



IBM Systems - iSeries

Semnarea obiectelor și verificarea semnăturii

Versiunea 5 Ediția 4





IBM Systems - iSeries

Semnarea obiectelor și verificarea semnăturii

Versiunea 5 Ediția 4

Notă

Înainte de a folosi aceste informații și produsul pe care îl suportă, citiți informațiile din “Notificări”, la pagina 47.

Ediția a patra (februarie 2006)

Această ediție se aplică versiunii 5, ediția 4, modificarea 0 a IBM i5/OS (număr produs 5722-SS1) și tuturor edițiilor și modificărilor ulterioare, până când se indică altceva în edițiile noi. Această versiune nu rulează pe toate modelele de calculator cu set redus de instrucțiuni (RISC) și cu atât mai mult pe modelele CISC.

© Copyright International Business Machines Corporation 2002, 2006. Toate drepturile rezervate.

Cuprins

Semnarea obiectelor și verificarea semnăturii. 1

PDF tipăribil	1
Concepte de semnare a obiectelor	2
Semnături digitale	2
Obiecte care se pot semna	3
Procesarea semnării obiectelor	4
Procesarea de verificare a semnăturilor	5
Funcția de verificare a integrității pentru verificatorul de cod	5
Scenarii de semnare a obiectelor	6
Scenariu: Utilizați DCM pentru a semna obiecte și pentru a verifica semnăturile	6
Scenariu: Utilizați API-uri pentru a semna obiecte și pentru a verifica semnăturile obiectelor	15
Scenariu: Utilizarea Administrării centrale din Navigatorul iSeries pentru a semna obiecte	26
Cerințe preliminare pentru semnarea obiectelor și verificarea semnăturilor	34

Gestiunea obiectelor semnate	36
Variabile de sistem și comenzi care afectează obiectele semnate	36
Considerații de salvare și restaurare pentru obiectele semnate	40
Comenzi de verificare a codurilor pentru asigurare integrității semnăturilor	41
Verificarea integrității funcției de verificare cod	42
Depanarea obiectelor semnate	43
Diagnosticarea erorilor de semnare obiecte	43
Depanarea erorilor de verificare a semnăturilor	43
Interpretarea mesajelor de eroare la verificarea verificatorului de cod	44
Informații înrudite pentru semnarea obiectelor și verificarea semnăturilor	45

Anexa. Notificări 47

Mărci comerciale	49
Termenii și condițiile	49

Semnarea obiectelor și verificarea semnăturii

Găsiți informații despre semnarea obiectelor i5/OS și verificarea semnăturilor, capacități de securitate pe care le puteți utiliza pentru a asigura integritatea obiectelor. Aflați cum să folosiți una din diversele metode i5/OS pentru crearea de semnături digitale pentru identificarea sursei obiectului și furnizarea unui mijloc pentru detectarea modificărilor aduse obiectului. Aflați cum să îmbunătățiți securitatea sistemului prin verificarea semnăturilor digitale pe obiecte, inclusiv obiectele sistemului de operare, pentru a determina dacă s-au adus modificări conținutului obiectului din momentul în care a fost semnat.

Semnarea obiectelor și verificarea semnăturilor sunt capacități de securitate pe care le puteți utiliza pentru a verifica integritatea unei varietăți de obiecte. Utilizați o cheie privată a certificatului digital pentru a semna un obiect și utilizați certificatul (care conține cheia privată corespunzătoare) pentru a verifica semnătura digitală. O semnătură digitală asigură integritatea de timp și conținut a obiectului pe care îl semnați. Semnătura furnizează dovada autenticității și autorizării. Aceasta poate fi utilizată pentru a arăta dovada originii și a detecta modificările. Prin semnarea obiectului, dumneavoastră identificați sursa obiectului și furnizați un mijloc pentru detectarea modificărilor aduse obiectului. Atunci când verificați semnătura unui obiect puteți determina dacă s-au adus modificări conținutului obiectului din momentul în care a fost semnat. Puteți de asemenea verifica sursa semnăturii pentru a determina originea obiectului.

Puteți implementa semnarea obiectelor și verificarea semnăturilor prin:

- API-uri care să semneze obiecte și să verifice semnăturile de pe obiecte în mod programat.
- DCM (Digital Certificate Manager) care să semneze obiectele și să vizualizeze sau să verifice semnăturile obiectelor.
- Administrarea centrală a Navigatorului iSeries care să semneze obiecte ca parte a distribuiri pachetelor pentru a fi utilizate de alte sisteme.
- Comenzi CL, cum ar fi CHKOBJITG (Check Object Integrity - Verificare integritate obiecte) care să verifice semnăturile.

Pentru a afla mai multe despre aceste metode de semnare a obiectelor și despre modul în care semnarea obiectelor poate îmbunătăți politica dumneavoastră actuală de securitate, reconsultați aceste subiecte:

Notă: Folosind exemplele de cod, sunteți de acord cu termenii din “Informații de licență și de declinare a responsabilității pentru cod” la pagina 46.

PDF tipăribil

Utilizați aceste informații pentru a tipări întregul subiect ca un fișier PDF.


Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectați Semnarea obiectelor și verificarea semnăturii (dimensiune fișier 605 KB).

Salvarea fișierelor PDF:

Pentru a salva un PDF pe stația dumneavoastră de lucru pentru vizualizare sau tipărire:

1. Faceți clic pe PDF în browser-ul dumneavoastră (faceți clic dreapta pe legătura de mai sus).
2. Faceți clic pe **Save Target As...** dacă utilizați Internet Explorer. Faceți clic pe **Save Link As...** dacă utilizați Netscape Communicator.
3. Navigați în directorul în care doriți să salvați PDF-ul.
4. Faceți clic pe **Save (Salvare)**.

Descărcarea Adobe Acrobat Reader

Aveți nevoie de Adobe Acrobat Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteți descărca o copie de pe situl Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Concepte de semnare a obiectelor

Utilizați aceste concepte și informațiile referință pentru a afla mai multe despre semnăturile digitale și despre funcționarea proceselor de semnare a obiectelor și de verificare a semnăturilor.

Înainte de a începe utilizarea capacităților de semnare a obiectelor și de verificare a semnăturilor, puteți considera utilă revizuirea câtorva dintre aceste concepte:

Semnături digitale

Aflați despre semnăturile digitale și despre tipul de protecție pe care o oferă.

i5/OS 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 și este asemănătoare unei semnături personale pe un document scris. O semnătură digitală face dovada originii obiectului și oferă un mijloc de verificare a integrității obiectului. Proprietarul unui certificat digital "semnează" un obiect utilizând cheia privată a certificatului. Persoana care primește obiectul utilizează cheia publică corespunzătoare a certificatului pentru decriptarea semnăturii, care verifică integritatea obiectului semnat și verifică expeditorul ca sursă.

Suportul pentru semnarea obiectelor extinde uneltele tradiționale ale serverului iSeries pentru controlarea persoanelor care pot modifica obiecte. Controalele tradiționale nu pot proteja un obiect de modificarea neautorizată în timp ce obiectul se află în tranzit prin Internet sau alte rețele care nu sunt de încredere. Deoarece puteți detecta dacă conținutul unui obiect a fost modificat din momentul în care acesta a fost semnat, puteți determina dacă să aveți sau nu încredere în obiectele pe care le obțineți în astfel de situații.

O semnătură digitală este un rezumat matematic cifrat al datelor din obiect. Obiectul și conținutul său nu sunt cifrate și făcute private prin semnătura digitală; totuși, rezumatul în sine este cifrat pentru a preveni modificările neautorizate asupra acestuia. Oricine dorește să se asigure că obiectul nu a fost modificat în tranzit și 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 obținerea altei copii a obiectului semnat.

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

Dacă decideți că utilizarea semnăturilor digitale corespunde nevoilor și politicilor dumneavoastră de securitate, trebuie să evaluați dacă să utilizați certificate publice versus emiterea de certificate locale. Dacă intenționați să distribuiți obiecte utilizatorilor din domeniul public general, trebuie să considerați utilizarea de certificate de la Autoritate de certificare (CA) publică bine cunoscută. Utilizarea certificatelor publice asigură că alte persoane pot verifica cu ușurință și fără costuri semnăturile pe care le puneți pe obiectele distribuite către acestea. Dacă, totuși, intenționați să distribuiți obiecte numai în cadrul organizației dumneavoastră, puteți prefera să utilizați Digital Certificate Manager (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 puțin costisitoare decât cumpărarea certificatelor de la o CA publică binecunoscută.

Tipuri de semnături digitale

Începând cu V5R2, puteți semna obiecte comandă (*CMD); puteți 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 toți octeții obiectului, cu excepția câtorva neesențiali.

- **Semnături obiect nucleu** Acest tip de semnătură include octeții esențiali ai obiectului *CMD. Totuși, semnătura nu include acești octeți care sunt subiectul modificărilor mai frecvente. Acest tip de semnătură permite efectuarea unor modificări asupra comenzii fără invalidarea semnăturii. Octeții pe care nu îi include semnătura obiectului de bază variază în funcție de obiectul *CMD specific; semnăturile de bază nu includ valorile implicite pentru parametrii obiectelor *CMD, de exemplu. Exemplele de modificări care nu vor invalida o semnătură a nucleului unui obiect includ:
 - Modificarea valorilor implicite ale comenzii.
 - Adăugarea unui program de verificare a validității 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 limitați).

Concepte înrudite

“Obiecte care se pot semna”

Aflați despre tipurile de obiecte pe care le puteți semna și despre opțiunile de semnare a obiectelor comandă (*CMD).

Informații înrudite

DCM (Digital Certificate Manager)

Obiecte care se pot semna

Aflați despre tipurile de obiecte pe care le puteți semna și despre opțiunile de semnare a obiectelor comandă (*CMD).

Puteți semna digital o varietate de tipuri de obiecte i5/OS, indiferent de metoda utilizată pentru semnarea lor. Puteți semna orice obiect (*STMF) pe care îl memorați în sistemul de fișiere integrat al sistemului, cu excepția obiectelor care sunt memorate într-o bibliotecă. Dacă obiectul are un program Java atașat, programul va fi de asemenea semnat. Puteți semna doar aceste obiecte din sistemul de fișiere QSYS.LIB: programe (*PGM), programe de serviciu (*SRVPGM), module (*MODULE), pachete SQL (*SQLPKG), *FILE (numai fișier de salvare) și comenzi (*CMD).

Pentru a semna un obiect, acesta trebuie să se afle pe sistemul local. De exemplu, dacă utilizați un server Windows 2000 pe un Server xSeries integrat pentru iSeries, aveți disponibil sistemul de fișiere QNTC în sistemul de fișiere integrat. Directoarele din acest sistem de fișiere nu sunt considerate locale deoarece conțin fișiere care sunt deținute de sistemul de operare Windows 2000. De asemenea, nu puteți semna obiecte goale sau obiecte care sunt compilate pentru o ediție anterioară V5R1.

Semnăturile obiectelor comandă (*CMD)

Atunci când semnați obiecte *CMD, puteți alege unul dintre cele două tipuri de semnături digitale pentru a-l aplica obiectelor *CMD. Puteți alege să semnați întregul obiect, sau să semnați doar partea de nucleu a obiectului. Atunci când alegeți să semnați întregul obiect, semnătura este aplicată pe toți octeții obiectului, cu excepția câtorva octeți neesențiali. Semnătura obiect completă include elementele conținute în semnătura obiect de bază.

Când alegeți să semnați doar nucleul obiectului, octeții esențiali sunt protejați de semnătură, în timp ce octeții care sunt supuși unor modificări frecvente nu sunt semnați. Octeții care nu sunt semnați variază în funcție de obiectul *CMD, dar pot include, printre altele, octeți 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 invalidarea semnăturii acesteia. Exemplele de modificări care nu vor invalida aceste tipuri de semnături includ:

- Modificarea valorilor implicite ale comenzii.
- Adăugarea unui program de verificare a validității 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 limitați).

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

Compoziția semnăturii nucleului pe obiecte *CMD

Partea obiectului	Relația cu semnătura obiect de bază
Valorile implicite ale comenzii modificate de CHGCMDDFT	Nu fac parte din semnătura nucleului obiectului
Programul de procesare a comenzii și biblioteca	Incluse întotdeauna în semnătura nucleului obiectului
Fișierul sursă REXX și 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 și biblioteca	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Numele programului de ieșire REXX, biblioteca și codul de ieșire	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Programul de verificare a validității și 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 limitați	Nu fac parte din semnătura nucleului obiectului
Cărțile de ajutor	Incluse dacă sunt specificate pentru comandă la momentul semnării, altfel nu fac parte din semnătura nucleului obiectului
Grupul de panouri de ajutor și 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 și 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 și 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 interfeței grafice utilizator (GUI)	Nu fac parte din semnătura nucleului obiectului

Concepte înrudite

“Semnături digitale” la pagina 2

Aflați despre semnăturile digitale și despre tipul de protecție pe care o oferă.

Informații înrudite

DCM (Digital Certificate Manager)

Procesarea semnării obiectelor

Aflați despre modul în care funcționează procesul de semnare a obiectelor și ce parametrii puteți seta pentru proces.

Atunci când semnați obiecte puteți specifica următoarele opțiuni pentru procesarea de semnare a obiectelor.

Procesarea la eroare

Puteți specifica ce tip de procesare a erorilor să utilizeze aplicația la crearea de semnături pentru mai mult de un obiect. Puteți preciza ca aplicația să se oprească din semnarea obiectelor când apare o eroare sau să continue semnarea celorlalte obiecte din proces.

Semnătura duplicat a obiectelor

Puteți specifica cum să trateze aplicația procesul de semnare atunci când aplicația re-semnează un obiect. Puteți specifica dacă se va păstra semnătura originală sau se va înlocui semnătura originală cu semnătura nouă.

Obiectele din subdirectoare

Puteți specifica cum să trateze aplicația semnarea obiectelor din subdirectoare. Puteți preciza ca aplicația să semneze individual obiectele din orice subdirectoare sau ca aplicația să semneze numai obiectele din cadrul directorului principal, ignorând toate subdirectoarele.

Domeniul semnăturii obiectului

Când semnați obiecte *CMD, puteți specifica dacă se va semna întregul obiect sau numai partea de nucleu a obiectului.

Procesarea de verificare a semnăturilor

Aflați despre modul de funcționare a procesului de verificare a semnăturilor obiectelor și ce parametrii puteți seta pentru proces.

Puteți specifica următoarele opțiuni pentru procesarea de verificare a semnăturilor.

Procesarea la eroare

Puteți specifica ce tip de procesare a erorilor să utilizeze aplicația la verificarea de semnături pentru mai mult de un obiect. Puteți preciza ca aplicația să se oprească din verificarea semnăturilor când apare o eroare sau să continue verificarea semnăturilor pe celelalte obiecte din proces.

Obiectele din subdirectoare

Puteți specifica cum să trateze aplicația verificarea semnăturilor pentru obiectele din subdirectoare. Puteți preciza ca aplicația să verifice individual semnăturile obiectelor din subdirectoare sau ca aplicația 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 și 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 și 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 eșuează. 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 conținute în depozitul de certificate *SIGNATUREVERIFICATION), cel puțin una dintre aceste semnături trebuie să fie corespunzătoare sau procesul de verificare eșuează. Dacă cel puțin o semnătură a întregului obiect este corespunzătoare, procesul de verificare continuă.
- Dacă obiectul are orice semnături a nucleului obiectului care este de încredere, cel puțin una dintre acestea trebuie să se potrivească cu un certificat din depozitul de certificate *SIGNATUREVERIFICATION sau procesul de verificare eșuează. Dacă cel puțin o semnătură a nucleului obiectului este corespunzătoare, procesul de verificare continuă.

Funcția de verificare a integrității pentru verificatorul de cod

Aflați cum puteți verifica integritatea funcției de verificare cod pe care o folosiți la verificarea integrității sistemului.

Începând cu V5R2, i5/OS este livrat cu o funcție de verificare a codului pe care o puteți utiliza pentru a verifica semnătura obiectelor semnate de pe sistemul dumneavoastră, incluzând tot codul sistemului de operare pe care îl livrează și semnează IBM pentru sistemul dumneavoastră. Acum în V5R3, puteți utiliza un API (Application Programming Interface) nou pentru a verifica integritatea chiar a funcției de verificare a codului, cât și a obiectelor cheie ale sistemului de operare.

API-ul Check System (QydoCheckSystem) asigură verificarea integrității sistemului i5/OS. Utilizați acest API pentru a verifica programele (*PGM) și programele serviciu (*SRVPGM) și 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) și API-ul Verificare obiect. Acest test asigură că aceste comenzi și API-ul Verificare obiect raportează corespunzător erorile de validare a semnăturilor; de exemplu, atunci când un obiect furnizat de sistem nu este semnat sau conține o semnătură nevalidă.

API-ul Verificare sistem raportează mesaje de eroare pentru eșecurile de verificare și pentru alte erori sau eșecuri de verificare în istoricul de job. Totuși, puteți specifica de asemenea una dintre cele două metode suplimentare de raportare a erorilor, în funcție de cum setați opțiunile următoare:

- Dacă valoarea de sistem QAUDLVL este setată pe *AUDFAIL, atunci API-ul Verificare sistem generează înregistrări de auditare pentru a raporta orice eșecuri și erori pe care le găsec comenzile Restaurare obiect (RSTOBJ), Restaurare bibliotecă (RSTLIB) și Verificare integritate obiect (CHKOBJITG).
- Dacă utilizatorul specifică faptul că API-ul Verificare sistem utilizează un fișier de rezultate din sistemul de fișiere integrat, atunci API-ul creează fișierul dacă acesta nu există sau API-ul adaugă la sfârșitul fișierului pentru a raporta orice erori pe care le găsește API-ul.

Operații înrudite

“Verificarea integrității funcției de verificare cod” la pagina 42

Aflați cum să verificați integritatea funcției de verificare cod pe care o folosiți la verificarea integrității sistemului i5/OS.

Scenarii de semnare a obiectelor

Utilizați aceste informații pentru a vedea scenarii care ilustrează câteva situații tipice pentru utilizarea capacităților de semnare a obiectelor și de verificare a semnăturilor. Fiecare scenariu furnizează și operațiile de configurare pe care trebuie să le realizați pentru a implementa scenariul așa cum este descris.

Sistemul dumneavoastră oferă câteva metode diferite pentru semnarea obiectelor și verificarea semnăturilor de pe obiecte. Modul în care optați să semnați obiecte și modul în care lucrați cu obiectele semnate variază în funcție de nevoile și obiectivele dumneavoastră de afaceri și de securitate. În unele cazuri, ați putea avea nevoie numai să verificați semnăturile obiectelor de pe sistemul dumneavoastră pentru a vă asigura că integritatea aceluși obiect este intactă. În alte cazuri, puteți opta să semnați obiecte pe care le distribuiți altor persoane. Semnarea obiectelor permite altor persoane să identifice originea obiectelor și să verifice integritatea obiectelor.

Metoda pe care alegeți să o folosiți depinde de mai mulți factori. Scenariile furnizate în acest subiect descriu câteva dintre cele mai obișnuite obiective de semnare a obiectelor și de verificare a semnăturilor în cadrul contextelor de afaceri tipice. Fiecare scenariu descrie de asemenea și cerințele preliminare și operațiile pe care trebuie să le realizați pentru a implementa scenariul așa cum este descris. Revedeți aceste scenarii pentru a vă ajuta să determinați modul în care puteți utiliza capacitățile de semnare a obiectelor, astfel încât să se potrivească cel mai bine cu necesitățile dumneavoastră de afaceri și de securitate.

Scenariu: Utilizați DCM pentru a semna obiecte și pentru a verifica semnăturile

Acest scenariu descrie o companie care dorește să semneze obiecte aplicație vulnerabile pe serverul Web public al acesteia. Aceasta dorește să poată determina mai ușor modificările neautorizate făcute asupra acestor obiecte. Pe baza nevoilor de afaceri și a scopurilor de securitate ale companiei, acest scenariu descrie modul de utilizare pentru DCM (Digital Certificate Manager) ca metodă primară pentru semnarea obiectelor și verificarea semnăturilor obiectelor.

Situație

Ca administrator pentru MyCo, Inc. sunteți responsabil pentru gestionarea celor două sisteme ale companiei dumneavoastră. Unul dintre aceste sisteme furnizează un sit Web public pentru compania dumneavoastră. Dumneavoastră utilizați sistemul de producție internă al companiei dumneavoastră pentru a dezvolta conținutul acestui sit Web public și pentru a transfera fișierele și obiectele program pe serverul Web public după testarea acestora.

Serverul Web public al companiei furnizează un site Web cu informații generale despre companie. Site-ul Web oferă de asemenea și diferite formulare pe care clienții le completează pentru înregistrarea produselor și pentru a cere informații despre produse, anunțuri despre actualizarea produselor, locațiile de distribuție ale produselor și așa mai departe. Sunteți preocupat de vulnerabilitatea programelor cgi-bin care furnizează aceste formulare; cunoașteți că acestea pot fi modificate. De aceea, doriți să puteți verifica integritatea acestor obiecte program și să detectați când s-au efectuat asupra lor modificări neautorizate. În consecință, v-ați decis să semnați digital aceste obiecte pentru a îndeplini acest scop de securitate.

Ați cercetat capacitățile de semnare a obiectelor i5/OS și ați aflat că există mai multe metode pe care le puteți utiliza pentru a semna obiectele și a verifica semnăturile obiectelor. Deoarece sunteți responsabil pentru gestionarea unui număr mic de sisteme și nu credeți că va trebui să semnați obiecte des, ați decis să utilizați Digital Certificate Manager (DCM) pentru a efectua aceste operații. V-ați decis de asemenea să creați o Autoritate de certificare locală (Local Certificate Authority - CA) și să utilizați 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 cumpărați un certificat de la o CA publică binecunoscută.

Acest exemplu servește ca o introducere utilă în pașii implicați în setarea și utilizarea semnării obiectelor atunci când doriți să semnați obiecte pe un număr redus de sisteme.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Semnarea obiectelor vă oferă un mijloc de verificare a integrității obiectelor vulnerabile și de determinare mai ușoară a modificărilor aduse obiectelor după ce acestea au fost semnate. Acest lucru poate reduce unele depanări pe care le veți face în viitor pentru a depista problemele aplicațiilor și alte probleme ale sistemului.
- Utilizarea interfeței utilizator grafică (GUI) a DCM pentru semnarea obiectelor și verificarea semnăturilor obiectelor vă permite dumneavoastră și altor persoane din companie să realizeze aceste operații rapid și ușor.
- Utilizarea DCM pentru semnarea obiectelor și verificarea semnăturilor reduce durata de timp pe care trebuie să o petreceți pentru înțelegerea și 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 puțin costisitoare de implementat.

Obiective

În acest scenariu, dumneavoastră doriți să semnați digital obiecte vulnerabile, cum ar fi programe cgi-bin care generează formulare, pe serverul public al companiei dumneavoastră. Ca administrator de sistem la MyCo, Inc, doriți să utilizați DCM (Digital Certificate Manager) pentru a semna aceste obiecte și pentru a verifica semnăturile obiectelor.

Obiectivele acestui scenariu sunt după cum urmează:

- Aplicațiile companiei și alte obiecte vulnerabile de pe serverul Web public (Sistem B) trebuie să fie semnate cu un certificat de la o CA locală pentru limitarea costurilor semnării aplicațiilor.
- Administratorii de sistem și alți utilizatori desemnați trebuie să poată verifica cu ușurință semnăturile digitale de pe sisteme pentru a verifica sursa și autenticitatea obiectelor semnate de companie. Pentru a realiza acest lucru, fiecare sistem trebuie să aibă o copie atât a certificatului de verificare a semnăturii al companiei, cât și a certificatului Autorității de certificare (CA) locale în fiecare depozit de certificate *SIGNATUREVERIFICATION a serverelor.
- Prin verificarea semnăturilor de pe aplicațiile companiei și de pe alte obiecte ale companiei, administratorii și alții pot detecta dacă conținutul obiectelor s-a modificat după ce acestea au fost semnate.

- Administratorul de sistem trebuie să utilizeze DCM pentru semnarea obiectelor; administratorul de sistem și alții trebuie să poată utiliza DCM pentru verificarea semnăturilor obiectelor.

Detalii

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

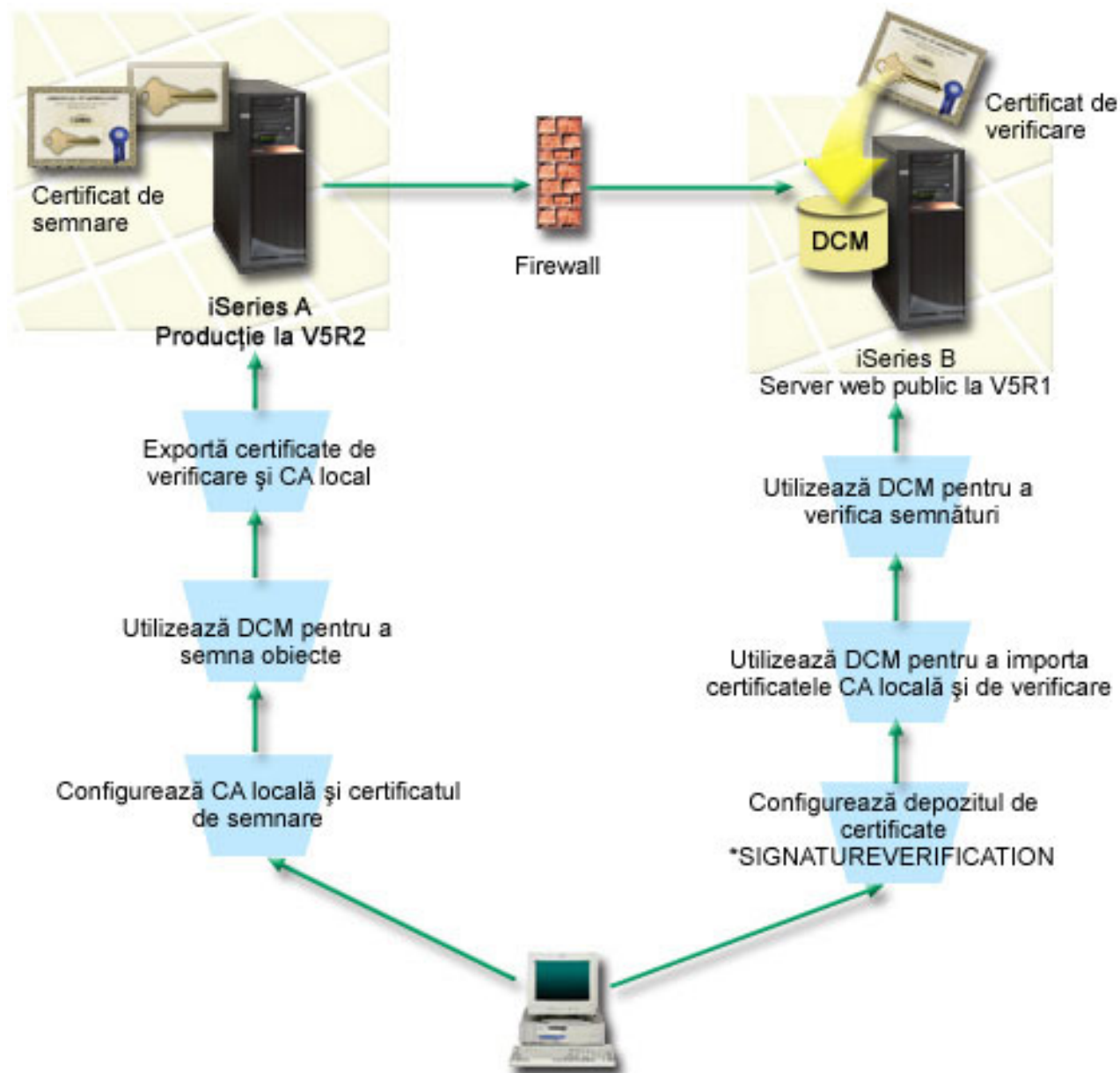


Figura ilustrează următoarele puncte relevante pentru acest scenariu:

Sistem A

- Sistemul A rulează i5/OS Versiune 5 Ediție 2 (V5R2).
- Sistem A este serverul de producție intern al companiei și platforma de dezvoltare pentru serverul Web iSeries public (Sistem B).

- Sistemul A are instalat un Cryptographic Access Provider 128-bit (Furnizor de acces criptografic pe 128 de biți) pentru iSeries (5722–AC3).
- Sistemul A are instalat și configurat DCM (Digital Certificate Manager) (i5/OS opțiunea 34) și IBM HTTP Server (5722–DG1).
- Sistemul A se comportă ca Autoritatea de certificare (CA) locală și certificatul de semnare a obiectelor se află pe acest sistem.
- Sistemul A utilizează DCM pentru semnarea obiectelor și este sistemul primar de semnare a obiectelor pentru aplicațiile publice și alte obiecte ale companiei.
- Sistemul A este configurat pentru activarea verificării semnăturilor.

Sistem B

- Sistemul B rulează i5/OS Versiune 5 Ediție 1 (V5R1).
- Sistemul B este serverul Web public extern al companiei din afara firewall-ului companiei.
- Sistemul B are instalat un Cryptographic Access Provider (Furnizor de acces criptografic) 128-bit (5722–AC3).
- Sistemul B are instalat și configurat DCM (Digital Certificate Manager) (i5/OS opțiunea 34) și IBM HTTP Server (5722–DG1).
- Sistemul B nu operează un CA local și nici nu semnează obiecte.
- Sistemul B este configurat pentru activarea verificării semnăturilor utilizând DCM pentru crearea depozitului de certificate *SIGNATUREVERIFICATION și pentru importarea verificării necesare și a certificatelor CA local.
- DCM este utilizat pentru a verifica semnăturile obiectelor.

Cerințe preliminare și presupuneri

Acest scenariu depinde de următoarele cerințe preliminare și supoziții:

1. Toate sistemele îndeplinesc cerințele preliminare pentru instalarea și utilizarea DCM.
2. Nimeni nu a configurat sau utilizat anterior DCM pe oricare din sisteme.
3. Toate sistemele au instalat cel mai înalt nivel al programului licențiat Cryptographic Access Provider 128-bit (5722-AC3).
4. Setarea implicită pentru variabila de sistem de verificare a semnăturilor în timpul restaurării (QVIFYOBJRST) pe toate sistemele din scenariu este 3 și nu a fost modificată de la această setare. Setarea implicită asigură că serverul poate verifica semnăturile obiectelor pe măsură ce restaurați obiectele semnate.
5. Administratorul de sistem pentru Sistem A trebuie să aibă autorizarea specială *ALLOBJ pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicația de semnare a obiectelor.
6. Administratorul de sistem sau oricine creează un depozit de certificate în DCM trebuie să aibă autorizările speciale *SECADM și *ALLOBJ.
7. Administratorul de sistem sau alții de pe toate celelalte sisteme trebuie să aibă autorizarea specială *AUDIT pentru verificarea semnăturilor obiectelor.

Pașii operației de configurare

Există două seturi de operații pe care trebuie să le efectuați pentru a implementa acest scenariu: Un set de operații vă permite să configurați Sistem A ca o Autoritate de certificare (CA) locală și să semnați și să verificați semnăturile obiectelor. Al doilea set de operații vă permite să configurați Sistemul B pentru verificarea semnăturilor pe care Sistemul A le creează.

Vedeți detaliile scenariului prezentate mai jos pentru a termina acești pași.

Pașii task-ului pentru Sistem A

Trebuie să efectuați fiecare dintre aceste task-uri pe Sistem A pentru a crea un CA local privat și pentru a semna obiecte și verifica semnăturile obiectelor așa cum descrie scenariul:

1. Efectuați toți pașii preliminari pentru a instala și configura toate produsele iSeries necesare
2. Utilizați DCM pentru a crea o Autoritate de certificare locală (CA) pentru a emite un certificat pentru semnarea obiectelor.
3. Utilizați DCM pentru a crea o definiție de aplicație
4. Utilizați DCM pentru a atribui un certificat pentru definiția de aplicație pentru semnarea obiectelor
5. Utilizați DCM pentru a semna obiectele program cgi-bin
6. Folosiți DCM pentru a exporta certificatele pe care celelalte sisteme trebuie să le folosească pentru verificarea semnăturilor obiectelor. Trebuie să exportați într-un fișier atât o copie a certificatului CA locală, cât și o copie a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor.
7. Transferați fișierele certificat pe serverul public al companiei (Sistem B) pentru ca dumneavoastră sau alții să puteți verifica semnăturile pe care le creează Sistemul A

Pașii task-ului pentru Sistem B

Dacă intenționați să restaurați obiectele semnate pe care le transferați pe serverul Web public din acest scenariu (Sistem B), trebuie să efectuați aceste operații de configurare pentru verificarea semnăturii pe Sistemul B înainte de a transfera obiectele semnate. Configurația verificării semnăturilor trebuie să fie terminată înainte ca dumneavoastră să puteți verifica semnăturile cu succes, pe măsură ce restaurați obiectele semnate pe serverul Web public.

Pe Sistem B trebuie să efectuați aceste task-uri pentru verificarea semnăturilor de pe obiecte așa cum descrie acest scenariu:

1. Utilizați DCM pentru a crea depozitul de certificate *SIGNATUREVERIFICATION
2. Utilizați DCM pentru a importa certificatul CA local și certificatul pentru verificarea semnăturii
3. Utilizați DCM pentru a verifica semnăturile pentru obiectele transferate

Informații înrudite

DCM (Digital Certificate Manager)

Detalii scenariu: Utilizați DCM pentru a semna obiecte și pentru a verifica semnăturile

Efectuați următorii pași de operație pentru configurare și utilizați Digital Certificate Manager pentru semnarea obiectelor așa cum descrie acest scenariu.

Pasul 1: Efectuați toți pașii preliminari

Trebuie să efectuați toate operațiile preliminare pentru instalarea și configurarea tuturor produselor iSeries necesare înainte de a putea realiza operațiile de configurare specifice pentru implementarea acestui scenariu.

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

Când utilizați DCM (Digital Certificate Manager) pentru crearea unei Autorizări de certificare (CA) locală, procesul vă cere să completați o serie de formulare. Aceste formulare vă ghidează prin procesul de creare a CA și de efectuare a altor operații necesare pentru începerea utilizării certificatelor digitale pentru SSL (Secure Sockets Layer), semnarea obiectelor și verificarea semnăturilor. Deși în acest scenariu nu trebuie să configurați certificate pentru SSL, trebuie să completați toate formularele din task-ul de configurare a sistemului pentru semnarea obiectelor.

Pentru a utiliza DCM la crearea și operarea unei CA locale, urmați acești pași: Acum că ați creat o CA locală și un certificat de semnare a obiectelor, trebuie să definiți o aplicație de semnare a obiectelor care să utilizeze certificatul înainte de a putea semna obiecte.

1. Porniți DCM.
2. În cadrul de navigare al DCM, selectați **Crearea unei Autorități de certificare (CA)** pentru a afișa o serie de formulare.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular din această operație ghidată, selectați butonul cu semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

3. Completați toate formularele pentru acest task ghidat. Pe măsură ce efectuați acest task, trebuie să faceți următoarele:
 - a. Să furnizați informații de identificare pentru CA locală.
 - b. Să instalați certificatul CA locală în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaște CA locală și să poată valida certificatele pe care CA locală le emite.
 - c. Să specificați datele de poliță pentru CA dumneavoastră locală.
 - d. Să utilizați noua CA locală pentru a emite un certificat server sau client pe care aplicațiile dumneavoastră să îl poată utiliza pentru conexiuni SSL.

Notă: Deși acest scenariu nu utilizează acest certificat, trebuie să îl creați înainte de a putea utiliza CA locală pentru emiterea certificatului de semnare a obiectelor de care aveți nevoie. Dacă anulați operația fără a crea acest certificat, trebuie să vă creați certificatul de semnare a obiectelor și depozitul de certificate *OBJECTSIGNING în care este memorat separat.

- e. Să selectați aplicațiile care pot utiliza certificatul server sau client pentru conexiuni SSL.

Notă: Pentru scopurile acestui scenariu, nu selectați nici o aplicație și faceți clic pe **Continuare** pentru a afișa următorul formular.

- f. Utilizați noua CA locală pentru emiterea unui certificat de semnare a obiectelor pe care aplicațiile îl pot utiliza pentru semnarea digitală a obiectelor. Acest subtask creează depozitul de certificate *OBJECTSIGNING. Acesta este depozitul de certificate pe care îl utilizați pentru gestionarea certificatelor de semnare a obiectelor.
- g. Selectați aplicațiile care vor avea încredere în CA locală.

Notă: Pentru scopurile acestui scenariu, nu selectați nici o aplicație și faceți clic pe **Continuare** pentru a termina operația.

Pasul 3: Creați o definiție de aplicație pentru semnarea obiectelor

După ce vă creați certificatul de semnare a obiectelor, trebuie să utilizați DCM (Digital Certificate Manager) pentru definirea unei aplicații de semnare a obiectelor pe care să o utilizați pentru semnarea obiectelor. Definiția de aplicație nu trebuie să se refere la o aplicație reală; definiția de aplicație pe care o creați poate descrie tipul sau grupul de obiecte pe care intenționați să le semnați. Aveți nevoie de definiție pentru a putea avea un ID de aplicație asociat cu certificatul pentru activarea procesului de semnare.

Pentru a utiliza DCM la crearea unei definiții a aplicației de semnare a obiectelor, urmați acești pași:

1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați *OBJECTSIGNING ca depozit de certificate pe care să-l deschideți.
2. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.
3. În cadrul de navigare, selectați **Gestiune aplicații** pentru a afișa o listă de operații.
4. Selectați **Adăugare aplicație** din lista de operații pentru afișarea unui formular pentru definirea aplicației.
5. Completați formularul și faceți clic pe **Adăugare**.

Acum trebuie să alocați certificatul dumneavoastră de semnare a obiectelor aplicației pe care ați creat-o.

Pasul 4: Alocați un certificat definiției aplicației de semnare a obiectelor

Pentru a aloca certificatul aplicației dumneavoastră de semnare a obiectelor, urmați acești pași:

1. În cadrul de navigare DCM, selectați **Gestiune certificate** pentru a afișa o listă de operații.
2. Din lista de operații, selectați **Alocare certificat** pentru afișarea unei liste de certificate pentru depozitul de certificate curent.

3. Selectați un certificat din listă și faceți clic pe **Alocare la aplicație** pentru a afișa o listă de definiții de aplicații pentru depozitul de certificate.
4. Selectați una sau mai multe aplicații din listă și faceți clic pe **Continuare**. Este afișată o pagină de mesaj pentru a confirma alocarea certificatului sau pentru a oferi informațiile de eroare dacă s-a produs o eroare.

Când terminați această operație, sunteți gata să utilizați DCM pentru semnarea obiectelor program pe care serverul Web public al companiei (Sistem B) le va utiliza.

Pasul 5: Semnați obiectele program

Pentru utilizarea DCM la semnarea obiectelor program pentru utilizare pe serverul Web public al companiei (Sistem B), urmați acești pași:

1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați ***OBJECTSIGNING** ca depozit de certificate pe care să-l deschideți.
2. Introduceți parola pentru depozitul de certificate ***OBJECTSIGNING** și faceți clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectați **Gestiune obiecte ce pot fi semnate** pentru afișarea unei liste de operații.
4. Din lista de operații, selectați **Semnarea unui obiect** pentru afișarea unei liste de definiții de aplicații pe care le puteți utiliza pentru semnarea obiectelor.
5. Selectați aplicația pe care ați definit-o în pasul anterior și faceți clic pe **Semnarea unui obiect**. Este afișat un formular care vă permite să specificați locația obiectului pe care doriți să-l semnați.
6. În câmpul furnizat, introduceți calea și numele de fișier complet determinate ale obiectului sau directorului de obiecte pe care doriți să-l semnați și faceți clic pe **Continuare**. Sau, introduceți o locație de director și faceți clic pe **Răsfoire** pentru a vedea conținutul directorului pentru selectarea obiectelor de semnat.

Notă: Trebuie să începeți numele obiectului cu un slash sau veți întâlni o eroare. Puteți de asemenea utiliza anumite caractere de înlocuire pentru a descrie partea din director pe care doriți să o semnați. Aceste caractere de înlocuire sunt asteriscul (*), care specifică *orice număr de caractere* și semnul de întrebare(?), care specifică *orice caracter singular*. De exemplu, pentru a semna toate obiectele dintr-un anumit director, puteți introduce `/mydirectory/*`; pentru a semna toate programele dintr-o anumită bibliotecă, puteți introduce `/QSYS.LIB/QGPL.LIB/*.PGM`. Puteți utiliza aceste caractere de înlocuire numai în ultima parte a numelui căii; de exemplu, `/mydirectory*/filename` dă un mesaj de eroare. Dacă doriți să utilizați funcția **Răsfoire** pentru a vedea o listă cu conținutul bibliotecii sau directorului, trebuie să introduceți caracterul de substituție ca parte a numelui de cale înainte de a face clic pe **Răsfoire**.

7. Selectați opțiunile de procesare pe care doriți să le utilizați pentru semnarea obiectului sau obiectelor selectate și faceți clic pe **Continuare**.

Notă: Dacă doriți să așteptați rezultatele jobului, fișierul de rezultate se va afișa direct în browser-ul dumneavoastră. Rezultatele pentru jobul curent sunt adăugate la sfârșitul fișierului de rezultate. În consecință, fișierul poate conține rezultate din orice alte joburi anterioare, în plus față de rezultatele jobului curent. Puteți utiliza câmpul de dată din fișier pentru a determina ce linii din fișier se aplică jobului curent. Câmpul de dată este în format AAAALLZZ. Primul câmp din fișier 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. Specificați calea și numele de fișier complet determinate care să fie utilizate pentru memorarea rezultatelor jobului pentru operația de semnare a obiectelor și faceți clic pe **Continuare**. Sau, introduceți o locație de director și faceți clic pe **Răsfoire** pentru a vedea conținutul directorului pentru selectarea unui fișier de stocare a rezultatelor jobului. Este afișat un mesaj care indică faptul că jobul a fost lansat pentru semnarea obiectelor. Pentru a vedea rezultatele jobului, consultați **QOJSGNBAT** a jobului din istoricul de job.

Pentru a vă asigura că dumneavoastră și alte persoane puteți verifica semnăturile, trebuie să exportați certificatele necesare într-un fișier și să transferați fișierul de certificare pe Sistem B. Trebuie de asemenea să efectuați toate operațiile de configurare a verificării semnăturilor pe Sistem B înainte de a transfera obiectele program semnate pe Sistem B. Configurarea verificării semnăturilor trebuie să fie încheiată înainte ca dumneavoastră să puteți verifica cu succes semnăturile, pe măsură ce restaurați obiectele semnate pe Sistem B.

Pasul 6: Exportați certificatele pentru a da posibilitatea verificării semnăturii pe Sistem B

Semnarea obiectelor pentru protejarea integrității conținutului necesită ca dumneavoastră și alte persoane să aveți un mijloc pentru verificarea autenticității semnăturilor. Pentru verificarea semnăturilor obiectelor pe același sistem care semnează obiectele (Sistem A), trebuie să utilizați DCM pentru crearea depozitului de certificate *SIGNATUREVERIFICATION. Acest depozit de certificate trebuie să conțină atât o copie a certificatului de semnare a obiectelor, cât și o copie a certificatului CA, pentru Autoritatea de certificare (CA) care a emis certificatul de semnare.

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

Pentru a utiliza DCM astfel încât să puteți verifica semnături pe același sistem care semnează obiectele (Sistem A în acest scenariu), urmați acești pași:

1. În cadrul de navigare, selectați **Creare depozit de certificare nou** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l creați.
2. Selectați **Da** pentru copierea certificatelor existente de semnare a obiectelor în noul depozit de certificate ca certificate de verificare a semnăturilor.
3. Specificați o parolă pentru noul depozit de certificate și faceți clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteți utiliza DCM pentru verificarea semnăturilor pe același sistem pe care îl utilizați pentru semnarea obiectelor.

Pentru a utiliza DCM la exportarea unei copii a certificatului CA locală și a unei copii a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor, astfel încât să puteți verifica semnăturile obiectelor pe alte sisteme (Sistem B), urmați acești pași:

1. În cadrul de navigare, selectați **Gestiune certificate**, și apoi selectați operația **Exportare certificate**.
2. Selectați **Autoritate de certificare (CA)** și faceți clic pe **Continuare** pentru a afișa o listă a certificatelor CA pe care le puteți exporta.
3. Selectați certificatul CA locală pe care l-ați creat mai devreme din listă și faceți clic pe **Export**.
4. Specificați **Fișier** ca destinație de export și faceți clic pe **Continuare**.
5. Specificați o cale și un nume de fișier complet determinate pentru certificatul CA locală și faceți clic pe **Continuare** pentru a exporta certificatul.
6. Faceți clic pe **OK** pentru a ieși din pagina de confirmare Export. Acum puteți exporta o copie a certificatului de semnare a obiectelor.
7. Re-selectați operația **Exportare certificat**.
8. Selectați **Semnare obiect** pentru a afișa o listă a certificatelor de semnare a obiectelor pe care le puteți exporta.
9. Selectați certificatul corespunzător de semnare a obiectelor din listă și faceți clic pe **Export**.
10. Selectați **Fișier, ca certificat de verificare a semnăturilor** ca destinație și faceți clic pe **Continuare**.
11. Specificați o cale și un nume de fișier complet determinate pentru certificatul de verificare a semnăturilor exportat și faceți clic pe **Continuare** pentru a exporta certificatul.

Acum puteți transfera aceste fișiere pe sistemele punct final pe care intenționați să verificați semnăturile pe care le-ați creat cu certificatul respectiv.

Pasul 7: Transferați fișierele certificat pe serverul public al companiei, Sistem B

Trebuie să transferați fișierele de certificare pe care le-ați creat pe Sistem A, pe Sistem B, serverul Web public al companiei în acest scenariu, înainte de a le putea configura pentru verificarea obiectelor pe care le semnați. Puteți utiliza câteva metode diferite pentru transferarea fișierelor de certificare. De exemplu, puteți utiliza FTP (File Transfer Protocol) sau distribuirea de pachete din Administrare centrală pentru a transfera fișierele.

Pasul 8: Task-uri de verificare a semnăturii: Crearea depozitului de certificate *SIGNATUREVERIFICATION

Pentru verificarea semnăturilor obiectelor pe Sistem B (serverul Web public al companiei), Sistem B trebuie să aibă o copie a certificatului corespunzător de verificare a semnăturilor în depozitul de certificate

*SIGNATUREVERIFICATION. Deoarece ați utilizat un certificat emis de o CA locală pentru semnarea obiectelor, acest depozit de certificate trebuie să conțină și o copie a certificatului CA locală.

Pentru crearea depozitului de certificate *SIGNATUREVERIFICATION, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare DCM (Digital Certificate Manager) selectați **Creare depozit de certificate nou** și selectați *SIGNATUREVERIFICATION ca depozit de certificate pe care să-l creați.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular în timpul utilizării DCM, selectați semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

3. Specificați o parolă pentru noul depozit de certificate și faceți clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteți importa certificatele în depozit și le puteți utiliza pentru verificarea semnăturilor.

Pasul 9: Task-uri de verificare a semnăturii: Importarea certificatelor

Pentru a verifica semnătura de pe un obiect, depozitul de certificate *SIGNATUREVERIFICATION trebuie să conțină o copie a certificatului de verificare a semnăturilor. Dacă certificatul de semnare este privat, acest depozit de certificate trebuie să aibă și o copie a certificatului Autorității de certificare (CA) locală care a emis certificatul de semnare. În acest scenariu, ambele certificate erau exportate într-un fișier și acel fișier era transferat pe fiecare sistem punct final.

Pentru a importa aceste certificate în depozitul *SIGNATUREVERIFICATION, urmați acești pași: Acum puteți utiliza DCM pe Sistem B pentru a verifica semnăturile obiectelor pe care le-ați creat cu certificatul de semnare corespunzător pe Sistem A.

1. În cadrul de navigare al DCM, faceți clic pe **Selectare depozit de certificate** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l deschideți.
2. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectați **Gestiune certificate** pentru a afișa o listă de operații.
4. Din lista de operații, selectați **Importare certificate**.
5. Selectați **Autoritate de certificare (CA)** ca tipul certificatului și faceți clic pe **Continuare**.

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

6. Specificați calea și numele de fișier complet determinate pentru fișierul de certificare CA și faceți clic pe **Continuare**. Este afișat un mesaj care confirmă că procesul de importare a reușit sau care furnizează un mesaj de eroare dacă procesul a eșuat.
7. Re-selectați operația **Importare certificat**.
8. Selectați **Verificare semnături** ca tipul de certificat de importat și faceți clic pe **Continuare**.
9. Specificați calea și numele de fișier complet determinate pentru fișierul certificat de verificare a semnăturilor și faceți clic pe **Continuare**. Este afișat un mesaj care confirmă că procesul de importare a reușit sau care furnizează informațiile de eroare dacă procesul a eșuat.

Pasul 10: operații de verificare a semnăturii: Verificați semnătura pentru obiectele program

Pentru a utiliza DCM la verificarea semnăturilor pe obiecte program transferate, urmați acești pași:

1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l deschideți.

2. Introduceți parola pentru depozitul de certificate *SIGNATUREVERIFICATION și faceți clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectați **Gestiune obiecte ce pot fi semnate** pentru afișarea unei liste de operații.
4. Din lista de operații, selectați **Verificare semnătură obiect** pentru a specifica locația obiectelor pentru care doriți să verificați semnăturile.
5. În câmpul furnizat, introduceți calea și numele de fișier complet determinate ale obiectului sau directorului de obiecte pentru care doriți să verificați semnăturile și faceți clic pe **Continuare**. Sau introduceți o locație de director și faceți clic pe **Răsfoire** pentru a vedea conținutul directorului pentru selectarea obiectelor pentru verificarea semnăturilor.

Notă: Puteți de asemenea utiliza anumite caractere de înlocuire pentru a descrie partea din director pe care doriți să o verificați. Aceste caractere de înlocuire sunt asteriscul (*), care specifică *orice număr de caractere* și semnul de întrebare(?), care specifică *orice caracter singular*. De exemplu, pentru a semna toate obiectele dintr-un anumit director, puteți introduce /mydirectory/*; pentru a semna toate programele dintr-o anumită bibliotecă, puteți introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteți utiliza aceste caractere de înlocuire numai în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă doriți să utilizați funcția Răsfoire pentru a vedea o listă cu conținutul bibliotecii sau directorului, trebuie să introduceți caracterul de substituție ca parte a numelui de cale înainte de a face clic pe **Răsfoire**.

6. Selectați opțiunile de procesare pe care doriți să le utilizați pentru verificarea semnăturilor pe obiectul sau obiectele selectate și faceți clic pe **Continuare**.

Notă: Dacă doriți să așteptați rezultatele jobului, fișierul de rezultate se va afișa direct în browser-ul dumneavoastră. Rezultatele pentru jobul curent sunt adăugate la sfârșitul fișierului de rezultate. În consecință, fișierul poate conține rezultate din orice alte joburi anterioare, în plus față de rezultatele jobului curent. Puteți utiliza câmpul de dată din fișier pentru a determina ce linii din fișier se aplică jobului curent. Câmpul de dată este în format AAAALLZZ. Primul câmp din fișier 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. Specificați calea și numele de fișier complet determinate care să fie utilizate pentru memorarea rezultatelor jobului pentru operația de verificare a semnăturilor și faceți clic pe **Continuare**. Sau, introduceți o locație de director și faceți clic pe **Răsfoire** pentru a vedea conținutul directorului pentru selectarea unui fișier de stocare a rezultatelor jobului. Este afișat un mesaj care indică faptul că jobul a fost lansat pentru verificarea semnăturilor obiectelor. Pentru a vedea rezultatele jobului, consultați **QOBJSGBAT** a jobului din istoricul de job.

Scenariu: Utilizați API-uri pentru a semna obiecte și pentru a verifica semnăturile obiectelor

Acest scenariu descrie o companie de dezvoltare de aplicații care dorește să semneze în mod programat aplicațiile pe care le vinde. Aceasta dorește să poată asigura clienții că aplicația provine de la companie și să le furnizeze un mijloc de detectare a modificărilor neautorizate asupra aplicațiilor atunci când le instalează. Pe baza nevoilor de afaceri și a scopurilor de securitate ale companiei, acest scenariu descrie modul de utilizare a API-ului Sign Object (Semnare obiect) și a API-ului Add Verifier (Adăugare verificator) pentru semnarea obiectelor și activarea verificării semnăturilor.

Situație

Compania dumneavoastră (MyCo, Inc.) este un partener de afaceri care dezvoltă aplicații pentru clienți. Ocupându-vă de dezvoltarea de software pentru companie, sunteți responsabil de împachetarea acestor aplicații pentru distribuția către clienți. Momentan, utilizați programe pentru împachetarea unei aplicații. Clienții pot comanda un compact disc (CD-ROM) sau pot vizita pagina dumneavoastră de Web și descărca aplicația.

Sunteți la curent cu noutățile din industrie, în special cu cele de securitate. În consecință, știți că clienții sunt preocupați în mod justificat de sursa și conținutul programelor pe care le primesc sau le descarcă. Există situații în care clienții cred că primesc sau descarcă un produs de la o sursă de încredere care se dovedește a nu fi adevărata sursă a produsului. Uneori această confuzie face ca clienții să instaleze un produs diferit de cel la care se așteptau. Uneori produsul instalat se dovedește a fi un program dăunător sau care a fost modificat și deteriorează sistemul.

Deși aceste tipuri de probleme nu sunt obișnuite pentru beneficiari, doriți să vă asigurați clienții că aplicațiile pe care le obțin de la dumneavoastră provin cu adevărat de la compania dumneavoastră. Doriți de asemenea să furnizați clienților o metodă de verificare a integrității acestor aplicații, astfel încât ei să poată determina dacă aplicațiile au fost modificate înainte de instalarea lor.

Pe baza cercetărilor dumneavoastră, v-ați decis să puteți utiliza capacitățile de semnare a obiectelor i5/OS pentru a vă atinge scopurile de securitate. Semnarea digitală a aplicațiilor dumneavoastră permite clienților să verifice că compania dumneavoastră este sursa legitimă a aplicației pe care o primesc sau o descarcă. Deoarece momentan vă împachetați aplicațiile în mod programat, v-ați decis să utilizați API-uri pentru a adăuga cu ușurință semnarea obiectelor la procesul dumneavoastră de împachetare existent. De asemenea vă decideți să utilizați un certificat public pentru semnarea obiectelor, astfel încât să faceți procesul de verificare a semnăturilor transparent pentru clienții dumneavoastră atunci când își instalează produsul dumneavoastră.

Ca parte din pachetul aplicației veți include o copie a certificatului digital pe care l-ați utilizat pentru semnarea obiectului. Când un client obține pachetul aplicației, el poate utiliza cheia publică a certificatului pentru verificarea semnăturii aplicației. Acest proces permite clientului să identifice și să verifice sursa aplicației, asigurându-se în același timp că conținutul obiectelor aplicației nu a fost modificat din momentul semnării lor.

Acest exemplu servește ca o introducere utilă în pașii implicați în semnarea programată a obiectelor pentru aplicațiile pe care le dezvoltați și le împachetați pentru a fi utilizate de către alte persoane.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Utilizarea API-urilor pentru împachetarea și semnarea obiectelor în mod programat reduce durata de timp pe care trebuie să o petreceți pentru implementarea acestei securități.
- Utilizarea API-urilor pentru semnarea obiectelor pe măsură ce le împachetați reduce numărul de pași pe care trebuie să îi efectuați pentru semnarea obiectelor, deoarece procesul de semnare face parte din procesul de împachetare.
- Semnarea unui pachet de obiecte vă permite să determinați mai ușor dacă obiectele au fost modificate după ce au fost semnate. Acest lucru poate reduce unele depanări pe care le veți face în viitor pentru depistarea problemelor aplicațiilor pentru clienți.
- Utilizarea unui certificat de la o Autorizare de certificare (CA) publică binecunoscută pentru semnarea obiectelor vă permite să utilizați API-ul Add Verifier ca parte a unui program de ieșire în programul de instalare al produsului dumneavoastră. Utilizarea acestui API vă permite să adăugați automat certificatul public pe care l-ați utilizat la semnarea aplicației pe sistemul clientului dumneavoastră. Acest lucru asigură clientului dumneavoastră transparența verificării semnăturilor.

Obiective

În acest scenariu, MyCo, Inc. dorește să semneze automat aplicațiile pe care le împachetează și le distribuie clienților săi. Ca dezvoltator de producere de aplicații la MyCo, Inc, împachetați curent aplicațiile companiei dumneavoastră prin program pentru distribuirea la clienți. În consecință, doriți să utilizați API-urile sistemului pentru semnarea aplicațiilor dumneavoastră și ca beneficiarii sistemului să verifice în mod programat semnătura în timpul instalării produsului.

Obiectivele acestui scenariu sunt după cum urmează:

- Persoana care se ocupă de dezvoltarea producției în cadrul companiei trebuie să poată semna obiecte utilizând API-ul Semnare obiect ca parte a unui proces existent de împachetare programată a aplicațiilor.
- Aplicațiile companiei trebuie să fie semnate cu un certificat public pentru a asigura clientului transparența procesului de verificare a semnăturii în timpul instalării produsului aplicație.
- Compania trebuie să poată utiliza API-urile sistemului pentru a adăuga în mod programat certificatul necesar de verificare a semnăturii în depozitul de certificate *SIGNATUREVERIFICATION al sistemului beneficiarului. Compania trebuie să poată crea prin program acest depozit de certificate pe sistemul beneficiarului ca parte din procesul de instalare a produsului, dacă acesta nu există încă.

- Clienții trebuie să poată verifica cu ușurință semnăturile digitale pe aplicația companiei după instalarea produsului. Clienții trebuie să poată verifica semnătura astfel încât să fie siguri de sursa și autenticitatea aplicației semnate și să poată de asemenea determina dacă au fost făcute modificări asupra aplicației din momentul în care a fost semnată.

Detalii

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

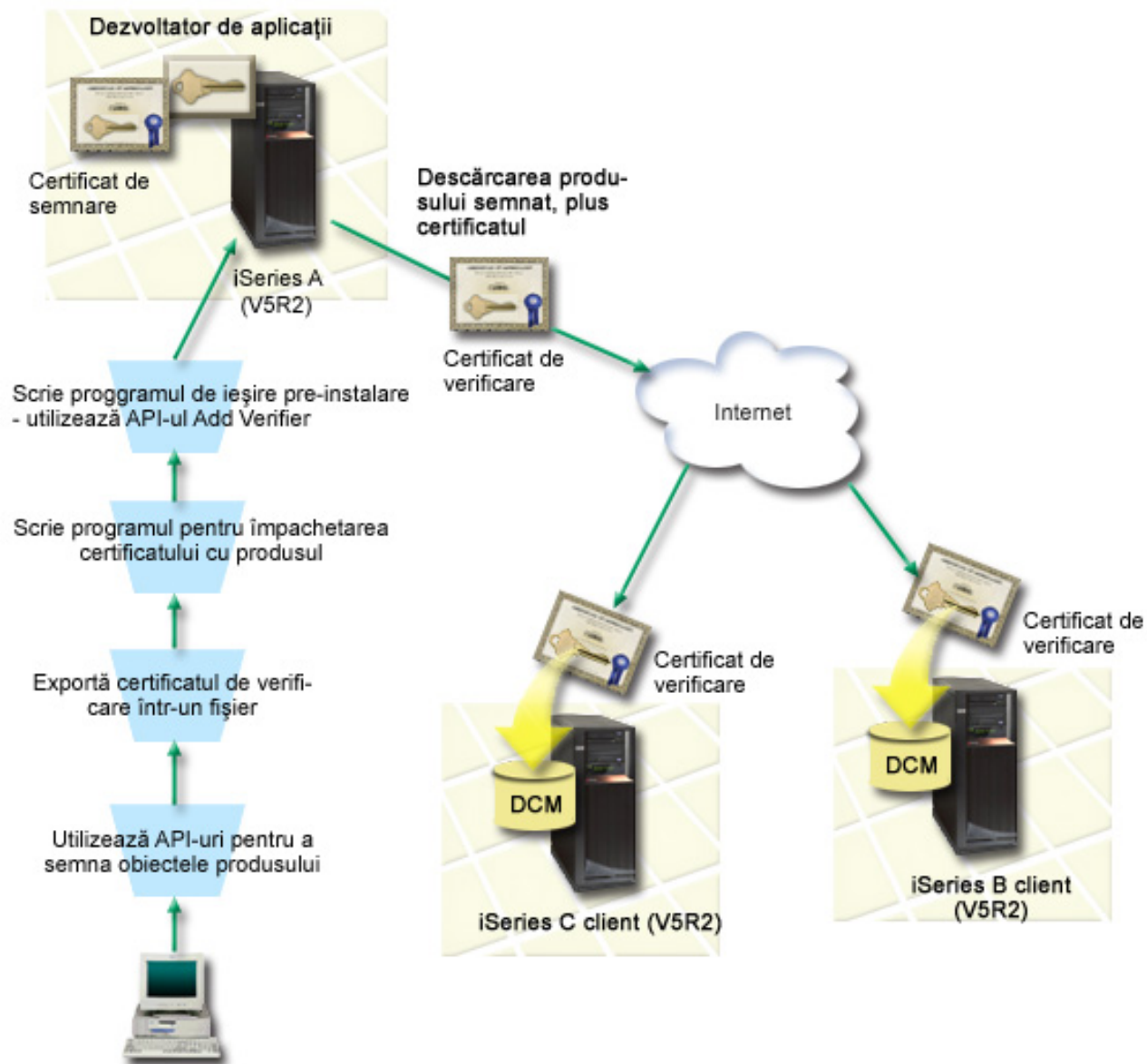


Figura ilustrează următoarele puncte relevante pentru acest scenariu:

Sistemul central A

- Sistemul A rulează i5/OS Versiune 5 Ediție 2 (V5R2).
- Sistemul A rulează programul de împachetare produs al dezvoltatorului de aplicații.
- Sistemul A are instalat un Cryptographic Access Provider 128-bit (Furnizor de acces criptografic pe 128 de biți) pentru iSeries (5722-AC3).

- Sistemul A are instalat și configurat DCM (Digital Certificate Manager) (i5/OS opțiunea 34) și IBM HTTP Server (5722–DG1).
- Sistemul A este sistemul primar de semnare a obiectelor pentru produsele aplicație ale companiei. Semnarea obiectelor produsului pentru distribuirea către client este realizată pe Sistem A prin efectuarea acestor operații:
 1. Utilizarea API-urilor pentru semnarea produsului aplicație al companiei.
 2. Utilizarea DCM pentru exportarea certificatului de verificare a semnăturilor într-un fișier astfel încât clienții să poată verifica obiectele semnate.
 3. Scrierea unui program pentru adăugarea certificatului de verificare a produsului aplicație semnat.
 4. Scrierea unui program de ieșire preinstalare pentru produsul care utilizează API-ul Add Verifier. Acest API permite procesului de instalare a produsului să adauge prin program certificatul de verificare în depozitul de certificate *SIGNATUREVERIFICATION pe sistemul beneficiarului (Sistemele B și C).

Sistemele beneficiarului B și C

- Sistemul B rulează OS/400 Versiune 5 Ediție 2 (V5R2) sau o ediție ulterioară de i5/OS.
- Sistemul C rulează OS/400 Versiune 5 Ediție 2 (V5R2) sau o ediție ulterioară de i5/OS.
- Sistemele B și C au instalat și configurat Digital Certificate Manager (opțiunea 34) și IBM HTTP Server (5722–DG1).
- Sistemele B și C achiziționează și descarcă o aplicație de pe situl Web al companiei dezvoltatorului de aplicații (care deține Sistemul A).
- Sistemele B și C obțin o copie a certificatului de verificare a semnăturii al MyCo atunci când procesul de instalare a aplicație MyCo creează depozitul de certificate *SIGNATUREVERIFICATION pe fiecare dintre aceste sisteme ale beneficiarului.

Cerințe preliminare și presupuneri

Acest scenariu depinde de următoarele cerințe preliminare și supoziții:

1. Toate sistemele îndeplinesc cerințele preliminare pentru instalarea și utilizarea DCM.

Notă: Îndeplinirea cerințelor preliminare pentru instalarea și utilizarea DCM este o cerință opțională pentru beneficiari (Sistemele B și C în acest scenariu). Deși API-ul Add Verifier creează depozitul de certificate *SIGNATUREVERIFICATION ca parte din procesul de instalare a produsului, dacă este necesar, îl creează cu o parolă implicită. Clienții trebuie să utilizeze DCM pentru modificarea parolei implicite pentru protejarea acestui depozit de certificate împotriva accesului neautorizat.
2. Nimeni nu a configurat sau utilizat anterior DCM pe oricare din sisteme.
3. Toate sistemele au instalat cel mai înalt nivel al programului licențiat Cryptographic Access Provider 128-bit (5722-AC3).
4. Setarea implicită pentru variabila de sistem de verificare a semnăturilor în timpul restaurării (QVIFYOBRST) pe toate sistemele din scenariu este 3 și nu a fost modificată de la această setare. Setarea implicită asigură că serverul poate verifica semnăturile obiectelor pe măsură ce restaurați obiectele semnate.
5. Administratorul de rețea pentru Sistem A trebuie să aibă autorizarea specială *ALLOBJ pentru profilul utilizator pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicația 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 și *ALLOBJ pentru profilul utilizator.
7. Administratorii de sistem sau alții de pe celelalte sisteme trebuie să aibă autorizarea specială *AUDIT pentru profilul utilizator pentru verificarea semnăturilor obiectelor.

Pașii operației de configurare

Pentru a semna obiectele așa cum se descrie în acest scenariu, vedeți subiectul cu detaliile scenariului de mai jos, pentru pașii de efectuat pe Sistem A pentru fiecare din următoarele task-uri:

1. Efectuați toți pașii preliminari pentru a instala și configura toate produsele iSeries necesare

2. Utilizați DCM pentru a crea o cerere de certificat pentru a obține un certificat pentru semnarea obiectelor de la o Autoritate de certificare (CA) publică bine cunoscută.
3. Utilizați DCM pentru a crea o definiție de aplicație pentru semnare obiecte
4. Utilizați DCM pentru a importa certificatul pentru semnare al obiectului semnat și pentru a-l atribui definiției dumneavoastră de aplicație pentru semnare obiecte
5. Utilizați 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 aplicației dumneavoastră
6. Actualizați programul dumneavoastră pentru împachetare de aplicații pentru a utiliza API-ul Sign Object pentru a vă semna aplicația
7. Creați un program de ieșire de pre-instalare care utilizează API-ul Add Verifier ca parte a procesului dumneavoastră de împachetare de aplicații. Acest program de ieșire vă permite să creați depozitul de certificate *SIGNATUREVERIFICATION și să adăugați certificatul necesar de verificare a semnăturilor pe un sistem al beneficiarului în timpul instalării produsului.
8. Puneți beneficiarii să utilizeze DCM pentru a reseta parola implicită pentru depozitul de certificate *SIGNATUREVERIFICATION pe sistemul lor

Informații înrudite

DCM (Digital Certificate Manager)

Detalii scenariu: Utilizați API-uri pentru a semna obiecte și pentru a verifica semnăturile obiectelor

Efectuați următorii pași de operație pentru utilizarea API-urilor i5/OS pentru semnarea obiectelor așa cum descrie acest scenariu.

Pasul 1: Efectuați toți pașii preliminari

Trebuie să efectuați toate operațiile preliminare pentru instalarea și configurarea tuturor produselor iSeries necesare înainte de a putea realiza operațiile de configurare specifice pentru implementarea acestui scenariu.

Pasul 2: Utilizați DCM pentru a obține un certificat de la o CA publică bine cunoscută

Acest scenariu presupune că nu ați utilizat anterior DCM (Digital Certificate Manager) pentru crearea și gestionarea certificatelor. În consecință, trebuie să creați 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 operațiile de care aveți nevoie pentru crearea și gestionarea certificatelor de semnare a obiectelor. Pentru a obține un certificat de la o Autoritate de certificare (CA) publică binecunoscută, utilizați DCM pentru crearea informațiilor de identificare și a perechii de chei publică-privată pentru certificat și trimiteți aceste informații către CA pentru obținerea certificatului dumneavoastră.

Pentru a crea informațiile de cerere a certificatului pe care trebuie să le furnizați la CA publice binecunoscute, astfel încât să vă obțineți certificatul de semnare a obiectelor, efectuați acești pași:

1. Porniți DCM.
2. În cadrul de navigare al DCM, selectați **Creare depozit de certificate nou** pentru a porni operația ghidată și pentru a completa o serie de formulare. Aceste formulare vă îndrumă prin procesul de creare a depozitului de certificate și a unui certificat pe care să-l puteți utiliza pentru semnarea obiectelor.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular din această operație ghidată, selectați butonul cu semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

3. Selectați ***OBJECTSIGNING** ca depozit de certificate de creat și faceți clic pe **Continuare**.
4. Selectați **Da** pentru crearea unui certificat ca parte a creației depozitului de certificate ***OBJECTSIGNING** și faceți clic pe **Continuare**.

5. Selectați **VeriSign sau altă Autoritare de certificare Internet (CA)** ca semnatar al noului certificat și faceți clic pe **Continuare** pentru a afișa un formular care vă permite să furnizați informații de identificare pentru noul certificat.
6. Completați formularul și faceți clic pe **Continuare** pentru a afișa o pagină de confirmare. Această pagină de confirmare afișează datele cererii pe care trebuie să le furnizați Autorității de certificare (CA) care vă va emite certificatul. Datele Certificate Signing Request - Cererii de semnare a certificatului (CSR) constau din cheia publică și alte informații pe care le-ați specificat pentru noul certificat.
7. Copiați și lipiți cu atenție datele CSR în formularul de cerere a certificatului, sau într-un fișier separat, pe care CA publică îl cere pentru solicitarea unui certificat. Trebuie să utilizați toate datele CSR, inclusiv liniile Început și Sfârșit cerere certificat nou. Când ieșiți din această pagină, datele se pierd și nu le mai puteți recupera.
8. Trimiteți formularul de solicitare sau fișierul către CA pe care ați ales-o pentru emiterea și semnarea certificatului dumneavoastră.
9. Așteptați ca Autoritatea de certificare (CA) să trimită înapoi certificatul semnat și completat înainte de a continua cu următorul pas de operație pentru scenariu.

Pasul 3: Creați o definiție de aplicație pentru semnarea obiectelor

Acum că ați trimis cererea dumneavoastră de certificat unei CA publice binecunoscute, puteți utiliza DCM pentru definirea unei aplicații de semnare a obiectelor pe care o puteți utiliza la semnarea obiectelor. Definiția de aplicație nu trebuie să se refere la o aplicație reală; definiția de aplicație pe care o creați poate descrie tipul sau grupul de obiecte pe care intenționați să le semnați. Aveți nevoie de definiție pentru a putea avea un ID de aplicație asociat cu certificatul pentru activarea procesului de semnare.

Pentru a utiliza DCM la crearea unei definiții a aplicației de semnare a obiectelor, urmați acești pași:

1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați ***OBJECTSIGNING** ca depozit de certificate pe care să-l deschideți.
2. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.
3. În cadrul de navigare, selectați **Gestiune aplicații** pentru a afișa o listă de operații.
4. Selectați **Adăugare aplicație** din lista de operații pentru afișarea unui formular pentru definirea aplicației.
5. Completați formularul și faceți clic pe **Adăugare**.

După ce obțineți certificatul semnat de la CA, puteți atribui certificatul aplicației pe care ați creat-o.

Pasul 4: Importați certificatul public semnat și atribuiți-l aplicației de semnare obiecte

Pentru a importa certificatul dumneavoastră și a-l alocă aplicației pentru a activa semnarea obiectelor, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați ***OBJECTSIGNING** ca depozit de certificate pe care să-l deschideți.
3. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.
4. După ce cadrul de navigare se reîmprospătează, selectați **Gestiune certificate** pentru a afișa o listă de operații.
5. Din lista de operații, selectați **Importare certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular din această operație ghidată, selectați butonul cu semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

6. Selectați **Alocare certificat** din lista de operații **Gestiune certificate** pentru a afișa o listă de certificate pentru depozitul de certificate curent.

7. Selectați un certificat din listă și faceți clic pe **Alocare la aplicație** pentru a afișa o listă de definiții de aplicații pentru depozitul de certificate.
8. Selectați aplicația dumneavoastră din listă și faceți clic pe **Continuare**. Este afișată o pagină cu un mesaj de confirmare pentru selecția de alocare sau cu un mesaj de eroare dacă a apărut o problemă.

Când terminați această operație, sunteți gata să semnați aplicații și alte obiecte utilizând API-urile i5/OS. Totuși, pentru a vă asigura că dumneavoastră sau alte persoane puteți verifica semnăturile, trebuie să exportați certificatele necesare într-un fișier și să le transferați pe orice sistem care instalează aplicațiile dumneavoastră semnate. Sistemele beneficiarilor trebuie să poată utiliza certificatul pentru verificarea semnăturilor pe aplicația dumneavoastră pe măsură ce aceasta se instalează. Puteți utiliza API-ul Add Verifier ca parte din programul de instalare a aplicației dumneavoastră pentru a face configurarea necesară a verificării de semnături pentru clienții dumneavoastră. De exemplu, puteți crea un program de ieșire de pre-instalare care apelează API-ul Add Verifier pentru a configura sistemul clientului dumneavoastră.

Pasul 5: Exportați certificatele pentru a da posibilitatea verificării semnăturii pe alte sisteme

Semnarea obiectelor necesită ca dumneavoastră și alte persoane să aveți un mijloc de verificare a autenticității semnăturilor și să îl utilizați pentru a determina dacă au fost făcute modificări asupra obiectelor semnate. Pentru verificarea semnăturilor pe același sistem care semnează obiectele, trebuie să utilizați DCM pentru crearea depozitului de certificate *SIGNATUREVERIFICATION. Acest depozit de certificate trebuie să conțină atât o copie a certificatului de semnare a obiectelor, cât și o copie a certificatului CA, pentru Autoritatea de certificare (CA) care a emis certificatul de semnare.

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

Pentru a utiliza DCM astfel încât să puteți verifica semnături pe același sistem care semnează obiectele (Sistem A în acest scenariu), urmați acești pași:

1. În cadrul de navigare, selectați **Creare depozit de certificare nou** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l creați.
2. Selectați **Da** pentru copierea certificatelor existente de semnare a obiectelor în noul depozit de certificate ca certificate de verificare a semnăturilor.
3. Specificați o parolă pentru noul depozit de certificate și faceți clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteți utiliza DCM pentru verificarea semnăturilor pe același sistem pe care îl utilizați 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, urmați acești pași:

1. În cadrul de navigare, selectați **Gestiune certificate**, și apoi selectați operația **Exportare certificate**.
2. Selectați **Semnare obiect** pentru a afișa o listă a certificatelor de semnare a obiectelor pe care le puteți exporta.
3. Selectați certificatul corespunzător de semnare a obiectelor din listă și faceți clic pe **Export**.
4. Selectați **Fișier, ca certificat de verificare a semnăturilor** ca destinație și faceți clic pe **Continuare**.
5. Specificați o cale și un nume de fișier complet determinate pentru certificatul de verificare a semnăturilor exportat și faceți clic pe **Continuare** pentru a exporta certificatul.

Acum puteți adăuga acest fișier la pachetul de instalare a aplicației pe care îl creați pentru produsul dumneavoastră. Utilizând API-ul Add Verifier ca parte din programul dumneavoastră de instalare, puteți adăuga acest certificat în depozitul de certificate *SIGNATUREVERIFICATION a clienților dumneavoastră. API-ul va crea și depozitul de certificate dacă aceasta nu există încă. Programul dumneavoastră de instalare poate apoi verifica semnătura de pe obiectele aplicației dumneavoastră pe măsură ce le restaurează pe sistemele clienților.

Pasul 6: Actualizați programul dumneavoastră de împachetare de aplicații pentru a utiliza API-urile sistemului pentru a vă semna aplicația

Acum că aveți fișierul cu certificatul de verificare a semnăturilor de adăugat la pachetul aplicației dumneavoastră, puteți utiliza API-ul Semnare obiect la scrierea sau editarea unei aplicații existente pentru semnarea bibliotecilor produsului pe măsură ce le împachetați pentru distribuirea către clienți.

Pentru a vă ajuta la mai buna înțelegere a modului de utilizare a API-ului Semnare obiect ca parte din programul dumneavoastră de împachetare a aplicațiilor, revedeți următorul exemplu de cod: Acest cod exemplu, scris în C, nu este un program complet de semnare și împachetare; este mai degrabă un exemplu al porțiunii dintr-un astfel de program care apelează API-ul Semnare obiect. Dacă doriți să utilizați acest exemplu de program, modificați-l pentru a-l adapta nevoilor dumneavoastră specifice. Din motive de securitate, IBM vă recomandă să individualizați exemplul de program, în loc să utilizați valorile implicite furnizate.

Notă: Folosind exemplele de cod, sunteți de acord cu termenii din “Informații de licență și de declinare a responsabilității pentru cod” la pagina 46.

Modificați acest cod pentru a-l adapta nevoilor dumneavoastră utilizând API-ul Semnare obiecte ca parte a unui program de împachetare pentru produsul aplicație al dumneavoastră. Trebuie să transmiteți doi parametrii acestui program: numele bibliotecii de semnat și numele ID-ului aplicației de semnare a obiectelor; ID-ul aplicației este sensibil la majuscule, numele librăriei nu este sensibil la majuscule. Programul pe care îl scrieți poate apela acest cod de mai multe ori dacă sunt utilizate mai multe biblioteci ca părți ale produsului pe care îl semnați.

```
/* ----- */
/* */
/* COPYRIGHT (C) IBM CORP. 2002, 2004 */
/* */
/* Utilizați API-ul Semnare obiect */
/* pentru a semna una sau mai multe biblioteci */
/* */
/* API-ul va semna digital toate obiectele dintr-o bibliotecă */
/* */
/* */
/* */
/* IBM vă acordă o licență copyright neexclusivă pentru a utiliza */
/* toate exemplele de cod de programare din care puteți genera */
/* funcții 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 condițiile. IBM, de aceea, nu poate garanta sau sugera */
/* siguranța, durabilitatea sau funcționarea acestor programe. Toate*/
/* programele conținute aici vă sunt furnizate "AȘA CUM SUNT" */
/* fără nici o garanție de orice fel. */
/* Garanțiile implicate de ne-încălcare, comercializare și adaptare */
/* pentru un anumit scop sunt declinate în mod expres. */
/* */
/* */
/* */
/* Parametrii sunt: */
/* */
/* char * numele bibliotecii de semnat */
/* char * numele ID-ului aplicației */
/* */

#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 aplicației 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 excepții pentru orice eroare */

/* ----- */
/* numelui căii constructului i se dă */
/* numele bibliotecii */
/* ----- */
    memset(libname, '\00', 11); /* inițializare 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 aplicație */
/* ----- */
    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) aplicație */
&applid_length, /* lungime ID aplicație */
"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: Creați un program de ieșire de pre-instalare care utilizează API-ul Add Verifier

Acum că aveți acces programat pentru semnarea aplicațiilor dumneavoastră, puteți utiliza API-ul Add Verifier ca parte a programului dumneavoastră de instalare pentru a crea produsul final pentru distribuire. De exemplu, puteți utiliza API-ul Add Verifier ca parte a unui program de ieșire de pre-instalare pentru a vă asigura că certificatul este adăugat în

depozitul de certificate înainte de a restaura obiectele aplicației semnate. Acest lucru permite programului dumneavoastră de instalare să verifice semnătura de pe obiectele aplicației dumneavoastră pe măsură ce ele sunt restaurate pe sistemul clientului.

Notă: Din motive de securitate, acest API nu vă permite să inserați un certificat CA (Autoritate de certificare) în depozitul de certificate *SIGNATUREVERIFICATION. Când adăugați un certificat CA în depozitul de certificate, sistemul consideră CA o sursă de încredere. În consecință, sistemul tratează certificatul pe care l-a emis CA-ul ca având originea într-o sursă de încredere. De aceea, nu puteți utiliza API-ul pentru crearea unui program de ieșire instalare care să insereze un certificat CA în depozitul de certificate. Trebuie să utilizați Digital Certificate Manager pentru adăugarea unui certificat CA în depozitul de certificate pentru a vă asigura că cineva trebuie să controleze, specific și 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 știință ca de încredere.

Dacă doriți să împiedicați ca oricine să utilizeze acest API pentru a adăuga un certificat de verificare în depozitul dumneavoastră de certificate *SIGNATUREVERIFICATION fără știința dumneavoastră, trebuie să considerați dezactivarea acestui API pe sistemul dumneavoastră. Puteți 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 bună înțelegere a modului de utilizare a API-ului Add Verifier ca parte a programului dumneavoastră de instalare a aplicației, revedeți următorul exemplu de cod program de ieșire preinstalare. Acest cod exemplu, scris în C, nu este un program de ieșire preinstalare complet; este mai degrabă un exemplu al porțiunii dintr-un astfel de program care apelează API-ul Add Verifier. Dacă doriți să utilizați acest exemplu de program, modificați-l pentru a-l adapta nevoilor dumneavoastră specifice. Din motive de securitate, IBM vă recomandă să individualizați exemplul de program, în loc să utilizați valorile implicite furnizate.

Notă: Folosind exemplul de cod, sunteți de acord cu termenii din “Informații de licență și de declinare a responsabilității pentru cod” la pagina 46.

Modificați acest cod pentru a-l adapta nevoilor dumneavoastră pentru folosirea API-ului Add Verifier ca parte a unui program de ieșire de preinstalare pentru a adăuga certificatul de verificare a semnăturii pe sistemul beneficiarului când instalați produsul.

```
/* ----- */
/* */
/* COPYRIGHT (C) IBM CORP. 2002, 2004 */
/* */
/* Utilizați API-ul Adăugare verificare pentru adăugarea unui */
/* fișier din sistemul de fișiere 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 licență copyright neexclusivă pentru a utiliza */
/* toate exemplele de cod de programare din care puteți genera */
/* funcții 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 condițiile. IBM, de aceea, nu poate garanta sau sugera */
/* siguranța, durabilitatea sau funcționarea acestor programe. Toate*/
/* programele conținute aici vă sunt furnizate "AȘA CUM SUNT" */
/* fără nici o garanție de orice fel. */
/* Garanțiile implicate de ne-încălcare, comercializare și adaptare */
/* pentru un anumit scop sunt declinate în mod expres. */
```

```

/*                                                                 */
/*                                                                 */
/*                                                                 */
/* Parametrii sunt:                                             */
/*                                                                 */
/* char *   numele de cale către fișierul din sistemul de fișiere */
/*          integrat care conține 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 excepții 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 operații efectuate, puteți să vă împachetați aplicația și să o trimiteți clienților dumneavoastră. Când aceștia instalează aplicația dumneavoastră, obiectele semnate ale aplicației sunt verificate ca parte a procesului de instalare. La o dată ulterioară, clienții pot utiliza DCM (Digital Certificate Manager) pentru verificarea semnăturii de pe obiectele aplicației dumneavoastră. Acest lucru permite clienților dumneavoastră să determine că sursa aplicației este de încredere și să determine ce modificări s-au produs din momentul în care ați semnat aplicația.

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 sfătuiți 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: Puneți clienții să reseteze parola implicită pentru depozitul de certificate *SIGNATUREVERIFICATION

S-ar putea ca API-ul Add Verifier să fi creat depozitul de certificate *SIGNATUREVERIFICATION ca parte a procesului de instalare a produsului pe sistemul clientului (beneficiarului) dumneavoastră. Dacă API-ul a creat depozitul de certificate, a creat o parolă implicită pentru acesta. Ca urmare, trebuie să vă sfătuiți clienții că trebuie să utilizeze DCM pentru a reseta această parolă pentru a proteja depozitul de certificate de accesul neautorizat.

Sfătuiți clienții dumneavoastră să efectueze acești pași pentru a reseta parola depozitului de certificate *SIGNATUREVERIFICATION:

1. Porniți DCM.
2. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l deschideți.
3. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular din această operație ghidată, selectați butonul cu semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

4. Specificați o nouă parolă pentru depozit, introduceți-o din nou pentru confirmare, selectați polița de expirare a parolei pentru depozitul de certificate și faceți clic pe **Continuare**.

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

Acest scenariu descrie o companie care dorește să semneze obiecte pe care le împachetează și le distribuie mai multor sisteme. Pe baza nevoilor de afaceri și a scopurilor de securitate ale companiei, acest scenariu descrie modul de utilizare a funcției Administrare centrală a Navigatorului iSeries pentru împachetarea și semnarea obiectelor pe care le distribuie altor sisteme.

Situație

Compania dumneavoastră (MyCo, Inc.) dezvoltă aplicații pe care le distribuie mai multor sisteme în mai multe locații din cadrul companiei. Ca administrator de rețea, dumneavoastră sunteți responsabil pentru a asigura faptul că aceste aplicații sunt instalate și actualizate pe toate serverele companiei. Utilizați curent funcția Administrare centrală a Navigatorului iSeries pentru a împacheta și distribui mai ușor aceste aplicații și pentru a efectua alte operații de administrare pentru care sunteți responsabil. Totuși, depistarea și corectarea problemelor cu aceste aplicații durează mai mult timp decât ați dori, din cauza modificărilor neautorizate făcute asupra obiectelor. În consecință, doriți să asigurați mai bine integritatea acestor obiecte prin semnarea lor digitală.

Ați cercetat capacitățile de semnare a obiectelor ale i5/OS și ați aflat că, începând cu V5R2, Administrarea centrală vă permite să semnați obiecte atunci când le împachetați și le distribuiți. Utilizând Administrarea centrală puteți îndeplini eficient și relativ ușor scopurile de securitate ale companiei dumneavoastră. Vă decideți de asemenea să creați o Autoritate de certificare (CA) locală și să o utilizați 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 cumpărați un certificat de la o CA publică bine cunoscută.

Acest exemplu servește ca o introducere utilă în pașii implicați în configurarea și utilizarea semnării obiectelor pentru aplicații pe care le distribuiți mai multor sisteme ale companiei.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Utilizarea Administrării centrale pentru împachetarea și semnarea obiectelor reduce durata de timp pe care trebuie să o petreceți pentru distribuirea obiectelor semnate către serverele companiei dumneavoastră.

- Utilizarea Administrării centrale pentru semnarea obiectelor reduce numărul de pași pe care trebuie să îi efectuați pentru semnarea obiectelor deoarece procesul de semnare face parte din procesul de împachetare.
- Semnarea unui pachet de obiecte vă permite să determinați mai ușor dacă obiectele au fost modificate după ce au fost semnate. Acest lucru poate reduce unele depanări pe care le veți face în viitor pentru depistarea problemelor aplicațiilor.
- Utilizarea unui certificat emis de o Autoritate de certificare (CA) locală pentru semnarea obiectelor face ca semnarea obiectelor să fie mai puțin costisitoare de implementat.

Obiective

În acest scenariu, MyCo, Inc. dorește să semneze digital aplicațiile pe care le distribuie mai multor sisteme în cadrul companiei. Ca administrator de rețea la MyCo, Inc, utilizați deja Administrarea centrală pentru un număr de task-uri de administrare. În consecință, doriți să extindeți utilizarea curentă a Administrării centrale pentru semnarea aplicațiilor companiei pe care le distribuiți altor sisteme.

Obiectivele acestui scenariu sunt după cum urmează:

- Aplicațiile companiei trebuie să fie semnate cu un certificat emis de o CA locală pentru a limita costurile semnării aplicațiilor.
- Administratorii de sistem și alți utilizatori desemnați trebuie să poată verifica cu ușurință semnăturile digitale de pe toate serverele pentru a verifica sursa și autenticitatea obiectelor semnate de companie. Pentru a realiza acest lucru, fiecare server trebuie să aibă o copie atât a certificatului de verificare a semnăturii al companiei, cât și a certificatului Autorității de certificare (CA) locală în fiecare depozit *SIGNATUREVERIFICATION a serverelor.
- Verificarea semnăturilor pe aplicațiile companiei permite administratorilor și altor persoane să detecteze dacă conținutul obiectelor s-a modificat din momentul în care acestea au fost semnate.
- Administratorii trebuie să poată utiliza Administrarea centrală pentru împachetarea, semnarea și distribuția aplicațiilor către sistemele lor.

Detalii

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

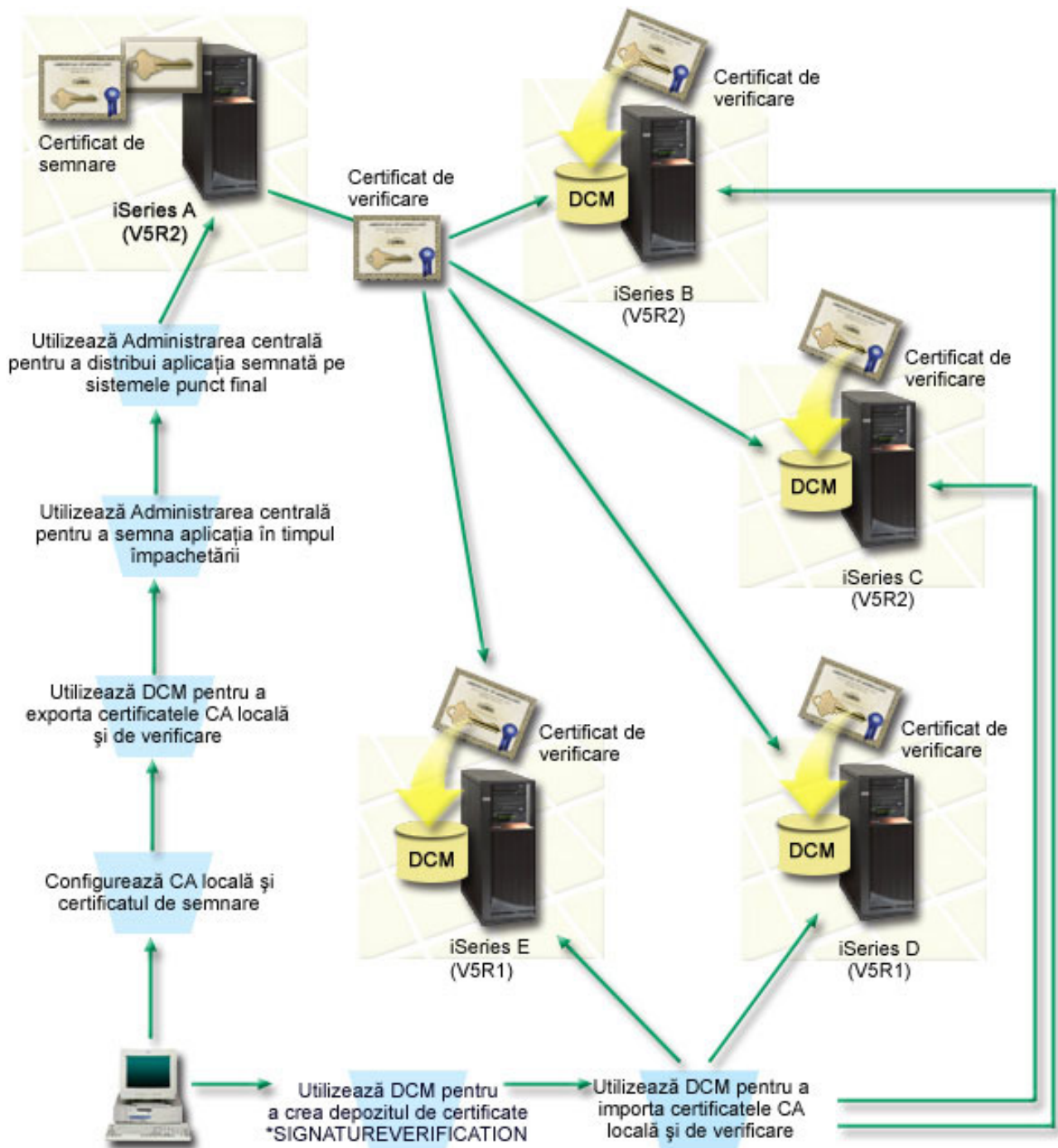


Figura ilustrează următoarele puncte relevante pentru acest scenariu:

Sistemul central (Sistem A)

- Sistemul A rulează i5/OS Versiune 5 Ediție 2 (V5R2).
- Sistemul A servește ca sistem central din care rulează funcțiile Administrării centrale, incluzând aplicațiile de împachetare și distribuire ale companiei.
- Sistemul A are instalat un Cryptographic Access Provider 128-bit (Furnizor de acces criptografic pe 128 de biți) pentru iSeries (5722-AC3).

- Sistemul A are instalat și configurat DCM (Digital Certificate Manager) (i5/OS opțiunea 34) și IBM HTTP Server (5722–DG1).
- Sistemul A se comportă ca Autoritatea de certificare (CA) locală și certificatul de semnare a obiectelor se află pe acest sistem.
- Sistemul A este sistemul primar de semnare a obiectelor pentru aplicațiile companiei. Semnarea obiectelor produsului pentru distribuirea către client este realizată pe Sistem A prin efectuarea acestor operații:
 1. Utilizarea DCM pentru crearea unei CA locale și utilizarea CA locală pentru crearea unui certificat de semnare a obiectelor.
 2. Utilizarea DCM pentru a exporta o copie a certificatului CA locală și a certificatului pentru verificarea semnăturii într-un fișier pentru ca sistemele punct final (Sistem B, C, D, și E) să poată verifica obiectele semnate.
 3. Utilizarea Administrării centrale pentru semnarea obiectelor aplicațiilor și împachetarea lor cu fișierele certificate de verificare.
 4. Utilizarea Administrării centrale pentru distribuirea aplicațiilor semnate și a fișierelor certificate către sistemele punct final.

Sistemele punct final (Sistemele B, C, D și E)

- Sistemele B și C rulează i5/OS Versiune 5 Ediție 2 (V5R2).
- Sistemele D și E rulează i5/OS Versiune 5 Ediție 1 (V5R1).
- Sistemele B, C, D și E au instalat și configurat Digital Certificate Manager (opțiune 34) și IBM HTTP Server (5722–DG1).
- Sistemele B, C, D și E primesc câte o copie a certificatului pentru verificarea semnăturii și al CA local ale companiei de la sistemul central (Sistem A) atunci când sistemele primesc aplicația semnată.
- DCM este utilizat pentru crearea depozitului de certificate *SIGNATUREVERIFICATION și pentru importarea CA locală și a certificatelor de verificare în acest depozit de certificate.

Cerințe preliminare și presupuneri

Acest scenariu depinde de următoarele cerințe preliminare și supoziții:

1. Toate sistemele îndeplinesc cerințele preliminare pentru instalarea și utilizarea DCM.
2. Nimeni nu a configurat sau utilizat anterior DCM pe oricare din sisteme.
3. Sistemul A îndeplinește cerințele pentru instalarea și utilizarea Navigatorului iSeries și a Administrării centrale.
4. Serverul Administrării centrale trebuie să ruleze pe toate sistemele punct final.
5. Toate sistemele au instalat cel mai înalt nivel al programului licențiat Cryptographic Access Provider 128-bit (5722-AC3).
6. Setarea implicită pentru variabila de sistem de verificare a semnăturilor în timpul restaurării (QVIFYOBJRST) pe toate sistemele din scenariu este 3 și nu a fost modificată de la această setare. Setarea implicită asigură că serverul poate verifica semnăturile obiectelor pe măsură ce restaurați obiectele semnate.
7. Administratorul de rețea pentru Sistem A trebuie să aibă autorizarea specială *ALLOBJ pentru profilul utilizator pentru a semna obiecte, sau profilul utilizator trebuie să fie autorizat pentru aplicația de semnare a obiectelor.
8. Administratorul de rețea sau oricine creează un depozit de certificate în DCM trebuie să aibă autorizările speciale *SECADM și *ALLOBJ pentru profilul utilizator.
9. Administratorii de sistem sau alții de pe celelalte sisteme trebuie să aibă autorizarea specială *AUDIT pentru profilul utilizator pentru verificarea semnăturilor obiectelor.

Pașii operației de configurare

Există două seturi de operații pe care trebuie să le efectuați pentru a implementa acest scenariu: Un set de task-uri vă permite să setați Sistemul A pentru utilizarea Administrării centrale la semnarea și distribuirea aplicațiilor. Celălalt set de operații permite administratorilor de sistem și altor persoane să verifice semnăturile de pe aceste aplicații pe toate celelalte servere. Vedeți subiectul cu detaliile scenariului pentru pașii pentru efectuarea acestor task-uri.

Pașii task-ului pentru semnarea obiectelor

Pentru a semna obiectele așa cum se descrie în acest scenariu, vedeți subiectul cu detaliile scenariului de mai jos, pentru pașii de efectuat pe Sistem A pentru fiecare din următoarele task-uri:

1. Efectuați toți pașii preliminari pentru a instala și configura toate produsele iSeries necesare
2. Utilizați DCM pentru a crea o Autoritate de certificare locală (CA) pentru a emite un certificat pentru semnarea privată a obiectelor.
3. Utilizați DCM pentru a crea o definiție de aplicație.
4. Utilizați DCM pentru a atribui un certificat pentru definiția de aplicație pentru semnarea obiectelor
5. Folosiți DCM pentru a exporta certificatele pe care celelalte sisteme trebuie să le folosească pentru verificarea semnăturilor obiectelor. Trebuie să exportați într-un fișier atât o copie a certificatului CA locală, cât și o copie a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor.
6. Transferați fișierele certificat pe fiecare sistem punct final pe care intenționați să verificați semnăturile.
7. Utilizați Administrarea centrală a Navigatorului iSeries pentru a semna obiectele aplicației

Pașii operației de configurare

Trebuie să efectuați aceste operații de configurare verificare semnătură pe fiecare sistem punct final înainte de a utiliza Administrarea centrală pentru a transfera obiectele aplicației semnate pe acestea. Configurația verificării semnăturilor trebuie să fie completă înainte ca să puteți verifica semnăturile cu succes, pe măsură ce restaurați obiectele semnate pe sisteme punct final.

Pe fiecare sistem punct final trebuie să efectuați aceste task-uri pentru verificarea semnăturilor pe obiecte așa cum descrie acest scenariu:

1. Utilizați DCM pentru a crea depozitul de certificate *SIGNATUREVERIFICATION
2. Utilizați DCM pentru a importa certificatul CA local și certificatul pentru verificarea semnăturii

Informații înrudite

DCM (Digital Certificate Manager)

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

Efectuați următorii pași de operație pentru configurarea Administrării centrale pentru semnarea obiectelor așa cum descrie acest scenariu.

Pasul 1: Efectuați toți pașii preliminari

Trebuie să efectuați toate operațiile preliminare pentru instalarea și configurarea tuturor produselor iSeries necesare înainte de a putea realiza operațiile de configurare specifice pentru implementarea acestui scenariu.

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

Când utilizați DCM (Digital Certificate Manager) pentru crearea unei Autorizări de certificare (CA) locală, procesul vă cere să completați o serie de formulare. Aceste formulare vă ghidează prin procesul de creare a CA și de efectuare a altor operații necesare pentru începerea utilizării certificatelor digitale pentru SSL (Secure Sockets Layer), semnarea obiectelor și verificarea semnăturilor. Deși în acest scenariu nu trebuie să configurați certificate pentru SSL, trebuie să completați toate formularele din task-ul de configurare a sistemului pentru semnarea obiectelor.

Pentru a utiliza DCM la crearea și operarea unei CA locale, urmați acești pași: Acum că ați creat o CA locală și un certificat de semnare a obiectelor, trebuie să definiți o aplicație de semnare a obiectelor care să utilizeze certificatul înainte de a putea semna obiecte.

1. Porniți DCM.

2. În cadrul de navigare al DCM, selectați **Crearea unei Autorități de certificare (CA)** pentru a afișa o serie de formulare.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular din această operație ghidată, selectați butonul cu semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

3. Completați toate formularele pentru acest task ghidat. Pe măsură ce efectuați acest task, trebuie să faceți următoarele:
 - a. Să furnizați informații de identificare pentru CA locală.
 - b. Să instalați certificatul CA locală în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaște CA locală și să poată valida certificatele pe care CA locală le emite.
 - c. Să specificați datele de poliță pentru CA dumneavoastră locală.
 - d. Să utilizați noua CA locală pentru a emite un certificat server sau client pe care aplicațiile dumneavoastră să îl poată utiliza pentru conexiuni SSL.

Notă: Deși acest scenariu nu utilizează acest certificat, trebuie să îl creați înainte de a putea utiliza CA locală pentru emiterea certificatului de semnare a obiectelor de care aveți nevoie. Dacă anulați operația fără a crea acest certificat, trebuie să vă creați certificatul de semnare a obiectelor și depozitul de certificate *OBJECTSIGNING în care este memorat separat.

- e. Să selectați aplicațiile care pot utiliza certificatul server sau client pentru conexiuni SSL.

Notă: Pentru scopurile acestui scenariu, nu selectați nici o aplicație și faceți clic pe **Continuare** pentru a afișa următorul formular.

- f. Utilizați noua CA locală pentru emiterea unui certificat de semnare a obiectelor pe care aplicațiile îl pot utiliza pentru semnarea digitală a obiectelor. Acest subtask creează depozitul de certificate *OBJECTSIGNING. Acesta este depozitul de certificate pe care îl utilizați pentru gestionarea certificatelor de semnare a obiectelor.
- g. Selectați aplicațiile care vor avea încredere în CA locală.

Notă: Pentru scopurile acestui scenariu, nu selectați nici o aplicație și faceți clic pe **Continuare** pentru a termina operația.

Pasul 3: Creați o definiție de aplicație pentru semnarea obiectelor

După ce vă creați certificatul de semnare a obiectelor, trebuie să utilizați DCM (Digital Certificate Manager) pentru definirea unei aplicații de semnare a obiectelor pe care să o utilizați pentru semnarea obiectelor. Definiția de aplicație nu trebuie să se refere la o aplicație reală; definiția de aplicație pe care o creați poate descrie tipul sau grupul de obiecte pe care intenționați să le semnați. Aveți nevoie de definiție pentru a putea avea un ID de aplicație asociat cu certificatul pentru activarea procesului de semnare.

Pentru a utiliza DCM la crearea unei definiții a aplicației de semnare a obiectelor, urmați acești pași:

1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați *OBJECTSIGNING ca depozit de certificate pe care să-l deschideți.
2. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.
3. În cadrul de navigare, selectați **Gestiune aplicații** pentru a afișa o listă de operații.
4. Selectați **Adăugare aplicație** din lista de operații pentru afișarea unui formular pentru definirea aplicației.
5. Completați formularul și faceți clic pe **Adăugare**.

Acum trebuie să alocați certificatul dumneavoastră de semnare a obiectelor aplicației pe care ați creat-o.

Pasul 4: Alocați un certificat definiției aplicației de semnare a obiectelor

Pentru a alocă certificatul aplicației dumneavoastră de semnare a obiectelor, urmați acești pași:

1. În cadrul de navigare DCM, selectați **Gestiune certificate** pentru a afișa o listă de operații.
2. Din lista de operații, selectați **Alocare certificat** pentru afișarea unei liste de certificate pentru depozitul de certificate curent.
3. Selectați un certificat din listă și faceți clic pe **Alocare la aplicație** pentru a afișa o listă de definiții de aplicații pentru depozitul de certificate.
4. Selectați una sau mai multe aplicații din listă și faceți clic pe **Continuare**. Este afișată o pagină de mesaj pentru a confirma alocarea certificatului sau pentru a oferi informațiile de eroare dacă s-a produs o eroare.

Când terminați această operație, sunteți gata să semnați obiecte utilizând Administrarea centrală când le împachetați și le distribuiți. Totuși, pentru a vă asigura că dumneavoastră sau alte persoane puteți verifica semnăturile, trebuie să exportați certificatele necesare într-un fișier și să le transferați pe toate sistemele punct final. Trebuie de asemenea să efectuați toate operațiile de configurare a verificării semnăturilor pe fiecare sistem punct final înainte de a utiliza Administrarea centrală pentru transferarea obiectelor aplicației semnate pe acestea. Configurația verificării semnăturilor trebuie să fie completă înainte ca să puteți verifica semnăturile cu succes, pe măsură ce restaurați obiectele semnate pe sisteme terminale.

Pasul 5: Exportați certificatele pentru a da posibilitatea verificării semnăturii pe alte sisteme

Semnarea obiectelor pentru protejarea integrității conținutului necesită ca dumneavoastră și alte persoane să aveți un mijloc pentru verificarea autenticității semnăturilor. Pentru verificarea semnăturilor pe același sistem care semnează obiectele, trebuie să utilizați DCM pentru crearea depozitului de certificate *SIGNATUREVERIFICATION. Acest depozit de certificate trebuie să conțină atât o copie a certificatului de semnare a obiectelor, cât și o copie a certificatului CA, pentru Autoritatea de certificare (CA) care a emis certificatul de semnare.

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

Pentru a utiliza DCM astfel încât să puteți verifica semnături pe același sistem care semnează obiectele (Sistem A în acest scenariu), urmați acești pași:

1. În cadrul de navigare, selectați **Creare depozit de certificare nou** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l creați.
2. Selectați **Da** pentru copierea certificatelor existente de semnare a obiectelor în noul depozit de certificate ca certificate de verificare a semnăturilor.
3. Specificați o parolă pentru noul depozit de certificate și faceți clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteți utiliza DCM pentru verificarea semnăturilor pe același sistem pe care îl utilizați pentru semnarea obiectelor.

Pentru a utiliza DCM la exportarea unei copii a certificatului CA locală și a unei copii a certificatului de semnare a obiectelor ca un certificat de verificare a semnăturilor astfel încât să verificați semnăturile obiectelor pe alte sisteme, urmați acești pași:

1. În cadrul de navigare, selectați **Gestiune certificate**, și apoi selectați operația **Exportare certificate**.
2. Selectați **Autoritate de certificare (CA)** și faceți clic pe **Continuare** pentru a afișa o listă a certificatelor CA pe care le puteți exporta.
3. Selectați certificatul CA locală pe care l-ați creat mai devreme din listă și faceți clic pe **Export**.
4. Specificați **Fișier** ca destinație de export și faceți clic pe **Continuare**.
5. Specificați o cale și un nume de fișier complet determinate pentru certificatul CA locală și faceți clic pe **Continuare** pentru a exporta certificatul.

6. Faceți clic pe **OK** pentru a ieși din pagina de confirmare Export. Acum puteți exporta o copie a certificatului de semnare a obiectelor.
7. Re-selectați operația **Exportare certificat**.
8. Selectați **Semnare obiect** pentru a afișa o listă a certificatelor de semnare a obiectelor pe care le puteți exporta.
9. Selectați certificatul corespunzător de semnare a obiectelor din listă și faceți clic pe **Export**.
10. Selectați **Fișier, ca certificat de verificare a semnăturilor** ca destinație și faceți clic pe **Continuare**.
11. Specificați o cale și un nume de fișier complet determinate pentru certificatul de verificare a semnăturilor exportat și faceți clic pe **Continuare** pentru a exporta certificatul.

Acum puteți transfera aceste fișiere pe sistemele punct final pe care intenționați să verificați semnăturile pe care le-ați creat cu certificatul respectiv.

Pasul 6: Transferați fișierele certificat pe sistemele punct final

Trebuie să transferați fișierele certificate pe care le-ați creat pe Sistemul A pe sistemele punct final din acest scenariu înainte de a le putea configura pentru verificarea obiectelor pe care le semnați. Puteți utiliza câteva metode diferite pentru transferarea fișierelor de certificare. De exemplu, puteți utiliza FTP (File Transfer Protocol) sau distribuirea de pachete din Administrare centrală pentru a transfera fișierele.

Pasul 7: Semnați obiectele utilizând Administrarea centrală

Procesul de semnare a obiectelor pentru Administrarea centrală este parte a procesului de distribuire a pachetelor software. Trebuie să efectuați toate task-urile de configurare a verificării semnăturilor pe fiecare sistem punct final înainte de a utiliza Administrarea centrală pentru transferarea obiectelor aplicației semnate pe acestea. Configurația verificării semnăturilor trebuie să fie completă înainte ca să puteți verifica semnăturile cu succes, pe măsură ce restaurați obiectele semnate pe sisteme terminale.

Pentru a semna o aplicație pe care o distribuiți sistemelor punct final așa cum descrie acest scenariu, urmați acești pași:

1. Utilizați Administrarea centrală pentru împachetarea și distribuirea produselor software.
2. Când vă este afișat panoul **Identificare** în vrăjitorul **Definiție produs**, faceți clic pe **Avansat** pentru afișarea panoului **Identificare avansată**.
3. În câmpul **Semnare digitală**, introduceți ID-ul de aplicație pentru aplicația de semnare a obiectelor pe care ați creat-o anterior și să faceți clic pe **OK**.
4. Completați vrăjitorul și continuați procesul pentru împachetarea și distribuirea produselor software cu Administrarea centrală.

Pasul 8: Task-uri de verificare a semnăturii: Crearea depozitului de certificate *SIGNATUREVERIFICATION pe sistemele punct final

Pentru verificarea semnăturilor pe sistemele punct final 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 conțină și o copie a certificatului CA locală.

Pentru crearea depozitului de certificate *SIGNATUREVERIFICATION, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare DCM (Digital Certificate Manager) selectați **Creare depozit de certificate nou** și selectați ***SIGNATUREVERIFICATION** ca depozit de certificate pe care să-l creați.

Notă: Dacă aveți întrebări despre modul de completare a unui anumit formular din acest task ghidat, selectați butonul cu semnul de întrebare (?) din partea de sus a paginii pentru a accesa ajutorul online.

3. Specificați o parolă pentru noul depozit de certificate și faceți clic pe **Continuare** pentru a crea depozitul de certificate. Acum puteți importa certificatele în depozit și le puteți utiliza pentru verificarea semnăturilor.

Pasul 9: Task-uri de verificare a semnăturii: Importarea certificatelor

Pentru a verifica semnătura de pe un obiect, depozitul de certificate *SIGNATUREVERIFICATION trebuie să conțină o copie a certificatului de verificare a semnăturilor. Dacă certificatul de semnare este privat, acest depozit de certificate trebuie să aibă și o copie a certificatului Autorității de certificare (CA) locală care a emis certificatul de semnare. În acest scenariu, ambele certificate erau exportate într-un fișier și acel fișier era transferat pe fiecare sistem punct final.

Pentru a importa aceste certificate în depozitul *SIGNATUREVERIFICATION, urmați acești pași: Puteți verifica semnăturile obiectelor pe care le-ați creat cu certificatul de semnare corespunzător când restaurați obiectele semnate.

1. În cadrul de navigare al DCM, faceți clic pe **Selectare depozit de certificate** și selectați *SIGNATUREVERIFICATION ca depozitul de certificate pe care să-l deschideți.
2. Când se afișează pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat și faceți clic pe **Continuare**.
3. După ce cadrul de navigare se reîmprospătează, selectați **Gestiune certificate** pentru a afișa o listă de operații.
4. Din lista de operații, selectați **Importare certificate**.
5. Selectați **Autoritate de certificare (CA)** ca tipul certificatului și faceți clic pe **Continuare**.

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

6. Specificați calea și numele de fișier complet determinate pentru fișierul de certificare CA și faceți clic pe **Continuare**. Este afișat un mesaj care confirmă că procesul de importare a reușit sau care furnizează un mesaj de eroare dacă procesul a eșuat.
7. Selectați din nou operația **Importare certificat**.
8. Selectați **Verificare semnături** ca tipul de certificat de importat și faceți clic pe **Continuare**.
9. Specificați calea și numele de fișier complet determinate pentru fișierul certificat de verificare a semnăturilor și faceți clic pe **Continuare**. Este afișat un mesaj care confirmă că procesul de importare a reușit sau care furnizează informațiile de eroare dacă procesul a eșuat.

Cerințe preliminare pentru semnarea obiectelor și verificarea semnăturilor

Utilizați aceste informații pentru a afla despre cerințele preliminare de configurare, ca și despre alte considerații de planificare pentru semnarea obiectelor și verificarea semnăturilor.

Capacitățile i5/OS de semnare a obiectelor și de verificare a semnăturilor vă oferă mijloace suplimentare puternice de controlare a obiectelor pe serverul dumneavoastră. Pentru a profita de aceste capacități, trebuie să îndepliniți cerințele preliminare pentru utilizarea lor.

Cerințe preliminare pentru semnarea obiectelor

Există un număr de metode pe care le puteți utiliza pentru semnarea obiectelor, în funcție de nevoile dumneavoastră de afaceri și de securitate:

- Puteți utiliza DCM (Digital Certificate Manager).
- Puteți scrie un program care utilizează API-ul Semnare obiect.
- Puteți utiliza funcțiile de Administrare centrală ale Navigatorului iSeries pentru semnarea obiectelor pe măsură ce le împachetați pentru distribuirea către sistemele punct final.

Metoda pe care o alegeți pentru semnarea obiectelor depinde de nevoile dumneavoastră de afaceri și de securitate. Indiferent de metoda pe care intenționați să o utilizați pentru semnarea obiectelor, trebuie să vă asigurați că sunt îndeplinite anumite condiții preliminare:

- Trebuie să îndepliniți cerințele preliminare pentru instalarea și utilizarea DCM (Digital Certificate Manager).

- Trebuie să utilizați DCM pentru crearea depozitului de certificate *OBJECTSIGNING. Creați acest depozit de certificate ca parte a procesului de creare a Autorității 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 conțină cel puțin un certificat, fie unul pe care l-ați creat utilizând o CA locală, fie unul pe care l-ați obținut de la o CA publică Internet.
- Trebuie să utilizați DCM pentru a crea cel puțin o definiție a aplicației de semnare a obiectelor de utilizat pentru semnarea obiectelor.
- Trebuie să utilizați DCM pentru a alocă un anumit certificat definiției aplicației de semnare a obiectelor.
- Profilul utilizator care semnează obiectele trebuie să aibă autorizarea specială *ALLOBJ. Profilul utilizator care creează depozitul de certificate *SIGNATUREVERIFICATION trebuie să aibă autorizările speciale *SECADM și *ALLOBJ.

Cerințele preliminare pentru verificarea semnăturii

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

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

Metoda pe care o alegeți pentru semnarea obiectelor depinde de nevoile dumneavoastră de afaceri și de securitate. Indiferent de metoda pe care intenționați să o utilizați, trebuie să vă asigurați că sunt îndeplinite anumite condiții preliminare:

- Trebuie să îndepliniți cerințele preliminare pentru instalarea și utilizarea DCM (Digital Certificate Manager).
- Trebuie să creați depozitul de certificate *SIGNATUREVERIFICATION. Puteți crea acest depozit de certificate într-unul din cele două moduri, în funcție de nevoile dumneavoastră. O puteți crea utilizând DCM (Digital Certificate Manager) pentru gestionarea certificatelor de verificare a semnăturilor. Sau, dacă utilizați un certificat public pentru semnarea obiectelor, puteți crea acest depozit de certificate prin scrierea unui program care utilizează API-ul Add Verifier (QYDOADDV).

Notă: API-ul Add Verifier creează depozitul de certificate cu o parolă implicită. Trebuie să utilizați 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 conțină o copie a certificatului care a semnat obiectele. Puteți adăuga acest certificat în depozitul de certificate în două moduri. Puteți utiliza DCM pe sistemul care semnează pentru exportarea certificatului într-un fișier și apoi să utilizați DCM pe sistemul destinație de verificare pentru importarea certificatului în depozitul de certificate *SIGNATUREVERIFICATION. Sau, dacă utilizați un certificat public la semnarea obiectelor, puteți adăuga certificatul la depozitul de certificate a sistemului destinație de verificare prin scrierea unui program care utilizează API-ul Add Verifier.
- depozitul de certificate *SIGNATUREVERIFICATION trebuie să conțină o copie a certificatului CA care a emis certificatul ce a semnat obiectele. Dacă utilizați un certificat public pentru a semna obiecte, depozitul de certificate de pe sistemul de verificare destinație poate avea deja o copie a certificatului CA necesar. Dacă utilizați un certificat emis de o CA locală la semnarea obiectelor, totuși, trebuie să utilizați DCM pentru adăugarea unei copii a certificatului CA locală în depozitul de certificate pe sistemul destinație de verificare.

Notă: Din motive de securitate, API-ul Add Verifier nu vă permite să inserați un certificat Autoritate de certificare (CA) în depozitul de certificate *SIGNATUREVERIFICATION. Când adăugați un certificat CA în depozitul de certificate, sistemul consideră CA o sursă de încredere. În consecință, sistemul tratează certificatul pe care l-a emis Autoritatea de certificare ca fiind originar dintr-o sursă de încredere. De aceea, nu puteți utiliza API-ul pentru crearea unui program de ieșire instalare care să insereze un certificat CA în depozitul de certificate. Trebuie să utilizați DCM (Digital Certificate Manager) pentru adăugarea unui certificat CA în depozitul de certificate pentru a vă asigura că cineva trebuie să controleze, specific și 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 știință ca de încredere.

Dacă utilizați un certificat emis de o CA locală la semnarea obiectelor, trebuie să utilizați DCM pe serverul gazdă CA local pentru exportarea unei copii a certificatului CA local într-un fișier. Puteți utiliza DCM pe serverul destinație de verificare pentru importarea certificatului CA local în depozitul de certificate *SIGNATUREVERIFICATION. Pentru a preveni o posibilă eroare, trebuie să importați certificatul CA locală în acest depozit de certificate înainte de a utiliza API-ul Add Verifier pentru a adăuga certificatul pentru verificarea semnăturii. În consecință, dacă utilizați un certificat emis de o CA locală, vă poate fi mai ușor să utilizați DCM pentru importarea certificatului CA și a certificatului de verificare în depozitul de certificate.

Dacă doriți să împiedicați ca oricine să utilizeze acest API pentru a adăuga un certificat de verificare în depozitul dumneavoastră de certificate *SIGNATUREVERIFICATION fără știința dumneavoastră, trebuie să considerați dezactivarea acestui API pe sistemul dumneavoastră. Puteți face acest lucru utilizând uneltele de servicii sistem (SST) pentru a nu permite modificări asupra variabilelor de sistem legate de securitate.

- Profilul utilizator al sistemului care verifică semnăturile trebuie să aibă autorizarea specială *AUDIT. Profilul utilizator al sistemului care creează depozitul de certificate *SIGNATUREVERIFICATION sau modifică parola pentru acesta trebuie să aibă autorizările speciale *SECADM și *ALLOBJ.

Gestiunea obiectelor semnate

Utilizați aceste informații pentru a afla despre comenzile și variabilele sistem pe care le puteți utiliza ca să lucrați cu obiectele semnate și despre modul în care obiectele semnate afectează procesele de copiere de siguranță și de recuperare.

Începând cu V5R1, IBM a început semnarea programelor licențiate i5/OS și a PTF-urilor ca metodă de marcare oficială a sistemului de operare ca având originea de la IBM și ca mijloc de detectare a modificărilor neautorizate asupra obiectelor sistemului. De asemenea, partenerii de afaceri și alți vânzători pot semna aplicațiile pe care le cumpărați. În consecință, chiar dacă nu semnați dumneavoastră obiecte, trebuie să înțelegeți modul de gestionare a obiectelor semnate și modul în care aceste obiecte semnate afectează operațiile administrative de rutină din sistem.

Obiectele semnate afectează în principal operațiile de copiere de siguranță și de recuperare, mai exact modul în care salvați obiecte și restaurați obiecte pe sistemul dumneavoastră.

Variabile de sistem și comenzi care afectează obiectele semnate

Aflați despre variabilele sistem și comenzile pe care le puteți utiliza pentru gestionarea obiectelor semnate sau care au efect asupra obiectelor semnate atunci când le rulați.

Pentru a gestiona efectiv obiectele semnate, trebuie să înțelegeți modul în care variabilele sistem și comenzile afectează obiectele semnate. Variabila sistem **Verificarea semnăturilor în timpul restaurării** (QVfyOBJRST) determină modul în care diferite comenzi de restaurare afectează obiectele semnate și modul în care sistemul dumneavoastră tratează obiectele semnate în timpul operațiilor de restaurare. Nu există anumite comenzi CL care să fie destinate exclusiv pentru gestionarea obiectelor semnate pe un sistem. Totuși, există un număr de comenzi CL obișnuite pe care le utilizați 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 și astfel anulând protecția 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 i5/OS 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 operațiilor de restaurare. Setarea pe care o utilizați pentru această variabilă sistem, în combinație cu alte două setări ale variabilelor sistem, afectează operațiile de restaurare pentru sistemul

dumneavoastră. În funcție de setarea pe care o selectați pentru această variabilă, ea poate permite sau nu restaurarea obiectelor pe baza stării semnăturii lor. (De exemplu, dacă obiectul este nesemnăat, are o semnătură nevalidă, este semnat de o sursă de încredere și așa 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 definește 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 și tratează obiectul ca și cum ar fi nesemnăat.

Există anumite valori pe care le puteți utiliza pentru variabila sistem QVIFYOBJRST, 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) și modulele (*MODULE). Se aplică de asemenea obiectelor fișier flux (*STMF) care au asociate programe Java create cu comanda Creare program Java (CRTJVAPGM). Nu se aplică pentru fișierele salvare (*SAV) sau fișierelor din sistemul de fișiere integrat.

Valori de sistem care afectează obiectele semnate

Variabila sistem **Verificarea semnăturilor obiectelor în timpul restaurării** (QVIFYOBJRST), membră a categoriei de restaurare a variabilelor sistem i5/OS 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 operațiilor de restaurare. Setarea pe care o utilizați pentru această variabilă sistem, în combinație cu alte două setări ale variabilelor sistem, afectează operațiile de restaurare pentru sistemul dumneavoastră. În funcție de setarea pe care o selectați pentru această variabilă, ea poate permite sau nu restaurarea obiectelor pe baza stării semnăturii lor. (De exemplu, dacă obiectul este nesemnăat, are o semnătură nevalidă, este semnat de o sursă de încredere și așa 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 definește 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 și tratează obiectul ca și cum ar fi nesemnăat.

Există anumite valori pe care le puteți utiliza pentru variabila sistem QVIFYOBJRST, 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) și modulele (*MODULE). Se aplică de asemenea obiectelor fișier flux (*STMF) care au asociate programe Java create cu comanda Creare program Java (CRTJVAPGM). Nu se aplică pentru fișierele salvare (*SAV) sau fișierelor din sistemul de fișiere integrat.

Comenzi CL care afectează obiectele semnate

Există mai multe comenzi CL care vă permit să gestionați obiectele semnate sau care afectează obiectele semnate de pe sistemul dumneavoastră. Puteți utiliza o varietate de comenzi pentru vizualizarea informațiilor de semnătură pentru obiecte, verificarea semnăturii de pe obiecte și salvarea și restaurarea obiectelor necesare pentru verificarea semnăturilor. În plus, există un grup de comenzi care, atunci când rulează, pot înlătura semnăturile de pe obiecte și anula protecția pe care semnăturile o oferă.

Comenzi pentru vizualizarea informațiilor de semnătură pentru un obiect

- Comanda de afișare a descrierii obiectului (DSPOBJD). Această comandă afișează numele și atributele obiectelor specificate din biblioteca specificată sau din bibliotecile din lista de biblioteci a firului de execuție. Puteți utiliza această comandă pentru a determina dacă un obiect este semnat și pentru a vizualiza informații despre semnătură.
- Comenzile sistem de fișiere integrat Afișare legături obiect (DSPLNK) și Gestiune legături obiect (WRKLNK). Puteți utiliza oricare dintre aceste comenzi pentru a afișa informațiile de semnătură pentru un obiect din sistemul de fișiere integrat.

Comenzi pentru verificarea semnăturilor obiectelor

- Comanda Check Object Integrity - Verificarea integrității obiectului (CHKOBJITG). Această comandă vă permite să determinați dacă obiectele de pe sistemul dumneavoastră au încălcări de integritate. Puteți utiliza această comandă pentru verificarea semnăturilor într-un mod asemănător cu cel în care utilizați un antivirus pentru a determina dacă un virus a corupt fișiere sau alte obiecte de pe sistemul dumneavoastră. Pentru a afla mai multe despre utilizarea acestei comenzi cu obiecte semnate și obiecte care se pot semna, consultați Comenzi de verificare a codurilor pentru asigurarea integrității semnăturilor.
- Comanda CHKPRDOPT (Check Product Option - Verificare opțiuni produs). Această comandă raportează diferențele dintre structura corectă și structura curentă a unui produs software. De exemplu, comanda raportează o eroare dacă un obiect este șters dintr-un produs instalat. Puteți utiliza parametrul CHKSIG pentru a specifica cum să trateze și să raporteze comanda problemele de semnătură posibile pentru produs. Pentru a afla mai multe despre utilizarea acestei comenzi cu obiecte semnate și obiecte care se pot semna, consultați Comenzi de verificare a codurilor pentru asigurarea integrității semnăturilor.
- Comanda SAVLICPGM (Save Licensed Program - Salvare program licențiat). Această comandă salvează o copie a obiectelor care alcătuiesc un program licențiat. Aceasta salvează programul licențiat într-o formă care poate fi restaurată prin comanda RSTLICPGM (Restore Licensed Program - Restaurare program licențiat). Puteți utiliza parametrul CHKSIG pentru a specifica cum să trateze și să raporteze comanda problemele de semnătură posibile pentru produs. Pentru a afla mai multe despre utilizarea acestei comenzi cu obiecte semnate și obiecte care se pot semna, consultați Comenzi de verificare a codurilor pentru asigurarea integrității semnăturilor.
- Comanda RST (Restore - Restaurare). Această comandă restaurează o copie a unui sau mai multor obiecte care pot fi utilizate în sistemul de fișiere integrat. Această comandă vă permite de asemenea să restaurați depozitele de certificate și conținutul lor pe sistem. Totuși, nu puteți utiliza această comandă pentru restaurarea depozitului de certificate *SIGNATUREVERIFICATION. Modul în care comanda de restaurare tratează obiectele semnate și obiectele care se pot semna este determinată de setarea pentru variabila sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVfyOBRST).
- Comanda RSTLIB (Restore Library - Restaurare bibliotecă). Această comandă restaurează o bibliotecă sau un grup de biblioteci care a fost salvat de comanda SAVLIB (Save Library - Salvare bibliotecă). Comanda RSTLIB restaurează întreaga bibliotecă, care include descrierea bibliotecii, descrierile obiectelor și conținutul obiectelor din bibliotecă. Modul în care această comandă tratează obiectele semnate și obiectele care se pot semna este determinat de setarea variabilei sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVfyOBRST).
- Comanda RSTLICPGM (Restore Licensed Program - Restaurare program licențiat). Această comandă încarcă sau restaurează un program licențiat, fie pentru instalarea inițială, fie pentru instalarea unei noi ediții. Modul în care această comandă tratează obiectele semnate și obiectele care se pot semna este determinat de setarea variabilei sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVfyOBRST).
- Comanda RSTOBJ (Restore object - Restaurare obiect). Această comandă restaurează unul sau mai multe obiecte dintr-o singură bibliotecă, ce au fost salvate pe dischetă, bandă, volum optic sau într-un fișier prin utilizarea unei singure comenzi. Modul în care această comandă tratează obiectele semnate și obiectele care se pot semna este determinat de setarea variabilei sistem Verificarea semnăturilor obiectelor în timpul restaurării (QVfyOBRST).

Comenzi pentru salvarea și restaurarea depozitelor de certificate

- Comanda SAV (Save - Salvare). Această comandă vă permite să salvați o copie a unui sau mai multor obiecte care poate fi utilizată în sistemul de fișiere integrat, incluzând depozitele de certificate. Totuși, nu puteți utiliza această comandă pentru salvarea depozitului de certificate *SIGNATUREVERIFICATION.
- Comanda SAVSECDTA (Save Security Data - Salvare date de securitate). Această comandă vă permite să salvați toate informațiile de securitate fără a solicita sistemului să fie într-o stare restricționată. Utilizarea acestei comenzi vă permite să salvați depozitul de certificate *SIGNATUREVERIFICATION și certificatele pe care le conține. Această comandă nu salvează nici un alt depozit de certificare.
- Comanda SAVSYS (Save System - Salvare sistem). Această comandă vă permite să salvați o copie a codului intern licențiat și a bibliotecii QSYS într-un format compatibil cu instalarea sistemului. Aceasta nu salvează obiecte din nici o altă bibliotecă. În plus, vă permite să salvați obiectele de securitate și de configurare pe care le puteți de asemenea salva utilizând comenzile SAVECDTA și SAVCFG. Utilizarea acestei comenzi vă permite să salvați depozitul de certificate *SIGNATUREVERIFICATION și certificatele pe care le conține.

- Comanda RST (Restore - Restaurare). Această comandă vă permite să restaurați depozitele de certificate și conținutul lor pe sistem. Totuși, nu puteți utiliza această comandă pentru restaurarea depozitului de certificate *SIGNATUREVERIFICATION.
- Comanda RSTUSRPRF (Restore User Profiles - Restaurare profiluri utilizator). Această comandă vă permite să restaurați părțile 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). Puteți utiliza această comandă pentru restaurarea depozitului de certificate *SIGNATUREVERIFICATION și a parolei ascunse pentru acesta și pentru toate celelalte depozite de certificate. Puteți restaura depozitul de certificate *SIGNATUREVERIFICATION fără restaurarea informațiilor de profil utilizator specificând *DCM ca valoare pentru parametrul SECDTA și *NONE pentru parametrul USRPRF. Pentru utilizarea acestei comenzi la restaurarea informațiilor de profil utilizator și a depozitelor de certificate și a parolelor acestora, specificați *ALL pentru parametrul USRPRF.

Comenzi care pot înlătura sau pierde semnături de pe obiecte

Atunci când utilizați comenzile următoare pe un obiect semnat, o puteți 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 veți mai putea verifica sursa obiectului dacă este de încredere și nu veți mai putea verifica semnătura pentru detectarea modificărilor aduse obiectului. Utilizați aceste comenzi doar pe acele obiecte semnate pe care le-ați creat (opus obiectelor semnate pe care le obțineți de la alții ca IBM sau vânzători). Dacă sunteți îngrijorat că o comandă a înlăturat sau a pierdut semnătura unui obiect, puteți utiliza comanda DSPOBJD (Display Object Description - Afișare descriere obiect) pentru a vedea dacă semnătura mai este acolo și să semnați din nou obiectul dacă este necesar.

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

- Comanda CHGPGM (Change Program - Modificare program). Această comandă modifică atributele unui program fără a cere recompilarea lui. De asemenea, puteți utiliza această comandă pentru a forța recrearea unui program chiar dacă atributele specificate sunt la fel ca atributele curente.
- Comanda CHGSRVPGM (Change Service Program - Modificare program de service). Această comandă modifică atributele unui program de serviciu fără a cere recompilarea lui. De asemenea, puteți utiliza această comandă pentru a forța recrearea unui program de serviciu chiar dacă atributele specificate sunt la fel ca atributele curente.
- Comanda CLRSVAVF (Clear Save File - Curățare fișier de salvare). Această comandă curăță conținutul unui fișier de salvare; ea curăță toate înregistrările existente din fișierul de salvare și reduce spațiul de stocare pe care îl utilizează fișierul.
- Comanda SAV (Save - Salvare). Această comandă salvează o copie a unuia sau mai multor obiecte care poate fi utilizată în sistemul de fișiere integrat. - Atunci când utilizați această comandă, puteți pierde semnătura din obiectele comandă (*CMD) de pe mediul de salvare dacă specificați o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu pot fi semnate în edițiile anterioare V5R2.
- Comanda SAVLIB (Save Library - Salvare bibliotecă). Această comandă vă permite să salvați o copie a uneia sau mai multor biblioteci. Atunci când utilizați această comandă, puteți pierde semnătura din obiectele comandă (*CMD) de pe mediul de salvare dacă specificați o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu pot fi semnate în ediții anterioare V5R2.
- Comanda SAVOBJ (Save Object - Salvare obiect). Această comandă salvează o copie a unui singur obiect sau a unui grup de obiecte localizate în aceeași bibliotecă. Atunci când utilizați această comandă, puteți pierde semnătura din obiectele comandă (*CMD) de pe mediul de salvare dacă specificați o valoare anterioară V5R2M0 pentru parametrul TGTRLS. Pierderea semnăturii se produce deoarece obiectele comandă nu pot fi semnate în ediții anterioare V5R2.

Concepte înrudite

“Considerații de salvare și restaurare pentru obiectele semnate” la pagina 40

Aflați despre modul în care obiectele semnate afectează realizarea operațiilor de salvare și restaurare pentru sistemul dumneavoastră.

Informații înrudite

Considerații de salvare și restaurare pentru obiectele semnate

Aflați despre modul în care obiectele semnate afectează realizarea operațiilor de salvare și restaurare pentru sistemul dumneavoastră.

Există anumite variabile sistem care pot afecta operațiile de restaurare pentru sistemul dumneavoastră. Doar una dintre aceste valori de sistem, valoarea de sistem **verificare semnături obiecte la restaurare (QVfyOBRST)**, determină cum tratează sistemul obiectele semnate la restaurarea acestora. Setarea pe care o alegeți pentru această variabilă sistem vă permite să determinați modul în care procesul de restaurare tratează verificarea obiectelor fără semnături sau cu semnături care nu sunt valide.

Unele comenzi de salvare și restaurare afectează obiectele semnate sau determină modul în care sistemul dumneavoastră tratează obiectele semnate și nesemnate în timpul operațiilor de salvare și restaurare. Trebuie să cunoașteți aceste comenzi și efectul acestora asupra obiectelor semnate pentru a vă gestiona mai bine sistemul și pentru a evita eventualele probleme care pot să apară.

Aceste comenzi pot verifica semnăturile pe obiecte în timpul operațiilor de salvare și restaurare:

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

Aceste comenzi vă permit să salvați și să restaurați depozite de certificate; depozitele de certificate sunt obiecte sensibile la securitate care conțin certificatele pe care le utilizați pentru semnarea obiectelor și verificarea semnăturilor:

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

Unele comenzi de salvare, în funcție de valorile parametrilor pe care le utilizați, pot pierde semnătura unui obiect de pe suportul magnetic de salvare, anulând astfel securitatea pe care semnătura o oferă. De exemplu, *orice* operație de salvare care se referă la un obiect comandă (*CMD) cu o ediție destinație anterioară V5R2M0 are ca efect salvarea comenzilor fără semnături. Înlăturarea semnăturii poate cauza probleme cu obiectele afectate. În cel mai bun caz, nu veți mai putea verifica sursa obiectului dacă este de încredere și nu veți mai putea verifica semnătura pentru detectarea modificărilor aduse obiectului. Utilizați aceste comenzi doar pe acele obiecte semnate pe care le-ați creat (opus obiectelor semnate pe care le obțineți de la alții ca IBM sau vânzători).

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

Trebuie să cunoașteți această posibilitate pentru următoarele comenzi de salvare specifice, cât și pentru comenzile de salvare în general:

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

Concepte înrudite

“Variabile de sistem și comenzi care afectează obiectele semnate” la pagina 36

Aflați despre variabilele sistem și comenzile pe care le puteți utiliza pentru gestionarea obiectelor semnate sau care au efect asupra obiectelor semnate atunci când le rulați.

Comenzi de verificare a codurilor pentru asigurare integrității semnăturilor

Învățați despre utilizarea comenzilor pentru a verifica semnăturile obiectului pentru a determina integritatea obiectului.

Puteți utiliza DCM (Digital Certificate Manager) sau API-urile pentru verificarea semnăturilor de pe obiecte. Puteți de asemenea să utilizați câteva comenzi pentru verificarea semnăturilor. Utilizarea acestor comenzi vă permite să verificați semnături într-un mod asemănător cu cel în care utilizați un antivirus pentru a determina dacă un virus a corupt fișiere 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.

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

Comanda de verificare integritate obiect (CHKOBJITG)

Comanda CHKOBJITG (Check Object Integrity - Verificare integritate obiect) vă permite să determinați dacă obiectele de pe sistemul dumneavoastră au încălcări de integritate. Puteți utiliza această comandă pentru verificarea încălcărilor de integritate pentru obiecte deținute 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 condiții:

- 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 și 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 comparații între rezumatul matematic cifrat care este creat când obiectul este semnat și 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, conținutul obiectului a fost modificat după semnarea lui și semnătura este considerată nevalidă.
- Un obiect are un atribut de domeniu incorect pentru tipul de obiect.

Dacă comanda detectează o încălcare a integrității pentru un obiect, adaugă numele obiectului, numele bibliotecii (sau numele de cale), tipul obiectului, proprietarul obiectului și tipul eșecului într-un fișier istoric bază de date. Comanda creează o intrare în istoric și în alte câteva cazuri, deși 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 și 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. Puteți specifica una din trei valori pentru acest parametru:

- *SIGNED - Când specificați 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 specificați 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 și pentru orice obiect cu o semnătură nevalidă.
- *NONE - Când specificați această valoare, comanda nu verifică semnăturile digitale de pe obiecte.

Comanda de verificare opțiune produs (CHKPRDOPT)

Comanda CHKPRDOPT (Check Product Option - Verificare opțiuni produs) raportează diferențele dintre structura corectă și structura reală a unui produs software. De exemplu, comanda raportează o eroare dacă un obiect este șters dintr-un produs instalat.

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

- *SIGNED - Când specificați 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 și identifică produsul ca fiind într-o stare eronată. Aceasta este valoarea implicită.
- *ALL - Când specificați această valoare, comanda verifică toate obiectele care se pot semna pentru a determina dacă au o semnătură și verifică semnătura pe aceste obiecte. Comanda trimite un mesaj în istoricul jobului pentru orice obiect care se poate semna dar nu are o semnătură; totuși, 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 și consideră produsul eronat.
- *NONE - Când specificați această valoare, comanda nu verifică semnăturile digitale pe obiectele produsului.

Comanda SAVLICPGM (Save Licensed Program - Salvare program cu licență)

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

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

- *SIGNED - Când specificați 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 și salvarea va eșua. Aceasta este valoarea implicită.
- *ALL - Când specificați această valoare, comanda verifică toate obiectele care se pot semna pentru a determina dacă au o semnătură și 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; totuși, procesul de salvare nu se termină. Dacă comanda determină că semnătura de pe un obiect nu este validă, trimite un mesaj în istoricul jobului și salvarea va eșua.
- *NONE - Când specificați această valoare, comanda nu verifică semnăturile digitale pe obiectele produsului.

Verificarea integrității funcției de verificare cod

Aflați cum să verificați integritatea funcției de verificare cod pe care o folosiți la verificarea integrității sistemului i5/OS.

Pentru a folosi noua funcție de verificare a integrității verificatorului de cod pe care îl folosiți la verificarea integrității sistemului, trebuie să aveți autorizarea specială *AUDIT.

Pentru a verifica funcția de verificare cod, rulați 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 rulați API-ul acesta verifică obiectele cheie ale sistemului, inclusiv programele și programele serviciu și 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 și 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) și a comenzii Verificare integritate obiect (CHKOBJITG).

4. Utilizează comenzile RSTOBJ și RSTLIB pe un fișier salvare (*SAV) special pentru a se asigura că erorile sunt raportate corect. Lipsa mesajelor de eroare sau un mesaj de eroare greșit indică o eventuală problemă.
5. Creează un obiect comandă (*CMD) care este proiectat să eșueze la verificarea corectă.
6. Rulează comanda CHKOBJITG și API-ul Verificare obiect pe acest obiect comandă special pentru a se asigura că comanda CHKOBJITG și API-ul Verificare obiect raportează corect erorile. Lipsa mesajelor de eroare sau un mesaj de eroare greșit indică o eventuală problemă.

Concepte înrudite

“Funcția de verificare a integrității pentru verificatorul de cod” la pagina 5

Aflați cum puteți verifica integritatea funcției de verificare cod pe care o folosiți la verificarea integrității sistemului.

Referințe înrudite

“Interpretarea mesajelor de eroare la verificarea verificatorului de cod” la pagina 44

Utilizați aceste informații pentru a învăța pentru a învăța ce mesaje sunt returnate de funcția de verificare a integrității verificatorului de cod și cum să utilizați aceste mesaje pentru a vă asigura că funcția de verificare a codului nu este coruptă, cât și soluții posibile dacă mesajele indică faptul că funcția sau obiecte cheie ale sistemului de operare pot fi corupte.

Depanarea obiectelor semnate

Utilizați aceste informații pentru a afla despre comenzile și variabilele sistem pe care le puteți utiliza ca să lucrați cu obiectele semnate și despre modul în care obiectele semnate afectează procesele de copiere de siguranță și de recuperare.

Atunci când semnați obiecte și lucrați cu obiecte semnate, puteți întâlni erori care vă împiedică să vă realizați sarcinile și obiectivele. Multe dintre erorile și problemele comune pe care le puteți întâlni fac parte din aceste categorii:

Diagnosticarea erorilor de semnare obiecte

Utilizați tabelul următor pentru a găsi informații care să vă ajute să diagnosticați unele dintre cele mai întâlnite probleme pe care le puteți întâlni la semnarea obiectelor.

Problemă	Soluție posibilă
Când utilizați API Semnare obiect pentru semnarea unui obiect cu o ediție destinație V4R5 sau anterioară, procesul de semnare eșuează și obiectul nu este semnat (mesaj de eroare CPFB721).	Sistemul nu asigură suport pentru semnarea obiectelor înainte de V5R1. Pentru acele obiecte care întorc un mesaj de eroare CPFB721, trebuie să creați din nou programele respective cu o ediție destinație V5R1 sau mai recentă pentru a le putea semna.

Depanarea erorilor de verificare a semnăturilor

Utilizați tabelul următor pentru a găsi informații care să vă ajute să diagnosticați unele dintre cele mai întâlnite probleme pe care le puteți întâlni la verificarea semnăturilor digitale pentru obiecte.

Problemă	Soluție posibilă
Procesul de restaurare eșuează pentru obiectele fără semnătură.	Dacă lipsa unei semnături nu este o problemă, verificați dacă valoarea de sistem QVfyOjRST este setată pe 5. O valoare 5 specifică faptul că obiectele nesignate nu pot fi restaurate. Modificați valoarea la 3 și încercați din nou restaurarea.

Problemă	Soluție posibilă
Procesul de restaurare eșuează pentru obiectele cu semnătură.	Acest lucru se poate întâmpla dacă depozitul de certificate *SIGNATUREVERIFICATION a fost transferat pe sistem și DCM nu a fost utilizat pentru modificarea parolei pentru acesta. Într-un astfel de caz, certificatele pe care depozitul le conține nu pot fi utilizate pentru verificarea semnăturilor pe obiecte în timpul procesului de restaurare. Utilizați DCM la modificarea parolei pentru depozitul de certificate. Dacă nu cunoașteți parola, va trebui să ștergeți depozitul de certificate; creați-l din nou și utilizați DCM pentru a schimba parola.
Când instalați un produs, primiți o eroare deoarece semnătura nu a trecut de verificare.	Când semnătura unui obiect nu se verifică în mod corect, eșuarea poate indica faptul că obiectul a fost modificat din momentul în care a fost semnat. Dacă integritatea obiectului este o problemă, nu modificați valoarea de sistem QVFYOBJRST și nu efectuați alte acțiuni care pot permite restaurarea obiectului suspect. Astfel puteți ocoli securitatea pe care o furnizează verificarea semnăturii și să permiteți un obiect dăunător pe sistemul dumneavoastră. În loc de a verifica valoarea de sistem, trebuie să contactați semnatarul obiectului pentru a determina acțiunea corespunzătoare pe care să o întreprindeți pentru a rezolva problema.

Interpretarea mesajelor de eroare la verificarea verificatorului de cod

Utilizați aceste informații pentru a învăța pentru a învăța ce mesaje sunt returnate de funcția de verificare a integrității verificatorului de cod și cum să utilizați aceste mesaje pentru a vă asigura că funcția de verificare a codului nu este coruptă, cât și soluții posibile dacă mesajele indică faptul că funcția sau obiecte cheie ale sistemului de operare pot fi corupte.

Tabelul următor furnizează o listă a mesajelor pe care funcția de verificare a verificatorului de cod le generează în timpul procesării. Acest tabel nu este o listă cuprinzătoare a tuturor mesajelor pe care le puteți recepționa. 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. Vedeți documentația pentru API-ul Verificare sistem (QydoCheckSystem) pentru o listă detaliată a mesajelor de eroare.

De asemenea, un număr de mesaje generate de funcția de verificare a verificatorului de cod pe parcursul procesării sunt mesaje informaționale și nu sunt listate aici. Pentru a învăța mai multe despre cum lucrează procesul de verificare a verificatorului de cod, vedeți Verificarea integrității funcției de verificare a codului.

Tabela 1. Mesaje de eroare la verificarea verificatorului de cod

Mesaj de eroare	Problema posibilă și soluția
CPFB729	Indică faptul că procesul de verificare a verificatorului de cod a eșuat să se termine așa cum se aștepta. Acest eșec poate fi cauzat de o gamă largă de probleme. Revedeți istoricul de job pentru mesaje de eroare mai detaliate pentru a determina natura exactă a eșecului și cauza posibilă. Dacă determinați că obiecte cheie ale sistemului de operare au eșuat la verificarea integrității, acest eșec poate indica faptul că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteți fi nevoit să reinstalați sistemul de operare pentru a asigura integritatea sistemului.

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

Mesaj de eroare	Problema posibilă și soluția
<p>La extragerea istoricului de job, vedeți mesaje ca CPF723, CPD37A1 sau CPD37A0 pentru aceste obiecte specifice:</p> <ul style="list-style-type: none"> • Obiecte program (*PGM): <ul style="list-style-type: none"> – QYDONOSIG în biblioteca QTEMP – QYDOBADSIG în biblioteca QTEMP • Obiecte comandă (*CMD): <ul style="list-style-type: none"> – QYDOBADSIG în biblioteca QTEMP – SIGNOFF în biblioteca QTEMP 	<p>Indică faptul că setul specificat de obiecte pe care le utilizează funcția de verificare a vericatorului de cod pentru testarea integrității a eșuat așa cum era de așteptat. Acest eșec indică faptul că comanda RSTOBJ, comanda RSTLIB, comanda CHKOBJITG și API-ul Verificare obiect raportează corect erorile. Nu este necesară nici o acțiune suplimentară.</p>
<p>CPF723 pentru orice alt obiect diferit de cele listate anterior în acest tabel.</p>	<p>Indică faptul că semnătura pe un obiect cheie al sistemului de operare a eșuat la verificare. Acest eșec poate indica că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteți fi nevoit să reinstalați sistemul de operare pentru a asigura integritatea sistemului.</p>
<p>CPF722 pentru orice alt obiect diferit de cele listate anterior în acest tabel.</p>	<p>Indică faptul că un obiect cheie al sistemului de operare nu are nici o semnătură atunci când este așteptată 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. Puteți fi nevoit să reinstalați sistemul de operare pentru a asigura integritatea sistemului.</p>
<p>CPF72A pentru orice alt obiect diferit de cele listate anterior în acest tabel.</p>	<p>Indică faptul că un obiect cheie al sistemului de operare a eșuat la verificarea integrității. Acest eșec poate indica că obiectul a fost modificat de când a fost semnat atunci când a fost livrat sistemul de operare. Puteți fi nevoit să reinstalați sistemul de operare pentru a asigura integritatea sistemului.</p>

Dacă trebuie să reinstalați cod care verifică integritatea funcției vericatorului de cod, trebuie să îl obțineți de la o sursă cunoscută, bună. De exemplu, puteți instala mediul de instalare pe care l-ați utilizat pentru a instala ediția curentă. Pentru a restaura funcția de verificare a vericatorului de cod, urmați acești pași de la un prompt de comenzi i5/OS:

1. Rulați comanda QSYS/DLTPGM QSYS/QYDOCHK. Această comandă șterge API-ul Verificare sistem (OPM, QYDOCHK; ILE, QydoCheckSystem).
2. Rulați comanda QSYS/DLTSRVPGM QSYS/QYDOCHK1. Această comandă șterge programul serviciu al vericatorului de cod cu API-ul Verificare sistem (OPM, QYDOCHK; ILE, QydoCheckSystem).
3. Rulați comanda QSYS/DLTF QSYS/QYDOCHKF. Această comandă șterge fișierul salvare care conține obiectele pe care le utilizează funcția de verificare cod pentru a testa semnăturile greșite și lipsa semnăturilor
4. Rulați comanda QSYS/RSTOBJ OBJ(QYDOCHK*) SAVLIB(QSYS) DEV(OPT01) OBJTYPE(*ALL) OPTFILE('Q5722SS1/Q5200M_/Q00/Q90'). Această comandă restaurează toate obiectele necesare pentru funcția de verificare a vericatorului de cod de pe mediul de instalare încărcat.

Operații înrudite


“Verificarea integrității funcției de verificare cod” la pagina 42


Aflați cum să verificați integritatea funcției de verificare cod pe care o folosiți la verificarea integrității sistemului i5/OS.

Informații înrudite pentru semnarea obiectelor și verificarea semnăturilor

Utilizați aceste informații pentru a găsi legături cu alte resurse pentru a afla mai multe despre semnarea obiectelor și verificarea semnăturilor obiectelor.

Semnarea obiectelor și verificarea semnăturilor sunt tehnologii de securitate relativ noi. Aici aveți o mică listă cu alte resurse pe care le puteți considera utile dacă sunteți interesat de o înțelegere mai aprofundată a acestor tehnologii și a modului în care ele funcționează:

- **Situl Web VeriSign Help Desk**  Situl Web VeriSign oferă o bibliotecă extensivă cu subiecte legate de certificate digitale, cum ar fi semnarea obiectelor, ca și alte subiecte de securitate a Internetului.
- **IBM eServer iSeries Wired Network Security: i5/OS V5R1 DCM and Cryptographic Enhancements**

SG24-6168  Acest manual IBM Redbook se concentrează pe îmbunătățirile de securitate ale rețelelor la V5R1. Cartea Redbook include multe subiecte inclusiv cum să utilizați posibilitățile de semnare a obiectelor, DCM (Digital Certificate Manager) și așa mai departe.

Informații de licență și de declinare a responsabilității pentru cod

IBM vă acordă o licență de copyright neexclusivă pentru utilizarea tuturor exemplurilor de coduri de programare din care puteți genera funcții similare, adaptate necesităților dumneavoastră specifice.

| EXCEPTÂND GARANȚIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE
| PROGRAME ȘI FURNIZORII SĂI NU ACORDĂ NICI O GARANȚIE SAU CONDIȚIE, EXPRESĂ SAU
| IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE SAU CONDIȚIILE IMPLI
| 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, CHIA R DACĂ AU FOST
| INFORMAȚI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

- | 1. PIERDEREA SAU DETERIORAREA DATELOR;
- | 2. PAGUBE DIRECTE, SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICIILE ECONOMICE DE
| CONSECINȚĂ; SAU
- | 3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAȚIE SAU ECONOMII
| PLANIFICATE.

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

Anexa. Notificări

Aceste informații au fost dezvoltate pentru produse și servicii oferite în U.S.A.

Este posibil ca IBM să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Luați legătura cu reprezentantul IBM local pentru informații despre produsele și 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 funcțional și care nu încalcă dreptul de proprietate intelectuală al IBM. Totuși, este responsabilitatea utilizatorului de a evalua și verifica funcționarea oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Furnizarea acestui document nu vă acordă nici o licență asupra acestor patente. Puteți cere informații despre licență, în scris, la:

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

Pentru întrebări privind licența pentru informațiile DBCS (double-byte), contactați departamentul de Proprietate intelectuală IBM din țara dumneavoastră sau trimiteți întrebările în scris la:

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

Paragraful următor nu se aplică în Marea Britanie sau orice altă țară unde asemenea clauze contravin legilor locale: INTERNATIONAL BUSINESS MACHINES CORPORATION FURNIZEAZĂ ACEASTĂ PUBLICAȚIE “AȘA CUM ESTE” FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICIT SAU IMPLICIT, INCLUZÂND, DAR NELIMITÂNDU-SE LA, GARANȚIILE IMPLICITE DE NE-ÎNCĂLCARE, COMERCIALIZARE SAU ADAPTARE PENTRU UN SCOP PARTICULAR. Unele state nu permit declinarea garanțiilor explicite sau implicite în anumite tranzacții, de aceea, este posibil ca această declarație să nu vi se aplice.

Aceste informații pot include greșeli tehnice sau erori de tipar. Periodic sunt efectuate modificări ale acestor informații; aceste modificări vor fi încorporate în edițiile noi ale publicației. IBM poate aduce îmbunătățiri și/sau modificări produsului (produselor) și/sau programului (programelor) descrise în această publicație în orice moment, fără notificare.

Orice referiri din aceste informații la situri Web non-IBM Web sunt furnizate doar pentru ușurință și nu servesc în nici o manieră ca un sprijin pentru acele situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informațiile pe care le furnizați, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație față de dumneavoastră.

Posesorii de licență ai acestui program care doresc să aibă informații despre acesta cu scopul posibilității de: (i) schimb de informații între programe create independent și alte programe (inclusiv acesta) și (ii) utilizarea mutuală a informațiilor care au fost schimbate, trebuie să contacteze:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Aceste informații pot fi disponibile, conform termenilor și condițiilor, incluzând în unele cazuri, plata unei taxe.

- | Programul licențiat la care se referă aceste informații și toate materialele licențiate disponibile pentru el sunt furnizate
- | de IBM conform termenilor din Contractul IBM cu Clientul, Contractul IBM pentru licență internațională de program,
- | Contractul IBM de licență pentru Codul mașină sau din alt acord echivalent încheiat între noi.

Orice date de performanță conținute aici au fost determinate într-un mediu controlat. De aceea, rezultatele obținute în alte medii de operare pot varia semnificativ. Este posibil ca unele măsurători să fie făcute pe sisteme la nivel de dezvoltare și nu este nici o garanție că aceste măsurători vor fi aceleași pe sistemele disponibile general. Mai mult, este posibil ca unele măsurători să fie estimate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informațiile cu privire la produse non-IBM au fost obținute de la furnizorii acestor produse, din anunțurile publicate ale acestora sau din alte surse disponibile public. IBM nu a testat acele produse și nu poate confirma acuratețea performanței, compatibilitatea sau orice alte pretenții legate de produse non-IBM. Întrebările despre capacitățile produselor non-IBM trebuie adresate furnizorilor acelor produse.

Toate declarațiile cu privire la direcția sau intenția viitoare IBM sunt subiectul modificărilor sau retragerii fără notificare și reprezintă doar scopuri și obiective.

Toate prețurile IBM arătate sunt prețurile cu amănuntul sugerate de IBM, sunt curente și pot fi modificate fără notificare. Prețurile dealer-ului pot fi diferite.

Aceste informații sunt doar în scop de planificare. Informațiile menționate aici se pot modifica înainte ca produsele descrise să devină disponibile pe piață.

Aceste informații conțin exemple de date și rapoarte utilizate în operații de afaceri de zi cu zi. Pentru a le ilustra cât mai complet posibil, exemplele includ nume de persoane, companii, mărci și produse. Toate aceste nume sunt inventate și orice similaritate cu numele și adresele utilizate de o întreprindere de afaceri reală este o pură coincidență.

LICENȚĂ COPYRIGHT:

Aceste informații conțin programe aplicație model în limbaj sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteți copia, modifica și distribui aceste programe eșantion după cum doriți, fără ca IBM să pretindă vreo plată pentru aceasta, dacă o faceți pentru dezvoltarea, folosirea, marketingul sau distribuirea programelor de aplicație în conformitate cu interfața de programare a aplicațiilor pentru platforma de operare pentru care a fost scris programul eșantion respectiv. Aceste exemple nu au fost testate temeinic în toate condițiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, capacitatea de service sau funcția acestor programe.

- | EXCEPTÂND GARANȚIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE
- | PROGRAME ȘI FURNIZORII SĂI NU ACORDĂ NICI O GARANȚIE SAU CONDIȚIE, EXPRESĂ SAU
- | IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE SAU CONDIȚIILE 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, CHIAI DACĂ AU FOST
- | INFORMAȚI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

- | 1. PIERDEREA SAU DETERIORAREA DATELOR;
- | 2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICIILE ECONOMICE DE
- | CONSECINȚĂ; SAU

| 3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAȚIE SAU ECONOMII
| PLANIFICATE.

| UNELE JURISDICȚII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALALE 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 porțiune din aceste programe eșantion sau lucrările derivate din ele trebuie să conțină un anunț de copyright, după cum urmează:

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

Dacă vizualizați aceste informații în formă electronică, este posibil ca fotografiile și ilustrațiile color să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale International Business Machines Corporation în Statele Unite, alte țări sau ambele:

| AIX
| AIX 5L
| e(logo)server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

Microsoft, Windows, Windows NT și logo-ul Windows sunt mărci comerciale ale Microsoft Corporation din Statele Unite, alte țări sau ambele.

Java și toate mărcile comerciale bazate pe Java sunt mărci comerciale ale Sun Microsystems, Inc. în Statele Unite, în alte țări sau ambele.

| Linux este marcă comercială a Linus Torvalds în Statele Unite, în alte țări sau ambele.

UNIX este o marcă comercială înregistrată, deținută de The Open Group în Statele Unite și în alte țări.

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

Termenii și condițiile

Permisunile pentru utilizarea acestor publicații sunt acordate în conformitate cu următorii termeni și condiții.

Utilizare personală: Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți distribui, afișa sau realiza lucrări derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

Utilizare comercială: Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit de la IBM.

În afara celor acordate expres prin această permisiune, nu se acordă nici o altă permisiune, licență sau drept, explicite sau implicite, pentru aceste publicații sau orice informații, date, software sau alte elemente pe care le conțin și care reprezintă o proprietate intelectuală.

IBM își păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreția sa, dacă folosirea publicațiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau re-exporta aceste informații decât cu respectarea tuturor legilor și reglementărilor în vigoare, inclusiv a tuturor legilor și reglementărilor de export ale Statelor Unite.

IBM NU OFERĂ GARANȚII DESPRE CONȚINUTUL ACESTOR PUBLICAȚII. PUBLICAȚIILE SUNT FURNIZATE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎCĂLCARE A UNOR DREPTURI SAU NORME ȘI DE POTRIVIRE PENTRU UN ANUMIT SCOP.



Tipărit în S.U.A.