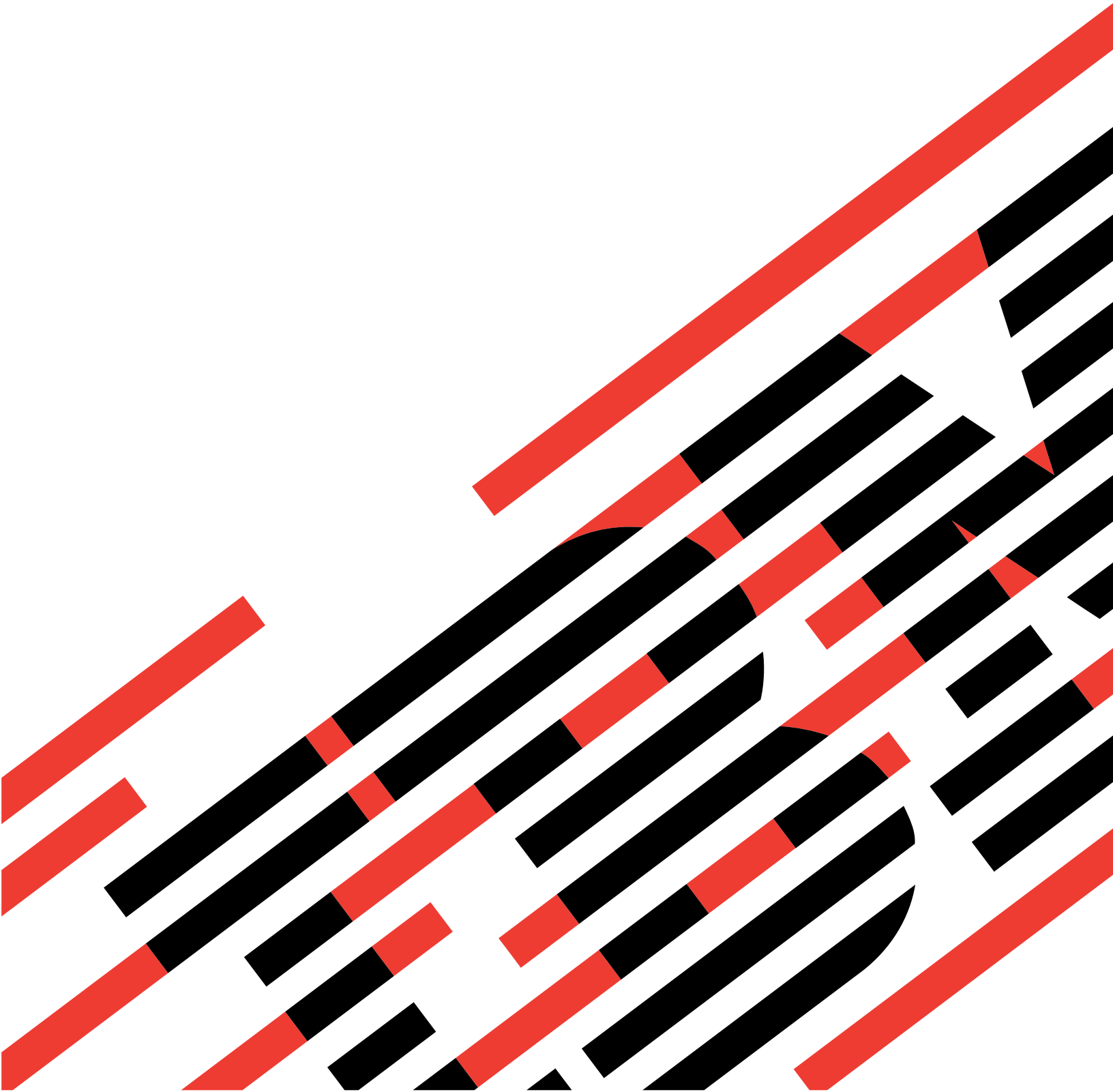
IBM

eserver

iSeries

Semnarea obiectelor şi verificarea semnăturilor



IBM

@server

iSeries

Semnarea obiectelor şi verificarea semnăturilor

Cuprins

Semnarea obiectelor şi verificarea semnăturilor

Semnarea obiectelor şi verificarea semnăturilor sunt capacităţi de securitate pe care le puteţi utiliza pentru a verifica integritatea unei varietăţi de obiecte iSeries. Utilizaţi o cheie privată a certificatului digital pentru a semna un obiect şi utilizaţi certificatul (care conţine cheia privată corespunzătoare) pentru a verifica semnătura digitală. O semnătură digitală asigură integritatea de timp şi conţinut a obiectului pe care îl semnaţi. Semnătura este o dovadă incontestabilă atât a autenticităţii, cât şi a autorizării. Aceasta poate fi utilizată pentru a arăta dovada originii şi a detecta modificările. Prin semnarea obiectului, dumneavoastră identificaţi sursa obiectului şi furnizaţi un mijloc pentru detectarea modificărilor aduse obiectului. Atunci când verificaţi semnătura unui obiect puteţi determina dacă s-au adus modificări conţinutului obiectului din momentul în care a fost semnat. Puteţi de asemenea verifica sursa semnăturii pentru a determina originea obiectului.

Puteţi implementa semnarea obiectelor şi verificarea semnăturilor pe iSeries prin:

- API-uri care să semneze obiecte şi să verifice semnăturile de pe obiecte în mod programat.
- Digital Certificate Manager (Managerul de certificare digitală) care să semneze obiectele şi să vizualizeze sau să verifice semnăturile obiectelor.
- Administrarea centrală a Navigatorului iSeries care să semneze obiecte ca parte a distribuirii pachetelor pentru a fi utilizate de alte sisteme.
- Comenzi CL, cum ar fi Check Object Integrity (CHKOBJITG - Verificarea integrităţii obiectelor) care să verifice semnăturile.

Pentru a afla mai multe despre aceste metode de semnare a obiectelor şi despre modul în care semnarea obiectelor poate îmbunătăţi politica dumneavoastră actuală de securitate, reconsultaţi aceste subiecte:

Ce e nou pentru V5R2
Utilizaţi aceste informaţii pentru a afla despre noile capacităţi de semnare a obiectelor şi de verificare a obiectelor iSeries, ca şi despre modificările aduse documentaţiei pentru această ediţie.

Tipăriţi acest subiect
Utilizaţi aceste informaţii pentru a tipări întregul subiect ca un fişier PDF.

Scenarii de semnare a obiectelor
Utilizaţi aceste informaţii pentru a revedea scenarii care ilustrează câteva situaţii tipice pentru utilizarea capacităţilor de semnare a obiectelor şi de verificare a semnăturilor iSeries. Fiecare scenariu furnizează şi task-urile de configurare pe care trebuie să le realizaţi pentru a implementa scenariul aşa cum este descris.

Concepte de semnare a obiectelor
Utilizaţi aceste concepte şi informaţiile referinţă pentru a afla mai multe despre semnăturile digitale şi despre funcţionarea proceselor de semnare a obiectelor şi de verificare a semnăturilor.

Cerinţe preliminare pentru semnarea obiectelor şi verificarea semnăturilor
Utilizaţi aceste informaţii pentru a afla despre cerinţele preliminare de configurare, ca şi despre alte consideraţii de planificare pentru semnarea obiectelor şi verificarea semnăturilor.

Gestiunea obiectelor semnate
Utilizaţi aceste informaţii pentru a afla despre comenzile şi variabilele sistem iSeries pe care le puteţi utiliza ca să lucraţi cu obiectele semnate şi despre modul în care obiectele semnate afectează procesele de copiere de siguranţă şi de recuperare.

Depanarea semnării obiectelor şi a verificării semnăturilor
Utilizaţi aceste informaţii pentru a afla modul de rezolvare a problemelor şi erorilor pe care le puteţi întâlni atunci când semnaţi obiecte şi verificaţi semnături.

Informaţii înrudite pentru semnarea obiectelor şi verificarea semnăturilor
Utilizaţi aceste informaţii pentru a găsi legături cu alte resurse pentru a afla mai multe despre semnarea obiectelor şi verificarea semnăturilor obiectelor.

Ce e nou pentru V5R2

Capacităţile de semnare a obiectelor şi de verificare a semnăturilor pentru iSeries au fost introduse pentru prima dată în V5R1. Totuşi, în V5R2 sunt disponibile noi funcţii şi îmbunătăţiri.

Funcţiile noi sau îmbunătăţite pentru semnarea obiectelor şi verificarea semnăturilor includ:

- Funcţiile de semnare a obiectelor din Administrarea centrală a Navigatorului **iSeries**
  Acum puteţi utiliza vrăjitorul Management Central Product Definition (Definire produs administrare centrală) pentru a semna obiectele pe care le împachetaţi pentru distribuire către sistemele terminaleiSerise.
- **Semnarea obiectelor comandă (*CMD)**
  Puteţi acum semna obiecte comandă (*CMD). Puteţi alege dacă să semnaţi un întreg obiect *CMD sau să semnaţi numai componentele nucleului unui obiect *CMD.
- **Noile API-uri de semnare şi verificare**
  Puteţi utiliza trei noi API-uri pentru a beneficia în mod programat de îmbunătăţirile capacităţilor OS/400& de semnare şi verificare.
  - API-ul de semnare buffer (QYDOSGNB, QydoSignBuffer)
    Acest API permite sistemului local să semneze digital un buffer pentru a atesta că buffer-ul este demn de încredere. După semnarea buffer-ului, sistemul întoarce semnătura digitală apelantului API-ului. De exemplu, puteţi utiliza acest API pentru a semna o parte a unui fişier XML şi a memora semnătura în altă parte a fişierului XML. Sau puteţi citi înregistrările fişierului bază de date într-un buffer şi utiliza API-ul pentru a le semna.
  - API-ul de verificare buffer (QYDOVFYB, QydoVerifyBuffer)
    Acest API permite sistemului local să verifice semnătura digitală pe un buffer semnat anterior.
  - API-ul de adăugare verificator (QYDOADDV, QydoAddVerifier)
    Acest API adaugă un certificat la memoria de certificare a sistemului *SIGNATUREVERIFICATION. Sistemul poate apoi utiliza certificatul adăugat pentru a verifica semnăturile pe obiectele pe care le-a creat certificatul respectiv. Verificarea semnăturii permite sistemului să verifice integritatea obiectelor semnate pentru a se asigura că obiectele nu au fost modificate din momentul în care au fost semnate. Dacă memoria de certificare nu există, acest API o creează şi adaugă certificatul.

    Notă: Din motive de securitate, acest API nu vă permite să inseraţi un certificat Certificate Authority (CA - Certificare autorizare) în memoria de certificare *SIGNATUREVERIFICATION. Când adăugaţi un certificat CA în memoria de certificare, sistemul consideră CA ca fiind o sursă de încredere de certificate. În consecinţă, sistemul tratează un certificat pe care l-a emis CA ca având originea într-o sursă de încredere. De aceea, nu puteţi utiliza API-ul pentru a crea un program de ieşire instalare care să insereze un certificat CA în memoria de certificare. Trebuie să utilizaţi Digital Certificate Manager (Managerul de certificare digitală) pentru a adăuga un certificat CA în memoria de certificare pentru a vă asigura că cineva trebuie să controleze, specific şi manual, CA-urile în care sistemul are încredere. Procedând astfel evitaţi posibilitatea ca sistemul să importe certificate din surse care nu au fost specificate cu bună ştiinţă de un administrator ca fiind de încredere.

    Dacă doriţi să împiedicaţi pe oricine să utilizeze acest API pentru a adăuga un certificat de verificare în memoria dumneavoastră de certificare *SIGNATUREVERIFICATION fără acceptul dumneavoastră, puteţi lua în considerare dezactivarea acestui API din sistemul dumneavoastră. Puteţi face acest lucru utilizând uneltele de servicii sistem (SST) pentru a nu permite modificări asupra variabilelor de sistem legate de securitate.

Anterior, informaţiile despre capacităţile de semnare a obiectelor şi de verificare a semnăturilor iSeries erau disponibile ca parte a subiectului Digital Certificate Management Information Center (Centrul de informare asupra gestiunii certificatelor digitale). Acum există metode suplimentare pe care le puteţi utiliza pentru semnarea obiectelor şi verificarea semnăturilor. În consecinţă, acest nou subiect al Centrului de informare este disponibil pentru a face mai uşoară utilizarea capacităţilor de semnare a obiectelor şi de verificare a semnăturilor prin furnizarea de informaţii centralizate despre utilizarea acestor capacităţi. Subiectul oferă informaţii îmbunătăţite şi complete, cum ar fi scenarii, pentru a vă ajuta să determinaţi când şi cum să utilizaţi aceste capacităţi pentru a vă suplimenta politica de securitate.

Informaţiile noi sau îmbunătăţite pentru acest subiect includ:

- Scenarii pe care le puteţi utiliza pentru a vă ajuta să determinaţi cum să folosiţi cel mai bine capacităţile de semnare a obiectelor şi de verificare a semnăturilor pentru a vă suplimenta politica de securitate.
- Secţiuni noi care descriu comenzile şi variabilele sistem pe care le puteţi utiliza pentru gestionarea obiectelor semnate pe sistemul dumneavoastră.
- Secţiuni noi care descriu planificarea şi alte informaţii conceptuale pentru semnarea obiectelor şi verificarea semnăturilor.

Pentru a găsi alte informaţii despre ce este nou sau modificat în această ediţie, consultaţi Notă către utilizatori .

Tipăriţi acest subiect

Pentru a vizualiza sau desărca versiunea PDF, selectaţi Semnarea obiectelor şi verificarea semnăturilor

(dimensiunea fişierului 350kB sau aproximativ 44 pagini).

Pentru a salva un PDF pe staţia dumnevoastră de lucru pentru vizualizare sau tipărire:

1. Deschideţi PDF-ul în browser-ul dumneavoastră (faceţi clic pe legătura de mai sus).
2. În meniul browser-ului dumneavoastră, faceţi clic pe **File (Fişier)**.
3. Faceţi clic pe **Save As... (Salvare ca...)**
4. Navigaţi în directorul în care doriţi să salvaţi PDF-ul.
5. Faceţi clic pe **Save (Salvare)**.

Dacă aveţi nevoie de Adobe Acrobat Reader pentru a vizualiza sau tipări PDF-ul, puteţi descărca o copie de la Site-ul web Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Scenarii de semnare a obiectelor

Serverul dumneavoastră iSeries oferă câteva metode diferite pentru semnarea obiectelor şi verificarea semnăturilor de pe obiecte. Modul în care optaţi să semnaţi obiecte şi modul în care lucraţi cu obiectele semnate variază în funcţie de nevoiele şi obiectivele dumneavoastră de afaceri şi de securitate. În unele cazuri, aţi putea avea nevoie numai să verificaţi semnăturile obiectelor de pe sistemul dumneavoastră pentru a vă asigura ca integritatea acelui obiect este intactă. În alte cazuri, puteţi opta să semnaţi obiecte pe care le distribuiţi altor persoane. Semnarea obiectelor permite altor persoane să identifice originea obiectelor şi să verifice integritatea obiectelor.

Metoda pe care alegeţi să o folosiţi depinde de mai mulţi factori. Scenariile furnizate în acest subiect descriu câteva dintre cele mai obişnuite obiective de semnare a obiectelor şi de verificare a semnăturilor în cadrul contextelor de afaceri tipice. Fiecare scenariu descrie de asemena şi cerinţele preliminare şi task-urile pe care trebuie să le realizaţi pentru a implementa scenariul aşa cum este descris. Revedeţi aceste scenarii pentru a vă ajuta să determinaţi modul în care puteţi utiliza capacităţile de semnare a obiectelor iSeries astfel încât să se potrivească cel mai bine cu necesităţile dumneavoastră de afaceri şi de securitate.

Scenariu: Utilizaţi Digital Certificate Manager (Managerul de certificare digitală) pentru a semna obiecte şi verifica semnături
Acest scenariu descrie o companie care doreşte să semneze obiecte aplicaţie vulnerabile pe serverul Web public al acesteia. Aceasta doreşte să poată determina mai uşor modificările neautorizate făcute asupra acestor obiecte. Pe baza nevoilor de afaceri şi a scopurilor de securitate ale companiei, acest scenariu descrie modul de utilizare a Managerului de certificare digitală (DCM) ca metodă primară pentru semnarea obiectelor şi verificarea semnăturilor obiectelor.

Scenariu: Utilizaţi API-uri pentru a semna obiecte şi verifica semnături
Acest scenariu descrie o companie de dezvoltare de aplicaţii care doreşte să semneze în mod programat aplicaţiile pe care le vinde. Aceasta doreşte să poată asigura clienţii că aplicaţia provine de la companie şi să le furnizeze un mijloc de detectare a modificărilor neautorizate asupra aplicaţiilor atunci când le instalează. Pe baza nevoilor de afaceri şi a scopurilor de securitate ale companiei, acest scenariu descrie modul de utilizare a API-ului Sign Object (Semnare obiect) şi a API-ului Add Verifier (Adăugare verificator) pentru semnarea obiectelor şi activarea verificării semnăturilor.

Scenariu: Utilizaţi Management Central (Administrarea centrală) pentru a semna obiecte
Acest scenariu descrie o companie care doreşte să semneze obiecte pe care le împachetează şi le distribuie mai multor servere iSeries. Pe baza nevoilor de afaceri şi a scopurilor de securitate ale companiei, acest scenariu descrie modul de utilizare a funcţiei Administrare centrală a Navigatorului iSeries pentru împachetarea şi semnarea obiectelor pe care aceştia le distribuie altor servere iSeries.

Scenariu: Utilizaţi DCM pentru a semna obiecte şi a verifica semnături

Situaţie

Ca administrator iSeries pentru MyCo., Inc. sunteţi responsabil pentru gestionarea celor două servere iSeries ale companiei dumneavoastră. Unul dintre aceste servere iSeries furnizează un site Web public pentru compania dumneavoastră. Dumneavoastră utilizaţi serverul iSeries de producţie internă al companiei dumneavoastră pentru a dezvolta conţinutul acestui site Web public şi pentru a transfera fişerele şi obiectele program pe serverul Web public după testarea acestora.

Severul Web public al companiei furnizează un site Web cu informaţii generale despre companie. Site-ul Web oferă de asemenea şi diferite formulare pe care clienţii le completează pentru înregistrarea produselor şi pentru a cere informaţii despre produse, anunţuri despre actualizarea produselor, locaţiile de distribuţie ale produselor şi aşa mai departe. Dumneavoastră sunteţi preocupat de vulnerabilitatea programelor cgi-bin care furnizează aceste formulare; ştiţi că ele ar putea fi modificate. De aceea, doriţi să puteţi verifica integritatea acestor obiecte program şi să detectaţi când s-au efectuat asupra lor modificări neautorizate. În consecinţă, v-aţi decis să semnaţi digital aceste obiecte pentru a îndeplini acest scop de securitate.

Aţi cercetat capacităţile de semnare a obiectelor OS/400 şi aţi aflat că există mai multe metode pe care le puteţi utiliza pentru a semna obiectele şi a verifica semnăturile obiectelor. Deoarece sunteţi responsabil pentru gestionarea unui număr redus de servere iSeries şi nu credeţi că va fi nevoie să semnaţi obiecte prea des, v-aţi decis să utilizaţi Digital Certificate Manager - Managerul de certificare digitală (DCM) pentru realizarea acestor task-uri. V-aţi decis de asemenea să creaţi o Autoritate de certificare locală (Local Certificate Authority - CA) şi să utilizaţi un certificat privat pentru semnarea obiectelor. Utilizarea unui certificat privat emis de o CA locală pentru semnarea obiectelor limitează costul utilizării acestei tehnologii de securitate deoarece nu trebuie să cumpăraţi un certificat de la o CA publică binecunoscută.

Acest exemplu serveşte ca o introducere utilă în paşii implicaţi în setarea şi utilizarea semnării obiectelor atunci când doriţi să semnaţi obiecte pe un număr redus de servere iSeries.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Semnarea obiectelor vă oferă un mijloc de verificare a integrităţii obiectelor vulnerabile şi de determinare mai uşoară a modificărilor aduse obiectelor după ce acestea au fost semnate. Acest lucru poate reduce unele depanări pe care le veţi face în viitor pentru a depista problemele aplicaţiilor şi alte probleme ale sistemului.
- Utilizarea interfeţei utilizator grafică (GUI) a DCM pentru semnarea obiectelor şi verificarea semnăturilor obiectelor vă permite duneavoastră şi altor persoane din companie să realizeze aceste task-uri rapid şi uşor.
- Utilizarea DCM pentru semnarea obiectelor şi verificarea semnăturilor reduce durata de timp pe care trebuie să o petreceţi pentru înţelegerea şi utilizarea semnării obiectelor ca parte a strategiei dumneavoastră de securitate.
- Utilizarea unui certificat emis de o Autoritate de certificare (CA) locală pentru semnarea obiectelor face ca semnarea obiectelor să fie mai puţin costisitoare de implementat.

Obiective

În acest scenariu, dumneavoastră doriţi să semnaţi digital obiecte vulnerabile, cum ar fi programe cgi-bin care generează formulare, pe serverul iSeries public al companiei dumneavoastră. Ca administrator de sistem la MyCo, Inc., doriţi să utilizaţi Managerul de certificare digitală (Digital Certificate Manager - DCM) pentru semnarea acestor obiecte şi verificarea semnăturilor de pe obiecte.

Obiectivele acestui scenariu sunt după cum urmează:

- Aplicaţiile companiei şi alte obiecte vulnerabile de pe serverul Web public (iSeries B) trebuie să fie semnate cu un certificat de la o CA locală pentru limitarea costurilor semnării aplicaţiilor.
- Administratorii de sistem şi alţi utilizatori desemnaţi trebuie să poată verifica cu uşurinţă semnăturile digitale de pe serverele iSeries pentru a verifica sursa şi autenticitatea obiectelor semnate de companie. Pentru a realiza acest lucru, fiecare server iSeries trebuie să aibă o copie atât a certificatului de verificare a semnăturii al companiei, cât şi a certificatului Autorităţii de certificare (CA) locale în fiecare memorie *SIGNATUREVERIFICATION a serverelor.
- Prin verificarea semnăturilor de pe aplicaţiile companiei şi de pe alte obiecte ale companiei, administratorii iSeries şi alţii pot detecta dacă conţinutul obiectelor s-a modificat după ce acestea au fost semnate.
- Administratorul de sistem trebuie să utilizeze DCM pentru semnarea obiectelor; administratorul de sistem şi alţii trebuie să poată utiliza DCM pentru verificarea semnăturilor obiectelor.

Detalii

Următoarea figură ilustrează procesul de semnare a obiectelor şi de verificare a semnăturilor pentru implementarea acestui scenariu:

Figura ilustrează următoarele puncte relevante pentru acest scenariu:

iSeries A

- iSeries A rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries A este serverul de producţie internă al companiei şi platforma de dezvoltare pentru serverul Web iSeries public (iSeries B).
- iSeries A are instalat un Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit pentru iSeries (5722–AC3).
- iSeries A are instalat şi configurat un Digital Certificate Manager - Manager de certificare digitală (OS/400 opţiune 34) şi Serverul HTTP IBM (5722–DG1).
- iSeries A se comportă ca Autoritatea de certificare locală (Local Certificate Authority - CA) şi certificatul de semnare a obiectelor se află pe acest sistem.

- iSeries A utilizează DCM pentru semnarea obiectelor şi este sistemul primar de semnare a obiectelor pentru aplicaţiile publice şi ale obiecte ale companiei.
- iSeries A este configurat pentru activarea verificării semnăturilor.

iSeries B

- iSeries B rulează OS/400 Versiune 5 Ediţie 1 (V5R1).
- iSeries B este serverul Web public extern al companiei din afara firewall-ului companiei.
- iSeries B are instalat un Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit (5722–AC3).
- iSeries B are instalat şi configurat Digital Certificate Manager - Manager de certificare digitală (OS/400 opţiune 34) şi Serverul HTTP IBM (5722–DG1).
- iSeries B nu operează o CA locală, nici nu semnează obiecte.
- iSeries B este configurat pentru activarea verificării semnăturilor utilizând DCM pentru crearea memoriei de certificare *SIGNATUREVERIFICATION şi pentru importarea verificării necesarea şi a certificatelor CA locală.
- DCM este utilizat pentru verificarea semnăturilor de pe obiecte.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:

1. Toate serverele iSeries îndeplinesc cerinţele pentru instalarea şi utilizarea Managerului de certificare digitală (DCM).
2. Nimeni nu a configurat sau utilizat anterior DCM sau unul din serverele iSeries.
3. Toate serverele iSeries au instalat cel mai înalt nivel al programului licenţiat Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit (5722-AC3).
4. Setarea implicită pentru variabila sistem de verificare a semnăturilor obiectelor în timpul restaurării (QVFYOBJRST) pe toate serverele iSeries din scenariu este 3 şi nu a fost modificată de la această setare. Setarea implicită asigură că serverul poate verifica semnăturile obiectelor pe măsură ce restauraţi obiectele semnate.
5. Administratorul de sistem pentru iSeries A trebuie să aibă autorizarea specială *ALLOBJ pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicaţia de semnare a obiectelor.
6. Administratorul de sistem sau oricine creează o memorie de certificare în DCM trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ.
7. Administratorul de sistem sau alţii de pe toate celelalte servere iSeries trebuie să aibă autorizarea specială *AUDIT pentru verificarea semnăturilor obiectelor.

Paşii de task

Există două seturi de task-uri pe care trebuie să le efectuaţi pentru a implementa acest scenariu: Un set de task-uri vă permite să configuraţi iSeries A ca o Autoritate de certificare (CA) locală şi să semnaţi şi să verificaţi semnăturile obiectelor. Al doilea set de task-uri vă permite să configuraţi iSeries B pentru verificarea semnăturilor pe care iSeries A le creează.

Paşii de task pentru **iSeries A**

Trebuie să efectuaţi fiecare dintre aceste task-uri pe iSeries A pentru a crea o CA locală privată şi pentru a semna obiecte şi verifica semnăturile obiectelor aşa cum descrie scenariul:

1. Efectuaţi toţi paşii preliminari pentru a instala şi configura toate produsele iSeries necesare.
2. Utilizaţi Managerul de certificare digitală (DCM) pentru a crea o Autoritate de certificare (CA) locală pentru emiterea unui certificat de semnare a obiectelor.

3. Utilizaţi DCM pentru a crea o definiţie de aplicaţie.
4. Utilizaţi DCM pentru a aloca un certificat definiţiei de aplicaţie care semnează obiecte.
5. Utilizaţi DCM pentru a semna obiectele program cgi-bin.
6. Utilizaţi DCM pentru a exporta certificatele pe care alte sisteme trebuie să le utilizeze pentru verificarea semnăturilor obiectelor. Trebuie să exportaţi într-un fişier atât o copie a certificatului CA locală, cât şi o copie a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor.
7. Transferaţi fişierele certificat pe serverul public iSeries al companiei (iSeries B) astfel încât dumneavoastră şi alte persoane să poată verifica semnăturile pe care iSeries A le creează.

Paşii de task pentru **iSeries B**

Dacă intenţionaţi să restauraţi obiectele semnate pe care le transferaţi pe serverul Web public în acest scenariu (iSeries B), trebuie să efectuaţi aceste task-uri de configurare a verificării semnăturilor pe iSeries B înainte de a putea transfera obiectele semnate. Configuraţia verificării semnăturilor trebuie să fie terminată înainte ca dumneavoastră să puteţi verifica semnăturile cu succes, pe măsură ce restauraţi obiectele semnate pe serverul Web public.

Pe iSeries B, trebuie să efectuaţi aceste task-uri pentru verificarea semnăturilor de pe obiecte aşa cum descrie acest scenariu:

8. Utilizaţi Managerul de certificare digitală (DCM) pentru a crea memoria de certificare *SIGNATUREVERIFICATION.
9. Utilizaţi DCM pentru a importa certificatul CA local şi certificatul de verificare a semnăturilor.
10. Utilizaţi DCM pentru a verifica semnăturile pe obiecte transferate.

Detalii de configurare

Efectuaţi următorii paşi de task pentru configurare şi utilizaţi Managerul de certificare digitală pentru semnarea obiectelor aşa cum descrie acest scenariu.

Pasul 1: Efectuaţi toţi paşii preliminari

Trebuie să efectuaţi toate task-urile preliminare pentru instalarea şi configurarea tuturor produselor iSeries necesare înainte de a putea realiza task-urile de configurare specifice pentru implementarea acestui scenariu.

Pasul 2: Creaţi o Autoritate de certificare locală pentru a emite un certificat privat de semnare a obiectelor

Atunci când utilizaţi Managerul de certificare digitală (DCM) pentru crearea unei Autorităţi de certificare locală (CA), procesul vă cere să completaţi o serie de formulare. Aceste formulare vă ghidează prin procesul de creare a CA şi de efectuare a altor task-uri necesare pentru începerea utilizării certificatelor digitale pentru Secure Sockets Layer (SSL), semnarea obiectelor şi verificarea semnăturilor. Deşi în acest scenariu nu trebuie să configuraţi certificate pentru SSL, trebuie să completaţi toate formularele din task pentru a configura sistemul să semneze obiecte.

Pentru a utiliza DCM la crearea şi operarea unei CA locale, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al DCM, selectaţi **Crearea unei Autorităţi de certificare (CA)** pentru a afişa o serie de formulare.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Completaţi toate formularele pentru acest task ghidat. Pe măsură ce efectuaţi acest task, trebuie să faceţi următoarele:

a. Să furnizaţi informaţii de identificare pentru CA locală.
b. Să instalaţi certificatul CA locală în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaşte CA locală şi să poată valida certificatele pe care CA locală le emite.
c. Să specificaţi datele de poliţă pentru CA locală a dumneavoastră.
d. Să utilizaţi noua CA locală pentru a emite un certificat server sau client pe care aplicaţiile dumneavoastră să le poată utiliza pentru conexiuni SSL.

   Notă: Deşi acest scenariu nu utilizează acest certificat, trebuie să îl creaţi înainte de a putea utiliza CA locală pentru emiterea certificatului de semnare a obiectelor de care aveţi nevoie. Dacă anulaţi task-ul fără a crea acest certificat, trebuie să vă creaţi certificatul de semnare a obiectelor şi memoria de certificare *OBJECTSIGNING în care acesta este memorat separat.
e. Să selectaţi aplicaţiile care pot utiliza certificatul server sau client pentru conexiuni SSL.

   Notă: Pentru scopurile acestui scenariu, nu selectaţi nici o aplicaţie şi faceţi clic pe **Continuare** pentru a afişa următorul formular.
f. Să utilizaţi noua CA locală pentru emiterea unui certificat de semnare a obiectelor pe care aplicaţiile îl pot utiliza pentru semnarea digitală a obiectelor. Acest subtask creează memoria de certificare *OBJECTSIGNING. Aceasta este memoria de certificare pe care o utilizaţi pentru gestionarea certificatelor de semnare a obiectelor.
g. Să selectaţi aplicaţiile care trebuie să aibă încredere în CA dumneavoastră locală.

   Notă: Pentru scopurile acestui scenariu, nu selectaţi nici o aplicaţie şi faceţi clic pe **Continuare** pentru a termina task-ul.

Acum că aţi creat o CA locală şi un certificat de semnare a obiectelor, trebuie să definiţi o aplicaţie de semnare a obiectelor care să utilizeze certificatul înainte de a putea semna obiecte.

Pasul 3: Creaţi o definiţie a aplicaţiei de semnare a obiectelor

După ce vă creaţi certificatul de semnare a obiectelor, trebuie să utilizaţi Managerul de certificare digitală (DCM) pentru definirea unei aplicaţii de semnare a obiectelor pe care să o utilizaţi pentru semnarea obiectelor. Definiţia aplicaţiei nu trebuie să se refere la o aplicaţie reală; definiţia aplicaţiei pe care o creaţi trebuie să descrie tipul sau grupul de obiecte pe care intenţionaţi să le semnaţi. Aveţi nevoie de definiţie pentru a putea avea un ID de aplicaţie asociat cu certificatul pentru activarea procesului de semnare.

Pentru a utiliza DCM la crearea unei definiţii a aplicaţiei de semnare a obiectelor, urmaţi aceşti paşi:
1. În cadrul de navigare, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***OBJECTSIGNING** ca memoria de certificare de deschis.
2. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atunci când aţi creat-o şi faceţi clic pe **Continuare**.
3. În cadrul de navigare, selectaţi **Gestiune aplicaţii** pentru a afişa o listă de task-uri.
4. Selectaţi **Adăugare aplicaţie** din lista de task-uri pentru afişarea unui formular pentru definirea aplicaţiei.
5. Completaţi formularul şi faceţi clic pe **Adăugare**.

Acum trebuie să alocaţi certificatul dumneavoastră de semnare a obiectelor aplicaţiei pe care aţi creat-o.

Pasul 4: Alocaţi un certificat definiţiei aplicaţiei de semnare a obiectelor

Pentru a aloca certificatul aplicaţiei dumneavoastră de semnare a obiectelor, urmaţi aceşti paşi:
1. În cadrul de navigare DCM, selectaţi **Gestiune certificate** pentru a afişa o listă de task-uri.

2. Din lista de task-uri, selectaţi **Alocare certificat** pentru afişarea unei liste de certificate pentru memoria de certificare curentă.
3. Selectaţi un certificat din listă şi faceţi clic pe **Alocare la aplicaţie** pentru a afişa o listă de definiţii de aplicaţii pentru memoria de certificare curentă.
4. Selectaţi una sau mai multe aplicaţii din listă şi faceţi clic pe **Continuare**. Este afişată o pagină de mesaj pentru a confirma alocarea certificatului sau pentru a oferi informaţiile de eroare dacă s-a produs o problemă.

Când terminaţi acest task, sunteţi gata să utilizaţi DCM pentru semnarea obiectelor program pe care serverul Web public al companiei (iSeries B) le va utiliza.

Pasul 5: Semnaţi obiectele program

Pentru utilizarea DCM la semnarea obiectelor program pentru utilizare pe serverul Web public al companiei (iSeries B), urmaţi aceşti paşi:

1. În cadrul de navigare, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***OBJECTSIGNING** ca memoria de certificare de deschis.
2. Introduceţi parola pentru memoria de certificare *OBJECTSIGNING şi faceţi clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune obiecte ce pot fi semnate** pentru afişarea unei liste de task-uri.
4. Din lista de task-uri, selectaţi **Semnarea unui obiect** pentru afişarea unei liste de definiţii de aplicaţii pe care le puteţi utiliza pentru semnarea obiectelor.
5. Selectaţi aplicaţia pe care aţi definit-o în pasul anterior şi faceţi clic pe **Semnarea unui obiect**. Este afişat un formular care vă permite să specificaţi locaţia obiectului pe care doriţi să-l semnaţi.
6. În câmpul furnizat, introduceţi calea şi numele de fişier complet determinate ale obiectului sau directorului de obiecte pe care doriţi să-l semnaţi şi faceţi clic pe **Continuare**. Sau, introduceţi o locaţie de director şi faceţi clic pe **Răsfoire** pentru a vedea conţinutul directorului pentru selectarea obiectelor de semnat.

   Notă: Trebuie să începeţi numele obiectului cu un slash sau veţi întâlni o eroare. Puteţi de asemenea utiliza anumite caractere wildcard pentru a descrie partea din director pe care doriţi să o semnaţi. Aceste carctere wildcard sunt asteriscul (*****), care specifică *orice număr de caractere*, şi semnul de întrebare(**?**), care specifică *orice caracter singular*. De exemplu, pentru semnarea tuturor obiectelor dintr-un anumit director, puteţi introduce /mydirectory/*; pentru semnarea tuturor programelor dintr-o anumită bibliotecă, puteţi introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteţi utiliza aceste caractere wildcard numai în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă doriţi să utilizaţi funcţia Răsfoire (Browse) pentru a vedea o listă cu conţinutul bibliotecii sau directorului, trebuie să introduceţi caracterul wildcard ca parte din numele căii înainte de a face clic pe **Răsfoire**.
7. Selectaţi opţiunile de procesare pe care doriţi să le utilizaţi pentru semnarea obiectului sau obiectelor selectate şi faceţi clic pe **Continuare**.

   Notă: Dacă doriţi să aşteptaţi rezultatele jobului, fişierul de rezultate se va afişa direct în browser-ul dumneavoastră. Rezultatele jobului curent sunt adăugate la sfârşitul fişierului de rezultate. În consecinţă, fişierul poate conţine rezultate din orice alte joburi anterioare, în plus faţă de rezultatele jobului curent. Puteţi utiliza câmpul de dată din fişier pentru a determina ce linii din fişier se aplică jobului curent. Câmpul de dată este în format AAAALLZZ. Primul câmp din fişier poate fi ID-ul de mesaj (dacă s-a produs o eroare în timpul procesării obiectului) sau câmpul de dată (care indică data la care a procesat jobul).
8. Specificaţi calea şi numele de fişier complet determinate care să fie utilizate pentru memorarea rezultatelor jobului pentru operaţia de semnare a obiectelor şi faceţi clic pe **Continuare**. Sau, introduceţi o locaţie de director şi faceţi clic pe **Răsfoire** pentru a vedea conţinutul directorului pentru a selecta un

fişier de memorare a rezultatelor jobului. Este afişat un mesaj care indică faptul că jobul a fost lansat pentru semnarea obiectelor. Pentru a vedea rezultatele jobului, consultaţi **QOBJSGNBAT** a jobului din istoricul de job.

Pentru a vă asigura că dumneavoastră şi alte persoane puteţi verifica semnăturile, trebuie să exportaţi certificatele necesare într-un fişier şi să transferaţi fişierul de certificare pe iSeries B. Trebuie de asemenea să efectuaţi toate task-urile de configurare a verificării semnăturilor pe iSeries B înainte de a transfera obiectele program semnate pe iSeries B. Configurarea verificării semnăturilor trebuie să fie încheiată înainte ca dumneavoastră să puteţi verifica cu succes semnăturile, pe măsură ce restauraţi obiectele semnate pe iSeries B.

Pasul 6: Exportaţi certificatele pentru a activa verificarea semnăturilor pe iSeries B

Semnarea obiectelor pentru protejarea integrităţii conţinutului necesită ca dumneavoastră şi alte persoane să aveţi un mijloc pentru verificarea autenticităţii semnăturii. Pentru verificarea semnăturilor obiectelor pe acelaşi sistem care semnează obiectele (iSeries A), trebuie să utilizaţi DCM pentru crearea memoriei de certificare *SIGNATUREVERIFICATION. Această memorie de certificare trebuie să conţină atât o copie a certificatului de semnare a obiectelor, cât şi o copie a certificatului CA, pentru CA care a emis certificatul de semnare.

Pentru a permite altor persoane să verifice semnătura, trebuie să le oferiţi o copie a certificatului care a semnat obiectul. Atunci când utilizaţi o Autoritate de certificare (CA) locală pentru emiterea certificatului, trebuie de asemenea să le oferiţi şi o copie a certificatului CA locală.

Pentru a utiliza DCM astfel încât să puteţi verifica semnături pe acelaşi sistem care semnează obiectele (iSeries A în acest scenariu), urmaţi aceşi paşi:

1. În cadrul de navigare, selectaţi **Creare memorie de certificare nouă** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de creat.
2. Selectaţi **Da** pentru copierea certificatelor existente de semnare a obiectelor în noua memorie de certificare ca certificate de verificare a semnăturilor.
3. Specificaţi o parolă pentru noua memorie de certificare şi faceţi clic pe **Continuare** pentru a crea memoria de certificare. Puteţi acum utiliza DCM pentru verificarea semnăturilor obiectelor pe acelaşi sistem pe care îl utilizaţi pentru semnarea obiectelor.

Pentru a utiliza DCM la exportarea unei copii a certificatului CA locală şi a unei copii a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor, astfel încât să puteţi verifica semnăturile obiectelor pe alte sisteme (iSeries B), urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Gestiune certificate**, iar apoi selectaţi task-ul **Exportare certificat**.
2. Selectaţi **Autoritate de certificare (CA)** şi faceţi clic pe **Continuare** pentru a afişa o listă a certificatelor CA pe care le puteţi exporta.
3. Selectaţi din listă certificatul CA locală pe care l-aţi creat mai devreme şi faceţi clic pe **Export**.
4. Specificaţi **Fişier** ca destinaţie de export şi faceţi clic pe **Continuare**.
5. Specificaţi o cale şi un nume de fişier complet determinate pentru certificatul CA locală şi faceţi clic pe **Continuare** pentru a exporta certificatul.
6. Faceţi clic pe **OK** pentru a ieşi din pagina de confirmare Export. Acum puteţi exporta o copie a certificatului de semnare a obiectelor.
7. Selectaţi din nou task-ul **Exportare certificat**.
8. Selectaţi **Semnare obiect** pentru a afişa o listă a certificatelor de semnare a obiectelor pe care le puteţi exporta.
9. Selectaţi certificatul corespunzător de semnare a obiectelor din listă şi faceţi clic pe **Exportare**.
10. Selectaţi **Fişier, ca certificat de verificare a semnăturilor** ca destinaţie şi faceţi clic pe **Continuare**.

11. Specificaţi o cale şi un nume de fişier complet determinate pentru certificatul de verificare a semnăturilor exportat şi faceţi clic pe **Continuare** pentru a exporta certificatul.

Acum puteţi transfera aceste fişier pe sistemele terminale iSeries pe care intenţionaţi să verificaţi semnăturile pe care le-aţi creat cu certificatul respectiv.

Pasul 7: Transferaţi fişierele de certificare pe serverul public iSeries B al companiei

Trebuie să transferaţi fişierele de certificare pe care le-aţi creat pe iSeries A, pe iSeries B, serverul Web public al companiei în acest scenariu, înainte de a le putea configura pentru verificarea obiectelor pe care le semnaţi. Puteţi utiliza câteva metode diferite pentru transferarea fişierelor de certificare. De exemplu, puteţi utiliza Protocolul de transfer fişiere (FTP) sau distribuţia de pachete a Administrării centrale pentru a transfera fişierele.

Pasul 8: Task-uri de verificare a semnăturilor: Creaţi memoria de certificare *SIGNATUREVERIFICATION

Pentru verificarea semnăturilor obiectelor pe iSeries B (serverul Web public al companiei), iSeries B trebuie să aibă o copie a certificatului corespunzător de verificare a semnăturilor în memoria de certificare *SIGNATUREVERIFICATION. Deoarece aţi utilizat un certificat emis de o CA locală pentru semnarea obiectelor, această memorie de certificare trebuie să conţină şi o copie a certificatului CA locală.

Pentru crearea memoriei de certificare *SIGNATUREVERIFICATION, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al Managerului de certificare digitală (DCM), selectaţi **Creare memorie de certificare nouă** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de creat.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular în timpul utilizării DCM, selectaţi semnul de întrebare (**?**) din partea de sus a paginii pentru accesarea ajutorului online.
3. Specificaţi o parolă pentru noua memorie de certificare şi faceţi clic pe **Continuare** pentru a crea memoria de certificare. Acum puteţi importa certificatele în memorie şi le puteţi utiliza pentru verificarea semnăturilor obiectelor.

Pasul 9: Task-uri de verificare a semnăturilor: Importaţi certificatele

Pentru a verifica semnătura de pe un obiect, memoria *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului de verificare a semnăturilor. Dacă certificatul de semnare este privat, această memorie de certificare trebuie să aibă şi o copie a certificatului Autorităţii de certificare (CA) locală care a emis certificatul de semnare. În acest scenariu, ambele certificate erau exportate într-un fişier şi acel fişier era transferat pe fiecare sistem terminal iSeries.

Pentru a importa aceste certificate în memoria *SIGNATUREVERIFICATION, urmaţi aceşti paşi:

1. În cadrul de navigare al DCM, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de deschis.
2. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atunci când aţi creat-o şi faceţi clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune certificate** pentru a afişa o listă de task-uri.
4. Din lista de task-uri, selectaţi **Importare certificat**.
5. Selectaţi **Autoritate de certificare (CA)** ca tipul certificatului şi faceţi clic pe **Continuare**.

   Notă: Trebuie să importaţi certificatul CA locală înainte de a importa un certificat privat de verificare a semnăturilor; altfel, procesul de importare pentru certificatul de verificare a semnăturilor va eşua.

6. Specificaţi calea şi numele de fişier complet determinate pentru fişierul de certificare CA şi faceţi clic pe **Continuare**. Este afişat un mesaj care confirmă că procesul de importare a reuşit sau care furnizează informaţiile de eroare dacă procesul a eşuat.
7. Selectaţi din nou task-ul **Importare certificat**.
8. Selectaţi **Verificare semnături** ca tipul de certificat de importat şi faceţi clic pe **Continuare**.
9. Specificaţi calea şi numele de fişier complet determinate pentru fişierul certificat de verificare a semnăturilor şi faceţi clic pe **Continuare**. Este afişat un mesaj care confirmă că procesul de importare a reuşit sau care furnizează informaţiile de eroare dacă procesul a eşuat.

Acum puteţi utiliza DCM pe iSeries B pentru a verifica semnăturile obiectelor pe care le-aţi creat cu certificatul de semnare corespunzător pe iSeries A.

Pasul 10: Task-uri de verificare a semnăturilor: Verificaţi semnăturile pe obiecte program

Pentru a utiliza DCM la verificarea semnăturilor pe obiecte program transferate, urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Selectarea unei memorii de certificare** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de deschis.
2. Introduceţi parola pentru memoria de certificare *SIGNATUREVERIFICATION şi faceţi clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune obiecte ce pot fi semnate** pentru afişarea unei liste de task-uri.
4. Din lista de task-uri, selectaţi **Verificare semnătură obiect** pentru a specifica locaţia obiectelor pentru care doriţi să verificaţi semnăturile.
5. În câmpul furnizat, introduceţi calea şi numele de fişier complet determinate ale obiectului sau directorului de obiecte pentru care doriţi să verificaţi semnăturile şi faceţi clic pe **Continuare**. Sau introduceţi o locaţie de director şi faceţi clic pe **Răsfoire** pentru a vedea conţinutul directorului pentru selectarea obiectelor pentru verificarea semnăturilor.

   Notă: Puteţi de asemenea utiliza anumite caractere wildcard pentru a descrie partea din director pe care doriţi să o verificaţi. Aceste caractere wildcard sunt asteriscul (*****), care specifică *orice număr de caractere*, şi semnul de întrebare (**?**), care specifică *orice caracter singular*. De exemplu, pentru semnarea tuturor obiectelor dintr-un anumit director, puteţi introduce /mydirectory/*; pentru semnarea tuturor programelor dintr-o anumită bibliotecă, puteţi introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteţi utiliza aceste caractere wildcard numai în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă doriţi să utilizaţi funcţia Răsfoire (Browse) pentru a vedea o listă cu conţinutul bibliotecii sau directorului, trebuie să introduceţi caracterul wildcard ca parte a numelui căii înainte de a face clic pe **Răsfoire**.
6. Selectaţi opţiunile de procesare pe care doriţi să le utilizaţi pentru verificarea semnăturilor pe obiectul sau obiectele selectate şi faceţi clic pe **Continuare**.

   Notă: Dacă doriţi să aşteptaţi rezultatele jobului, fişierul de rezultate se va afişa direct în browser-ul dumneavoastră. Rezultatele pentru jobul curent sunt adăugate la sfârşitul fişierului de rezultate. În consecinţă, fişierul poate conţine rezultate din orice alte joburi anterioare, în plus faţă de rezultatele jobului curent. Puteţi utiliza câmpul de dată din fişier pentru a determina ce linii din fişier se aplică jobului curent. Câmpul de dată este în format AAAALLZZ. Primul câmp din fişier poate fi ID-ul de mesaj (dacă s-a produs o eroare în timpul procesării obiectului) sau câmpul de dată (care indică data la care a procesat jobul).
7. Specificaţi calea şi numele de fişier complet determinate care să fie utilizate pentru memorarea rezultatelor jobului pentru operaţia de verificare a semnăturilor şi faceţi clic pe **Continuare**. Sau, introduceţi o locaţie de director şi faceţi clic pe **Răsfoire** pentru a vedea conţinutul directorului pentru selectarea unui fişier de memorare a rezultatelor jobului. Este afişat un mesaj care indică faptul că jobul a fost lansat pentru verificarea semnăturilor obiectelor. Pentru a vedea rezultatele jobului, consultaţi **QOBJSGNBAT** a jobului din istoricul de job.

Scenariu: Utilizaţi API-uri pentru semnarea obiectelor şi verificarea semnăturilor

Situaţie

Compania dumneavoastră (MyCo, Inc.) este un partener de afaceri iSeries care dezvoltă aplicaţii pentru clienţi. Ocupându-vă de dezvoltarea de software pentru companie, sunteţi responsabil de împachetarea acestor aplicaţii pentru distribuirea către clienţi. Momentan, utilizaţi programe pentru împachetarea unei aplicaţii. Clienţii pot comanda un compact disc (CD-ROM) sau pot vizita pagina dumneavostră de Web şi descărca aplicaţia.

Sunteţi la curent cu noutăţile din industrie, în special cu cele de securitate. În consecinţă, ştiţi că clienţii sunt preocupaţi în mod justificat de sursa şi conţinutul programelor pe care le primesc sau le descarcă. Există situaţii în care clienţii cred că primesc sau descarcă un produs de la o sursă de încredere care se dovedeşte a nu fi adevărata sursă a produsului. Uneori această confuzie face ca clienţii să instaleze un produs diferit de cel la care se aşteptau. Uneori produsul instalat se dovedeşte a fi un program dăunător sau care a fost modificat şi deteriorează sistemul.

Deşi aceste tipuri de probleme nu sunt obişnuite pentru clienţii iSeries, doriţi să vă asiguraţi clienţii că aplicaţiile pe care le obţin de la dumneavoastră provin cu adevărat de la compania dumneavoastră. Doriţi de asemenea să oferiţi clienţilor o metodă de verificare a integrităţii acestor aplicaţii, astfel încât ei să poată determina dacă aplicaţiile au fost modificate înainte de instalarea lor.

Pe baza cercetărilor dumneavoastră, v-aţi decis să puteţi utiliza capacităţile de semnare a obiectelor OS/400 pentru a vă atinge scopurile de securitate. Semnarea digitală a aplicaţiilor dumneavoastră permite clienţilor să verifice că compania dumneavoastră este sursa legitimă a aplicaţiei pe care o primesc sau o descarcă. Deoarece momentan vă împachetaţi aplicaţiile în mod programat, v-aţi decis să utilizaţi API-uri pentru a adăuga cu uşurinţă semnarea obiectelor la procesul dumneavoastră de împachetare existent. De asemenea vă decideţi să utilizaţi un certificat public pentru semnarea obiectelor, astfel încât să faceţi procesul de verificare a semnăturilor transparent pentru clienţii dumneavoastră atunci când îşi instalează produsul dumneavoastră.

Ca parte din pachetul aplicaţiei veţi include o copie a certificatului digital pe care l-aţi utilizat pentru semnarea obiectului. Când un client obţine pachetul aplicaţiei, el poate utiliza cheia publică a certificatului pentru verificarea semnăturii aplicaţiei. Acest proces permite clientului să identifice şi să verifice sursa aplicaţiei, asigurându-se în acelaşi timp că conţinutul obiectelor aplicaţiei nu a fost modificat din momentul semnării lor.

Acest exemplu serveşte ca o introducere utilă în paşii implicaţi în semnarea programată a obiectelor pentru aplicaţiile pe care le dezvoltaţi şi le împachetaţi pentru a fi utilizate de către alte persoane.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Utilizarea API-urilor pentru împachetarea şi semnarea obiectelor în mod programat reduce durata de timp pe care trebuie să o petreceţi pentru implementarea acestei securităţi.
- Utilizarea API-urilor pentru semnarea obiectelor pe măsură ce le împachetaţi reduce numărul de paşi pe care trebuie să îi efectuaţi pentru semnarea obiectelor, deoarece procesul de semnare face parte din procesul de împachetare.
- Semnarea unui pachet de obiecte vă permite să determinaţi mai uşor dacă obiectele au fost modificate după ce au fost semnate. Acest lucru poate reduce unele depanări pe care le veţi face în viitor pentru depistarea problemelor aplicaţiilor pentru clienţi.
- Utilizarea unui certificat de la o Autorizare de certificare (CA) publică binecunoscută pentru semnarea obiectelor vă permite să utilizaţi API-ul Adăugare verificator ca parte a unui program de ieşire în

programul de instalare al produsului dumneavoastră. Utilizarea acestui API vă permite să adăugaţi automat certificatul public pe care l-aţi utilizat la semnarea aplicaţiei pe sistemul clientului dumneavoastră. Acest lucru asigură clientului dumneavoastră transparenţa verificării semnăturilor.

Obiective

În acest scenariu, MyCo, Inc. doreşte să semneze automat aplicaţiile pe care le împachetează şi le distribuie clienţilor săi. Ocupându-vă de dezvoltarea producţiei de aplicaţii la MyCo, Inc., momentan dumneavoastră împachetaţi programat aplicaţiile pentru distribuirea către clienţi. În consecinţă, doriţi să utilizaţi API-urile iSeries pentru semnarea aplicaţiilor dumneavoastră şi ca clienţii iSeries să verifice programat semnătura în timpul instalării produsului.

Obiectivele acestui scenariu sunt după cum urmează:

- Persoana care se ocupă de dezvoltarea producţiei în cadrul companiei trebuie să poată semna obiecte utilizând API-ul Semnare obiect ca parte a unui proces existent de împachetare programată a aplicaţiilor.
- Aplicaţiile companiei trebuie să fie semnate cu un certificat public pentru a asigura clientului transparenţa procesului de verificare a semnăturii în timpul instalării produsului aplicaţie.
- Compania trebuie să poată utiliza API-urile iSeries pentru a adăuga în mod programat certificatul necesar de verificare a semnăturii în memoria de certificare a serverului clientului iSeries *SIGNATUREVERIFICATION. Compania trebuie să poată crea programat această memorie de certificare pe serverul iSeries al clientului ca parte din procesul de instalare a produsului, dacă aceasta nu există încă.
- Clienţii trebuie să poată verifica cu uşurinţă semnăturile digitale pe aplicaţia companiei după instalarea produsului. Clienţii trebuie să poată verifica semnătura astfel încât să fie siguri de sursa şi autenticitatea aplicaţiei semnate şi să poată de asemenea determina dacă au fost făcute modificări asupra aplicaţiei din momentul în care a fost semnată.

Detalii

Următoarea figură ilustrează procesul de semnare a obiectelor şi de verificare a semnăturilor pentru implementarea acestui scenariu:

Figura ilustrează următoarele puncte relevante pentru acest scenariu:

Sistemul central (iSeries A)

- iSeries A rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries A rulează programul de împachetare a produselor al persoanei care dezvoltă aplicaţia.
- iSeries A are instalat un Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit pentru iSeries (5722–AC3).
- iSeries A are instalat şi configurat un Digital Certificate Manager - Manager de certificare digitală (OS/400 opţiune 34) şi Serverul HTTP IBM (5722–DG1).
- iSeries A este sistemul primar de semnare a obiectelor pentru produsele aplicaţie ale companiei. Semnarea obiectelor produsului pentru distribuirea către clienţi este realizată pe iSeries A prin efectuarea acestor task-uri:
  1. Utilizarea API-urilor pentru semnarea produsului aplicaţie al companiei.
  2. Utilizarea DCM pentru exportarea certificatului de verificare a semnăturilor într-un fişier astfel încât clienţii să poată verifica obiectele semnate.
  3. Scrierea unui program pentru adăugarea certificatului de verificare produsului aplicaţie semnat.

4. Scrierea unui program de ieşire preinstalare pentru produsul care utilizează API-ul Adăugare verificator. Acest API permite procesului de instalare a produsului să adauge programat certificatul de verificare în memoria de certificare *SIGNATUREVERIFICATION pe serverul iSeries al clientului (iSeries B şi C).

Serverele iSeries B şi C ale clientului

- iSeries B rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries C rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries B şi C au instalat şi configurat Digital Certificate Manager - Managerul de certificare digitală (opţiune 34) şi Serverul HTTP IBM (5722–DG1).
- iSeries B şi C cumpără şi descarcă aplicaţii de pe site-ul Web al companiei de dezvoltare a aplicaţiilor (care deţine iSeries A).
- iSeries B şi C obţin o copie a certificatului de verificare a semnăturii MyCo atunci când procesul de instalarea a aplicaţiei MyCo creează memoria de certificare *SIGNATUREVERIFICATION pe fiecare dintre aceste servere iSeries ale clientului.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:

1. Toate serverele iSeries îndeplinesc cerinţele pentru instalarea şi utilizarea Managerului de certificare digitală (DCM).

   Notă: Îndeplinirea cerinţelor preliminare pentru instalarea şi utilizarea DCM este o cerinţă opţională pentru clienţi (iSeries B şi C în acest scenariu). Deşi API-ul Adăugare verificator creează memoria de certificare *SIGNATUREVERIFICATION ca parte din procesul de instalare a produsului, dacă este necesar, o creează cu o parolă implicită. Clienţii trebuie să utilizeze DCM pentru modificarea parolei implicite pentru protejarea acestei memorii de certificare împotriva accesului neautorizat.
2. Nimeni nu a configurat sau utilizat anterior DCM sau unul din serverele iSeries.
3. Toate serverele iSeries au instalat cel mai înalt nivel al programului licenţiat Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit (5722-AC3).
4. Setarea implicită pentru variabila sistem de verificare a semnăturilor în timpul restaurării (QVFYOBJRST) pe toate serverele iSeries din scenariu este 3 şi nu a fost modificată de la această setare. Setarea implicită asigură că serverul poate verifica semnăturile obiectelor pe măsură ce restauraţi obiectele semnate.
5. Administratorul de sistem pentru iSeries A trebuie să aibă autorizarea specială *ALLOBJ în profilul utilizator pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicaţia de semnare a obiectelor.
6. Administratorul de sistem sau oricine creează o memorie de certificare în DCM (inclusiv un program) trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ în profilul utilizator.
7. Administratorii de sistem sau alţii de pe toate celelalte servere iSeries trebuie să aibă autorizarea specială *AUDIT în profilul utilizator pentru verificarea semnăturilor obiectelor.

Paşii de task

Trebuie să efectuaţi fiecare dintre aceste task-uri pe iSeries A pentru semnarea obiectelor aşa cum descrie scenariul:

1. Efectuaţi toţi paşii preliminari pentru instalarea şi configurarea tuturor produselor iSeries necesare.
2. Utilizaţi DCM pentru crearea unei cereri de certificat pentru obţinerea unui certificat de semnare a obiectelor de la o Autoritate de certificare (CA) publică binecunoscută.
3. Uilizaţi DCM pentru crearea unei definiţii a aplicaţiei de semnare a obiectelor.

4. Utilizaţi DCM pentru importarea certificatului de semnare a obiectelor şi alocarea acestuia la definiţia aplicaţiei dumneavoastră de semnare a obiectelor.
5. Utilizaţi DCM pentru exportarea certificatului dumneavoastră de semnare a obiectelor ca certificat de verificare a semnăturilor astfel încât clienţii dumneavoastră să-l poată utiliza pentru verificarea semnăturilor de pe obiectele dumneavoastră aplicaţie.
6. Rescrieţi programul dumneavoastră de împachetare a aplicaţiilor pentru a include fişierul certificat de verificare a semnăturilor ca parte a produsului şi pentru a utiliza API-ul Semnare obiect pentru semnarea aplicaţiei dumneavoastră pe măsură ce o împachetaţi pentru distribuirea către clienţi.
7. Creaţi un program de ieşire preinstalare care utilizează API-ul Adăugare verificator ca parte din procesul dumneavoastră de împachetare a aplicaţiilor. Acest program de ieşire vă permite să creaţi memoria de certificare *SIGNATUREVERIFICATION şi să adăugaţi certificatul necesar de verificare a semnăturilor pe un server iSeries al unui client în timpul instalării produsului.
8. Faceţi clienţii să utilizeze DCM pentru resetarea parolei implicite pentru memoria de certificare *SIGNATUREVERIFICATION pe serverele lor iSeries.

Detalii de configurare

Efectuaţi următorii paşi de task pentru utilizarea API-urilor OS/400 pentru semnarea obiectelor aşa cum descrie acest scenariu.

Pasul 1: Efectuaţi toţi paşii preliminari

Trebuie să efectuaţi toate task-urile preliminare pentru instalarea şi configurarea tuturor produselor iSeries necesare înainte de a putea realiza task-urile de configurare specifice pentru implementarea acestui scenariu.

Pasul 2: Utilizaţi DCM pentru obţinerea unui certificat de la o CA publică binecunoscută

Acest scenariu presupune că nu aţi utilizat anterior Managerul de certificare digitală (DCM) pentru crearea şi gestionarea certificatelor. În consecinţă, trebuie să creaţi memoria de certificare *OBJECTSIGNING ca parte a procesului de creare a certificatului dumneavoastră de semnare a obiectelor. Această memorie de certificare, când este creată, furnizează task-urile de care aveţi nevoie pentru crearea şi gestionarea certificatelor de semnare a obiectelor. Pentru a obţine un certificat de la o Autoritate de certificare (CA) publică binecunoscută, utilizaţi DCM pentru crearea informaţiilor de identificare şi a perechii de chei publică-privată pentru certificat şi trimiteţi aceste informaţii către CA pentru obţinerea certificatului dumneavoastră.

Pentru a crea informaţiile de cerere a certificatului pe care trebuie să le furnizaţi CA publice binecunoscute, astfel încât să vă obţineţi certificatul de semnare a obiectelor, efectuaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al DCM, selectaţi **Creare memorie de certificare nouă** pentru a porni task-ul ghidat şi a completa o serie de formulare. Aceste formulare vă îndrumă prin procesul de creare a memoriei de certificare şi a unui certificat pe care să-l puteţi utiliza pentru semnarea obiectelor.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectaţi semnul de întrebare (**?**) din partea de sus a paginii pentru accesarea ajutorului online.
3. Selectaţi ***OBJECTSIGNING** ca memoria de certificare de creat şi faceţi clic pe **Continuare**.
4. Selectaţi **Da** pentru crearea unui certificat ca parte a creaţiei memoriei de certificare *OBJECTSIGNING şi faceţi clic pe **Continuare**.
5. Selectaţi **VeriSign sau altă Autoritare de certificare (CA)** ca semnatar al noului certificat şi faceţi clic pe **Continuare** pentru a afişa un formular care vă permite să oferiţi informaţii de identificare pentru noul certificat.
6. Completaţi formularul şi faceţi clic pe **Continuare** pentru a afişa o pagină de confirmare. Această pagină de confirmare afişează datele cererii pe care trebuie să le furnizaţi Autorităţii de certificare (CA) care vă

va emite certificatul. Datele Certificate Signing Request - Cererii de semnare a certificatului (CSR) constau din cheia publică şi alte informaţii pe care le-aţi specificat pentru noul certificat.

7. Copiaţi şi lipiţi cu atenţie datele CSR în formularul de cerere a certificatului, sau într-un fişier separat, pe care CA publică îl cere pentru solicitarea unui certificat. Trebuie să utilizaţi toate datele CSR, inclusiv liniile Început şi Sfârşit cerere certificat nou. Când ieşiţi din această pagină, datele se pierd şi nu le mai puteţi recupera.
8. Trimiteţi formularul de solicitare sau fişierul către CA pe care aţi ales-o pentru emiterea şi semnarea certificatului dumneavoastră.
9. Aşteptaţi ca CA să trimită înapoi certificatul semnat şi completat înainte de a continua cu următorul pas de task pentru scenariu.

Pasul 3: Creaţi o definiţie a aplicaţiei de semnare a obiectelor

Acum că aţi trimis cererea dumneavoastră de certificat unei CA publice binecunoscute, puteţi utiliza DCM pentru definirea unei aplicaţii de semnare a obiectelor pe care o puteţi utiliza la semnarea obiectelor. Definiţia aplicaţiei nu trebuie să se refere la o aplicaţie reală; definiţia aplicaţiei pe care o creaţi trebuie să descrie tipul sau grupul de obiecte pe care intenţionaţi să le semnaţi. Aveţi nevoie de definiţie pentru a putea avea un ID de aplicaţie asociat cu certificatul pentru activarea procesului de semnare.

Pentru a utiliza DCM la crearea unei definiţii a aplicaţiei de semnare a obiectelor, urmaţi aceşti paşi:

1. În cadrul de navigare, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***OBJECTSIGNING** ca memoria de certificare de deschis.
2. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atunci când aţi creat-o şi faceţi clic pe **Continuare**.
3. În cadrul de navigare, selectaţi **Gestiune aplicaţii** pentru a afişa o listă de task-uri.
4. Selectaţi **Adăugare aplicaţie** din lista de task-uri pentru afişarea unui formular pentru definirea aplicaţiei.
5. Completaţi formularul şi faceţi clic pe **Adăugare**.

Când primiţi înapoi certificatul semnat de la CA, puteţi aloca certificatul aplicaţiei pe care aţi creat-o.

Pasul 4: Importaţi certificatul public semnat şi alocaţi-l aplicaţiei de semnare a obiectelor

Pentru a importa certificatul dumneavoastră şi a-l aloca aplicaţiei pentru a activa semnarea obiectelor, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***OBJECTSIGNING** ca memoria de certificare de deschis.
3. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atunci când aţi creat-o şi faceţi clic pe **Continuare**.
4. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune certificate** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Importare certificat** pentru a începe procesul de importare a certificatului semnat în memoria de certificare.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectaţi semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
6. Selectaţi **Alocare certificat** din lista de task-uri **Gestiune certificate** pentru a afişa o listă de certificate pentru memoria de certificare curentă.
7. Selectaţi un certificat din listă şi faceţi clic pe **Alocare la aplicaţie** pentru a afişa o listă de definiţii de aplicaţii pentru memoria de certificare curentă.

8. Selectaţi aplicaţia dumneavoastră din listă şi faceţi clic pe **Continuare**. Este afişată o pagină cu un mesaj de confirmare pentru selecţia de alocare sau cu un mesaj de eroare dacă a apărut o problemă.

Când terminaţi acest task, sunteţi gata să semnaţi aplicaţii şi alte obiecte utilizând API-urile iSeries. Totuşi, pentru a vă asigura că dumneavoastră sau alte persoane puteţi verifica semnăturile, trebuie să exportaţi certificatele necesare într-un fişier şi să le transferaţi pe orice server iSeries care instalează aplicaţiile dumneavoastră semnate. Serverele iSeries ale clienţilor trebuie să poată utiliza certificatul pentru verificare semnăturilor pe aplicaţia dumneavoastră pe măsură ce aceasta se instalează. Puteţi utiliza API-ul Adăugare verificator ca parte din programul de instalare a aplicaţiei dumneavoastră pentru a face configurarea necesară a verificării de semnături pentru clienţii dumneavoastră. De exemplu, puteţi crea un program de ieşire preinstalare care apelează API-ul Adăugare verificator pentru configurarea serverelor iSeries ale clienţilor dumneavoastră.

Pasul 5: Exportaţi certificatele pentru a activa verificarea semnăturilor pe alte servere iSeries

Semnarea obiectelor necesită ca dumneavoastră şi alte persoane să aveţi un mijloc de verificare a autenticităţii semnăturilor şi să îl utilizaţi pentru a determina dacă au fost făcute modificări asupra obiectelor semnate. Pentru verificarea semnăturilor pe acelaşi sistem care semnează obiectele, trebuie să utilizaţi DCM pentru crearea memoriei de certificare *SIGNATUREVERIFICATION. Această memorie de certificare trebuie să conţină atât o copie a certificatului de semnare a obiectelor, cât şi o copie a certificatului CA, pentru CA care a emis certificatul de semnare.

Pentru a permite altor persoane să verifice semnătura, trebuie să le oferiţi o copie a certificatului care a semnat obiectul. Atunci când utilizaţi o Autoritate de certificare (CA) locală pentru emiterea certificatului, trebuie de asemenea să le oferiţi şi o copie a certificatului CA locală.

Pentru a utiliza DCM astfel încât să puteţi verifica semnături pe acelaşi sistem care semnează obiectele (iSeries A în acest scenariu), urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Creare memorie de certificare nouă** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de creat.
2. Selectaţi **Da** pentru copierea certificatelor existente de semnare a obiectelor în noua memorie de certificare ca certificate de verificare a semnăturilor.
3. Specificaţi o parolă pentru noua memorie de certificare şi faceţi clic pe **Continuare** pentru a crea memoria de certificare. Acum puteţi utiliza DCM pentru verificarea semnăturilor pe acelaşi sistem pe care îl utilizaţi pentru semnarea obiectelor.

Pentru a utiliza DCM la exportarea unei copii a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor, astfel încât alte persoane să poată verifica semnăturile obiectelor dumneavoastră, urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Gestiune certificate** şi apoi selectaţi task-ul **Exportare certificat**.
2. Selectaţi **Semnare obiecte** pentru a afişa o listă a certificatelor de semnare a obiectelor pe care le puteţi exporta.
3. Selectaţi certificatul corespunzător de semnare a obiectelor din listă şi faceţi clic pe **Exportare**.
4. Selectaţi **Fişier, ca certificat de verificare a semnăturilor** ca destinaţie şi faceţi clic pe **Continuare**.
5. Specificaţi o cale şi un nume de fişier complet determinate pentru certificatul de verificare a semnăturilor exportat şi faceţi clic pe **Continuare** pentru a exporta certificatul.

Acum puteţi adăuga acest fişier la pachetul de instalare a aplicaţiei pe care îl creaţi pentru produsul dumneavoastră. Utilizând API-ul Adăugare verificator ca parte din programul dumneavoastră de instalare, puteţi adăuga acest certificat în memoria de certificare *SIGNATUREVERIFICATION a clienţilor dumneavoastră. API-ul va crea şi memoria de certificare dacă aceasta nu există încă. Programul dumneavoastră de instalare poate apoi verifica semnătura de pe obiectele aplicaţiei dumneavoastră pe măsură ce le restaurează pe serverele iSeries ale clienţilor.

Pasul 6: Actualizaţi-vă programul de împachetare a aplicaţiilor pentru a utiliza API-uri iSeries la semnarea aplicaţiilor

Acum că aveţi fişierul cu certificatul de verificare a semnăturilor de adăugat la pachetul aplicaţiei dumneavoastră, puteţi utiliza API-ul Semnare obiect la scrierea sau editarea unei aplicaţii existente pentru semnarea bibliotecilor produsului pe măsură ce le împachetaţi pentru distribuirea către clienţi.

Pentru a vă ajuta la mai buna înţelegere a modului de utilizare a API-ului Semnare obiect ca parte din programul dumneavoastră de împachetare a aplicaţiilor, revedeţi următorul exemplu de cod: Acest cod exemplu, scris în C, nu este un program complet de semnare şi împachetare; este mai degrabă un exemplu al porţiunii dintr-un astfel de program care apelează API-ul Semnare obiect. Dacă doriţi să utilizaţi acest exemplu de program, modificaţi-l pentru a-l adapta nevoilor dumneavoastră specifice. Din motive de securitate, IBM vă recomandă să individualizaţi exemplul de program, în loc să utilizaţi valorile implicite furnizate.

Notă: IBM vă acordă o licenţă copyright neexclusivă pentru utilizarea tuturor exemplelor de coduri de programare din care puteţi genera funcţii similare adaptate nevoilor dumneavoastră specifice. Toate codurile exemplu sunt oferite de IBM numai pentru scopuri ilustrative. Aceste exemple nu au fost testate temeinic în toate condiţiile. De aceea, IBM nu poate garanta încredere, service sau funcţionare pentru aceste programe. Toate programele conţinute aici vă sunt oferite ″AŞA CUM SUNT″ fără nici un fel de garanţii. Garanţiile implicate de mercantibilitate şi portivire pentru un anumit scop sunt în mod expres neasumate.

Modificaţi acest cod pentru a-l adapta nevoilor dumneavoastră utilizând API-ul Semnare obiecte ca parte a unui program de împachetare pentru produsul aplicaţie al dumneavoastră. Trebuie să transmiteţi doi parametri acestui program: numele bibliotecii de semnat şi numele ID-ului aplicaţiei de semnare a obiectelor; ID-ul aplicaţiei este sensibil la majuscule, numele librăriei nu este sensibil la majuscule. Programul pe care îl scrieţi poate apela acest cod de mai multe ori dacă sunt utilizate mai multe biblioteci ca părţi ale produsului pe care îl semnaţi.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2002                                  */
/*                                                               */
/* Utilizaţi API-ul Semnare obiect                               */ /* pentru a semna una sau mai multe biblioteci
/*                                                               */
/* API-ul va semna digital toate obiectele dintr-o bibliotecă    */
/*                                                               */
/*                                                               */
/*                                                               */
/* Acest material conţine codul sursă de programare pentru a fi  */
/* consultat de dumneavoastră. Acest exemplu nu a fost testat    */
/* temeinic în toate condiţiile. De aceea, IBM nu poate garanta  */
/* încredere, service sau funcţionare pentru aceste programe.    */
/* Toate programele conţinute aici vă sunt oferite "AŞA CUM SUNT". */
/* GARANŢIILE IMPLICATE DE MERCANTIBILITATE ŞI POTRIVIRE PENTRU  */
/* UN ANUMIT SCOP SUNT ÎN MOD EXPLICIT NEASUMATE. IBM nu oferă   */
/* service pentru aceste programe şi fişiere.                    */
/*                                                               */
/*                                                               */
/*                                                               */
/* Parametrii sunt:                                              */
/*                                                               */
/*  char *   numele bibliotecii de semnat                        */
/*  char *   numele ID-ului aplicaţiei                           */
/*                                                               */

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

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

    /* parametri:

       char * biblioteca în care se semnează obiecte,
       char * identificatorul aplicaţiei cu care se semnează

     */

    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;    /* întoarce excepţii pentru orice eroare */


    /* ------------------------------------ */
    /* numelui căii constructului i se dă     */                                    /* numele bibliotecii
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* iniţializare nume bibliotecă */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* completarea numelui bibliotecii */

    /* construire parametru nume cale pentru apelul API */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* ---------------------------- */
    /* găsirea lungimii id aplicaţie */
    /* ---------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* ------------------------------- */
    /* semnarea tuturor obiectelor din  */                                        /* această bibliotecă
    /* ------------------------------- */
    QYDOSGNO  (path_name,             /* numele căii către obiect         */
               &path_length,      /* lungimea numelui căii         */
               "OBJN0100",            /* nume format                 */
               argv[2],               /* identificator (ID) aplicaţie */
               &applid_length,        /* lungime ID aplicaţie   */
               "1",                   /* înlocuirea semnăturii duplicat */
               multi_objects,         /* modul de tratare
                                            a obiectelor multiple      */
               &multiobj_length,      /* lungimea structurii obiectelor
                                         multiple de utilizat
                                       (0=fără structură obiecte multiple)*/
               &error_code);          /* cod de eroare                 */



       return 0;

 }
```

Pasul 7: Creaţi un program de ieşire preinstalare care utilizează API-ul Adăugare verificator

Acum că aveţi acces programat pentru semnarea aplicaţiilor dumneavoastră, puteţi utiliza API-ul Adăugare verificator ca parte a programului dumneavoastră de instalare pentru a crea produsul final pentru distribuire. De exemplu, aţi putea utiliza API-ul Adăugare verificator ca parte a programului de ieşire preinstalare pentru a vă asigura că certificatul este adăugat în memoria de certificare înainte de restaurarea obiectelor semnate ale aplicaţiei. Acest lucru permite programului dumneavoastră de instalare să verifice semnătura de pe obiectele aplicaţiei dumneavoastră pe măsură ce ele sunt restaurate pe serverul iSeries al clientului.

Notă: Din motive de securitate, acest API nu vă permite să inseraţi un certificat CA (Autoritate de certificare) în memoria de certificare *SIGNATUREVERIFICATION. Când adăugaţi un certificat CA în memoria de certificare, sistemul consideră CA ca fiind o sursă de certificate de încredere. În consecinţă, sistemul tratează certificatul pe care CA l-a emis ca având originea într-o sursă de încredere. De aceea, nu puteţi utiliza API-ul pentru crearea unui program de ieşire instalare pentru inserarea unui certificat CA în memoria de certificare. Trebuie să utilizaţi Managerul de certificare digitală pentru adăugarea unui certificat CA în memoria de certificare pentru a vă asigura că cineva trebuie să controleze, specific şi manual, CA-urile în care sistemul are încredere. Procedând astfel, evitaţi posibilitatea ca sistemul să importe certificate din surse care nu au fost specificate cu bună ştiinţă de un administrator ca fiind de încredere.

Dacă doriţi să împiedicaţi pe oricine să utilizeze acest API pentru a adăuga un certificat de verificare în memoria dumneavoastră de certificare *SIGNATUREVERIFICATION fără acceptul dumneavoastră, puteţi lua în considerare dezactivarea acestui API din sistemul dumneavoastră. Puteţi face acest lucru utilizând uneltele de servicii sistem (SST) pentru a nu permite modificări asupra variabilelor de sistem legate de securitate.

Pentru a vă ajuta la mai buna înţelegere a modului de utilizare a API-ului Adăugare verificator ca parte a programului dumneavoastră de instalare a aplicaţiei, revedeţi următorul exemplu de cod program de ieşire preinstalare. Acest cod exemplu, scris în C, nu este un program de ieşire preinstalare complet; este mai degrabă un exemplu al porţiunii dintr-un astfel de program care apelează API-ul Adăugare verificator. Dacă doriţi să utilizaţi acest exemplu de program, modificaţi-l pentru a-l adapta nevoilor dumneavoastră specifice. Din motive de securitate, IBM vă recomandă să individualizaţi exemplul de program, în loc să utilizaţi valorile implicite furnizate.

Notă: IBM vă acordă o licenţă copyright neexclusivă pentru utilizarea tuturor exemplelor de coduri de programare din care puteţi genera funcţii similare adaptate nevoilor dumneavoastră specifice. Toate codurile exemplu sunt oferite de IBM numai pentru scopuri ilustrative. Aceste exemple nu au fost testate temeinic în toate condiţiile. De aceea, IBM nu poate garanta încredere, service sau funcţionare pentru aceste programe. Toate programele conţinute aici vă sunt oferite ″AŞA CUM SUNT″ fără nici un fel de garanţii. Garanţiile implicate de mercantibilitate şi potrivire pentru un anumit scop sunt în mod expres neasumate.

Modificaţi acest cod pentru a-l adapta nevoilor dumneavoastră pentru utilizarea API-ului Adăugare verificator ca parte a unui program de ieşire preinstalare pentru a adăuga certificatul necesar de verificare a semnăturilor pe serverele iSeries aleclienţilor dumneavoastră pe măsură ce aceştia instalează produsul dumneavoastră.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2002                                  */
/*                                                               */
/* Utilizaţi API-ul Adăugare verificare pentru adăugarea unui    */
/* certificat în fişierul IFS specificat în memoria de           */                        /* certificare *SIGNATUREVE
/*                                                               */
/* API-ul va crea memoria de certificare dacă aceasta nu există. */
/* Dacă memoria de certificare este creată, i se va da o parolă  */
/* implicită care trebuie modificată cât mai curând utilizând DCM. */
/* Acest avertisment trebuie dat proprietarilor sistemului care  */
/* utilizează acest program.                                     */
/*                                                               */
/*                                                               */
```

```
/*                                                                  */
/* Acest material conţine codul sursă de programare pentru a fi     */
/* consultat de dumneavoastră. Acest exemplu nu a fost testat       */
/* temeinic în toate condiţiile. De aceea, IBM nu poate garanta     */
/* încredere, service sau funcţionare pentru aceste programe.       */
/* Toate programele conţinute aici vă sunt oferite "AŞA CUM SUNT".  */
/* GARANŢIILE IMPLICATE DE MERCANTIBILITATE ŞI POTRIVIRE PENTRU     */
/* UN ANUMIT SCOP SUNT ÎN MOD EXPLICIT NEASUMATE. IBM nu oferă      */
/* service pentru aceste programe şi fişiere.                       */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametrii sunt:                                                 */
/*                                                                  */
/*  char *   numele căii la fişierul IFS care deţine certificatul   */
/*  char *   eticheta de atribuit certificatului                    */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* ---------------------------------------------------------------- */

#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];

    /* găsirea lungimii numelui căii */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* găsirea lungimii etichetei certificatului */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;     /* întoarce excepţii pentru orice eroare  */

    QydoAddVerifier (pathname,         /* numele căii de clasat cu certificatul */
                     &pathname_length, /* lungimea numelui căii             */
                     "OBJN0100",       /* nume format                       */
                     certlabel,        /* etichetă certificat               */
                     &cert_label_length, /* lungimea etichetei certificatului */
                     &error_code);     /* cod de eroare                       */

    return 0;
}
```

Cu aceste task-uri efectuate, puteţi să vă împachetaţi aplicaţia şi să o trimiteţi clienţilor dumneavoastră. Când aceştia instalează aplicaţia dumneavoastră, obiectele semnate ale aplicaţiei sunt verificate ca parte a procesului de instalare. La o dată ulterioară, clienţii pot utiliza Managerul de certificare digitală (DCM) pentru verificarea semnăturii de pe obiectele aplicaţiei dumneavoastră. Acest lucru permite clienţilor dumneavoastră să determine că sursa aplicaţiei este de încredere şi să determine ce modificări s-au produs din momentul în care aţi semnat aplicaţia.

Notă: S-ar putea ca programul dumneavoastră de instalare să fi creat memoria de certificare *SIGNATUREVERIFICATION cu o parolă implicită pentru clientul dumneavoastră. Ar fi necesar să vă sfătuiţi clienţii dumneavoastră să utilizeze DCM la resetarea parolei pentru memoria de certificare cât mai curând posibil pentru a o proteja de accesul neautorizat.

Pasul 8: Sfătuiţi clienţii să reseteze parola implicită pentru memoria de certificare *SIGNATUREVERIFICATION

S-ar putea ca API-ul Adăugare verificator să fi creat memoria de certificare *SIGNATUREVERIFICATION ca parte a procesului de instalare a produsului pe serverul iSeries al clientului dumneavoastră. Dacă API-ul a creat memoria de certificare, a creat o parolă implicită pentru aceasta. În consecinţă, ar trebui să vă sfătuiţi clienţii să utilizeze DCM la resetarea acestei parole pentru a proteja memoria de certificare împotriva accesului neautorizat.

Sfătuiţi clienţii dumneavoastră să efectueze aceşi paşi pentru a reseta parola memoriei de certificare *SIGNATUREVERIFICATION:

1. Porniţi DCM.
2. În cadrul de navigare, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de deschis.
3. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atunci când aţi creat-o şi faceţi clic pe **Continuare**.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectaţi semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
4. Specificaţi o nouă parolă pentru memorie, introduceţi-o din nou pentru confirmare, selectaţi poliţa de expirare a parolei pentru memoria de certificare şi faceţi clic pe **Continuare**.

Scenariu: Utilizaţi Management Central (Administrarea centrală) pentru a semna obiecte

Situaţie

Compania dumneavoastră (MyCo, Inc.) dezvoltă aplicaţii pe care le distribuie mai multor servere iSeries în mai multe locaţii din cadrul companiei. Ca administrator de reţea, dumneavoastră sunteţi responsabil pentru a asigura faptul că aceste aplicaţii sunt instalate şi actualizate pe toate serverele iSeries ale companiei. Momentan utilizaţi funcţiile de Management Central (Administrare centrală) ale Navigatorului iSeries pentru a împacheta şi distribui cu mai multă uşurinţă aceste aplicaţii şi pentru a realiza alte task-uri administrative de care sunteţi răspunzător. Totuşi, depistarea şi corectarea problemelor cu aceste aplicaţii durează mai mult timp decât aţi dori, din cauza modificărilor neautorizate făcute asupra obiectelor. În consecinţă, doriţi să asiguraţi mai bine integritatea acestor obiecte prin semnarea lor digitală.

Aţi cercetat capacităţile de semnare a obiectelor ale OS/400 şi aţi aflat că, începând cu V5R2, Administrarea centrală vă permite să semnaţi obiecte atunci când le împachetaţi şi le distribuiţi. Utilizând Administrarea centrală puteţi îndeplini eficient şi relativ uşor scopurile de securitate ale companiei dumneavoastră. Vă decideţi de asemenea să creaţi o Autoritate de certificare (CA) locală şi să o utilizaţi pentru emiterea unui certificat de semnare a obiectelor. Utilizarea unui certificat emis de o CA locală pentru semnarea obiectelor limitează costul utilizării acestei tehnologii de securitate deoarece nu trebuie să cumpăraţi un certificat de la o CA publică binecunoscută.

Acest exemplu serveşte ca o introducere utilă în paşii implicaţi în configurarea şi utilizarea semnării obiectelor pentru aplicaţii pe care le distribuiţi mai multor servere iSeries ale companiei.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Utilizarea Administrării centrale pentru împachetarea şi semnarea obiectelor reduce durata de timp pe care trebuie să o petreceţi pentru distribuirea obiectelor semnate către serverele iSeries ale companiei dumneavoastră.
- Utilizarea Administrării centrale pentru semnarea obiectelor reduce numărul de paşi pe care trebuie să îi efectuaţi pentru semnarea obiectelor deoarece procesul de semnare face parte din procesul de împachetare.
- Semnarea unui pachet de obiecte vă permite să determinaţi mai uşor dacă obiectele au fost modificate după ce au fost semnate. Acest lucru poate reduce unele depanări pe care le veţi face în viitor pentru depistarea problemelor aplicaţiilor.
- Utilizarea unui certificat emis de o Autoritate de certificare (CA) locală pentru semnarea obiectelor face ca semnarea obiectelor să fie mai puţin costisitoare de implementat.

Obiective

În acest scenariu, MyCo, Inc. doreşte să semneze digital aplicaţiile pe care le distribuie mai multor servere iSeries în cadrul companiei. Ca administrator de reţea la MyCo, Inc., deja utilizaţi Administrarea centrală pentru câteva task-uri administrative iSeries. În consecinţă, doriţi să extindeţi utilizarea curentă a Administrării centrale pentru semnarea aplicaţiilor companiei pe care le distribuiţi altor servere iSeries.

Obiectivele acestui scenariu sunt după cum urmează:

- Aplicaţiile companiei trebuie să fie semnate cu un certificat emis de o CA locală pentru a limita costurile semnării aplicaţiilor.
- Administratorii de sistem şi alţi utilizatori desemnaţi trebuie să poată verifica cu uşurinţă semnăturile digitale pe toate serverele iSeries pentru a verifica sursa şi autenticitatea obiectelor semnate de companie. Pentru a realiza acest lucru, fiecare server iSeries trebuie să aibă o copie atât a certificatului de verificare a semnăturii al companiei, cât şi a certificatului Autorităţii de certificare (CA) locală în fiecare memorie *SIGNATUREVERIFICATION a serverelor.
- Verificarea semnăturilor pe aplicaţiile companiei permite administratorilor iSeries şi altor persoane să detecteze dacă conţinutul obiectelor s-a modificat din momentul în care acestea au fost semnate.
- Administratorii trebuie să poată utiliza Administrarea centrală pentru împachetarea, semnarea şi distribuirea aplicaţiilor către serverele iSeries.

Detalii

Următoarea figură ilustrează procesul de semnare a obiectelor şi de verificare a semnăturilor pentru implementarea acestui scenariu:

Figura ilustrează următoarele puncte relevante pentru acest scenariu:

Sistemul central (iSeries A)

- iSeries A rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries A serveşte ca sistem central din care rulează funcţiile Administrării centrale, incluzând aplicaţiile de împachetare şi distribuire ale companiei.
- iSeries A are instalat un Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit iSeries (5722–AC3).
- iSeries A are instalat şi configurat Digital Certificate Manager (Managerul de certificare digitală) (OS/400 opţiune 34) şi Serverul HTTP IBM (5722–DG1).
- iSeries A se comportă ce Autoritatea de certificare (CA) locală şi certificatul de semnare a obiectelor se află pe acest sistem.

- iSeries A este sistemul primar de semnare a obiectelor pentru aplicaţiile companiei. Semnarea obiectelor produsului pentru distribuirea către clienţi este realizată pe iSeries A prin efectuarea acestor task-uri:
  1. Utilizarea DCM pentru crearea unei CA locale şi utilizarea CA locală pentru crearea unui certificat de semnare a obiectelor.
  2. Utilizarea DCM pentru exportarea unei copii a certificatului CA locală şi a certificatului de verificare a semnăturilor într-un fişier, astfel încât sistemele terminale (iSeries B, C, D, şi E) să poată verifica obiectele semnate.
  3. Utilizarea Administrării centrale pentru semnarea obiectelor aplicaţiilor şi împachetarea lor cu fişierele certificate de verificare.
  4. Utilizarea Administrării centrale pentru distribuirea aplicaţiilor semnate şi a fişierelor certificate către sistemele terminale.

Sistemele terminale (serverele iSeries B, C, D şi E)

- iSeries B şi C rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries D şi E rulează OS/400 Versiune 5 Ediţie 1 (V5R1).
- iSeries B, C, D şi E au instalat şi configurat Managerul de certificare digitală (opţiune 34) şi Serverul HTTP IBM (5722–DG1).
- iSeries B, C, D şi E primesc o copie a certificatului de verificare a semnăturilor al companiei şi a CA locală de la sistemul central (iSeries A) atunci când sistemele primesc aplicaţiile semnate.
- DCM este utilizat pentru crearea memoriei de certificare *SIGNATUREVERIFICATION şi pentru importarea CA locală şi a certificatelor de verificare în această memorie de certificare.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:

1. Toate serverele iSeries îndeplinesc cerinţele pentru instalarea şi utilizarea Managerului de certificare digitală (DCM).
2. Nimeni nu a configurat sau utilizat anterior DCM sau unul din serverele iSeries.
3. iSeries A indeplineşte cerinţele pentru instalarea şi utilizarea Navigatorului iSeries şi a Administrării centrale.
4. Serverul Administrării centrale trebuie să ruleze pe toate sistemele terminale iSeries.
5. Toate serverele iSeries au instalat cel mai înalt nivel al programului licenţiat Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit (5722-AC3).
6. Setarea implicită pentru variabila de sistem de verificare a semnăturilor în timpul restaurării (QVFYOBJRST) pe toate serverele iSeries din scenarii este 3 şi nu a fost modificată de la această setare. Setarea implicită asigură că serverul poate verifica semnăturile obiectelor pe măsură ce restauraţi obiectele semnate.
7. Administratorul de reţea pentru iSeries A trebuie să aibă autorizarea specială *ALLOBJ în profilul utilizator pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicaţia de semnare a obiectelor.
8. Administratorul de reţea sau oricine creează o memorie de certificare în DCM trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ în profilul utilizator.
9. Administratorii de sistem sau alţii de pe celelalte servere iSeries trebuie să aibă autorizarea specială *AUDIT în profilul utilizator pentru verificarea semnăturilor obiectelor.

Paşii de task

Există două seturi de task-uri pe care trebuie să le efectuaţi pentru a implementa acest scenariu: Un set de task-uri vă permite să setaţi iSeries A pentru utilizarea Administrării centrale la semnarea şi distribuirea

aplicaţiilor. Celălalt set de task-uri permite administratorilor de sistem şi altor persoane să verifice semnăturile de pe aceste aplicaţii pe toate celelalte servere iSeries.

Paşii de task pentru semnarea obiectelor

Trebuie să efectuaţi fiecare dintre aceste task-uri pe iSeries A pentru semnarea obiectelor aşa cum descrie acest scenariu:

1. Efectuaţi toţi paşii preliminari pentru configurarea tuturor produselor iSeries necesare.
2. Utilizaţi Managerul de certificare digitală (DCM) pentru a crea o Autoritate de certificare (CA) locală pentru emiterea unui certificat privat de semnare a obiectelor.
3. Utilizaţi DCM pentru a crea o definiţie de aplicaţie.
4. Utilizaţi DCM pentru a aloca un certificat definiţiei de aplicaţie care semnează obiecte.
5. Utilizaţi DCM pentru a exporta certificatele pe care alte sisteme trebuie să le utilizeze pentru verificarea semnăturilor obiectelor. Trebuie să exportaţi într-un fişier atât o copie a certificatului CA locală, cât şi o copie a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor.
6. Transferaţi fişierele certificate pe fiecare sistem terminaliSeries pe care intenţionaţi să verificaţi semnături.
7. Utilizaţi Administrarea centrală pentru a semna obiectele aplicaţiei.

Paşii de task pentru verificarea semnăturilor

Trebuie să efectuaţi aceste task-uri de configurare a verificării semnăturilor pe fiecare sistem terminal iSeries înainte de a utiliza Administrarea centrală pentru transferarea obiectelor aplicaţii semnate pe acestea. Configuraţia verificării semnăturilor trebuie să fie completă înainte ca să puteţi verifica semnăturile cu succes, pe măsură ce restauraţi obiectele semnate pe sisteme terminale.

Pe fiecare sistem terminal iSeries, trebuie să efectuaţi aceste task-uri pentru verificarea semnăturilor pe obiecte aşa cum descrie acest scenariu:

8. Utilizaţi Digital Certificate Manager (Managerul de certificare digitală - DCM) pentru crearea memoriei de certificare *SIGNATUREVERIFICATION.
9. Utilizaţi DCM pentru importarea certificatului CA locală şi a certificatului de verificare a semnăturilor.

Detalii de configurare

Efectuaţi următorii paşi de task pentru configurarea Administrării centrale pentru semnarea obiectelor aşa cum descrie acest scenariu.

Pasul 1: Efectuaţi toţi paşii preliminari

Trebuie să efectuaţi toate task-urile preliminare pentru instalarea şi configurarea tuturor produselor iSeries necesare înainte de a putea realiza task-urile de configurare specifice pentru implementarea acestui scenariu.

Pasul 2: Creaţi o Autoritate de certificare locală pentru emiterea unui certificat privat de semnare a obiectelor

Când utilizaţi Managerul de certificare digitală (DCM) pentru crearea unei Autorizări de certificare (CA) locală, procesul vă cere să completaţi o serie de formulare. Aceste formulare vă ghidează prin procesul de creare a CA şi de efectuare a altor task-uri necesare pentru începerea utilizării certficatelor digitale pentru Secure Sockets Layer (SSL), semnarea obiectelor şi verificarea semnăturilor. Deşi în acest scenariu nu trebuie să configuraţi certificate pentru SSL, trebuie să completaţi toate formularele din task pentru a configura sistemul să scaneze obiecte.

Pentru a utiliza DCM la crearea şi operarea unei CA locale, urmaţi aceşti paşi:

1. Porniţi DCM.

2. În cadrul de navigare al DCM, selectaţi **Crearea unei Autorităţi de certificare (CA)** pentru a afişa o serie de formulare.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Completaţi toate formularele pentru acest task ghidat. Pe măsură ce efectuaţi acest task, trebuie să faceţi următoarele:
   a. Să furnizaţi informaţii de identificare pentru CA locală.
   b. Să instalaţi certificatul CA locală în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaşte CA locală şi să poată valida certificatele pe care CA locală le emite.
   c. Să specificaţi datele de poliţă pentru CA dumneavoastră locală.
   d. Să utilizaţi noua CA locală pentru a emite un certificat server sau client pe care aplicaţiile dumneavoastră să îl poată utiliza pentru conexiuni SSL.

      Notă: Deşi acest scenariu nu utilizează acest certificat, trebuie să îl creaţi înainte de a putea utiliza CA locală pentru emiterea certificatului de semnarea obiectelor de care aveţi nevoie. Dacă anulaţi task-ul fără a crea acest certificat, trebuie să vă creaţi certificatul de semnare a obiectelor şi memoria de certificare *OBJECTSIGNING în care este memorat separat.
   e. Să selectaţi aplicaţiile care pot utiliza certificatul server sau client pentru conexiuni SSL.

      Notă: Pentru scopurile acestui scenariu, nu selectaţi nici o aplicaţie şi faceţi clic pe **Continuare** pentru a afişa următorul formular.
   f. Utilizaţi noua CA locală pentru emiterea unui certificat de semnare a obiectelor pe care aplicaţiile îl pot utiliza pentru semnarea digitală a obiectelor. Acest subtask creează memoria de certificare *OBJECTSIGNING. Aceasta este memoria de certificare pe care o utilizaţi pentru gestionarea certificatelor de semnare a obiectelor.
   g. Să selectaţi aplicaţiile care trebuie să aibă încredere în CA dumneavoastră locală.

      Notă: Pentru scopurile acestui scenariu, nu selectaţi nici o aplicaţie şi faceţi clic pe **Continuare** pentru a termina task-ul.

Acum că aţi creat o CA locală şi un certificat de semnare a obiectelor, trebuie să definiţi o aplicaţie de semnare a obiectelor care să utilizeze certificatul înainte de a putea semna obiecte.

Pasul 3: Creaţi o definiţie a aplicaţiei de semnare a obiectelor

După ce vă creaţi certificatul de semnare a obiectelor, trebuie să utilizaţi Managerul de certificare digitală (DCM) pentru definirea unei aplicaţii de semnare a obiectelor pe care să o utilizaţi pentru semnarea obiectelor. Definiţia aplicaţiei nu trebuie să se refere la o aplicaţie reală; definiţia aplicaţiei pe care o creaţi trebuie să descrie tipul sau grupul de obiecte pe care intenţionaţi să le semnaţi. Aveţi nevoie de definiţie pentru a putea avea un ID de aplicaţie asociat cu certificatul pentru activarea procesului de semnare.

Pentru a utiliza DCM la crearea unei definiţii a aplicaţiei de semnare a obiectelor, urmaţi aceşti paşi:
1. În cadrul de navigare, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***OBJECTSIGNING** ca memoria de certificare de deschis.
2. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atunci când aţi creat-o şi faceţi clic pe **Continuare**.
3. În cadrul de navigare, selectaţi **Gestiune aplicaţii** pentru a afişa o listă de task-uri.
4. Selectaţi **Adăugare aplicaţie** din lista de task-uri pentru afişarea unui formular pentru definirea aplicaţiei.
5. Completaţi formularul şi faceţi clic pe **Adăugare**.

Acum trebuie să alocaţi certificatul dumneavoastră de semnare a obiectelor aplicaţiei pe care aţi creat-o.

Pasul 4: Alocaţi un certificat definiţiei aplicaţiei de semnare a obiectelor

Pentru a aloca certificatul aplicaţiei dumneavoastră de semnare a obiectelor, urmaţi aceşti paşi:

1. În cadrul de navigare DCM, selectaţi **Gestiune certificate** pentru a afişa o listă de task-uri.
2. Din lista de task-uri, selectaţi **Alocare certificat** pentru afişarea unei liste de certificate pentru memoria de certificare curentă.
3. Selectaţi un certificat din listă şi faceţi clic pe **Alocare la aplicaţie** pentru a afişa o listă de definiţii de aplicaţii pentru memoria de certificare.
4. Selectaţi una sau mai multe aplicaţii din listă şi faceţi clic pe **Continuare**. Este afişată o pagină de mesaj pentru a confirma alocarea certificatului sau pentru a oferi informaţiile de eroare dacă s-a produs o eroare.

Când terminaţi acest task, sunteţi gata să semnaţi obiecte utilizând Administrarea centrală când le împachetaţi şi le distribuiţi. Totuşi, pentru a vă asigura că dumneavoastră sau alte persoane puteţi verifica semnăturile, trebuie să exportaţi certificatele necesare într-un fişier şi să le transferaţi pe toate sistemele terminale iSeries. Trebuie de asemenea să efectuaţi toate task-urile de configurare a verificării semnăturilor pe fiecare sistem terminal iSeries înainte de a utiliza Administrarea centrală pentru transferarea obiectelor aplicaţii semnate pe acestea. Configuraţia verificării semnăturilor trebuie să fie completă înainte ca să puteţi verifica semnăturile cu succes, pe măsură ce restauraţi obiectele semnate pe sisteme terminale.

Pasul 5: Exportaţi certificatele pentru a activa verificarea semnăturilor pe alte sisteme iSeries

Semnarea obiectelor pentru protejarea integrităţii conţinutului necesită ca dumneavoastră şi alte persoane să aveţi un mijloc pentru verificarea autenticităţii semnăturilor. Pentru verificarea semnăturilor pe acelaşi sistem care semnează obiectele, trebuie să utilizaţi DCM pentru crearea memoriei de certificare *SIGNATUREVERIFICATION. Această memorie de certificare trebuie să conţină atât o copie a certificatului de semnare a obiectelor, cât şi o copie a certificatului CA, pentru CA care a emis certificatul de semnare.

Pentru a permite altor persoane să verifice semnătura, trebuie să le oferiţi o copie a certificatului care a semnat obiectul. Atunci când utilizaţi o Autoritate de certificare (CA) locală pentru emiterea certificatului, trebuie de asemenea să le oferiţi şi o copie a certificatului CA locală.

Pentru a utiliza DCM astfel încât să puteţi verifica semnături pe acelaşi sistem care semnează obiectele (iSeries A în acest scenariu), urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Creare memorie de certificare nouă** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de creat.
2. Selectaţi **Da** pentru copierea certificatelor existente de semnare a obiectelor în noua memorie de certificare ca certificate de verificare a semnăturilor.
3. Specificaţi o parolă pentru noua memorie de certificare şi faceţi clic pe **Continuare** pentru a crea memoria de certificare. Acum puteţi utiliza DCM pentru verificarea semnăturilor pe acelaşi sistem pe care îl utilizaţi pentru semnarea obiectelor.

Pentru a utiliza DCM la exportarea unei copii a certificatului CA locală şi a unei copii a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor astfel încât să verificaţi semnăturile obiectelor pe alte sisteme, urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Gestiune certificate**, şi apoi selectaţi task-ul **Exportare certificate**.
2. Selectaţi **Autoritate de certificare (CA)** şi faceţi clic pe **Continuare** pentru a afişa o listă a certificatelor CA pe care le puteţi exporta.
3. Selectaţi certificatul CA locală pe care l-aţi creat mai devreme din listă şi faceţi clic pe **Export**.
4. Specificaţi **Fişier** ca destinaţie de export şi faceţi clic pe **Continuare**.

5. Specificaţi o cale şi un nume de fişier complet determinate pentru certificatul CA locală şi faceţi clic pe **Continuare** pentru a exporta certificatul.
6. Faceţi clic pe **OK** pentru a ieşi din pagina de confirmare Export. Acum puteţi exporta o copie a certificatului de semnare a obiectelor.
7. Selectaţi din nou task-ul **Exportare certificat**.
8. Selectaţi **Semnare obiect** pentru a afişa o listă a certificatelor de semnare a obiectelor pe care le puteţi exporta.
9. Selectaţi certificatul corespunzător de semnare a obiectelor din listă şi faceţi clic pe **Exportare**.
10. Selectaţi **Fişier, ca certificat de verificare a semnăturilor** ca destinaţie şi faceţi clic pe **Continuare**.
11. Specificaţi o cale şi un nume de fişier complet determinate pentru certificatul de verificare a semnăturilor exportat şi faceţi clic pe **Continuare** pentru a exporta certificatul.

Acum puteţi transfera aceste fişiere pe sistemele terminale iSeries pe care intenţionaţi să verificaţi semnăturile pe care le-aţi creat cu certificatul respectiv.

Pasul 6: Transferaţi fişierele certificate pe sistemele terminale iSeries

Trebuie să transferaţi fişierele certificate pe care le-aţi creat pe iSeries A pe sistemele terminale iSeries din acest scenariu înainte de a le putea configura pentru verificarea obiectelor pe care le semnaţi. Puteţi utiliza câteva metode diferite pentru transferarea fişierelor de certificare. De exemplu, puteţi utiliza Protocolul de transfer fişiere (FTP) sau distribuţia de pachete a Administrării centrale pentru a transfera fişierele.

Pasul 7: Semnaţi obiectele utilizând Administrarea centrală

Procesul de semnare a obiectelor pentru Administrarea centrală este parte a procesului de distribuire a pachetelor software. Trebuie să efectuaţi toate task-urile de configurare a verificării semnăturilor pe fiecare sistem terminal iSeries înainte de a utiliza Administrarea centrală pentru transferarea obiectelor aplicaţiei semnate pe acestea. Configuraţia verificării semnăturilor trebuie să fie completă înainte ca să puteţi verifica semnăturile cu succes, pe măsură ce restauraţi obiectele semnate pe sisteme terminale.

Pentru a semna o aplicaţie pe care o distribuiţi sistemelor terminale iSeries aşa cum descrie acest scenariu, urmaţi aceşti paşi:

1. Utilizaţi Administrarea centrală pentru împachetarea şi distribuirea produselor software.
2. Când vă este afişat panoul **Identificare** în vrăjitorul **Definiţie produs**, faceţi clic pe **Avansat** pentru afişarea panoului **Identificare avansată**.
3. În câmpul **Semnare digitală**, introduceţi ID-ul de aplicaţie pentru aplicaţia de semnare a obiectelor pe care aţi creat-o anterior şi să faceţi clic pe **OK**.
4. Completaţi vrăjitorul şi continuaţi procesul pentru împachetarea şi distribuirea produselor software cu Administrarea centrală.

Pasul 8: Task-uri de verificare a semnăturilor: Creaţi memoria de certificare *SIGNATUREVERIFICATION pe sistemele terminale iSeries

Pentru verificarea semnăturilor pe sistemele terminale iSeries din acest scenariu, fiecare sistem trebuie să aibă o copie a certificatului corespunzător de verificare a semnăturilor în memoria de certificare *SIGNATUREVERIFICATION. Dacă un certificat privat a semnat obiectele, această memorie de certificare trebuie să conţină şi o copie a certificatului CA locală.

Pentru crearea memoriei de certificare *SIGNATUREVERIFICATION, urmaţi aceşti paşi:

1. Porniţi DCM.

2. În cadrul de navigare al Managerului de certificare digitală (DCM) selectaţi **Creare memorie de certificare nouă** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de creat.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectaţi semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Specificaţi o parolă pentru noua memorie de certificare şi faceţi clic pe **Continuare** pentru a crea memoria de certificare. Acum puteţi importa certificatele în memorie şi le puteţi utiliza pentru verificarea semnăturilor.

Pasul 9: Task-uri de verificare a semnăturilor: Importaţi certificatele

Pentru a verifica semnătura de pe un obiect, memoria de certificare *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului de verificare a semnăturilor. Dacă certificatul de semnare este privat, această memorie de certificare trebuie să aibă şi o copie a certificatului Autorităţii de certificare (CA) locală care a emis certificatul de semnare. În acest scenariu, ambele certificate erau exportate într-un fişier şi acel fişier era transferat pe fiecare sistem terminal iSeries.

Pentru a importa acest certificate în memoria *SIGNATUREVERIFICATION, urmaţi aceşti paşi:
1. În cadrul de navigare al DCM, faceţi clic pe **Selectarea unei memorii de certificare** şi selectaţi ***SIGNATUREVERIFICATION** ca memoria de certificare de deschis.
2. Când se afişează pagina Memorie de certificare şi parolă, oferiţi parola pe care aţi specificat-o pentru memoria de certificare atnci când aţi creat-o şi faceţi clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune certificate** pentru a afişa o listă de task-uri.
4. Din lista de task-uri, selectaţi **Importare certificate**.
5. Selectaţi **Autoritate de certificare (CA)** ca tipul certificatului şi faceţi clic pe **Continuare**.

   Notă: Trebuie să importaţi certificatul CA locală înainte de a importa un certificat privat de verificare a semnăturilor; altfel, procesul de importare pentru certificatul de verificare va eşua.
6. Specificaţi calea şi numele de fişier complet determinate pentru fişierul de certificare CA şi faceţi clic pe **Continuare**. Este afişat un mesaj care confirmă că procesul de importare a reuşit sau care furnizează un mesaj de eroare dacă procesul a eşuat.
7. Selectaţi din nou task-ul **Importare certificat**.
8. Selectaţi **Verificare semnături** ca tipul de certificat de importat şi faceţi clic pe **Continuare**.
9. Specificaţi calea şi numele de fişier complet determinate pentru fişierul certificat de verificare a semnăturilor şi faceţi clic pe **Continuare**. Este afişat un mesaj care confirmă că procesul de importare a reuşit sau care furnizează informaţiile de eroare dacă procesul a eşuat.

Sistemul dumneavoastră iSeries poate acum verifica semnăturile de pe obiectele care au fost create cu certificatul corespunzător de semnare când restauraţi obiectele semnate.

Concepte de semnare a obiectelor

Înainte de a începe utilizarea capacităţilor iSeries de semnare a obiectelor şi de verificare a semnăturilor, puteţi considera utilă revizuirea câtorva dintre aceste concepte:

Semnături digitale
Aflaţi despre semnăturile digitale şi despre tipul de protecţie pe care o oferă.

Obiecte care se pot semna
Aflaţi despre tipurile de obiecte iSeries pe care le puteţi semna şi despre opţiunile de semnare a obiectelor comandă (*CMD).

Procesarea de semnare a obiectelor
Aflaţi despre modul în care funcţionează procesul de semnare a obiectelor şi ce parametri puteţi seta pentru proces.

Procesarea de verificare a semnăturilor
Aflaţi despre modul de funcţionare a procesului de verificare a semnăturilor obiectelor şi ce parametri puteţi seta pentru proces.

Semnături digitale

OS/400 oferă suport pentru utilizarea certificatelor digitale la ″semnarea″ digitală a obiectelor. O semnătură digitală pe un obiect este creată prin utilizarea unei forme de criptografie şi este asemănătoare unei semnături personale pe un document scris. O semnătură digitală face dovada originii obiectului şi oferă un mijloc de verificare a integrităţii obiectului. Proprietarul unui certificat digital ″semnează″ un obiect utilizând cheia privată a certificatului. Persoana care primeşte obiectul utilizează cheia publică corespunzătoare a certificatului pentru decriptarea semnăturii, care verifică integritatea obiectului semnat şi verifică expeditorul ca sursă.

Suportul pentru semnarea obiectelor extinde uneltele tradiţionale ale serverului iSeries pentru controlarea persoanelor care pot modifica obiecte. Controalele tradiţionale nu pot proteja un obiect de modificarea neautorizată în timp ce obiectul se află în tranzit prin Internet sau alte reţele care nu sunt de încredere. Deoarece puteţi detecta dacă conţinutul unui obiect a fost modificat din momentul în care acesta a fost semnat, puteţi determina dacă să aveţi sau nu încredere în obiectele pe care le obţineţi în astfel de situaţii.

O semnătură digitală este un rezumat matematic cifrat al datelor din obiect. Obiectul şi conţinutul său nu sunt cifrate şi făcute private prin semnătura digitală; totuşi, rezumatul în sine este cifrat pentru a preveni modificările neautorizate asupra acestuia. Oricine doreşte să se asigure că obiectul nu a fost modificat în tranzit şi că obiectul are originea într-o sursă acceptată, legitimă, poate utiliza cheia publică a certificatului de semnare pentru verificarea semnăturii digitale originale. Dacă semnătura nu mai corespunde, este posibil ca datele să fi fost modificate. Într-un astfel de caz, primitorul poate evita utilizarea obiectului, în schimb contactând semnatarul pentru obţinerea altei copii a obiectului semnat.

Semnătura de pe un obiect reprezintă sistemul care a semnat obiectul, şi nu un utilizator specific de pe acel sistem (deşi utilizatorul trebuie să aibă autorizarea corespunzătoare pentru utilizarea certificatului la semnarea obiectelor).

Dacă vă decideţi că utilizarea semnăturilor digitale se potriveşte cu nevoile şi poliţele dumneavoastră de securitate, ar trebuie să evaluaţi dacă veţi utiliza certificate publice sau emite certificate locale. Dacă intenţionaţi să distribuţi obiecte către utilizatori din publicul general, ar trebui să luaţi în considerare utilizarea certificatelor de la o Autoritate de certificare (CA) publică binecunoscută, pentru semnarea obiectelor. Utilizarea certificatelor publice asigură că alte persoane pot verifica cu uşurinţă şi fără costuri semnăturile pe care le puneţi pe obiectele distribuite către acestea. Dacă, totuşi, intenţionaţi să distribuiţi obiecte numai în cadrul organizaţiei dumneavoastră, puteţi prefera să utilizaţi Digital Certificate Manager - Managerul de certificare digitală (DCM) la operarea unei CA locale proprii pentru emiterea certificatelor de semnare a obiectelor. Utilizarea certificatelor private de la o CA locală pentru semnarea obiectelor este mai puţin costisitoare decât cumpărarea certificatelor de la o CA publică binecunoscută.

Tipuri de semnături digitale

Începând cu V5R2, puteţi semna obiecte comandă (*CMD); puteţi de asemenea alege unul dintre cele două tipuri de semnături pentru obiecte *CMD: semnături pentru nucleul obiectului sau semnături pentru întregul obiect.

- **Semnături pentru întregul obiect**
  Acest tip de semnătură acoperă toţi octeţii obiectului, mai puţin câţiva octeţi neesenţiali.

- **Semnături pentru nucleul obiectului**
  Acest tip de semnătură acoperă octeţii esenţiali ai obiectului *CDM. Totuşi, semnătura nu acoperă acei octeţi care sunt supuşi unor modificări frecvente. Acest tip de semnătură permite efectuarea unor modificări asupra comenzii fără nevalidarea semnăturii. Octeţii pe care semnătura nucleului obiectului nu îi acoperă variază în funcţie de obiectul *CMD specific; semnăturile nucleului nu acoperă valorile implicite ale parametrilor pe obiectele *CMD, de exemplu. Exemplele de modificări care nu vor nevalida o semnătură a nucleului unui obiect includ:
  - Modificarea valorilor implicite ale comenzii.
  - Adăugarea unui program de verificare a validităţii la o comandă care nu are un astfel de program.
  - Modificarea parametrului Where allowed to run (Locul permis de rulare).
  - Modificarea parametrului Allow limited users (Permitere utilizatori limitaţi).

Pentru a afla mai multe despre tipul de obiecte iSeries pe care le puteţi semna şi despre octeţii unui obiect *CMD care sunt acoperiţi de o semnătură a nucleului obiectului, consultaţi Obiecte care se pot semna.

Obiecte care se pot semna

Puteţi semna digital o varietate de tipuri de obiecte OS/400, indiferent de metoda utilizată pentru semnarea lor. Puteţi semna orice obiect (*STMF) pe care îl memoraţi în sistemul de fişiere integrat al sistemului, cu excepţia obiectelor care sunt memorate într-o bibliotecă. Dacă obiectul are un program Java ataşat, programul va fi de asemenea semnat. Puteţi semna doar aceste obiecte din sistemul de fişiere QSYS.LIB: programe (*PGM), programe de serviciu (*SRVPGM), module (*MODULE), pachete SQL (*SQLPKG), *FILE (numai fişier de salvare) şi comenzi (*CMD).

Pentru a semna un obiect, acesta trebuie să se afle pe sistemul local. De exemplu, dacă operaţi un server Windows 2000 pe un Server xSeries integrat pentru iSeries, aveţi sistemul de fişiere QNTC disponibil în sistemul de fişiere integrat. Directoarele din acest sistem de fişiere nu sunt considerate locale deoarece conţin fişiere care sunt deţinute de sistemul de operare Windows 2000. De asemenea, nu puteţi semna obiecte vide sau obiecte care sunt compilate pentru o ediţie anterioară V5R1.

Semnăturile obiectelor comandă (*CMD)

Când semnaţi obiecte *CMD, puteţi alege unul din cele două tipuri de semnături pentru a le aplica obiectului *CMD. Puteţi alege să semnaţi întregul obiect, sau să semnaţi doar partea de nucleu a obiectului. Atunci când alegeţi să semnaţi întregul obiect, semnătura este aplicată pe toţi octeţii obiectului, cu excepţia câtorva octeţi neesenţiali. Semnătura întregului obiect acoperă elementele conţinute în semnătura nucleului obiectului.

Când alegeţi să semnaţi doar nucleul obiectului, octeţii esenţiali sunt protejaţi de semnătură, în timp ce octeţii care sunt supuşi unor modificări frecvente nu sunt semnaţi. Octeţii care nu sunt semnaţi variază în funcţie de obiectul *CMD, dar pot include, printre altele, octeţi care determină modul în care obiectul este valid sau locul în care obiectul poate rula. Semnăturile nucleului nu acoperă valorile implicite ale parametrilor pe obiectele *CMD, de exemplu. Acest tip de semnătură permite efectuarea unor modificări asupra comenzii, fără nevalidarea semnăturii acesteia. Exemplele de modificări care nu vor nevalida aceste tipuri de semnături includ:

- Modificarea valorilor implicite ale comenzii.
- Adăugarea unui program de verificare a validităţii la o comandă care nu are un astfel de program.
- Modificarea parametrului Where allowed to run (Locul permis de rulare).
- Modificarea parametrului Allow limited users (Permitere utilizatori limitaţi).

Următorul tabel descrie exact ce octeţi dintr-un obiect *CMD sunt incluşi în semnătura nucleului obiectului.

Compoziţia semnăturii nucleului pe obiecte *CMD

Partea din obiect	Relaţia cu semnătura nucleului obiectului
Valorile implicite ale comenzii modificate de CHGCMDDFT	Nu fac parte din semnătura nucleului obiectului
Programul de procesare a comenzii şi biblioteca	Incluse întotdeauna în semnătura nucleului obiectului
Fişierul sursă REXX şi biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Membrul sursei REXX	Inclus dacă este specificat pentru comandă la momentul semnării, altfel nu face parte din semnătura nucleului obiectului
Mediul REXX al comenzii şi biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Numele programului de ieşire REXX, biblioteca şi codul de ieşire	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Programul de verificare a validităţii şi biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Modul în care este valid	Nu face parte din semnătura nucleului obiectului
Locul permis de rulare	Nu face parte din semnătura nucleului obiectului
Permitere utilizatori limitaţi	Nu face parte din semnătura nucleului obiectului
Cărţile de ajutor	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Grupul de panouri de ajutor şi biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Identificatorul de ajutor	Inclus dacă este specificat pentru comandă la momentul semnării, altfel nu face parte din semnătura nucleului obiectului
Indexul de căutare de ajutor şi biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Biblioteca curentă	Inclusă dacă este specificată pentru comandă la momentul semnării, altfel nu face parte din semnătura nucleului obiectului
Biblioteca produsului	Inclusă dacă este specificată pentru comandă la momentul semnării, altfel nu face parte din semnătura nucleului obiectului
Programul de evitare a promptului şi biblioteca	Inclus dacă este specificat pentru comandă la momentul semnării, altfel nu face parte din semnătura nucleului obiectului
Text (descriere)	Nu face parte nici din semnătura nucleului obiectului, nici din semnătura întregului obiect, deoarece nu este memorat în obiect
Activarea interfeţei grafice utilizator (GUI)	Nu face parte din semnătura nucleului obiectului

Procesarea de semnare a obiectelor

Atunci când semnaţi obiecte puteţi specifica următoarele opţiuni pentru procesarea de semnare a obiectelor.

- **Procesarea la eroare**
  Puteţi specifica ce tip de procesare la eroare trebuie să utilizeze aplicaţia atunci când creează semnături pe mai multe obiecte. Puteţi preciza ca aplicaţia să se oprească din semnarea obiectelor când apare o eroare sau să continue semnarea celorlalte obiecte din proces.

- **Semnătura duplicat a obiectelor**
  Puteţi specifica modul în care aplicaţia trebuie să trateze procesul de semnare atunci când aplicaţia semnează din nou un obiect. Puteţi specifica dacă se va păstra semnătura originală sau se va înlocui semnătura originală cu semnătura nouă.
- **Obiectele din subdirectoare**
  Puteţi specifica modul în care aplicaţia trebuie să trateze semnarea obiectelor din subdirectoare. Puteţi preciza ca aplicaţia să semneze individual obiectele din orice subdirectoare sau ca aplicaţia să semneze numai obiectele din cadrul directorului principal, ignorând toate subdirectoarele.
- **Domeniul semnăturii obiectului**
  Când semnaţi obiecte *CMD, puteţi specifica dacă se va semna întregul obiect sau numai partea de nucleu a obiectului.

Procesarea de verificare a semnăturilor

Puteţi specifica următoarele opţiuni pentru procesarea de verificare a semnăturilor.

- **Procesarea la eroare**
  Puteţi specifica ce tip de procesare la eroare trebuie să utilizeze aplicaţia atunci când verifică semnături pe mai multe obiecte. Puteţi preciza ca aplicaţia să se oprească din verificarea semnăturilor când apare o eroare sau să continue verificarea semnăturilor pe celelalte obiecte din proces.
- **Obiectele din subdirectoare**
  Puteţi specifica modul în care aplicaţia trebuie să trateze verificarea semnăturilor pe obiectele din subdirectoare. Puteţi preciza ca aplicaţia să verifice individual semnăturile obiectelor din subdirectoare sau ca aplicaţia să verifice numai semnăturile pentru obiectele din cadrul directorului principal, ignorând toate subdirectoarele.
- **Verificarea semnăturii nucleului sau verificarea semnăturii întregului obiect**
  Există reguli ale sistemului care determină modul în care sistemul trebuie să trateze semnăturile nucleului şi semnăturile întregului obiect în timpul procesului de verificare. Aceste reguli sunt după cum urmează:
  - Dacă nu există semnături pe obiect, procesul de verificare raportează că obiectul nu este semnat şi continuă verificarea altor obiecte din proces.
  - Dacă obiectul a fost semnat de o sursă de încredere a sistemului (IBM), semnătura trebuie să corespundă sau procesul de verificare eşuează. Dacă semnătura corespunde, procesului de verificare continuă. Semnătura este un rezumat matematic cifrat al datelor din obiect; de aceea, semnătura este considerată corespunzătoare dacă datele din obiect în timpul verificării se potrivesc cu datele din obiect atunci când a fost semnat.
  - Dacă obiectul are orice semnătură a întregului obiect care este de încredere (bazată pe certificatele conţinute în memoria de certificare *SIGNATUREVERIFICATION), cel puţin una dintre aceste semnături trebuie să fie corespunzătoare sau procesul de verificare eşuează. Dacă cel puţin o semnătură a întregului obiect este corespunzătoare, procesul de verificare continuă.
  - Dacă obiectul are orice semnătură a nucleului obiectului care este de încredere, cel puţin una dintre acestea trebuie să se potrivească cu un certificat din memoria de certificare *SIGNATUREVERIFICATION sau procesul de verificare eşuează. Dacă cel puţin o semnătură a nucleului obiectului este corespunzătoare, procesul de verificare continuă.

Cerinţe preliminare pentru semnarea obiectelor şi verificarea semnăturilor

Capacităţile OS/400 de semnare a obiectelor şi de verificare a semnăturilor vă oferă mijloace suplimentare puternice de controlare a obiectelor pe serverul dumneavoastră iSeries. Pentru a profita de aceste capacităţi, trebuie să îndepliniţi cerinţele preliminare pentru utilizarea lor.

Cerinţe preliminare pentru semnarea obiectelor

Există un număr de metode pe care le puteţi utiliza pentru semnarea obiectelor, în funcţie de nevoile dumneavoastră de afaceri şi de securitate:

- Puteţi utiliza Digital Certificate Manager - Managerul de certificare digitală (DCM).
- Puteţi scrie un program care utilizează API-uul Semnare obiect.
- Puteţi utiliza funcţiile de Administrare centrală ale Navigatorului iSeries pentru semnarea obiectelor pe măsură de le împachetaţi pentru distribuirea către sisteme terminale iSeries.

Metoda pe care o alegeţi pentru semnarea obiectelor depinde de nevoile dumneavoastră de afaceri şi de securitate. Indiferent de metoda pe care intenţionaţi să o utilizaţi pentru semnarea obiectelor, trebuie să vă asiguraţi că sunt îndeplinite anumite condiţii preliminare:

- Trebuie să îndepliniţi cerinţele preliminare pentru instalarea şi utilizarea Managerului de certificare digitală (DCM).
  - Trebuie să utilizaţi DCM pentru crearea memoriei de certificare *OBJECTSIGNING. Creaţi această memorie de certificare ca parte a procesului de creare a Autorităţii de certificare (CA) locală sau ca parte a gestionării certificatelor de semnare a obiectelor de la o CA publică Internet.
  - Memoria de certificare *OBJECTSIGNING trebuie să conţină cel puţin un certificat, fie unul pe care l-aţi creat utilizând o CA locală, fie unul pe care l-aţi obţinut de la o CA publică Internet.
  - Trebuie să utilizaţi DCM pentru a crea cel puţin o definiţie a aplicaţiei de semnare a obiectelor de utilizat pentru semnarea obiectelor.
  - Trebuie să utilizaţi DCM pentru a aloca un anumit certificat definiţiei aplicaţiei de semnare a obiectelor.
- Profilul utilizator iSeries care semnează obiecte trebuie să aibă autorizarea specială *ALLOBJ. Profilul utilizator iSeries care creează memoria de certificare *SIGNATUREVERIFICATION trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ.

Cerinţe preliminare pentru verificarea semnăturilor

Există un număr de metode pe care le puteţi utiliza pentru verificarea semnăturilor pe obiecte:

- Puteţi utiliza Digital Certificate Manager - Managerul de certificare digitală (DCM).
- Puteţi scrie un program care utilizează API-ul Verificare obiect (QYDOVFYO).
- Puteţi utiliza una dintre comenzi, cum ar fi comanda CHKOBJITG (Check Object Integrity - Verificare integritate obiect).

Metoda pe care o alegeţi pentru semnarea obiectelor depinde de nevoile dumneavoastră de afaceri şi de securitate. Indiferent de metoda pe care intenţionaţi să o utilizaţi, trebuie să vă asiguraţi că sunt îndeplinite anumite condiţii preliminare:

- Trebuie să îndepliniţi cerinţele preliminare pentru instalarea Managerului de certificare digitală (DCM).
- Trebuie să creaţi memoria de certificare *SIGNATUREVERIFICATION. Puteţi crea această memorie de certificare într-unul din cele două moduri, în funcţie de nevoile dumneavoastră. O puteţi crea utilizând Managerul de certificare digitală (DCM) pentru gestionarea certificatelor de verificare a semnăturilor. Sau, dacă utilizaţi un certificat public pentru semnarea obiectelor, puteţi crea această memorie de certificare prin scrierea unui program care utilizează API-ul Adăugare verificator (QYDOADDV).

  Notă: API-ul Adăugare verificator creează memoria de certificare cu o parolă implicită. Trebuie să utilizaţi DCM pentru resetarea acestei parole implicite, modificând-o cu una la alegerea dumneavoastră, pentru a preveni accesul neautorizat la memoria de certificare.
- Memoria de certificare *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului care a semnat obiectele. Puteţi adăuga acest certificat în memoria de certificare în două moduri. Puteţi utiliza DCM pe sistemul care semnează pentru exportarea certificatului într-un fişier şi apoi să utilizaţi DCM pe sistemul destinaţie de verificare pentru importarea certificatului în memoria de certificare *SIGNATUREVERIFICATION. Sau, dacă utilizaţi un certificat public la semnarea obiectelor, puteţi adăuga certificatul la memoria de certificare a sistemului destinaţie de verificare prin scrierea unui program care utilizează API-ul Adăugare verificator.

- Memoria de certificare *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului CA care a emis certificatul ce a semnat obiectele. Dacă utilizaţi un certificat public la semnarea obiectelor, memoria de certificare de pe sistemul destinaţie de verificare ar trebui să aibă deja o copie a certificatului CA necesar. Dacă utilizaţi un certificat emis de o CA locală la semnarea obiectelor, totuşi, trebuie să utilizaţi DCM pentru adăugarea unei copii a certificatului CA locală în memoria de certificare pe sistemul destinaţie de verificare.

  Notă: Din motive de securitate, API-ul Adăudare verificator nu vă permite să inseraţi un certificat Autoritate de certificare (CA) în memoria de certificare *SIGNATUREVERIFICATION. Când adăugaţi un certificat CA în memoria de certificare, sistemul consideră CA ca fiind o sursă de încredere. În consecinţă, sistemul tratează certificatul pe care l-a emis CA ca având originea într-o sursă de încredere. De aceea, nu puteţi utiliza API-ul pentru crearea unui program de ieşire instalare care să insereze un certificat CA în memoria de certificare. Trebuie să utilizaţi Managerul de certificare digitală pentru adăugarea unui certificat CA în memoria de certificare pentru a vă asigura că cineva trebuie să controleze, specific şi manual, CA-urile în care sistemul are încredere. Procedând astfel, evitaţi posibilitatea ca sistemul să importe certificate din surse care nu au fost specificate cu bună ştiinţă de un administrator ca fiind de încredere.

  Dacă utilizaţi un certificat emis de o CA locală la semnarea obiectelor, trebuie să utilizaţi DCM pe serverul gazdă iSeries al CA locală pentru exportarea unei copii a certificatului CA locală într-un fişier. Puteţi utiliza DCM pe serverul destinaţie iSeries de verificare pentru importarea certificatul CA locală în memoria de verificare *SIGNATUREVERIFICATION. Pentru a preveni o posibilă eroare, trebuie să importaţi certificatul CA locală în această memorie de certificare înainte de utilizarea API-ului Adăugare verificator pentru adăugarea certificatului de verificare a semnăturilor. În consecinţă, dacă utilizaţi un certificat emis de o CA locală, vă poate fi mai uşor să utilizaţi DCM pentru importarea certificatului CA şi a certificatului de verificare în memoria de certificare.

  Dacă doriţi să împiedicaţi pe oricine să utilizeze acest API pentru a adăuga un certificat de verificare în memoria dumneavoastră de certificare *SIGNATUREVERIFICATION fără acceptul dumneavoastră, puteţi lua în considerare dezactivarea acestui API din sistemul dumneavoastră. Puteţi face acest lucru utilizând uneltele de servicii sistem (SST) pentru a nu permite modificări asupra variabilelor de sistem legate de securitate.
- Profilul utilizator iSeries care verifică semnăturile trebuie să aibă autorizarea specială *AUDIT. Profilul utilizator iSeries care creează memoria de certificare *SIGNATUREVERIFICATION sau modifică parola pentru aceasta trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ.

Gestiunea obiectelor semnate

Începând cu V5R1, IBM a început semnarea programelor licenţiate OS/400 şi a PTF-urilor ca metodă de marcare oficială a sistemului de operare ca având originea de la IBM şi ca mijloc de detectare a modificărilor neautorizate asupra obiectelor sistemului. De asemenea, partenerii de afaceri şi alţi vânzători pot semna aplicaţiile pe care le cumpăraţi. În consecinţă, chiar dacă nu semnaţi dumneavoastră obiecte, trebuie să înţelegeţi modul de gestionare a obiectelor semnate şi modul în care aceste obiecte semnate afectează task-urile administrative de rutină din sistem.

Obiectele semnate afectează în principal task-urile de copiere de siguranţă şi de recuperare, mai exact modul în care salvaţi obiecte şi restauraţi obiecte pe sistemul dumenavoastră.

Variabilele sistem şi comenzile care afectează obiectele semnate
Aflaţi despre variabilele sistem şi comenzile pe care le puteţi utiliza pentru gestionarea obiectelor semnate sau care au efect asupra obiectelor semnate atunci când le rulaţi.

Consideraţii de salvare şi restaurare pentru obiectele semnate
Aflaţi despre modul în care obiectele semnate afectează realizarea task-urilor de salvare şi restaurare pentru sistemul dumneavoastră.

Comenzi de verificare a codurilor pentru a asigura integritatea semnăturilor
Aflaţi detalii despre utilizarea comenzilor pentru verificarea semnăturilor obiectelor pentru determinarea integrităţii obiectelor.

Variabilele sistem şi comenzile care afectează obiectele semnate

Pentru a gestiona efectiv obiectele semnate, trebuie să înţelegeţi modul în care variabilele sistem şi comenzile afectează obiectele semnate. Variabila sistem **Verificarea semnăturilor în timpul restaurării** (QVFYOBJRST) determină modul în care diferite comenzi de restaurare afectează obiectele semnate şi modul în care sistemul dumneavoastră tratează obiectele semnate în timpul operaţiilor de restaurare. Nu există anumite comenzi CL care să fie destinate exclusiv pentru gestionarea obiectelor semnate pe un sistem iSeries. Totuşi, există un număr de comenzi CL obişnuite pe care le utilizaţi pentru gestionarea obiectelor semnate (sau pentru gestionarea obiectelor de infrastructură care fac posibilă semnarea obiectelor). Alte comenzi pot afecta în mod negativ obiectele semnate de pe sistemul dumneavoastră prin înlăturarea semnăturii de pe obiectele semnate şi astfel anulând protecţia pe care o oferă semnătura.

Variabilele sistem care afectează obiectele semnate

Variabila sistem **Verificarea semnăturilor obiectelor în timpul restaurării** (QVFYOBJRST), membră a categoriei de restaurare a variabilelor sistem OS/400 determină modul în care comenzile afectează obiectele semnate de pe sistemul dumneavoastră. Variabila sistem, care este disponibilă prin Navigatorul iSeries, controlează modul în care sistemul tratează verificarea semnăturilor în timpul operaţiilor de restaurare. Setarea pe care o utilizaţi pentru această variabilă sistem, în combinaţie cu alte două setări ale variabilelor sistem, afectează operaţiile de retaurare pentru sistemul dumneavoastră. În funcţie de setarea pe care o selectaţi pentru această variabilă, ea poate permite sau nu restaurarea obiectelor pe baza stării semnăturii lor. (De exemplu, dacă obiectul este nesemnat, are o semnătură nevalidă, este semnat de o sursă de încredere şi aşa mai departe.) Setarea implicită pentru această variabilă sistem permite restaurarea obiectelor nesemnate, dar asigură că obiectele semnate pot fi restaurate numai dacă obiectele au o semnătură validă. Sistemul defineşte un obiect ca semnat numai dacă obiectul are o semnătură în care sistemul dumneavoastră are încredere; sistemul ignoră celelalte semnături care nu sunt de încredere de pe obiecte şi tratează obiectul ca şi um ar fi nesemnat.

Există anumite valori pe care le puteţi utiliza pentru variabila sistem QVFYOBJRST, de la ignorarea tuturor semnăturilor la necesitatea semnăturilor valide pentru toate obiectele pe care sistemul le restaurează. Această variabilă sistem afectează numai obiectele executabile care sunt restaurate, cum ar fi programele (*PGM), comenzile (*CMD), programele de serviciu (*SRVPGM), pachetele SQL (*SQLPKG) şi modulele (*MODULE). Se aplică de asemenea şi obiectelor fişiere şir (*STMF) care au asociate programe Java create prin comanda Create Java Program (Creare program Java - CRTJVAPGM). Nu se aplică fişierelor de salvare (*SAV) sau fişierelor IFS.

Pentru a afla mai multe despre utilizarea acestei variabile sistem şi a altor variabile sistem, consultaţi System Value Finder (Găsirea variabilelor sistem) din Centrul de informare.

Comenzi CL care afectează obiectele semnate

Există mai multe comenzi CL care vă permit să gestionaţi obiectele semnate sau care afectează obiectele semnate de pe serverul dumneavoastră iSeries. Puteţi utiliza o varietate de comenzi pentru vizualizarea informaţiilor de semnătură pentru obiecte, verificarea semnăturii de pe obiecte şi salvarea şi restaurarea obiectelor necesare pentru verificarea semnăturilor. În plus, există un grup de comenzi care, atunci când rulează, pot înlătura semnăturile de pe obiecte şi anula protecţia pe care semnăturile o oferă.

Comenzi pentru vizualizarea informaţiilor de semnătură pentru un obiect

- Comanda Display Object Description - Afişare descriere obiect (DSPOBJD)
  Această comandă afişează numele şi atributele obiectelor specificate din biblioteca specificată sau din

bibliotecile din lista de biblioteci a firului de execuţie. Puteţi utiliza această comandă pentru a determina dacă un obiect este semnat şi pentru a vizualiza informaţii despre semnătură.

- Comenzile sistemului de fişiere integrat Display Object Link - Afişare legături obiect (DSPLNK) şi Work with Object Links - Gestionare legături obiect (WRKLNK).
  Puteţi utiliza oricare dintre aceste comenzi pentru a afişa informaţiile de semnătură pentru un obiect din sistemul de fişiere integrat.

Comenzi pentru verificarea semnăturilor obiectelor

- Comanda Check Object Integrity - Verificarea integrităţii obiectului (CHKOBJITG).
  Această comandă vă permite să determinaţi dacă obiectele de pe sistemul dumneavoastră au încălcări de integritate. Puteţi utiliza această comandă pentru verificarea semnăturilor într-un mod asemănător cu cel în care utilizaţi un antivirus pentru a determina dacă un virus a corupt fişiere sau alte obiecte de pe sistemul dumneavoastră. Pentru a afla mai multe despre utilizarea acestei comenzi cu obiecte semnate şi obiecte care se pot semna, consultaţi Comenzi de verificare a codurilor pentru asigurarea integrităţii semnăturilor.
- Comanda Check Product Option - Verificarea opţiunilor produsului (CHKPRDOPT).
  Această comandă raportează diferenţele dintre structura corectă şi structura curentă a unui produs software. De exemplu comanda raportează o eroare dacă un obiect este şters dintr-un produs instalat. Puteţi utiliza parametrul CHKSIG pentru a specifica modul în care comanda trebuie să trateze şi să raporteze posibilele probleme de semnătură pentru produs. Pentru a afla mai multe despre utilizarea acestei comenzi cu obiecte semnate şi obiecte care se pot semna, consultaţi Comenzi de verificare pentru asigurarea integrităţii semnăturilor.
- Comanda Save Licensed Program - Salvare program licenţiat (SAVLICPGM).
  Această comandă salvează o copie a obiectelor care alcătuiesc un program licenţiat. Aceasta salvează programul licenţiat într-o formă care poate fi apoi restaurată de comanda Restore Licensed Program - Restaurare program licenţiat (RSTLICPGM). Puteţi utiliza parametrul CHKSIG pentru a specifica modul în care comanda trebuie să trateze şi să raporteze posibilele probleme de semnătură pentru produs. Pentru a afla mai multe despre utilizarea acestei comenzi cu obiecte semnate şi obiecte care se pot semna, consultaţi Comenzi de verificare a codurilor pentru asigurarea integrităţii semnăturilor.
- Comanda Restore - Restaurare (RST).
  Această comandă restaurează o copie a unuia sau mai multor obiecte care poate fi utilizată în sistemul de fişiere integrat (IFS). Această comandă vă permite de asemenea să restauraţi memorii de certificare şi conţinutul lor pe sistem. Totuşi, nu puteţi utiliza această comandă pentru restaurarea memoriei de certificare *SIGNATUREVERIFICATION. Modul în care comanda de restaurare tratează obiectele semnate şi obiectele care se pot semna este determinată de setarea pentru variabila sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVFYOBJRST).
- Comanda Restore Library - Restaurare bibliotecă (RSTLIB).
  Acesată comandă restaurează o bibliotecă sau un grup de biblioteci care a fost salvat de comanda Save Library - Salvare bibliotecă (SAVLIB). Comanda RSTLIB restaurează întreaga bibliotecă, care include descrierea bibliotecii, descrierile obiectelor şi conţinutul obiectelor din bibliotecă. Modul în care această comandă tratează obiectele semnate şi obiectele care se pot semna este determinat de setarea variabilei sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVFYOBJRST).
- Comanda Restore Licensed Program - Restaurare program licenţiat (RSTLICPGM).
  Această comandă încarcă sau restaurează un program licenţiat, fie pentru instalarea iniţială, fie pentru instalarea unei noi ediţii. Modul în care această comandă tratează obiectele semnate şi obiectele care se pot semna este determinat de setarea variabilei sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVFYOBJRST).
- Comanda Restore object - Restaurare obiect (RSTOBJ).
  Această comandă restaurează unul sau mai multe obiecte dintr-o singură bibliotecă, ce au fost salvate pe dischetă, bandă, volum optic sau într-un fişier prin utilizarea unei singure comenzi. Modul în care această comandă tratează obiectele semnate şi obiectele care se pot semna este determinat de setarea pentru variabila sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVFYOBJRST).

Comenzi pentru salvarea şi restaurarea memoriilor de certificare

- Comanda Save - Salvare (SAV).
  Această comandă vă permite să salvaţi o copie a unuia sau mai multor obiecte care poate fi utilizată în sistemul de fişiere integrat, incluzând memoriile de certificare. Totuşi, nu puteţi utiliza această comandă pentru salvarea memoriei de certificare *SIGNATUREVERIFICATION.
- Comanda Save Security Data - Salvare date de securitate (SAVSECDTA).
  Această comandă vă permite să salvaţi toate informaţiile de securitate fără a solicita sistemului să fie într-o stare restricţionată. Utilizarea acestei comenzi vă permite să salvaţi memoria de certificare *SIGNATUREVERIFICATION şi certificatele pe care le conţine. Această comandă nu salvează nici o altă memorie de certificare.
- Comanda Save System - Salvare sistem (SAVSYS).
  Această comandă vă permite să salvaţi o copie a codului intern licenţiat şi a bibliotecii QSYS într-un format compatibil cu instalarea serverului iSeries. Aceasta nu salvează obiecte din nici o altă bibliotecă. În plus, vă permite să salvaţi obiectele de securitate şi de configurare pe care le puteţi de asemenea salva utilizând comenzile SAVECDTA şi SAVCFG. Utilizarea acestei comenzi vă permite să salvaţi memoria de certificare *SIGNATUREVERIFICATION şi certificatele pe care le conţine.
- Comanda Restore - Restaurare (RST).
  Această comandă vă permite să restauraţi memoriile de certifcare şi conţinutul lor pe sistem. Totuşi, nu puteţi utiliza această comandă pentru restaurarea memoriei de certificare *SIGNATUREVERIFICATION.
- Comanda Restore User Profiles - Restaurare profile utilizator (RSTUSRPRF).
  Această comandă vă permite să restauraţi părţile de bază ale unui profil utilizator sau un set de profile utilizator salvate prin comenzile Save System - Salvare sistem (SAVSYS) sau Save Security Data - Salvare date de securitate (SAVSECDTA). Puteţi utiliza această comandă pentru restaurarea memoriei de certificare *SIGNATUREVERFICATION şi a parolei pentru aceasta şi pentru restaurarea tuturor celorlaltor memorii de certificare. Puteţi restaura memoria de certificare *SIGNATUREVERIFICATION fără restaurarea informaţiilor de profil utilizator specificând *DCM ca valoare pentru parametrul SECDTA şi *NONE pentru parametrul USRPRF. Pentru utilizarea acestei comenzi la restaurarea informaţiilor de profil utilizator şi a memoriilor de certificare şi a parolelor acestora, specificaţi *ALL pentru parametrul USRPRF.

Comenzi care pot înlătura sau pierde semnături de pe obiecte

Când utilizaţi următoarele comenzi pe un obiect semnat, puteţi proceda într-un mod care ar putea înlătura sau pierde semnătura de pe obiect. Înlăturarea semnăturii poate cauza probleme cu obiectul afectat. În cel mai bun caz, nu veţi mai putea verifica sursa obiectului dacă este de încredere şi nu veţi mai putea verifica semnătura pentru detectarea modificărilor aduse obiectului. Ar trebui să utilizaţi aceste comenzi numai pe acele obiecte semnate pe care le-aţi creat dum neavoastră (în opoziţie cu obiectele semnate pe care le obţineţi de la alţii, cum ar fi IBM sau alţi vânzători). Dacă sunteţi îngrijorat că o comandă a înlăturat sau a pierdut semnătura unui obiect, puteţi utiliza comnada Display Object Description - Afişare descriere obiect (DSPOBJD) pentru a vedea dacă semnătura mai este acolo şi să semnaţi din nou obiectul dacă este necesar.

Notă: Pentru a verifica dacă o comandă Salvare a pierdut semnătura unui obiect, trebuie să restauraţi obiectul într-o bibliotecă diferită de cea în care l-aţi salvat (de exemplu, QTEMP). Puteţi utiliza comanda DSPOBJD pentru a determina dacă obiectul de pe suportul magnetic de salvare şi-a pierdut semnătura.

- Comanda Change Program - Modificare program (CHGPGM).
  Această comandă modifică atributele unui program fără a cere recompilarea lui. De asemenea, puteţi utiliza această comandă pentru a forţa recrearea unui program chiar dacă atributele specificate sunt la fel ca atributele curente.
- Comanda Change Service Program - Modificare program de serviciu (CHGSRVPGM).
  Această comandă modifică atributele unui program de serviciu fără a cere recompilarea lui. De asemenea, puteţi utiliza această comandă pentru a forţa recrearea unui program de serviciu chiar dacă atributele specificate sunt la fel ca atributele curente.

- Comanda Clear Save File - Curăţare fişier de salvare (CLRSAVF).
  Această comandă curăţă conţinutul unui fişier de salvare; ea curăţă toate înregistrările existente din fişierul de salvare şi reduce cantitatea de memorie pe care o utilizează fişierul.
- Comanda Save - Salvare (SAV).
  Această comandă salvează o copie a unuia sau mai multor obiecte care poate fi utilizată în sistemul de fişiere integrat. —Când utilizaţi această comandă, puteţi pierde semnătura obiectelor comandă (*CMD) de pe suportul magnetic de salvare dacă specificaţi o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu pot fi semnate în ediţii anterioare V5R2.
- Comanda Save Library - Salvare bibilotecă (SAVLIB).
  Această comandă vă permite să salvaţi o copie a uneia sau mai multor biblioteci. Când utilizaţi această comandă, puteţi pierde semnătura obiectelor comandă (*CMD) de pe suportul magnetic de salvare dacă specificaţi o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu pot fi semnate în ediţii anterioare V5R2.
- Comanda Save Object - Salvare obiect (SAVOBJ).
  Această comandă salvează o copie a unui singur obiect sau a unui grup de obiecte localizate în aceeaşi bibliotecă. Când utilizaţi această comandă, puteţi pierde semnătura obiectelor comandă (*CMD) de pe suportul magnetic dacă specificaţi o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu por fi semnate în ediţii anterioare V5R2.

Consideraţii de salvare şi restaurare pentru obiectele semnate

Există anumite variabile sistem care pot afecta operaţiile de restaurare pentru serverul dumneavoastră iSeries. Numai una dintre aceste variabile sistem, variabila sistem **verificarea semnăturilor obiectelor în timpul restaurării (QVFYOBJRST)**, determină modul în care sistemul tratează obiectele semnate atunci când le restaurează. Setarea pe care o alegeţi pentru această variabilă sistem vă permite să determinaţi modul în care procesul de restaurare tratează verificarea obiectelor fără semnături sau cu semnături care nu sunt valide.

Unele comenzi de salvare şi restaurare afectează obiectele semnate sau determină modul în care sistemul dumneavoastră tratează obiectele semnate şi nesemnate în timpul operaţiilor de salvare şi restaurare. Trebuie să înţelegeţi aceste comenzi şi impactul lor asupra obiectelor semnate astfel încât să puteţi gestiona mai bine sistemul dumneavoastră şi să evitaţi potenţialele probleme care pot apărea.

Aceste comenzi pot verifica semnăturile pe obiecte în timpul operaţiilor de salvare şi restaurare:

- Comanda Save Licensed Program - Salvare program licenţiat (SAVLICPGM).
- Comanda Restore - Restaurare (RST).
- Comanda Restore Library - Restaurare bibliotecă (RSTLIB).
- Comanda Restore Licensed Program - Restaurare program licenţiat (RSTLICPGM).
- Comanda Restore object - Restaurare obiect (RSTOBJ).

Aceste comenzi vă permit să salvaţi şi să restauraţi memorii de certificare; memoriile de certificare sunt obiecte sensibile la securitate care conţin certificatele pe care le utilizaţi pentru semnarea obiectelor şi verificarea semnăturilor:

- Comanda Save - Salvare (SAV).
- Comanda Save Security Data - Salvare date de securitate (SAVSECDTA).
- Comanda Save System - Salvare sistem (SAVSYS).
- Comanda Restore - Restaurare (RST).
- Comanda Restore User Profiles - Restaurare profile utilizator (RSTUSRPRF).

Unele comenzi de salvare, în funcţie de valorile parametrilor pe care le utilizaţi, pot pierde semnătura unui obiect de pe suportul magnetic de salvare, anulând astfel securitatea pe care semnătura o oferă. De exemplu, *orice* operaţie de salvare care referă un obiect comandă (*CMD) cu o ediţie destinaţie anterioară

V5R2M0 determină salvarea comenzii fără semnături. Înlăturarea semnăturii poate cauza probleme cu obiectele afectate. În cel mai bun caz, nu veţi mai putea verifica sursa obiectului dacă este de încredere şi nu veţi mai putea verifica semnătura pentru detectarea modificărilor aduse obiectului. Ar trebuie să utilizaţi acest comenzi numai pe acele obiecte semnate pe care le-aţi creat dumneavoastră (în opoziţie cu obiectele semnate pe care la obţineţi de la alţii, cum ar fi IBM sau alţi vânzători).

Notă: Pentru a verifica dacă o comandă Salvare a pierdut semnătura unui obiect, trebuie să restauraţi obiectul într-o bibliotecă diferită de cea în care l-aţi salvat (de exemplu, QTEMP). Puteţi utiliza comanda DSPOBJD pentru a determina dacă obiectul de pe suportul magnetic de salvare şi-a pierdut semnătura.

Trebuie să cunoaşteţi aceste lucruri pentru următoarele comenzi de salvare specifice, ca şi pentru comenzile de salvare în general:

- Comanda Save - Salvare (SAV).
- Comanda Save Library - Salvare bibliotecă (SAVLIB).
- Comanda Save Object - Salvare obiect (SAVOBJ).

Pentru informaţii suplimentare despre modul în care aceste comenzi afectează obiectele semnate şi semnăturile obiectelor în timpul operaţiilor de salvare şi restaurare, consultaţi Variabile sistem şi comenzi care afectează obiectele semnate.

Comenzi de verificare a codurilor pentru a asigura integritatea semnăturilor

Puteţi utiliza Managerul de certificare digitală (DCM) sau API-urile pentru verificarea semnăturilor de pe obiecte. Puteţi de asemenea să utilizaţi câteva comenzi pentru verificarea semnăturilor. Utilizarea acestor comenzi vă permite să verificaţi semnături într-un mod asemnător cu cel în care utilizaţi un antivirus pentru a determina dacă un virus a corupt fişiere sau alte obiecte pe sistemul dumneavoastră. Majoritatea semnăturilor sunt verificate pe măsură ce obiectul este restaurat sau instalat pe sistem, de exemplu prin utilizarea comenzii RSTLIB.

Puteţi alege una din trei comenzi pentru verificarea semnăturilor obiectelor care sunt deja pe sistem. Dintre acestea, comanda Check Object Integrity - Verificarea integrităţii obiectului (CHKOBJITG) este desemnată specific pentru verificarea semnăturilor obiectelor. Verificarea semnăturilor pentru fiecare dintre aceste comenzi este controlată de parametrul CHKSIG. Acest parametru vă permite să verificaţi semnăturile pe toate tipurile de obiecte care pot fi semnate, să ignoraţi toate semnăturile sau să verificaţi numai obiectele care au semnături. Ultima opţiune este valoarea implicită pentru parametru.

Comanda Check Object Integrity - Verificarea integrităţii obiectului (CHKOBJITG)

Comanda Check Object Integrity - Verificarea integrităţii obiectului (CHKOBJITG) vă permite să determinaţi dacă obiectele de pe sistemul dumneavoastră au încălcări de integritate. Puteţi utiliza această comandă pentru verificarea încălcărilor de integritate pentru obiecte deţinute de un anumit profil utilizator, pentru obiecte care se potrivesc cu un anumit nume de cale sau pentru toate obiectele de pe sistem. O intrare în istoricul de încălcări de integritate apare atunci când este îndeplinită una dintre aceste condiţii:

- O comandă, un program, un obiect modul sau atributele unei biblioteci au fost modificate.
- Semnătura digitală de pe un obiect este nevalidă. Semnătura este un rezumat matematic cifrat al datelor din obiect; de aceea, semnătura este considerată corespunzătoare şi validă dacă datele din obiect în timpul verificării se potrivesc cu datele din obiect atunci când acesta a fost semnat. O semnătură nevalidă este determinată pe baza unei comparaţii între rezumatul matematic cifrat care este creat când obiectul este semnat şi rezumatul matematic cifrat realizat în timpul verificării semnăturii. Procesul de verificare a semnăturilor compară cele două valori ale rezumatelor. Dacă valorile nu sunt la fel, conţinutul obiectului a fost modificat după semnarea lui şi semnătura este considerată nevalidă.
- Un obiect are un atribut de domeniu incorect pentru tipul de obiect.

•

Dacă comanda detectează o încălcare de integritate pentru un obiect, adaugă numele obiectului, numele bibliotecii (sau numele căii), tipul obiectului, proprietarul obiectului şi tipul de eşuare în fişierul istoric al bazei de date. Comanda creează o intrare în istoric şi în alte câteva cazuri, deşi aceste cazuri nu sunt încălcări de integritate. De exemplu, comanda creează o intrare în istoric pentru obiecte care se pot semna dar nu au o semnătură digitală, pentru obiecte care nu pot fi verificate şi pentru obiecte într-un format care necesită modificări pentru a fi utilizate pe implementarea curentă a sistemului (conversie IMPI la RISC).

Valoarea parametrului CHKSIG controlează modul în care comanda tratează semnăturile digitale de pe obiecte. Puteţi specifica una din trei valori pentru acest parametru:

- *SIGNED – Când specificaţi această valoare, comanda verifică obiectele cu semnături digitale. Comanda creează o intrare în istoric pentru orice obiect cu o semnătură nevalidă. Aceasta este valoarea implicită.
- *ALL – Când specificaţi această valoare, comanda verifică toate obiectele care se pot semna pentru a determina dacă au o semnătură. Comanda creează o intrare în istoric pentru orice obiect care se poate semna dar nu are o semnătură şi pentru orice obiect cu o semnătură nevalidă.
- *NONE – Când specificaţi această valoare, comanda nu verifică semnăturile digitale de pe obiecte.

Comanda Check Product Option - Verificarea opţiunilor produsului (CHKPRDOPT)

Comanda Check Product Option - Verificarea opţiunilor produsului (CHKPRDOPT) raportează diferenţele dintre structura corectă şi structura reală a unui produs software. De exemplu, comanda raportează o eroare dacă un obiect este şters dintr-un produs instalat.

Valoarea parametrului CHKSIG controlează modul în care comanda tratează semnăturile digitale de pe obiecte. Puteţi specifica una din trei valori pentru acest parametru:

- *SIGNED – Când specificaţi această valoare, comanda verifică obiectele cu semnături digitale. Comanda verifică semnăturile pe orice obiecte semnate. Dacă comanda determină că semnătura de pe un obiect nu este validă, comanda trimite un mesaj în istoricul jobului şi identifică produsul ca fiind într-o stare eronată. Aceasta este valoarea implicită.
- *ALL – Când specificaţi această valoare, comanda verifică toate obiectele care se pot semna pentru a determina dacă au o semnătură şi verifică semnătura pe aceste obiecte. Comanda trimite un mesaj în istoricul jobului pentru orice obiect care se poate semna dar nu are o semnătură; totuşi, comanda nu identifică produsul ca fiind eronat. Dacă comanda determină că semnătura de pe un obiect nu este validă, trimite un mesaj în istoricul jobului şi consideră produsul eronat.
- *NONE – Când specificaţi această valoare, comanda nu verifică semnăturile digitale pe obiectele produsului.

Comanda Save Licensed Program - Salvare program licenţiat (SAVLICPGM)

Comanda Save Licensed Program - Salvare program licenţiat (SAVLICPGM) vă permite să salvaţi o copie a obiectelor care alcătuiesc un program licenţiat. Aceasta salvează programul licenţiat într-o formă care poate fi restaurată prin comanda Restore Licensed Program - Restaurare program licenţiat (RSTLICPGM).

Valoarea parametrului CHKSIG controlează modul în care comenzile tratează semnăturile digitale de pe obiecte. Puteţi specifica una din trei valori pentru acest parametru:

- *SIGNED – Când specificaţi această valoare, comanda verifică obiectele cu semnături digitale. Comanda verifică semnăturile de pe orice obiecte semnate dar nu verifică obiectele nesemnate. Dacă comanda determină că semnătura de pe un obiect nu este validă, comanda trimite un mesaj în istoricul jobului pentru identificarea obiectului şi salvarea va eşua. Aceasta este valoarea implicită.
- *ALL – Când specificaţi această valoare, comanda verifică toate obiectele care se pot semna pentru a determina dacă au o semnătură şi verifică semnătura de pe aceste obiecte. Comanda trimite un mesaj în

istoricul jobului pentru orice obiect care se poate semna dar nu are o semnătură; totuşi, procesul de salvare nu este oprit. Dacă comanda determină că semnătura de pe un obiect nu este validă, trimite un mesaj în istoricul jobului şi salvarea va eşua.

- *NONE – Când specificaţi această valoare, comanda nu verifică semnăturile digitale pe obiectele produsului.

Depanarea obiectelor semnate

Puteţi utiliza următoarele tabele pentru găsirea informaţiilor care să vă ajute la depanarea câtorva probleme obişnuite pe care le puteţi întâlni în timpul lucrului cu capacităţile iSeries de semnare a obiectelor şi de verificare a semnăturilor.

Probleme obişnuite la semnarea obiectelor

Problemă	Soluţie posibilă
Când utilizaţi API Semnare obiect pentru semnarea unui obiect cu o ediţie destinaţie V4R5 sau anterioară, procesul de semnare eşuează şi obiectul nu este semnat (mesaj de eroare CPFB721).	iSeries nu oferă suport pentru semnarea obiectelor până la V5R1. Pentru acele obiecte care întorc un mesaj de eroare CPFB721, trebuie să creaţi din nou programele respective cu o ediţie destinaţie V5R1 sau mai recentă pentru a le putea semna.

Probleme comune la verificarea semnăturilor

Problemă	Soluţie posibilă
Procesul de restaurare eşuează pentru obiectele fără semnătură.	Dacă lipsa semnăturii nu este o problemă, verificaţi dacă variabila sistem QVFYOBJRST este setată la 5. O valoare de 5 specifică faptul că obiectele nesemnate nu pot fi restaurate. Modificaţi valoarea la 3 şi încercaţi din nou restaurarea.
Procesul de restaurare eşuează pentru obiectele cu semnătură.	Acest lucru se poate întâmpla dacă memoria de certificare *SIGNATUREVERIFICATION a fost transferată pe sistem şi DCM nu a fost utilizat pentru modificarea parolei pentru aceasta. Într-un astfel de caz, certificatele pe care memoria le conţine nu pot fi utilizate pentru verificarea semnăturilor pe obiecte în timpul procesului de restaurare. Utilizaţi DCM la modificarea parolei pentru memoria de certificare. Dacă nu cunoaşteţi parola, va trebuie să ştergeţi memoria de certificare; creaţi-o din nou şi utilizaţi DCM pentru modificarea parolei.
Când instalaţi un produs, primiţi o eroare deoarece semnătura nu a trecut de verificare.	Când semnătura unui obiect nu se verifică în mod corect, eşuarea poate indica faptul că obiectul a fost modificat din momentul în care a fost semnat. Dacă integritatea obiectului este problema, nu trebuie să modificaţi variabila sistem QVFYOBJRST sau să efectuaţi alte acţiuni care ar putea permite obiectului în cauză să fie restaurat. Procedând astfel, veţi anula securitatea pe care verificarea semnăturilor o oferă şi veţi permite intrarea obiectelor dăunătoare în sistemul dumneavoastră. În schimb, ar trebui să contactaţi semnatarul obiectului pentru a determina acţiunea corespunzătoare de efectuat pentru rezolvarea problemei.

Informaţii înrudite pentru semnarea obiectelor şi verificarea semnăturilor

Semnarea obiectelor şi verificarea semnăturilor sunt tehnologii de securitate relativ noi. Aici aveţi o mică listă cu alte resurse pe care le puteţi considera utile dacă sunteţi interesat de o înţelegere mai aprofundată a acestor tehnologii şi a modului în care ele funcţionează:

- **Site-ul Web VeriSign Help Desk**
  Site-ul Web VeriSign oferă o bibliotecă extensivă cu subiecte legate de certificate digitale, cum ar fi semnarea obiectelor, ca şi alte subiecte de securitate a Internetului.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM şi Cryptographic Enhancements (Îmbunătăţiri criptografice) SG24-6168**
  Această IBM Redbook (Carte roşie) este axată pe îmbunătăţirile de securitate a reţelelor în V5R1. Cartea roşie acoperă multe subiecte inclusiv modul de utilizare a capacităţilor iSeries de semnare a obiectelor, Digital Certificate Manager - Managerul de certificare digitală (DCM), şi aşa mai departe.

Tipărit în S.U.A.