prywatnego certyfikatu i przechowywać go w specjalnym pliku klucza.

Wyboru opcji przechowywania klucza dokonuje się podczas tworzenia lub odnawiania certyfikatu. Także w przypadku przechowywania klucza prywatnego certyfikatu za pomocą koprocesora można zmienić przypisanie koprocesora dla tego klucza.

Aby można było użyć koprocesora do przechowywania klucza prywatnego, powinien być on udostępniony w systemie przed użyciem programu Menedżer certyfikatów cyfrowych (DCM). W przeciwnym razie podczas procesu tworzenia lub odnawiania certyfikatu w programie DCM nie będzie dostępna strona z wyborem opcji przechowywania klucza.

W procesie tworzenia lub odnawiania certyfikatu serwera lub klienta wyboru opcji przechowywania klucza prywatnego dokonuje się po wyborze typu ośrodka, który podpisał bieżący certyfikat. W procesie tworzenia lub odnawiania certyfikatu lokalnego ośrodka certyfikacji (CA) pierwszą czynnością jest wybór opcji przechowywania klucza prywatnego.

Przechowywanie klucza prywatnego certyfikatu bezpośrednio w koprocesorze

Aby lepiej zabezpieczyć zarówno dostęp do klucza prywatnego certyfikatu jak i jego wykorzystanie, można przechowywać go bezpośrednio w koprocesorze szyfrującym IBM 4758–023 PCI. Wyboru tej opcji dokonuje się w procesie tworzenia lub odnawiania certyfikatu w programie Menedżer certyfikatów cyfrowych (DCM).

Aby przechowywać klucz prywatny certyfikatu bezpośrednio w koprocesorze, wykonaj następujące czynności na stronie **Wybór miejsca przechowywania klucza**:

1. Wybierz **Sprzęt** jako opcję przechowywania.
2. Kliknij **Kontynuuj**. Spowoduje to wyświetlenie strony **Wybór opisu urządzenia szyfrującego**.
3. Z listy urządzeń wybierz to, którego chcesz użyć do przechowywania klucza prywatnego certyfikatu.
4. Kliknij **Kontynuuj**. Program DCM wyświetli kolejne strony, które należy wypełnić, podając między innymi informacje identyfikujące tworzony lub odnawiany certyfikat.

Korzystanie z klucza głównego koprocatora do szyfrowania klucza prywatnego certyfikatu

Aby lepiej zabezpieczyć zarówno dostęp do klucza prywatnego certyfikatu jak i jego wykorzystanie, można użyć klucza głównego koprocatora szyfrującego IBM 4758–023 PCI do zaszyfrowania tego klucza i zapisania go w specjalnym pliku klucza. Wyboru tej opcji dokonuje się w procesie tworzenia lub odnawiania certyfikatu w programie Menedżer certyfikatów cyfrowych (DCM).

Aby użyć tej opcji, należy skorzystać z przeglądarkowego interfejsu konfiguracyjnego koprocatora szyfrującego IBM 4758–023 PCI w celu utworzenia specjalnego pliku klucza. Za pomocą tego samego interfejsu należy również powiązać ten plik z opisem urządzenia koprocatora, którego zamierza się użyć. Przeglądarkowy interfejs konfiguracyjny koprocatora jest dostępny na stronie Zadania iSeries.

Jeśli w systemie zainstalowano i udostępniono kilka koprocatorów, istnieje możliwość współużytkowania klucza prywatnego certyfikatu między wieloma urządzeniami. Aby opisy urządzeń mogły współużytkować klucz prywatny, wszystkie urządzenia muszą mieć taki sam klucz główny. Proces dystrybucji tego samego klucza głównego do różnych urządzeń nazywa się *klonowaniem*. Współużytkowanie klucza przez urządzenia umożliwia zastosowanie wyrównywania obciążeń protokołu Secure Sockets Layer (SSL), co może poprawić wydajność bezpiecznych sesji komunikacyjnych.

Aby użyć klucza głównego koprocatora do zaszyfrowania klucza prywatnego certyfikatu i zapisania go w specjalnym pliku klucza, wykonaj następujące czynności na stronie **Wybór miejsca przechowywania klucza**:

1. Wybierz **Zaszyfrowany sprzętowo** jako opcję przechowywania klucza.
2. Kliknij **Kontynuuj**. Spowoduje to wyświetlenie strony **Wybór opisu urządzenia szyfrującego**.
3. Z listy urządzeń wybierz to, którego chcesz użyć do zaszyfrowania klucza prywatnego certyfikatu.
4. Kliknij **Kontynuuj**. Jeśli w systemie zainstalowano i udostępniono kilka koprocatorów, wyświetli się strona **Wybór dodatkowych opisów urządzeń szyfrujących**.

Uwaga: Jeśli w systemie jest dostępne tylko jedno urządzenie koprocatora, program DCM wyświetli kolejne strony, które należy wypełnić, podając między innymi informacje identyfikujące tworzony lub odnawiany certyfikat.

5. Z listy urządzeń wybierz przynajmniej jeden opis urządzenia, z którym ma być współużytkowany klucz prywatny certyfikatu.

Uwaga: Wybrane opisy urządzeń muszą mieć ten sam klucz główny, co urządzenie wybrane na poprzedniej stronie. Aby sprawdzić, czy wybrane urządzenia mają ten sam klucz główny, należy użyć zadania Weryfikacja klucza głównego w przeglądarkowym interfejsie konfiguracyjnym koprocatora szyfrującego 4758. Przeglądarkowy interfejs konfiguracyjny koprocatora jest dostępny na stronie Zadania iSeries.

6. Kliknij **Kontynuuj**. Program DCM wyświetli kolejne strony, które należy wypełnić, podając między innymi informacje identyfikujące tworzony lub odnawiany certyfikat.

Zarządzanie miejscem położenia ośrodków certyfikacji PKIX

Ośrodek certyfikacji infrastruktury klucza publicznego X.509 (Public Key Infrastructure for X.509 - PKIX) wystawia certyfikaty na podstawie najnowszych internetowych standardów X.509 opisujących implementację infrastruktury klucza publicznego. Standardy PKIX są przedstawione w dokumencie Request For Comments (RFC) 2560.

Ośrodki certyfikacji PKIX wymagają bardziej rygorystycznej identyfikacji przed wystawieniem certyfikatu; zwykle żądają, aby występujący o certyfikat podmiot przedstawił dowód tożsamości poprzez ośrodek rejestracji (RA). Kiedy wnioskodawca dostarczy do ośrodka rejestracji wymagane świadectwa tożsamości, ośrodek ten potwierdza jego tożsamość. Następnie, zależnie od procedury przyjętej przez ośrodek certyfikacji (CA), ośrodek rejestracji lub wnioskodawca składa potwierdzony wniosek w ośrodku certyfikacji (CA). W miarę powszechniejszego przyjmowania tych standardów, ośrodki certyfikacji zgodne z PKIX staną

się bardziej dostępne. Jeśli przyjęte wymogi bezpieczeństwa żądają ścisłej kontroli dostępu do zasobów udostępnianych użytkownikom przez aplikacje obsługujące SSL, należy rozważyć skorzystanie z usług ośrodka certyfikacji (CA) zgodnego ze standardami PKIX. Taki ośrodek certyfikacji zgodny ze standardem PKIX udostępnia do użytku publicznego na przykład system Lotus Domino.

Jeśli dla posiadanych aplikacji wybierze się certyfikaty wystawione przez ośrodek PKIX, będzie można użyć programu Menedżer certyfikatów cyfrowych (DCM) do zarządzania tymi certyfikatami. W programie DCM konfiguruje się adres URL ośrodka PKIX. Dzięki temu w programie DCM ośrodek ten będzie dostępny jako opcja uzyskiwania podpisanych certyfikatów.

Aby używać programu DCM do zarządzania certyfikatami z ośrodka PKIX, należy go skonfigurować do używania miejsca położenia tego ośrodka. W tym celu wykonaj następujące czynności:

1. Uruchom sesję DCM.
2. W ramce nawigacji wybierz **Zarządzanie położeniami żądań PKIX**, aby wyświetlić formularz, który umożliwi podanie adresu URL dla ośrodka certyfikacji PKIX lub powiązanego z nim ośrodka rejestracji.
3. Wpisz pełny adres URL ośrodka PKIX, do którego zamierzasz wystąpić o certyfikat, na przykład: <http://www.thawte.com>, i kliknij **Dodaj**. Dodanie adresu URL konfiguruje program DCM do udostępniania ośrodka PKIX jako opcji uzyskiwania certyfikatów.

Po dodaniu miejsca składania wniosków do ośrodka PKIX program DCM dodaje ten ośrodek jako opcję przy określaniu ośrodka wystawiającego certyfikat w zadaniu **Tworzenie certyfikatu**.

Podpisywanie obiektów

Istnieją trzy metody podpisywania obiektów. Pierwszą z nich jest napisanie programu wywołującego funkcję API Sign Object. Można też do podpisywania obiektów użyć programu Menedżer certyfikatów cyfrowych (DCM). Począwszy od wersji V5R2, można użyć opcji Centrum Zarządzania programu iSeries Navigator, aby podpisywała obiekty podczas tworzenia z nich pakietów, które mają być przesłane do innych systemów iSeries.

Certyfikatów, którymi zarządza się w programie DCM, można użyć do podpisywania dowolnych obiektów zintegrowanego systemu plików, z wyjątkiem obiektów przechowywanych w bibliotekach. Można podpisywać jedynie te obiekty, które przechowuje się w systemie plików QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG i *FILE (tylko zbiory składowania). W wersji V5R2 można podpisywać obiekty komend (*CMD). Nie można podpisywać obiektów przechowywanych na innych serwerach iSeries.

Obiekty można podpisywać certyfikatami nabytymi w publicznych ośrodkach certyfikacji (CA) lub utworzonymi w prywatnym lokalnym ośrodku certyfikacji (CA) za pomocą programu DCM. Proces podpisywania wygląda tak samo, niezależnie od tego, czy używa się certyfikatów prywatnych, czy publicznych.

Wymagania wstępne do podpisywania obiektów

Programu DCM (lub funkcji API Sign Object) można użyć do podpisywania obiektów dopiero wtedy, gdy spełni się pewne wstępne wymagania:

- Istniejąca baza certyfikatów *OBJECTSIGNING, powstała w procesie tworzenia lokalnego ośrodka certyfikacji lub w procesie zarządzania certyfikatami podpisującymi obiekty z publicznych ośrodków certyfikacji.
- Baza certyfikatów *OBJECTSIGNING musi zawierać przynajmniej jeden certyfikat: albo utworzony za pomocą lokalnego ośrodka, albo uzyskany z ośrodka publicznego.
- Stworzenie definicji aplikacji podpisującej obiekty.
- Aplikacji, która ma być używana do podpisywania obiektów, musi być przypisany certyfikat.

Korzystanie z programu DCM do podpisywania obiektów

Aby podpisać jeden lub kilka obiektów za pomocą programu DCM, wykonaj następujące czynności:

1. Uruchom sesję DCM.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza podczas korzystania z programu DCM należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
3. Wpisz hasło do bazy certyfikatów ***OBJECTSIGNING** i kliknij **Kontynuuj**.
4. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie podpisywanymi obiektami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Podpisanie obiektu**, aby wyświetlić listę definicji aplikacji, których można użyć do podpisywania obiektów.
6. Wybierz aplikację i kliknij **Podpisanie obiektu**, aby wyświetlić formularz do podania miejsca położenia obiektów, które mają być podpisywane.

Uwaga: Jeśli wybrana aplikacja nie ma przypisanego certyfikatu, nie można jej użyć do podpisywania obiektów. Należy najpierw użyć zadania **Aktualizowanie przypisania certyfikatów** na stronie **Zarządzanie aplikacjami**, aby przypisać certyfikat do definicji aplikacji.

7. W wyświetlone pola wpisz pełną ścieżkę i nazwę pliku obiektu lub katalogu obiektów, które chcesz podpisać, i kliknij **Kontynuuj**. Można również wpisać położenie katalogu i kliknąć **Przeglądaj**, aby przejrzeć zawartość katalogu i wybrać obiekty do podpisu.

Uwaga: Nazwa obiektu musi zaczynać się od ukośnika, w przeciwnym razie mogą wystąpić błędy. Do określenia części obiektów katalogu, które mają zostać podpisane, można także użyć znaków zastępczych. Te znaki to gwiazdka (*), która określa "dowolny ciąg znaków", i znak zapytania (?), który określa "dowolny pojedynczy znak". Aby na przykład podpisać wszystkie obiekty w określonym katalogu, można wpisać /moj_katalog*/; aby podpisać wszystkie programy w określonej bibliotece, można wpisać /QSYS.LIB/QGPL.LIB/*.PGM. Znaków zastępczych można używać tylko w ostatnim członie nazwy ścieżki; wpisanie na przykład /moj_katalog*/nazwa_pliku spowoduje wyświetlenie komunikatu o błędzie. Aby użyć funkcji Przeglądaj do wyświetlenia listy zawartości biblioteki lub katalogu, należy użyć znaków zastępczych w nazwie ścieżki, a następnie kliknąć przycisk **Przeglądaj**.

8. Wybierz opcje przetwarzania, których chcesz użyć do podpisywania wybranych obiektów, i kliknij **Kontynuuj**.

Uwaga: Wybranie opcji oczekiwania na wyniki zadania spowoduje wyświetlenie pliku wynikowego bezpośrednio w przeglądarce. Wyniki bieżącego zadania zostaną dopisane na końcu pliku wyników. W rezultacie plik ten może zawierać oprócz wyników bieżącego zadania także wyniki poprzednich zadań. Aby określić, które wiersze pliku odnoszą się do bieżącego zadania, można użyć pola daty. Pole to ma format RRRRMMDD. Pierwszym polem w pliku może być albo ID komunikatu (jeśli podczas przetwarzania obiektów wystąpił błąd) lub pole daty (określające datę przetwarzania zadania).

9. Podaj pełną ścieżkę i nazwę pliku do zapisywania wyników zadania dla operacji podpisywania obiektów i kliknij **Kontynuuj**. Można także wpisać ścieżkę do katalogu i kliknąć **Przeglądaj**, aby wyświetlić zawartość tego katalogu i wybrać plik do zapisywania wyników zadania. Wyświetli się komunikat informujący, że wprowadzono zadanie w celu podpisania obiektów. Aby wyświetlić wyniki zadania, znajdź zadanie **QOJSGNBAT** w protokole zadania.

Weryfikowanie podpisów obiektów

Za pomocą programu Menedżer certyfikatów cyfrowych (DCM) można weryfikować autentyczność podpisów cyfrowych na obiektach. Weryfikacja podpisu pozwala upewnić się, że dane obiektu nie zostały zmienione od czasu, kiedy właściciel obiektu go podpisał.

Wymagania wstępne dla weryfikacji podpisów

Przed użyciem programu DCM do weryfikowania podpisów na obiektach muszą być spełnione pewne wymagania wstępne:

- Musi istnieć baza certyfikatów *SIGNATUREVERIFICATION, aby można było zarządzać certyfikatami do weryfikacji podpisów.

Uwaga: W przypadku weryfikacji podpisów na obiektach podpisanych w tym samym systemie można korzystać z bazy certyfikatów *OBJECTSIGNING. Czynności wykonywane w programie DCM przy weryfikacji podpisów są takie same dla obydwu baz certyfikatów. Jednak baza certyfikatów *SIGNATUREVERIFICATION musi istnieć i powinna się w niej znajdować kopia certyfikatu, którym podpisano obiekt, nawet wtedy, gdy weryfikuje się podpisy pracując z bazą *OBJECTSIGNING.

- Baza *SIGNATUREVERIFICATION musi zawierać kopię certyfikatu, którym podpisano obiekty.
- Baza *SIGNATUREVERIFICATION musi zawierać kopię certyfikatu ośrodka certyfikacji (CA), z którego pochodzi certyfikat użyty do podpisania obiektów.

Korzystanie z programu DCM do weryfikowania podpisów na obiektach

Aby weryfikować podpisy na obiektach za pomocą programu DCM, wykonaj następujące czynności:

1. Uruchom sesję DCM.

Uwaga: W przypadku pojawienia się pytań dotyczących określonego formularza podczas korzystania z programu DCM należy kliknąć przycisk znaku zapytania (?) u góry strony, aby uzyskać dostęp do systemu pomocy.

2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SIGNATUREVERIFICATION**, aby otworzyć tę bazę certyfikatów.
3. Wpisz hasło do bazy certyfikatów *SIGNATUREVERIFICATION i kliknij **Kontynuuj**.
4. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie podpisywanymi obiektami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Sprawdzanie podpisu obiektu**, aby określić położenie obiektów, dla których chcesz weryfikować podpisy.
6. W wyświetlone pola wpisz pełną ścieżkę i nazwę pliku obiektu lub katalogu obiektów, których podpisy chcesz zweryfikować, i kliknij **Kontynuuj**. Można również wpisać położenie katalogu i kliknąć **Przeglądaj**, aby przejrzeć zawartość katalogu i wybrać obiekty do weryfikacji podpisu.

Uwaga: Do określenia części obiektów katalogu, które mają zostać zweryfikowane, można także użyć znaków zastępczych. Te znaki to gwiazdka (*), która określa "dowolny ciąg znaków", i znak zapytania (?), który określa "dowolny pojedynczy znak". Aby na przykład podpisać wszystkie obiekty w określonym katalogu, można wpisać /moj_katalog/*; aby podpisać wszystkie programy w określonej bibliotece, można wpisać /QSYS.LIB/QGPL.LIB/*.PGM. Znaków zastępczych można używać tylko w ostatnim członie nazwy ścieżki; wpisanie na przykład /moj_katalog*/nazwa_pliku spowoduje wyświetlenie komunikatu o błędzie. Aby użyć funkcji Przeglądaj do wyświetlenia listy zawartości biblioteki lub katalogu, należy użyć znaków zastępczych w nazwie ścieżki, a następnie kliknąć przycisk **Przeglądaj**.

7. Wybierz opcje przetwarzania, których chcesz użyć do weryfikowania podpisów wybranych obiektów i kliknij **Kontynuuj**.

Uwaga: Wybranie opcji oczekiwania na wyniki zadania spowoduje wyświetlenie pliku wynikowego bezpośrednio w przeglądarce. Wyniki bieżącego zadania zostaną dopisane na końcu pliku wyników. W rezultacie plik ten może zawierać oprócz wyników bieżącego zadania także wyniki poprzednich zadań. Aby określić, które wiersze pliku odnoszą się do bieżącego zadania, można użyć pola daty. Pole to ma format RRRRMMDD. Pierwszym polem w pliku może być albo ID komunikatu (jeśli podczas przetwarzania obiektów wystąpił błąd), albo pole daty (określające datę przetwarzania zadania).

8. Podaj pełną ścieżkę i nazwę pliku do zapisywania wyników zadania dla operacji weryfikacji podpisów obiektów i kliknij **Kontynuuj**. Można także wpisać ścieżkę do katalogu i kliknąć **Przeglądaj**, aby

wyświetlić zawartość tego katalogu i wybrać plik do zapisywania wyników zadania. Wyświetli się komunikat informujący, że wprowadzono zadanie w celu weryfikacji podpisów obiektów. Aby wyświetlić wyniki zadania, znajdź zadanie **QOBJSGNBAT** w protokole zadania.

Do wyświetlenia informacji o certyfikacie, którym podpisano obiekt, można także użyć programu DCM. Pozwala to sprawdzić przed rozpoczęciem pracy z obiektem, czy pochodzi on z zaufanego źródła.

Rozdział 9. Rozwiązywanie problemów związanych z programem DCM

Na następujących stronach można znaleźć informacje pomocne przy rozwiązywaniu niektórych najczęściej spotykanych problemów mogących wystąpić podczas pracy z programem Menedżer certyfikatów cyfrowych (DCM).

Poniżej opisano problemy, z jakimi może się zetknąć użytkownik, oraz sposoby ich rozwiązania.

Rozwiązywanie problemów związanych z hasłami i problemów ogólnych

W sekcji opisano najczęstsze problemy związane z interfejsem użytkownika programu DCM oraz sposoby ich rozwiązywania.

Rozwiązywanie problemów związanych z bazami certyfikatów i bazami kluczy

W sekcji opisano najczęstsze problemy związane z bazami certyfikatów i bazami kluczy oraz sposoby ich rozwiązywania.

Rozwiązywanie problemów związanych z przeglądarką

W sekcji opisano problemy, jakie mogą wystąpić podczas korzystania z przeglądarki w celu dostępu do programu DCM, oraz sposoby ich rozwiązania.

Rozwiązywanie problemów związanych z serwerem HTTP Server for iSeries

W sekcji opisano najczęstsze problemy związane z serwerem HTTP i sposoby ich rozwiązywania.

Błędy migracji i procedury odtwarzania

W sekcji opisano problemy występujące najczęściej podczas migracji programu DCM z poprzednich wersji oraz sposoby rozwiązywania tych problemów.

Rozwiązywanie problemów związanych z przypisywaniem certyfikatów użytkowników

W sekcji opisano najczęstsze problemy, które mogą wystąpić podczas rejestracji certyfikatu użytkownika, oraz sposoby ich rozwiązywania.

Rozwiązywanie problemów związanych z hasłami i problemów ogólnych

W przedstawionej poniżej tabeli można znaleźć informacje pomocne przy rozwiązywaniu niektórych najczęściej spotykanych problemów związanych z hasłami oraz problemów ogólnych, które mogą wystąpić podczas pracy z programem Menedżer certyfikatów cyfrowych (DCM).

| Problem | Możliwe rozwiązanie |
|--|---|
| Nie można znaleźć dodatkowej pomocy dla DCM. | W programie DCM kliknij "?". Można także przeszukać Centrum informacyjne i zewnętrzne serwisy WWW. |
| Podczas próby otworzenia bazy certyfikatów wystąpił błąd NET.DATA. | W zadaniu Wybór ośrodka certyfikacji należy kliknąć przyciskiem myszy Kontynuuj , nie zaś używać klawisza Enter na klawiaturze. |
| Hasło do bazy certyfikatów lokalnego ośrodka certyfikacji i do bazy certyfikatów *SYSTEM nie działa. | W hasłach rozróżnia się wielkie i małe litery. Sprawdź, czy klawisz Caps Lock ma ten sam stan, co w trakcie przypisywania hasła. |
| Próba zmiany hasła podczas zadania Wybór ośrodka certyfikacji nie powiodła się. | Funkcja zmiany hasła działa tylko wtedy, gdy program DCM zapisał hasło. Program DCM automatycznie zapisuje hasło podczas tworzenia baz certyfikatów. Jednak w przypadku zmiany hasła dla Innej bazy certyfikatów systemu, aby program DCM kontynuował składowanie hasła, należy zaznaczyć opcję Automatyczne logowanie . |

| Problem | Możliwe rozwiązanie |
|---|--|
| | <p>Podobnie gdy baza certyfikatów przenoszona jest z jednego systemu do drugiego, należy w nowym systemie zmienić hasło dla bazy certyfikatów, aby program DCM zeszkładował je automatycznie. Aby zmienić hasło, podczas gdy baza certyfikatów otwierana jest w nowym systemie, należy podać oryginalne hasło tej bazy. Gdy baza certyfikatów zostaje otwarta za pomocą oryginalnego hasła i zmienia się hasło w celu zeszkładowania go, nie można użyć opcji zmiany hasła. Jeśli hasło nie zostanie zmienione i zeszkładowane, program DCM oraz protokół SSL nie będą mogły automatycznie go odzyskać, gdy będzie ono potrzebne w innych funkcjach. Jeśli przenoszona baza certyfikatów będzie używana jako Inna baza certyfikatów systemu, podczas zmiany hasła należy zaznaczyć opcję Automatyczne logowanie, co zapewni, że program DCM zeszkładowuje nowe hasło dla tego typu bazy certyfikatów.</p> |
| | <p>Należy w systemowych narzędziach serwisowych SST (System Service Tools (SST)) w opcji Praca z ochroną systemu sprawdzić wartość atrybutu "Zezw. na nowe certyfikaty cyfrowe". Hasło bazy certyfikatów nie może zostać zmienione, jeśli atrybut ten ma ustawioną wartość 2 (Nie). Używając komendy STRSST, po wprowadzeniu ID użytkownika narzędzi serwisowych i hasła, można podglądać i zmienić wartość tego atrybutu. Następnie należy zaznaczyć opcję "Praca z ochroną systemu". ID użytkownika narzędzi serwisowych jest prawdopodobnie ID użytkownika z uprawnieniem specjalnym QSECOFR.</p> |
| <p>Nie można znaleźć źródła certyfikatu ośrodka certyfikacji, który ma być odebrany w systemie iSeries.</p> | <p>Niektóre ośrodki certyfikacji (CA) nie udostępniają swoich certyfikatów. Jeśli nie można uzyskać certyfikatu ośrodka, należy skontaktować się ze sprzedawcą oprogramowania, który mógł podpisać specjalne porozumienie z ośrodkiem certyfikacji (CA).</p> |
| <p>Nie można znaleźć bazy certyfikatów *SYSTEM.</p> | <p>Baza certyfikatów *SYSTEM musi znajdować się w pliku /qibm/userdata/icss/cert/server/default.kdb. Jeśli ta baza certyfikatów nie istnieje, należy ją utworzyć za pomocą programu DCM. W tym celu należy skorzystać z zadania Tworzenie nowej bazy certyfikatów.</p> |
| <p>W programie DCM wystąpił błąd, który powtarza się pomimo usunięcia jego przyczyn.</p> | <p>Należy wyczyścić pamięć podręczną przeglądarki. W tym celu należy ustawić wielkość pamięci podręcznej na 0 i restartować przeglądarkę.</p> |
| <p>Problem z serwerem LDAP. Przypisania certyfikatów nie są wyświetlane, podczas gdy informacje o aplikacjach chronionych są wyświetlane zaraz po przypisaniu certyfikatu. Problem ten pojawia się najczęściej podczas pobierania przeglądarki Netscape Communications za pomocą programu iSeries Navigator. Według ustawionych preferencji pamięci podręcznej, dokument w pamięci porównywany jest z dokumentem w sieci "Jeden raz podczas sesji".</p> | <p>Należy zmienić tę wartość domyślną, aby pamięć podręczna była sprawdzana za każdym razem.</p> |
| <p>Użycie programu DCM do zaimportowania certyfikatu podpisanego przez zewnętrzny ośrodek certyfikacji, na przykład Entrust, powoduje wystąpienie komunikatu o błędzie informującego, że okres ważności nie obejmuje bieżącej daty lub nie pokrywa się z okresem ważności certyfikatu wystawiającego.</p> | <p>System przedstawia okres ważności w formacie czasu GTF. Należy poczekać jeden dzień i ponowić próbę. Należy również sprawdzić, czy w lokalnym systemie iSeries wprowadzono prawidłową wartość poprawki UTC (dspsysval qutcoffset). Jeśli widnieje tam wartość Daylight Savings Time, wartość poprawki może być nieprawidłowa.</p> |

| Problem | Możliwe rozwiązanie |
|---|--|
| Przy próbie zaimportowania certyfikatu Entrust pojawia się błąd podstawowy 64. | Certyfikat ten znajduje się na liście certyfikatów o specyficznym formacie, takim jak format PEM. Jeśli funkcja kopiowania w przeglądarce nie działa prawidłowo, można skopiować dodatkowe dane, które nie należą do certyfikatu, na przykład znaki odstępu na początku każdego wiersza. W takiej sytuacji certyfikat nie będzie nadawał się do użycia w systemie iSeries. Niektóre strony WWW powodują ten błąd. Inne strony WWW zostały zaprojektowane tak, aby uniknąć tego problemu. Należy porównać wygląd oryginalnego certyfikatu z wynikiem wklejenia. Powinny być takie same. |
| Podczas migracji z wersji V4R3 pomijane są wygasłe certyfikaty systemu. | Wygasły certyfikat systemu jest niewłaściwy i nie może być przeniesiony do bazy certyfikatów *SYSTEM. Należy usunąć stary plik kluczy lub usunąć go z wersji V4R3 przed rozpoczęciem migracji, zignorować komunikat o niepowodzeniu migracji lub ponownie spróbować przeprowadzić migrację. |
| Nie można znaleźć przykładowego kodu do dodawania certyfikatów do list weryfikacji. | Przykładowy kod nie jest jeszcze dostępny. |

Rozwiązywanie problemów związanych z bazami certyfikatów i bazami kluczy

W przedstawionej poniżej tabeli można znaleźć informacje pomocne przy rozwiązywaniu niektórych najczęściej spotykanych problemów związanych z bazami certyfikatów oraz bazami kluczy, które mogą wystąpić podczas pracy z programem Menedżer certyfikatów cyfrowych (DCM).

| Problem | Możliwe rozwiązanie |
|---|--|
| System nie znalazł bazy kluczy lub znalazł błędną bazę. | Należy sprawdzić hasło i nazwę pliku, szukając błędów w pisowni oraz upewnić się, czy do nazwy pliku dołączona jest ścieżka razem z pierwszym ukośnikiem. |
| Błąd tworzenia bazy kluczy. | Należy sprawdzić, czy nie ma konfliktu nazw. Konflikt może dotyczyć innego pliku niż ten, którego dotyczy pytanie. |
| System nie akceptuje pliku tekstowego ośrodka certyfikacji (CA), który został przesłany binarnie z innego systemu. Akceptuje ten plik po przesłaniu w kodzie ASCII (American National Standard Code for Information Interchange). | Pliki kluczy i bazy kluczy mają format binarny i dlatego są różne. Dla plików tekstowych ośrodka certyfikacji (CA) należy użyć protokołu FTP w trybie ASCII, a dla plików binarnych, takich jak pliki z rozszerzeniami: .kdb, .kyr, .sth, .rdb, itd., protokołu FTP w trybie binarnym. |
| Nie można zmieniać hasła bazy kluczy. Certyfikat w bazie kluczy jest nieważny. | Po sprawdzeniu, czy problemem nie jest niewłaściwe hasło, należy znaleźć i usunąć z bazy certyfikatów niepoprawny certyfikat lub certyfikaty i spróbować zmienić hasło. Jeśli w bazie certyfikatów znajdują się wygasłe certyfikaty, certyfikaty te są niepoprawne. Z tego powodu funkcja zmiany hasła bazy certyfikatów może uniemożliwiać zmianę hasła i proces szyfrowania nie szyfruje prywatnych kluczy wygasłego certyfikatu. Zapobiega to wprowadzeniu zmiany hasła i system może informować, że jedną z przyczyn jest błąd bazy certyfikatów. Należy usunąć niewłaściwe (wygasłe) certyfikaty z bazy certyfikatów. |

| Problem | Możliwe rozwiązanie |
|--|--|
| Zastosowanie certyfikatów jest niezbędne w przypadku użytkowników internetowych. To powoduje konieczność użycia listy weryfikacji. Jednak funkcje list weryfikacji w programie DCM są niedostępne. | Partnerzy handlowi, którzy tworzą aplikacje używające list weryfikacji, muszą napisać własny kod przypisujący listy weryfikacji do ich aplikacji. Muszą także napisać kod, który określa, kiedy tożsamość użytkownika internetowego jest prawidłowo zatwierdzana, tak aby do listy weryfikacji mógł być dodany certyfikat. Należy zapoznać się z tematem poświęconym funkcji API QsyAddVldCertificate w Centrum informacyjnym. Więcej informacji o konfigurowaniu używania list weryfikacji w instancji serwera chronionego zawiera Webmaster's Guide. |

Rozwiązywanie problemów związanych z przeglądarką

W przedstawionej poniżej tabeli można znaleźć informacje pomocne przy rozwiązywaniu niektórych najczęściej spotykanych problemów dotyczących przeglądarek, które mogą wystąpić podczas pracy z programem Menedżer certyfikatów cyfrowych (DCM).

| Problem | Możliwe rozwiązanie |
|--|---|
| W przeglądarce Microsoft Internet Explorer nie można wybrać innego certyfikatu, zanim nie zostanie uruchomiona nowa sesja przeglądarki. | Należy uruchomić nową sesję przeglądarki Internet Explorer. |
| Przeglądarka Internet Explorer nie wyświetla wszystkich możliwych certyfikatów klienta/użytkownika na liście wyboru. Internet Explorer wyświetla tylko certyfikaty wystawione przez zaufane ośrodki certyfikacji (CA) i zezwala na użycie tylko takich certyfikatów w chronionym systemie. | Ośrodek certyfikacji musi być zaufanym ośrodkiem w bazie kluczy, jak i w chronionej aplikacji. Należy sprawdzić, czy podczas wpisywania się do komputera PC z przeglądarką Internet Explorer podano tę samą nazwę użytkownika, co wpisana do certyfikatu w przeglądarce. Należy uzyskać inny certyfikat użytkownika z systemu, z którym ma być nawiązane połączenie. Administrator systemu powinien sprawdzić, czy baza certyfikatów (baza kluczy) wciąż ufa ośrodkowi certyfikacji (CA), który podpisał certyfikaty użytkownika i systemu. |
| Przeglądarka Internet Explorer 5 odbiera certyfikat ośrodka certyfikacji, ale nie może otworzyć pliku lub znaleźć dysku, na którym zapisano certyfikat. | Jest to nowa funkcja przeglądarki Internet Explorer dotycząca certyfikatów, które nie są jeszcze uznane za zaufane. Można wybrać lokalizację w komputerze PC. |
| Przeglądarka wyświetla ostrzeżenie, że nazwa systemu i certyfikat systemu nie są zgodne. | Niektóre przeglądarki różnie rozpoznają wielkie i małe litery w nazwach systemów. Należy wpisać adres URL takimi samymi literami, jakie zostały użyte w certyfikacie systemu. Można też utworzyć certyfikat systemu z pisownią nazwy systemu, która będzie zgodna z pisownią stosowaną przez większość użytkowników. Najlepszym rozwiązaniem jest pozostawienie nazwy serwera lub nazwy systemu bez zmian. Należy także sprawdzić, czy serwer nazw domen został prawidłowo skonfigurowany. |
| Po uruchomieniu przeglądarki Internet Explorer z protokołem HTTPS zamiast HTTP zostaje wyświetlone ostrzeżenie o pomieszaniu sesji chronionej i niechronionej. | Należy zaakceptować i zignorować to ostrzeżenie; w przyszłych wersjach przeglądarki Internet Explorer problem ten zostanie usunięty. |
| Netscape Communicator 4.04 for Windows przekształcił szesnastkowe wartości A1 i B1 na B2 i 9A w polskiej stronie kodowej. | Jest to błąd przeglądarki, który ma wpływ na obsługę NLS. Należy użyć innej przeglądarki lub nawet tej samej wersji przeglądarki, ale na innej platformie, na przykład Netscape Communicator 4.04 for AIX. |

| Problem | Możliwe rozwiązanie |
|--|---|
| W profilu użytkownika Netscape Communicator 4.04 poprawnie wyświetla wielkie znaki NLS w certyfikacie użytkownika, ale małe znaki wyświetla błędnie. | Niektóre znaki narodowe wpisane poprawnie jako jeden znak nie są później poprawnie wyświetlane. Na przykład w wersji przeglądarki Netscape Communicator 4.04 for Windows znaki szesnastkowe A1 i B1 w polskiej stronie kodowej są przekształcane na znaki B2 i 9A, co powoduje wyświetlanie innych znaków narodowych. |
| Przeglądarka wciąż informuje użytkownika, że ośrodek certyfikacji (CA) nie jest jeszcze oznaczony jako zaufany. | Należy użyć programu DCM do włączenia opcji Status ośrodka certyfikacji , aby oznaczyć ten ośrodek jako zaufany. |
| Przeglądarka Internet Explorer żąda odrzucenia połączenia HTTPS. | Jest to problem funkcjonowania przeglądarki lub jej konfiguracji. Przeglądarka odrzuca połączenie z serwisem używającym certyfikatu podpisanego przez ten sam system lub nieprawidłowego z innych powodów. |
| Przeglądarka i produkty serwera Netscape Communicator używają certyfikatów głównych z ośrodków publicznych, takich jak VeriSign i inne, jako funkcji umożliwiającej komunikację SSL — a w szczególności uwierzytelnianie. Wszystkie certyfikaty główne okresowo tracą ważność. Niektóre certyfikaty przeglądarki i serwera Netscape tracą ważność w okresie między 25 grudnia 1999 a 31 grudnia 1999. Jeśli nie usunie się tego problemu do 14 grudnia 1999, zostanie wyświetlony komunikat o błędzie. | Wcześniejsze wersje przeglądarki (Netscape Communicator 4.05 lub wcześniejsze) używały certyfikatów, które traciły ważność. Należy zaktualizować przeglądarkę do bieżącej wersji. Informacje o certyfikatach głównych przeglądarek można znaleźć w wielu serwisach, w tym http://home.netscape.com/security/ i http://www.verisign.com/server/cus/rootcert/webmaster.html . Bezpłatną przeglądarkę można pobrać z serwisu http://www.netcenter.com . |

Rozwiązywanie problemów związanych z serwerem HTTP Server for iSeries

W przedstawionej poniżej tabeli można znaleźć informacje pomocne przy rozwiązywaniu niektórych najczęściej spotykanych problemów związanych z serwerem HTTP Server for iSeries, które mogą wystąpić podczas pracy z programem Menedżer certyfikatów cyfrowych (DCM).

| Problem | Możliwe rozwiązanie |
|---|---|
| Protokół Hypertext Transfer Protocol Secure (HTTPS) nie działa. | Należy sprawdzić, czy serwer HTTP jest prawidłowo skonfigurowany do korzystania z protokołu SSL. W wersji V5R1 lub nowszej plik konfiguracyjny musi mieć wartość SSLAppName ustawioną za pomocą graficznego interfejsu użytkownika (GUI) serwera HTTP. Także port SSL, używany przez wirtualny host, powinien być skonfigurowany za pomocą wewnętrznej opcji SSLEnable tego hosta. Należy również zainstalować dwie Dyrektywy nasłuchiwanie określające dwa porty: jeden dla komunikacji SSL i drugi dla komunikacji bez stosowania protokołu SSL. Należy także sprawdzić, czy instancja serwera została utworzona i czy certyfikat serwera jest podpisany. |

| Problem | Możliwe rozwiązanie |
|---|---|
| <p>Proces rejestrowania instancji serwera HTTP Server jako aplikacji chronionej wymaga wyjaśnienia.</p> | <p>W systemie iSeriesSeries należy przejść do przeglądarkowego interfejsu serwera HTTP, aby wykonać czynności konfiguracyjne dla serwera HTTP. Najpierw, aby aktywować komunikację SSL należy zdefiniować wirtualny host. Można to wykonać na ekranie Zarządzanie kontekstami. Aby korzystać z portu SSL, zdefiniowanego wcześniej w Dyrektywie nasłuchiwania, musi zostać zdefiniowany wirtualny host. Następnie na ekranie Ogólne ustawienia SSL należy włączyć komunikację SSL dla wcześniej zdefiniowanego wirtualnego hosta. Wszystkie wprowadzone zmiany muszą zostać wpisane do pliku konfiguracyjnego. Podczas rejestrowania instancji serwera nie jest automatycznie wybierana instancja certyfikatu, który będzie używany przez ten serwer. Należy użyć programu DCM, aby przypisać określony certyfikat do aplikacji przed restartowaniem instancji serwera.</p> |
| <p>Problemy z konfigurowaniem serwera HTTP Server do używania list weryfikacji i opcjonalnego uwierzytelniania użytkowników.</p> | <p>Opis opcji konfigurowania instancji znajduje się w HTTP Server Webmaster's Guide. Informacje te dostępne są również w Centrum informacyjnym w temacie Usługi sieciowe.</p> |
| <p>Przeglądarka Netscape Communicator czeka na wygaśnięcie dyrektyw konfiguracyjnych w kodzie serwera HTTP, zanim umożliwi wybór innego certyfikatu.</p> | <p>Duże wartości certyfikatów utrudniają rejestrację drugiego certyfikatu, ponieważ przeglądarka wciąż używa pierwszego certyfikatu.</p> |
| <p>Nie można spowodować, aby przeglądarka przedstawiła serwerowi HTTP certyfikat X.509, co pozwoliłoby użyć tego certyfikatu jako danych wejściowych dla funkcji API QsyAddVldCertificate.</p> | <p>Należy użyć funkcji SSLEnable i SSLClientAuth ON, aby serwer HTTP Server załadował zmienną środowiskową HTTPS_CLIENT_CERTIFICATE. Informacje o tych funkcjach API znajdują się w temacie API OS/400. Można także przejrzeć funkcje API związane z listami weryfikacji lub certyfikatami:</p> <ul style="list-style-type: none"> • QsyListVldCertificates i QSYLSTVC • QsyRemoveVldCertificate i QRMVVC • QsyCheckVldCertificate i QSYCHKVC • QsyParseCertificate i QSYPARSC, itd. |
| <p>Nie można znaleźć pliku żądania tworzonoego w trakcie instalacji serwera HTTP Server. System używa tego pliku do wskazania poprawnych plików kluczy znalezionych w dyrektywie KEYFILE, w plikach konfiguracyjnych w swoim katalogu.</p> | <p>Więcej informacji zawiera sekcja Migracja z wcześniejszych wersji programu DCM. Dla serwera HTTP prawidłowy plik to /qibm/userdata/httpsvr/keyring/keymreq.crt. Dla protokołu LDAP prawidłowy plik to /qibm/userdata/os400/dirsrv/qdirsvr.crt .</p> |
| <p>Serwer HTTP powoduje przekroczenie czasu odpowiedzi w przypadku żądania listy certyfikatów z listy weryfikacji, na której znajduje się ponad 10 000 pozycji.</p> | <p>Należy utworzyć zadanie wsadowe, które wyszuka i usunie certyfikaty odpowiadające pewnym kryteriom, takie jak wszystkie wygasłe lub pochodzące z danego ośrodka CA.</p> |
| <p>Występuje problem z bazami certyfikatów po zainstalowaniu wersji V5R2 na wersji V4R3 i istnieje teraz plik /qibm/userdata/httpsvr/keyring/keymreq.crt lub /qibm/usedata/os400/dirsrv/qdirsvr.crt. System nie mógł zakończyć automatycznej migracji pliku kluczy do bazy kluczy.</p> | <p>Należy podać stare pliki kluczy jako bazę certyfikatów oraz znaleźć i usunąć nieprawidłowe certyfikaty z plików kluczy przed wywołaniem qicss/qyepmgrt w celu ponowienia próby migracji. Można też zignorować lub usunąć plik .crt, jeśli podczas migracji wszystkie istotne certyfikaty zostały przeniesione.</p> |
| <p>Serwer HTTP nie uruchamia się poprawnie z ustawioną wartością SSLEnable i w protokole zadania pojawia się komunikat o błędzie HTP8351. W protokole zadania serwera *ADMIN, gdy nie powiedzie się uruchomienie serwera HTTP, pojawia się błąd informujący, że Operacja inicjowania SSL nie powiodła się z kodem błędu 107.</p> | <p>Błąd 107 oznacza, że certyfikat wygasł. Jeśli instancja serwera to *ADMIN, wówczas tymczasowo należy podać wartość SSLDisable, aby można było użyć programu DCM w serwerze *ADMIN. Należy użyć programu DCM, aby przypisać aplikacji inny certyfikat, na przykład QIBM_HTTP_SERVER_ADMIN, jeśli instancją serwera jest serwer *ADMIN.</p> |

Błędy migracji i procedury odtwarzania

Błędy i odtwarzanie po błędach

Pojawienie się następujących plików wskazuje na ewentualne błędy podczas migracji:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT

Obecność tego pliku po pomyślnej instalacji obydwu opcji, 34 i 5722-DG1, oznacza, że migracja pliku kluczy wykonywana przez użyciu opcji 5722-DG1 nie powiodła się. Może wystąpić konieczność migracji bazy kluczy do bazy certyfikatów *SYSTEM.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

Obecność tego pliku po pomyślnej instalacji opcji 34 oznacza, że migracja pliku kluczy dla serwera LPAR nie powiodła się.

Poza powyższymi błędami możliwe jest pojawienie się błędów migracji, których system mógł nie zasygnalizować. Kiedy na przykład, system znajdzie pliki kluczy, które ma migrować do bazy certyfikatów *SYSTEM, może stwierdzić konflikty z plikami danych użytkownika istniejącymi w zintegrowanym systemie plików. W takim przypadku system nie może zakończyć migracji pliku kluczy, mimo że instalacja zakończyła się pomyślnie.

Niekiedy możliwe jest wykonanie migracji pliku kluczy z częściowo zakończonym przypisaniem certyfikatów systemu, zanim błąd uniemożliwi dokończenie migracji. Może to spowodować błędy, jeśli instancja *ADMIN serwera IBM HTTP Server została uruchomiona z parametrem SSLMODE o wartości ON. Możliwe są następujące przyczyny błędu:

- Plik kluczy poddawany migracji miał jako certyfikat domyślny ustawiony zły certyfikat systemu.
- Program DCM zakończył migrację w celu zachowania danych użytkownika istniejących w pliku o kluczowej nazwie.
- Wystąpił nieprzewidziany błąd w programie migracji.

Można uruchomić serwer IBM HTTP Server, tymczasowo nadając parametrowi SSLMODE wartość OFF dla instancji serwera *ADMIN przed jej uruchomieniem. Umożliwia to zbadanie baz certyfikatów za pomocą programu DCM i rozwiązanie problemu przed zakończeniem instancji *ADMIN. Po zakończeniu instancji *ADMIN można przywrócić parametrowi SSLMODE wartość ON i uruchomić instancję *ADMIN w celu prawidłowej inicjacji protokołu SSL.

Po migracji opcji 34 mogą wystąpić błędy podczas normalnych żądań DCM korzystających z baz certyfikatów. Są to błędy pojawiające się w przeglądarce. Oto ich przykłady:

Database error (Błąd bazy danych)
Database Read error (Błąd odczytu bazy danych)
Database Write error (Błąd zapisu bazy danych)
Database corruption (Uszkodzenie bazy danych)
Database table corrupted (Uszkodzenie tabeli bazy danych)

Ponadto, w systemie mógł znajdować się plik, niebędący prawidłową bazą danych, o nazwie default.kdb w tym samym katalogu co /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR lub /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. W takim przypadku konieczne jest ręczne wykonanie następującej migracji przed użyciem programu DCM do tworzenia nowych certyfikatów:

Uwaga: Jeśli migracja pliku kluczy nie jest konieczna, ponieważ ma być utworzony nowy ośrodek certyfikacji (CA) i nowy certyfikat systemu, należy pominąć poniższą procedurę ręcznej migracji.

- Jeśli planuje się instalowanie serwera HTTP Server for iSeries (5722-DG1), należy wykonać to w tym momencie, przed rozpoczęciem dalszych czynności.

Uwagi:

1. Program instalujący produkt 5769–SS1 opcja 34 nie podejmie ponownej próby migracji po zainstalowaniu opcji 34. Prosta reinstalacja opcji 34 nic nie da.
 2. Odpowiednie pliki znajdują się w katalogach USERDATA, utworzonych z uprawnieniem PUBLIC *EXCLUDE. Upewnij się, że masz do nich odpowiednie uprawnienia.
- Sprawdź, czy istnieją następujące pliki:
 - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
 - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

Jeśli istnieją, użyj komendy WRKLNK do zmiany ich nazwy i utworzenia plików zapasowych.

- Z profilu użytkownika posiadającego uprawnienia *ALLOBJ wywołaj z wiersza komend program QICSS/QYEPMGRT:
CALL QICSS/QYEPMGRT

Jeśli program zakończył się pomyślnie, upewnij się, że w systemie nie ma żadnego z poniższych plików:

- /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
- /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

Program DCM zwykle przechowuje zapasową kopię danych użytkownika zapisywanych w plikach o nazwach powodujących konflikt z nazwami używanymi przez program DCM. Jeśli następujące pliki nie istnieją:

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR

ale istnieją poniższe pliki:

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH

system próbuje zmienić ich nazwę, dodając rozszerzenie .OLD. Jeśli takie pliki również istnieją, system nie tworzy żadnych kopii zapasowych. Zamiast tego po prostu nadpisuje istniejące pliki .STH.

Inne uwagi

Jeśli kolejne próby utworzenia ośrodka certyfikacji (CA) i certyfikatu systemu kończą się niepowodzeniem ze względu na konflikty nazw plików, możesz mieć do czynienia z jedną z następujących sytuacji:

- **Konflikty nazw różnych plików.** Program DCM usiłuje chronić dane użytkownika w katalogach, które tworzy, nawet jeśli miałyby to uniemożliwić utworzenie potrzebnych plików. Rozwiązaniem może być skopiowanie wszystkich plików, których dotyczy konflikt nazw, do innego katalogu i, w miarę możliwości, użycie programu DCM do usunięcia odpowiednich plików. Jeśli nie można użyć do tego programu DCM, należy ręcznie usunąć te pliki z oryginalnego katalogu zintegrowanego systemu plików, gdzie powodowały one konflikt z programem DCM. Należy zanotować nazwy i miejsce docelowe przeniesionych plików. Kopie plików umożliwią odtworzenie ich, gdyby okazały się potrzebne. Po przeniesieniu następujących plików konieczne jest utworzenie nowego ośrodka certyfikacji (CA):

```
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH.OLD
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT
```

```
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT
```

Po przeniesieniu następujących plików należy utworzyć nową bazę certyfikatów *SYSTEM i nowy certyfikat systemu:

```
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN
/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP
```

- **Niespełnione warunki wstępne.** Upewnij się, że wymagane wstępnie programy licencjonowane (LPP) zostały prawidłowo zainstalowane.
- **Błąd programu.** Skontaktuj się z przedstawicielem serwisu.

Rozwiązywanie problemów związanych z przypisywaniem certyfikatów użytkowników

Podczas wykonywania zadania **Przypisanie certyfikatu użytkownika**, program Menedżer certyfikatów cyfrowych (DCM) przed zarejestrowaniem certyfikatu wyświetla informacje o certyfikacie w celu ich akceptacji. Jeśli program DCM nie może wyświetlić certyfikatu, przyczyną problemu może być jedna z poniższych sytuacji:

1. Przeglądarka nie zażądała wyboru certyfikatu do przedstawienia serwerowi. Może się to zdarzyć, jeśli przeglądarka przechowała w pamięci podręcznej poprzedni certyfikat (przy dostępie do innego serwera). Spróbuj opróżnić pamięć podręczną przeglądarki i ponów czynność. Przeglądarka powinna teraz zażądać wyboru certyfikatu.
2. Certyfikat, który chcesz zarejestrować, jest już zarejestrowany w DCM.
3. Ośrodek certyfikacji, który wystawił certyfikat, nie jest uznawany przez system za użytkownika zaufanego. Dlatego przedstawiany certyfikat jest nieważny. Dowiedz się od administratora systemu, czy twój certyfikat został wystawiony przez właściwy ośrodek certyfikacji (CA). Jeśli ośrodek jest właściwy, administrator systemu powinien użyć zadania **Import**, aby zaimportować certyfikat ośrodka do bazy certyfikatów *SYSTEM. W celu rozwiązania problemu, administrator może również użyć zadania **Praca z certyfikatami ośrodków certyfikacji**, aby uznać ośrodek za zaufanego użytkownika systemu.
4. Nie musisz rejestrować certyfikatu. Sprawdź certyfikaty użytkownika w swojej przeglądarce, żeby przekonać się, czy jest to przyczyną problemu.
5. Certyfikat, który próbujesz zarejestrować, jest przeterminowany lub niepełny. W celu rozwiązania problemu musisz albo odnowić certyfikat, albo skontaktować się z ośrodkiem certyfikacji (CA), który wystawił certyfikat.
6. IBM HTTP Server for iSeries nie jest prawidłowo skonfigurowany do zarejestrowania certyfikatu za pomocą SSL i uwierzytelniania klienta w bezpiecznej instancji serwera *ADMIN. Jeśli żadna z powyższych wskazówek nie rozwiązuje błędu, skontaktuj się z administratorem i poinformuj o błędzie.

Aby użyć zadania **Przypisanie certyfikatu użytkownika**, należy połączyć się z programem Menedżer certyfikatów cyfrowych (DCM) poprzez sesję SSL. Jeśli sesja SSL nie zostanie użyta podczas wykonywania zadania **Przypisanie certyfikatu użytkownika**, program DCM wyświetli komunikat, że użycie SSL jest konieczne. W oknie komunikatu znajduje się przycisk, za pomocą którego można połączyć się z DCM poprzez SSL. Jeśli w oknie komunikatu nie ma takiego przycisku, poinformuj o tym administratora systemu. Może być konieczne ponowne uruchomienie serwera WWW w celu uaktywnienia dyrektyw konfiguracyjnych dotyczących użycia SSL.

Rozdział 10. Informacje pokrewne tematowi DCM

W miarę upowszechniania się stosowania certyfikatów cyfrowych dostępnych będzie również więcej źródeł informacji na ten temat. Poniżej przedstawiono niewielką listę innych zasobów, dzięki którym można pogłębić swoje wiadomości o certyfikatach cyfrowych i ich zastosowaniu do rozszerzenia strategii ochrony systemu iSeries:

- **Serwis WWW VeriSign Help Desk** 
Zawiera on bogatą bibliotekę publikacji poświęconych certyfikatom cyfrowym, a także innym zagadnieniom związanym z bezpieczeństwem w Internecie.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements**
SG24-6168 
W dokumentacji IBM opisano rozszerzenia wprowadzone w wersji V5R1 dotyczące ochrony sieci. W dokumentacji tej wyjaśniono m.in., jak podpisywać obiekty iSeries, używać Menedżera certyfikatów cyfrowych (DCM) oraz koprocatora szyfrującego 4758 dla sesji SSL.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)** 
W dokumentacji tej opisano możliwe zastosowania certyfikatów cyfrowych na serwerze iSeries. Wyjaśniono w niej także, jak skonfigurować różne serwery i klientów do korzystania z certyfikatów cyfrowych. Ponadto zaprezentowano w niej informacje o zastosowaniu funkcji API systemu OS/400 do zarządzania i wykorzystania certyfikatów cyfrowych w aplikacjach użytkownika.
- **Wyszukiwarka RFC Index Search** 
Wyszukiwarka ta umożliwi przeszukiwanie repozytorium dokumentów Request for Comments (RFC). Dokumenty RFC opisują standardy protokołów internetowych, takich jak SSL, PKIX, i innych, związanych z zastosowaniami certyfikatów cyfrowych.

IBM