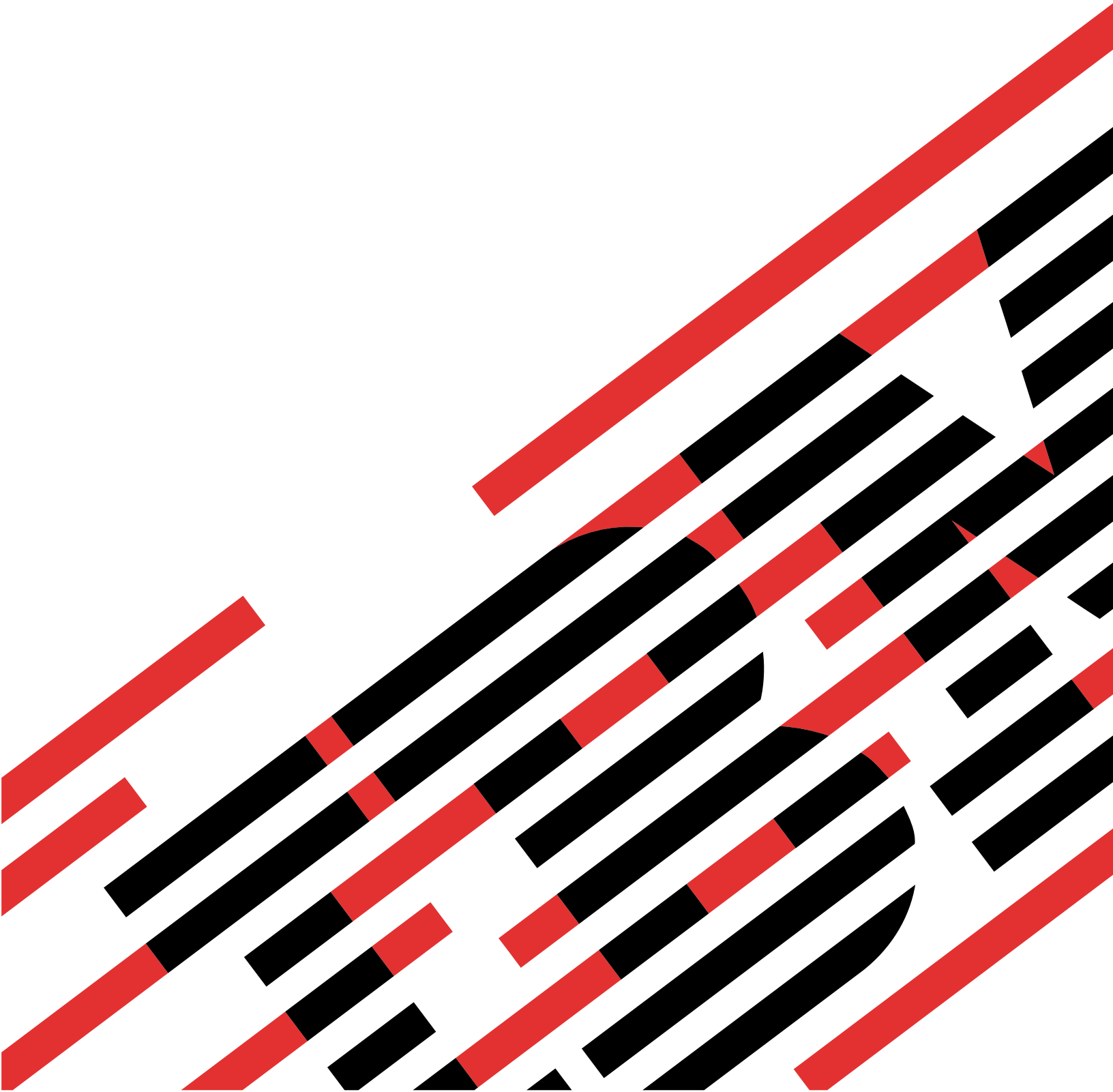
IBM

eserver

iSeries

Podpisywanie obiektów i weryfikacja podpisów



IBM

@server

iSeries

Podpisywanie obiektów i weryfikacja podpisów

Spis treści

Podpisywanie obiektów i weryfikacja podpisów

Podpisywanie obiektów i weryfikacja podpisów stanowią elementy ochrony systemu i służą sprawdzeniu integralności różnorodnych obiektów serwera iSeries. Klucz prywatny certyfikatu cyfrowego służy do podpisania obiektu, zaś certyfikat (zawierający odpowiadający mu klucz publiczny) do weryfikowania podpisu cyfrowego. Podpis cyfrowy zapewnia integralność czasu i zawartości podpisywanego obiektu. Podpis jest niezaprzeczalnym dowodem autentyczności i autoryzacji. Można go użyć do sprawdzenia pochodzenia i do wykrycia fałszerstwa. Podpisując obiekt identyfikuje się jego źródło i zapewnia możliwość wykrycia zmian w tym obiekcie. Podczas weryfikowania podpisu obiektu można określić, czy od czasu podpisania zawartość obiektu uległa zmianie. Można także zweryfikować źródło podpisu, aby upewnić się co do pochodzenia obiektu.

W serwerze iSeries do podpisywania obiektów i weryfikacji podpisów służą:

- funkcje API do programowego podpisywania obiektów i weryfikowania podpisów,
- program Menedżer certyfikatów cyfrowych do podpisywania obiektów i do przeglądania i weryfikowania podpisów na obiektach,
- Centrum Zarządzania programu iSeries Navigator do podpisywania obiektów wchodzących w skład pakietów rozpowszechnianych do innych systemów,
- komendy CL, takie jak Sprawdzanie integralności obiektu (Check Object Integrity - CHKOBJITG), do weryfikowania podpisów.

Więcej o metodach podpisywania obiektów i o ich wpływie na udoskonalenie strategii ochrony można przeczytać w artykułach:

Co nowego w wersji V5R2
Informacje zawarte w tym artykule pomogą poznać możliwości związane z podpisywaniem obiektów i weryfikowaniem podpisów na serwerze iSeries, a także zmiany wprowadzone w dokumentacji dla tej wersji.

Drukowanie tego dokumentu
Informacje zawarte w tym artykule pomogą w wydrukowaniu całego dokumentu z pliku w formacie PDF.

Scenariusze podpisywania obiektów
Artykuł zawiera scenariusze przedstawiające niektóre sytuacje związane z wykorzystaniem podpisywania obiektów i weryfikowania podpisów na serwerze iSeries. Każdy scenariusz prezentuje także zadania konfigurowania, które należy wykonać, aby go zaimplementować.

Koncepcje związane z podpisywaniem obiektów
Artykuł przedstawia koncepcje i informacje związane z podpisami cyfrowymi, podpisywaniem obiektów i metodą weryfikowania podpisów.

Wymagania wstępne dla podpisywania obiektów i weryfikowania podpisów
Artykuł przedstawia wymagania wstępne i inne założenia związane z podpisywaniem obiektów i weryfikowaniem podpisów.

Zarządzanie podpisanymi obiektami
Artykuł przedstawia komendy serwera iSeries i wartości systemowe używane do przetwarzania podpisanych obiektów, a także wpływ podpisanych obiektów na procesy składowania i odtwarzania.

Rozwiązywanie problemów związanych z podpisywaniem obiektów i weryfikowaniem podpisów
Artykuł przedstawia dane, które pomogą rozwiązywać problemy i usuwać błędy, które mogą wystąpić przy podpisywaniu obiektów i weryfikowaniu podpisów.

Informacje związane z podpisywaniem obiektów i weryfikowaniem podpisów
Artykuł przedstawia odsyłacze do innych zasobów zawierających informacje na temat podpisywania obiektów i weryfikowania podpisów.

Co nowego w wersji V5R2

Możliwości podpisywania obiektów i weryfikowania podpisów na serwerze iSeries zostały wprowadzone po raz pierwszy w wersji V5R1. W wersji V5R2 pojawiły się nowe funkcje i udoskonalenia.

Poniżej przedstawione zostały nowe lub rozszerzone funkcje podpisywania obiektów i weryfikowania podpisów:

- **Funkcja podpisywania obiektów w Centrum Zarządzania programu iSeries Navigator**
  Obecnie kreator definicji produktu w Centrum Zarządzania umożliwia podpisywanie obiektów rozsyłanych do systemów końcowych iSeries.
- **Podpisywanie obiektów typu komenda (*CMD)**
  Można teraz podpisywać całe obiekty typu komenda (*CMD) lub tylko ich rdzenne elementy.
- **Nowe funkcje API związane z podpisywaniem i weryfikowaniem**
  Wprowadzone zostały trzy nowe funkcje API, pozwalające z poziomu programu korzystać z rozszerzonych możliwości podpisywania i weryfikowania w systemie OS/400:
  - Funkcja API Sign Buffer (QYDOSGNB, QydoSignBuffer)
    Funkcja API umożliwia systemowi lokalnemu cyfrowe podpisanie bufora, certyfikując tym samym, że jest on pewny. Po podpisaniu bufora system zwraca podpis cyfrowy do programu wywołującego funkcję API. Można na przykład, korzystając z tej funkcji API, podpisać część pliku XML i zachować podpis w innej części tego pliku. Można także odczytać rekordy zbioru bazy danych, umieścić je w buforze i użyć funkcji API do jego podpisania.
  - Funkcja API Verify Buffer (QYDOVFYB, QydoVerifyBuffer)
    Funkcja API umożliwia systemowi lokalnemu zweryfikowanie podpisu cyfrowego uprzednio podpisanego bufora.
  - Funkcja API Add Verifier (QYDOADDV, QydoAddVerifier)
    Funkcja API dodaje certyfikat do bazy certyfikatów *SIGNATUREVERIFICATION systemu. Następnie system może wykorzystać dodane certyfikaty do weryfikowania podpisów utworzonych za pomocą tych certyfikatów. Weryfikowanie podpisu umożliwia sprawdzenie integralności podpisanych obiektów i daje pewność, że nie zostały one zmienione od czasu podpisania. Jeśli baza certyfikatów nie istnieje, funkcja API tworzy ją dodając certyfikat.

    Uwaga: Ze względów bezpieczeństwa ta funkcja API nie pozwoli na dodanie do bazy certyfikatów *SIGNATUREVERIFICATION certyfikatu ośrodka certyfikacji. W momencie dodawania certyfikatu ośrodka certyfikacji do bazy certyfikatów system zakłada, że ośrodek CA jest zaufanym źródłem certyfikatów. W konsekwencji system traktuje certyfikat wystawiony przez ośrodek CA jako pochodzący z zaufanego źródła. Dlatego nie można korzystać z funkcji API w celu utworzenia programu instalacyjnego obsługi wyjścia w celu dodania certyfikatu ośrodka certyfikacji do bazy certyfikatów. Aby dodać certyfikat ośrodka CA do bazy certyfikatów, należy użyć programu Menedżer certyfikatów cyfrowych; takie rozwiązanie daje pewność, że sprawowana jest ręczna, dokładna kontrola nad ośrodkami CA, którym system ufa. Dzięki temu system nie może importować certyfikatów ze źródeł, których administrator świadomie nie określił jako zaufane.

    Jeśli nie chcesz, aby ktokolwiek mógł dodać certyfikat do bazy certyfikatów *SIGNATUREVERIFICATION korzystając z tej funkcji API, zablokuj tę funkcję w systemie. Można to zrobić korzystając z systemowych narzędzi serwisowych (SST) umożliwiających ustawienie odrzucania zmian wprowadzonych w wartościach systemowych związanych z ochroną.

W poprzedniej wersji dokumentacji informacje o możliwościach podpisywania obiektów i weryfikowania podpisów serwera iSeries udostępniono jako część artykułu Centrum informacyjnego Zarządzanie certyfikatami cyfrowymi. Obecnie pojawiły się nowe metody podpisywania obiektów i weryfikowania podpisów, które opisano w tym samym artykule, co stanowi duże udogodnienie dzięki dostarczeniu scentralizowanej informacji o używaniu tych metod. Artykuł ten zawiera rozszerzone i dokładniejsze informacje, takie jak scenariusze, pomagające określić, gdzie i jak stosować te metody, uzupełniając strategię ochrony.

Nowe lub rozszerzone informacje w tym artykule to:

- scenariusze, które pomagają określić, jak najlepiej zastosować możliwości podpisywania obiektów i weryfikowania podpisów do uzupełnienia strategii ochrony,
- nowe sekcje opisujące komendy i wartości systemowe używane do zarządzania w systemie podpisanymi obiektami,
- nowe sekcje opisujące planowanie i inne informacje związane z koncepcją podpisywania obiektów i weryfikowania podpisów.

Więcej informacji o nowościach i zmianach w tej wersji zawiera artykuł Informacje dla użytkowników .

Drukowanie

Aby przejrzeć lub pobrać wersję PDF, wybierz Podpisywanie obiektów i weryfikowanie podpisów (350 kB lub 44 strony).

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

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

Program Adobe Acrobat Reader, potrzebny do przeglądania i drukowania tych plików, można pobrać z serwisu WWW firmy Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Scenariusze podpisywania obiektów

Serwer iSeries udostępnia kilka różnych metod podpisywania obiektów i weryfikowania podpisów na obiektach. Sposób podpisywania obiektów i przetwarzanie podpisanych obiektów zależy od wymagań i celów związanych z firmą i realizowaną strategią ochrony. Czasami potrzeba tylko zweryfikować podpis na obiekcie, aby upewnić się, że nie została naruszona integralność obiektu. Kiedy indziej zaś podpisać obiekty wysyłane do innych użytkowników lub systemów. Podpisanie obiektów umożliwia innym określenie pochodzenia obiektów i sprawdzenie ich integralności.

Wybór metody zależy od wielu czynników. Przedstawione w tym artykule scenariusze opisują niektóre z podstawowych celów podpisywania obiektów i weryfikowania podpisów realizowanych w typowej firmie. Każdy scenariusz opisuje także wymagania wstępne i zadania, które trzeba wykonać, aby go zaimplementować zgodnie z opisem. Aby określić, jak korzystać z możliwości podpisywania obiektów serwera iSeries dopasowując je do wymagań firmy i realizowanej strategii ochrony, należy przejrzeć poniższe scenariusze.

Scenariusz: korzystanie z Menedżera certyfikatów cyfrowych do podpisywania obiektów i weryfikowania podpisów

Scenariusz przedstawia przedsiębiorstwo, które chce podpisywać aplikacje dostępne na ich publicznym serwerze WWW, aby łatwo określić, czy zostały w nich wprowadzone nieuprawnione zmiany. Scenariusz opisuje także wykorzystanie programu Menedżer certyfikatów cyfrowych jako podstawowej metody podpisywania obiektów i weryfikowania podpisów obiektów, uwzględnia też potrzeby przedsiębiorstwa i jego strategię ochrony.

Scenariusz: korzystanie z funkcji API do podpisywania obiektów i weryfikowania podpisów
Scenariusz przedstawia przedsiębiorstwo projektujące aplikacje, które chce sprzedawane przez siebie aplikacje podpisywać programowo, aby klienci podczas instalacji byli pewni, że aplikacje pochodzą od producenta i aby mieli możliwość wykrycia w nich zmian wprowadzonych przez osoby bez uprawnień. Scenariusz opisuje także wykorzystanie funkcji API Sign Object i Add Verifier do podpisywania obiektów i weryfikowania podpisów, uwzględnia też potrzeby przedsiębiorstwa i jego strategię ochrony.

Scenariusz: korzystanie z Centrum Zarządzania do podpisywania obiektów
Scenariusz przedstawia przedsiębiorstwo, które chce podpisywać pakiety tworzone i rozpowszechniane do wielu serwerów iSeries. Scenariusz opisuje także wykorzystanie funkcji Centrum Zarządzania programu iSeries Navigator do tworzenia i podpisywania pakietów, które następnie będą rozpowszechniane do innych serwerów iSeries, uwzględnia też potrzeby przedsiębiorstwa i jego strategię ochrony.

Scenariusz: korzystanie z programu DCM do podpisywania obiektów i weryfikowania podpisów

Opis sytuacji

Jako administrator serwerów iSeries przedsiębiorstwa MojaFirma jesteś odpowiedzialny za zarządzanie dwoma serwerami iSeries. Jeden z serwerów iSeries jest firmowym, publicznym serwerem WWW. Zawartość tego serwera jest tworzona na wewnętrznym, produkcyjnym serwerze iSeries a pliki oraz obiekty programów po przetestowaniu są przenoszone na publiczny serwer WWW.

Publiczny serwer WWW przedsiębiorstwa zawiera serwis WWW z ogólnymi informacjami o przedsiębiorstwie. Znajdują się tam też formularze, które klienci wypełniają podczas rejestrowania produktów, żądania informacji o produkcie, zawiadomienia o aktualizacji produktu, informacje o miejscach dystrybucji produktu itp. Jeśli znasz problem słabych punktów zabezpieczeń programów cgi-bin, które obsługują te formularze, wiesz, że mogą one zostać zmodyfikowane. Dlatego należy stworzyć możliwość sprawdzania integralności tych programów i wykrywania zmian wprowadzonych przez nieuprawnione osoby. Aby osiągnąć ten cel ochrony, wystarczy podpisać cyfrowo te obiekty.

Przegląd możliwości podpisywania obiektów systemu OS/400 pokazuje, że jest kilka metod, z których można skorzystać do podpisywania obiektów i weryfikowania podpisów obiektów. Z uwagi na niewielką liczbę zarządzanych serwerów iSeries i nikłą potrzebę podpisywania obiektów możesz decydować się na skorzystanie z programu Menedżer certyfikatów cyfrowych (DCM). Ponadto chcesz utworzyć lokalny ośrodek CA i do podpisywania obiektów używać certyfikatów prywatnych. Wykorzystanie certyfikatów prywatnych, wydawanych przez lokalny ośrodek CA, ogranicza wydatki związane z używaniem tej technologii ochrony, gdyż nie trzeba kupować certyfikatu od ogólnie znanego ośrodka CA.

Przykład ten jest praktycznym wprowadzeniem do konfigurowania i korzystania z podpisywania obiektów dla małej liczby serwerów iSeries.

Zalety scenariusza

Scenariusz ten ma następujące zalety:

- Podpisywanie obiektów umożliwia sprawdzanie integralności obiektów narażonych na atak i łatwe określenie, czy zostały one zmienione od czasu podpisania. Pozwala zmniejszyć nakłady na przyszłe rozwiązywanie i śledzenie problemów w aplikacji lub w systemie.
- Wykorzystanie do podpisywania obiektów i weryfikowania podpisów obiektów graficznego interfejsu użytkownika programu DCM umożliwia szybkie i łatwe wykonywanie tych zadań.
- Program DCM zastosowany do podpisywania obiektów i weryfikowania podpisów obiektów pozwala zredukować czas przeznaczony na zrozumienie i wykorzystanie podpisywania obiektów jako części strategii ochrony.
- Wykorzystanie do podpisywania obiektów certyfikatu wystawionego przez prywatny ośrodek certyfikacji obniża koszty wprowadzenia podpisywania obiektów.

Cele

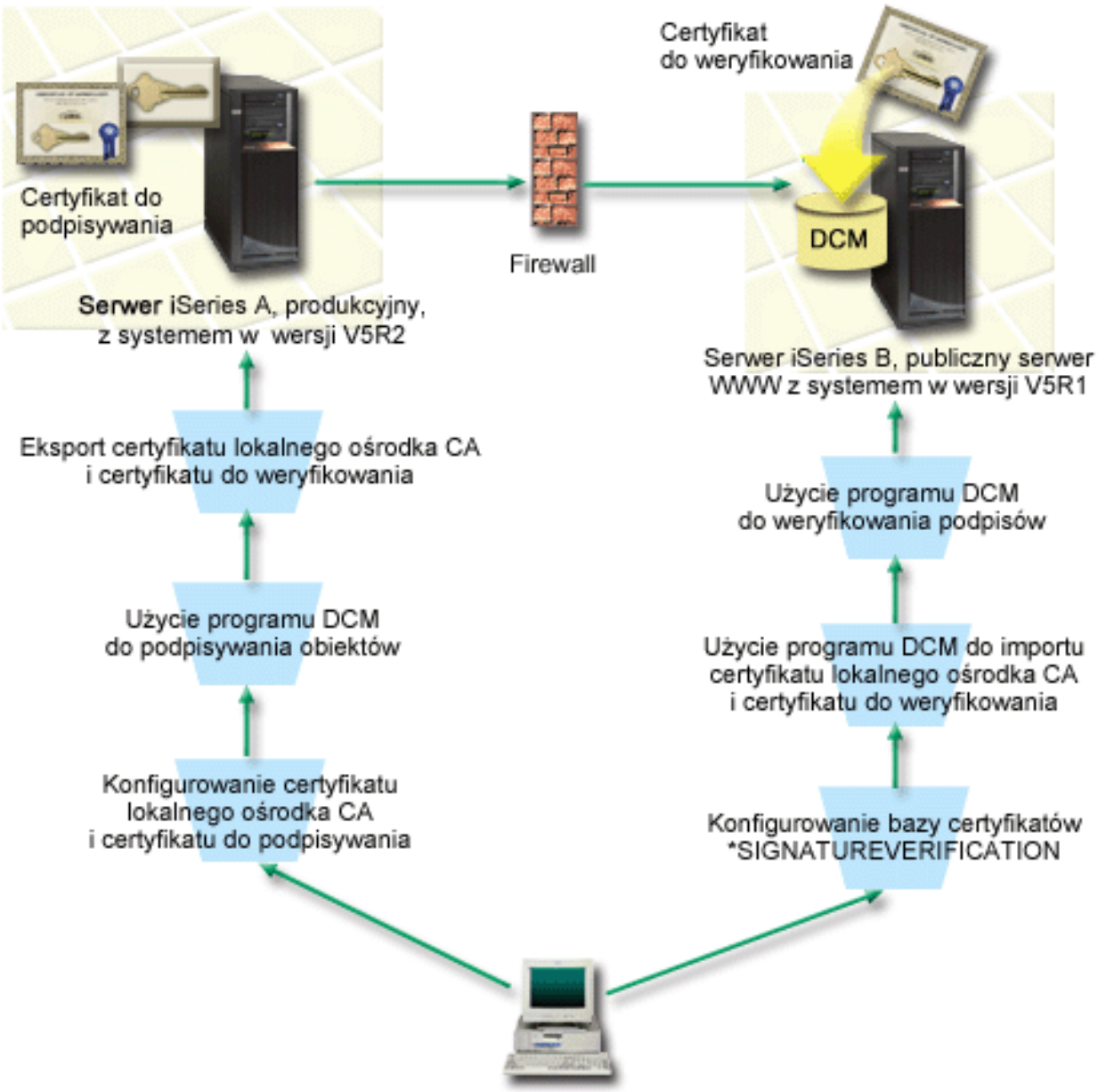
W scenariuszu zakładamy, że chcesz cyfrowo podpisywać narażone na atak obiekty, takie jak generujące formularze programy cgi-bin, znajdujące się na publicznym serwerze iSeries przedsiębiorstwa. Jako administrator systemu przedsiębiorstwa MojaFirma chcesz do podpisywania tych obiektów i do weryfikowania ich podpisów użyć programu Menedżer certyfikatów cyfrowych (DCM).

Główne założenia scenariusza są następujące:

- Aplikacje przedsiębiorstwa i inne narażone na atak obiekty, które znajdują się na dostępnym publicznie serwerze WWW (iSeries B) muszą być podpisane certyfikatem pochodzącym z lokalnego ośrodka CA, aby ograniczyć koszty podpisywania aplikacji.
- Administratorzy systemu i inni wyznaczeni użytkownicy muszą mieć możliwość prostego weryfikowania podpisów cyfrowych na serwerze iSeries, pozwalającego sprawdzić źródło i autentyczność obiektów podpisanych przez przedsiębiorstwo. Aby osiągnąć postawiony cel, każdy serwer iSeries musi mieć w bazie certyfikatów *SIGNATUREVERIFICATION zarówno kopię certyfikatu przedsiębiorstwa do weryfikowania podpisów, jak i certyfikat lokalnego ośrodka CA.
- Dzięki weryfikowaniu podpisów na aplikacjach przedsiębiorstwa oraz na innych obiektach, administratorzy serwera iSeries i inni użytkownicy mogą wykryć, czy zawartość obiektu została zmieniona od czasu jego podpisania.
- Administrator systemu musi korzystać z programu DCM do podpisywania obiektów, ponadto zarówno administrator systemu, jak i inni użytkownicy, powinni korzystać z programu DCM do weryfikowania podpisów obiektów.

Szczegóły

Poniższy rysunek przedstawia proces podpisywania obiektu i weryfikowania podpisu według scenariusza:



Rysunek ilustruje następujące punkty scenariusza:

Serwer **iSeries A**

- serwer iSeries A z systemem OS/400 w wersji 5 wydanie 2 (V5R2),
- serwer iSeries A to wewnętrzny serwer produkcyjny przedsiębiorstwa i platforma do opracowywania programów dla publicznego serwera WWW (serwer iSeries B),
- na serwerze iSeries A jest zainstalowany program Cryptographic Access Provider 128-bit for iSeries (5722–AC3),
- na serwerze iSeries A musi być zainstalowany i skonfigurowany program Menedżer certyfikatów cyfrowych (opcja 34 systemu OS/400) i serwer IBM HTTP (5722–DG1),
- serwer iSeries A funkcjonuje jako lokalny ośrodek CA i w tym systemie znajdują się certyfikaty podpisujące obiekty,

- serwer iSeries A za pomocą programu DCM podpisuje obiekty i jest podstawowym systemem podpisującym obiekty dla publicznych aplikacji i innych obiektów przedsiębiorstwa,
- serwer iSeries A został skonfigurowany tak, aby umożliwiał weryfikowanie podpisów.

Serwer **iSeries B**

- serwer iSeries B z systemem OS/400 w wersji 5 wydanie 1 (V5R1),
- serwer iSeries B jest zewnętrznym, publicznym serwerem WWW, znajdującym się poza siecią przedsiębiorstwa chronioną przez firewall,
- na serwerze iSeries B jest zainstalowany program Cryptographic Access Provider 128-bit (5722–AC3),
- na serwerze iSeries B musi być zainstalowany program Menedżer certyfikatów cyfrowych (opcja 34 systemu OS/400) i serwer IBM HTTP (5722–DG1),
- serwer iSeries B nie jest ani lokalnym ośrodkiem CA, ani nie podpisuje obiektów,
- serwer iSeries B ma włączone weryfikowanie podpisów przy użyciu programu DCM tworzącego bazę certyfikatów *SIGNATUREVERIFICATION i importującego niezbędne certyfikaty: weryfikacji i lokalnego ośrodka CA,
- program DCM używany jest do weryfikowania podpisów na obiektach.

Założenia i wymagania wstępne

Scenariusz zależy od spełnienia następujących założeń i wymagań wstępnych:

1. Wszystkie serwery iSeries spełniają wymagania konieczne do zainstalowania programu Menedżer certyfikatów cyfrowych (DCM).
2. Na żadnym z serwerów iSeries nie był wcześniej konfigurowany ani używany program DCM.
3. Wszystkie serwery iSeries mają zainstalowaną najnowszą wersję programu licencjonowanego Cryptographic Access Provider 128-bit (5722-AC3).
4. Ustawienie domyślne wartości systemowej Weryfikowanie podpisów obiektów podczas odtwarzania (QVFYOBJRST) w całym scenariuszu serwera iSeries wynosi 3 i pozostaje niezmienione. Ustawienie domyślne daje gwarancje, że serwer będzie mógł zweryfikować podpisy po odtworzeniu podpisanych obiektów.
5. Aby administrator systemu serwera iSeries A mógł podpisywać obiekty, musi mieć uprawnienia specjalne *ALLOBJ albo jego profil użytkownika musi być uprawniony do korzystania z aplikacji podpisującej obiekty.
6. Administrator systemu lub inna osoba, która tworzy bazę certyfikatów w programie DCM, musi mieć uprawnienia specjalne *SECADM i *ALLOBJ.
7. Administrator systemu lub inni użytkownicy pozostałych serwerów iSeries do weryfikowania podpisu obiektu muszą mieć uprawnienie specjalne *AUDIT.

Kolejne zadania

Poniżej przedstawiono dwa zestawy zadań, które należy wykonać, aby zaimplementować ten scenariusz. Jeden zestaw zadań pozwala skonfigurować serwer iSeries A jako lokalny ośrodek CA i podpisywać oraz weryfikować podpisy obiektów. Drugi zestaw zadań pozwala skonfigurować serwer iSeries B do weryfikowania utworzonych przez serwer iSeries A podpisów obiektów.

Zadania do wykonania na serwerze **iSeries A**

Aby zgodnie ze scenariuszem serwer iSeries A stał się lokalnym ośrodkiem CA i mógł podpisywać obiekty oraz weryfikować podpisy obiektów, należy:

1. Zrealizować wszystkie wymagania wstępne konieczne do zainstalowania wszystkich potrzebnych produktów serwera iSeries.

2. Korzystając z programu Menedżer certyfikatów cyfrowych utworzyć lokalny ośrodek CA do wystawiania certyfikatu podpisującego obiekt.
3. Użyć programu DCM do utworzenia definicji aplikacji.
4. Użyć programu DCM do przypisania certyfikatu do definicji aplikacji podpisującej obiekty.
5. Użyć programu DCM do podpisania programów cgi-bin.
6. Użyć programu DCM do eksportu certyfikatów, których inne systemy będą musiały użyć do weryfikowania podpisów obiektów. Konieczne jest wyeksportowanie do pliku zarówno kopii certyfikatu lokalnego ośrodka CA, jak i kopii certyfikatu do podpisywania obiektów, jako certyfikatu do weryfikowania podpisów.
7. Przesłać pliki certyfikatów do publicznego serwera iSeries przedsiębiorstwa (iSeries B), aby można było weryfikować podpisy tworzone przez serwer iSeries A.

Zadania do wykonania na serwerze **iSeries B**

Jeśli planujesz odtwarzanie podpisanych obiektów przesłanych do publicznego serwera WWW (iSeries B), to przed przesłaniem podpisanych obiektów wykonaj następujące zadania konfigurowania weryfikacji podpisu na serwerze iSeries B. Konfigurowanie weryfikacji podpisu należy zakończyć przed rozpoczęciem weryfikowania na publicznym serwerze WWW podpisów odtworzonych podpisanych obiektów.

Na serwerze iSeries B, aby zgodnie ze scenariuszem weryfikować podpisy, należy wykonać następujące czynności:

8. Korzystając z programu Menedżer certyfikatów cyfrowych utworzyć bazę certyfikatów *SIGNATUREVERIFICATION.
9. Użyć programu DCM do importu certyfikatu lokalnego ośrodka CA i certyfikatu do weryfikowania podpisu.
10. Użyć programu DCM do weryfikowania podpisów na przesłanych obiektach.

Szczegóły konfigurowania

Aby zgodnie ze scenariuszem podpisać obiekty, należy wykonać następujące czynności związane z konfigurowaniem i użyciem programu Menedżer certyfikatów cyfrowych.

Krok 1: wypełnienie wszystkich wymagań wstępnych

Przed wykonaniem dalszych czynności konfiguracyjnych związanych z implementacją tego scenariusza, należy wypełnić wszystkie wymagania wstępne konieczne do zainstalowania i skonfigurowania wszystkich potrzebnych produktów serwera iSeries.

Krok 2: tworzenie lokalnego ośrodka CA do wystawiania prywatnych certyfikatów podpisujących obiekty

Podczas tworzenia lokalnego ośrodka CA za pomocą programu Menedżer certyfikatów cyfrowych należy wypełnić szereg formularzy. Formularze te prowadzą przez proces tworzenia ośrodka CA i inne czynności niezbędne, aby rozpocząć korzystanie z certyfikatów cyfrowych w połączeniu z protokołem SSL, czyli podpisywanie obiektów i weryfikowanie podpisów. Wprawdzie w tym scenariuszu nie trzeba konfigurować certyfikatów w połączeniu z protokołem SSL, ale w celu skonfigurowania systemu do podpisywania obiektów należy wypełnić wszystkie formularze.

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

1. Uruchom program DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić 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. Wypełnij wszystkie formularze zadań. Po zakończeniu tego zadania, wykonaj poniższe czynności:
   a. Wprowadź informacje identyfikujące lokalny ośrodek CA.
   b. Zainstaluj certyfikat lokalnego ośrodka CA w swojej przeglądarce, aby oprogramowanie mogło go rozpoznać i sprawdzać poprawność certyfikatów wystawionych przez ten ośrodek.
   c. Zdefiniuj strategię lokalnego ośrodka CA.
   d. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu klienta lub serwera, z którego aplikacja będzie mogła skorzystać do połączeń z użyciem protokołu SSL.

      Uwaga: Wprawdzie opisywany scenariusz nie korzysta z tego certyfikatu, jego utworzenie jest jednak niezbędne przed użyciem lokalnego ośrodka CA do wystawienia potrzebnego certyfikatu podpisującego obiekt. Jeśli zadanie zostanie anulowane bez utworzenia certyfikatu, to należy utworzyć certyfikat podpisujący obiekt i bazę certyfikatów *OBJECTSIGNING, w której będzie on przechowywany.
   e. Wybierz aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL.

      Uwaga: Na potrzeby tego scenariusza nie wybieraj żadnej aplikacji, tylko kliknij **Kontynuuj**, aby wyświetlić następny formularz.
   f. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu podpisującego obiekt, z którego aplikacja będzie mogła skorzystać do cyfrowego podpisywania obiektów. W tym podzadaniu tworzona jest baza certyfikatów *OBJECTSIGNING. Jest to baza umożliwiająca zarządzanie certyfikatami do podpisywania obiektów.
   g. Wybierz aplikacje, które powinny ufać lokalnemu ośrodkowi CA.

      Uwaga: Na potrzeby tego scenariusza nie wybieraj żadnej aplikacji, tylko kliknij **Kontynuuj**, aby zakończyć zadanie.

Po utworzeniu lokalnego ośrodka CA i certyfikatu podpisującego obiekt, a przed podpisywaniem obiektów, należy zdefiniować korzystającą z certyfikatu aplikację podpisującą obiekty.

Krok 3: tworzenie definicji aplikacji podpisującej obiekty

Po utworzeniu certyfikatu podpisującego obiekt należy za pomocą programu Menedżer certyfikatów cyfrowych utworzyć definicję aplikacji podpisującej obiekty, która będzie używana do podpisywania obiektów. Definicja aplikacji nie musi odnosić się do istniejącej aplikacji, tworzona definicja aplikacji powinna opisywać rodzaj lub grupę obiektów, które zamierzasz podpisywać. Definicja jest niezbędna, żeby można było powiązać identyfikator aplikacji z certyfikatem i umożliwić proces podpisywania.

Aby utworzyć definicję aplikacji podpisującej obiekty za pomocą programu DCM, wykonaj następujące czynności:

1. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
2. Gdy pojawi się strona Baza certyfikatów i hasło, wpisz hasło bazy certyfikatów (określone przy tworzeniu tej bazy) i kliknij **Kontynuuj**.
3. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Dodaj aplikację**, aby wyświetlić formularz definiowania aplikacji.
5. Wypełnij formularz i kliknij **Dodaj**.

Należy teraz przypisać certyfikat podpisujący obiekt do utworzonej aplikacji.

Krok 4: przypisywanie certyfikatu do definicji aplikacji podpisującej obiekty

Aby przypisać certyfikat do aplikacji podpisującej obiekty, wykonaj następujące czynności:

1. W ramce nawigacji programu DCM wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
2. Z listy tej wybierz **Przypisanie certyfikatu**, aby wyświetlić listę certyfikatów bieżącej bazy certyfikatów.
3. Wybierz certyfikat z listy i kliknij **Przypisz do aplikacji**, aby wyświetlić listę definicji aplikacji bieżącej bazy certyfikatów.
4. Wybierz jedną lub więcej aplikacji z listy i kliknij **Kontynuuj**. Pojawi się strona komunikatów, przedstawiająca albo potwierdzenie przypisania certyfikatu, albo informacje o błędzie, jeśli wystąpił jakiś problem.

Po zakończeniu tych czynności wszystko jest gotowe do wykorzystania programu DCM do podpisywania programów używanych przez publiczny serwer WWW przedsiębiorstwa (iSeries B).

Krok 5: podpisywanie programów

Aby za pomocą programu DCM podpisywać programy używane na publicznym serwerze WWW przedsiębiorstwa (iSeries B), wykonaj następujące czynności:

1. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
2. Wpisz hasło do bazy certyfikatów *OBJECTSIGNING i kliknij **Kontynuuj**.
3. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie obiektami do podpisywania**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Podpisanie obiektu**, aby wyświetlić listę definicji aplikacji, których można użyć do podpisywania obiektów.
5. Wybierz aplikację zdefiniowaną w poprzednim punkcie i kliknij **Podpisanie obiektu**. Pojawi się formularz umożliwiający podanie położenia obiektów, które mają być podpisane.
6. 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 zastępuje *dowolny ciąg znaków*, i znak zapytania (**?**), który zastępuje *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 należy 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 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 zaznaczyć, 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 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 zostało uruchomione podpisanie obiektów. Aby wyświetlić jego wyniki, znajdź zadanie **QOBJSGNBAT** w protokole zadania.

Aby upewnić się, że możesz wyeksportować certyfikaty musisz najpierw wyeksportować niezbędne certyfikaty do pliku a plik certyfikatów przesłać do serwera iSeries B. Przed przesłaniem podpisanych programów do serwera iSeries B musisz także zakończyć wszystkie zadania konfiguracyjne na tym serwerze. Przed weryfikowaniem podpisów odtworzonych obiektów na serwerze iSeries B należy zakończyć konfigurowanie weryfikowania podpisów.

Krok 6: eksport certyfikatów umożliwiających weryfikowanie podpisów na serwerze iSeries B

Podpisywanie obiektów w celu ochrony integralności ich zawartości ma sens tylko wtedy, gdy istnieją metody weryfikowania autentyczności podpisu. Aby weryfikować podpisy obiektów na tym samym systemie, który podpisuje obiekty (iSeries A), należy użyć programu DCM do utworzenia bazy certyfikatów *SIGNATUREVERIFICATION. Musi ona zawierać zarówno kopię certyfikatu podpisującego obiekt, jak i kopię certyfikatu ośrodka CA, który wystawił certyfikat podpisujący.

Aby inni użytkownicy mogli weryfikować podpis, należy im dostarczyć kopię certyfikatu podpisującego obiekt. Jeśli do wystawienia certyfikatu korzysta się z lokalnego ośrodka CA, trzeba im zapewnić także kopię certyfikatu lokalnego ośrodka CA.

Aby za pomocą programu DCM weryfikować podpisy w tym samym systemie, który podpisuje obiekty (w tym scenariuszu jest to serwer iSeries A), wykonaj następujące czynności:

1. W oknie nawigacji wybierz **Tworzenie nowej bazy certyfikatów**, a następnie, jako bazę certyfikatów do utworzenia wybierz ***SIGNATUREVERIFICATION**.
2. Wybierz **Tak**, aby skopiować do nowej bazy certyfikatów istniejące certyfikaty podpisujące obiekty jako certyfikaty weryfikujące podpisy.
3. Podaj hasło dla nowej bazy certyfikatów i kliknij **Kontynuuj**, aby ją utworzyć. Od tego momentu za pomocą programu DCM możesz weryfikować podpisy obiektów na tym samym systemie, którego używasz do podpisywania obiektów.

Aby użyć programu DCM do eksportowania kopii certyfikatu lokalnego CA i kopii certyfikatu podpisującego obiekty jako certyfikatu weryfikującego podpisy, w celu weryfikacji podpisów obiektów na innych systemach (iSeries B), wykonaj następujące czynności:

1. W ramce nawigacji wybierz **Zarządzanie certyfikatami**, a następnie wybierz zadanie **Eksport certyfikatu**.
2. Wybierz **Ośrodek certyfikacji** i kliknij **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodków certyfikacji, które możesz wyeksportować.
3. Wybierz z listy uprzednio utworzony certyfikat lokalnego CA i kliknij **Eksportuj**.
4. Podaj **Plik** jako miejsce docelowe i kliknij **Kontynuuj**.
5. Podaj pełną ścieżkę i nazwę dla pliku eksportowanego certyfikatu lokalnego CA i kliknij **Kontynuuj**, aby wyeksportować certyfikat.
6. Kliknij **OK**, aby opuścić stronę potwierdzenia eksportu. Możesz już eksportować kopię certyfikatu podpisującego obiekty.
7. Ponownie wybierz zadanie **Eksportuj certyfikat**.
8. Wybierz **Podpisywanie obiektów**, aby wyświetlić listę certyfikatów podpisujących obiekty, które można eksportować.
9. Wybierz z listy odpowiedni certyfikat podpisujący obiekty i kliknij **Eksportuj**.
10. Wybierz **Plik, jako certyfikat do weryfikowania podpisów** jako miejsce docelowe i kliknij **Kontynuuj**.
11. Podaj pełną ścieżkę i nazwę dla pliku eksportowanego certyfikatu do weryfikowania podpisów i kliknij **Kontynuuj**, aby wyeksportować certyfikat.

Należy teraz przesłać te pliki do systemów końcowych serwerów iSeries, na których mają być weryfikowane podpisy utworzone za pomocą tego certyfikatu.

Krok 7: przesłanie plików certyfikatów do publicznego serwera przedsiębiorstwa (iSeries B)

Zanim będzie można skonfigurować serwery do weryfikowania podpisanych obiektów, należy przesłać pliki certyfikatów utworzone na serwerze iSeries A do serwera iSeries B, który w tym scenariuszu jest publicznym serwerem WWW przedsiębiorstwa. Do przesłania plików certyfikatów można użyć kilku metod, na przykład skorzystać z protokołu FTP lub z rozpowszechniania pakietów w programie Centrum Zarządzania.

Krok 8: zadania weryfikowania podpisu: tworzenie bazy certyfikatów *SIGNATUREVERIFICATION

Aby weryfikować podpisy obiektów na serwerze iSeries B (publiczny serwer WWW przedsiębiorstwa), należy w znajdującej się na nim bazie certyfikatów *SIGNATUREVERIFICATION umieścić kopię odpowiedniego certyfikatu do weryfikowania podpisów. Ponieważ do podpisywania obiektów korzysta się z certyfikatu wystawionego przez lokalny ośrodek CA, baza certyfikatów musi zawierać także kopię jego certyfikatu.

Aby utworzyć bazę certyfikatów *SIGNATUREVERIFICATION, wykonaj następujące czynności:

1. Uruchom program DCM.
2. W ramce nawigacji programu Menedżer certyfikatów cyfrowych wybierz **Tworzenie nowej bazy certyfikatów** i ***SIGNATUREVERIFICATION** jako nową bazę certyfikatów.

   Uwaga: W przypadku wątpliwości dotyczących określonego formularza podczas korzystania z programu DCM należy kliknąć przycisk znaku zapytania (**?**) u góry strony, aby uzyskać dostęp do systemu pomocy.
3. Podaj hasło dla nowej bazy certyfikatów i kliknij **Kontynuuj**, aby ją utworzyć. Możesz teraz importować certyfikaty do bazy i korzystać z nich do weryfikowania podpisów obiektów.

Krok 9: zadania weryfikowania podpisu: importowanie certyfikatów

Aby weryfikować podpis na obiekcie, baza *SIGNATUREVERIFICATION musi zawierać kopię certyfikatu do weryfikowania podpisów. Jeśli certyfikat podpisujący jest prywatny, to w bazie certyfikatów musi znaleźć się również kopia certyfikatu lokalnego ośrodka CA, który go wystawił. W opisywanym scenariuszu obydwa certyfikaty zostały wyeksportowane do pliku, a plik przesłany do każdego systemu końcowego serwera iSeries.

Aby zaimportować te certyfikaty do bazy *SIGNATUREVERIFICATION, wykonaj następujące czynności:

1. W oknie nawigacji programu DCM kliknij **Wybór ośrodka certyfikacji** i wybierz ***SIGNATUREVERIFICATION** jako bazę certyfikatów do otwarcia.
2. Gdy pojawi się strona Baza certyfikatów i hasło, wpisz hasło bazy certyfikatów (określone przy tworzeniu tej bazy) i kliknij **Kontynuuj**.
3. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Import certyfikatu**.
5. Jako typ certyfikatu wybierz **Ośrodek certyfikacji** i kliknij **Kontynuuj**.

   Uwaga: Przed zaimportowaniem prywatnego certyfikatu do weryfikowania podpisów należy zaimportować certyfikat lokalnego ośrodka CA, inaczej proces importu certyfikatu do weryfikowania podpisów nie powiedzie się.
6. Podaj pełną ścieżkę i nazwę dla pliku certyfikatu ośrodka CA i kliknij **Kontynuuj**. Pojawi się komunikat potwierdzający pomyślne zakończenie importu lub informacja o błędzie, jeśli proces nie powiódł się.
7. Ponownie wybierz zadanie **Importuj certyfikat**.

8. Jako typ certyfikatu wybierz **Sprawdzania podpisu** i kliknij **Kontynuuj**.
9. Podaj pełną ścieżkę i nazwę dla pliku certyfikatu do weryfikowania podpisów i kliknij **Kontynuuj**. Pojawi się komunikat potwierdzający pomyślne zakończenie importu lub informacja o błędzie, jeśli proces nie powiódł się.

Od tego momentu można już używać programu DCM na serwerze iSeries B do weryfikowania podpisów na obiektach, podpisanych odpowiednim certyfikatem podpisującym na serwerze iSeries A.

Krok 10: zadania weryfikowania podpisu: weryfikowanie podpisów na obiektach programów

Aby użyć programu do weryfikowania podpisów na przesłanych obiektach programów, wykonaj następujące czynności:

1. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SIGNATUREVERIFICATION**, aby otworzyć tę bazę certyfikatów.
2. Wpisz hasło do bazy certyfikatów *SIGNATUREVERIFICATION i kliknij **Kontynuuj**.
3. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie obiektami do podpisywania**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Sprawdzanie podpisu obiektu**, aby określić położenie obiektów, dla których chcesz weryfikować podpisy.
5. 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 zastępuje *dowolny ciąg znaków*, i znak zapytania (**?**), który zastępuje *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 skorzystać ze znaków zastępczych w nazwie ścieżki, a następnie kliknąć przycisk **Przeglądaj**.
6. 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 zaznaczyć, 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).
7. 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 zostało wprowadzone zadanie w celu weryfikacji podpisów obiektów. Aby wyświetlić wyniki zadania, znajdź zadanie **QOBJSGNBAT** w protokole zadania.

Scenariusz: korzystanie z funkcji API do podpisywania obiektów i weryfikowania podpisów obiektów

Opis sytuacji

Przedsiębiorstwo (MojaFirma) jest partnerem handlowym iSeries, dostarczającym aplikacje dla klientów. Jako twórca oprogramowania dla przedsiębiorstwa jesteś odpowiedzialny za tworzenie pakietów rozpowszechnianych wśród klientów. Do utworzenia pakietu aplikacji używasz pewnych programów. Klienci mogą zamówić dysk CD-ROM lub pobrać aplikację z serwisu WWW.

Na bieżąco zapoznajesz się z nowinkami technicznymi, szczególnie dotyczącymi ochrony. Dlatego wiesz, że klienci są żywotnie zainteresowani źródłem pochodzenia i zawartością otrzymywanych lub pobieranych programów. Zdarzają się przypadki, że klienci myślą, że otrzymali lub pobrali produkt z zaufanego źródła, potem jednak okazuje się, że nie jest to prawdziwe miejsce pochodzenia tego produktu. Czasami wynika to z faktu, że klienci instalują inny program, niż oczekiwali. Czasami zaś program okazuje się być innym programem lub został zamieniony i powoduje uszkodzenie systemu.

Wprawdzie nie są to zazwyczaj problemy klientów korzystających z serwerów iSeries, ale chcesz dać klientom pewność pochodzenia otrzymanych przez nich aplikacji. Chcesz także dostarczyć klientom narzędzia do sprawdzenia integralności oraz autentyczności pochodzenia instalowanych aplikacji.

Po analizie możliwych rozwiązań zdecydowałeś się wykorzystać możliwość podpisywania obiektów systemu OS/400. Cyfrowe podpisywanie aplikacji umożliwia klientom sprawdzenie, czy dane przedsiębiorstwo jest prawowitym źródłem aplikacji, które otrzymali lub pobrali. Ponieważ tworzenie pakietów aplikacji odbywa się programowo, zdecydowałeś się użyć funkcji API, aby w prosty sposób dołączyć podpisywanie obiektów do istniejącego procesu tworzenia pakietów. Ponadto podjąłeś decyzję o użyciu do podpisywania obiektów certyfikatu publicznego, aby proces weryfikowania podpisu był dla klientów instalujących produkt całkowicie przezroczysty.

Do tworzonego pakietu dołączasz kopię certyfikatu cyfrowego użytego do podpisania obiektu. Po otrzymaniu pakietu klient skorzysta z klucza publicznego certyfikatu do zweryfikowania podpisu na aplikacji. Dzięki temu procesowi klient może określić i sprawdzić źródło aplikacji oraz zyskać pewność, że zawartość aplikacji nie uległa zmianie od czasu jej podpisania.

Przykład ten jest praktycznym wprowadzeniem do programowego podpisywania obiektów, takich jak opracowywane aplikacje czy pakiety przeznaczone dla innych osób.

Zalety scenariusza

Scenariusz ten ma następujące zalety:

- Korzystanie z funkcji API do programowego tworzenia pakietów i podpisywania obiektów pozwala na redukcję czasu spędzonego na implementowaniu tego środka ochrony.
- Korzystanie z funkcji API do podpisywania obiektów podczas tworzenia pakietów zmniejsza ilość koniecznych działań, gdyż proces podpisywania jest częścią procesu tworzenia pakietów.
- Podpisywanie pakietu obiektów umożliwia łatwe określenie, czy obiekty zostały zmienione od czasu podpisania. Pozwala zmniejszyć nakłady na przyszłe rozwiązywanie i śledzenie problemów pojawiających się w aplikacjach działających u klientów.
- Wykorzystanie do podpisania obiektów certyfikatu powszechnie znanego publicznego ośrodka CA pozwala na zastosowanie w części programu obsługi wyjścia programu instalacyjnego produktu funkcji API Add Verifier. Wykorzystanie tej funkcji pozwala automatycznie dodać do systemu klienta publiczny certyfikat użyty do podpisania aplikacji. To zaś daje pewność, że weryfikowanie podpisu jest przezroczyste dla klienta.

Cele

W scenariuszu zakładamy, że przedsiębiorstwo MojaFirma chce programowo podpisywać tworzone pakiety aplikacji rozpowszechniane do klientów. Jako programista tworzący aplikacje w przedsiębiorstwie programowo tworzysz pakiety aplikacji, które następnie są rozpowszechniane do klientów. Dlatego chcesz

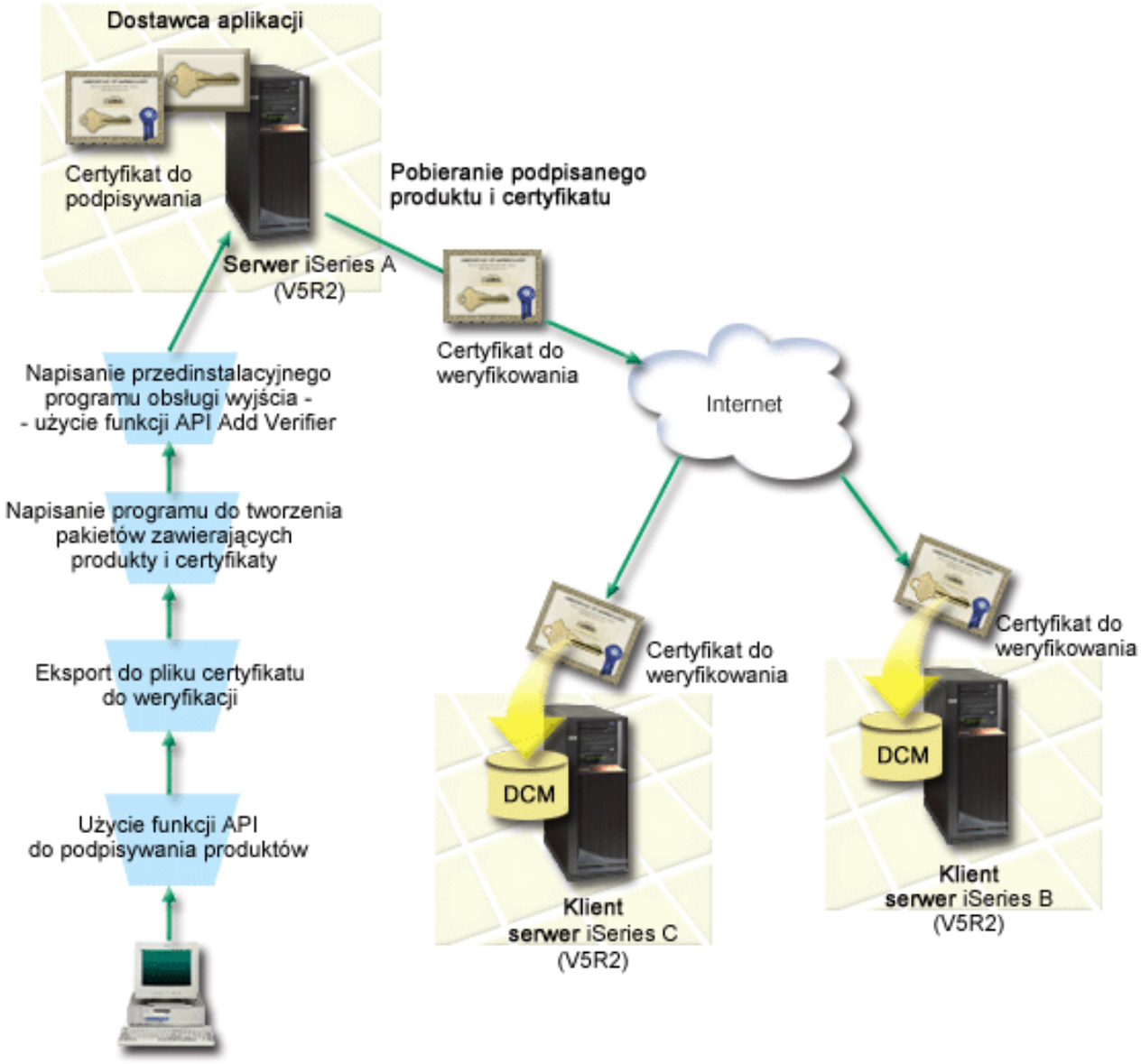
użyć funkcji API serwera iSeries do podpisania tych aplikacji tak, aby serwer iSeries klienta mógł programowo zweryfikować podpis podczas instalacji produktu.

Główne założenia scenariusza są następujące:

- Dostawca aplikacji musi mieć możliwość podpisywania obiektów za pomocą funkcji API Sign Object w trakcie opracowanego już procesu tworzenia pakietu aplikacji.
- Aplikacje muszą być podpisane certyfikatem publicznym, aby proces weryfikowania podpisu, następujący w trakcie instalacji aplikacji, był całkowicie przezroczysty dla klienta.
- Przedsiębiorstwo musi korzystać z funkcji API serwera iSeries do programowego dodawania żądanego certyfikatu weryfikującego podpis do bazy certyfikatów *SIGNATUREVERIFICATION serwera iSeries klienta. Jeśli ta baza certyfikatów nie istnieje, należy stworzyć możliwość jej programowego utworzenia na serwerze iSeries klienta podczas procesu instalacji.
- Po zainstalowaniu produktu klienci muszą mieć możliwość prostego weryfikowania podpisów cyfrowych na aplikacji. Jest to niezbędne, aby ustalić źródło i autentyczność podpisanej aplikacji oraz określić, czy od czasu podpisania aplikacja nie została zmieniona.

Szczegóły

Poniższy rysunek przedstawia proces podpisywania obiektu i weryfikowania podpisu według scenariusza:



Rysunek ilustruje następujące punkty scenariusza:

System centralny (serwer iSeries A)

- serwer iSeries A z systemem OS/400 w wersji 5 wydanie 2 (V5R2),
- na serwerze iSeries A jest uruchomiony program tworzący pakiety aplikacji,
- na serwerze iSeries A jest zainstalowany program Cryptographic Access Provider 128-bit for iSeries (5722–AC3),
- na serwerze iSeries A musi być zainstalowany i skonfigurowany program Menedżer certyfikatów cyfrowych (opcja 34 systemu OS/400) i serwer IBM HTTP (5722–DG1),
- serwer iSeries A jest podstawowym systemem podpisującym obiekty dla aplikacji w przedsiębiorstwie. Podpisywanie produktów przeznaczonych do dystrybucji do klientów na serwerze iSeries A przebiega następująco:
  1. Aplikacja jest podpisywana za pomocą funkcji API.
  2. Certyfikat do weryfikowania podpisów jest eksportowany do pliku za pomocą programu DCM, aby klienci mogli weryfikować podpisane obiekty.

3. Powstaje program służący do dodawania certyfikatu weryfikującego do podpisywanej aplikacji.
4. Powstaje program przedinstalacyjny obsługi wyjścia korzystający z funkcji API Add Verifier. Funkcja ta umożliwia procesowi instalacji produktu programowe dodanie certyfikatu weryfikującego do bazy certyfikatów *SIGNATUREVERIFICATION na serwerze iSeries klienta (serwery iSeries B i C).

Serwery iSeries klienta (B i C)

- serwer iSeries B z systemem OS/400 w wersji 5 wydanie 2 (V5R2),
- serwer iSeries C z systemem OS/400 w wersji 5 wydanie 2 (V5R2),
- serwery iSeries B i C muszą mieć zainstalowane i skonfigurowane programy Menedżer certyfikatów cyfrowych (opcja 34) i serwer IBM HTTP Server (5722–DG1),
- serwery iSeries B i C nabywają i pobierają aplikacje z serwisu WWW producenta (właściciela serwera iSeries A),
- serwery iSeries B i C otrzymują kopię certyfikatu do weryfikowania podpisów przedsiębiorstwa MojaFirma, podczas gdy proces instalacji aplikacji tego przedsiębiorstwa tworzy bazę certyfikatów *SIGNATUREVERIFICATION na każdym z tych serwerów iSeries klientów.

Założenia i wymagania wstępne

Scenariusz zależy od spełnienia następujących założeń i wymagań wstępnych:

1. Wszystkie serwery iSeries spełniają wymagania konieczne do zainstalowania programu Menedżer certyfikatów cyfrowych (DCM).

   Uwaga: Spełnienie przez serwery klientów (w tym scenariuszu są to serwery iSeries B i C) wymagań wstępnych związanych z instalacją i korzystaniem z programu DCM jest opcjonalne. Jednak funkcja API Add Verifier podczas procesu instalacji produktu, jeśli jest to potrzebne, tworzy bazę certyfikatów *SIGNATUREVERIFICATION z hasłem domyślnym. Aby zaś lepiej chronić bazę certyfikatów przez dostępem bez uprawnień i móc zmienić to hasło, klienci muszą korzystać z programu DCM.
2. Na żadnym z serwerów iSeries nie był wcześniej konfigurowany ani używany program DCM.
3. Wszystkie serwery iSeries mają zainstalowaną najnowszą wersję programu licencjonowanego Cryptographic Access Provider 128-bit (5722-AC3).
4. Ustawienie domyślne wartości systemowej Weryfikowanie podpisów obiektów podczas odtwarzania (QVFYOBJRST) w całym scenariuszu serwera iSeries wynosi 3 i pozostaje niezmienione. Ustawienie domyślne daje gwarancje, że serwer będzie mógł zweryfikować podpisy po odtworzeniu podpisanych obiektów.
5. Aby administrator sieci serwera iSeries A mógł podpisywać obiekty, musi mieć uprawnienia specjalne profilu użytkownika *ALLOBJ albo jego profil użytkownika musi być uprawniony do korzystania z aplikacji podpisującej obiekty.
6. Administrator systemu lub inna osoba, która tworzy bazę certyfikatów w programie DCM, musi mieć uprawnienia specjalne profilu użytkownika *SECADM i *ALLOBJ.
7. Do weryfikowania podpisów obiektów administratorzy systemów lub inni użytkownicy pozostałych serwerów iSeries muszą mieć uprawnienia specjalne profilu użytkownika *AUDIT.

Kolejne zadania

Aby zgodnie ze scenariuszem serwer iSeries A mógł podpisywać obiekty, należy:

1. Spełnić w całości wymagania wstępne konieczne do zainstalowania wszystkich potrzebnych produktów serwera iSeries.
2. Użyć programu DCM do utworzenia wniosku o certyfikat w celu uzyskiwania certyfikatu podpisującego obiekty od powszechnie znanego publicznego ośrodka CA.
3. Użyć programu DCM do utworzenia definicji aplikacji podpisującej obiekty.

4. Użyć programu DCM do importowania podpisanego certyfikatu do podpisywania obiektów i przypisania go do definicji aplikacji podpisującej obiekty.
5. Użyć programu DCM do eksportowania certyfikatu podpisującego obiekty jako certyfikatu służącego do weryfikowania podpisów, aby klienci mogli go użyć do weryfikowania podpisów na aplikacjach.
6. Zmienić program przeznaczony do tworzenia pakietów aplikacji, tak aby dodawał do pakietu plik certyfikatu do weryfikowania podpisów i użyć funkcji API Sign Object w celu podpisania aplikacji podczas tworzenia pakietu rozpowszechnianego wśród klientów.
7. Utworzyć w ramach procesu tworzenia pakietu aplikacji program przedinstalacyjny obsługi wyjścia korzystający z funkcji Add Verifier. Program obsługi wyjścia umożliwia utworzenie podczas instalacji produktu bazy certyfikatów *SIGNATUREVERIFICATION i dodanie niezbędnego certyfikatu do weryfikowania podpisów na serwerze iSeries klienta.
8. Aby klienci mogli zmienić hasło domyślne bazy certyfikatów *SIGNATUREVERIFICATION na swoich serwerach iSeries, muszą skorzystać z programu DCM.

Szczegóły konfigurowania

Aby zgodnie ze scenariuszem użyć funkcji API systemu OS/400 do podpisywania obiektów, należy wykonać następujące czynności.

Krok 1: wypełnienie wszystkich wymagań wstępnych

Przed wykonaniem dalszych czynności konfiguracyjnych związanych z implementacją tego scenariusza, należy w całości spełnić wymagania wstępne konieczne do zainstalowania i skonfigurowania wszystkich potrzebnych produktów serwera iSeries.

Krok 2: użycie programu DCM do pobrania certyfikatu z powszechnie znanego publicznego ośrodka CA

Scenariusz zakłada, że wcześniej nie korzystałeś z programu Menedżer certyfikatów cyfrowych do tworzenia i zarządzania certyfikatami. Dlatego jako część procesu tworzenia własnego certyfikatu podpisującego obiekty musisz utworzyć bazę certyfikatów *OBJECTSIGNING. Podczas tworzenia bazy certyfikatów zrealizowane zostaną zadania potrzebne do tworzenia i zarządzania certyfikatami podpisującymi obiekty. Aby uzyskać od powszechnie znanego publicznego ośrodka CA certyfikat, użyj programu DCM do utworzenia informacji identyfikujących i pary kluczy publiczny-prywatny dla certyfikatu i wysłania tych informacji do ośrodka CA.

Aby utworzyć wniosek o certyfikat, który należy dostarczyć do powszechnie znanego publicznego ośrodka CA w celu otrzymania certyfikatu podpisującego obiekty, wykonaj następujące czynności:

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 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. Wybierz ***OBJECTSIGNING** jako bazę certyfikatów do utworzenia i kliknij **Kontynuuj**.
4. Wybierz **Tak**, aby w ramach tworzenia bazy certyfikatów *OBJECTSIGNING utworzyć certyfikat, 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 wystawiającego certyfikat. Dane Certificate Signing Request (CSR) zawierają klucz publiczny i inne informacje podane do certyfikatu.

7. Uważnie skopiuj dane CSR i wklej je do formularza wniosku o certyfikat lub do osobnego pliku wymaganego przez publiczny ośrodek 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, który ma wystawić i podpisać certyfikat.
9. Przed przejściem do następnego zadania w tym scenariuszu zaczekaj aż ośrodek CA odeśle podpisany, wypełniony certyfikat.

Krok 3: tworzenie definicji aplikacji podpisującej obiekty

Po wysłaniu wniosku o certyfikat do powszechnie znanego, publicznego ośrodka CA, można użyć programu DCM do utworzenia definicji aplikacji podpisującej obiekty, która będzie służyć do podpisywania obiektów. Definicja aplikacji nie musi odnosić się do istniejącej aplikacji, tworzona definicja aplikacji powinna opisywać rodzaj lub grupę obiektów, które zamierzasz podpisywać. Definicja jest niezbędna, żeby można było powiązać identyfikator aplikacji z certyfikatem i umożliwić proces podpisywania.

Aby utworzyć definicję aplikacji podpisującej obiekty za pomocą programu DCM, wykonaj następujące czynności:

1. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
2. Gdy pojawi się strona Baza certyfikatów i hasło, wpisz hasło bazy certyfikatów (określone przy tworzeniu tej bazy) i kliknij **Kontynuuj**.
3. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Dodaj aplikację**, aby wyświetlić formularz definiowania aplikacji.
5. Wypełnij formularz i kliknij **Dodaj**.

Po otrzymaniu od ośrodka CA podpisanego certyfikatu można przypisać certyfikat do utworzonej aplikacji.

Krok 4: importowanie podpisanego certyfikatu publicznego i przypisywanie go do aplikacji podpisującej obiekty

Aby zaimportować certyfikat, przypisać go do aplikacji i włączyć podpisywanie obiektów, wykonaj następujące czynności:

1. Uruchom program DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
3. Gdy pojawi się strona Baza certyfikatów i hasło, wpisz hasło bazy certyfikatów (określone przy tworzeniu tej bazy) 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.

   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. Wybierz **Przypisanie certyfikatu** z listy zadań **Zarządzanie certyfikatami**, aby wyświetlić listę certyfikatów bieżącej bazy certyfikatów.
7. Wybierz certyfikat z listy i kliknij **Przypisz do aplikacji**, aby wyświetlić listę definicji aplikacji bieżącej bazy certyfikatów.
8. Wybierz swoją aplikację z listy i kliknij **Kontynuuj**. Pojawi się strona z komunikatem potwierdzającym wybór przypisania, albo komunikat o błędzie, jeśli wystąpi jakiś problem.

Po zakończeniu tych czynności możesz korzystać z podpisywania aplikacji i innych obiektów za pomocą funkcji API systemu OS/400. Aby mieć pewność, że jesteś w stanie weryfikować podpisy, musisz wyeksportować niezbędne certyfikaty do pliku i przesłać je do serwera iSeries, na którym instalowane będą podpisane aplikacje. Serwery iSeries klienta muszą być przygotowane na użycie certyfikatu do weryfikowania podpisu na aplikacji podczas jej instalowania. Do konfigurowania weryfikacji podpisów u klientów możesz użyć funkcji API Add Verifier jako części swojego programu instalacyjnego aplikacji. Możesz na przykład utworzyć przedinstalacyjny program obsługi wyjścia wywołujący funkcję API Add Verifier do konfigurowania serwera iSeries klienta.

Krok 5: eksport certyfikatów umożliwiających weryfikowanie podpisu na pozostałych serwerach iSeries

Podpisywanie obiektów ma sens tylko wtedy, gdy istnieją metody weryfikowania autentyczności podpisu i określania czy do podpisanego obiektu zostały wprowadzone jakieś zmiany. Aby zweryfikować podpisy obiektów na tym samym systemie, który podpisuje obiekty, należy użyć programu DCM do utworzenia bazy certyfikatów *SIGNATUREVERIFICATION. Musi ona zawierać zarówno kopię certyfikatu podpisującego obiekt, jak i kopię certyfikatu ośrodka CA, który wystawił certyfikat podpisujący.

Aby inni użytkownicy mogli weryfikować podpis, należy im dostarczyć kopię certyfikatu podpisującego obiekt. Jeśli do wystawienia certyfikatu korzysta się z lokalnego ośrodka CA, trzeba im zapewnić także kopię certyfikatu lokalnego ośrodka CA.

Aby za pomocą programu DCM weryfikować podpisy w tym samym systemie, który podpisuje obiekty (w tym scenariuszu jest to serwer iSeries A), wykonaj następujące czynności:

1. W oknie nawigacji wybierz **Tworzenie nowej bazy certyfikatów**, a następnie, jako bazę certyfikatów do utworzenia wybierz ***SIGNATUREVERIFICATION**.
2. Wybierz **Tak**, aby skopiować do nowej bazy certyfikatów istniejące certyfikaty podpisujące obiekty jako certyfikaty weryfikujące podpisy.
3. Podaj hasło dla nowej bazy certyfikatów i kliknij **Kontynuuj**, aby ją utworzyć. Od tego momentu za pomocą programu DCM możesz weryfikować podpisy obiektów na tym samym systemie, którego używasz do podpisywania obiektów.

Aby użyć programu DCM do eksportowania kopii certyfikatu podpisującego obiekt jako certyfikatu weryfikującego podpis, tak aby inni użytkownicy mogli weryfikować podpisy obiektów, wykonaj następujące czynności:

1. W ramce nawigacji wybierz **Zarządzanie certyfikatami**, a następnie wybierz zadanie **Eksport certyfikatu**.
2. Wybierz **Podpisywanie obiektów**, aby wyświetlić listę certyfikatów podpisujących obiekty, które można eksportować.
3. Wybierz z listy odpowiedni certyfikat podpisujący obiekty i kliknij **Eksportuj**.
4. Wybierz **Plik, jako certyfikat do weryfikowania podpisów** jako miejsce docelowe i kliknij **Kontynuuj**.
5. Podaj pełną ścieżkę i nazwę dla pliku eksportowanego certyfikatu do weryfikowania podpisów i kliknij **Kontynuuj**, aby wyeksportować certyfikat.

Możesz teraz dodawać ten plik do pakietów instalacyjnych aplikacji tworzonych dla produktu. Za pomocą funkcji API Add Verifier jako części programu instalacyjnego możesz dodać ten certyfikat do bazy certyfikatów *SIGNATUREVERIFICATION klienta. Jeśli baza certyfikatów jeszcze nie istnieje, funkcja ta ją utworzy. Następnie program instalacyjny produktu może zweryfikować podpis na aplikacji podczas odtwarzania go na serwerze iSeries klienta.

Krok 6: aktualizacja programu tworzącego pakiet aplikacji aby używał funkcji API serwera iSeries do podpisywania aplikacji

Gdy masz już plik zawierający certyfikat do weryfikowania podpisów i chcesz go dodać do pakietu aplikacji, możesz skorzystać z funkcji API Sign Object i napisać nową lub zmienić istniejącą aplikację w taki sposób, aby podpisywała biblioteki produktu podczas tworzenia pakietu rozpowszechnianego wśród klientów.

Aby lepiej zrozumieć wykorzystanie funkcji API Sign Object jako części programu tworzącego pakiet aplikacji, przejrzyj przykład przedstawiony poniżej. Przykład ten jest fragmentem kodu programu napisanego w języku C, nie jest on pełnym programem do podpisywania i tworzenia pakietów, jest to raczej wycinek programu, w którym następuje wywołanie funkcji API Sign Object. Jeśli chcesz skorzystać z tego przykładu, dostosuj go do swoich potrzeb. Ze względów bezpieczeństwa firma IBM zaleca zindywidualizowanie przykładu i zmianę dostarczonych wartości domyślnych.

Uwaga: IBM udziela niewyłącznej licencji na prawa autorskie, stosowanej przy używaniu wszelkich przykładowych kodów programów, na podstawie których można wygenerować podobne funkcje dostosowane do indywidualnych wymagań. Cały kod przykładowy jest udostępniany przez IBM jedynie do celów ilustracyjnych. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować lub sugerować niezawodności, użyteczności i funkcjonalności tych programów. Wszelkie zawarte tu programy są dostarczane w stanie, w jakim się znajdują (″AS IS″) bez udzielania jakichkolwiek gwarancji. Nie udziela się domniemanych gwarancji nienaruszania praw osób trzecich, gwarancji przydatności handlowej oraz przydatności do określonego celu.

Dostosuj ten przykład do swoich potrzeb w celu wykorzystania funkcji API Sign Object jako części programu tworzącego pakiety aplikacji. Do programu należy dostarczyć dwa parametry: nazwę biblioteki do podpisania i nazwę identyfikatora aplikacji podpisującej obiekt; w identyfikatorze aplikacji rozróżnia się wielkie i małe litery, których nie rozróżnia się w nazwie biblioteki. Jeśli podpisywany obiekt składa się z kilku bibliotek, program może wywoływać ten fragment kodu wielokrotnie.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Wykorzystanie funkcji API Sign Object do podpisywania bibliotek  */
/*                                                                  */
/* Funkcja API podpisuje cyfrowo wszystkie obiekty w bibliotece     */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Niniejszy materiał zawiera kod źródłowy programu przeznaczony    */
/* do wglądu. Przykład nie został gruntownie przetestowany pod      */
/* względem wszystkich warunków. W związku z tym firma IBM          */
/* nie może ręczyć za jego niezawodność, przydatność i funkcje.     */
/* of these programs.  Wszystkie programy zawarte tutaj są          */
/* dostarczane na zasadzie "as is" (taki, jaki jest). DOMNIEMANE    */
/* GWARANCJE PRZYDATNOŚCI HANDLOWEJ LUB UŻYTECZNOŚCI DO OKREŚLONEGO */
/* CELU SĄ WYRAŹNIE ODRZUCONE. Firma IBM nie udostępnia usług       */
/* serwisowych dla tych programów i plików.                         */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametry programu:                                              */
/*                                                                  */
/*  char *   nazwa podpisywanej biblioteki                          */
/*  char *   nazwa identyfikatora aplikacji                         */
/*                                                                  */

#include <qydosgno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main (int argc, char *argv[])
{

    /* parametry:
```

```
   char * biblioteka obiektów do podpisania
   char * identyfikator aplikacji podpisującej

 */

int         lib_length, applid_length, path_length, multiobj_length;
Qus_EC_t    error_code;
char        libname[11];
char        path_name[256];

Qydo_Multi_Objects_T * multi_objects = NULL;
multiobj_length = 0;
error_code.Bytes_Provided = 0;    /* wyjątki zwracane dla błędów      */


/* ------------------------------------ */
/* budowa nazwy ścieżki dla biblioteki    */
/* ------------------------------------ */
memset(libname, '\00', 11); /* inicjowanie nazwy biblioteki */
for(lib_length = 0;
    ((*(argv[1] + lib_length) != ' ') &&
     (*(argv[1] + lib_length) != '\00'));
    lib_length++);
memcpy(argv[1], libname, lib_length); /* wpisanie nazwy biblioteki */

/* budowa parametru nazwa ścieżki do wywołania funkcji API */
sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
path_length = strlen(path_name);

/* ---------------------------- */
/* szukanie długości ID aplikacji*/
/* ---------------------------- */
for(applid_length = 0;
    ((*(argv[2] + applid_length) != ' ') &&
     (*(argv[2] + applid_length) != '\00'));
    applid_length++);

/* ------------------------------- */
/* podpisanie obiektów w bibliotece */
/* ------------------------------- */
QYDOSGNO  (path_name,             /* nazwa ścieżki do obiektu    */
           &path_length,          /* długość nazwy ścieżki       */
           "OBJN0100",            /* nazwa formatu               */
           argv[2],               /* identyfikator aplikacji (ID)*/
           &applid_length,        /* długość ident. aplikacji    */
           "1",                   /* zastąpienie podwójnego podp.*/
           multi_objects,         /* jak obsługiwać wiele
                                        obiektów               */
           &multiobj_length,      /* długość używanej struktury
                                     zawier. wiele obiektów
                                   (0=bez str. zaw. wiele ob.) */
           &error_code);          /* kod błędu                   */



  return 0;

}
```

Krok 7: tworzenie korzystającego z funkcji API Add Verifier programu przedinstalacyjnego obsługi wyjścia

Po zakończeniu procesu tworzenia programu do podpisywania aplikacji możesz korzystać z funkcji API Add Verifier jako części programu instalacyjnego do tworzenia rozpowszechnianego produktu końcowego. Jeśli na przykład użyjesz funkcji API Add Verifier jako części programu przedinstalacyjnego obsługi wyjścia,

zyskasz pewność, że przed odtworzeniem podpisanych obiektów aplikacji certyfikat zostanie dodany do bazy certyfikatów. Umożliwi to programowi instalacyjnemu weryfikację podpisu na obiekcie aplikacji podczas odtwarzania go na serwerze iSeries klienta.

Uwaga: Ze względów bezpieczeństwa ta funkcja API nie pozwoli na dodanie do bazy certyfikatów *SIGNATUREVERIFICATION certyfikatu ośrodka certyfikacji. W momencie dodawania certyfikatu ośrodka certyfikacji do bazy certyfikatów system zakłada, że ośrodek CA jest zaufanym źródłem certyfikatów. W konsekwencji system traktuje certyfikat wystawiony przez ośrodek CA jako pochodzący z zaufanego źródła. Dlatego nie można korzystać z funkcji API w celu utworzenia programu instalacyjnego obsługi wyjścia w celu dodania certyfikatu ośrodka certyfikacji do bazy certyfikatów. Aby dodać certyfikat ośrodka CA do bazy certyfikatów, należy użyć programu Menedżer certyfikatów cyfrowych; takie rozwiązanie daje pewność, że sprawowana jest ręczna, dokładna kontrola nad ośrodkami CA, którym system ufa. Dzięki temu system nie może importować certyfikatów ze źródeł, których administrator świadomie nie określił jako zaufane.

Jeśli nie chcesz, aby ktokolwiek mógł dodać certyfikat do bazy certyfikatów *SIGNATUREVERIFICATION korzystając z tej funkcji API, zablokuj tę funkcję w systemie. Aby zrealizować to zadanie, skorzystaj z systemowych narzędzi serwisowych (SST) umożliwiających ustawienie odrzucania zmian wprowadzonych w wartościach systemowych związanych z ochroną.

Aby lepiej zrozumieć wykorzystanie funkcji API Add Verifier jako części programu instalacyjnego aplikacji, przejrzyj przedstawiony poniżej przykład programu przedinstalacyjnego obsługi wyjścia. Przykład ten jest fragmentem kodu programu napisanego w języku C, nie jest on pełnym programem przedinstalacyjnym obsługi wyjścia, jest to raczej wycinek programu, w którym następuje wywołanie funkcji API Add Verifier. Jeśli chcesz skorzystać z tego przykładu, dostosuj go do swoich potrzeb. Ze względów bezpieczeństwa firma IBM zaleca zindywidualizowanie przykładu i zmianę dostarczonych wartości domyślnych.

Uwaga: IBM udziela niewyłącznej licencji na prawa autorskie, stosowanej przy używaniu wszelkich przykładowych kodów programów, na podstawie których można wygenerować podobne funkcje dostosowane do indywidualnych wymagań. Cały kod przykładowy jest udostępniany przez IBM jedynie do celów ilustracyjnych. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować lub sugerować niezawodności, użyteczności i funkcjonalności tych programów. Wszelkie zawarte tu programy są dostarczane w stanie, w jakim się znajdują (″AS IS″) bez udzielania jakichkolwiek gwarancji. Nie udziela się domniemanych gwarancji nienaruszania praw osób trzecich, gwarancji przydatności handlowej oraz przydatności do określonego celu.

Dostosuj ten przykład do swoich potrzeb w celu wykorzystania funkcji API Add Verifier jako części programu przedinstalacyjnego obsługi wyjścia do dodawania niezbędnego certyfikatu weryfikującego podpisy do serwera iSeries klienta podczas instalowania Twojego produktu.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Wykorzystanie funkcji API Add Verifier do dodania certyfikatu    */
/* w określonym pliku IFS bazy certyfikatów *SIGNATUREVERIFICATION. */
/*                                                                  */
/* Jeśli baza certyfikatów nie istnieje, funkcja API utworzy ją.    */
/* Jeśli baza certyfikatów jest tworzona, otrzyma hasło domyślne,   */
/* które należy zmienić najszybciej jak to możliwe korzystając z    */
/* programu DCM. To ostrzeżenie należy przedstawić właścicielowi    */
/* systemu, który będzie korzystał z tego programu.                 */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Niniejszy materiał zawiera kod źródłowy programu przeznaczony    */
/* do wglądu. Przykład nie został gruntownie przetestowany pod      */
/* względem wszystkich warunków. W związku z tym firma IBM          */
/* nie może ręczyć za jego niezawodność, przydatność i funkcje.     */
/* of these programs.  Wszystkie programy zawarte tutaj są          */
```

```
/* dostarczane na zasadzie "as is" (taki, jaki jest). DOMNIEMANE    */
/* GWARANCJE PRZYDATNOŚCI HANDLOWEJ LUB UŻYTECZNOŚCI DO OKREŚLONEGO */
/* CELU SĄ WYRAŹNIE ODRZUCONE. Firma IBM nie udostępnia usług       */
/* serwisowych dla tych programów i plików.                         */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametry programu:                                              */
/*                                                                  */
/*  char *   nazwa ścieżki do pliku IFS zawierającego certyfikat    */
/*  char *   etykieta dla certyfikatu                               */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* ---------------------------------------------------------------- */

#include <qydoadd1.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[])
{

    int         pathname_length, cert_label_length;
    Qus_EC_t    error_code;
    char      * pathname = argv[1];
    char      * certlabel = argv[2];

    /* szukanie dł. nazwy ścieżki */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* szukanie dł. etykiety certyfikatu */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;     /* wyjątki zwracane dla błędów       */

    QydoAddVerifier (pathname,         /* nazwa śc. do pliku z certyfikatem */
                     &pathname_length, /* długość nazwy ścieżki             */
                     "OBJN0100",       /* nazwa formatu                     */
                     certlabel,        /* etykieta certyfikatu              */
                     &cert_label_length, /* długość etykiety certyfikatu    */
                     &error_code);     /* kod błędu                         */

   return 0;
}
```

Po zakończeniu tych zadań możesz tworzyć pakiety swoich aplikacji i rozpowszechniać je wśród klientów. Podczas instalowania przez klientów podpisanych obiektów aplikacji zostaną one zweryfikowane w ramach procesu instalacji. Klienci dysponują także możliwością weryfikowania podpisów na obiektach aplikacji za pomocą programu Menedżer certyfikatów cyfrowych. Daje to klientom możliwość sprawdzenia, czy aplikacja pochodzi z zaufanego źródła i czy od czasu jej podpisania nie została zmieniona.

Uwaga: Program instalacyjny może utworzyć u klienta bazę certyfikatów *SIGNATUREVERIFICATION z hasłem domyślnym. Należy poinformować klienta, że powinien jak najszybciej za pomocą programu DCM zmienić hasło do bazy certyfikatów, aby ochronić bazę przed dostępem bez uprawnień.

Krok 8: zmiana domyślnego hasła do bazy certyfikatów *SIGNATUREVERIFICATION u klienta

Funkcja API Add Verifier może podczas procesu instalacji na serwerze iSeries klienta utworzyć bazę certyfikatów *SIGNATUREVERIFICATION. Jeśli funkcja ta tworzy bazę certyfikatów, to dla bazy powstaje równocześnie hasło domyślne. Należy więc doradzić klientowi skorzystanie z programu DCM i zmianę hasła, aby chronić bazę certyfikatów przed dostępem nieuprawnionych osób.

W tym celu do klientów kierowane są następujące polecenia:

1. Uruchom program DCM.
2. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***SIGNATUREVERIFICATION**, aby otworzyć tę bazę certyfikatów.
3. Gdy pojawi się strona Baza certyfikatów i hasło kliknij **Zerowanie hasła**, aby wyświetlić stronę Zerowanie hasła bazy certyfikatów.

   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.
4. Podaj nowe hasło dla tej bazy, wpisz je ponownie w celu potwierdzenia, wybierz strategię dla ważności hasła do bazy certyfikatów i kliknij **Kontynuuj**.

Scenariusz: korzystanie z Centrum Zarządzania do podpisywania obiektów

Opis sytuacji

Przedsiębiorstwo (MojaFirma) tworzy aplikacje, które następnie rozpowszechnia wśród wielu serwerów iSeries znajdujących się w różnych miejscach przedsiębiorstwa. Jako administrator sieci jesteś odpowiedzialny za zainstalowanie i aktualizację aplikacji na serwerach iSeries w całym przedsiębiorstwie. Do tworzenia pakietów aplikacji i ich rozpowszechniania oraz do innych zadań administracyjnych, korzystasz z funkcji Centrum Zarządzania programu iSeries Navigator. Jednak śledzenie i rozwiązywanie problemów spowodowanych wprowadzonymi do tych aplikacji zmianami dokonanymi przez nieuprawnionych użytkowników zajmuje dużo czasu. Dlatego też chcesz lepiej chronić integralność tych obiektów i podpisywać je cyfrowo.

Przegląd możliwości podpisywania obiektów systemu OS/400 pokazuje, że począwszy od wersji V5R2 Centrum Zarządzania umożliwia podpisywanie obiektów w trakcie tworzenia i dystrybucji pakietów. Dzięki programowi Centrum Zarządzania możesz działać szybko i efektywnie, aby łatwo sprostać założonym celom ochrony przedsiębiorstwa. Zdecydowałeś się też na utworzenie lokalnego ośrodka CA, aby wystawiał certyfikaty do podpisywania obiektów. Wykorzystanie certyfikatów wydawanych przez lokalny ośrodek CA ogranicza wydatki związane z używaniem tej technologii ochrony, gdyż nie trzeba kupować certyfikatu od ogólnie znanego ośrodka CA.

Przykład ten jest praktycznym wprowadzeniem do konfigurowania i korzystania z podpisywania obiektów aplikacji, które mają być rozpowszechniane wśród wielu serwerów iSeries w przedsiębiorstwie.

Zalety scenariusza

Scenariusz ten ma następujące zalety:

- Korzystanie z programu Centrum Zarządzania do tworzenia pakietów i podpisywania obiektów pozwala na redukcję czasu potrzebnego na dystrybucję podpisanych obiektów do serwerów iSeries przedsiębiorstwa.
- Korzystanie z Centrum Zarządzania do podpisywania obiektów w pakietach zmniejsza ilość koniecznych działań, gdyż proces podpisywania jest częścią procesu tworzenia pakietów.

- Podpisywanie pakietu obiektów umożliwia łatwe określenie, czy obiekty zostały zmienione od czasu podpisania. Pozwala zmniejszyć nakłady na przyszłe rozwiązywanie i śledzenie problemów w aplikacjach.
- Wykorzystanie do podpisywania obiektów certyfikatu wystawionego przez prywatny ośrodek certyfikacji obniża koszty wprowadzenia podpisywania obiektów.

Cele

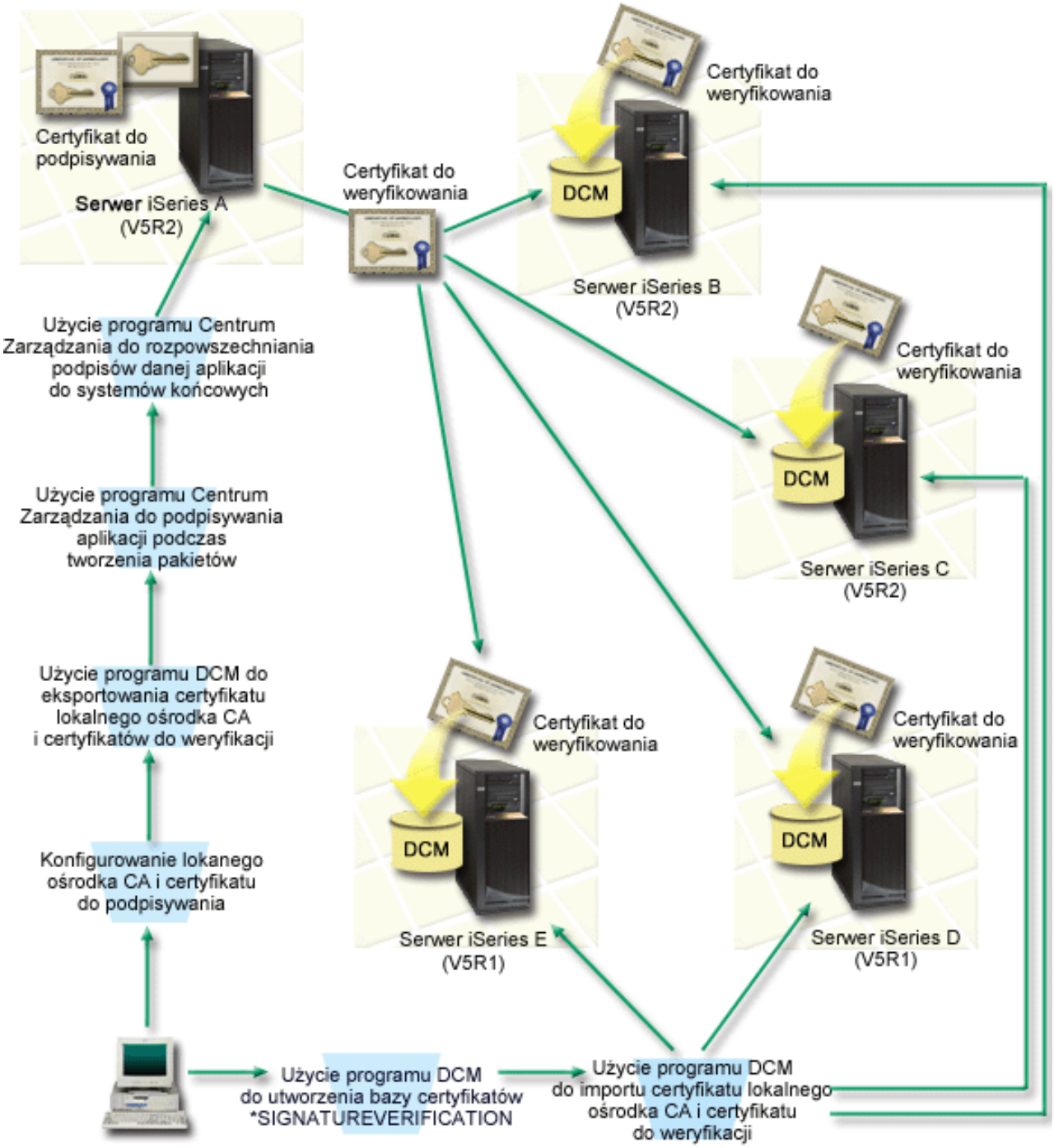
W scenariuszu zakładamy, że przedsiębiorstwo MojaFirma chce podpisywać cyfrowo aplikacje, które rozpowszechnia wśród wielu serwerów iSeries w przedsiębiorstwie. Jako administrator sieci w przedsiębiorstwie korzystasz z programu Centrum Zarządzania do wykonywania wielu zadań administracyjnych na serwerach iSeries. Dlatego chcesz rozszerzyć obecne wykorzystanie programu Centrum Zarządzania o podpisywanie aplikacji przedsiębiorstwa, które są rozpowszechniane wśród innych serwerów iSeries.

Główne założenia scenariusza są następujące:

- Aplikacje przedsiębiorstwa muszą być podpisane certyfikatem wystawionym przez lokalny ośrodek CA, aby ograniczyć koszty podpisywania aplikacji.
- Administratorzy systemu i inni wyznaczeni użytkownicy powinni mieć możliwość prostego weryfikowania podpisów cyfrowych na wszystkich serwerach iSeries, pozwalającego sprawdzić źródło i autentyczność obiektów podpisanych przez przedsiębiorstwo. Aby osiągnąć postawiony cel, każdy serwer iSeries musi mieć w bazie certyfikatów *SIGNATUREVERIFICATION zarówno kopię certyfikatu przedsiębiorstwa do weryfikowania podpisów, jak i certyfikat lokalnego ośrodka CA.
- Weryfikowanie podpisów na aplikacjach przedsiębiorstwa umożliwia administratorom serwerów iSeries, a także innym użytkownikom wykrycie zmian wprowadzonych w obiektach od czasu ich podpisania.
- Administratorzy powinni używać programu Centrum Zarządzania do tworzenia pakietów i ich rozpowszechniania wśród swoich serwerów iSeries.

Szczegóły

Poniższy rysunek przedstawia proces podpisywania obiektu i weryfikowania podpisu według scenariusza:



Rysunek ilustruje następujące punkty scenariusza:

System centralny (serwer iSeries A)

- serwer iSeries A z systemem OS/400 w wersji 5 wydanie 2 (V5R2),
- serwer iSeries A funkcjonuje jako system centralny, z którego uruchamiane są funkcje programu Centrum Zarządzania, włącznie z aplikacjami przedsiębiorstwa służącymi do tworzenia pakietów i ich rozpowszechniania,
- na serwerze iSeries A jest zainstalowany program Cryptographic Access Provider 128-bit for iSeries (5722–AC3),

- na serwerze iSeries A musi być zainstalowany i skonfigurowany program Menedżer certyfikatów cyfrowych (opcja 34 systemu OS/400) i serwer IBM HTTP (5722–DG1),
- serwer iSeries A funkcjonuje jako lokalny ośrodek CA i w tym systemie znajdują się certyfikaty podpisujące obiekty,
- serwer iSeries A jest podstawowym systemem podpisującym obiekty dla aplikacji przedsiębiorstwa. Podpisywanie produktów przeznaczonych do dystrybucji do klientów na serwerze iSeries A przebiega następująco:
  1. Użycie programu DCM do utworzenia lokalnego ośrodka CA, a następnie lokalnego ośrodka CA do utworzenia certyfikatu do podpisywania obiektów.
  2. Użycie programu DCM do wyeksportowania kopii certyfikatu lokalnego ośrodka CA i certyfikatu do weryfikowania podpisów do pliku, aby systemy końcowe (serwery iSeries B, C, D i E) mogły weryfikować podpisane obiekty.
  3. Użycie programu Centrum Zarządzania do podpisania obiektów aplikacji i utworzenia z nich pakietów z plikami certyfikatów do weryfikowania.
  4. Użycie programu Centrum Zarządzania do rozpowszechnienia podpisanych aplikacji i plików certyfikatów do systemów końcowych.

Systemy końcowe (serwery iSeries B, C, D i E)

- serwery iSeries B i C z systemem OS/400 w wersji 5 wydanie 2 (V5R2),
- serwery iSeries D i E z systemem OS/400 w wersji 5 wydanie 1 (V5R1),
- serwery iSeries B, C, D i E muszą mieć zainstalowane i skonfigurowane programy Menedżer certyfikatów cyfrowych (opcja 34) i serwer IBM HTTP (5722–DG1),
- serwery iSeries B, C, D i E otrzymują wraz z podpisaną aplikacją kopie obydwu certyfikatów, tzn. przeznaczonego do weryfikowania podpisów i pochodzącego z lokalnego ośrodka CA przedsiębiorstwa, z systemu centralnego (serwer iSeries A),
- program DCM służy do utworzenia bazy certyfikatów *SIGNATUREVERIFICATION i zaimportowania do niej certyfikatów lokalnego ośrodka CA i do weryfikacji podpisów.

Założenia i wymagania wstępne

Scenariusz zależy od spełnienia następujących założeń i wymagań wstępnych:

1. Wszystkie serwery iSeries spełniają wymagania konieczne do zainstalowania programu Menedżer certyfikatów cyfrowych (DCM).
2. Na żadnym z serwerów iSeries nie był wcześniej konfigurowany ani używany program DCM.
3. Serwer iSeries A spełnia wymagania niezbędne do zainstalowania i używania programów iSeries Navigator i Centrum Zarządzania.
4. Na wszystkich systemach końcowych iSeries musi działać serwer Centrum Zarządzania.
5. Wszystkie serwery iSeries mają zainstalowaną najnowszą wersję programu licencjonowanego Cryptographic Access Provider 128-bit (5722-AC3).
6. Ustawienie domyślne wartości systemowej Weryfikowanie podpisów obiektów podczas odtwarzania (QVFYOBJRST) w całym scenariuszu serwera iSeries wynosi 3 i pozostaje niezmienione. Ustawienie domyślne daje gwarancje, że serwer będzie mógł zweryfikować podpisy po odtworzeniu podpisanych obiektów.
7. Aby administrator sieci serwera iSeries A mógł podpisywać obiekty, musi mieć uprawnienia specjalne profilu użytkownika *ALLOBJ albo jego profil użytkownika musi być uprawniony do korzystania z aplikacji podpisującej obiekty.
8. Administrator sieci lub inna osoba, która tworzy bazę certyfikatów w programie DCM, musi mieć uprawnienia specjalne profilu użytkownika *SECADM i *ALLOBJ.
9. Do weryfikowania podpisów obiektów administratorzy systemów lub inni użytkownicy pozostałych serwerów iSeries muszą mieć uprawnienia specjalne profilu użytkownika *AUDIT.

Kolejne zadania

Aby przedstawiony scenariusz wprowadzić w życie, należy wykonać dwie grupy czynności; jedna polega na takim skonfigurowaniu serwera iSeries A, aby do podpisywania i rozpowszechniania aplikacji korzystał z programu Centrum Zarządzania. Druga grupa czynności umożliwia administratorom systemów i pozostałym użytkownikom weryfikowanie podpisów na tych aplikacjach na wszystkich pozostałych serwerach iSeries.

Czynności związane z podpisywaniem obiektów

Aby zgodnie ze scenariuszem serwer iSeries A mógł podpisywać obiekty, należy:

1. Zrealizować w całości wymagania wstępne konieczne do zainstalowania wszystkich potrzebnych produktów serwera iSeries.
2. Korzystając z programu Menedżer certyfikatów cyfrowych utworzyć lokalny ośrodek CA do wystawiania certyfikatu podpisującego obiekt.
3. Użyć programu DCM do utworzenia definicji aplikacji.
4. Użyć programu DCM do przypisania certyfikatu do definicji aplikacji podpisującej obiekty.
5. Użyć programu DCM do eksportu certyfikatów, których inne systemy będą musiały użyć do weryfikowania podpisów obiektów. Konieczne jest wyeksportowanie do pliku zarówno kopii certyfikatu lokalnego ośrodka CA, jak i kopii certyfikatu do podpisywania obiektów, jako certyfikatu do weryfikowania podpisów.
6. Przesłać pliki certyfikatów do każdego systemu końcowego serwera iSeries, na którym mają być weryfikowane podpisy.
7. Użyć programu Centrum Zarządzania do podpisania obiektów aplikacji.

Czynności związane z weryfikowaniem podpisów

Przed wysłaniem za pomocą programu Centrum Zarządzania podpisanych obiektów aplikacji do każdego z systemów końcowych iSeries, należy na nich skonfigurować weryfikowanie podpisów. Konfigurowanie weryfikowania podpisów musi zostać zakończone przed weryfikowaniem podpisów odtworzonych podpisanych obiektów na systemach końcowych.

Na każdym systemie końcowym iSeries, aby zgodnie ze scenariuszem weryfikować podpisy na obiektach, należy wykonać następujące czynności:

8. Korzystając z programu Menedżer certyfikatów cyfrowych utworzyć bazę certyfikatów *SIGNATUREVERIFICATION.
9. Użyć programu DCM do importu certyfikatu lokalnego ośrodka CA i certyfikatu do weryfikowania podpisów.

Szczegóły konfigurowania

Aby zgodnie ze scenariuszem skonfigurować program Centrum Zarządzania do podpisywania obiektów, należy wykonać następujące czynności.

Krok 1: wypełnienie wszystkich wymagań wstępnych

Przed wykonaniem dalszych czynności konfiguracyjnych związanych z implementacją tego scenariusza, należy wypełnić wszystkie wymagania wstępne konieczne do zainstalowania i skonfigurowania wszystkich potrzebnych produktów serwera iSeries.

Krok 2: tworzenie lokalnego ośrodka CA do wystawiania prywatnych certyfikatów podpisujących obiekty

Podczas tworzenia lokalnego ośrodka CA za pomocą programu Menedżer certyfikatów cyfrowych należy wypełnić szereg formularzy. Formularze te prowadzą przez proces tworzenia ośrodka CA i inne czynności

niezbędne, aby rozpocząć korzystanie z certyfikatów cyfrowych w połączeniu z protokołem SSL, czyli podpisywanie obiektów i weryfikowanie podpisów. Wprawdzie w tym scenariuszu nie trzeba konfigurować certyfikatów w połączeniu z protokołem SSL, ale w celu skonfigurowania systemu do podpisywania obiektów należy wypełnić wszystkie formularze.

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

1. Uruchom program DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić 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. Wypełnij wszystkie formularze zadań. Po zakończeniu tego zadania, wykonaj poniższe czynności:
   a. Wprowadź informacje identyfikujące lokalny ośrodek CA.
   b. Zainstaluj certyfikat lokalnego ośrodka CA w swojej przeglądarce, aby oprogramowanie mogło go rozpoznać i sprawdzać poprawność certyfikatów wystawionych przez ten ośrodek.
   c. Zdefiniuj strategię lokalnego ośrodka CA.
   d. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu klienta lub serwera, z którego aplikacja będzie mogła skorzystać do połączeń z użyciem protokołu SSL.

      Uwaga: Wprawdzie opisywany scenariusz nie korzysta z tego certyfikatu, jego utworzenie jest jednak niezbędne przed użyciem lokalnego ośrodka CA do wystawienia potrzebnego certyfikatu podpisującego obiekt. Jeśli zadanie zostanie anulowane bez utworzenia certyfikatu, to należy utworzyć certyfikat podpisujący obiekt i bazę certyfikatów *OBJECTSIGNING, w której będzie on przechowywany.
   e. Wybierz aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL.

      Uwaga: Na potrzeby tego scenariusza nie wybieraj żadnej aplikacji, tylko kliknij **Kontynuuj**, aby wyświetlić następny formularz.
   f. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu podpisującego obiekt, z którego aplikacja będzie mogła skorzystać do cyfrowego podpisywania obiektów. W tym podzadaniu tworzona jest baza certyfikatów *OBJECTSIGNING. Jest to baza umożliwiająca zarządzanie certyfikatami do podpisywania obiektów.
   g. Wybierz aplikacje, które powinny ufać lokalnemu ośrodkowi CA.

      Uwaga: Na potrzeby tego scenariusza nie wybieraj żadnej aplikacji, tylko kliknij **Kontynuuj**, aby zakończyć zadanie.

Po utworzeniu lokalnego ośrodka CA i certyfikatu podpisującego obiekt, a przed podpisywaniem obiektów, należy zdefiniować korzystającą z certyfikatu aplikację podpisującą obiekty.

Krok 3: tworzenie definicji aplikacji podpisującej obiekty

Po utworzeniu certyfikatu podpisującego obiekt należy za pomocą programu Menedżer certyfikatów cyfrowych utworzyć definicję aplikacji podpisującej obiekty, która będzie używana do podpisywania obiektów. Definicja aplikacji nie musi odnosić się do istniejącej aplikacji, tworzona definicja aplikacji powinna opisywać rodzaj lub grupę obiektów, które zamierzasz podpisywać. Definicja jest niezbędna, żeby można było powiązać identyfikator aplikacji z certyfikatem i umożliwić proces podpisywania.

Aby utworzyć definicję aplikacji podpisującej obiekty za pomocą programu DCM, wykonaj następujące czynności:

1. W ramce nawigacji kliknij **Wybór ośrodka certyfikacji** i wybierz ***OBJECTSIGNING**, aby otworzyć tę bazę certyfikatów.
2. Gdy pojawi się strona Baza certyfikatów i hasło, wpisz hasło bazy certyfikatów (określone przy tworzeniu tej bazy) i kliknij **Kontynuuj**.
3. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Dodaj aplikację**, aby wyświetlić formularz definiowania aplikacji.
5. Wypełnij formularz i kliknij **Dodaj**.

Należy teraz przypisać certyfikat podpisujący obiekt do utworzonej aplikacji.

Krok 4: przypisywanie certyfikatu do definicji aplikacji podpisującej obiekty

Aby przypisać certyfikat do aplikacji podpisującej obiekty, wykonaj następujące czynności:
1. W ramce nawigacji programu DCM wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
2. Z listy tej wybierz **Przypisanie certyfikatu**, aby wyświetlić listę certyfikatów bieżącej bazy certyfikatów.
3. Wybierz certyfikat z listy i kliknij **Przypisz do aplikacji**, aby wyświetlić listę definicji aplikacji bieżącej bazy certyfikatów.
4. Wybierz jedną lub więcej aplikacji z listy i kliknij **Kontynuuj**. Pojawi się strona komunikatów, przedstawiająca albo potwierdzenie przypisania certyfikatu, albo informacje o błędzie, jeśli wystąpił jakiś problem.

Po zakończeniu tych czynności możesz korzystać z podpisywania obiektów za pomocą programu Centrum Zarządzania podczas tworzenia pakietów i ich rozpowszechniania. Aby mieć pewność, że jesteś w stanie weryfikować podpisy, musisz wyeksportować niezbędne certyfikaty do pliku i przesłać plik do wszystkich systemów końcowych iSeries. Przed wysłaniem za pomocą programu Centrum Zarządzania podpisanych obiektów aplikacji do każdego z systemów końcowych iSeries, musisz na nich skonfigurować weryfikowanie podpisów. Konfigurowanie weryfikowania podpisów musi zostać zakończone przed weryfikowaniem podpisów odtworzonych podpisanych obiektów na systemach końcowych.

Krok 5: eksport certyfikatów umożliwiających weryfikowanie podpisu na pozostałych systemach iSeries

Podpisywanie obiektów w celu ochrony integralności ich zawartości ma sens tylko wtedy, gdy istnieją metody weryfikowania autentyczności podpisu. Aby zweryfikować podpisy obiektów na tym samym systemie, który podpisuje obiekty, należy użyć programu DCM do utworzenia bazy certyfikatów *SIGNATUREVERIFICATION. Musi ona zawierać zarówno kopię certyfikatu podpisującego obiekt, jak i kopię certyfikatu ośrodka CA, który wystawił certyfikat podpisujący.

Aby inni użytkownicy mogli weryfikować podpis, należy im dostarczyć kopię certyfikatu podpisującego obiekt. Jeśli do wystawienia certyfikatu korzysta się z lokalnego ośrodka CA, trzeba im zapewnić także kopię certyfikatu lokalnego ośrodka CA.

Aby za pomocą programu DCM weryfikować podpisy w tym samym systemie, który podpisuje obiekty (w tym scenariuszu jest to serwer iSeries A), wykonaj następujące czynności:
1. W oknie nawigacji wybierz **Tworzenie nowej bazy certyfikatów**, a następnie, jako bazę certyfikatów do utworzenia wybierz ***SIGNATUREVERIFICATION**.
2. Wybierz **Tak**, aby skopiować do nowej bazy certyfikatów istniejące certyfikaty podpisujące obiekty jako certyfikaty weryfikujące podpisy.
3. Podaj hasło dla nowej bazy certyfikatów i kliknij **Kontynuuj**, aby ją utworzyć. Od tego momentu za pomocą programu DCM możesz weryfikować podpisy obiektów na tym samym systemie, którego używasz do podpisywania obiektów.

Aby użyć programu DCM do eksportowania kopii certyfikatu lokalnego CA i kopii certyfikatu podpisującego obiekty jako certyfikatu weryfikującego podpisy, w celu weryfikacji podpisów obiektów na innych systemach, wykonaj następujące czynności:

1. W ramce nawigacji wybierz **Zarządzanie certyfikatami**, a następnie wybierz zadanie **Eksport certyfikatu**.
2. Wybierz **Ośrodek certyfikacji** i kliknij **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodków certyfikacji, które możesz wyeksportować.
3. Wybierz z listy uprzednio utworzony certyfikat lokalnego CA i kliknij **Eksportuj**.
4. Podaj **Plik** jako miejsce docelowe i kliknij **Kontynuuj**.
5. Podaj pełną ścieżkę i nazwę dla pliku eksportowanego certyfikatu lokalnego CA i kliknij **Kontynuuj**, aby wyeksportować certyfikat.
6. Kliknij **OK**, aby opuścić stronę potwierdzenia eksportu. Możesz już eksportować kopię certyfikatu podpisującego obiekty.
7. Ponownie wybierz zadanie **Eksportuj certyfikat**.
8. Wybierz **Podpisywanie obiektów**, aby wyświetlić listę certyfikatów podpisujących obiekty, które można eksportować.
9. Wybierz z listy odpowiedni certyfikat podpisujący obiekty i kliknij **Eksportuj**.
10. Wybierz **Plik, jako certyfikat do weryfikowania podpisów** jako miejsce docelowe i kliknij **Kontynuuj**.
11. Podaj pełną ścieżkę i nazwę dla pliku eksportowanego certyfikatu do weryfikowania podpisów i kliknij **Kontynuuj**, aby wyeksportować certyfikat.

Należy teraz przesłać te pliki do systemów końcowych serwerów iSeries, na których mają być weryfikowane podpisy utworzone za pomocą tego certyfikatu.

Krok 6: przesłanie plików certyfikatów do systemów końcowych iSeries

Przed konfigurowaniem systemów końcowych iSeries do weryfikowania podpisanych obiektów należy do nich przesłać pliki certyfikatów utworzone na serwerze iSeries. Do przesłania plików certyfikatów można użyć kilku metod, na przykład skorzystać z protokołu FTP lub z rozpowszechniania pakietów w programie Centrum Zarządzania.

Krok 7: podpisywanie pakietów w programie Centrum Zarządzania

Proces podpisywania obiektów jest dla programu Centrum Zarządzania częścią procesu dystrybucji pakietów oprogramowania. Przed wysłaniem do systemów końcowych iSeries podpisanych obiektów aplikacji, na każdym z tych systemów końcowych należy wykonać wszystkie czynności konfiguracyjne związane z weryfikacją podpisu. Konfigurowanie weryfikowania podpisów musi zostać zakończone przed weryfikowaniem podpisów odtworzonych podpisanych obiektów na systemach końcowych.

Aby zgodnie ze scenariuszem podpisać aplikację rozpowszechnianą wśród systemów końcowych iSeries, wykonaj następujące czynności:

1. Użyj programu Centrum Zarządzania do utworzenia pakietu i dystrybucji oprogramowania.
2. Po pojawieniu się panelu **Identyfikacja** w kreatorze **Definicja produktu** kliknij **Zaawansowane**, aby wyświetlić panel **Zaawansowana identyfikacja**.
3. W polu **Cyfrowo podpisuje** wprowadź identyfikator wcześniej utworzonej aplikacji podpisującej i kliknij **OK**.
4. Zakończ kreatora i kontynuuj proces tworzenia pakietów i dystrybucji oprogramowania w programie Centrum Zarządzania.

Krok 8: zadania weryfikowania podpisu: tworzenie bazy certyfikatów *SIGNATUREVERIFICATION na systemach końcowych iSeries

Aby zgodnie ze scenariuszem weryfikować podpisy obiektów na systemach końcowych iSeries, każdy system musi mieć kopię odpowiedniego certyfikatu do weryfikowania podpisów w swojej bazie certyfikatów *SIGNATUREVERIFICATION. Jeśli obiekt był podpisany certyfikatem prywatnym, w bazie certyfikatów musi również znaleźć się kopia tego certyfikatu lokalnego ośrodka CA.

Aby utworzyć bazę certyfikatów *SIGNATUREVERIFICATION, wykonaj następujące czynności:

1. Uruchom program DCM.
2. W ramce nawigacji programu Menedżer certyfikatów cyfrowych wybierz **Tworzenie nowej bazy certyfikatów** i ***SIGNATUREVERIFICATION** jako nową bazę certyfikatów.

   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. Podaj hasło dla nowej bazy certyfikatów i kliknij **Kontynuuj**, aby ją utworzyć. Możesz teraz importować certyfikaty do bazy i korzystać z nich do weryfikowania podpisów obiektów.

Krok 9: zadania weryfikowania podpisu: importowanie certyfikatów

Aby weryfikować podpis na obiekcie, baza *SIGNATUREVERIFICATION musi zawierać kopię certyfikatu do weryfikowania podpisów. Jeśli certyfikat podpisujący jest prywatny, to w bazie certyfikatów musi znaleźć się również kopia certyfikatu lokalnego ośrodka CA, który go wystawił. W opisywanym scenariuszu obydwa certyfikaty zostały wyeksportowane do pliku, a plik przesłany do każdego systemu końcowego serwera iSeries.

Aby zaimportować te certyfikaty do bazy *SIGNATUREVERIFICATION, wykonaj następujące czynności:

1. W oknie nawigacji programu DCM kliknij **Wybór ośrodka certyfikacji** i wybierz ***SIGNATUREVERIFICATION** jako bazę certyfikatów do otwarcia.
2. Gdy pojawi się strona Baza certyfikatów i hasło, wpisz hasło bazy certyfikatów (określone przy tworzeniu tej bazy) i kliknij **Kontynuuj**.
3. Po odświeżeniu widoku ramki nawigacji wybierz **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Import certyfikatu**.
5. Jako typ certyfikatu wybierz **Ośrodek certyfikacji** i kliknij **Kontynuuj**.

   Uwaga: Przed zaimportowaniem prywatnego certyfikatu do weryfikowania podpisów należy zaimportować certyfikat lokalnego ośrodka CA, inaczej proces importu certyfikatu do weryfikowania podpisów nie powiedzie się.
6. Podaj pełną ścieżkę i nazwę dla pliku certyfikatu ośrodka CA i kliknij **Kontynuuj**. Pojawi się komunikat potwierdzający pomyślne zakończenie importu lub informacja o błędzie, jeśli proces nie powiódł się.
7. Ponownie wybierz zadanie **Importuj certyfikat**.
8. Jako typ certyfikatu wybierz **Sprawdzania podpisu** i kliknij **Kontynuuj**.
9. Podaj pełną ścieżkę i nazwę dla pliku certyfikatu do weryfikowania podpisów i kliknij **Kontynuuj**. Pojawi się komunikat potwierdzający pomyślne zakończenie importu lub informacja o błędzie, jeśli proces nie powiódł się.

System iSeries będzie teraz mógł weryfikować podpisy na obiektach, które zostały utworzone z odpowiednim certyfikatem podpisującym, podczas odtwarzania podpisanych obiektów.

Koncepcje związane z podpisywaniem obiektów

Przed skorzystaniem z możliwości podpisywania obiektów i weryfikacji podpisów serwera iSeries warto zapoznać się z niektórymi związanymi z tym koncepcjami:

Podpisy cyfrowe
Czym są podpisy cyfrowe i jaką zapewniają ochronę.

Obiekty do podpisywania
Opis, które obiekty serwera iSeries można podpisać i opis opcji podpisywania obiektów typu komendy (*CMD).

Przetwarzanie podpisywania obiektów
Opis procesu podpisywania obiektów i parametrów tego procesu.

Weryfikowanie podpisów
Opis procesu weryfikowania podpisu obiektu i parametrów tego procesu.

Podpisy cyfrowe

System OS/400 ma obsługę certyfikatów cyfrowych i możliwości cyfrowego ″podpisania″ obiektów. Podpis cyfrowy na obiekcie jest tworzony metodą kryptograficzną i działa jak osobisty podpis na dokumencie. Podpis cyfrowy stanowi świadectwo pochodzenia obiektu i daje możliwość sprawdzenia jego integralności. Właściciel certyfikatu cyfrowego ″podpisuje″ obiekt za pomocą klucza prywatnego certyfikatu. Odbiorca obiektu korzysta z klucza publicznego tego samego certyfikatu w celu deszyfrowania podpisu, co weryfikuje integralność podpisanego obiektu oraz nadawcę.

Obsługa podpisywania obiektów wspomaga tradycyjne narzędzia serwera iSeries, służące do kontroli uprawnień użytkowników do zmiany obiektów. Tradycyjne narzędzia nie mogą jednak ochronić obiektów przed nieuprawnioną modyfikacją podczas ich przesyłania poprzez Internet lub inne sieci niechronione. Ponieważ można wykryć, czy zawartość obiektu uległa zmianie od czasu jego podpisania, można również łatwo określić, czy w takich przypadkach można zaufać danemu obiektowi.

Podpis cyfrowy to zaszyfrowana suma danych w obiekcie. Obiekt i jego zawartość nie są zaszyfrowane przez podpis cyfrowy; zaszyfrowana jest tylko suma kontrolna, aby uniemożliwić dokonanie bez uprawnień zmian 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 może, zamiast użyć obiektu, skontaktować się z nadawcą i poprosić o przesłanie kopii podpisanego obiektu.

Podpis na obiekcie reprezentuje system, który podpisał ten obiekt, a nie konkretnego użytkownika tego systemu (chociaż użytkownik musi mieć odpowiednie uprawnienia, aby użyć certyfikatu do podpisania 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 podpisywania obiektów certyfikatów z ogólnie znanego publicznego ośrodka certyfikacji. 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 programu Menedżer certyfikatów cyfrowych (DCM) w celu poprowadzenia własnego ośrodka certyfikacji i wystawiania prywatnych certyfikatów do podpisywania obiektów. Korzystanie z prywatnych certyfikatów lokalnego ośrodka CA jest tańsze niż certyfikaty pochodzące od powszechnie znanego publicznego ośrodka CA.

Typy podpisów cyfrowych

Począwszy od wersji V5R2 można podpisywać obiekty typu komenda (*CMD) i wybierać pomiędzy dwoma typami podpisów tych obiektów: rdzenia obiektu i całego obiektu.

- **Podpis całego obiektu**
  Ten typ podpisu obejmuje wszystkie, w tym część mniej ważnych, bajty obiektu.

- **Podpis rdzenia obiektu**
  Ten typ podpisu obejmuje najważniejsze bajty obiektu *CMD. Nie obejmuje natomiast tych bajtów, które są narażone na częstsze zmiany. Umożliwia wprowadzenie pewnych zmian do komendy, bez naruszenia podpisu. Które bajty podpisywanego rdzenia obiektu są pominięte zależy od danego obiektu *CMD, na przykład podpisy rdzenia nie obejmują domyślnych parametrów. Przykłady zmian, które nie wpłyną na podpis rdzenia to:
  - zmiana wartości domyślnych komendy,
  - dodanie do komendy programu sprawdzania poprawności,
  - zmiana parametru Dozwolone środowisko wykonania,
  - zmiana parametru Zezwolenie na ograniczenie użytkowników.

Więcej informacji o tym, które obiekty serwera iSeries można podpisywać i które bajty obiektu *CMD obejmuje podpis rdzenia obiektu zawiera sekcja Obiekty do podpisywania.

Obiekty do podpisywania

Niezależnie od użytych do podpisywania metod, można podpisywać cyfrowo różne typy obiektów systemu OS/400. Podpisywać można dowolny obiekt (*STMF) przechowywany w systemowym zintegrowanym systemie plików, poza obiektami przechowywanymi w bibliotece. Jeśli do obiektu dołączony jest program w języku Java, to również on zostanie podpisany. W systemie plików QSYS.LIB można podpisywać tylko następujące obiekty: programy (*PGM), programy serwisowe (*SRVPGM), moduły (*MODULE), pakiety SQL (*SQLPKG), *FILE (tylko zbiory składowania) i komendy (*CMD).

Aby obiekt mógł być podpisany, musi znajdować się w systemie lokalnym. Na przykład w czasie pracy z serwerem Windows 2000 na serwerze Integrated xSeries Server for iSeries w zintegrowanym systemie plików dostępny jest system plików QNTC. Katalogi w tym systemie plików nie są widziane jako lokalne, gdyż zawierają pliki należące do systemu operacyjnego Windows 2000. Nie można też podpisywać pustych obiektów lub obiektów skompilowanych dla wersji systemu wcześniejszych niż wersja V5R1.

Podpisywanie obiektów typu komenda (*CMD)

Do podpisywania obiektów *CMD można wybrać jeden z dwóch typów podpisów. Można wybrać pomiędzy podpisaniem całego obiektu lub tylko jego rdzennej części. Jeśli podpisywany jest cały obiekt, podpis obejmuje wszystkie, w tym część mniej ważnych, bajty obiektu. Podpis całego obiektu obejmuje elementy zawarte w podpisie rdzenia obiektu.

Jeśli wybrane zostanie podpisywanie tylko rdzenia obiektu, chronione przez podpis będą tylko najważniejsze bajty, zaś bajty, które ulegają częstszym zmianom nie zostaną podpisane. Które bajty zostaną niepodpisane zależy od obiektu *CMD, ale można w podpisie zawrzeć między innymi określenie trybu, w którym obiekt jest poprawny lub określenie, czy obiekt ma prawo być uruchamiany. Na przykład podpisy rdzenia nie obejmują domyślnych parametrów obiektu *CMD. Umożliwia to wprowadzenie pewnych zmian do komendy, bez naruszenia jej podpisu. Przykłady zmian, które nie wpłyną na ten typ podpisu to:

- zmiana wartości domyślnych komendy,
- dodanie do komendy programu sprawdzania poprawności,
- zmiana parametru Dozwolone środowisko wykonania,
- zmiana parametru Zezwolenie na ograniczenie użytkowników.

Tabela przedstawia, które dokładnie bajty obiektu *CMD zostaną zawarte w podpisywanym rdzeniu obiektu.

Skład podpisywanego rdzenia obiektu dla obiektów *CMD

Część obiektu	Czy należy do podpisywanego rdzenia obiektu
Wartości domyślne komendy zmienione przez CHGCMDDFT	Nie są częścią podpisywanego rdzenia obiektu

Część obiektu	Czy należy do podpisywanego rdzenia obiektu
Program do przetwarzania komend z biblioteką	Zawsze jest częścią podpisywanego rdzenia obiektu
Zbiór źródłowy REXX z biblioteką	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Podzbiór źródłowy REXX	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Środowisko komend REXX z biblioteką	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Nazwa programu obsługi wyjścia REXX, biblioteki i kod wyjścia	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Program sprawdzania poprawności z biblioteką	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Poprawny tryb dla komendy	Nie jest częścią podpisywanego rdzenia obiektu
Dozwolone środowisko wykonania	Nie jest częścią podpisywanego rdzenia obiektu
Zezwolenie na ograniczenie użytkowników	Nie jest częścią podpisywanego rdzenia obiektu
Półka pomocy	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Panel grupowy pomocy z biblioteką	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Identyfikator pomocy	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Indeks wyszukiwania pomocy z biblioteką	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Biblioteka bieżąca	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Biblioteka produktu	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Program przesłaniający podpowiedzi i biblioteka	Włączany do podpisu, jeśli został określony dla komendy w momencie podpisywania, w przeciwnym razie nie jest częścią podpisywanego rdzenia obiektu
Tekst (opis)	Nie jest częścią podpisywanego rdzenia obiektu ani podpisu całego obiektu, gdyż nie jest przechowywany w obiekcie
Włączenie interfejsu GUI	Nie jest częścią podpisywanego rdzenia obiektu

Przetwarzanie podpisywania obiektów

Podczas podpisywania obiektów można dla tego procesu określić następujące opcje.

- **Przetwarzanie po wystąpieniu błędu**
  Pozwala określić, jakiego typu przetwarzania po wystąpieniu błędu powinna użyć aplikacja podczas

tworzenia podpisów na więcej niż jednym obiekcie. Do wyboru jest zatrzymanie podpisywania obiektów po wystąpieniu błędu lub kontynuacja podpisywania na pozostałych obiektach.

- **Podwójny podpis na obiekcie**
  Pozwala określić, jak aplikacja powinna obsłużyć proces podpisywania, jeśli obiekt jest podpisywany ponownie. Do wyboru jest zostawienie pierwotnego podpisu lub zastąpienie go nowym.
- **Obiekty w podkatalogach**
  Pozwala określić, jak aplikacja powinna obsłużyć podpisywane obiekty znajdujące się w podkatalogach. Do wyboru jest indywidualne podpisywanie przez aplikację obiektów we wszystkich podkatalogach lub podpisywanie tylko w katalogu głównym z wyłączeniem podkatalogów.
- **Zasięg podpisu obiektu**
  Podczas podpisywania obiektów *CMD można określić, czy podpisywany ma być cały obiekt, czy tylko jego rdzenna część.

Weryfikowanie podpisów

Przy weryfikowaniu podpisów można określić następujące opcje.

- **Przetwarzanie po wystąpieniu błędu**
  Pozwala określić, jakiego typu przetwarzania po wystąpieniu błędu powinna użyć aplikacja podczas weryfikowania podpisów na więcej niż jednym obiekcie. Do wyboru jest zatrzymanie weryfikowania podpisów po wystąpieniu błędu lub kontynuacja weryfikacji na pozostałych obiektach.
- **Obiekty w podkatalogach**
  Pozwala określić, jak aplikacja powinna obsłużyć podpisy weryfikowane na obiektach znajdujących się w podkatalogach. Do wyboru jest indywidualne weryfikowanie przez aplikację podpisów na obiektach we wszystkich podkatalogach lub weryfikowanie podpisów tylko dla obiektów w katalogu głównym z wyłączeniem podkatalogów.
- **Weryfikowanie podpisu rdzenia a weryfikowanie podpisu całości**
  Istnieją pewne reguły systemowe, określające jak system powinien w procesie weryfikacji obsłużyć podpisy rdzenia lub całego obiektu. Reguły są następujące:
  - Jeśli na obiekcie nie ma żadnego podpisu, proces weryfikujący zgłasza, że obiekt nie jest podpisany, a następnie weryfikuje kolejne przetwarzane obiekty.
  - Jeśli obiekt został podpisany przez zaufane źródło (IBM), to podpis musi być zgodny, inaczej proces weryfikacji nie powiedzie się. Jeśli podpis jest zgodny, to proces weryfikacji trwa nadal. Podpis jest zaszyfrowaną sumą danych w obiekcie, dlatego zakłada się, że podpis będzie zgodny, jeśli dane w obiekcie podczas weryfikowania są zgodne z danymi w obiekcie w czasie jego podpisywania.
  - Jeśli obiekt ma jakikolwiek zaufany podpis całego obiektu (zaufanie określane w oparciu o certyfikaty znajdujące się w bazie certyfikatów *SIGNATUREVERIFICATION), to przynajmniej jeden z tych podpisów musi być zgodny, inaczej proces weryfikacji nie powiedzie się. Jeśli przynajmniej jeden z podpisów całego obiektu jest zgodny, to proces weryfikacji trwa nadal.
  - Jeśli obiekt ma jakikolwiek zaufany podpis rdzenia obiektu, to przynajmniej jeden z podpisów musi być zgodny z certyfikatem z bazy certyfikatów *SIGNATUREVERIFICATION, inaczej proces weryfikacji nie powiedzie się. Jeśli przynajmniej jeden z podpisów rdzenia obiektu jest zgodny, to proces weryfikacji trwa nadal.

Wymagania wstępne dotyczące podpisywania obiektów i weryfikacji podpisów

Możliwości podpisywania obiektów i weryfikacji podpisów systemu OS/400 dostarczają silnych dodatkowych narzędzi służących do nadzorowania obiektów na serwerze iSeries. Aby skorzystać z tych możliwości, należy spełnić następujące wymagania wstępne.

Wymagania wstępne dotyczące podpisywania obiektów

W zależności od wymagań firmy i ochrony możesz wybrać spośród kilku metod podpisywania obiektów:

- użyj programu Menedżer certyfikatów cyfrowych (DCM),
- napisz program korzystający z funkcji API Sign Object,
- użyj funkcji Centrum Zarządzania programu iSeries Navigator do podpisania obiektów w trakcie tworzenia pakietów przeznaczonych do dalszej dystrybucji do systemów końcowych iSeries.

Wybór metody podpisywania obiektów zależy od wymagań firmy i oczekiwanej ochrony. Niezależnie jednak od planowanej metody podpisywania obiektów, należy spełnić pewne wymagania wstępne:

- Należy zrealizować wymagania wstępne niezbędne do zainstalowania i korzystania z programu Menedżer certyfikatów cyfrowych (DCM).
  - Następnie trzeba przy użyciu programu DCM utworzyć bazę certyfikatów *OBJECTSIGNING. Tworzenie bazy certyfikatów może być częścią procesu tworzenia lokalnego ośrodka CA lub częścią procesu zarządzania certyfikatami podpisującymi obiekty pochodzącymi od publicznego, internetowego ośrodka CA.
  - Baza certyfikatów *OBJECTSIGNING musi zawierać przynajmniej jeden certyfikat, który może być utworzony przez lokalny ośrodek CA lub otrzymany od publicznego internetowego ośrodka CA.
  - Należy użyć programu DCM do utworzenia przynajmniej jednej definicji aplikacji podpisującej obiekt, używanej do podpisywania obiektów.
  - Należy użyć programu DCM do przypisania określonego certyfikatu do definicji aplikacji podpisującej obiekt.
- Profil użytkownika serwera iSeries, wykorzystywany do podpisywania obiektów, musi mieć uprawnienia specjalne *ALLOBJ. Profil użytkownika serwera iSeries, wykorzystywany do tworzenia bazy certyfikatów *SIGNATUREVERIFICATION, musi mieć uprawnienia specjalne *SECADM i *ALLOBJ.

Wymagania wstępne dotyczące weryfikacji podpisów

Istnieje kilka metod, których możesz użyć do weryfikowania podpisów na obiektach:

- użyj programu Menedżer certyfikatów cyfrowych (DCM),
- napisz program korzystający z funkcji API Verify Object (QYDOVFYO),
- wybierz spośród komend na przykład komendę Sprawdzanie integralności obiektu (Check Object Integrity - CHKOBJITG).

Wybór metody weryfikacji podpisów zależy od wymagań firmy i ochrony. Niezależnie jednak od planowanej metody weryfikacji należy spełnić następujące wymagania wstępne:

- Należy zrealizować wymagania wstępne niezbędne do zainstalowania i korzystania z programu Menedżer certyfikatów cyfrowych (DCM).
- Należy utworzyć bazę certyfikatów *SIGNATUREVERIFICATION. W zależności od potrzeb, można skorzystać z dwóch metod. Można użyć programu Menedżer certyfikatów cyfrowych (DCM) do zarządzania certyfikatami do weryfikacji podpisów. Jeśli do podpisywania obiektów korzysta się z certyfikatów publicznych, można utworzyć bazę certyfikatów pisząc program korzystający z funkcji API Add Verifier (QYDOADDV).

  Uwaga: Funkcja ta tworzy bazę certyfikatów z domyślnym hasłem. Następnie należy użyć programu DCM do zmiany tego hasła, aby zapobiec nieuprawnionemu dostępowi do bazy certyfikatów.
- Baza *SIGNATUREVERIFICATION musi zawierać kopię certyfikatu, którym podpisano obiekty. Certyfikat można dodać do bazy na dwa sposoby. Można za pomocą programu DCM systemu podpisującego wyeksportować certyfikat do pliku i następnie, za pomocą tego samego programu na docelowym systemie weryfikującym, zaimportować certyfikat do bazy certyfikatów *SIGNATUREVERIFICATION. Można również, jeśli do podpisywania obiektów używa się certyfikatów publicznych, dodać certyfikat do bazy certyfikatów docelowego systemu weryfikującego za pomocą programu korzystającego z funkcji API Add Verifier.
- Baza *SIGNATUREVERIFICATION musi zawierać kopię certyfikatu ośrodka certyfikacji, z którego pochodzi certyfikat użyty do podpisania obiektów. Jeśli do podpisywania obiektów korzysta się z

certyfikatu publicznego, to baza certyfikatów docelowego systemu weryfikującego musi zawierać kopię certyfikatu żądanego ośrodka CA. Jeśli do podpisywania obiektów korzysta się z certyfikatu wystawionego przez lokalny ośrodek CA, to należy za pomocą programu DCM dodać na docelowym systemie weryfikującym kopię certyfikatu lokalnego ośrodka CA do bazy certyfikatów.

Uwaga: Ze względów bezpieczeństwa funkcja API Add Verifier nie pozwoli na dodanie do bazy certyfikatów *SIGNATUREVERIFICATION certyfikatu ośrodka certyfikacji. W momencie dodawania certyfikatu ośrodka certyfikacji do bazy certyfikatów system zakłada, że ośrodek CA jest zaufanym źródłem certyfikatów. W konsekwencji system traktuje certyfikat wystawiony przez ośrodek CA jako pochodzący z zaufanego źródła. Dlatego nie można korzystać z funkcji API w celu utworzenia programu instalacyjnego obsługi wyjścia w celu dodania certyfikatu ośrodka certyfikacji do bazy certyfikatów. Aby dodać certyfikat ośrodka CA do bazy certyfikatów, należy użyć programu Menedżer certyfikatów cyfrowych; takie rozwiązanie daje pewność, że sprawowana jest ręczna, dokładna kontrola nad ośrodkami CA, którym system ufa. Dzięki temu system nie może importować certyfikatów ze źródeł, których administrator świadomie nie określił jako zaufane.

Jeśli do podpisywania obiektów korzysta się z certyfikatu wystawionego przez lokalny ośrodek CA, to należy za pomocą programu DCM na serwerze iSeries, będącym lokalnym ośrodkiem CA, wyeksportować kopię tego certyfikatu do pliku. Następnie można użyć programu DCM na docelowym serwerze weryfikującym iSeries aby zaimportować certyfikat lokalnego ośrodka CA do bazy certyfikatów *SIGNATUREVERIFICATION. Aby zapobiec możliwym błędom, należy zaimportować ten certyfikat przed użyciem funkcji API Add Verifier do dodania certyfikatu do weryfikowania podpisów. Dlatego, jeśli korzysta się z certyfikatu wystawionego przez lokalny ośrodek CA, można uznać za łatwiejsze użycie programu DCM do importu do bazy certyfikatów zarówno certyfikatu ośrodka CA, jak i certyfikatu weryfikującego.

Jeśli nie chcesz, aby ktokolwiek mógł dodać certyfikat do bazy certyfikatów *SIGNATUREVERIFICATION korzystając z tej funkcji API, zablokuj tę funkcję w systemie. Aby zrealizować to zadanie, skorzystaj z systemowych narzędzi serwisowych (SST) umożliwiających ustawienie odrzucania zmian wprowadzonych w wartościach systemowych związanych z ochroną.

- Profil użytkownika serwera iSeries, wykorzystywany do weryfikacji podpisów, musi mieć uprawnienia specjalne *AUDIT. Profil użytkownika serwera iSeries, wykorzystywany do tworzenia bazy certyfikatów lub zmiany hasła dla tej bazy, musi mieć uprawnienia specjalne *SECADM i *ALLOBJ.

Zarządzanie podpisanymi obiektami

Począwszy od wersji V5R1 firma IBM podpisuje programy licencjonowane i poprawki PTF systemu OS/400, zaznaczając w ten sposób oficjalnie, że pochodzą one z firmy IBM i umożliwiając wykrycie ewentualnych zmian w obiektach systemowych. Partnerzy handlowi i inni sprzedawcy mogą także podpisywać dostarczane przez siebie aplikacje. Dlatego nawet jeśli nie podpisujesz samodzielnie obiektów, musisz wiedzieć, jak pracować z podpisanymi obiektami i jak one wpływają na rutynowe zadania administracyjne systemu.

Przede wszystkim podpisane obiekty wpływają na zadania składowania i odtwarzania, a dokładnie na to, jak obiekty są składowane i odtwarzane w systemie.

Wartości systemowe i komendy wpływające na podpisane obiekty
Wartości systemowe i komendy, których można używać do zarządzania podpisanymi obiektami lub których uruchomienie ma na nie wpływ.

Założenia związane ze składowaniem i odtwarzaniem podpisanych obiektów
Wpływ podpisanych obiektów na zadania składowania i odtwarzania w systemie.

Komendy sprawdzające kod w celu upewnienia się o integralności podpisu
Dokładniejsze informacje o wykorzystaniu komend weryfikujących podpisy obiektów do określenia integralności obiektu.

Wartości systemowe i komendy wpływające na podpisane obiekty

Aby efektywnie zarządzać podpisanymi obiektami, należy zrozumieć jak wartości systemowe i komendy wpływają na podpisane obiekty. Wartość systemowa **Weryfikowanie podpisów obiektów podczas odtwarzania** (QVFYOBJRST) określa, w jaki sposób różne komendy odtwarzania wpływają na podpisane obiekty i jak system obsłuży podpisane obiekty w trakcie operacji odtwarzania. W systemie iSeries nie istnieją komendy języka CL przeznaczone wyłącznie do pracy z podpisanymi obiektami. Jednak istnieją pewne wspólne komendy, których można użyć do zarządzania podpisanymi obiektami (lub do zarządzania obiektami infrastruktury umożliwiającymi podpisywanie obiektów). Inne komendy mogą niekorzystnie wpłynąć na podpisane obiekty w systemie, poprzez usunięcie podpisu z obiektu i tym samym zlikwidowanie ochrony, jakiej ten podpis dostarczał.

Wartości systemowe wpływające na podpisane obiekty

Wartość systemowa **Weryfikowanie podpisów obiektów podczas odtwarzania** (QVFYOBJRST), należąca do kategorii wartości systemowych dotyczących odtwarzania w systemie OS/400, określa, w jaki sposób komendy w systemie wpływają na podpisane obiekty. Ta wartość systemowa, dostępna poprzez program iSeries Navigator, steruje obsługą weryfikacji podpisów przez system podczas operacji odtwarzania. Ustawienia tej wartości systemowej, wraz z ustawieniami dwóch innych wartości systemowych wpływają na operacje odtwarzania w systemie. W zależności od wybranego ustawienia tej wartości, może ona zezwalać lub zabraniać odtwarzania obiektów na podstawie statusu ich podpisu (na przykład tego, czy obiekt nie jest podpisany, ma niepoprawny podpis, został podpisany przez zaufane źródło itp.) 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 ośrodka certyfikacji, któremu system ufa; system ignoruje inne ″niewiarygodne″ podpisy obiektów i traktuje te obiekty jako niepodpisane.

Istnieje kilka ustawień, których można użyć dla wartości systemowej QVFYOBJRST, począwszy od ignorowania wszystkich podpisów, aż do wymagania prawidłowych podpisów dla wszystkich obiektów odtwarzanych w systemie. Wartość ta dotyczy jedynie odtwarzanych obiektów wykonywalnych, takich jak programy (*PGM), komendy (*CMD), programy serwisowe (*SRVPGM), pakiety SQL (*SQLPKG) czy moduły (*MODULE). Dotyczy także obiektów plików strumieniowych (*STMF) powiązanych z programami w języku Java, utworzonymi za pomocą komendy Tworzenie programu Java (Create Java Program - CRTJVAPGM). Nie dotyczy natomiast plików systemu IFS ani zbiorów składowania (*SAV).

Więcej informacji o korzystaniu z tych i pozostałych wartości systemowych zawiera artykuł Wyszukiwanie wartości systemowych w Centrum informacyjnym.

Komendy języka CL wpływające na podpisane obiekty

Istnieje kilka komend języka CL umożliwiających pracę z podpisanymi obiektami lub mających wpływ na podpisane obiekty serwera iSeries. Można skorzystać z kilku komend do podglądania informacji o podpisie obiektu, sprawdzania podpisu na obiekcie i składowania oraz odtwarzania obiektów ochrony niezbędnych do weryfikowania podpisów. Ponadto istnieje grupa komend, których uruchomienie może usunąć podpis z obiektu, usuwając w ten sposób ochronę, jakiej ten podpis dostarczał.

Komendy służące do podglądania informacji o podpisie obiektu

- Komenda Wyświetlenie opisu obiektu (Display Object Description - DSPOBJD)
  Komenda pokazuje nazwy i atrybuty określonych obiektów w określonej bibliotece lub w określonych bibliotekach z listy bibliotek wątku. Za pomocą tej komendy można określić, czy obiekt został podpisany i przejrzeć informacje o podpisie.

- Komendy zintegrowanego systemu plików, Wyświetlenie dowiązań obiektu (Display Object Links - DSPLNK) i Praca z dowiązaniami obiektów (Work with Object Links - WRKLNK)
  Komend tych można użyć do wyświetlenia informacji o podpisie na obiekcie znajdującym się w zintegrowanym systemie plików.

Komendy służące do weryfikowania podpisów obiektów

- Komenda Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG)
  Umożliwia określenie, czy została naruszona integralność obiektów w systemie. Komendy tej można użyć do weryfikacji podpisów w podobny sposób, jak używa się programu antywirusowego do określenia, czy wirus uszkodził jakieś pliki lub inne obiekty w systemie. Więcej informacji o korzystaniu z tej komendy z podpisanymi obiektami zawiera artykuł Komendy sprawdzające kod i integralność podpisu.
- Komenda Sprawdzenie opcji produktu (Check Product Option - CHKPRDOPT)
  Komenda ta przedstawia różnice pomiędzy prawidłową a bieżącą strukturą oprogramowania. Na przykład pokaże błąd, jeśli z zainstalowanego produktu zostanie usunięty jakiś obiekt. Parametru CHKSIG można użyć do określenia, jak komenda powinna obsłużyć i zgłosić ewentualne problemy z podpisem danego produktu. Więcej informacji o korzystaniu z tej komendy z podpisanymi obiektami zawiera artykuł Komendy sprawdzające kod i integralność podpisu.
- Komenda Składowanie programu licencjonowanego (Save Licensed Program - SAVLICPGM)
  Komenda składuje kopie obiektów tworzących program licencjonowany. Składuje go w takiej postaci, z której może zostać odtworzony komendą Odtworzenie programu licencjonowanego (Restore Licensed Program - RSTLICPGM). Parametru CHKSIG można użyć do określenia, jak komenda powinna obsłużyć i zgłosić ewentualne problemy z podpisem danego produktu. Więcej informacji o korzystaniu z tej komendy z podpisanymi obiektami zawiera artykuł Komendy sprawdzające kod i integralność podpisu.
- Komenda Odtworzenie (Restore - RST)
  Komenda odtwarza kopię jednego lub większej liczby obiektów, z których można korzystać w systemie plików IFS. Umożliwia także odtworzenie baz certyfikatów i ich zawartości. Nie można jednak jej użyć do odtworzenia bazy certyfikatów *SIGNATUREVERIFICATION. Sposób obsługi przez tę komendę podpisanych obiektów jest określony przez ustawienie wartości systemowej Verify object signatures during restore (QVFYOBJRST).
- Komenda Odtworzenie biblioteki (Restore Library - RSTLIB)
  Komenda odtwarza bibliotekę lub grupę bibliotek składowanych komendą Składowanie biblioteki (Save Library - SAVLIB). Komenda odtwarza całą bibliotekę, włącznie z opisem biblioteki, opisem obiektu i zawartością obiektów w bibliotece. Sposób obsługi przez tę komendę podpisanych obiektów jest określony przez ustawienie wartości systemowej Verify object signatures during restore (QVFYOBJRST).
- Komenda Odtworzenie programu licencjonowanego (Restore Licensed Program - RSTLICPGM)
  Komenda ładuje i odtwarza programy licencjonowane dla instalacji początkowej lub instalacji nowej wersji. Sposób obsługi przez tę komendę podpisanych obiektów jest określony przez ustawienie wartości systemowej Verify object signatures during restore (QVFYOBJRST).
- Komenda Odtworzenie obiektu (Restore object - RSTOBJ)
  Komenda odtwarza jeden lub więcej obiektów pojedynczej biblioteki zapisanych na dyskietce, taśmie, nośniku optycznym lub w zbiorze składowania za pomocą pojedynczej komendy. Sposób obsługi przez tę komendę podpisanych obiektów jest określony przez ustawienie wartości systemowej Verify object signatures during restore (QVFYOBJRST).

Komendy do składowania i odtwarzania baz certyfikatów

- Komenda Składowanie (Save - SAV)
  Komenda umożliwia składowanie kopii jednego lub większej liczby obiektów, z których można korzystać w systemie plików IFS, włącznie z bazami certyfikatów. Nie można jednak jej użyć do składowania bazy certyfikatów *SIGNATUREVERIFICATION.
- Komenda Składowanie danych ochrony (Save Security Data - SAVSECDTA)
  Komenda umożliwia składowanie wszystkich informacji o ochronie bez potrzeby przenoszenia systemu w stan zastrzeżony. Komenda umożliwia składowanie bazy certyfikatów *SIGNATUREVERIFICATION wraz z zawartymi w niej certyfikatami. Nie składuje jednak innych baz certyfikatów.

- Komenda Składowanie systemu (Save System - SAVSYS)
  Komenda umożliwia składowanie kopii licencjonowanego kodu wewnętrznego i biblioteki QSYS w formacie zgodnym z instalacją serwera iSeries. Nie składuje obiektów z żadnej innej biblioteki. Umożliwia ponadto składowanie obiektów ochrony i konfiguracyjnych, które można również składować komendami SAVSECDTA i SAVCFG. Komenda umożliwia składowanie bazy certyfikatów *SIGNATUREVERIFICATION wraz z zawartymi w niej certyfikatami.
- Komenda Odtworzenie (Restore - RST)
  Umożliwia odtworzenie baz certyfikatów i ich zawartości. Nie można jednak jej użyć do odtworzenia bazy certyfikatów *SIGNATUREVERIFICATION.
- Komenda Odtworzenie profili użytkowników (Restore User Profiles - RSTUSRPRF)
  Komenda umożliwia odtworzenie podstawowych części profilu użytkownika lub ustawienie profili użytkowników składowanych za pomocą komend Składowanie systemu (Save System - SAVSYS) lub Składowanie danych ochrony (Save Security Data - SAVSECDTA). Za pomocą tej komendy można odtworzyć bazę certyfikatów *SIGNATUREVERIFICATION i ukryte hasła dla tej bazy oraz innych baz certyfikatów. Można odtworzyć bazę certyfikatów *SIGNATUREVERIFICATION bez odtwarzania informacji o profilach użytkowników podając *DCM jako wartość parametru SECDTA i *NONE jako wartość parametru USRPRF. Aby za pomocą tej komendy odtworzyć informacje o profilach użytkowników i bazy certyfikatów wraz z hasłami, należy podać *ALL jako parametr USRPRF.

Komendy służące do usuwania podpisów z obiektów

Korzystając z tych komend można usunąć podpis z obiektu. Usunięcie podpisu może spowodować problemy z obiektem, z którego podpis został usunięty. W ostateczności nie będzie można zweryfikować źródła obiektu jako zaufanego lub zweryfikować podpisu w celu wykrycia zmian w obiekcie. Należy używać tych komend tylko na utworzonych przez siebie podpisanych obiektach, a nie na obiektach otrzymanych od innych firm, na przykład od firmy IBM czy innego dostawcy. Jeśli istnieją podejrzenia, że komenda usunęła podpis obiektu, można użyć komendy Wyświetlenie opisu obiektu (Display Object Description - DSPOBJD) do sprawdzenia, czy podpis jest tam nadal, i do ponownego podpisania obiektu, jeśli będzie to konieczne.

Uwaga: Aby sprawdzić, czy komenda Składowanie (Save) straciła podpis obiektu, należy odtworzyć obiekt w innej bibliotece, niż był składowany (na przykład w bibliotece QTEMP). Można następnie użyć komendy DSPOBJD do sprawdzenia, czy obiekt składowany utracił swój podpis.

- Komenda Zmiana programu (Change Program - CHGPGM)
  Komenda zmienia atrybuty programu bez potrzeby jego ponownej kompilacji. Można ją także wykorzystać do wymuszenia ponownego utworzenia programu, nawet jeśli określone atrybuty są identyczne jak bieżące.
- Komenda Zmiana programu usługowego (Change Service Program - CHGSRVPGM)
  Komenda zmienia atrybuty programu serwisowego bez potrzeby jego ponownej kompilacji. Można ją także wykorzystać do wymuszenia ponownego utworzenia programu serwisowego, nawet jeśli określone atrybuty są identyczne jak bieżące.
- Komenda Usuwanie zawartości zbioru składowania (Clear Save File - CLRSAVF)
  Komenda usuwa zawartość zbioru składowania, wszystkie istniejące rekordy zbioru składowania, zmniejszając ilość wykorzystywanej przez ten zbiór pamięci.
- Komenda Składowanie (Save - SAV)
  Komenda składuje kopię jednego lub większej liczby obiektów, z których można korzystać w zintegrowanym systemie plików. Podczas korzystania z tej komendy, jeśli dla parametru TGTRLS zostanie podana wartość wersji wcześniejsza niż V5R2M0, można utracić podpis z obiektów typu komenda (*CMD). Dzieje się tak dlatego, że w wersjach systemu wcześniejszych niż V5R2 nie było możliwości podpisywania komend.
- Komenda Składowanie biblioteki (Save Library - SAVLIB)
  Komenda umożliwia składowanie kopii jednej lub większej liczby bibliotek. Podczas korzystania z tej komendy, jeśli dla parametru TGTRLS zostanie podana wartość wersji wcześniejsza niż V5R2M0, można utracić podpis z obiektów typu komenda (*CMD). Dzieje się tak dlatego, że w wersjach systemu wcześniejszych niż V5R2 nie było możliwości podpisywania komend.

- Komenda Składowanie obiektu (Save Object - SAVOBJ)
  Komenda składuje kopię pojedynczego obiektu lub grupy obiektów położonych w tej samej bibliotece. Podczas korzystania z tej komendy, jeśli dla parametru TGTRLS zostanie podana wartość wersji wcześniejsza niż V5R2M0, można utracić podpis z obiektów typu komenda (*CMD). Dzieje się tak dlatego, że w wersjach systemu wcześniejszych niż V5R2 nie było możliwości podpisywania komend.

Założenia związane ze składowaniem i odtwarzaniem podpisanych obiektów

Istnieje kilka wartości systemowych mających wpływ na operacje odtwarzania na serwerze iSeries. Tylko jedna z tych wartości systemowych, **verify object signatures during restore (QVFYOBJRST)**, określa, jak system obsługuje podpisane obiekty podczas ich odtwarzania. Ustawienia tej wartości systemowej pozwalają określić, jak proces odtwarzania obsługuje weryfikację obiektów bez podpisów lub obiektów, których podpisy są niepoprawne.

Niektóre komendy składowania i odtwarzania mają wpływ na podpisane obiekty lub określają, jak system obsługuje podpisane i niepodpisane obiekty podczas operacji składowania i odtwarzania. Aby lepiej zarządzać systemem i uniknąć potencjalnie możliwych problemów, należy być świadomym istnienia tych komend i ich wpływu na podpisane obiekty.

Następujące komendy mogą weryfikować podpisy na obiektach podczas operacji składowania i odtwarzania:

- Komenda Składowanie programu licencjonowanego (Save Licensed Program - SAVLICPGM)
- Komenda Odtworzenie (Restore - RST)
- Komenda Odtworzenie biblioteki (Restore Library - RSTLIB)
- Komenda Odtworzenie programu licencjonowanego (Restore Licensed Program - RSTLICPGM)
- Komenda Odtworzenie obiektu (Restore object - RSTOBJ)

Następujące komendy umożliwiają składowanie i odtwarzanie baz certyfikatów, które są istotne dla ochrony, gdyż zawierają certyfikaty używane do podpisywania obiektów i weryfikowania podpisów:

- Komenda Składowanie (Save - SAV)
- Komenda Składowanie danych ochrony (Save Security Data - SAVSECDTA)
- Komenda Składowanie systemu (Save System - SAVSYS)
- Komenda Odtworzenie (Restore - RST)
- Komenda Odtworzenie profili użytkowników (Restore User Profiles - RSTUSRPRF)

Niektóre komendy składowania, w zależności od użytych wartości parametrów, mogą usunąć podpis z obiektu umieszczanego na nośniku składowania, tym samym likwidując ochronę, jakiej dostarczał ten podpis. Na przykład *dowolna* operacja składowania, odnosząca się do obiektu typu komenda (*CMD), z docelową wersją systemu wcześniejszą niż V5R2M0, sprawia, że komenda zostanie składowana bez podpisu. Usunięcie podpisu może spowodować problemy z obiektami, z których podpis został usunięty. W ostateczności nie będzie można zweryfikować źródła obiektu jako zaufanego lub zweryfikować podpisu w celu wykrycia zmian w obiekcie. Należy używać tych komend tylko na utworzonych przez siebie podpisanych obiektach, a nie na obiektach otrzymanych od innych firm, na przykład od firmy IBM czy innego dostawcy.

Uwaga: Aby sprawdzić, czy komenda Składowanie (Save) straciła podpis obiektu, należy odtworzyć obiekt w innej bibliotece, niż był składowany (na przykład w bibliotece QTEMP). Można następnie użyć komendy DSPOBJD do sprawdzenia, czy obiekt składowany utracił swój podpis.

Należy mieć świadomość tej możliwości przy następujących komendach składowania (i przy komendach składowania ogólnie):

- Komenda Składowanie (Save - SAV)

- Komenda Składowanie biblioteki (Save Library - SAVLIB)
- Komenda Składowanie obiektu (Save Object - SAVOBJ)

Więcej informacji o wpływie tych komend na podpisane obiekty i podpisy obiektów w trakcie operacji składowania i odtwarzania zawiera artykuł Wartości systemowe i komendy mające wpływ na podpisane obiekty.

Komendy sprawdzające kod w celu upewnienia się o integralności podpisu

Do weryfikowania podpisów na obiektach można użyć programu Menedżer certyfikatów cyfrowych (DCM) lub funkcji API. Można także do tego celu użyć kilku komend. Korzysta się z nich w podobny sposób, jak z programu antywirusowego do określenia, czy wirus uszkodził jakieś pliki lub inne obiekty w systemie. Większość podpisów jest sprawdzana podczas odtwarzania lub instalowania obiektu na systemie, na przykład za pomocą komendy RSTLIB.

Do sprawdzenia podpisów na obiektach już znajdujących się w systemie, można użyć jednej z trzech komend. Jedna z nich, komenda Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) jest przeznaczona specjalnie do weryfikacji podpisów obiektów. Na sprawdzanie podpisów przez każdą z tych komend ma wpływ parametr CHKSIG. Umożliwia on sprawdzenie wszystkich typów obiektów, ignorowanie wszystkich podpisów lub sprawdzanie tylko takich obiektów, które mają podpisy. Ostatnia opcja jest wartością domyślną tego parametru.

Komenda Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG)

Komenda Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) umożliwia określenie, czy została naruszona integralność obiektów w systemie. Można za pomocą tej komendy sprawdzić naruszenie integralności obiektów należących do określonego profilu użytkownika, obiektów znajdujących się w miejscu o określonej nazwie ścieżki wszystkich obiektów w systemie. W protokole zostaje umieszczony wpis o naruszeniu integralności, jeśli nastąpiło jedno z następujących zdarzeń:

- Zostały zmienione atrybuty programu, komendy, obiektu modułu lub biblioteki.
- Podpis cyfrowy na obiekcie jest niepoprawny. Podpis jest zaszyfrowaną sumą danych w obiekcie, dlatego zakłada się, że podpis będzie zgodny i poprawny, jeśli dane w obiekcie podczas weryfikowania są zgodne z danymi w obiekcie w czasie jego podpisywania. Niepoprawny podpis jest określany przez porównanie zaszyfrowanej sumy tworzonej w momencie podpisywania obiektu i zaszyfrowanej sumy tworzonej w momencie weryfikowania podpisu. Proces weryfikacji podpisu porównuje te dwie wartości. Jeśli nie są identyczne, zawartość obiektu została zmieniona od czasu podpisania i zakłada się, że podpis jest niepoprawny.
- Obiekt ma niepoprawny atrybut domeny dla tego typu obiektu.

Jeśli komenda wykryje naruszenie integralności obiektu, to do protokołu bazy danych dodaje nazwę obiektu, nazwę biblioteki (lub ścieżki), typ obiektu, właściciela obiektu i rodzaj błędu. Komenda tworzy także pozycję protokołu w różnych innych przypadkach, nawet jeśli nie są one związane z naruszeniem integralności. Na przykład tworzona jest pozycja protokołu dla obiektów, które można podpisać, ale które nie mają podpisu cyfrowego, dla obiektów, których nie można sprawdzić i obiektów, które mają format, który wymagałby zmiany w bieżącej implementacji systemu (konwersji IMPI do RISC).

Wartość parametru CHKSIG określa, jak komenda obsługuje cyfrowe podpisy na obiektach. Jako wartość tego parametru można podać jedną z trzech wartości:

- *SIGNED – podanie tej wartości powoduje, że komenda sprawdza obiekty z podpisami cyfrowymi. Komenda tworzy pozycje protokołu dla każdego obiektu, który ma niepoprawny podpis. Jest to wartość domyślna.

- *ALL – podanie tej wartości powoduje, że komenda sprawdza wszystkie obiekty, które można podpisywać, aby określić, czy są one podpisane. Komenda tworzy pozycje protokołu dla każdego obiektu, który można podpisywać, a który nie ma podpisu lub ma niepoprawny podpis.
- *NONE – podanie tej wartości powoduje, że komenda nie sprawdza podpisów cyfrowych na obiektach.

Komenda Sprawdzenie opcji produktu (Check Product Option - CHKPRDOPT)

Komenda Sprawdzenie opcji produktu (Check Product Option - CHKPRDOPT) przedstawia różnice pomiędzy prawidłową a bieżącą strukturą oprogramowania. Na przykład pokaże błąd, jeśli z zainstalowanego produktu zostanie usunięty jakiś obiekt.

Wartość parametru CHKSIG określa, jak komenda obsługuje cyfrowe podpisy na obiektach. Jako wartość tego parametru można podać jedną z trzech wartości:

- *SIGNED – podanie tej wartości powoduje, że komenda sprawdza obiekty z podpisami cyfrowymi. Komenda weryfikuje podpisy na dowolnych podpisanych obiektach. Jeśli komenda wykryje, że podpis na obiekcie jest niepoprawny, wyśle komunikat do protokołu zadania i oznaczy produkt jako błędny. Jest to wartość domyślna.
- *ALL – podanie tej wartości powoduje, że komenda sprawdza wszystkie obiekty, które można podpisywać, aby określić, czy są one podpisane i weryfikuje te podpisy. Komenda wysyła komunikat do protokołu zadania dla każdego obiektu, który można podpisywać, a który nie ma podpisu, jednak nie oznaczy produktu jako błędnego. Jeśli komenda wykryje, że podpis na obiekcie jest niepoprawny, wyśle komunikat do protokołu zadania i oznaczy produkt jako błędny.
- *NONE – podanie tej wartości powoduje, że komenda nie sprawdza podpisów cyfrowych na obiektach.

Komenda Składowanie programu licencjonowanego (Save Licensed Program - SAVLICPGM)

Komenda Składowanie programu licencjonowanego (Save Licensed Program - SAVLICPGM) pozwala składować kopie obiektów tworzących program licencjonowany. Składuje go w takiej postaci, z której może zostać odtworzony komendą Odtworzenie programu licencjonowanego (Restore Licensed Program - RSTLICPGM).

Wartość parametru CHKSIG określa, jak komenda obsługuje cyfrowe podpisy na obiektach. Jako wartość tego parametru można podać jedną z trzech wartości:

- *SIGNED – podanie tej wartości powoduje, że komenda sprawdza obiekty z podpisami cyfrowymi. Komenda weryfikuje podpisy na dowolnych podpisanych obiektach, ale nie sprawdza niepodpisanych obiektów. Jeśli komenda wykryje, że podpis na obiekcie jest niepoprawny, wyśle komunikat do protokołu zadania, aby zidentyfikować produkt i składowanie nie powiedzie się. Jest to wartość domyślna.
- *ALL – podanie tej wartości powoduje, że komenda sprawdza wszystkie obiekty, które można podpisywać, aby określić, czy są one podpisane i weryfikuje te podpisy. Komenda wysyła komunikat do protokołu zadania dla każdego obiektu, który można podpisywać, a który nie ma podpisu; jednak proces składowania nie zostanie zakończony. Jeśli komenda wykryje, że podpis na obiekcie jest niepoprawny, wyśle komunikat do protokołu zadania i składowanie nie powiedzie się.
- *NONE – podanie tej wartości powoduje, że komenda nie sprawdza podpisów cyfrowych na obiektach.

Rozwiązywanie problemów z podpisanymi obiektami

Aby znaleźć informacje które pomogą w rozwiązywaniu najczęstszych problemów, na jakie można napotkać w trakcie pracy z podpisywaniem obiektów i weryfikacją podpisów serwera iSeries, skorzystaj z następującej tabeli.

Powszechne problemy z podpisywaniem obiektów

Problem	Możliwe rozwiązanie
Podczas korzystania z funkcji API Sign Object do podpisywania obiektów z domyślną wersją systemu V4R5 lub z wcześniejszą, proces podpisywania kończy się błędem i obiekt pozostaje niepodpisany (komunikat o błędzie CPFB721).	Dopiero od wersji V5R1 serwer iSeries obsługuje podpisywanie obiektów. Dla obiektów, które zwracają komunikat o błędzie CPFB721 trzeba w celu podpisania ponownie utworzyć te programy z docelową wersją systemu V5R1 lub nowszą.

Najczęściej spotykane problemy z weryfikacją podpisów

Problem	Możliwe rozwiązanie
Proces odtwarzania nie powiódł się dla obiektów bez podpisów.	Jeśli brak podpisu nie powinien niepokoić, należy sprawdzić, czy wartość systemowa QVFYOBJRST została ustawiona na 5. Wartość 5 określa, że niepodpisane obiekty nie będą odtwarzane. Należy zmienić tę wartość na 3 i spróbować ponowić odtwarzanie.
Proces odtwarzania dla podpisanych obiektów nie powiódł się.	Może się tak zdarzyć, jeśli baza certyfikatów *SIGNATUREVERIFICATION została przesłana do systemu, ale użyto programu DCM do zmiany hasła dla tej bazy. W takim przypadku certyfikaty zawarte w bazie nie mogą być użyte do weryfikowania podpisów na obiektach w czasie procesu odtwarzania. Należy użyć programu DCM i zmienić hasło bazy certyfikatów. Jeśli hasło jest nieznane, należy usunąć bazę certyfikatów, utworzyć ją ponownie i zmienić za pomocą programu DCM jej hasło.
Podczas odtwarzania lub instalowania produktu pojawia się błąd, podpis nie daje się weryfikować.	Jeśli podpis nie daje się poprawnie weryfikować, może to oznaczać, że obiekt został zmieniony od czasu podpisania. Jeśli ważna jest integralność obiektu, nie należy zmieniać wartości systemowej QVFYOBJRST ani podejmować innych działań w celu odtworzenia podejrzanego obiektu. Może to bowiem spowodować oszukanie ochrony zapewnianej przez weryfikację podpisów i umożliwić przedostanie się do systemu obiektu, który może spowodować uszkodzenia. Należy natomiast skontaktować się z osobą podpisującą obiekt, aby określić, jaką akcję podjąć w celu rozwiązania problemu.

Informacje związane z podpisywaniem obiektów i weryfikowaniem podpisu

Podpisywanie obiektów i weryfikacja podpisów są stosunkowo nową technologią ochrony. Oto krótka lista innych pomocnych źródeł informacji dla osób zainteresowanych szerszym zrozumieniem tych technologii i ich działania:

- **VeriSign Help Desk Web site**
  Serwis WWW firmy VeriSign udostępnia bogatą bibliotekę tematów związanych z certyfikatami cyfrowymi, takich jak podpisywanie obiektów, a także innych tematów związanych z ochroną w sieci Internet.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Dokumentacja techniczna firmy IBM, kładąca nacisk na udoskonalenia ochrony sieci w wersji V5R1. Dokumentacja zawiera wiele tematów, włącznie z opisem użycia możliwości podpisywania obiektów serwera iSeries, programu Menedżer certyfikatów cyfrowych itp.