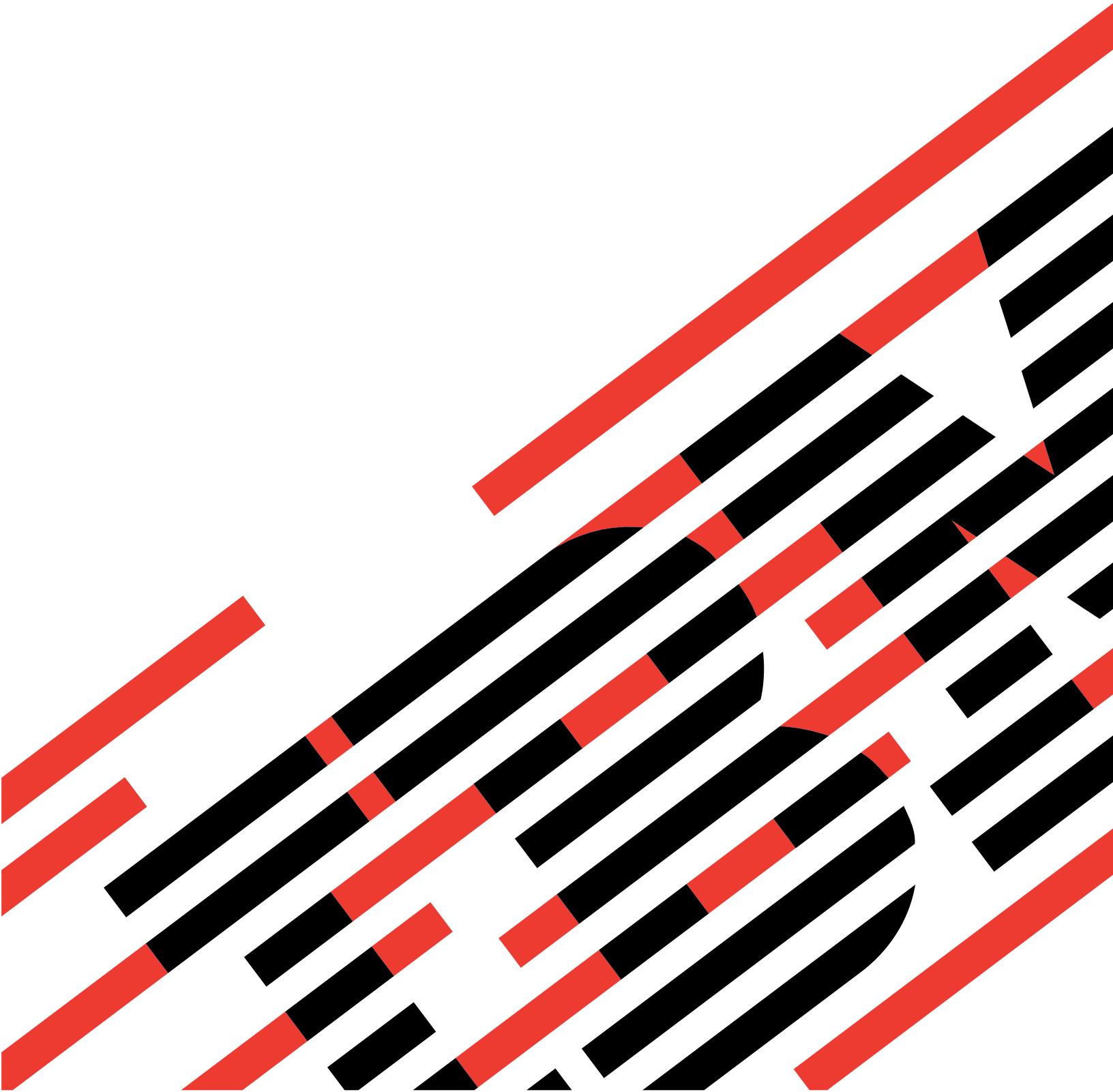
IBM

eserver

iSeries

Semnarea obiectelor şi verificarea semnăturii

Versiunea 5 Ediţia 3



IBM

@server

iSeries

Semnarea obiectelor şi verificarea semnăturii

Versiunea 5 Ediţia 3

Notă

Înainte de a utiliza aceste informaţii şi produsul la care se referă, aveţi grijă să citiţi “Observaţii”, la pagina 47.

Ediţia a treia (august 2005)

Această ediţie este valabilă pentru IBM Operating System/400 (număr produs 5722–SS1) versiunea 5, ediţia 3, modificarea 0 şi pentru toate ediţiile şi modificările următoare, până când este indicat altfel în ediţiile noi. Această versiune nu rulează pe toate modelele RISC (computer cu set de instrucţiuni redus) şi nici pe modelele CISC.

Cuprins

Semnarea obiectelor şi verificarea semnăturii

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 furnizează dovada autenticităţii şi 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 este nou pentru V5R3
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
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 operaţiile de configurare pe care trebuie să le realizaţi pentru a implementa scenariul aşa cum este descris.

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

Această declinare a responsabilităţii pentru cod se aplică pentru exemplele de cod care sunt furnizate în cadrul acestui subiect.

Ce este nou pentru V5R3

Capacităţile de semnare a obiectelor şi de verificare a semnăturilor pentru iSeries au fost introduse pentru prima dată în V5R1. Totuşi, există unele funcţii şi îmbunătăţiri noi disponibile în V5R3.

Funcţiile noi sau îmbunătăţite pentru semnarea obiectelor şi verificarea semnăturilor includ:
- **Verificarea integrităţii sistemului iSeries**
  Începând cu V5R3, puteţi verifica integritatea întregului cod furnizat de IBM pentru sistemul dumneavoastră iSeries.
- **Verificarea funcţiei de verificare a codului**
  Începând cu V5R3, puteţi verifica integritatea funcţiei de verificare a codului care verifică codul sistemului şi alte obiecte semnate de pe sistemul dumneavoastră iSeries.

Pentru a afla alte informaţii despre ceea ce este nou sau modificat în această ediţie, vedeţi Memo către utilizatori .

Cum să vedeţi ce este nou sau modificat

Pentru a vă ajuta să vedeţi unde au fost efectuate modificări tehnice, această informare utilizează:
- Imaginea pentru a marca unde încep informaţiile noi sau modificate.
- Imaginea pentru a marca unde se termină informaţiile noi sau modificate.

Tipăriţi acest subiect

Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectaţi Semnarea obiectelor şi verificarea semnăturii (dimensiune fişier 605 KB).

Salvarea fişierelor PDF:

Pentru a salva un PDF pe staţia dumnevoastră de lucru pentru vizualizare sau tipărire:
1. Faceţi clic pe PDF în browser-ul dumneavoastră (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe **Save Target As...** dacă utilizaţi Internet Explorer. Faceţi clic pe **Save Link As...** dacă utilizaţi Netscape Communicator.
3. Navigaţi în directorul în care doriţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save (Salvare)**.

Descărcarea Adobe Acrobat Reader

Aveţi nevoie de Adobe Acrobat Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca o copie de pe situl Web Adobe (www.adobe.com/products/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 nevoile 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 că 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 operaţiile 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

Situaţia

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

Severul Web public al companiei furnizează un sit Web cu informaţii generale despre companie. Situl 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. Sunteţi preocupat de vulnerabilitatea programelor cgi-bin care furnizează aceste formulare; cunoaşteţi că acestea pot 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 mic de servere iSeries şi nu credeţi că va trebui să semnaţi obiecte des, aţi decis să utilizaţi Managerul de certificate digitale (DCM) pentru a efectua aceste operaţii. 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 dumneavoastră şi altor persoane din companie să realizeze aceste operaţii 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 certificate digitale (DCM) pentru a semna aceste obiecte şi pentru a verifica semnăturile obiectelor.

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) locală în fiecare depozit de certificate *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:

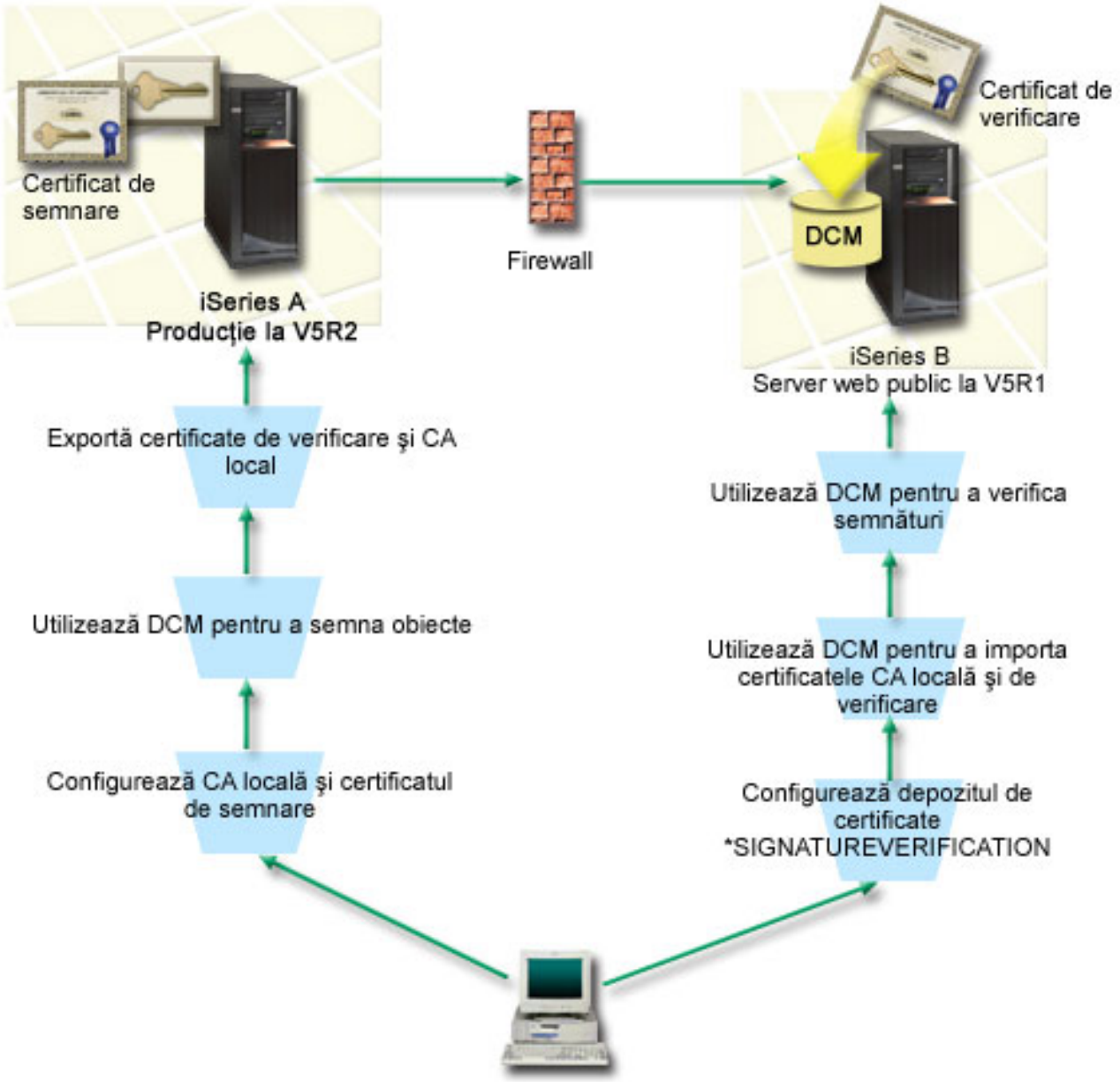


Figura ilustrează următoarele puncte relevante pentru acest scenariu:

iSeries A

- iSeries A rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries A este serverul de producţie intern al companiei şi platforma de dezvoltare pentru serverul Web iSeries public (iSeries B).
- iSeries A are instalat un Furnizor de acces criptografic pe 128 de biţi pentru 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 ca Autoritatea de certificare (CA) locală 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 alte 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, iar iSeries B nu semnează obiecte.
- iSeries B este configurat pentru activarea verificării semnăturilor utilizând DCM pentru crearea depozitului de certificate *SIGNATUREVERIFICATION şi pentru importarea verificării necesare şi a certificatelor CA local.
- DCM este utilizat pentru a verifica semnăturile obiectelor.

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 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.
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 un depozit de certificate 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 operaţiei de configurare

Există două seturi de operaţii pe care trebuie să le efectuaţi pentru a implementa acest scenariu: Un set de operaţii 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 operaţii vă permite să configuraţi iSeries B pentru verificarea semnăturilor pe care iSeries A le creează.

Paşii pentru operaţiile pe **iSeries A**

Trebuie să efectuaţi fiecare dintre aceste operaţii 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 DCM pentru a crea o Autoritate de certificare locală (CA) pentru a emite un certificat pentru semnarea obiectelor.
3. Utilizaţi DCM pentru a crea o definiţie de aplicaţie
4. Utilizaţi DCM pentru a atribui un certificat pentru definiţia de aplicaţie pentru semnarea obiectelor
5. Utilizaţi DCM pentru a semna obiectele program cgi-bin
6. Utilizaţi DCM pentru a exporta certificatele pe care trebuie să le utilizeze celelalte sisteme 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 iSeries public al companiei (iSeries B) pentru ca dumneavoastră sau alţii să puteţi verifica semnăturile pe care le creează iSeries A

Paşii operaţiilor pe **iSeries B**

Dacă intenţionaţi să restauraţi obiectele semnate pe care le transferaţi pe serverul Web public din acest scenariu (iSeries B), trebuie să efectuaţi aceste operaţii de configurare pentru verificarea semnăturii pe iSeries B înainte de a 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 operaţii pentru verificarea semnăturilor de pe obiecte aşa cum descrie acest scenariu:

8. Utilizaţi Managerul de certificate digitale (DCM) pentru a crea depozitul de certificate *SIGNATUREVERIFICATION
9. Utilizaţi DCM pentru a importa certificatul CA locale şi certificatul pentru verificarea semnăturii
10. Utilizaţi DCM pentru a verifica semnăturile pentru obiectele transferate

Detalii scenariu: Utilizaţi DCM pentru a semna obiecte şi pentru a verifica semnăturile

Efectuaţi următorii paşi de operaţie 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 operaţiile preliminare pentru instalarea şi configurarea tuturor produselor iSeries necesare înainte de a putea realiza operaţiile de configurare specifice pentru implementarea acestui scenariu.

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

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 operaţii 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 operaţie 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 acestă operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Completaţi toate formularele pentru acestă operaţie ghidată. Pe măsură ce efectuaţi acestă operaţie, 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 operaţia fără a crea acest certificat, trebuie să vă creaţi certificatul de semnare a obiectelor şi depozitul de certificate *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 depozitul de certificate *OBJECTSIGNING. Aceasta este depozitul de certificate pe care îl utilizaţi pentru gestionarea certificatelor de semnare a obiectelor.
g. Selectaţi aplicaţiile care vor avea încredere în CA locală.

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

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 de aplicaţie pentru semnarea 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 de aplicaţie nu trebuie să se refere la o aplicaţie reală; definiţia de aplicaţie pe care o creaţi poate 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 **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** ca depozitul de certificate pe care să-l deschideţi.
2. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.
3. În cadrul de navigare, selectaţi **Gestiune aplicaţii** pentru a afişa o listă de operaţii.
4. Selectaţi **Adăugare aplicaţie** din lista de operaţii 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 operaţii.
2. Din lista de operaţii, selectaţi **Alocare certificat** pentru afişarea unei liste de certificate pentru depozitul de certificate curent.
3. Selectaţi un certificat din listă şi faceţi clic pe **Alocare la aplicaţie** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate.
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 această operaţie, 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 **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** ca depozitul de certificate pe care să-l deschideţi.
2. Introduceţi parola pentru depozitul de certificate *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 operaţii.
4. Din lista de operaţii, 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 a semna toate obiectele dintr-un anumit director, puteţi introduce /mydirectory/*; pentru a semna toate programele 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** pentru a vedea o listă cu conţinutul bibliotecii sau directorului, trebuie să introduceţi caracterul de substituţie ca parte a numelui de cale 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 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).
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 şi 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 operaţiile 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 da posibilitatea verificării semnăturii pe iSeries B

Semnarea obiectelor pentru protejarea integrităţii conţinutului necesită ca dumneavoastră şi alte persoane să aveţi un mijloc pentru verificarea autenticităţii semnăturilor. Pentru verificarea semnăturilor obiectelor pe acelaşi sistem care semnează obiectele (iSeries A), trebuie să utilizaţi DCM pentru crearea depozitului de certificate *SIGNATUREVERIFICATION. Aceast depozit de certificate 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 furnizaţi o copie a certificatului care a semnat obiectul. Atunci când utilizaţi o Autoritate de certificare (CA) locală pentru a emite certificatul, trebuie de asemenea să le furnizaţi 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 depozit de certificate nou** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate pe care să-l creaţi.
2. Selectaţi **Da** pentru copierea certificatelor existente de semnare a obiectelor în noul depozit de certificate ca certificate de verificare a semnăturilor.

3. Specificaţi o parolă pentru noul depozit de certificate şi faceţi clic pe **Continuare** pentru a crea depozitul de certificate. 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 puteţi verifica semnăturile obiectelor pe alte sisteme (iSeries B), urmaţi aceşti paşi:

1. În cadrul de navigare, selectaţi **Gestiune certificate**, şi apoi selectaţi operaţia **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. Re-selectaţi operaţia **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 7: Transferaţi fişierele certificat pe serverul public al companiei iSeries B

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 FTP (File Transfer Protocol) sau distribuirea de pachete din Administrare centrală pentru a transfera fişierele.

Pasul 8: operaţii de verificare a semnăturii: Creaţi depozitul de certificate *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 depozitul de certificate *SIGNATUREVERIFICATION. Deoarece aţi utilizat un certificat emis de o CA locală pentru semnarea obiectelor, acest depozit de certificate trebuie să conţină şi o copie a certificatului CA locală.

Pentru crearea depozitului de certificate *SIGNATUREVERIFICATION, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al Managerului de certificare digitală (DCM) selectaţi **Creare depozit de certificate nou** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate pe care să-l creaţi.

   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 a accesa ajutorul online.
3. Specificaţi o parolă pentru noul depozit de certificate şi faceţi clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteţi importa certificatele în depozit şi le puteţi utiliza pentru verificarea semnăturilor obiectelor.

Pasul 9: operaţii de verificare a semnăturii: Importaţi certificatele

Pentru a verifica semnătura de pe un obiect, depozitul de certificate *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului de verificare a semnăturilor. Dacă certificatul de semnare este privat, acest depozit de certificate

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 depozitul *SIGNATUREVERIFICATION, urmaţi aceşti paşi:
1. În cadrul de navigare al DCM, faceţi clic pe **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de verificare pe care să-l deschideţi.
2. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune certificate** pentru a afişa o listă de operaţii.
4. Din lista de operaţii, 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. Re-selectaţi operaţia **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: operaţii de verificare a semnăturii: Verificaţi semnătura pentru obiectele program

Pentru a utiliza DCM la verificarea semnăturilor pe obiecte program transferate, urmaţi aceşti paşi:
1. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate care să fie deschis.
2. Introduceţi parola pentru depozitul de certificate *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 operaţii.
4. Din lista de operaţii, 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 a semna toate obiectele dintr-un anumit director, puteţi introduce /mydirectory/*; pentru a semna toate programele 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 pentru a vedea o listă cu conţinutul bibliotecii sau directorului, trebuie să introduceţi caracterul de substituţie ca parte a numelui de cale 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

Situaţia

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 dumneavoastră 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 furnizaţi 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. Ca dezvoltator de producere de aplicaţii la MyCo, Inc, împachetaţi curent aplicaţiile companiei dumneavoastră prin program pentru distribuirea la 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 depozitul de certificate a serverului clientului iSeries *SIGNATUREVERIFICATION. Compania trebuie să poată crea prin program acest depozit de certificate pe serverul iSeries al clientului ca parte din procesul de instalare a produsului, dacă acesta 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:

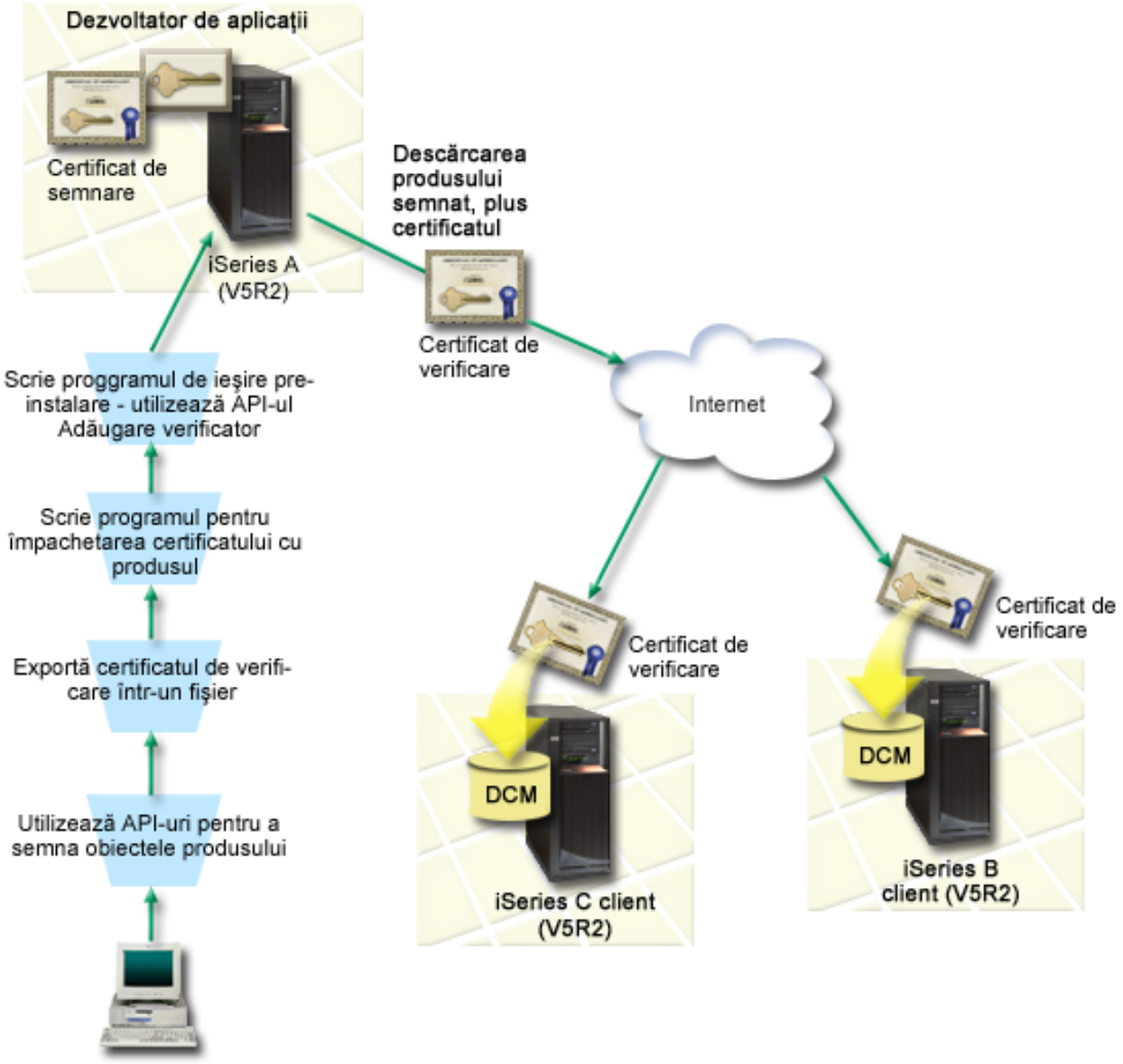


Figura ilustrează următoarele puncte relevante pentru acest scenariu:

Sistemul central (iSeries A)

- iSeries A rulează OS/400 Versiune 5 Ediţie 2 (V5R2).
- iSeries A rulează programul de împachetare produs al dezvoltatorului de aplicaţii.
- iSeries A are instalat un Furnizor de acces criptografic pe 128 de biţi pentru 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 este sistemul primar de semnare a obiectelor pentru produsele aplicaţie ale companiei. Semnarea obiectelor produsului pentru distribuirea către client este realizată pe iSeries A prin efectuarea acestor operaţii:
  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 a 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 prin program certificatul de verificare în depozitul de certificate *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 achiziţionează şi descarcă o aplicaţie de pe situl Web al companiei dezvoltatorului de aplicaţii (care deţine iSeries A).
- iSeries B şi C obţin o copie a certificatului de verificare a semnăturii al MyCo atunci când procesul de instalare a aplicaţie MyCo crează depozitul de certificate *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 depozitul de certificate *SIGNATUREVERIFICATION ca parte din procesul de instalare a produsului, dacă este necesar, îl 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 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.
5. Administratorul de reţea pentru iSeries A trebuie să aibă autorizarea specială *ALLOBJ pentru profilul utilizator pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicaţia de semnare a obiectelor.
6. Administratorul de sistem sau altcineva (inclusiv un program) care creează un depozit de certificate în DCM trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilul utilizator.
7. Administratorii de sistem sau alţii de pe celelalte servere iSeries trebuie să aibă autorizarea specială *AUDIT pentru profilul utilizator pentru verificarea semnăturilor obiectelor.

Paşii operaţiei de configurare

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

1. Efectuaţi toţi paşii preliminari pentru a instala şi configura toate produsele iSeries necesare
2. Utilizaţi DCM pentru a crea o cerere de certificat pentru a obţine un certificat pentru semnarea obiectelor de la o Autoritate de certificare (CA) publică bine cunoscută.
3. Utilizaţi DCM pentru a crea o definiţie de aplicaţie pentru semnare obiecte
4. Utilizaţi DCM pentru a importa certificatul pentru semnare al obiectului semnat şi pentru a-l atribui definiţiei dumneavoastră de aplicaţie pentru semnare obiecte
5. Utilizaţi DCM pentru a exporta certificatul dumneavoastră pentru semnare obiecte ca un certificat pentru verificarea semnăturii pentru ca clientul dumneavoastră să îl poată utiliza pentru a verifica semnătura pentru obiectele aplicaţiei dumneavoastră
6. Actualizaţi programul dumneavoastră pentru împachetare de aplicaţii pentru a utiliza API-ul Sign Object pentru a vă semna aplicaţia

7. Creaţi un program de ieşire de pre-instalare care utilizează API-ul Add Verifier ca parte a procesului dumneavoastră de împachetare de aplicaţii
   Acest program de ieşire vă permite să creaţi depozitul de certificate *SIGNATUREVERIFICATION şi să adăugaţi certificatul necesar de verificare a semnăturilor pe un server iSeries al unui client în timpul instalării produsului.
8. Puneţi clienţii să utilizeze DCM pentru a reseta parola implicită pentru depozitul de certificate *SIGNATUREVERIFICATION pe serverul lor iSeries

Detalii scenariu: Utilizaţi API-uri pentru a semna obiecte şi pentru a verifica semnăturile obiectelor

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

Pasul 1: Efectuaţi toţi paşii preliminari

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

Pasul 2: Utilizaţi DCM pentru a obţine un certificat de la o CA publică bine cunoscută

Acest scenariu presupune că nu aţi utilizat anterior Managerul de certificare digitală (DCM) pentru crearea şi gestionarea certificatelor. În consecinţă, trebuie să creaţi depozitul de certificate *OBJECTSIGNING ca parte a procesului de creare a certificatului dumneavoastră de semnare a obiectelor. Acest depozit de certificate, atunci când este creat, furnizează operaţiile 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 la 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 depozit de certificate nou** pentru a porni operaţia ghidată şi pentru a completa o serie de formulare. Aceste formulare vă îndrumă prin procesul de creare a depozitului de certificate 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 această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Selectaţi ***OBJECTSIGNING** ca depozit de certificate de creat şi faceţi clic pe **Continuare**.
4. Selectaţi **Da** pentru crearea unui certificat ca parte a creaţiei depozitului de certificate *OBJECTSIGNING şi faceţi clic pe **Continuare**.
5. Selectaţi **VeriSign sau altă Autoritare de certificare Internet (CA)** ca semnatar al noului certificat şi faceţi clic pe **Continuare** pentru a afişa un formular care vă permite să furnizaţi 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 operaţie pentru scenariu.

Pasul 3: Creaţi o definiţie de aplicaţie pentru semnarea 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 de aplicaţie nu trebuie să se refere la o aplicaţie reală; definiţia de aplicaţie pe care o creaţi poate 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 **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** ca depozit de certificate pe care să-l deschideţi.
2. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.
3. În cadrul de navigare, selectaţi **Gestiune aplicaţii** pentru a afişa o listă de operaţii.
4. Selectaţi **Adăugare aplicaţie** din lista de operaţii pentru afişarea unui formular pentru definirea aplicaţiei.
5. Completaţi formularul şi faceţi clic pe **Adăugare**.

După ce obţineţi certificatul semnat de la CA, puteţi atribui certificatul aplicaţiei pe care aţi creat-o.

Pasul 4: Importaţi certificatul public semnat şi atribuiţi-l aplicaţiei de semnare obiecte

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 **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** ca depozitul de certificate pe care să-l deschideţi.
3. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.
4. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune certificate** pentru a afişa o listă de operaţii.
5. Din lista de operaţii, selectaţi **Importare certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
6. Selectaţi **Alocare certificat** din lista de operaţii **Gestiune certificate** pentru a afişa o listă de certificate pentru depozitul de certificate curent.
7. Selectaţi un certificat din listă şi faceţi clic pe **Alocare la aplicaţie** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate.
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 această operaţie, 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 verificarea 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 de pre-instalare care apelează API-ul Add Verifier API pentru a configura serverul iSeries al clientului dumneavoastră.

Pasul 5: Exportaţi certificatele pentru a da posibilitatea verificării semnăturii 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 depozitului de certificate *SIGNATUREVERIFICATION. Acest depozit de certificate 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 furnizaţi 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 furnizaţi 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 depozit de certificare nou** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate pe care să-l creaţi.
2. Selectaţi **Da** pentru copierea certificatelor existente de semnare a obiectelor în noul depozit de certificate ca certificate de verificare a semnăturilor.
3. Specificaţi o parolă pentru noul depozit de certificate şi faceţi clic pe **Continuare** pentru a crea depozitul de certificate. 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 operaţia **Exportare certificate**.
2. Selectaţi **Semnare obiect** 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 depozitul de certificate *SIGNATUREVERIFICATION a clienţilor dumneavoastră. API-ul va crea şi depozitul de certificate 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 programul dumneavoastră de împachetare de aplicaţii pentru a utiliza API-urile iSeries pentru a vă semna aplicaţia

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 ne-exclusivă de a utiliza toate exemplele de cod de programare din care puteţi genera funcţii similare adaptate pentru nevoile dumneavoastră specifice. Tot codul exemplu este furnizat de către IBM doar pentru scopuri ilustrative. Aceste exemple nu au fost testate temeinic în toate condiţiile. IBM, de aceea, nu poate garanta sau implica siguranţa, durabilitatea sau funcţionarea acestor programe. Toate programele conţinute aici vă sunt oferite ″CA ATARE″, fără nici un fel de garanţie. Responsabilitatea pentru garanţiile implicite de neîncălcare, vandabilitate şi conformitate pentru un scop particular este declinată în mod expres.

Modificaţi acest cod pentru a-l adapta nevoilor dumneavoastră utilizând API-ul Sign Object, ca parte a unui program de împachetare pentru produsul dumneavoastră aplicaţie. 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.

Notă: Citiţi “Declinarea responsabilităţii pentru cod” la pagina 45 pentru informaţii importante cu caracter juridic.

```
/* ------------------------------------------------------------ */
/*                                                              */
/* COPYRIGHT (C) IBM CORP. 2002, 2004                           */
/*                                                              */
/* Folosiţi API-ul Sign Object pentru a semna biblioteci        */
/*                                                              */
/* API-ul va semna digital toate obiectele dintr-o bibliotecă   */
/*                                                              */
/*                                                              */
/*                                                              */
/* IBM vă acordă o licenţă copyright neexclusivă pentru a utiliza   */
/* toate exemplele de cod de programare din care puteţi genera      */
/* funcţii similare adecvate pentru nevoile dumneavoastră specifice.*/
/* Tot codul exemplu este furnizat de IBM doar pentru scopuri       */
/* ilustrative. Aceste exemple nu au fost testate suficient în      */
/* toate condiţiile.  IBM, de aceea, nu poate garanta sau sugera    */
/* siguranţa, durabilitatea sau funcţionarea acestor programe. Toate*/
/* programele conţinute aici vă sunt furnizate "CA ATARE"           */
/* fără nici o garanţie de orice fel.                    .      */
/* Garanţiile implicate de ne-încălcare, comercilizare şi adaptare  */
/* pentru un anumit scop sunt declinate în mod expres.              */
/*                                                              */
/*                                                              */
/*                                                              */
/* 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[])
{

    /* parametrii:

       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 de pre-instalare care utilizează API-ul Add Verifier

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, puteţi utiliza API-ul Add Verifier ca parte a unui program de ieşire de pre-instalare pentru a vă asigura că certificatul este adăugat în depozitul de certificate înainte de a restaura obiectele aplicaţiei semante. 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 depozitul de certificate *SIGNATUREVERIFICATION. Când adăugaţi un certificat CA în depozitul de certificate, 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 depozitul de certificate. Trebuie să utilizaţi Managerul de certificare digitală pentru adăugarea unui certificat CA în depozitul de certificate pentru a vă asigura că cineva trebuie să controleze, specific şi manual, CA-urile în care sistemul are încredere. Aceasta previne posibilitatea ca sistemul să importe certificate din surse pe care un administrator nu le-a specificat cu ştiinţă ca de încredere.

Dacă doriţi să împiedicaţi ca oricine să utilizeze acest API pentru a adăuga un certificat de verificare în depozitul dumneavoastră de certificate *SIGNATUREVERIFICATION fără ştiinţa dumneavoastră, trebuie să consideraţi dezactivarea acestui API pe 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 ne-exclusivă de a utiliza toate exemplele de cod de programare din care puteţi genera funcţii similare adaptate pentru nevoile dumneavoastră specifice. Tot codul exemplu este furnizat de către IBM doar pentru scopuri ilustrative. Aceste exemple nu au fost testate temeinic în toate condiţiile. IBM, de aceea, nu poate garanta sau implica siguranţa, durabilitatea sau funcţionarea acestor programe. Toate programele conţinute aici vă sunt oferite ″CA ATARE″, fără nici un fel de garanţie. Responsabilitatea pentru garanţiile implicite de neîncălcare, vandabilitate şi conformitate pentru un scop particular este declinată în mod expres.

Modificaţi acest cod pentru a-l adapta nevoilor dumneavoastră pentru foloisrea API-ului Add Verifier ca parte a unui program de ieşire de preinstalare pentru a adăuga certificatul de verificare a semnăturii pe serverul iSeries beneficiarului când instalaţi produsul.

Notă: Citiţi “Declinarea responsabilităţii pentru cod” la pagina 45 pentru informaţii importante cu caracter juridic.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002, 2004                               */
/*                                                                  */
/* Utilizaţi API-ul Adăugare verificare pentru adăugarea unui       */
/* fişier din sistemul de fişiere integrat în depozitul             */
/* de certificate *SIGNATUREVERIFICATION.                           */
/*                                                                  */
/*                                                                  */
/* API-ul va crea depozitul de certificate dacă aceasta nu există.    */
/* Dacă depozitul de certificate este creat, 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.                                        */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* IBM vă acordă o licenţă copyright neexclusivă pentru a utiliza   */
/* toate exemplele de cod de programare din care puteţi genera      */
/* funcţii similare adecvate pentru nevoile dumneavoastră specifice.*/
/* Tot codul exemplu este furnizat de IBM doar pentru scopuri       */
/* ilustrative. Aceste exemple nu au fost testate suficient în      */
/* toate condiţiile.  IBM, de aceea, nu poate garanta sau sugera    */
/* siguranţa, durabilitatea sau funcţionarea acestor programe. Toate*/
/* programele conţinute aici vă sunt furnizate "CA ATARE"           */
/* fără nici o garanţie de orice fel.                          .    */
/* Garanţiile implicate de ne-încălcare, comercilizare şi adaptare  */
/* pentru un anumit scop sunt declinate în mod expres.              */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametrii sunt:                                                 */
/*                                                                  */
/*  char *   numele de cale către fişierul din sistemul de fişiere  */
/*           integrat care conţine 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 operaţii 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 depozitul de certificate *SIGNATUREVERIFICATION cu o parolă implicită pentru clientul dumneavoastră. Trebuie să vă sfătuiţi clientul că trebuie să utilizeze DCM pentru a reseta parola pentru depozitul de certificate cât mai repede posibil pentru a-l proteja de accesul neautorizat.

Pasul 8: Puneţi clienţii să reseteze parola implicită pentru depozitul de certificate *SIGNATUREVERIFICATION

S-ar putea ca API-ul Adăugare verificator să fi creat depozitul de certificate *SIGNATUREVERIFICATION ca parte a procesului de instalare a produsului pe serverul iSeries al clientului dumneavoastră. Dacă API-ul a creat depozitul de certificate, a creat o parolă implicită pentru acesta. Ca urmare, trebuie să vă sfătuiţi clienţii că trebuie să utilizeze DCM pentru a reseta această parolă pentru a proteja depozitul de certificate de accesul neautorizat.

Sfătuiţi clienţii dumneavoastră să efectueze aceşti paşi pentru a reseta parola depozitului de certificate *SIGNATUREVERIFICATION:

1. Porniţi DCM.
2. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate pe care să-l deschideţi.
3. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
4. Specificaţi o nouă parolă pentru depozit, introduceţi-o din nou pentru confirmare, selectaţi poliţa de expirare a parolei pentru depozitul de certificate şi faceţi clic pe **Continuare**.

Scenariu: Utilizarea Administrării centrale din Navigatorul iSeries pentru a semna obiecte

Situaţia

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. Utilizaţi curent funcţia Administrare centrală a Navigatorului iSeries pentru a împacheta şi distribui mai uşor aceste aplicaţii şi pentru a efectua alte operaţii de administrare pentru care sunteţi responsabil. 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 cheltuielile utilizării acestei tehnologii de securitate deoarece nu trebuie să cumpăraţi un certificat de la o CA publică bine cunoscută.

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, utilizaţi deja Administrarea centrală pentru un număr de operaţii de administrare 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 depozit *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:

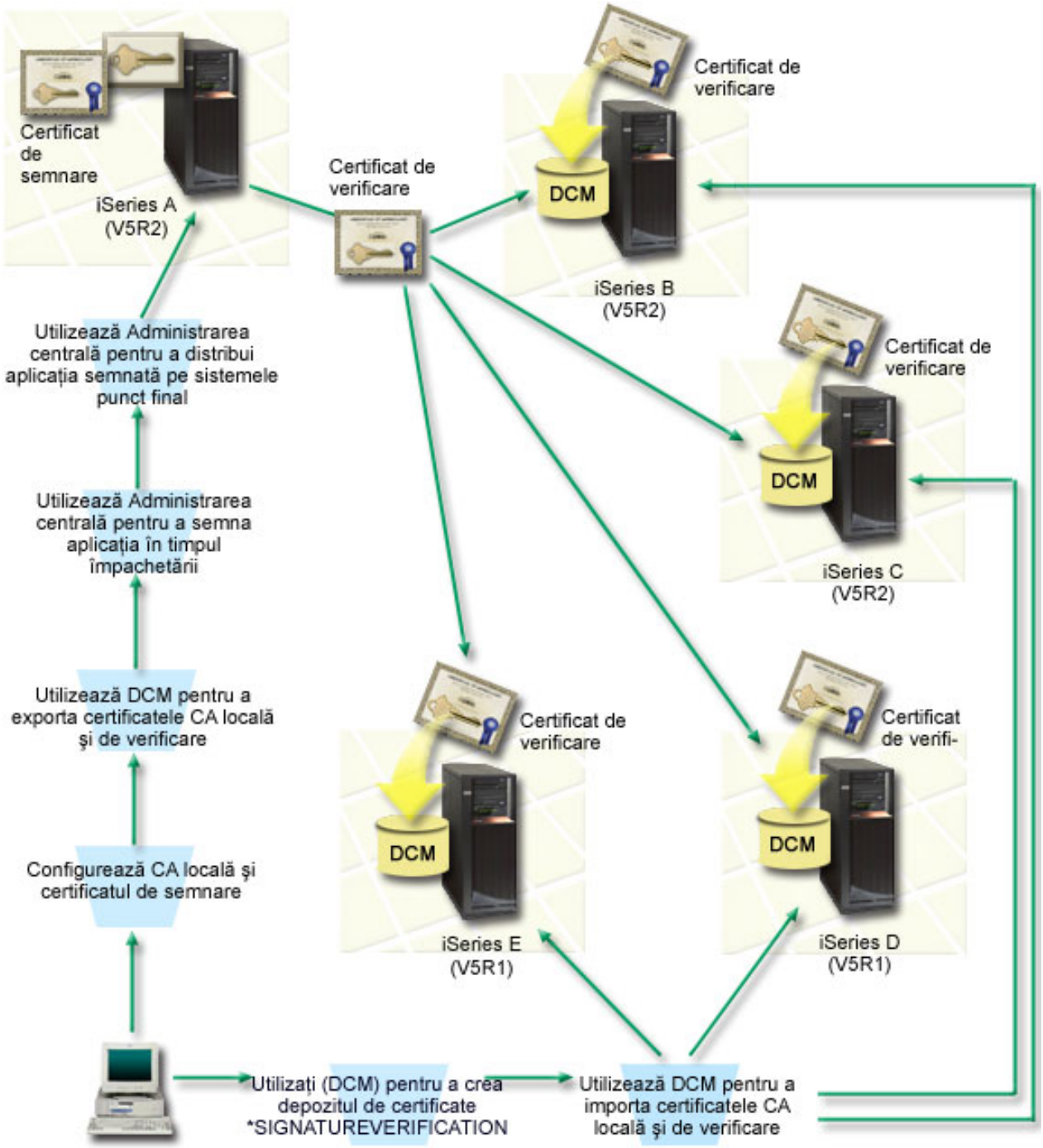


Figura ilustrează următoarele puncte relevante pentru acest scenariu:

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 Furnizor de acces criptografic pe 128 de biţi pentru 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 ca 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 operaţii:
  1. Utilizarea DCM pentru crearea unei CA locale şi utilizarea CA locală pentru crearea unui certificat de semnare a obiectelor.
  2. Utilizarea DCM pentru a exporta o copie a certificatului CA locală şi a certificatului pentru verificarea semnăturii într-un fişier pentru ca sistemele punct final (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 câte o copie a certificatului pentru verificarea semnăturii şi al CA locală ale companiei de la sistemul central (iSeries A) atunci când sistemele primesc aplicaţia semnată.
- DCM este utilizat pentru crearea depozitului de certificate *SIGNATUREVERIFICATION şi pentru importarea CA locală şi a certificatelor de verificare în acest depozit de certificate.

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 îndeplineşte 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 pentru 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 un depozit de certificate în DCM trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilul utilizator.
9. Administratorii de sistem sau alţii de pe celelalte servere iSeries trebuie să aibă autorizarea specială *AUDIT pentru profilul utilizator pentru verificarea semnăturilor obiectelor.

Paşii operaţiei de configurare

Există două seturi de operaţii pe care trebuie să le efectuaţi pentru a implementa acest scenariu: Un set de operaţii vă permite să setaţi iSeries A pentru utilizarea Administrării centrale la semnarea şi distribuirea aplicaţiilor. Celălalt set de operaţii permite administratorilor de sistem şi altor persoane să verifice semnăturile de pe aceste aplicaţii pe toate celelalte servere iSeries.

Paşii de operaţie pentru semnarea obiectelor

Trebuie să efectuaţi fiecare dintre aceste operaţii pe iSeries A pentru semnarea obiectelor aşa cum descrie acest scenariu:
1. Efectuaţi toţi paşii preliminari pentru a instala şi configura toate produsele iSeries necesare
2. Utilizaţi DCM pentru a crea o Autoritate de certificare locală (CA) pentru a emite un certificat pentru semnarea obiectelor privat.
3. Utilizaţi DCM pentru a crea o definiţie de aplicaţie
4. Utilizaţi DCM pentru a atribui un certificat pentru definiţia de aplicaţie pentru semnarea obiectelor
5. Utilizaţi DCM pentru a exporta certificatele pe care trebuie să le utilizeze celelalte sisteme 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 certificat pe fiecare sistem punct final iSeries pe care intenţionaţi să verificaţi semnăturile.
7. Utilizaţi Administrarea centrală a Navigatorului iSeries pentru a semna obiectele aplicaţiei

Paşii operaţiei de configurare

Trebuie să efectuaţi aceste operaţii de configurare verificare semnătură pe fiecare sistem punct final iSeries înainte de a utiliza Administrarea centrală pentru a transfera obiectele 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.

Pe fiecare sistem terminal iSeries, trebuie să efectuaţi aceste operaţii pentru verificarea semnăturilor pe obiecte aşa cum descrie acest scenariu:
8. Utilizaţi (DCM) pentru a crea depozitul de certificate *SIGNATUREVERIFICATION
9. Utilizaţi DCM pentru a importa certificatul CA locale şi certificatul pentru verificarea semnăturii

Detalii scenariu: Utilizarea Administrării centrale din Navigatorul iSeries pentru a semna obiecte

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

Pasul 1: Efectuaţi toţi paşii preliminari

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

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

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 operaţii 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 operaţia pentru configurarea sistemului 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 această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Completaţi toate formularele pentru această operaţie ghidată. Pe măsură ce efectuaţi această operaţie, 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 operaţia fără a crea acest certificat, trebuie să vă creaţi certificatul de semnare a obiectelor şi depozitul de certificate *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 depozitul de certificate *OBJECTSIGNING. Acesta este depozitul de certificate pe care îl utilizaţi pentru gestionarea certificatelor de semnare a obiectelor.
g. Selectaţi aplicaţiile care vor avea încredere în CA locală.

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

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 de aplicaţie pentru semnarea 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 de aplicaţie nu trebuie să se refere la o aplicaţie reală; definiţia de aplicaţie pe care o creaţi poate 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 **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** ca depozitul de certificate pe care să-l deschideţi.
2. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.
3. În cadrul de navigare, selectaţi **Gestiune aplicaţii** pentru a afişa o listă de operaţii.
4. Selectaţi **Adăugare aplicaţie** din lista de operaţii 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 operaţii.
2. Din lista de operaţii, selectaţi **Alocare certificat** pentru afişarea unei liste de certificate pentru depozitul de certificate curent.
3. Selectaţi un certificat din listă şi faceţi clic pe **Alocare la aplicaţie** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate.
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 această operaţie, 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 operaţiile 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 da posibilitatea verificării semnăturii 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 depozitului de certificate *SIGNATUREVERIFICATION. Acest depozit de certificate 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 furnizaţi 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 furnizaţi 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 depozit de certificate nou** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate pe care să-l creaţi.
2. Selectaţi **Da** pentru copierea certificatelor existente de semnare a obiectelor în noul depozit de certificate ca certificate de verificare a semnăturilor.
3. Specificaţi o parolă pentru noul depozit de certificate şi faceţi clic pe **Continuare** pentru a crea depozitul de certificate. 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 operaţia **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. Re-selectaţi operaţia **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 certificat pe sistemele punct final 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 FTP (File Transfer Protocol) sau distribuirea de pachete din Administrare centrală 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 operaţiile 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: Operaţii de verificare a semnăturii: Creaţi depozitul de certificate *SIGNATUREVERIFICATION pe sistemele punct final 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 depozitul de certificate *SIGNATUREVERIFICATION. Dacă un certificat privat a semnat obiectele, acest depozit de certificate trebuie să conţină şi o copie a certificatului CA locală.

Pentru crearea depozitului de certificate *SIGNATUREVERIFICATION, urmaţi aceşti paşi:
1. Porniţi DCM.
2. În cadrul de navigare al Managerului de certificare digitală (DCM) selectaţi **Creare depozit de certificate nou** şi selectaţi ***SIGNATUREVERIFICATION** ca depozit de certificate pe care să-l creaţi.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Specificaţi o parolă pentru noul depozit de certificate şi faceţi clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteţi importa certificatele în depozit şi le puteţi utiliza pentru verificarea semnăturilor.

Pasul 9: Operaţii de verificare a semnăturii: Importaţi certificatele

Pentru a verifica semnătura de pe un obiect, depozitul de certificate *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului de verificare a semnăturilor. Dacă certificatul de semnare este privat, acest depozit de certificate 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 **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** ca depozitul de certificate pe care să-l deschideţi.
2. Când se afişează pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat şi faceţi clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectaţi **Gestiune certificate** pentru a afişa o listă de operaţii.
4. Din lista de operaţii, 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 operaţia **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 parametrii puteţi seta pentru proces.

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

| **Verificarea integrităţii funcţiei de verificare cod**
| Aflaţi cum puteţi verifica integritatea funcţiei de verificare cod pe care o folosiţi la verificarea integrităţii
| sistemului iSeries.

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, 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 decideţi că utilizarea semnăturilor digitale corespunde nevoilor şi politicilor dumneavoastră de securitate, trebuie să evaluaţi dacă să utilizaţi certificate publice versus emiterea de certificate locale. Dacă intenţionaţi să distribuiţi obiecte utilizatorilor din domeniul public general, trebuie să consideraţi utilizarea de certificate de la Autoritate de certificare (CA) publică bine cunoscută. 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 include toţi octeţii obiectului cu excepţia câtorva neesenţiali.
- **Semnături pentru nucleul obiectului**
  Acest tip de semnătură include octeţii esenţiali ai obiectului *CMD. Totuşi, semnătura nu include aceşti octeţi care sunt subiectul modificărilor mai frecvente. Acest tip de semnătură permite efectuarea unor modificări asupra comenzii fără nevalidarea semnăturii. Octeţii pe care nu îi include semnătura obiectului de bază variază în funcţie de obiectul *CMD specific; semnăturile de bază nu includ valorile implicite pentru parametrii obiectelor *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 învăţa mai multe despre ce obiecte iSeries puteţi semna şi ce octeţi ai unui obiect *CMD include o semnătură obiect de bază, vedeţi Obiecte care pot fi semnate.

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 utilizaţi un server Windows 2000 pe un Server xSeries integrat pentru iSeries, aveţi disponibil sistemul de fişere QNTC 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 goale sau obiecte care sunt compilate pentru o ediţie anterioară V5R1.

Semnăturile obiectelor comandă (*CMD)

Atunci când semnaţi obiecte *CMD, puteţi alege unul dintre cele două tipuri de semnături digitale pentru a-l aplica obiectelor *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 obiet completă include elementele conţinute în semnătura obiect de bază.

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 de bază nu includ valorile implicite pentru parametrii obiectelor *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 obiectului	Relaţia cu semnătura obiect de bază
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 fac parte din semnătura nucleului obiectului
Locul permis de rulare	Nu fac parte din semnătura nucleului obiectului
Permitere utilizatori limitaţi	Nu fac 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	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac 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	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Biblioteca produsului	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Programul de evitare a promptului şi biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac 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 fac 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 a erorilor să utilizeze aplicaţia la crearea de semnături pentru mai mult de un obiect. 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 cum să trateze aplicaţia procesul de semnare atunci când aplicaţia re-semnează un obiect. Puteţi specifica dacă se va păstra semnătura originală sau se va înlocui semnătura originală cu semnătura nouă.
- **Obiectele din subdirectoare**
  Puteţi specifica cum să trateze aplicaţia semnarea obiectelor din subdiretoare. 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 a erorilor să utilizeze aplicaţia la verificarea de semnături pentru mai mult de un obiect. 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 cum să trateze aplicaţia verificarea semnăturilor pentru obiectele din subdiretoare. 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 de sistem care determină modul în care sistemul tratează semnăturile de bază şi complete pentru obiecte 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 semnături pentru întregul obiect care sunt de încredere (bazate pe certificatele conţinute în depozitul de certificate *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 semnături a nucleului obiectului care este de încredere, cel puţin una dintre acestea trebuie să se potrivească cu un certificat din depozitul de certificate *SIGNATUREVERIFICATION sau procesul de verificare eşuează. Dacă cel puţin o semnătură a nucleului obiectului este corespunzătoare, procesul de verificare continuă.

Funcţia de verificare a integrităţii pentru verificatorul de cod

Începând cu V5R2, OS/400 este livrat cu o funcţie de verificare a codului pe care o puteţi utiliza pentru a verifica semnătura obiectelor semnate de pe sistemul dumneavoastră, incluzând tot codul sistemului de operare pe care îl livrează şi semnează IBM pentru sistemul dumneavoastră iSeries. Acum în V5R3, puteţi utiliza un API (Application Programming Interface) nou pentru a verifica integritatea chiar a funcţiei de verificare a codului, cât şi a obiectelor cheie ale sistemului de operare.

API-ul Check System (QydoCheckSystem) asigură verificarea integrităţii sistemului OS/400. Utilizaţi acest API pentru a verifica programele (*PGM) şi programele serviciu (*SRVPGM) şi anumite obiecte comandă (*CMD) din biblioteca QSYS. Suplimentar, API-ul Verificare sistem testează comanda Restaurare obiect (RSTOBJ), comanda Restaurare

bibliotecă (RSTLIB), comanda Verificare integritate obiect (CHKOBJITG) şi API-ul Verificare obiect. Acest test asigură că aceste comenzi şi API-ul Verificare obiect raportează corespunzător erorile de validare a semnăturilor; de exemplu, atunci când un obiect furnizat de sistem nu este semnat sau conţine o semnătură nevalidă.

API-ul Verificare sistem raportează mesaje de eroare pentru eşecurile de verificare şi pentru alte erori sau eşecuri de verificare în istoricul de job. Totuşi, puteţi specifica de asemenea una dintre cele două metode suplimentare de raportare a erorilor, în funcţie de cum setaţi opţiunile următoare:

- Dacă valoarea de sistem QAUDLVL este setată pe *AUDFAIL, atunci API-ul Verificare sistem generează înregistrări de auditare pentru a raporta orice eşecuri şi erori pe care le găsesc comenzile Restaurare obiect (RSTOBJ), Restaurare bibliotecă (RSTLIB) şi Verificare interitate obiect (CHKOBJITG).
- Dacă utilizatorul specifică faptul că API-ul Verificare sistem utilizează un fişier de rezultate din sistemul de fişiere integrat, atunci API-ul creează fişierul dacă acesta nu există sau API-ul adaugă la sfârşitul fişierului pentru a raporta orice erori pe care le găseşte API-ul.

Pentru a învăţa mai multe despre cum să utilizaţi API-ul Verificare sistem pentru a verifica integritatea sistemului dumneavoastră, vedeţi Verificarea integrităţii funcţiei de verificare a codului.

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 Managerul de ceritificate digitale (DCM).
- Puteţi scrie un program care utilizează API-ul Semnare obiect.
- Puteţi utiliza funcţiile de Administrare centrală ale Navigatorului iSeries pentru semnarea obiectelor pe măsură ce 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 depozitului de certificate *OBJECTSIGNING. Creaţi acest depozit de certificate 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.
  - depozitul de certificate *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 depozitul de certificate *SIGNATUREVERIFICATION trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ.

Cerinţe preliminare pentru verificarea semnăturii

Există un număr de metode pe care le puteţi utiliza pentru verificarea semnăturilor pe obiecte:
- Puteţi utiliza Managerul de ceritificate digitale (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 şi utilizarea Managerului de certificare digitală (DCM).
- Trebuie să creaţi depozitul de certificate *SIGNATUREVERIFICATION. Puteţi crea acest depozit de certificate 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 acest depozit de certificate prin scrierea unui program care utilizează API-ul Adăugare verificator (QYDOADDV).

  Notă: API-ul Adăugare verificator creează depozitul de certificate 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 depozitul de certificate.
- depozitul de certificate *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului care a semnat obiectele. Puteţi adăuga acest certificat în depozitul de certificate 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 depozitul de certificate *SIGNATUREVERIFICATION. Sau, dacă utilizaţi un certificat public la semnarea obiectelor, puteţi adăuga certificatul la depozitul de certificate a sistemului destinaţie de verificare prin scrierea unui program care utilizează API-ul Adăugare verificator.
- depozitul de certificate *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului CA care a emis certificatul ce a semnat obiectele. Dacă utilizaţi un certificat public pentru a semna obiecte, depozitul de certificate de pe sistemul de verificare destinaţie poate avea 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 depozitul de certificate pe sistemul destinaţie de verificare.

  Notă: Din motive de securitate, API-ul Adăugare verificator nu vă permite să inseraţi un certificat Autoritate de certificare (CA) în depozitul de certificate *SIGNATUREVERIFICATION. Când adăugaţi un certificat CA în depozitul de certificate, 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 depozitul de certificate. Trebuie să utilizaţi Managerul de certificare digitală pentru adăugarea unui certificat CA în depozitul de certificate pentru a vă asigura că cineva trebuie să controleze, specific şi manual, CA-urile în care sistemul are încredere. Aceasta previne posibilitatea ca sistemul să importe certificate din surse pe care un administrator nu le-a specificat cu ştiinţă ca 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 acest depozit de certificate înainte de a utiliza API-ul Adăugare verificator pentru a adăuga certificatul pentru verificarea semnăturii. 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 depozitul de certificate.

  Dacă doriţi să împiedicaţi ca oricine să utilizeze acest API pentru a adăuga un certificat de verificare în depozitul dumneavoastră de certificate *SIGNATUREVERIFICATION fără ştiinţa dumneavoastră, trebuie să consideraţi dezactivarea acestui API pe 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 depozitul de certificate *SIGNATUREVERIFICATION sau modifică parola pentru acesta 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 operaţiile administrative de rutină din sistem.

Obiectele semnate afectează în principal operaţiile de copiere de siguranţă şi de recuperare, mai exact modul în care salvaţi obiecte şi restauraţi obiecte pe sistemul dumneavoastră.

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 operaţiilor de salvare şi restaurare pentru sistemul dumneavoastră.

Comenzi de verificare a codurilor pentru a asigura integritatea semnăturilor
Învăţaţi despre utilizarea comenzilor pentru a verifica semnăturile obiectului pentru a determina integritatea obiectului.

Verificarea integrităţii funcţiei de verificare cod
Aflaţi cum să verificaţi integritatea funcţiei de verificare cod pe care o folosiţi la verificarea integrităţii sistemului OS/400.

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.

Valori de 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 cum 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 obiectelor fişier flux (*STMF) care au asociate programe Java create cu comanda Creare program Java (CRTJVAPGM). Nu se aplică pentru fişierele salvare (*SAV) sau fişierelor din sistemul de fişiere integrat.

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 sistem de fişiere integrat Afişare legături obiect (DSPLNK) şi Gestiune 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 cum să trateze şi să raporteze comanda problemele de semnătură posibile 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 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 restaurată prin comanda Restore Licensed Program - Restaurare program licenţiat (RSTLICPGM). Puteţi utiliza parametrul CHKSIG pentru a specifica cum să trateze şi să raporteze comanda problemele de semnătură posibile 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 pot fi utilizate în sistemul de fişiere integrat. Această comandă vă permite de asemenea să restauraţi memorii de certificare şi conţinutul lor pe sistem. Totuşi, nu puteţi utiliza această comandă pentru restaurarea depozitului de certificate *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 variabilei 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 depozitului de certificate *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 depozitul de certificate *SIGNATUREVERIFICATION şi certificatele pe care le conţine. Această comandă nu salvează nici un alt depozit 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 depozitul de certificate *SIGNATUREVERIFICATION şi certificatele pe care le conţine.
- Comanda Restore - Restaurare (RST).
  Această comandă vă permite să restauraţi memoriile de certificare şi conţinutul lor pe sistem. Totuşi, nu puteţi utiliza această comandă pentru restaurarea depozitului de certificate *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 depozitului de certificate *SIGNATUREVERFICATION şi a parolei pentru aceasta şi pentru restaurarea tuturor celorlaltor memorii de certificare. Puteţi restaura depozitul de certificate *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

Atunci când utilizaţi comenzile următoare pe un obiect semnat, o puteţi face într-o manieră care poate înlătura sau pierde semnătura din 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. Utilizaţi aceste comenzi doar pe acele obiecte semnate pe care le-aţi creat (opus obiectelor semnate pe care le obţineţi de la alţii ca IBM sau 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 spaţiul de stocare pe care îl 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. — Atunci când utilizaţi această comandă, puteţi pierde semnătura din obiectele comandă (*CMD) de pe mediul de salvare dacă specificaţi o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu pot fi semnate în ediţiile anterioare V5R2.
- Comanda Save Library - Salvare bibilotecă (SAVLIB).
  Această comandă vă permite să salvaţi o copie a uneia sau mai multor biblioteci. Atunci când utilizaţi această comandă, puteţi pierde semnătura din obiectele comandă (*CMD) de pe mediul 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. Atunci când utilizaţi această comandă, puteţi pierde semnătura din obiectele comandă (*CMD) de pe mediul de salvare 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. Doar una dintre aceste valori de sistem, valoarea de sistem **verificare semnături obiecte la restaurare (QVFYOBJRST)**, determină cum tratează sistemul obiectele semnate la restaurarea acestora. 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 cunoaşteţi aceste comenzi şi efectul acestora asupra obiectelor semnate pentru a vă gestiona mai bine sistemul şi pentru a evita eventualele probleme care pot să apară.

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 se referă la un obiect comandă (*CMD) cu o ediţie destinaţie anterioară V5R2M0 are ca efect salvarea comenzilor 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. Utilizaţi aceste comenzi doar pe acele obiecte semnate pe care le-aţi creat (opus obiectelor semnate pe care le obţineţi de la alţii ca IBM sau 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 această posibilitate pentru următoarele comenzi de salvare specifice, cât 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 Verificare integritate obiect (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 a integrităţii pentru un obiect, adaugă numele obiectului, numele bibliotecii (sau numele de cale), tipul obiectului, proprietarul oiectului şi tipul eşecului într-un fişier istoric bază 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 obiectele care pot fi semnate dar nu au o semnătură digitală, obiectele pe care nu le poate verifica şi obiectele într-un format care necesită modificări pentru a fi utilizat pe implementarea curentă a sistemului (conversia 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 Verificare opţiune produs (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 Salvare program cu licenţă (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 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 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 pe aceste obiecte. Comanda trimite un mesaj în istoricul de job pentru orice obiect care poate fi semnat care nu are o semnătură; totuşi, procesul de salvare nu se termină. 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.

Verificarea integrităţii funcţiei de verificare cod

Pentru a folosi noua funcţie de verificare a integrităţii verificatorului de cod pe care îl folosiţi la verificarea integrităţii sistemului iSeries, trebuie să aveţi autorizarea specială *AUDIT.

Pentru a verifica funcţia de verificare cod, rulaţi API-ul Verificare sistem (QydoCheckSystem) pentru a determina dacă a fost modificat orice obiect cheie al sistemului de operare de la ultima semnare a acestuia. Atunci când rulaţi API-ul acesta verifică obiectele cheie ale sistemului, inclusiv programele şi programele serviciu şi anumite obiecte comandă (*CMD) din biblioteca QSYS, după cum urmează:

1. Verifică toate obiectele program (*PGM) spre care indică tabela de puncte de intrare sistem.
2. Verifică toate obiectele program serviciu (*SRVPGM) din biblioteca QSYS şi verifică integritatea API-ului Verificare obiect.
3. Rulează API-ul Verificare obiect (QydoVerifyObject) pentru a verifica integritatea comenzii Restaurare obiect (RSTOBJ), comenzii Restaurare bibliotecă (RSTLIB) şi a comenzii Verificare integritate obiect (CHKOBJITG).
4. Utilizează comenzile RSTOBJ şi RSTLIB pe un fişier salvare (*SAV) special pentru a se asigura că erorile sunt raportate corect. Lipsa mesajelor de eroare sau un mesaj de eroare greşit indică o eventuală problemă.
5. Creează un obiect comandă (*CMD) care este proiectat să eşueze la verificarea corectă.
6. Rulează comanda CHKOBJITG şi API-ul Verificare obiect pe acest obiect comandă special pentru a se asigura că comanda CHKOBJITG şi API-ul Verificare obiect raportează corect erorile. Lipsa mesajelor de eroare sau un mesaj de eroare greşit indică o eventuală problemă.

Pentru a învăţa cum să interpretaţi mesajele de eroare pe care le generează funcţia de verificare a integrităţii codului, vedeţi Interpretarea mesajelor de eroare la verificarea verificatorului de cod.

Depanarea obiectelor semnate

Atunci când semnaţi obiecte şi lucraţi cu obiecte semnate, puteţi întâlni erori care vă împieică să vă realizaţi sarcinile şi obiectivele. Multe dintre erorile şi problemele comune pe care le puteţi întâlni fac parte din aceste categorii:

Diagnosticarea erorilor de semnare obiecte
Utilizaţi aceste informaţii pentru a învăţa despre problemele uzuale pe care le puteţi întâlni la verificarea semnăturilor digitale pentru obiecte şi despre cum puteţi să le corectaţi.

Depanarea erorilor de verificare a semnăturilor
Utilizaţi aceste informaţii pentru a învăţa despre problemele uzuale cu depozitele de certificate şi bazele de date de chei pe care le puteţi întâlni şi despre cum puteţi să le corectaţi.

Interpreţaţi mesajele de eroare pentru verificarea verificatorului de cod
Utilizaţi aceste informaţii pentru a învăţa pentru a învăţa ce mesaje sunt returnate de funcţia de verificare a indegrităţii verificatorului de cod şi cum să utilizaţi aceste mesaje pentru a vă asigura că funcţia de verificare a codului nu este coruptă, cât şi soluţii posibile dacă mesajele indică faptul că funcţia sau obiecte cheie ale sistemului de operare pot fi corupte.

Diagnosticarea erorilor de semnare obiecte

Utilizaţi tabelul următor pentru a găsi informaţii care să vă ajute să diagnosticaţi unele dintre cele mai întâlnite probleme pe care le puteţi întâlni 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 asigură suport pentru semnarea obiectelor înainte de 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.

Depanarea erorilor de verificare a semnăturilor

Utilizaţi tabelul următor pentru a găsi informaţii care să vă ajute să diagnosticaţi unele dintre cele mai întâlnite probleme pe care le puteţi întâlni la verificarea semnăturilor digitale pentru obiecte:

Problemă	Soluţie posibilă
Procesul de restaurare eşuează pentru obiectele fără semnătură.	Dacă lipsa unei semnături nu este o problemă, verificaţi dacă valoarea de sistem QVFYOBJRST este setată pe 5. O valoare 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 depozitul de certificate *SIGNATUREVERIFICATION a fost transferat pe sistem şi DCM nu a fost utilizat pentru modificarea parolei pentru acesta. 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 depozitul de certificate. Dacă nu cunoaşteţi parola, va trebui să ştergeţi depozitul de certificate; creaţi-l din nou şi utilizaţi DCM pentru a schimba parola.
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 o problemă, nu modificaţi valoarea de sistem QVFYOBJRST şi nu efectuaţi alte acţiuni care pot permite restaurarea obiectului suspect. Astfel puteţi ocoli securitatea pe care o furnizează verificarea semnăturii şi să permiteţi un obiect dăunător pe sistemul dumneavoastră. În loc de a verifica valoarea de sistem, trebuie să contactaţi semnatarul obiectului pentru a determina acţiunea corespunzătoare pe care să o întreprindeţi pentru a rezolva problema.

Interpretarea mesajelor de eroare la verificarea verificatorului de cod

Tabelul următor furnizează o listă a mesajelor pe care funcţia de verificare a verificatorului de cod le generează în timpul procesării. Acest tabel nu este o listă cuprinzătoare a tuturor mesajelor pe care le puteţi recepţiona. În loc, tabelul listează acele mesaje care de obicei indică faptul că verificarea verificatorului de cod s-a terminat cu succes complet sau că a întâlnit o problemă serioasă. Vedeţi documentaţia pentru API-ul Verificare sistem (QydoCheckSystem) pentru o listă detaliată a mesajelor de eroare.

De asemenea, un număr de mesaje generate de funcţia de verificare a verificatorului de cod pe parcursul procesării sunt mesaje informaţionale şi nu sunt listate aici. Pentru a învăţa mai multe despre cum lucrează procesul de verificare a verificatorului de cod, vedeţi Verificarea integrităţii funcţiei de verificare a codului.

Tabela 1. Mesaje de eroare la verificarea verificatorului de cod

Mesaj de eroare	Problema posibilă şi soluţia
CPFB729	Indică faptul că procesul de verificare a verificatorului de cod a eşuat să se termine aşa cum se aştepta. Acest eşec poate fi cauzat de o gamă largă de probleme. Revedeţi istoricul de job pentru mesaje de eroare mai detaliate pentru a determina natura exactă a eşecului şi cauza posibilă. Dacă determinaţi că obiecte cheie ale sistemului de operare au eşuat la verificarea integrităţii, acest eşec poate indica faptul că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteţi fi nevoit să reinstalaţi sistemul de operare penru a asigura integritatea sistemului.

Tabela 1. Mesaje de eroare la verificarea verificatorului de cod (continuare)

Mesaj de eroare	Problema posibilă şi soluţia
La extragerea istoricului de job, vedeţi mesaje ca CPFB723, CPD37A1 sau CPD37A0 pentru aceste obiecte specifice: • Obiecte program (*PGM): – QYDONOSIG în biblioteca QTEMP – QYDOBADSIG în biblioteca QTEMP • Obiecte comandă (*CMD): – QYDOBADSIG în biblioteca QTEMP – SIGNOFF în biblioteca QTEMP	Indică faptul că setul specificat de obiecte pe care le utilizează funcţia de verificare a verificatorului de cod pentru testarea integrităţii a eşuat aşa cum era de aşteptat. Acest eşec indică faptul că comanda RSTOBJ, comanda RSTLIB, comanda CHKOBJITG şi API-ul Verificare obiect raportează corect erorile. Nu este necesară nici o acţiune suplimentară.
CPFB723 pentru orice alt obiect diferit de cele listate anterior în acest tabel.	Indică faptul că semnătura pe un obiect cheie al sistemului de operare a eşuat la verificare. Acest eşec poate indica că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteţi fi nevoit să reinstalaţi sistemul de operare penru a asigura integritatea sistemului.
CPFB722 pentru orice alt obiect diferit de cele listate anterior în acest tabel.	Indică faptul că un obiect cheie al sistemului de operare nu are nici o semnătură atunci când este aşteptată o semnătură. Această lipsă a semnăturii poate indica faptul că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteţi fi nevoit să reinstalaţi sistemul de operare penru a asigura integritatea sistemului.
CPF72A pentru orice alt obiect diferit de cele listate anterior în acest tabel.	Indică faptul că un obiect cheie al sistemului de operare a eşuat la verificarea integrităţii. Acest eşec poate indica că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteţi fi nevoit să reinstalaţi sistemul de operare penru a asigura integritatea sistemului.

Dacă trebuie să reinstalaţi cod care verifică integritatea funcţiei verificatorului de cod, trebuie să îl obţineţi de la o sursă cunoscută, bună. De exemplu, puteţi instala mediul de instalare pe care l-aţi utilizat pentru a instala ediţia curentă. Pentru a restaura funcţia de verificare a verificatorului de cod, urmaţi aceşti paşi de la un prompt de comenzi OS/400:

1. Rulaţi comanda QSYS/DLTPGM QSYS/QYDOCHKS. Această comndă şterge API-ul Verificare sistem (OPM, QYDOCHKS; ILE, QydoCheckSystem).
2. Rulaţi comanda QSYS/DLTSRVPGM QSYS/QYDOCHK1. Această comandă şterge programul serviciu al verificatorului de cod cu API-ul Verificare sistem (OPM, QYDOCHKS; ILE, QydoCheckSystem).
3. Rulaţi comanda QSYS/DLTF QSYS/QYDOCHKF. Această comandă şterge fişierul salvare care conţine obiectele pe care le utilizează funcţia de verificare cod pentru a testa semnăturile greşite şi lipsa semnăturilor
4. Rulaţi comanda QSYS/RSTOBJ OBJ(QYDOCHK*) SAVLIB(QSYS) DEV(OPT01) OBJTYPE(*ALL) OPTFILE('Q5722SS1/Q5200M_/Q00/Q90'). Această comandă restaurează toate obiectele necesare pentru funcţia de verificare a verificatorului de cod de pe mediul de instalare încărcat.

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:

- **Situl Web VeriSign Help Desk**
  Situl 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 include multe subiecte inclusiv cum să utilizaţi posibilităţile de semnare a obiectelor ale iSeries, Managerul de certificate digitale (DCM) şi aşa mai departe.

Declinarea responsabilităţii pentru cod

Acest document conţine exemple de programare.

IBM vă acordă o licenţă copyright ne-exclusivă de a utiliza toate exemplele de cod de programare din care puteţi genera funcţii similare adaptate pentru nevoile dumneavoastră specifice.

Tot codul exemplu este furnizat de către IBM doar pentru scopuri ilustrative. Aceste exemple nu au fost testate temeinic în toate condiţiile. IBM, de aceea, nu poate garanta sau implica siguranţa, durabilitatea sau funcţionarea acestor programe.

Toate programele conţinute aici vă sunt oferite ″CA ATARE″, fără nici un fel de garanţie. Responsabilitatea pentru garanţiile implicite de neîncălcare, vandabilitate şi conformitate pentru un scop particular este declinată în mod expres.

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Totuşi, este responsabilitatea utilizatorului de a evalua şi verifica funcţionarea oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Furnizarea acestui document nu vă acordă nici o licenţă pentru aceste brevete. Puteţi cere informaţii despre licenţă, în scris, la:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Pentru întrebări despre licenţă cu privire la informaţii pe doi octeţi (DBCS), contactaţi Departamentul de proprietate intelectuală IBM din ţara dumneavoastră sau trimiteţi întrebări, în scris, la:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE "CA ATARE", FĂRĂ NICI UN FEL DE GARANŢIE, EXPRIMATĂ SAU PRESUPUSĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot conţine greşeli tehnice sau erori de tipar. Periodic sunt efectuate modificări ale acestor informaţii; aceste modificări vor fi încorporate în ediţiile noi ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului(elor) şi/sau programului(elor) descrise în această publicaţie în orice moment fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe acele situri Web nu fac parte din materialele pentru acest produs IBM şi utilizarea acestor situri Web este pe riscul dumneavoastră.

| IBM poate utiliza sau distribui orice informaţii pe care le furnizaţi în orice mod crede de cuviinţă, fără nici o obligaţie
| pentru dumneavoastră.

Posesorii de licenţă ai acestui program care doresc să aibă informaţii despre acesta cu scopul posibilităţii de: (i) schimb de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (ii) utilizarea mutuală a informaţiilor care au fost schimbate, trebuie să contacteze:

| IBM Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile, conform termenilor şi condiţiilor, incluzând în unele cazuri, plata unei taxe.

Programul licenţiat la care se referă aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM conform termenilor din Contractul IBM cu Clientul, Contractul IBM pentru licenţă internaţională de program, Contractul IBM de licenţă pentru Codul maşină sau din alt acord echivalent încheiat între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult de atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse şi nu poate confirma acurateţea performanţelor, compatibilitatea sau oricare alte pretenţii legate de produsele non-IBM. Întrebările legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM-ului pot fi schimbate sau se poate renunţa la ele, fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

LICENŢĂ - COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără să plătiţi ceva IBM-ului, în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform cu interfaţa de programare aplicaţii pentru platforma de operare pentru acre au fost scrise exemplele de program. Aceste exemple nu au fost testate temeinic pentru toate condiţiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

EXCEPTÂND GARANŢIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE PROGRAME ŞI FURNIZORII SĂI NU ACORDĂ NICI O GARANŢIE SAU CONDIŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SAU CONDIŢIILE IMPLICITE DE VANDABILITATE, DE POTRIVIRE PENTRU UN ANUMIT SCOP SAU DE NEÎNCĂLCARE A UNUI DREPT, REFERITOARE LA PROGRAM SAU LA SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

ÎN NICI O ÎMPREJURARE IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII NU VOR FI RESPONSABILI PENTRU ORICARE DINTRE URMĂTOARELE PAGUBE, CHIAR DACĂ AU FOST INFORMAŢI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

1. PIERDEREA SAU DETERIORAREA DATELOR;
2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICII ECONOMICE DE CONSECINŢĂ; SAU
3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAŢIE SAU ECONOMII PLANIFICATE.

UNELE JURISDICŢII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALE SAU INDIRECTE, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU FIE VALABILE PENTRU DUMNEAVOASTRĂ.

Fiecare copie sau porţiune din aceste programe eşantion sau lucrările derivate din ele trebuie să conţină un anunţ de copyright, după cum urmează:

© (numele companiei dumneavoastră) (anul). Porţiuni din acest cod sunt derivate din IBM Corp. Sample Programs. © Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vizualizaţi aceste informaţii în formă electronică, este posibil ca fotografiile şi ilustraţiile color să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

e(logo)server
eServer
IBM
iSeries
Operating System/400
OS/400
Redbooks
xSeries
400

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale deţinute de Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termeni şi condiţii pentru descărcarea şi tipărirea publicaţiilor

Permisiunile pentru utilizarea informaţiilor selectate pentru descărcare sunt acordate cu următoarele condiţii şi termeni şi indicarea de către dumneavoastră a acceptării acestora.

Utilizare personală: Puteţi reproduce aceste informaţii pentru uzul dumneavoastră personal, necomercial cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau efectua lucrări derivate din aceste informaţii sau porţiuni ale acestora fără consimţământul expres al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste informaţii doar în cadrul întrepruinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi efectua lucrări derivate din acestor informaţii sau reproduce, distribui sau afişa aceste informaţii sau porţiuni ale acestora fără consimţământul expres al IBM.

Cu excepţia permisiunilor acordate explicit aici, nu se acordă nici o altă permisiune, licenţă sau drept, explicit sau implicit, pentru informaţiile, datele, software-ul sau altă proprietate intelectuală conţinută aici.

IBM îşi rezervă dreptul de a retrage aceste permisiuni acordate aici oricând consideră, după cum crede de cuviinţă, că utilizarea informaţiilor nu este în interesul său sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau re-exporta aceste informaţi decât cu respectarea tuturor legilor şi reglementărilor în vigoare, inclusiv a tuturor legilor şi reglementărilor de export ale Statelor Unite. IBM NU OFERĂ NICI O GARANŢIE CU PRIVIRE LA CONŢINUTUL ACESTOR INFORMAŢII. INFORMAŢIILE SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA

LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Drepturile de autor pentru toate materialele aparţin IBM Corporation.

Descărcând şi tipărind informaţii de pe acest sit, v-aţi indicat acordul cu aceşti termeni şi condiţii.

Informaţii de declinarea responsabilităţii pentru cod

IBM vă acordă o licenţă de copyright neexclusivă pentru utilizarea tuturor exemplelor de coduri de programare din care puteţi genera funcţii similare, adaptate necesităţilor dumneavoastră specifice.

EXCEPTÂND GARANŢIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE PROGRAME ŞI FURNIZORII SĂI NU ACORDĂ NICI O GARANŢIE SAU CONDIŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SAU CONDIŢIILE IMPLICITE DE VANDABILITATE, DE POTRIVIRE PENTRU UN ANUMIT SCOP SAU DE NEÎNCĂLCARE A UNUI DREPT, REFERITOARE LA PROGRAM SAU LA SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

ÎN NICI O ÎMPREJURARE IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII NU VOR FI RESPONSABILI PENTRU ORICARE DINTRE URMĂTOARELE PAGUBE, CHIAR DACĂ AU FOST INFORMAŢI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

1. PIERDEREA SAU DETERIORAREA DATELOR;
2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICII ECONOMICE DE CONSECINŢĂ; SAU
3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAŢIE SAU ECONOMII PLANIFICATE.

UNELE JURISDICŢII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALE SAU INDIRECTE, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU FIE VALABILE PENTRU DUMNEAVOASTRĂ.

Tipărit în S.U.A.