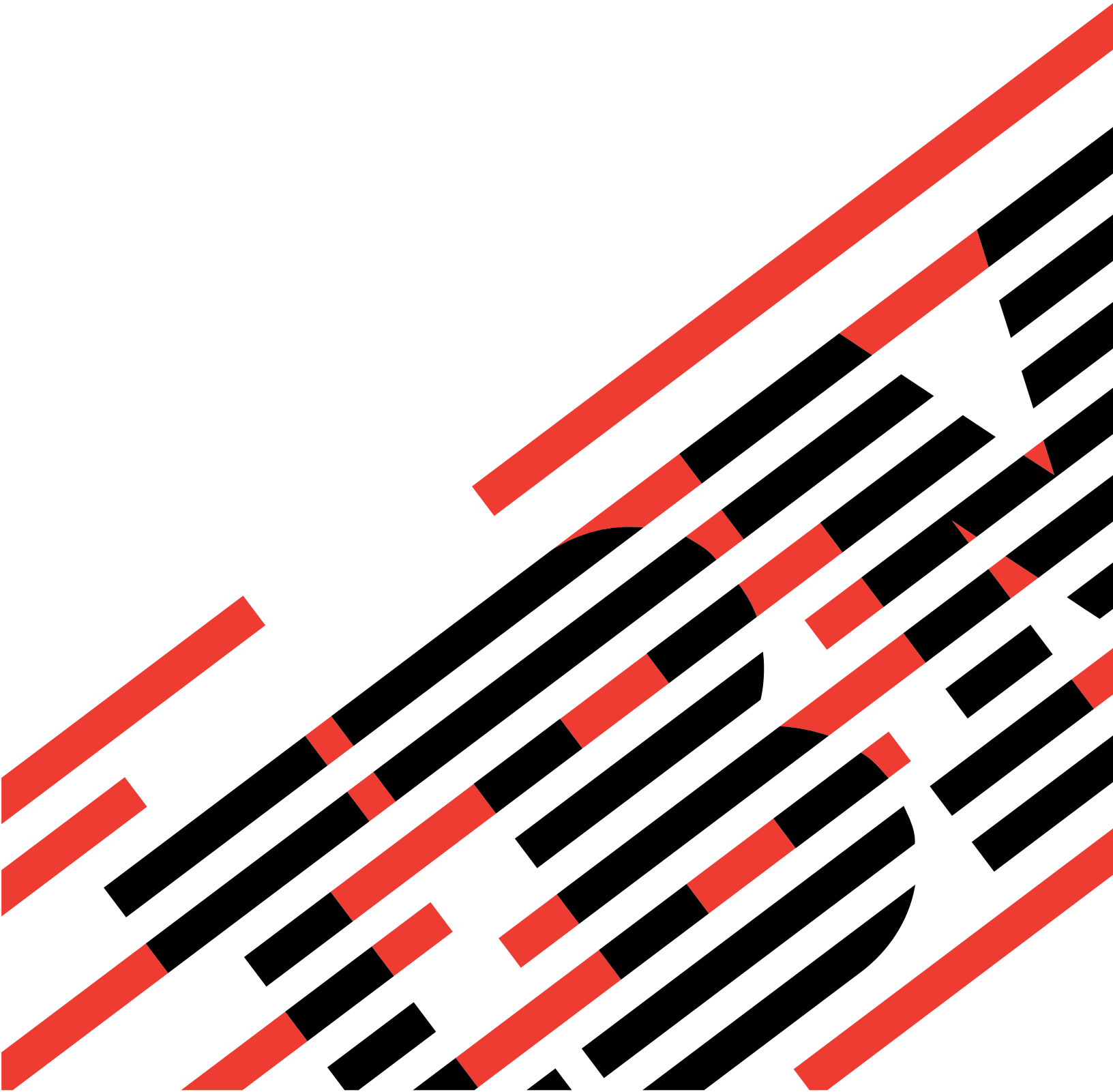
IBM

eserver

iSeries

DCM (Digital Certificate Manager)



IBM

@server

iSeries

DCM (Digital Certificate Manager)

Cuprins

Componentă 1. Digital Certificate Manager

Un certificat digital este o acreditare electronică pe care o puteţi folosi pentru a vă demonstra identitatea pentru o tranzacţie electronică. Există un număr din ce în ce mai mare de modalităţi de folosire a certificatelor digitale pentru a se asigura măsuri de securitate crescânde în reţea. De exemplu, certificatele digitale sunt esenţiale pentru configurarea şi folosirea Secure Sockets Layer (SSL). Utilizarea SSL vă permite să creaţi conexiuni sigure între utilizatori şi aplicaţii server peste o reţea ce nu este de încredere, cum ar fi Internet. SSL oferă una dintre cele mai bune soluţii pentru protecţia intimităţii datelor sensibile, cum ar fi nume utilizator şi parolă, pe Internet. Multe servicii şi aplicaţii iSeries, cum sunt FTP, Telnet, HTTP Server pentru iSeries şi multe altele, furnizează suport SSL pentru a asigura ascunderea datelor.

iSeries furnizează suport extensiv pentru certificate digitale care vă permit să folosiţi certificatele digitale drept acreditări într-un număr de aplicaţii de securitate. În plus faţă de folosirea certificatelor pentru configurarea SSL, le puteţi folosi şi drept credite în autentificarea clienţilor pentru tranzacţii SSL şi VPN (reţele private virtuale). De asemenea, puteţi folosi certificatele digitale şi cheile de securitate asociate lor pentru a semna obiecte . Semnarea obiectelor vă permite să detectaţi modificările sau posibilele deteriorări ale conţinutului obiectelor prin verificarea semnăturilor asupra obiectelor pentru a le asigura integritatea.

Beneficierea de suportul iSeries pentru certificate este simplă când folosiţi Digital Certificate Manager (DCM), o opţiune iSeries gratis, pentru a gestiona centralizat certificatele pentru aplicaţiile dumneavoastră. DCM vă permite să gestionaţi certificate pe care le obţineţi de la orice CA (autoritate de certificare). De asemenea, puteţi folosi DCM pentru a crea şi lucra cu propriul dumneavoastră CA local pentru a emite certificate private către aplicaţiile şi utilizatorii din organizaţia dumneavoastră.

Cheile folosirii efective a certificatelor pentru beneficiile lor în ceea ce priveşte securitatea sunt planificarea şi evaluarea corectă. Ar trebui să revedeţi aceste subiecte pentru a afla mai multe despre cum lucrează certificatele şi despre cum puteţi folosi DCM pentru a le gestiona pe ele şi aplicaţiile care le folosesc:

Ce este nou în V5R2
Folosiţi aceste informaţii pentru a afla despre modificările opţiunii Digital Certificate Manager şi modificările informaţiilor din subiect pentru această ediţie.

Tipăriţi acest subiect
Folosiţi această pagină pentru a afla cum să tipăriţi întregul subiect ca un fişier PDF.

Migrare în DCM de la o ediţie anterioară
Folosiţi această informaţie pentru a afla ce task-trebuie să realizaţi şi alte consideraţii pe care trebuie să le înţelegeţi dacă migraţi o versiune existentă a DCM în versiunea curentă.

Scenarii DCM
Folosiţi această infomaţie pentru a revedea două scenarii care ilustrează scheme tipice de implementare a certificatelor pentru a vă ajuta să vă planificaţi propria implementare de certificate ca parte a politicii de securitate iSeries a dumneavoastră. Fiecare scenariu furnizează de asemenea toate taskurile de configurare necesare pe care trebuie să le realizaţi pentru a face scenariul după descriere.

Concepte de certificate digitale
Folosiţi acest concept şi informaţiile referinţă pentru a înţelege mai bine ce sunt certificatele digitale şi cum lucrează. Aflaţi despre diferitele tipuri de certificate şi cum le puteţi folosi ca parte a politicii de securitate a dumneavoastră.

Plan pentru DCM
Folosiţi aceste informaţii pentru a vă ajuta în decizia a cum şi unde ar trebui să folosiţi certificate digitale pentru a vă îndeplini scopul în ceea ce priveşte securitatea. Folosiţi această informaţie pentru a afla despre orice cerinţe preliminare de care aveţi nevoie pentru instalare, ca şi de alte cerinţe de care trebuie să ţineţi cont înainte de folosirea DCM.

Configurarea DCM
Folosiţi această informaţie pentru a afla cum să configuraţi tot ce vă trebuie pentru a vă asigura că puteţi folosi DCM pentru a vă gestiona certificatele dumneavoastră şi cheile lor.

Gestionare DCM
Folosiţi aceste informaţii pentru a învăţa să folosiţi DCM pentru gestionarea certificatelor şi a aplicaţiilor care le folosesc. De asemenea, puteţi învăţa cum să semnaţi digital obiecte şi cum să creaţi şi să operaţi propriile Autorităţi de certificare.

Depanare DCM
Folosiţi aceste informaţii pentru a învăţa cum să rezolvaţi unele dintre cele mai comune erori pe care le puteţi întâlni când folosiţi DCM.

Informaţii înrudite pentru DCM
Folosiţi această pagină pentru a găsi link-uri către alte resurse pentru a afla mai multe despre certificatele digitale, infrastructura cheilor publice, Digital Certificate Manager şi alte informaţii înrudite.

Capitol 1. Ce este nou în V5R2

Îmbunătăţirile aduse la V5R2 Digital Certificate Manager (DCM) şi capabilităţile iSeries pentru certificate digitale includ:

- **Funcţia de asignare certificate**
  Acest nou task DCM vă permite să asignaţi un certificat cu una sau mai multe aplicaţii mai rapid şi mai uşor. Puteţi accesa acest task ori din lista de taskuri **Gestionare certificate**, ori din paginile **Lucrul cu serverul şi cu certificate** şi **Lucrul cu certificate de semnare a obiectelor**. Această funcţie este disponibilă doar pentru depozitele de certificate *SYSTEM şi *OBJECTSIGNING.
- **Semnare obiecte comandă (*CMD)**
  Puteţi folosi acum DCM pentru a crea semnături digitale pe obiecte comandă (*CMD) pentru a oferi un mijloc de verificare a integrităţii lor. De asemenea, puteţi alege domeniul de valabilitate al semnăturii pentru obiecte *CMD; puteţi alege dacă să semnaţi întregul obiect *CMD sau să semnaţi doar componentele de bază ale obiectului *CMD. Când folosiţi DCM pentru a vedea semnătura de pe obiecte *CMD, DCM oferă informaţii despre domeniul de valabilitate al semnăturii.
- **API-uri pentru crearea de certificate utilizator semnate de CA local fără a folosi DCM**
  Acum există două noi API-uri pe care le puteţi folosi pentru a emite dintr-un program certificate semnate de Autoritate de Certificare (Certificate Authority - CA) Locală a dvs. către utilizatori non-iSeries. Aceste API-uri vă permit să emiteţi certificate către utilizatori fără profile utilizator iSeries şi fără ca utilizatorii să trebuiască să folosească DCM pentru a obţine individual un certificat pentru autentificarea clientului.

Informaţii noi sau îmbunătăţite legate de acest subiect includ:

- Două noi scenarii pe care le puteţi folosi pentru a vă ajuta să determinaţi cum să utilizaţi în mod optim certificate pentru a realiza scopurile dvs. de securitate.
- Informaţii reorganizate care vă uşurează găsirea de informaţii de care aveţi nevoie pentru a folosi DCM.

Pentru a găsi alte informaţii despre noutăţi sau schimbări în această ediţie, vedeţi Memo către utilizatori  .

Capitol 2. Tipărirea acestui articol

Pentru a vizualiza sau descărca versiunea PDF, selectaţi Digital Certificate Manager  (dimensiunea fişierului este aproximativ 468 KB sau cca. 110 pagini).

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

1. Deschideţi PDF-ul în browser-ul propriu (selectaţi legătura de mai sus).
2. În meniul browser-ului, selectaţi **File**.
3. Apoi selectaţi **Save As...**
4. Navigaţi în directorul în care doriţi să salvaţi fişierul PDF.
5. Selectaţi **Save**.

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

 .

Capitol 3. Migrarea de la o versiune anterioară a DCM

Când migraţi de la versiunea V4R3 a Digital Certificate Manager (DCM) către V5R2, DCM actualizează automat fişierele dvs. existente inel de chei ale Autorităţii de Certificare locale şi ale certificatelor sistem. DCM actualizează aceste fişiere, care sunt denumite default.kyr, în fişierele depozit de certificate corespunzătoare, care sunt denumite default.kdb. DCM transferă de asemenea toate certificatele valide în fişierele inel chei asociate cu server-ele HTTP (Hypertext Transfer Protocol) şi LDAP (Lightweight Directory Access Protocol). DCM migrează certificatele valide din depozitul de certificate *SYSTEM (default.kdb).

Notă: Dacă migraţi de la versiunea V4R4, V4R5 sau V5R1 a DCM, nu este nevoie să efectuaţi nici o operaţie de migrare deoarece fişierele certificate din aceste versiuni sunt compatibile cu versiunea V5R2 a DCM.

Migrarea de la inel de chei (Key ring) la depozit de certificate – migrarea V4R3

În timpul instalării V5R2 DCM, sistemul migrează următoarele fişiere inele de chei:
- Fişierele inel de chei implicite ale DCM.
- Inele de chei folosite de fişierele de configurare server HTTP.
- Inele de chei folosite de fişierele de configurare server LDAP.

Dacă folosiţi un fişier .kyr pe care DCM nu l-a actualizat automat, DCM îl converteşte într-un fişier .kyr.kdb atunci când lucraţi cu acesta pentru prima oară în DCM. De exemplu, prima oară când specificaţi fişierul secure.kyr din interfaţa utilizator DCM, acesta converteşte fişierul într-un depozit de certificate cu numele de fişier secure.kyr.kdb.

Notă: Inelele cheie sunt diferite pentru depozitele de certificate, deci trebuie să convetiţi fişierele inel cheie pe care DCM nu le-a actualizat automat lucrând cu ele prin interfaţa utilizator DCM. Schimbarea manuală a extensiilor numelui fişierului la .kdb va produce erori atunci când veţi încerca să lucraţi cu acele fişiere prin interfaţa utilizator DCM.

Dacă încercaţi să ştergeţi fişierul secure.kyr în timp ce folosiţi DCM, DCM îl arhivează de fapt şi şterge, în schimb, fişierul secure.kyr.kdb.

Parolă implicită depozit certificate.

Dacă fişierul /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR există, sistemul migrează acest fişier inel cheie şi orice alte fişiere inel cheie eligibile în depozitul de certificate *SYSTEM. Parola originală asociată cu fişierul /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR este folosită ca parolă pentru depozitul de certificate *SYSTEM.

Dacă fişierul /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR nu există, dar sunt alte fişiere inel cheie eligibile pentru migrare (de exemplu, fişierele inel cheie pe care le folosesc fişierele de configurare ale server-ului HTTP), sistemul crează depozitul de certificate *SYSTEM cu parola DEFAULT (cu litere mari) şi realizează migrarea.

Pentru informaţii despre erorile care pot apare în timpul procesului de migrare a fişierelor şi pentru informaţii despre cum să le rezolvaţi, vedeţi: Erori de migrare şi soluţii de rezolvare.

Capitol 4. Scenarii DCM

Digital Certificate Manager şi suportul de certificate digitale pe care îl furnizează iSeries vă permite să folosiţi certificate pentru a îmbunătăţi politica de securitate în mai multe moduri. Cum alegeţi să folosiţi certificatele depinde atât de obiectivele dumneavoastră de afaceri cât şi de nevoile dvs. de securitate.

Folosirea certificatelor digitale vă poate ajuta să vă îmbunătăţiţi securitatea în mai multe moduri. Certificatele digitale permit folosirea Secure Sockets Layer (SSL) pentru acces sigur la pagini de Web şi alte servicii Internet. Puteţi folosi certificate digitale pentru a configura conexiuni VPN (reţea privată virtuală). De asemenea, puteţi folosi cheia unui certificat pentru a semna digital obiecte sau pentru a verifica semnăturile digitale pentru a vă asigura de autenticitatea obiectelor. Asemenea semnături digitale asigură că originea unui obiect este de încredere şi protejează integritatea obiectului.

Securitatea sistemului poate fi îmbunătăţită atunci când se utilizează certificate digitale (în locul numelor de utilizatori şi a parolelor) pentru a autentifica şi autoriza sesiunile dintre utilizatori şi servere. De asemenea, puteţi folosi DCM să asociaţi un certificat al unui utilizator cu profilul său de utilizator iSeries. Certificatul are astfel aceleaşi autorizări şi permisiuni precum profilul asociat.

În consecinţă, cum alegeţi să folosiţi certificatele poate fi complicat şi depinde de o multitudine de factori. Scenariiile furnizate în acest subiect descriu unele din cele mai comune obiective de securitate ale certificatelor digitale în anumite contexte de afaceri. Fiecare scenariu descrie de asemenea toate cerinţele de sistem şi software preliminare necesare şi toate taskurile de configurare pe care trebuie să le realizaţi pentru a implementa scenariul. Citiţi aceste scenarii pentru a vă ajuta să determinaţi în ce fel folosirea certificatelor pentru securitate se potriveşte mai bine nevoilor dumneavoastră:

Scenariu: Folosiţi certificatele pentru a proteja accesul la aplicaţii şi resurse publice
Acest scenariu descrie când şi cum să folosiţi certificatele pentru a proteja şi limita accesul de utilizatori publici la resurse şi aplicaţii publice sau extranet.

Scenariu: Folosiţi certificatele pentru a proteja accesul la aplicaţii şi resurse interne
Acest scenariu descrie când şi cum să folosiţi certificatele pentru a proteja şi restricţiona resursele şi aplicaţiile pe care le pot accesa utilizatorii interni pe serverele dumneavoastră interne.

Scenariu: Folosiţi certificatele pentru a proteja accesul la aplicaţii şi resurse publice

Situaţie

Dvs. lucraţi pentru o companie de asigurări (MyCo., Inc) şi sunteţi responsabil pentru menţinerea de diverse aplicaţii pe site-urile intranet şi extranet ale companiei dvs. O anumită aplicaţie pentru care sunteţi responsabil este o aplicaţie de calculare a ratei care permite ca sute de agenţi independenţi să genereze baremuri pentru clienţii lor. Deoarece informaţia pe care această aplicaţie o furnizează este oarecum sensibilă, doriţi să vă asiguraţi că doar agenţii înregistraţi o pot folosi. Mai mult, doriţi să furnizaţi în cele din urmă o metodă de acces utilizator la aplicaţie mai sigură decât metoda curentă cu nume utilizator şi parolă. Sunteţi îngrijorat că utilizatori neautorizaţi pot captura această informaţie când este transmisă printr-o reţea nesigură. De asemenea, diverşi agenţi pot împărţi această informaţie între ei fără a avea autorizarea să facă acest lucru.

După cercetare, decideţi că folosirea certificatelor digitale vă poate furniza securitatea de care aveţi nevoie. Folosirea certificatelor vă permite să folosiţi Secure Sockets Layer (SSL) pentru a proteja transmisia datelor despre rată. Deşi doriţi ca în final toţi agenţii să folosească un certificat pentru a accesa aplicaţia, ştiţi că s-ar putea ca agenţii şi compania dvs. să aibă nevoie de ceva timp înainte ca acest scop să fie realizat. În acest moment, planificaţi să continuaţi cu metoda curentă de autentificare cu nume utilizator şi parolă deoarece SSL asigură securitatea acestor date sensibile în timpul transmisiei.

În funcţie de tipul de aplicaţie şi de utilizatorii ei şi de scopul dvs. viitor de autentificare prin certificate pentru utilizatori, decideţi să folosiţi un certificat public de la o Autoritate certificare (CA) bine-cunoscută pentru a configura SSL pentru aplicaţiile dvs.

Avantajele scenariului

Acest scenariu are următoarele avantaje:
- Folosirea certificatelor digitale pentru a configura accesul SSL la aplicaţia dvs. de calculare a ratei asigură că informaţia transmisă între server şi client este protejată şi privată.
- Folosirea certificatelor digitale de fiecare dată când este posibilă pentru autentificarea clientului furnizează o metodă mai sigură de identificare a utilizatorilor autorizaţi. Chiar şi unde nu este posibilă, autentificarea clientului prin metoda cu nume utilizator şi parolă este protejată şi ţinută privată de sesiunea SSL, făcând schimbul acestor date sensibile mai sigur.
- Folosirea certificatelor digitale *publice* pentru a limita sau permite accesul la aplicaţiile şi datele dvs. este o alegere practică în aceste condiţii sau în condiţii similare:
  - Datele şi aplicaţiile dvs. necesită diferite nivele de securitate.
  - Există o rată înaltă de modificări (turnover) între utilizitorii de încredere.
  - Furnizaţi acces public la aplicaţii şi date, cum ar fi un site de web Internet sau o aplicaţie extranet.
  - Nu doriţi să lucraţi cu propria Autoritate certificare (CA) datorită unui număr mare de utilizatori care accesează aplicaţiile şi resursele dvs. din alte motive administrative.
- Folosirea unui certificat public pentru a configura aplicaţia de calculare a ratei pentru SSL în acest scenariu scade numărul de configurări pe care utilizatorii trebuie să le realizeze pentru a accesa aplicaţia. Majoritatea software-ului client conţine certificate CA pentru majoritatea CA-urilor bine-cunoscute.

Obiective

În acest scenariu, MyCo., Inc. doreşte să folosească certificate digitale pentru a proteja informaţia despre calculul ratei pe care aplicaţia lor o furnizează utilizatorilor publici autorizaţi. Compania de asemenea doreşte o metodă mai sigură de autentificare a acelor utilizatori care au accesul permis la această aplicaţie.

Obiectivele acestui scenariu sunt următoarele:
- Aplicaţia publică a companiei pentru calculul ratei trebuie să folosească SSL pentru a proteja siguranţa datelor pe care o furnizează utilizatorilor.
- Configurarea SSL trebuie realizată cu certificate publice de la o Autoritate certificare (CA) Internet publică bine-cunoscută.
- Utilizatorii autorizaţi trebuie să furnizeze un nume utilizator şi parolă valide pentru a accesa aplicaţia în modul SSL. În cele din urmă, utilizatorii autorizaţi trebuie să poată folosi una din cale două metode de autentificare sigură pentru a li se permite accesul la aplicaţie. Agenţii trebuie fie să prezinte un certificat digital public de la o Autoritate certificare (CA) bine-cunoscută fie un nume utilizator şi o parolă valide.

Detalii

Următoarea figură ilustrează situaţia de configurare a reţelei pentru acest scenariu:

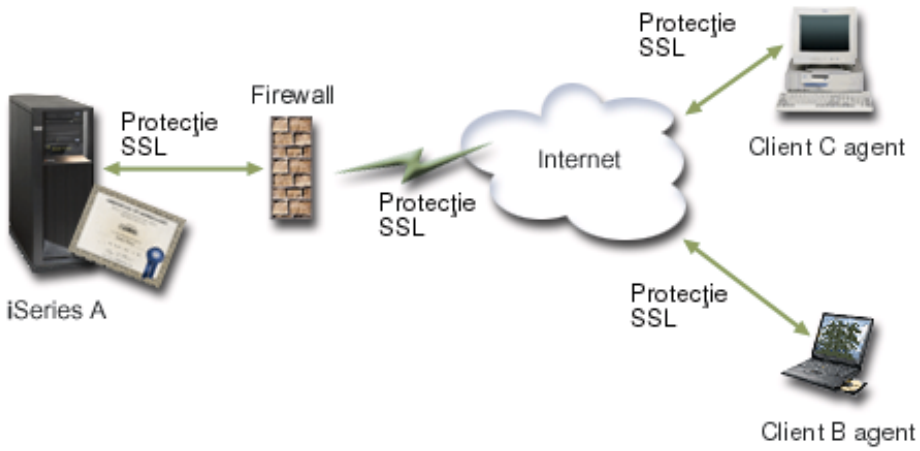


Figura ilustrează următoarele informaţii despre situaţia pentru acest scenariu:

Server public al companiei – iSeries A
- iSeries A este serverul care găzduieşte aplicaţia companiei de calcul a ratei.
- iSeries A rulează OS/400 Version 5 Release 2 (V5R2).
- iSeries A are instalat un furnizor de acces criptografic (5722–AC3).
- iSeries A are instalate şi configurate Digital Certificate Manager (OS/400 opţiunea 34) şi IBM Server HTTP pentru iSeries (5722–DG1).
- iSeries A rulează aplicaţia de calcul a ratei, care este configurată astfel încât:
  - Necesită modul SSL.
  - Foloseşte un certificat public de la o Autoritate certificare bine cunoscută (CA) pentru configurarea SSL.
  - Necesită autentificarea utilizatorului prin nume utilizator şi parolă.
- iSeries A îşi prezintă certificatul pentru a iniţia o sesiune SSL când Clienţii B şi C accesează aplicaţia.
- După iniţializarea sesiunii SSL, iSeries A cere ca Clienţii B şi C să furnizeze un nume utilizator şi o parolă valide înainte de a permite accesul la aplicaţia de calcul a ratei.

Sistemele client agent – Client B şi Client C
- Clienţii B şi C sunt agenţi independenţi care accesează aplicaţia de calcul a ratei.
- Clienţii B şi C au o copie a certificatuui de la un CA bine-cunoscut care a emis certificatul de aplicaţie instalat în software-ul lor client.
- Clienţii B şi C accesează aplicaţia de calcul a ratei pe iSeries A, care îşi prezintă certificatul către software-ul lor client pentru a-i verifica identitatea şi a iniţia o sesiune SSL.
- Software-ul client de pe Clienţii B şi C este configurat să accepte certificatul de la iSeries A şi sesiunea SSL începe.
- După ce sesiunea SSL începe, Clienţii B şi C trebuie să furnizeze un nume de utilizator şi o parolă valide înainte ca iSeries A să permită accesul la aplicaţie.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:
1. Aplicaţia de calcul a ratei de pe iSeries A este o aplicaţie generică care poate fi configurată să folosească SSL. Majoritatea aplicaţiilor, inclusiv multe aplicaţii iSeries, furnizează suport SSL. Paşii de configurare SSL variază foarte mult de la aplicaţie la aplicaţie. În consecinţă, acest scenariu nu furnizează instrucţiuni specifice pentru configurarea aplicaţiei de calcul a ratei să folosească SSL. Acest scenariu furnizează instrucţiuni pentru configurarea şi gestionarea certificatelor care sunt necesare pentru ca orice aplicaţie să folosească SSL.

2. *Opţional*, aplicaţia de calcul a ratei poate avea capabilitatea de a cere certificate pentru autentificarea unui client. Acest scenariu furnizează instrucţiuni despre cum să folosiţi Digital Certificate Manager (DCM) pentru a configura încrederea în certificate pentru acele aplicaţii care furnizează acest suport. Deoarece paşii de configurare pentru autentificarea unui client diferă de la aplicaţie la aplicaţie, acest scenariu nu dă instrucţiuni specifice pentru configurarea unui certificat de autentificare a unui client pentru aplicaţia de calcul a ratei.
3. iSeries A îndeplineşte cerinţele pentru instalarea şi folosirea Digital Certificate Manager (DCM).
4. Nimeni nu a configurat sau folosit anterior DCM pe iSeries A.
5. Oricine foloseşte DCM pentru a realiza taskurile din acest scenariu trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilele lor de utilizator.
6. iSeries A nu are instalat un Coprocesor Criptografic IBM 4758-023 PCI.

Paşii task-ului

Pentru a implementa acest scenariu, trebuie să realizaţi aceste taskuri pe iSeries A:

1. Efectuaţi toţi paşii cerinţelor preliminare pentru a instala şi configura toate produsele iSeries necesare.
2. Folosiţi Digital Certificate Manager (DCM) pentru a crea o cerere de certificat de server.
3. Configuraţi-vă aplicaţia să folosească SSL.
4. Folosiţi DCM pentru a importa şi asigna certificatul server sau client semnat la ID-ul aplicaţiei pentru aplicaţia dvs.
5. Porniţi aplicaţia în modul SSL, dacă este necesar.
6. *Taskuri opţionale*: Folosiţi DCM să definiţi o listă de CA-uri de încredere pentru a activa autentificarea unui client pe baza certificatelor pentru aplicaţii care furnizează acest suport.

Notă: Situaţia pe care o descrie acest scenariu nu necesită ca aplicaţia de calcul a ratei să folosească certificate pentru autentificarea unui client. Multe aplicaţii furnizează suport pentru certificate de autentificare a unui client; cum configuraţi acest suport depinde de la aplicaţie la aplicaţie. Acest task opţional este furnizat pentru a vă ajuta să înţelegeţi cum să folosiţi DCM pentru a activa încrederea în certificate pentru autentificarea clientului ca un fundament pentru configurarea suportului aplicaţiei dumneavoastră pentru certificate de autentificare a unui client.

Detalii de configurare

Efectuaţi următorii paşi ai taskului pentru a folosi certificatele pentru configurarea accesului public protejat la aplicaţii şi resurse după cum descrie acest scenariu.

Pas 1: Efectuaţi taskurile cerinţelor preliminare pentru a instala toate produsele iSeries necesare

Trebuie să efectuaţi toate taskurile cerinţelor preliminare pentru a instala şi configura toate produsele iSeries necesare înainte să puteţi realiza anumite taskuri de configurare pentru implementarea acestui scenariu.

Pas 2: Creaţi o cerere de certificat server sau client

Pentru a începe procesul de folosire a SSL pentru a proteja comunicarea datelor unei aplicaţii după cum descrie acest scenariu, trebuie să obţineţi întâi un certificat digital de la un CA public. Puteţi folosi DCM să creaţi informaţia pe care o cere CA-ul public pentru emiterea unui certificat.

Pentru a începe procesul de obţinere a certificatului dvs., urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al DCM, selectaţi **Crearea unui nou depozit de certificate** pentru a porni task-ul asistat şi pentru a completa o serie de formulare. Aceste formulare vă vor ghida prin procesul de creare a unui depozit de certificate şi a unui certificat pe care aplicaţiile le pot folosi pentru sesiuni SSL.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Selectaţi ***SYSTEM** ca depozit de certificat pentru creare şi apăsaţi **Continuare**.
4. Selectaţi **Da** pentru a crea un certificat ca parte a creării depozitului de certificate *SYSTEM şi apăsaţi **Continuare**.
5. Selectaţi **VeriSign sau altă CA Internet (autoritate de certificare)** ca semnatar al noului certificat şi efectuaţi un clic pe **Continuare** pentru a se afişa un formular care vă va permite să introduceţi informaţii de identificare pentru noul certificat.
6. Completaţi formularul şi apăsaţi **Continuare** pentru a se afişa pagina de confirmare. Această pagină de confirmarea va afişa datele cererii certificatului pe care trebuie să îl furnizaţi Autorităţii de certificare publice care va emite certificatul. Datele CSR (cerere de semnare a certificatului) consistă în cheia publică şi alte informaţii pe care le specificaţi pentru noul certificat.
7. Copiaţi cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fişier separat, pe care îl cere CA publică pentru cererea unui certificat. Trebuie să folosiţi toate datele CSR, inclusiv liniile Begin şi End New Certificate Request. Atunci când părăsiţi această pagină, datele vor fi pierdute şi nu se vor mai putea recupera.
8. Trimiteţi formularul sau fişierul aplicaţiei către CA aleasă pentru emiterea şi semnarea certificatului.
9. Aşteptaţi ca CA să returneze certificatul complet, semnat înainte de a continua cu pasul următor al taskului pentru scenariu.

După ce CA returnează certificatul complet semnat, puteţi configura aplicaţia dvs. să folosească SSL, importaţi certificatul în depozitul de certificate *SYSTEM şi asignaţi-l aplicaţiei dvs. să îl folosească pentru SSL.

Pas 3: Configuraţi aplicaţia să folosească SSL

Când vă primiţi înapoi certificatul semnat de la CA-ul public, puteţi continua procesul de actviare a comunicaţiilor SSL pentru aplicaţia dvs. publică. Trebuie să vă configuraţi aplicaţia să folosească SSL înainte de a lucra cu certificatul dvs. semnat. Unele aplicaţii, cum sunt Serverul HTTP pentru iSeries generează un ID de aplicaţie unic şi înregistrează ID-ul cu DCM când configuraţi aplicaţia să folosească SSL. Trebuie să ştiţi ID-ul aplicaţiei înainte de a putea folosi DCM pentru a asigna la ea certificatul dvs. semnat şi să terminaţi procesul de configurare SSL.

Cum vă configuraţi aplicaţia să folosească SSL depinde de aplicaţie. Acest scenariu nu se referă la o anumită sursă pentru aplicaţia de calcul a ratei pe care o descrie deoarece sunt mai multe moduri prin care MyCo., Inc. poate furniza această aplicaţie agenţilor ei.

Pentru a vă configura aplicaţia să folosească SSL, urmaţi instrucţiunile pe care le furnizează documentaţia aplicaţiei dvs. De asemenea, puteţi afla mai multe despre configurarea multor aplicaţii IBM uzuale pentru a folosi SSL, citind subiectul din Centrul de informare, Aplicaţii sigure cu SSL.

Pas 4: Importaţi şi asignaţi certificatul public semnat

După ce vă configuraţi aplicaţia să folosească SSL, puteţi folosi DCM pentru a importa certificatul dvs. semnat şi să-l asignaţi aplicaţiei dvs.

Pentru a importa şi asigna certificatul dvs. către aplicaţia dvs. pentru a completa procesul de configurare SSL, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apăsaţi **Continuare**.
4. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate *SYSTEM.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
6. Apoi, selectaţi **Asignare certificat** din lista de taskuri **Gestionare certificate** pentru a afişa o listă de certificate pentru depozitul de certificate curent.
7. Selectaţi un certificat din listă şi apăsaţi **Asignare către aplicaţii** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate curent.
8. Selectaţi aplicaţia dvs. din listă şi apăsaţi **Continuare** . Apare o pagină fie cu un mesaj de confirmare pentru selecţia dvs. de asignare fie cu un mesaj de eroare dacă a apărut o problemă.

Cu aceste taskuri completate, vă puteţi porni aplicaţia în modul SSL şi puteţi începe protejarea securităţii datelor pe care le furnizează.

Pas 5: Porniţi aplicaţia în modul SSL

După ce terminaţi procesul de importare şi asignare a certificatului către aplicaţia dvs., s-ar putea să trebuiască să terminaţi şi să reporniţi aplicaţia în modul SSL. Acest lucru e necesar în unele cazuri deoarece s-ar putea ca aplicaţia să nu poată să determine că asignarea certificatului există în timp ce aplicaţia se execută. Revedeţi documentaţia pentru aplicaţia dvs. pentru a determina dacă aveţi nevoie să restartaţi aplicaţia sau pentru alte informaţii despre pornirea aplicaţiei în modul SSL.

Pasul opţional 6: Definiţi o listă de încredere CA pentru o aplicaţie care necesită certificate pentru autentificarea unui client

Aplicaţiile care suportă folosirea certificatelor pentru autentificare client în timpul unei sesiuni Secure Sockets Layer (SSL) trebuie să determine dacă vor accepta sau nu un certificat ca probă validă a identităţii. Unul dintre criteriile pe care le foloseşte o aplicaţie pentru autentificarea unui certificat este dacă aceasta are încredere în CA (autoritatea de certificare) care a emis certificatul.

Situaţia pe care o descrie acest scenariu nu necesită ca aplicaţia de calcul a ratei să folosească certificate pentru autentificarea unui client. Multe aplicaţii furnizează suport pentru certificate de autentificare a unui client; cum configuraţi acest suport depinde de la aplicaţie la aplicaţie. Acest task opţional este furnizat pentru a vă ajuta să înţelegeţi cum să folosiţi DCM pentru a activa încrederea în use pentru autentificarea clientului ca un fundament pentru configurarea suportului aplicaţiei dumneavoastră pentru certificate de autentificare a clientului.

Înainte de a se putea defini o listă de încredere CA pentru o aplicaţie, trebuie să fie îndeplinite mai multe condiţii:

- Aplicaţia trebuie să suporte utilizarea certificatelor pentru autentificare client.
- Definiţia DCM pentru aplicaţie trebuie să specifice că aplicaţia foloseşte o listă de încredere CA.

Dacă definiţia pentru o aplicaţie specifică faptul că o aplicaţie foloseşte o listă de încredere CA, trebuie să definiţi lista înainte ca aplicaţia să poată efectua cu succes autentificarea client a certificatului. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Pentru a folosi DCM să definiţi o listă de încredere CA pentru aplicaţia dvs., urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare, alegeţi **Selecţia unui depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apăsaţi **Continuare**.
4. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Setare stare CA** pentru a afişa o listă de certificate CA.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
6. Selectaţi din listă certificatul CA în care ar trebui să aibă încredere aplicaţia dvs. şi apăsaţi **Activare** pentru a afişa o listă de aplicaţii care folosesc o listă de încredere CA.
7. Selectaţi din listă aplicaţia care ar trebui să adauge CA-ul selectat la lista sa de încredere şi apăsaţi **OK**. Apare un mesaj la începutul paginii pentru a indica faptul că aplicaţiile pe care le-aţi selectat vor avea încredere în CA şi în certificatele pe care le emite.

Acum puteţi să vă configuraţi aplicaţia să ceară certificate pentru autentificarea unui client. Urmaţi instrucţiunile furnizate de documentaţie pentru aplicaţia dvs.

Scenariu: Folosirea certificatelor pentru a proteja accesul la aplicaţii şi resurse interne

Situaţie

Sunteţi administratorul de reţea pentru o companie (MyCo., Inc.) al cărei departament de resurse umane este preocupat cu probleme precum chestiuni legale şi securitatea înregistrărilor. Angajaţii companiei au cerut să poată accesa online informaţiile despre beneficiile lor personale şi sănătate. Compania a răspuns la această cerere prin crearea unui site web intern pentru a furniza aceste informaţii către angajaţi. Dvs. sunteţi responsabil pentru administrarea acestui site web intern.

Deoarece angajaţii sunt situaţi în două birouri separate geografic şi unii angajaţi călătoresc frecvent, dvs. sunteţi preocupat de păstrarea acestor informaţii private la transportul lor prin Internet. De asemenea, dvs. folosiţi în mod tradiţional autentificarea prin nume de utilizator şi parolă pentru a limita accesul la datele companiei. Datorită naturii sensibile şi private a acestor date, realizaţi că limitarea accesului la ele pe baza parolelor ar putea să nu fie suficient. La urma urmei, oamenii pot partaja, pot uita şi chiar fura parole.

După unele cercetări, vă hotărâţi că folosirea de certificate digitale poate furniza securitatea de care aveţi nevoie. Folosirea certificatelor vă permite să folosiţi Secure Sockets Layer (SSL) pentru a proteja transmisia datelor. În plus, puteţi folosi certificate în locul parolelor pentru autentificarea mai sigură a utilizatorilor şi pentru limitarea informaţiilor despre resurse umane pe care le pot accesa ei.

De aceea, vă hotărâţi să setaţi o Autoritate de Certificare (CA) Locală privată şi să emiteţi certificate către toţi angajaţii şi să îi puneţi să asocieze certificatele lor cu profilele lor utilizator iSeries. Acest tip de implementare a certificatelor private vă permite să controlaţi mai strâns accesul la date sensibile, precum şi să controlaţi securitatea datelor prin folosirea SSL. În ultimă instanţă, prin emiterea de către dvs. a certificatelor, măriţi probabilitatea ca datele să rămână sigure şi să fie accesibile doar unor utilizatori individuali specifici.

Avantajele scenariului

Acest scenariu are următoarele avantaje:
- Folosirea de certificate digitale pentru a configura accesul SSL la serverul web dvs. de resurse umane asigură că informaţiile transmise între server şi client este protejată şi privată.
- Folosirea de certificate digitale pentru autentificarea clienţilor furnizează o metodă mai sigură de identificare a utilizatorilor autorizaţi.
- Folosirea de certificate digitale *private* pentru a limita sau pentru a permite accesul la aplicaţiile şi datele dvs. este o alegere practică în aceste condiţii sau în condiţii similare:
  - Necesitaţi un grad înalt de securitate, în special în ceea ce priveşte autentificarea utilizatorilor.
  - Aveţi încredere în persoanele către care acordaţi (lansaţi) certificate.
  - Utilizatorii au deja profile de utilizator iSeries pentru a controla accesul la aplicaţii şi date.
  - Dvs. doriţi să operaţi asupra propriului Certificate Authority (CA).
- Folosirea de certificate private pentru autentificarea clienţilor vă permite să asociaţi mai uşor certificatul cu profilul utilizator iSeries al utilizatorului autorizat. Această asociere a unui certificat cu un profil utilizator permite Serverului HTTP să determine profilul utilizator al proprietarului certificatului în timpul autentificării. Serverul HTTP poate apoi să ruleze sub acel profil utilizator sau să efectueze acţiuni pentru acel utilizator pe baza informaţiilor din profilul utilizator.

Obiective

În acest scenariu, MyCo., Inc. doreşte să folosească certificate digitale pentru a proteja informaţiile personale sensibile pe care le furnizează site-ul lor web intern de resurse umane către angajaţii companiei. Compania doreşte de asemenea o metodă mai sigură de autentificare a acelor utilizatori cărora le este permis accesul la acest web site.

Obiectivele acestui scenariu sunt următoarele:
- Site-ul web intern de resurse umane al companiei trebuie să folosească SSL pentru a proteja securitatea datelor pe care le furnizează utilizatorilor.
- Configurarea SSL trebuie să fie realizată cu certificate private de la un CA local intern.
- Utilizatorii autorizaţi trebuie să furnizeze un certificat valid pentru a accesa site-ul web de resurse umane în modul SSL.

Detalii

Următoarea figură ilustrează situaţia de configurare a reţelei pentru acest scenariu:

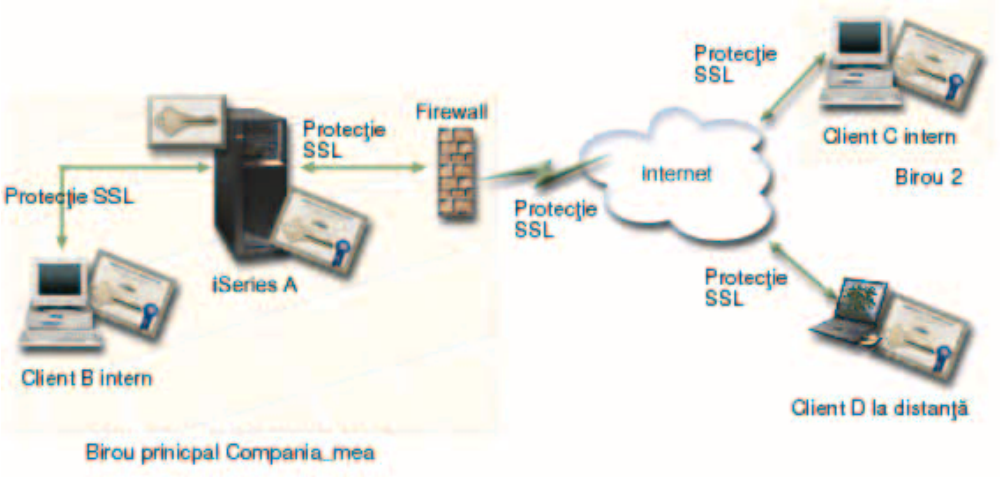


Figura ilustrează următoarele informaţii despre situaţia pentru acest scenariu:

Serverul web de resurse umane al companiei – iSeries A

- iSeries A este serverul care găzduieşte aplicaţia de resurse umane bazată pe web a companiei.
- iSeries A rulează OS/400 Version 5 Release 2 (V5R2).
- iSeries A are instalat un furnizor de acces criptografic (5722–AC3).
- iSeries A are instalate şi configurate Digital Certificate Manager (OS/400 opţiunea 34) şi IBM Server HTTP pentru iSeries (5722–DG1).
- iSeries A rulează aplicaţia de resurse umane, care este configurată astfel încât:
  - Necesită modul SSL.
  - Foloseşte un certificat privat de la o Autoritate certificare bine cunoscută (CA) pentru configurarea SSL.
  - Necesită certificate pentru autentificarea clienţilor.
- iSeries A îşi prezintă certificatul pentru a iniţia o sesiune SSL când Clienţii B, C şi D accesează aplicaţia.
- După iniţializarea sesiunii SSL, iSeries A cere ca Clienţii B, C şi D să furnizeze un certificat valid înainte de a permite accesul la aplicaţia de resurse umane. Acest schimb de certificate este transparent utilizatorilor Clienţilor B, C şi D.

Sisteme client angajaţi – Client B, Client C şi Client D

- Client B este un angajat care lucrează biroul principal din MyCo’s unde se află iSeries A.
- Client C este un angajat care lucrează biroul secundar din MyCo’s care este geografic separat de biroul principal.
- Client D este un angajat care lucrează de la distanţă şi călătoreşte frecvent cu afacerile companiei şi trebuie să poată accesa în siguranţă site-ul web de resurse umane indiferent de locaţia fizică.
- Clienţii B, C şi D sunt angajaţii companiei care accesează aplicaţia de resurse umane.
- Clienţii B, C şi D au toţi o copie a certificatului CA local care a emis certificatul aplicaţiei instalat în software-ul lor client.
- Clienţii B, C şi D accesează aplicaţia de resurse umane de pe iSeries A, care îşi prezintă certificatul către software-ul lor client pentru a-i verifica identitatea şi a iniţia o sesiune SSL.
- Software-ul client de pe Clienţii B, C şi D este configurat să accepte certificatul de la iSeries A şi sesiunea SSL începe.
- După ce sesiunea SSL începe, Clienţii B, C şi D trebuie să furnizeze un certificat valid înainte ca iSeries A să permită accesul la aplicaţie şi la resursele ei.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:

1. IBM Serverul HTTP pentru iSeries rulează aplicaţia de resurse umane de pe iSeries A. Există două tipuri de Servere HTTP pentru iSeries (originală şi motorizată de Apache) şi o versiune revizuită semnificant a Serverului HTTP va fi disponibilă după publicarea acestei informaţii. În consecinţă, acest scenariu nu furnizează instrucţiuni *specifice* pentru configurarea Serverului HTTP să folosească SSL. Acest scenariu furnizează instrucţiuni pentru configurarea şi gestionarea certificatelor care sunt necesare pentru ca orice aplicaţie să folosească SSL.
2. Serverul HTTP poate avea capabilitatea de a cere certificate pentru autentificarea unui client. Acest scenariu furnizează instrucţiuni despre cum să folosiţi Digital Certificate Manager (DCM) pentru a configura cerinţele de gestionare a certificatelor pentru acest scenariu. Totuşi, acest scenariu nu furnizează *anumiţi* paşi de configurare pentru configurarea autentificării unui client prin certificate pentru Serverul HTTP.
3. Serverul HTTP de resurse umane de pe iSeries A deja foloseşte protecţie prin parolă.
4. iSeries A îndeplineşte cerinţele pentru instalarea şi folosirea Digital Certificate Manager (DCM).
5. Nimeni nu a configurat sau folosit anterior DCM pe iSeries A.
6. Oricine foloseşte DCM pentru a realiza taskurile din acest scenariu trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilele lor de utilizator.
7. iSeries A nu are instalat un Coprocesor Criptografic IBM 4758-023 PCI.

Paşii task-ului

Există două seturi de taskuri pe care trebuie să le efectuaţi pentru a implementa acest scenariu: Un set de taskuri vă permite să setaţi aplicaţia de resurse umane de pe iSeries A să folosească SSL şi să ceară certificate pentru autentificarea unui utilizator. Celălalt set de taskuri permite utilizatorilor dvs. de pe Clienţii B, C şi D să participe în sesiunile SSL cu aplicaţia de resurse umane şi să obţină certificate pentru autentificarea utilizatorilor.

Paşii taskului aplicaţiei server web de resurse umane

Pentru a implementa acest scenariu, trebuie să realizaţi aceste taskuri pe iSeries A:

1. Efectuaţi toţi paşii cerinţelor preliminare pentru a instala şi configura toate produsele iSeries necesare.
2. Configuraţi-vă serverul HTTP de resurse umane să folosească SSL şi notaţi ID-ul aplicaţiei pentru instanţa serverului.
3. Folosiţi Digital Certificate Manager (DCM) pentru a crea şi opera un CA local şi folosiţi-l pentru a emite un certificat pentru serverul HTTP de resurse umane. Acest task asistat asigură de asemenea că dvs. asignaţi certificatul către aplicaţia de pe serverul web şi adăugaţi CA-ul la lista acelora în care are încredere aplicaţia.
4. Configuraţi-vă serverul web de resurse umane să ceară certificate pentru autentificarea clienţilor.
5. Porniţi Serverul HTTP de resurse umane în modul SSL.

Paşii taskului de configurare a clientului

Pentru a implementa acest scenariu, fiecare utilizator (Clienţii B, C şi D) care vor accesa serverul web de resurse umane de pe iSeries A trebuie să realizeze aceste taskuri:

6. Instalaţi o copie a certificatului CA local din browser-ul lor.
7. Cereţi un certificat de la CA local.

Detalii de configurare

Efectuaţi următorii paşi ai taskului pentru a folosi certificatele pentru configurarea accesului protejat la aplicaţii şi resurse interne după cum descrie acest scenariu.

Pas 1: Efectuaţi taskurile cerinţelor preliminare pentru a instala toate produsele iSeries necesare

Trebuie să efectuaţi toate taskurile cerinţelor preliminare pentru a instala şi configura toate produsele iSeries necesare înainte să puteţi realiza anumite taskuri de configurare pentru implementarea acestui scenariu.

Pas 2: Configuraţi Serverul HTTP de resurse umane să folosească SSL

Paşii de configurare SSL pentru Serverul HTTP de resurse umane de pe iSeries A variază în funcţie de situaţia în care folosiţi originalul sau versiunea motorizată de Apache.

Pentru informaţii specifice despre configurarea Serverului HTTP (original) să folosească SSL, vedeţi Configurarea unui server sigur pe Serverul HTTP.

Pentru informaţii specifice despre configurarea Serverului HTTP (administrat de Apache) să folosească SSL, vedeţi Scenariu: JKL activează protecţia SSL pe Serverul lor HTTP (administrat de Apache). Acest scenariu furnizează toţi paşii taskului pentru crearea unei gazde virtuale şi configurarea ei să folosească SSL. Pentru paşii specifici de configurare SSL, vedeţi titlul ″Activare SSL pentru o gazdă virtuală.″

Pentru informaţii suplimentare despre configurarea atât versiunilor curentă cât şi viitoare a Serverului HTTP pentru iSeries (original sau administrat de Apache), vedeţi subiectul Servicii Web.

Pas 3: Creaţi şi operaţi un CA local

După ce aţi configurat Serverul HTTP de resurse umane să folosească SSL, trebuie să configuraţi un certificat pe care să îl folosească serverul pentru a iniţia SSL. În funcţie de obiectivele pentru acest scenariu, aţi ales să creaţi şi să operaţi un CA local să emită un certificat către server.

Când folosiţi DCM pentru a crea un CA local, sunteţi îndrumat printr-un proces care se asigură că configuraţi tot ce aveţi nevoie pentru a activa SSL pentru aplicaţia dvs. Aceasta include asignarea certificatului pe care CA local îl emite către aplicaţia de pe serverul dvs. web. De asemenea, adăugaţi CA local la lista de încredere CA a aplicaţiei de pe serverul web. Având un CA local în lista de încredere a aplicaţiei asigură că aplicaţia poate recunoaşte şi autentifica utilizatori care prezintă certificate pe care le emite CA local.

Pentru a folosi DCM pentru a crea şi opera un CA local şi emite un certificat către aplicaţia de pe serverul dvs. de resurse umane, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al DCM, selectaţi **Crearea unei Autorităţi de certificare (CA)** pentru a se afişa o serie de formulare. Aceste formulare vă îndrumă prin procesul creării unui CA local şi completării altor taskuri necesare pentru a începe folosirea certificatelro digitale pentru SSL, semanrea obiectelor şi verificarea semnăturii.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.

3. Completaţi formularele pentru acest task asistat. În folosirea aceste formulare pentru a realiza toate taskurile de care aveţi nevoie pentru a seta un CA local care funcţionează, duumneavoastră:
   a. Furnizaţi informaţiile de identificare pentru CA local.
   b. Instalaţi certificatul CA local pe PC-ul dvs. sau în browserul dvs. astfel încât software-ul dvs. să poată recunoaşte CA local şi să valideze certificatele pe care le emite CA local.
   c. Alegeţi datele politicii pentru CA-ul dvs. Local.

      Notă: Asiguraţi-vă că selectaţi ca CA local să poată emite certificate utilizator.
   d. Folosiţi noul CA local pentru a emite un certificat server sau client pe care aplicaţiile dvs. să îl poată folosi pentru conexiuni SSL.
   e. Selectaţi aplicaţiile care pot folosi certificatul client sau server pentru conexiuni SSL.

      Notă: Asiguraţi-vă că selectaţi ID-ul aplicaţiei pentru Serverul HTTP de resurse umane al dvs.
   f. Folosiţi noul CA local pentru a emite un certificat de semnare obiect pe care aplicaţiile să îl poată folosi pentru a semna digital obiecte. Acest subtask crează depozitul de certificate *OBJECTSIGNING; acesta este depozitul de certificate pe care îl folosiţi pentru a gestiona certificate care semnează obiecte.

      Notă: Deşi acest scenariu nu foloseşte certificate de semnare obiect, asiguraţi-vă că realizaţi acest pas. Dacă anulaţi în acest moment din task, taskul se termină şi dvs. trebuie să realizaţi taskuri separate pentru a completa configurarea certificatelor dvs. SSL.
   g. Selectaţi aplicaţiile care ar trebui să aibă încredere în CA local.

      Notă: Asiguraţi-vă că selectaţi ID-ul aplicaţiei pentru Serverul HTTP de resurse umane al dvs. ca una din aplicaţiile care are încredere în CA local.

Acum că aţi completat configurarea certificatului pe care îl cere aplicaţia de pe serverul dvs. web pentru a folosi SSL, puteţi configura aplicaţia de pe serverul web să ceară certificate pentru autentificarea utilizatorilor.

Pas 4: Configuraţi serverul web de resurse umane să ceară certificate pentru autentificarea clienţilor

Paşii de configurare SSL pentru cererea de certificate pentru autentificarea clienţilor pentru Serverul HTTP de resurse umane de pe iSeries A variază în funcţie de situaţia în care folosiţi originalul sau versiunea motorizată de Apache a aplicaţiei.

Pentru informaţii mai specifice despre configurarea Serverului HTTP (original) să ceară certificate pentru autentificarea clienţilor, vedeţi Creare setări de protecţie pe Serverul HTTP (original).

Pentru informaţii specifice despre configurarea Serverului HTTP (administrat de Apache) să folosească certificate pentru autentificarea clienţilor, vedeţi Scenariu: JKL activează protecţia SSL pe Serverul lor HTTP (administrat de Apache). Acest scenariu pentru Serverul HTTP furnizează toţi paşii taskului pentru crearea unei gazde virtuale şi configurarea ei să folosească SSL şi certificate pentru autentificarea clienţilor. Pentru paşii specifici de configurare SSL şi certificate pentru autentificarea clienţilor, vedeţi titlul ″Activare SSL pentru o gazdă virtuală.″

Pentru informaţii suplimentare despre configurarea atât versiunilor curentă cât şi viitoare a Serverului HTTP pentru iSeries (original sau administrat de Apache), vedeţi subiectul Servicii Web.

Pas 5: Porniţi serverul web de resurse umane în modul SSL

S-ar putea să fie nevoie să opriţi şi să reporniţi Serverul dvs. HTTP pentru a asigura că serverul poate să determine că asignarea certificatului există şi să îl folosească pentru a iniţia sesiuni SSL.

Pentru a opri şi porni Serverul HTTP (original), folosiţi formularele de configurare şi administrare şi urmaţi aceşti paşi:

1. Apăsaţi **Administrare**.
2. Apăsaţi **Gestiune servere HTTP**.
3. Selectaţi serverul.
4. Introduceţi parametrii de startup opţionali în câmpul care este furnizat în formular.
5. Selectaţi **Pornire**.

Notă: Dacă serverul rula când aţi făcut asignările de certificate, ar trebui să Opriţi, apoi Porniţi serverul. Apăsând pe **Repornire** nu asigură întotdeauna că serverul poate să determine orice schimbare de certificat care a apărut în timp ce rula..

Pentru a opri şi porni Serverul HTTP (administrat de Apache), folosiţi formularele de configurare şi administrare şi urmaţi aceşti paşi:

1. Apăsaţi **Administrare**.
2. În meniul din stânga, apăsaţi **Gestiune Servere HTTP** din **Administrare generală server**.
3. Selectaţi serverul cu care doriţi să lucraţi, apoi apăsaţi **Pornire** sau **Oprire**. Căutaţi în ajutorul online mai multe informaţii despre parametrii de pornire.

Pentru informaţii suplimentare despre gestionarea versiunilor curentă şi viitoare a Serverului HTTP pentru iSeries (original sau administrat de Apache), vedeţi subiectul Servicii Web.

Cu aceste taskuri completate, vă puteţi porni aplicaţia de resurse umane în modul SSL şi puteţi începe protejarea securităţii datelor pe care le furnizează.

Pas 6: Puneţi-vă utilizatorii să instaleze o copie a certificatului CA local din browser-ul lor.

Când utilizatorii accesează un server care furnizează o conexiune SSL, serverul prezintă un certificat către software-ul client al utilizatorului ca dovadă a identităţii sale. Software-ul client trebuie să valideze apoi certificatul server înainte ca serverul să poată stabili sesiunea. Pentru a valida certificatul server, software-ul client trebuie să aibă acces la o copie memorată local a certificatului pentru CA care a emis certificatul server. Dacă serverul prezintă un certificat de la un CA Internet public, browserul utilizatorului sau alt software client ar trebui să aibă deja o copie a certificatului CA. În cazul în care, ca în acest scenariu, serverul prezintă un certificat de la un CA local privat, fiecare utilizator trebuie să folosească Digital Certificate Manager (DCM) pentru a instala o copie a certificatului CA local.

Fiecare utilizator (Clienţii B, C şi D) trebuie să facă aceşti paşi pentru a obţine o copie a certificatului CA local:

1. Pornire DCM.
2. În cadrul de navigare, selectaţi **Instalare certificat CA local pe PC-ul dumneavoastră** pentru a afişa o pagină care vă permite să descărcaţi certificatul CA local în browserul dumneavoastră sau să-l memoraţi într-un fişier pe sistemul dumneavoastră.
3. Selectaţi opţiunea de instalare a certificatului. Această opţiune descarcă certificatul CA local ca o rădăcină de încredere în browser-ul dvs. Aceasta asigură că browser-ul dvs.

poate stabili sesiuni de comunicaţii sigure cu serverele web care folosesc un certificat de la acest CA. Browser-ul va afişa o serie de ferestre care vă vor ajuta să terminaţi instalarea.

4. Apăsaţi **OK** pentru a reveni la pagina de bază (home) a Digital Certificate Manager.

Pas 7: Puneţi fiecare utilizator să ceară un certificat de la CA local

În paşii anteriori, aţi configurat serverul web de resurse umane să ceară certificate pentru autentificarea utilizatorilor. Acum utilizatorii trebuie să prezinte un certificat valid de la CA local înainte să li se permită să acceseze serverul web. Fiecare utilizator trebuie să folosească DCM pentru a obţine un certificat folosind taskul **Creare Certificat**. Pentru a obţine un certificat de la CA local, politica CA local trebuie să permită CA să emită certificate utilizator.

Fiecare utilizator (Clienţii B, C şi D) trebuie să urmeze aceşti paşi pentru a obţine un certificat:

1. Pornire DCM.
2. În cadrul de navigare, selectaţi **Crearea certificatelor**.
3. Selectaţi **Certificate utilizator** pentru tipul certificatului pe care îl creaţi. Se va afişa un formular în care veţi putea introduce informaţii de identificare pentru certificat.
4. Completaţi formularul şi apăsaţi **Continuare**.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
5. În acest punct, DCM lucrează cu browser-ul pentru a crea cheile private şi publice pentru certificate. Browserul poate afişa mai multe ferestre pentru a vă ghida prin acest proces. Se urmează instrucţiunile browserului pentru aceste procese. După ce browser-ul generează cheile, se va afişa o pagină de confirmare care va indica faptul că DCM-ul a creat certificatele.
6. Instalaţi noul certificat în browser-ul dumneavoastră. Browserul poate afişa mai multe ferestre pentru a vă ghida prin acest proces. Urmaţi instrucţiunile date de browser pentru a termina acest task.
7. Apăsaţi **OK** pentru a termina taskul.

În timpul prelucrării, Digital Certificate Manager asociază automat certificatul cu profilul de utilizator iSeries.

Capitol 5. Concepte de certificate digitale

Înainte să începeţi să folosiţi certificate digitale pentru mărirea politicii de securitatea a sistemului şi a reţelei, ar trebui să înţelegeţi ce sunt acestea şi ce avantaje de securitate oferă.

Un certificat digital este un credential digital care validează identitatea proprietarului certificatului, cum o face un paşaport. O parte de încredere, numită o Autoritate certificare (CA) emite certificate digitale utilizatorilor şi aplicaţiilor server sau client. Încrederea în CA stă la baza încrederii în certificat ca o scrisoare de acreditare validă.

Pentru a afla mai multe despre conceptele de certificate digitale, revedeţi aceste subiecte:

Numele distinctiv
Citiţi această informaţie pentru a afla mai multe despre caracteristicile de identificare a certificatelor digitale.

Semnături digitale
Citiţi această informaţie pentru a afla ce sunt semnăturile digitale şi cum funcţionează ele pentru a asigura integritatea obiectului.

Perechea de chei publică-privată
Citiţi această informaţie pentru a afla mai multe despre cheile de securitate asociate cu certificatele digitale.

Certificate Authority (CA)
Citiţi aceste informaţii pentru a afla mai multe despre CA-uri, entităţile care emit certificate digitale.

Locaţii CRL
Citiţi aceste informaţii pentru a afla ce sunt CRL-urile (listele de revocare a certificatelor) şi cum sunt ele folosite în procesul de validare şi de autentificare a certificatelor.

Stocarea certificatelor
Citiţi aceste informaţii pentru a ala ce sunt depozitele de certificate şi cum să folosiţi DCM (Digital Certificate Manager) pentru a lucra cu ele şi cu certificatele pe care le conţin.

Criptografierea
Citiţi aceste informaţii pentru a afla ce este criptografia şi cum folosesc certificatele digitale funcţiile criptografice pentru a oferi securitate.

Secure Sockets Layer (SSL)
Citiţi această informaţie pentru o descriere scurtă a SSL.

Numele distinctiv

Fiecare CA are o politică pentru a hotărî informaţiile de identificare pe care le solicita CA pentru a emite un certificat. Anumite Autorităţi de certificare Internet pot cere puţine informaţii, cum ar fi un nume si o adresă de mail. Alte CA-uri publice pot cere mai multe informaţii şi să necesite o dovadă mai strictă decât informaţiile de identificare înainte de a emite un certificat. De exemplu, CA-urile care suportă standardurile PKIX (schimb de infrastructură a cheilor), pot cere ca cel care cere să îşi verifice identitatea printr-un RA (autoritate de înregistrare) înainte de a emite certificatul. În consecinţă, dacă aveţi de gând să acceptaţi şi să folosiţi certificate şi credenţiale, trebuie să revedeţi cerinţele de identificare pentru o CA pentru a determina dacă cerinţele ei se potrivesc cu nevoile dvs. de securitate.

DN (nume distinct) este un termen care descrie informaţiile de identificare a proprietarului certificatului şi este o partea a certificatului. În funcţie de politica de identificare a CA care emite certificatul, DN-ul (numele distinct) poate include o varietate de informaţii. Puteţi folosi

DCM (Digital Certificate Manager) pentru a opera o Autoritate de certificare privată şi pentru a emite certificate private. De asemenea, puteţi folosi DCM pentru a genera informaţiile DN şi perechea de chei pentru certificatul pe care o CA publică Internet îl emite pentru organizaţia Dvs.. Informaţiile DN pe care le puteţi furniza pentru unul dintre tipurile de certificate includ:
- Numele comun al deţinătorului certificatului.
- Organizaţia
- Unitatea organizaţională
- Oraşul
- Statul
- Ţara

Atunci când folosiţi DCM pentru a emite certificate private, puteţi furniza informaţii DN suplimentare pentru certificat, incluzând:
- Adresă de IP versiuna 4
- Numele complet calificat al domeniului
- Adresa de e-mail

Această informaţie adiţională este folositoare dacă aveţi de gând să folosiţi certificatul pentru a configura o conexiune pe o reţea privată virtuală (VPN).

Semnături digitale

O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme de criptografie şi este echivalentă cu o o semnătură personală pe un document scris. O semnătură digitală furnizează dovada originii obiectului şi un mijloc prin care să fie verificată integritatea obiectului. Un proprietar de certificat digital ″semnează″ un obiect prin folosirea cheii private a certificatului. Destinatarul obiectului foloseşte cheia publică corespunzătoare a certificatului pentru a decripta semnătura, care verifică integritatea obiectului semnat ca şi emitentul ca sursă.

O Autoritate certificare (CA) semnează certificatele pe care le emite. Această semnătură este compusă dintr-un şir de date care este criptat cu cheia privată a Autorităţii de certificare. Orice utilizator poate să verifice semnătura de pe certificat utilizând cheia publică a Autorităţii de certificare pentru a decripta semnătura.

O semnătură digitală este o semnătură electronică pe care dvs. sau o aplicaţie o creaţi pe un obiect prin folosirea unei chei private a unui certificat digital. Semnătura digitală pe un obiect furnizează o legare electronică unică a identităţii semnatarului (proprietarul cehii de semnare) de originea obiectului. Când accesaţi un obiect care conţine o semnătură digitală, puteţi verifica semnătura de pe obiect pentru a verifica sursa obiectului ca validă (de exemplu, că o aplicaţie pe care o descărcaţi chiar vine de la o sursă autorizată cum este IBM). Acest proces de verificare vă permite de asemenea să determinaţi dacă au fost făcute modificări neautorizate asupra obiectului de când a fost semnat.

Un exemplu de cum funcţionează o semnătură digitală

Un dezvoltator de software a creat o aplicaţie iSeries pe care el doreşte să o distribuie pe Internet ca o măsură convenabilă şi ieftină pentru clienţii săi. Totuşi, el ştie că clienţii sunt pe bună dreptate îngrijoraţi de descărcarea programului de pe Internet datorită crescândelor probleme a obiectelor care se dau drept programe legitime dar de fapt conţin programe distructive, cum sunt viruşii.

În consecinţă, el decide să semneze digital aplicaţia astfel încât clienţii săi să poată face verificarea că compania lui este sursa legitimă a aplicaţiei. El foloseşte cheia privată de la un certificat digital pe care l-a obţinut de la un CA public bine-cunoscut pentru a semna aplicaţia. Apoi îl face disponibil de descărcat pentru clienţii săi. Ca parte a pachetului de descărcat, el

include o copie a certificatului digital pe care l-a folosit pentru a semna obiectul. Când un client descarcă pachetul cu aplicaţia, clientul poate folosi cheia publică a certificatului pentru a verifica semnătura de pe aplicaţie. Acest proces permite clientului să identifice şi să verifice sursa aplicaţiei, cât şi să se asigure că conţinutul obiectului aplicaţie nu a fost alterat de când a fost semnat.

Perechea de chei publică-privată

Fiecare certificat digital are o pereche de chei criptografice asociate. Această pereche de chei constă dintr-o cheie publică şi o cheie privată. (Certificatele care verifică semnătura sunt o excepţie de la această regulă şi au sociată doar o cheie publică.)

O cheie publică este o parte a certificatului digital al proprietarului şi este disponibilă pentru ca oricine să o folosească. Totuşi, o cheie privată este protejată şi este doar la îndemâna proprietarului acesteia. Acest acces limitat asigură siguranţa comunicării prin chei.

Proprietarul unui certificat poate folosi aceste chei pentru a profita de caracteristicile de securitate criptografică pe care le furnizează cheile. De exemplu, proprietarul certificatului poate folosi o cheie privată a certificatului pentru a ″semna″ şi cripta datele trimise între utilizatori şi servere, cum sunt mesajele, documentel şi obiectele codate. Receptorul obiectului semnat poate apoi să folosească cheia publică conţinută în certificatul semnatarului pentru a decripta semnătura. Asemenea semnături digitale asigură încrederea originii unui obiect şi furnizează un mijloc de verificare a integrităţii obiectului.

Certificate Authority (CA)

Autoritatea de certificare (CA) este o entitate administrativă centrală de încredere care poate emite certificate digitale utilizatorilor şi serverelor. Încrederea în CA stă la baza încrederii în certificat ca o scrisoare de acreditare validă. O CA foloseşte propria cheie privată pentru a crea o semnătură digitală pe certificatul emis pentru a certifica originea autentificărilor . Cheia publică a certificatului CA poate fi utilizată de alţii pentru a se verifica autenticitatea certificatelor pe care le emite şi semnează CA.

O CA poate fi o entitate comercială publică, aşa cum e VeriSign, sau poate fi o entitate privată pe care operează o organizaţie în scopuri interne. Anumite firme furnizează servicii de Certificate Authority pentru utilizatorii Internet. DCM vă permite să gestionaţi certificatele provenite de la CA-uri publice sau private.

De asemenea, puteţi folosi DCM pentru a opera propria CA privată care să emită certificate private sistemelor şi utilizatorilor. Când CA emite un certificat utilizator, DCM automat asociază certificatul cu profilul utilizator al sistemului iSeries al utilizatorului. Aceasta asigura că drepturile de acces si autorizările pentru certificat sunt aceleasi ca ale deţinatorului profilului utilizator

Stare rădăcină de încredere

Termenul rădăcină de încredere se referă la o desemnare specială dată unui certificat Autoritate de certificare. Această desemnare rădăcină de încredere permite unui browser sau unei alte aplicaţii să autentifice şi să accepte certificate emise de CA (autoritate de certificare).

Când se procură un certificat al Autorităţii de certificare în propriul browser, acesta vă permite să îl desemnaţi drept rădăcină de încredere. Alte aplicaţii care suportă folosirea certificatelor trebuie să fie de asemenea configurate să aibă încredere în CA înainte ca această aplicaţie să poată autentifica şi să aibă încredere în certificatele emise de o CA specială.

Puteţi folosi DCM pentru a activa sau a dezactiva starea de încredere a unei CA (autorităţi de certificare) din depozitul de certificate. Atunci când activaţi un certificat CA, puteţi specifica faptul că aplicaţiile îl pot utiliza pentru a autentifica şi accepta certificatele emise de CA. Când dezactivaţi un certificat CA, nu puteţi specifica faptul că aplicaţiile îl pot utiliza pentru a autentifica şi accepta certificatele emise de CA.

Date de politică Autoritate de certificare

Când creaţi o Autoritate de certificare (CA) cu DCM, puteţi specifica datele politicii pentru CA. Datele politicii pentru o CA descriu privilegiile de semnare pe care le deţine aceasta. Datele politicii determină:
- Dacă CA poate emite şi semna certificate utilizator.
- Cât timp certificatele lansate de CA rămân valide.

Locaţii CRL (listă de revocare a certificatelor)

O listă de revocare a certificatelor (CRL) este un fişier care conţine informaţii despre toate certificatele invalide şi revocate pentru o Autoritate de certificare (CA) specifică. CA-urile actualizează periodic CRL-urile lor şi le fac disponibile şi altora pentru ca aceştia să le publice în directoarele Lightweight Directory Access Protocol (LDAP). Puţine CA-uri, cum ar fi SSH în Finlanda, îşi publică singure CRL-urile în directoarele LDAP pe care le puteţi accesa direct. Dacă o CA îşi publică propria CRL, certificatul indică acest lucru incluzând o extensie punct distribuţie CRL în formularul Uniform Resource Identifier (URI - identificator resursă uniform).

Digital Certificate Manager (DCM) vă permite să definiţi şi să gestionaţi informaţiile despre locaţiile CRL pentru a asigura o autentificare mai stringentă pentru certificatele pe care le folosiţi sau le acceptaţi de la alţii. O definiţie locaţie CRL descrie locaţia unui, şi informaţiile de acces pentru server-ul Lightweight Directory Access Protocol (LDAP) care păstrează CRL-ul.

Aplicaţiile care efectuează autentificarea certificatelor accesează locaţia CRL, dacă este definită una, pentru o CA specifică pentru a se asigura că aceasta nu a revocat un anume certificat. DCM vă permite să definiţi şi să gestionaţi informaţiile despre locaţia CRL de care au nevoie aplicaţiile pentru a efectua procesare CRL în timpul autentificării certificatului. Exemple de aplicaţii şi procese care pot efectua procesare CRL pentru autentificarea certificatelor: server-ul VPN (reţea privată virtuală) IKE (Internet Key Exchange - schimb de chei Internet), aplicaţiile-active Secure Sockets Layer (SSL) şi procesele care semnează aplicaţii. De asemenea, atunci când definiţi locaţii CRL şi le asociaţi cu un certificat CA, DCM efectuează procesarea CRL ca parte a procesului de validare pentru certificatele pe care le emite CA specificată. .

Stocarea certificatelor

Un depozit de certificate este un fişier bază de date cheie special pe care DCM îl foloseşte pentru a memora certificatele digitale. Depozitul de certificate de asemenea conţine cheia privată a certificatului dacă nu aţi ales în schimb să folosiţi un Coprocesor Criptografic 4758 pentru a memora cheia. DCM vă permite să creaţi şi să gestionaţi mai multe tipuri de depozite de certificate. DCM controlează accesul la depozitele de certificate prin parole împreună cu controlul accesului la catalogul IFS şi la fişierele IFS care constituie depozitul de certificate.

Depozitele de certificate sunt clasificate pe baza tipurilor de certificate pe care le conţin. Task-urile de management pe care le puteţi efectua pentru fiecare depozit de certificate variază în funcţie de tipul certificatului pe care îl conţine depozitul de certificate. DCM furnizează următoarele depozite de certificate predefinite pe care le puteţi crea şi gestiona:

Autoritatea certificare locală (CA)
DCM foloseşte acest depozit de certificate pentru a păstra certificatul CA local şi cheia sa privată dacă dvs. creaţi o CA locală. Puteţi folosi certificatul din aceste depozit de certificare pentru a semna certificatele pe care le folosiţi pentru a le emite CA locală. Atunci când CA locală emite un certificat, DCM ca pune o copie a certificatului CA (fără cheia privată) în depozitul de certificate corespunzător (de exemplu, *SYSTEM) în scopuri de autentificare. Aplicaţiile folosec certificate CA pentru a verifica originea certificatelor pe care trebuie să le valideze ca parte a negocierilor SSL pentru a garanta autorizaţii pentru resurse.

***SYSTEM**
DCM furnizează depozitul de certificate pentru gestionarea certificatelor server sau client pe care le folosesc aplicaţiile pentru a participa la sesiuni de comunicare Secure Sockets Layer (SSL). Aplicaţiile IBM iSeries (şi multe alte aplicaţii ale dezvoltatorilor de software) sunt scrise pentru a folosi certificate doar în depozitul de certificate *SYSTEM. Când folosiţi DCM pentru a crea un CA local, DCM crează acest depozit de certificate ca parte a procesului. Când alegeţi să obţineţi certificate de la un CA public, cum sunt VeriSign, pentru ca aplicaţia dvs. server sau client să le folosească, trebuie să creaţi acest depozit de certificate.

***OBJECTSIGNING**
DCM furnizează acest depozit de certificate pentru gestionarea certificatelor pe care le folosiţi pentru a semna digital obiecte. De asemenea, taskurile din acest depozit de certificate vă permit să creaţi semnături digitale pe obiecte, cât şi să vizualizaţi şi să verificaţi semnăturile de pe obiecte. Când folosiţi DCM pentru a crea un CA local, DCM crează acest depozit de certificate ca parte a procesului. Când alegeţi să obţineţi certificate de la un CA public, cum sunt VeriSign, pentru semnarea obiectelor, trebuie să creaţi acest depozit de certificate.

***SIGNATUREVERIFICATION**
DVM furnizează acest depozit de certificate pentru gestionarea certificatelor pe care le folosiţi pentru a verifica autenticitatea semnăturilor digitale de pe obiecte. Pentru a verifica o semnătură digitală, acest depozit de certificate trebuie să conţină o copie a certificatului care a semnat obiectul. Depozitul de certificate trebuie să conţină de asemenea o copie a certificatului CA pentru CA-ul care a emis certificatul de semnat obiecte. Obţineţi aceste certificate fie exportând certificatele de semnat obiecte de pe sistemul curent în depozit, fie importând certificatele pe care le primiţi de la semnatarul obiectului.

Alt depozit de certificate sistem
Acest depozit de certificate oferă o locaţie alternativă de depozitare a certificatelor client sau server pe care le folosiţi pentru sesiuni SSL. Alte depozite de certificate sistem sunt depozite secundare de certificate definite de utilizatori pentru certificate SSL. Opţiunea Alte depozite de certificate sistem vă permite să gestionaţi certificate pentru aplicaţiile pe care dvs. sau alţii le scrieţi şi care folosesc API SSL_Init pentru a accesa şi a folosi programat un certificat pentru a stabili o sesiune SSL. Acest API permite unei aplicaţii să folosească mai repede certificatul implicit pentru un depozit de certificate decât certificatul identificat implicit. Mai des, folosiţi acest depozit de certificate atunci când transferaţi certificate de la o ediţie anterioară a DCM, sau când creaţi un subset special de certificate folosite pentru SSL.

Notă: Dacă aveţi un Coprocesor Criptografic 4758 PCI instalat pe serverul dvs. iSeries, puteţi alege alte opţiuni de stocare a cheilor private pentru certificatele dvs. (cu excepţia certificatelor de semnare a obiectelor). Puteţi alege să păstraţi cheia privată chiar pe coprocesor sau să îl folosiţi pe acesta pentru a cripta cheia privată şi să o păstraţi într-un fişier special cheie privată în loc de depozitul de certificate.

DCM controlează accesul la depozitele de certificate prin parole. De asemenea, DCM menţine controlul accesului la directoarele şi fişierele sistemului de fişiere integrat care constituie depozitele de certificate. Depozitele de certificate Autoritate de certificare (CA) locală, *SYSTEM, *OBJECTSIGNING şi *SIGNATUREVERIFICATION trebuie să fie localizate în căi specifice ale sistemului de fişiere integrat, iar Alte depozite de certificate sistem pot fi localizate oriunde în sistemul de fişiere integrat.

Criptografia

Criptografia este ştiinţa de a ţine datele în siguranţă. Criptografia vă permite stocarea de informaţii sau comunicarea cu terţi în timp ce preveniţi ca părţile neimplicate să înţeleagă informaţiile stocate sau să înţeleagă comunicaţia. Encriptarea transformă textul inteligibil într-unul neinteligibil (ciphertext). Decriptarea reface textul inteligibil din date cifrate. Ambele procese presupun o formulă matematică sau un algoritm şi o secvenţă secretă de date (cheia).

Sunt două tipuri de criptografieri:

- În criptografia **partajată sau cu cheie secretă (simetrică)**, o cheie este un secret partajat între două părţi în comunicare. Criptarea şi decriptarea folosesc aceeaşi cheie.
- În criptografia **cu cheie publică (asimetrică)** , criptarea şi decriptarea folosesc fiecare chei diferite. O grupare are o pereche de chei constând într-o cheie publică şi o cheie privată. Cheia publică este distribuită gratuit, de obicei în cadrul unui certificat digital, în timp ce cheia privată este ţinută în siguranţă de proprietar. Cele două chei sunt matematice, dar este virtual imposibil să derivaţi cheia privată din cheia publică. Un obiect, cum ar fi un mesaj care este criptat cu cheia publică a cuiva poate fi decriptat doar cu cheia asociată privată. Alternativ, un server sau utilizator poate folosi cheia privată pentru a ″semna″ un obiect şi receptorul poate folosi cheia privată corespunzătoare pentru decriptarea acestei semnături digitale. .

Secure Sockets Layer (SSL)

Original creat de Netscape, Secure Sockets Layer (SSL) este standardul industrial pentru encriptarea sesiunilor între clienţi şi servere. SSL foloseşte criptografie cu chei asimetrice sau publice pentru a cripta sesiuni între server şi client. Aplicaţiile client şi server negociază această cheie sesiune în timpul unui schimb de certificate digitale. Cheia expiră automat după 24 de ore şi procesul SSL crează o cheie diferită pentru fiecare conexiune server şi fiecare client. Astfel, chiar dacă utilizatorii neautorizaţi interceptează şi decriptează cheia sesiunii (ceea ce nu este de dorit), ei nu o pot utiliza pentru a trage cu urechea sau pentru sesiuni ulterioare.

Capitol 6. Plan pentru DCM

Pentru a folosi Digital Certificate Manager - DCM pentru a gestiona efectiv certificatele digitale ale companiei dvs., trebuie să aveţi un plan general despre cum veţi folosi certificate digitale ca parte a politicii dvs. de securitate.

Pentru a afla mai multe despre cum să plănuiţi utilizarea DCM şi pentru a înţelege mai bine cum pot fi incluse certificatele digitale în politica dvs. de securitate, revedeţi aceste subiecte:

Cerinţe pentru utilizarea DCM
Citiţi pentru a afla ce software trebuie să instalaţi şi alte informaţii de care aveţi nevoie pentru a vă seta calculatorul pentru a folosi DCM.

Tipuri de certificate digitale
Folosiţi aceste informaţii pentru a învăţa diferitele tipuri de certificate pentru administrarea cărora puteţi folosi DCM.

Certificate publice contra certificate private
Folosiţi aceste informaţii pentru a învăţa cum să determinaţi ce tip de certificate se potriveşte cel mai bine cu nevoile dvs. după ce decideţi cum doriţi să folosiţi certificatele pentru a profita de securitatea adiţională pe care o oferă. Puteţi folosi certificate de la o CA publică sau puteţi crea şi opera o CA privată pentru a emite certificate. Alegerea modului în care obţineţi certificatele depinde de modul în care intenţionaţi să le utilizaţi.

Certificate digitale pentru comunicaţia SSL (Secure Sockets Layer)
Folosiţi aceste informaţii pentru a învăţa cum să folosiţi certificate pentru ca aplicaţiile să poată stabili sesiuni de comunicare sigure.

Certificatele digitale pentru autentificarea utilizatorului
Folosiţi aceste informaţii pentru a afla despre cum să folosiţi certificate pentru a furniza un mijloc pentru o autentificare mai puternică a utilizatorilor care accesează resurse de pe un server iSeries.

Certificate digitale pentru autentificarea conexiunilor pe reţele private virtuale (VPN)
Folosiţi aceste informaţii pentru a învăţa cum să folosiţi certificate ca parte a configurării unei conexiuni VPN.

Certificatele digitale pentru semnarea obiectelor
Folosiţi aceste informaţii pentru a învăţa cum să folosiţi certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticităţii sale.

Certificate digitale pentru verificarea semnăturilor obiectelor
Folosiţi aceste informaţii pentru a afla despre cum să folosiţi certificate pentru a verifica semnătura digitală a unui obiect pentru a verifica autenticitatea acestuia.

Cerinţe de setare DCM

Digital Certificate Manager (DCM) este o opţiune iSeries gratuită care vă permite să gestionaţi centralizat certificatele pentru aplicaţiile dumneavoastră. Pentru a folsoi cu succes DCM, asiguraţi-vă că faceţi următoarele:

- Instalaţi programul cu licenţă pentru furnizarea accesului criptografic (5722–AC3). Acest produs criptografic determină lungimea maximă a cheii care este permisă pentru algoritmii criptografici bazaţi pe reguli de export şi import. Trebuie să instalaţi acest produs înainte să puteţi crea certificate.
- Instalaţi opţiunea 34 a OS/400. Aceasta este facilitatea DCM bazată pe browser.
- Instalaţi IBM HTTP Server pentru iSeries (5722–DG1) şi porniţi instanţa *ADMIN a serverului.

- Asiguraţi-vă că TCP este configurat pentru sistem pentru a putea folosi browser-ul de web şi instanţa *ADMIN a server-ului HTTP pentru a accesa facilitatea DCM.

Notă: Nu veţi putea crea certificate decât dacă aţi instalat toate produsele necesare. Dacă un produs cerut nu este instalat, DCM va afişa un mesaj de eroare spunându-vă să instalaţi componenta care lipseşte.

Tipuri de certificate digitale

Există mai multe clasificări ale certificatelor digitale. Aceste clasificări descriu cum este folosit certificatul. Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona următoarele tipuri de certificate:

Certificate ale Autorităţii de Certificare (CA - Certificate Authority)
O Autoritate de certificare este un credential digital care validează identitatea CA (autorităţii de certificare) care este proprietară a certificatului. Certificatul Autorităţii de Certificare conţine informaţii de identificare despre Autoritatea de Certificare, precum şi cheia publică a acesteia. Cheia publică a certificatului CA poate fi utilizată de alţii pentru a se verifica autenticitatea certificatelor pe care le emite şi semnează CA. Un certificat Autoritate de certificare poate fi semnat de altă CA, ca VeriSign, sau poate fi semnat automat în cazul în care este o entitate independentă. O CA creată de dvs. în Digital Certificate Manager este o entitate independentă. Cheia publică a certificatului CA poate fi utilizată de alţii pentru a se verifica autenticitatea certificatelor pe care le emite şi semnează CA. Pentru a folosi un certificat pentru SSL, pentru semnarea obiectelor sau pentru verificarea semnăturilor obiectelor, trebuie să aveţi şi o copie a certificatului CA pentru CA care a emis certificatul.

Certificate server sau client
Un certificat client sau server este un credential digital care identifică aplicaţia server sau client care foloseşte certificatul pentru comunicaţii sigure. Certificatele server sau client conţin informaţii de identificare despre organizaţia proprietară a aplicaţiei, cum ar fi numele distinct al sistemului. Certificatul conţine de asemenea cheia publică a sistemului. Un server trebuie să aibă un certificat digital pentru a folosi Secure Sockets Layer (SSL) pentru comunicaţii sigure. Aplicaţiile care suportă certificatele digitale pot examina certificatul server-ului pentru a verifica identitatea acestuia când clienţii accesează serverul. Aplicaţia poate folosi mai apoi autentificarea certificatului ca bază pentru iniţializarea unei sesiuni SSL-encriptat între client şi server. Puteţi gestiona aceste tipuri de certificate doar din depozitul de certificate *SYSTEM.

Certificate pentru semnarea obiectelor
Un certificat pentru semnarea obiectelor este un certificat pentru a ″semna″ digital un obiect. Prin semnarea obiectului, furnizaţi un mijloc prin care puteţi verifica atât integritatea obiectului cât şi originea sau proprietarul obiectului. Puteţi folosi certificatul pentru a semna o varietate de obiecte, inclusiv majoritatea obiectelor din Sistemul integrat de fişiere (Integrated File System - IFS) şi obiectele *CMD. Puteţi găsi o listă completă a obiectelor ce pot fi semnate în capitolul despre Semnarea obiectelor şi verificarea semnăturilor. Atunci când se foloseşte cheia privată a unui certificat care semnează obiecte pentru a se semna un obiect, cel care va primi acest obiect trebuie să aibă acces la o copie a certificatului de verificare a semnăturii corespunzător pentru a putea autentifica corect semnătura obiectului. Puteţi administra aceste tipuri de certificate doar din depozitul de certificate *OBJECTSIGNING.

Certificate pentru verificarea semnăturilor
Un certificat de verificare a semnăturii este un certificat de semnare a obiectelor care nu are cheia privată a certificatului. Folosiţi cheia publică a certificatului pentru verificarea semnăturii pentru a autentifica semnătura digitală creată cu un certificat pentru semnarea obiectelor. Verificarea semnăturii vă permite să determinaţi originea obiectului şi dacă a fost modificat de când a fost semnat. Puteţi administra aceste tipuri de certificate doar din depozitul de certificate *SIGNATUREVERIFICATION.

Certificate ale utilizatorului
Un certificat utilizator este un credential digital ce validează identitatea clientului sau utilizatorului ce deţine certificatul. În prezent, multe aplicaţii furnizează un suport care vă permite să folosiţi certificatele pentru a autentifica utilizatori pentru resurse în loc de a se folosi nume de utilizatori şi parole. Digital Certificate Manager (DCM) asociază automat certificate utilizator pe care Autoritatea de certificare privată a dvs. le emite cu profilul de utilizator iSeries al utilizatorului. Puteţi de asemenea folosi DCM pentru a asocia certificate utilizator pe care alte Autorităţi de Certificare le emit cu profilul utilizator iSeries al utilizatorului.

Atunci când se foloseşte DCM (administratorul de certificare digitale) pentru a se gestiona certificatele, aceste le organizează după aceste clasificări şi le plasează pe ele şi cheile lor private asociate în depozitul de certificate.

Notă: Dacă aveţi un Coprocesor Criptografic IBM 4758 PCI instalaz pe serverul dvs. iSeries, puteţi alege alte opţiuni de stocare a cheilor private pentru certificatele dvs. (cu excepţia certificatelor de semnare a obiectelor). Puteţi alege să păstraţi cheia privată chiar pe coprocesor. Sau, puteţi folosi coprocesorul pentru a cripta cheia privată şi a o păstra într-un fişier special cheie privată în loc de a o păstra în depozitul de certificate. Totuşi, certificatele utilizator şi cheile lor private sunt depozitate în sistemul utilizatorului, sau în software-ul browser-ului sau într-un fişier care să fie folosit de alte pachete software client.

Certificate publice contra certificate private

După ce aţi decis să folosiţi certificate, va trebui să alegeţi tipul de implementare pentru certificat care se potriveşte cel mai bine cu nevoile proprii de securitate. Opţiunile pe care le aveţi pentru obţinerea certificatelor includ:
- Obţinerea certificatelor de la o Autoritate de certificare (CA) publică.
- Operarea propriului CA pentru a emite certificate private pentru utilizatori şi aplicaţii.
- Folosirea unei combinaţii între CA-uri Internet şi propria CA.

Alegerea uneia dintre aceste opţiuni de implementare depinde de un număr de factori, unul dintre cei mai importanţi fiind mediul în care sunt folosite certificatele. Mai jos sunt nişte informaţii care vă vor ajuta să determinaţi mai bine care opţiune de implementare este potrivită pentru cerinţele dvs. de afacere şi de securitate.

Folosirea certificatelor publice

CA-urile publice Internet lansează certificate către oricine plăteşte taxa corespunzătoare. Totuşi, o CA Internet necesită încă o dovadă a identităţii înainte să poată lansa un certificat. Acest nivel al dovezii variază, în funcţie de politica de identificare a CA. Ar trebui să consideraţi dacă stricteţea politicii de identificare a CA se potriveşte cu cerinţele de securitate înainte de a avea încredere în certificatele pe care le emite. Deoarece standardele pentru Public Key Infrastructure for X.509 (PKIX) au evoluat, unele CA-uri publice noi oferă acum standarde mult mai stringente de identificare pentru emiterea de certificate. În timp ce procesul de obţinere a certificatelor de la un asemenea CA PKIX este mai evoluat, certificatele emise de CA oferă o mai bună asigurare a securităţii accesului la aplicaţii prin utilizatori specifici. Digital Certificate Manager (DCM) vă permite să folosiţi şi să gestionaţi certificatele provenite de la CA-uri PKIX care folosesc aceste noi standarde pentru certificate.

Trebuie să consideraţi de asemenea costul asociat cu folosirea unei CA publice pentru a emite certificate. Dacă aveţi nevoie ca certificatele să fie emise unui număr limitat de aplicaţii client şi server şi utilizatori, s-ar putea ca pentru dvs. costul să nu fie un factor important. Totuşi, costul poate fi foarte important dacă aveţi un număr mare de utilizatori *privaţi* care au nevoie de certificate publice pentru autentificare client. În acest caz, ar trebui să consideraţi şi efortul

administrativ şi de programare necesar configurării aplicaţiilor server pentru a accepta doar un subset specific de certificate pe care le emite CA publică.

Folosirea certificatelor provenite de la o CA publică vă poate salva timp şi resurse deoarece multe aplicaţii server, client şi utilizator sunt configurate pentru a recunoaşte majoritatea dintre cele mai cunoscute CA-uri publice. De asemenea, alte companii şi utilizatori pot recunoaşte şi avea mai multă încredere în certificatele emise de o CA publică binecunoscută decât în cele emise de CA privată.

Folosirea certificatelor private

Dacă vă creaţi propriul CA local, puteţi emite certificate către sisteme şi utilizatori într-un domeniu mult mai limitat, precum în interiorul companiei sau organizaţiei dvs. Crearea şi întreţinerea propriei CA vă permite să emiteţi certificate doar pentru acei utilizatori care sunt membrii de încredere ai grupului dvs. Aceasta oferă o securitate mai bună, deoarece puteţi controla mai strâns cine are acces la certificate şi de aceea cine are acces la resursele dvs. Un potenţial dezavantaj al menţinerii propriei CA local este cantitatea de timp şi resurse pe care trebuie să le investiţi. Oricum, Digital Certificate Manager (DCM) face acest proces mai uşor pentru dvs.

Când folosiţi un CA local pentru a emite certificate către utilizatori pentru autentificarea clienţilor, ar trebui să decideţi dacă vreţi ca certificatele utilizatorilor dvs. să fie asociate cu profilele de utilizator iSeries. Puteţi face ca utilizatorii să-şi obţină certificatele lor de la CA locală prin DCM dacă vreţi ca certificatele lor să fie asociate cu un profil utilizator iSeries. Sau, începând cu V5R2, puteţi să folosiţi API-uri pentru a emite dintr-un program certificate către utilizatori non-iSeries astfel încât aceşti utilizatori să nu trebuiască să aibe un profil utilizator iSeries pentru a folosi certificate private pentru autentificarea clienţilor.

Notă: Indiferent de CA folosită pentru emiterea de certificate, administratorul de sistem controlează care CA trebuie să fie de încredere pentru aplicaţiile din sistem. Dacă o copie a unui certificat pentru o CA binecunoscută poate fi găsită în browser-ul dvs., acesta poate fi setat să aibă încredere în certificate server ce au fost emise de acea CA. Oricum, dacă acel certificat CA nu este în depozitul de certificate *SYSTEM, server-ul nu va avea încredere în certificatele utilizator sau client care au fost emise de acea CA. Pentru a avea încredere în certificate utilizator ce au fost emise de o CA, trebuie să obţineţi o copie a certificatului CA de la CA. El trebuie să fie în formatul de fişier corect şi trebuie să adăugaţi certificatul în depozitul de certificate DCM.

Aţi putea găsi folositor să treceţi în revistă unele scenarii comune de folosire a certificatelor pentru a vă ajuta să alegeţi dacă folosirea de certificate publice sau private se potriveşte cel mai bine cu afacerea dvs. şi cu necesităţile de securitate.

Task-uri înrudite

După ce decideţi cum doriţi să folosiţi certificatele şi ce tip să folosiţi, revedeţi aceste proceduri pentru a afla mai multe despre cum să folosiţi DCM (Digital Certificate Manager) pentru a vă pune planul în acţiune:

- Crearea şi operarea CA-urilor private descrie task-urile pe care trebuie să le efectuaţi dacă decideţi să operaţi cu o CA pentru a emite certificate private.
- Gestionarea certificatelor de la o CA publică Internet descrie task-urile pe care trebuie să le efectuaţi pentru a folosi certificatele de la o CA publică bine cunoscută, incluzând CA PKIX.
- Folosirea unei CA local pe alte servere iSeries descrie operaţiile pe care trebuie să le efectuaţi dacă vreţi să folosiţi certificate de la o CA privată pe mai mult de un sistem.

Certificatele digitale pentru comunicaţiile sigure SSL

Puteţi folosi certificate digitale pentru a configura aplicaţiile să folosească Secure Sockets Layer (SSL) pentru sesiuni de comunicare securizate. Pentru a stabili o sesiune SSL, serverul dvs. oferă întotdeauna o copie a certificatului său pentru a fi validat de către clientul care cere o conexiune. Folosirea conexiunii SSL:

- Asigură clientul sau utilizatorul-final, că site-ul este autentic.
- Oferă o sesiune de comunicaţii criptate pentru a se asigura că datele care trec prin conexiune rămân private.

Aplicaţiile client şi server lucrează împreună pentru a asigura securizarea datelor după cum urmează.

1. Aplicaţia server prezintă certificatul către aplicaţia client (utilizator) ca dovadă a identităţii server-ului.
2. Aplicaţia client verifică identitatea server-ului folosind o copie a certificatului Autorităţii de certificare emiţătoare. (Aplicaţia client trebuie să aibă acces la copia stocată local a certificatului CA relevant.)
3. Aplicaţiile server şi client se pun de acord cu o cheie simetrică pentru criptare şi o folosesc pentru a cripta sesiunea de comunicare.
4. Opţional, server-ul poate cere client-ului să furnizeze o dovadă a identităţii înainte de a permite accesul la resursele cerute. Pentru a se folosi certificate ca dovadă a identităţii, aplicaţiile care comunică trebuie să suporte folosirea certificatelor pentru autentificarea utilizatorilor.

SSL foloseşte algoritmi cu cheie asimetrică (cheie publică) în timpul procesării contact SSL pentru a negocia o cheie simetrică ce este folosită apoi pentru criptarea şi decriptarea datelor aplicaţiei pentru o anumită sesiune SSL. Aceasta înseamnă că serverul dvs. şi clientul folosesc chei-sesiune diferite, ce expiră automat după un timp stabilit anterior, pentru fiecare conexiune. Este un fenomen neobişnuit ca cineva să intercepteze şi să decripteze o anumită cheie-sesiune particulară, nu se poate folosi sesiunea pentru a se deduce alte chei viitoare.

Certificatele digitale pentru autentificarea utilizatorului

Tradiţional, utilizatorii primesc acces la resurse de la o aplicaţie sau sistem pe baza numelui de utilizator şi a parolei. Se poate creşte securitatea sistemului prin utilizarea certificatelor digitale (în locul numelor de utilizatori şi a parolelor) pentru a autentifica şi autoriza sesiunile dintre mai multe aplicaţii server utilizatori. De asemenea, puteţi folosi Digital Certificate Manager (DCM) pentru a asoca certificatul unui utilizator cu profilul utilizator iSeries al acelui utilizator. Certificatul are astfel aceleaşi autorizări şi permisiuni precum profilul asociat. Începând cu V5R2, puteţi folosi API-uri pentru a folosi în programe propria Autoritate de Certificare locală pentru a emite certificate către utilizatori non-iSeries. Aceste API-uri vă furnizează abilitatea să emiteţi certificate private către utilizatori când nu doriţi ca aceşti utilizatori să aibe un profil utilizator iSeries.

Un certificat digital se comportă ca un credential electronic şi verifică dacă persoana ce se prezintă este cea care se pretinde a fi. Astfel, un certificat este similar unui paşaport. Ambele stabilesc o identitate individuală, şi ambele conţin un unic număr în scopul identificării şi au autorităţi de emitere care pot recunoaşte dacă este autentic credentialul. În cazul unui certificat, funcţiile unei Autorităţi de certificare (CA) fiind a treia parte, de încredere, care emite certificatul şi îl verifică dacă este un credential autentic.

Pentru autentificare, certificatele se folosesc de o cheie publică şi de o cheie privată. Autoritatea de certificare care emite leagă aceste chei, împreună cu alte informaţii despre proprietarul certificatului, de certificat pentru identificare.

Un număr crescut de aplicaţii oferă acum suport pentru folosirea certificatelor pentru autentificare client în timpul unei sesiuni SSL. În prezent, aceste aplicaţii iSeries oferă suport pentru certificate de autentificare a clienţilor:

- Server Telnet
- IBM HTTP Server (original şi motorizat de Apache)
- Server Directory Services (LDAP)
- Management Central
- Client Access Express (including iSeries Navigator)
- Server FTP

De-a lungul timpului, aplicaţii adiţionale pot furniza suport pentru certificate de autentificare a clienţilor; citiţi documentaţia pentru aplicaţii particulare pentru a determina dacă oferă acest suport.

Certificatele pot oferi mijloace mai puternice pentru autentificarea utilizatorilor din mai multe motive:

- Există posibilitatea ca un individ să uite propria parolă. De aceea, utilizatorii trebuie să memoreze sau să îşi înregistreze numele de utilizator şi parola pentru a se asigura că le ţin minte. Ca rezultat, utilizatori neautorizaţi pot obţine mai uşor nume şi parole de la utilizatori autorizaţi. Deoarece depozitele de certificate sunt depozitate într-un fişier sau altă locaţie electronică, aplicaţiile client (mai repede decât cele utilizator) manevrează accesul şi prezentarea certificatului pentru autentificare. Acest lucru asigura faptul că este mai puţin probabil ca utilizatorii să împartă certificate cu utilizatori neautorizaţi, cu excepţia cazului în care utilizatorii neautorizaţi au acces la sistemul utilizatorului. De asemenea, certificatele pot fi instalate pe smart card-uri ca o metodă suplimentară de protejare împotriva unei folosiri neautorizate.
- Un certificat conţine o cheie privată ce nu este niciodată trimisă cu certificatul pentru identificare. În schimb, această cheie este folosită de sistem în timpul proceselor de criptare şi decriptare. Ceilalţi pot folosi cheia publică corespunzătoare a certificatului pentru a verifica identitatea celui care a trimis obiectele care sunt semnate cu cheia privată.
- Multe sisteme necesită parole de o lungime maximă de 8 caractere, făcând aceste parole mai vulnerabile la atacuri prin ghicire. Cheile criptografice ale unui certificat au sute de caractere în lungime. Această lungime împreună cu natura lor aleatoare, fac astfel încât cheile criptografice să fie mult mai greu de ghicit în comparaţie cu parolele.
- Cheile certificatelor digitale oferă câteva moduri potenţiale de utilizare pe care nu le oferă parolele, cum ar fi integritatea datelor şi intimitatea. Puteţi folosi certificatele şi cheile lor asociate pentru a:
  - Asigura integritatea datelor prin detectarea modificărilor aduse lor.
  - Dovedi faptul că o anume acţiune a fost realizată. Acest proces este numit nerepudiere.
  - Asigura intimitatea transferurilor de date folosind Secure Sockets Layer (SSL) pentru a encripta sesiuni de comunicare.

Pentru a afla mai multe despre configurarea aplicaţiilor iSeries server pentru a folosi certificate pentru autentificarea clienţilor în timpul unei sesiuni SSL, vedeţi Securizarea aplicaţiilor cu SSL.

Certificatele digitale pentru conexiuni VPN

Puteţi folosi certificate digitale ca un mijloc de a stabili o conexiune de reţea privată virtuală (VPN) iSeries . Ambele capete ale unei conexiuni dinamice VPN trebuie să poată comunica pentru a se autentifica una alteia înainte de a se activa conexiuea. Autentificarea la punctul-terminal este făcută prin server-ul IKE (Internet Key Exchange - schimb de chei Internet) la fiecare capăt. După o autentificare cu succes, server-ele IKE pot negocia metode şi algoritmi de criptare pe care le vor folosi pentru a securiza conexiunea VPN.

Înainte de V5R1, server-ele IKE se puteau autentifica unul pe celălalt doar prin folosirea unei chei pre-partajate. Folosirea unei chei pre-partajate este mai puţin sigură deoarece trebuie să comunicaţi manual această cheie administratorului celuilalt punct terminal al VPN-ului. În consecinţă, este posibil ca aceasta să fie văzută de alţii în timpul procesului de comunicare al ei.

Puteţi evita acest risc folosind certificatele digitale pentru a autentifica punctele finale în loc de a folosi o cheie pre-împărţită. Server-ul IKE poate autentifica certificatul celuilalt server pentru a stabili o conexiune pentru a stabili metodele şi algoritmii de criptare pe care le vor folosi server-ele pentru a securiza conexiunea.

Puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele pe care server-ele IKE le folosesc pentru a stabili conexiuni dinamice VPN. Trebuie să decideţi mai întâi dacă pentru server-ul IKE veţi folosi certificate publice sau veţi emite certificate private .

Unele implementări VPN cer ca certificatul să conţină informaţii nume subiect alternative, cum ar fi un nume domeniu sau o adresă de mail, suplimentare faţă de informaţia standard legată de numele distinct. Atunci când folosiţi CA privată a facilităţii DCM pentru a emite un certificat puteţi specifica informaţii nume subiect alternative pentru certificat. Specificând această informaţie vă asiguraţi că conexiunea VPN iSeries este compatibilă cu alte implementări VPN care o pot cere pentru autentificare.

Pentru a afla mai multe despre cum să gestionaţi certificate pentru conexiuni VPN, revedeţi aceste subiecte:

- Dacă nu aţi folosit niciodată DCM pentru a gestiona certificate, aceste articole vă vor ajuta să începeţi:
  - Creând şi operând cu un CA local, privat descrie cum să folosiţi DCM pentru a emite certificate private pentru aplicaţiile dumneavoastră.
  - Gestionarea certificatelor de la o CA publică Internet descrie cum să utilizaţi DCM pentru a lucra cu certificatele provenite de la o CA publică.
- Dacă nu folosiţi în curent DCM pentru a gestiona certificate pentru alte aplicaţii, revedeţi aceste surse pentru a afla cum să specificaţi dacă o aplicaţie foloseşte un certificat existent şi ce certificate poate accepta şi autentifica aplicaţia:
  - Gestionarea atribuirii certificatului pentru o aplicaţie vă descrie cum să folosiţi DCM pentru a atribui un certificat existent unei aplicaţii, cum ar fi server-ul IKE.
  - Definirea listei de încredere CA pentru o aplicaţie vă descrie cum să specificaţi în care CA-uri poate avea încredere o aplicaţie atunci când aceasta acceptă certificate pentru autentificare client (sau VPN).

Certificatele digitale pentru semnarea obiectelor

Începând cu V5R1, OS/400 furnizează suport pentru folosirea certificatelor pentru a ″semna″ digital obiecte. Semnarea digitală a obiectelor furnizează un mod de a verifica atât integritatea conţinutului obiectului cât şi originea lui. Suportul pentru semnarea obiectelor îmbunătăţeşte uneltele de sistem tradiţionale iSeries pentru a controla cine poate modifica obiecte. Controlul tradiţional nu poate proteja un obiect de atacurile neautorizate în timp ce obiectul este în tranzit peste Internet sau alte reţele care nu sunt de încredere, sau în timp ce obiectul este depozitat pe un sistem non-iSeries. De asemenea, controalele tradiţionale nu pot determina întotdeuna dacă s-au făcut modificări sau alterări ale unui obiect. Folosirea semnăturilor digitale asupra obiectelor furnizează un mijloc sigur pentru detectarea modificărilor obiectelor semnate.

Plasarea unei semnături digitale pe un obiect constă din folosirea cheii private a certificatului pentru a adăuga un rezumat criptat matematic al datelor din obiect. Semnătura protejează

datele de modificările neautorizate. Obiectul şi conţinutul său nu sunt criptate şi nu sunt făcute private de semnătura digitală; totuşi, rezumatul este criptat pentru a se preveni modificările neautorizate ce se pot încerca asupra lui. Oricine vrea să se asigure că obiectul nu a fost modificat în timpul tranzitului şi că el provine de la o sursă acceptată, legitimă, poate folosi cheia publică a certificatului care a semnat pentru a verifica semnătura digitală originală. Dacă semnăturile nu se mai potrivesc, s-ar putea ca datele să fie alterate. În acest caz, receptorul poate evita folosirea obiectului şi poate în schimb să-l contacteze pe semnatar şi să obţină altă copie a obiectului semnat.

Dacă decideţi că folosirea semnăturilor digitale se potriveşte cu cerinţele şi politica de securitate, ar trebui să vă gândiţi dacă trebuie să folosiţi certificate publice sau să emiteţi certificate private. Dacă intenţionaţi să distribuiţi obiecte către utilizatori publici generali, ar trebui să luaţi în considerare folosirea certificatelor de la o Autoritate de Certificare (Certificate Authority - CA) publică cunoscută pentru a semna obiectele. Folosirea certificatelor publice asigură faptul că ceilalţi pot verifica uşor şi necostisitor semnăturile pe care le-aţi plasat pe obiectele pe care le-aţi distribuit. Dacă, oricum, itenţionaţi să distribuiţi obiecte doar în cadrul organizaţiei dvs., aţi putea prefera să folosiţi Digital Certificate Manager (DCM) pentru a opera propriul dvs. CA local pentru a emite certificate pentru semnarea obiectelor. Folosirea certificatelor private de la un CA local pentru a semna obiecte este mai puţin costisitoare decât cumpărarea de certificate de la o CA publică cunoscută.

Semnătura de pe un obiect reprezintă sistemul care a semnat obiectul, nu un utilizator specific de pe acel sistem (deşi utilizatorul trebuie să aibă autoritatea necesară pentru a folosi certificatul pentru a semna obiecte). Folosiţi Digital Certificate Manager (DCM) pentru a administra certificatele pe care le folosiţi ca să semnaţi obiecte şi pentru a verifica semnăturile obiectelor. De asemenea, puteţi folosi DCM pentru a semna obiecte şi pentru a verifica semnăturile obiectelor.

Certificate digitale pentru verificarea semnăturilor obiectelor

Începând cu V5R1, iSeries furnizează suport pentru folosirea certificatelor pentru a verifica semnăturile digitale ale obiectelor. Oricine doreşte să se asigure că un obiect semnat nu a fost modificat la transport şi că obiectul provine de la o sursă acceptată şi legitimă poate folosi cheia publică a certificatului semnatar pentru a verifica semnătura digitală originală. Dacă semnăturile nu se mai potrivesc, s-ar putea ca datele să fie alterate. În acest caz, receptorul poate evita folosirea obiectului şi poate în schimb să-l contacteze pe semnatar şi să obţină altă copie a obiectului semnat.

Semnătura unui obiect reprezintă sistemul care a semnat obiectul, nu un utilizator specific de pe acel sistem. Ca parte a procesului de verificare a semnăturilor digitale, trebuie să decideţi în care Autorităţi de certificare aveţi încredere şi în care certificate aveţi încredere pentru a semna obiecte. Atunci când alegeţi să aveţi încredere într-o CA puteţi alege dacă aveţi încredere în semnăturile create de cineva prin folosirea unui certificat emis de CA de încredere. Când alegeţi să nu aveţi încredere într-o CA, alegeţi şi să nu aveţi încredere în certificatele emise de CA sau în semnăturile create de cineva folosind aceste certificate.

Verificarea valorii sistem restaurare obiect (QVFYOBJRST)

Dacă vă decideţi să efectuaţi verificarea semnăturilor, una dintre primele decizii importante pe care trebuie să le luaţi este să determinaţi cât de importante sunt semnăturile pentru obiectele restaurate pe sistemul dvs. Controlaţi aceasta cu o valoare sistem numită QVFYOBJRST. Setările implicite pentru această valoare sistem permit obiectelor nesemnate să fie restaurate, dar asigură faptul că obiectele semnate nu pot fi restaurate decât dacă ele au o semnătură validă. Sistemul defineşte un obiect ca fiind semnat doar dacă el are o semnătură în care are încredere sistemul; acesta ignoră alte semnături ″ce nu sunt de încredere″ ale obiectului şi îl tratează ca şi când nu ar fi semnat.

Sunt mai multe valori pe care le puteţi folosi pentru valoarea sistem QVFYOBJRST, care variază între ignorarea tuturor semnăturilor şi necesitatea de semnături valide pentru toate obiectele pe care le restaurează sistemul. Această valoare sistem afectează numai obiectele executabile care sunt restaurate, nu şi fişierele de salvare sau IFS. Pentru a afla mai multe despre folosirea acesteia şi a altor valori sistem, vedeţi System Value Finder în Centrul de Informaţii.

Folosiţi DCM pentru a implementa certificatul dvs. şi deciziile de încredere CA cât şi pentru a gestiona certificatele pe care le folosiţi pentru a verifica semnăturile obiectelor. Puteţi de asemenea folosi DCM pentru a semna obiecte şi pentru a verifica semnăturile obiectelor.

Capitol 7. Configurare DCM

DCM (Digital Certificate Manager) furnizează o interfaţă cu utilizatorul bazată pe browser pe care o puteţi folosi pentru a gestiona certificate digitale pentru aplicaţii şi utilizatori. Interfaţa cu utilizatorul este divizată în două cadre principale: un cadru de navigare şi un cadru de task.

Puteţi folosi cadrul de navigare pentru a selecta task-urile care să administreze certificatele sau aplicaţiile care le folosesc. În timp ce unele task-uri individuale apar direct în cadrul principal de navigare, majoritatea task-urilor din cadrul de navigare sunt organizate în categorii. De exemplu, **Gestionare certificate** este o categorie de task-uri care conţine o varietate de task-uri individuale asistate, cum ar fi Vizualizare certificate, Reînnoire certificat, Import certificat şi aşa mai departe. Dacă un articol din cadrul de navigare este o categorie cu mai mult de un task, va apărea o săgeată, la stânga acesteia. Săgeata indică faptul că atunci când veţi selecta legătura categorie, va fi afişată o listă extinsă de task-uri, asfel încât să puteţi alege task-ul dorit pentru executare.

Cu excepţia categoriei **Cale rapidă**, fiecare task din cadrul de navigare este un task asistat care vă trece printr-o serie de paşi pentru a se efectua task-ul uşor şi rapid. Categoria Cale rapidă oferă un grup de funcţii de gestionare a certificatelor şi aplicaţiilor care permit utilizatorilor experimentaţi ai DCM să acceseze rapid o varietate de task-uri înrudite dintr-un singur set central de pagini.

Task-urile care sunt disponibile în cadrul de navigare variază pe baza depozitului de certificate în care lucraţi. De asemenea, categoria şi numărul de task-uri pe care le vedeţi în fereastra de navigare variază în funcţie de autorizaţiile pe care le are profilul dvs. de utilizator iSeries. Toate task-urile pentru operarea unui CA, pentru administrarea certificatelor pe care le folosesc aplicaţiile şi alte task-uri la nivelul sistemului sunt sunt disponibile doar pentru ofiţeri de securitate sau administratori iSeries. Ofiţerul de securitate sau administratorul trebuie să deţină autorizările speciale *SECADM şi *ALLOBJ pentru a vizualiza şi utiliza aceste procese. Utilizatorii fără aceste autorizări speciale au acces doar la funcţiile de certificare utilizator.

Pentru a învăţa cum să configuraţi DCM şi să începeţi să-l folosiţi pentru administrarea certificatelor, revedeţi aceste subiecte:

Pornire DCM
Citiţi aceasta pentru a învăţa să accesaţi caracteristica Digital Certificate Manager din iSeries.

Setare certificate pentru prima dată
Citiţi aceasta pentru a învăţa cum să începeţi să folosiţi DCM pentru a seta tot ce aveţi nevoie pentru începerea folosirii certificatelor pentru prima dată. Învăţaţi cum să faceţi primii paşi în administrarea certificatelor de la o Autoritate Publică de Certificare Internet (Internet Certificate Authority - CA) sau cum să creaţi şi să operaţi un CA local privat pentru emiterea de certificate.

Dacă doriţi mai multe informaţii educaţionale despre folosirea certificatelor digitale într-un mediu Internet pentru sporirea securităţii sistemului şi reţelei dvs., site-ul de web VeriSign este o resursă excelentă. Site-ul de web VeriSign oferă o librărie extensibilă de articole despre certificatele digitale, ca şi un număr de alte subiecte legate de securitatea pe Internet. Puteţi accesa biblioteca lor la VeriSign Help Desk .

Pornire Digital Certificate Manager

Înainte de a folosi oricare din aceste funcţii, va trebui să porniţi DCM (Digital Certificate Manager). Efectuaţi aceste task-uri pentru a vă asigura că aţi pornit cu succes DCM:

1. Instalaţi 5722 SS1 Opţiunea 34. Acesta este Digital Certificate Manager - DCM.

   Instalaţi 5722 DG1. Acesta este IBM HTTP Server for iSeries.

   Instalare 5722 AC3. Acesta este produsul de criptografie pe care V5R2 DCM îl foloseşte să genereze o pereche de chei publică-privată pentru certificate, pentru a cripta fişier certificat exportate şi pentru a decripta fişiere certificat importate.
2. Folosiţi iSeries Navigator pentru a porni instanţa *ADMIN a Serverului HTTP:
   a. Porniţi **iSeries Navigator**.
   b. Dublu-clic pe serverul dvs. iSeries în vederea arbore principală.
   c. Efectuaţi un dublu clic pe **Reţea**.
   d. Efectuaţi un dublu clic pe **Servere**.
   e. Efectuaţi un dublu clic pe **TCP/IP**.
   f. Efectuaţi un clic dreapta pe **Administrare HTTP**.
   g. Selectaţi **Pornire**.
3. Porniţi browserul web.
4. Folosind browserul dvs., mergeţi la pagina iSeries Tasks de pe sistemul dvs. la http://*numele_sistemului_dvs*:2001.
5. Selectaţi **Digital Certificate Manager** din lista de produse de pe pagina iSeries Tasks pentru a accesa caracteristica DCM.

Dacă migraţi de la o versiune anterioară a DCM, această pagină vă va oferi detalii de care aveţi nevoie pentru a vă actualiza sistemul.

Setare certificate pentru prima dată

Cadrul stâng al DCM (administrator de certificate digitale) este cadrul de navigare task. Puteţi folosi acest cadru pentru a selecta o varietate largă de task-uri pentru gestionarea certificatelor şi a aplicaţiilor care le folosesc. Task-urile care sunt disponibile depind de depozitul de certificate pe care l-aţi deschis (dacă aţi deschis unul) şi de autoritatea profilului Dvs. de utilizator. Majoritatea task-urilor sunt disponibile doar dacă aveţi autorizaţii speciale *ALLOBJ şi *SECADM.

Când folosiţi pentru prima dată DCM (Digital Certificate Manager), nu există nici un depozit de certificate (cu excepţia cazului în care aţi migrat de la o versiune anterioară a DCM). În consecinţă, cadrul de navigare afişează doar aceste task-uri atunci când aveţi autorizaţiile necesară:

- Gestionarea certificatelor utilizator.
- Crearea unui nou Depozit de certificate.
- Crearea unei CA (autorităţi de certificare). (Notă: După ce folosiţi acest task pentru a crea o CA privată, acesta nu va mai apare în listă.)
- Gestionarea locaţiilor CRL.
- Gestionarea locaţiei cererii PKIX.

Chiar dacă există deja pe sistemul dvs. depozite de certificate (de exemplu, dacă migraţi dintr-o versiune anterioară a DCM), DCM afişează doar un număr limitat de task-uri sau categorii de task-uri în fereastra de navigare din stânga. Trebuie să accesaţi mai întâi depozitul necesar de certificate înainte de a putea începe lucrul cu majoritatea task-urilor de gestiune a certificatelor şi a aplicaţiilor. Pentru a deschide un depozit de certificate specific, alegeţi în cadrul de navigare **Selectare depozit de certificate**.

Cadrul de navigare al DCM oferă de asemenea un buton **Conexiune sigură**. Puteţi folosi acest buton pentru a face să apară o a doua fereastră a browser-ului pentru iniţierea unei conexiuni sigure prin folosirea Secure Sockets Layer (SSL). Pentru a folosi cu succes această funcţie, trebuie să configuraţi mai întâi Serverul HTTP IBM pentru iSeries pentru a folosi SSL să operaţi în modul securizat. Trebuie să porniţi apoi Serverul HTTP în modul securizat. Dacă nu aţi configurat şi pornit Serverul HTTP pentru operare SSL, veţi vedea un mesaj de eroare şi browserul dvs. nu va deschide o sesiune securizată.

Pornirea

Deşi s-ar putea să doriţi să folosiţi certificate pentru a realiza un număr de cerinţe legate de securitate, ceea ce veţi face mai întâi depinde de cum veţi planifica să vă obţineţi certificatele. Există două căi primare pe care le puteţi urma atunci când folosiţi pentru prima oară DCM, diferind dacă vreţi să folosiţi certificate private sau emiterea de certificate private:

Creaţi şi operaţi un CA local pentru a emite certificate către aplicaţiile dvs.

Administraţi certificate de la un CA Internet public pentru a le folosi aplicaţiile dvs.

Crearea şi operarea cu un CA local

După ce revedeţi cu atenţie poliţele şi nevoile dvs. de securitate, vă decideţi să operaţi cu un CA local pentru a emite certificate private pentru aplicaţiile dvs. Puteţi folosi DCM să creaţi şi să operaţi cu propriul dvs. CA local. DCM vă oferă un task asistat care vă poartă prin acest proces de creare a CA şi de folosire a ei pentru a emite certificate pentru aplicaţii. Calea task-ului asistat se asigură că aveţi toate de care aveţi nevoie pentru a începe utilizarea certificatelor digitale pentru a configura aplicaţiile să folosească SSL şi să semneze obiecte şi să verifice semnătura obiectelor.

Notă: Pentru a folosi certificate cu Serverul HTTP IBM pentru iSeries, trebuie să creaţi şi să vă configuraţi serverul dumneavoastră web înainte de a lucra cu DCM. Când configuraţi un server web să folosească SSL, este generat un ID aplicaţie pentru server. Trebuie să notaţi acest ID aplicaţie pentru a folosi DCM pentru a specifica ce certificat ar trebui să folosească această aplicaţie păntru SSL.

Nu terminaţi şi reporniţi serverul până nu folosiţi DCM să asigneze un certificat către server. Dacă terminaţi şi reporniţi instanţa *ADMIN a serverului web înainte de asignarea unui certificat către ea, serverul nu va porni şi nu veţi putea să folosiţi DCM să asignaţi un certificat către server.

Pentru a folosi DCM să creeze şi să opereze cu un CA local, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare al DCM, selectaţi **Crearea unei Autorităţi de certificare (CA)** pentru a se afişa o serie de formulare. Aceste formulare vă îndrumă prin procesul creării unui CA local şi completării altor taskuri necesare pentru a începe folosirea certificatelro digitale pentru SSL, semanrea obiectelor şi verificarea semnăturii.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Completaţi toate formularele pentru acest task. În folosirea aceste formulare pentru a realiza toate taskurile de care aveţi nevoie pentru a seta un CA local care funcţionează, duumneavoastră:
   a. Alegeţi cum să memoraţi cheia privată pentru certificatul CA local. (Acest pas este inclus doar dacă aveţi un Coprocesor Criptografic IBM 4758–023 PCI instalat pe iSeries-ul dvs. Dacă sistemul nu are un coprocesor criptografic, DCM va plasa automat certificatul şi cheia privată în Autoritatea de certificare locală.)

b. Furnizaţi informaţiile de identificare pentru CA local.
c. Instalaţi certificatul CA local pe PC-ul dvs. sau în browserul dvs. astfel încât software-ul dvs. să poată recunoaşte CA local şi să valideze certificatele pe care le emite CA.
d. Alegeţi datele politicii pentru CA-ul dvs. Local.
e. Folosiţi noul CA local pentru a emite un certificat server sau client pe care aplicaţiile dvs. să îl poată folosi pentru conexiuni SSL. (Dacă iSeries-ul dumneavoastră are un Coprocesor Criptografic IBM 4758–023 PCI instalat, acest pas vă permite să selectaţi cum să memoraţi cheia privată pentru certificatul server sau client. Dacă sistemul nu are un coprocesor, DCM va plasa automat certificatul şi cheia privată în depozitul de certificate *SYSTEM. DCM crează depozitul de certificate *SYSTEM ca parte a acestui subtask.)
f. Selectaţi aplicaţiile care pot folosi certificatul client sau server pentru conexiuni SSL.

   Notă: Dacă aţi folosit DCM pentru a crea anterior depozitul de certificate *SYSTEM pentru a gestiona certificate pentru SSL de la o CA publică Internet, nu efectuaţi acest lucru sau pasul anterior.
g. Folosiţi noul CA local pentru a emite un certificat de semnare obiect pe care aplicaţiile să îl poată folosi pentru a semna digital obiecte. Acest subtask crează depozitul de certificate *OBJECTSIGNING; acesta este depozitul de certificate pe care îl folosiţi pentru a gestiona certificate care semnează obiecte.
h. Selectaţi aplicaţiile care pot folosi certificatul care semnează obiecte pentru a plasa semnături digitale pe obiecte.

   Notă: Dacă aţi folosit anterior DCM pentru a crea depozitul de certificate *OBJECTSIGNING pentru a gestiona certificate care semnează obiecte de la o CA publică Internet, nu efectuaţi acest lucru sau pasul anterior.
i. Selectaţi aplicaţiile care ar trebui să aibă încredere în CA-ul dvs. Local.

Atunci când terminaţi task-ul asistat, sunteţi gata să începeţi configurarea aplicaţiilor pentru a folosi SSL pentru comunicaţii sigure.

După ce vă configuraţi aplicaţiile, utilizatorii care accesează aplicaţiile printr-o conexiune SSL trebuie să folosescă DCM pentru a obţine o copie a certificatului CA local. Fiecare utilizator trebuie să aibă o copie a certificatului pentru ca software-ul client al utilizatorului să îl poată folosi pentru a autentifica identitatea serverului ca parte a procesului de negociere SSL. Utilizatorii pot folosi DCM fie pentru a copia certificatul CA local într-un fişier, fie pentru a descărca certificatul în browser-ul lor. Cum memorează utilizatorii certificatul CA local depinde de software-ul client pe care îl folosesc pentru a stabili o conexiune SSL la o aplicaţie.

De asemenea, puteţi folosi acest CA local pentru a emite certificate către aplicaţii de pe alte sisteme iSeries din reţeaua dvs.

Pentru a afla mai multe despre folosirea DCM pentru gestionarea certificatelor utilizator şi cum pot obţine utilizatorii o copie a certificatului CA local pentru a autentifica certificatele pe care le emite CA local, revedeţi aceste subiecte:

Gestionare certificate utilizator
Aflaţi cum pot folosi utilizatorii dvs. DCM pentru a obţine certificate sau să asocieze certificate existente cu profilele lor utilizator iSeries.

Folosiţi API-uri pentru a emite prin programe certificate către utilizatori non-iSeries
Aflaţi cum puteţi folosi CA local pentru a emite certificate private către utilizatori fără a asocia certificatul cu un profil utilizator iSeries.

Obţineţi o copie a certificatului CA privat
Aflaţi cum să obţineţi o copie a certificatului CA privat şi instalaţi-l pe PC-ul dvs. astfel încât să puteţi autentifica orice certificate server pe care le emite CA.

Gestionare certificate utilizator

Dvs. şi utilizatorii dvs. puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele pe care Dvs. şi utilizatorii dvs. le folosiţi şi de care aveţi nevoie pentru a participa în sesiuni Secure Sockets Layer (SSL).

Dacă utilizatorii accesează serverele publice sau interne printr-o conexiune SSL, aceştia trebuie să aibă o copie a certificatului CA (autoritate de certificare) care a emis certificatul serverului. Ei trebuie să aibă certificatul CA pentru ca software-ul client să poată valida autenticitatea certificatului server pentru a stabili o conexiune. Dacă server-ul foloseşte un certificat care provine de la o CA publică, software-ul utilizatorilor trebuie să aibă deja o copie a certificatului CA. În consecinţă, nici dvs. ca administrator al DCM, nici utilizatorii dvs. nu trebuie să luaţi nici o acţiune înainte de a participa într-o sesiune SSL. Totuşi, dacă serverul dumneavoastră foloseşte un certificat de la un CA local privat, utilizatorii dumneavoastră trebuie să obţină o copie a certificatului CA local înainte să poată stabili o sesiune SSL cu serverul.

În plus, dacă aplicaţia server suportă şi cere autentificarea clienţilor prin certificate, utilizatorii trebuie să prezinte un certificat utilizator acceptat pentru a accesa resursele pe care le furnizează server-ul. În funcţie de nevoile dumneavoastră de securitate, utilizatorii pot prezenta un certificat de la un CA Internet public sau unul pe care îl obţin de la CA local pe care îl folosiţi dumneavoastră. Dacă aplicaţia server a dumneavoastră furnizează acces la resurse pentru utilizatorii interni care au în acest moment iSeries profile utilizator, puteţi folosi DCM pentru a le adăuga certificatele lor la profilele lor de utilizator. Această asociere asigură faptul că utilizatorii au acelaşi acces şi aceleaşi restricţii pentru resurse când prezintă certificate ca şi cele garantate de profilul lor de utilizator.

Digital Certificate Manager (DCM) vă permite să gestionaţi certificate care sunt asignate unui profil de utilizator iSeries. Dacă aveţi un profil de utilizator cu autorizaţii speciale *ALLOBJ, puteţi gestiona atribuirea de certificate profil de utilizator pentru Dvs. ca şi pentru alţi utilizatori. Când nu este deschis nici un depozit de certificate, sau când depozitul de certificate CA (autoritate de certificare) locală este deschis, puteţi selecta **Gestionarea certificatelor utilizator** din cadrul de navigare pentru a accesa task-urile necesare. Dacă este deschis un depozit de certificate diferit, task-urile certificat utilizator sunt integrate în task-uri sub **Gestionarea certificatelor**.

Utilizatoriii fără autorizările speciale de profil de utilizator *SECADM şi *ALLOBJ îşi pot gestiona doar propriile asignări de certificate. Ei pot selecta **Gestionare certificate Utilizator** pentru a accesa taskuri care le permit să vizualizeze certificatele asociate cu profilele lor de utilizator , să şteargă un certificat din profilele lor de utilizator sau să asigneze un certificat de la un CA diferit la profilele lor de utilizator. Utilizatorii, indiferent de autorizările speciale pentru profilele lor de utilizator, pot obţine un certificat utilizator de la CA local prin selectarea taskului **Creare certificate** din cadrul de navigaţie principal.

Pentru a afla mai multe despre cum să folosiţi DCM pentru a gestiona şi crea certificate utilizator, revedeţi aceste subiecte:

Crearea unui certificat utilizator
Folosiţi această informaţie pentru a afla cum pot utilizatorii să folosească CA local pentru a emite un certificat pentru autentificarea clientului.

Asignarea unui certificat utilizator
Folosiţi aceste informaţii pentru a afla cum să asociaţi un certificat pe care îl deţineţi cu profilul dvs. de utilizator. Certificatul poate fi de la un CA local privat de pe alt sistem sau de la un CA Internet bine-cunoscut. Înainte de a putea atribui un certificat profilului utilizator, Autoritatea de certificare care emite trebuie să fie de încredere pentru server, iar certificatul nu trebuie să fie deja asociat cu un profil utilizator de pe sistem.

Crearea unui certificat utilizator: Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă folosiţi Digital Certificate Manager (DCM) pentru a lucra cu o Autoritate de Certificare locală privată (CA), puteţi folosi CA local pentru a emite certificate către fiecare utilizator. Fiecare utilizator trebuie să acceseze DCM pentru a obţine un certificat folosind task-ul **Crearea certificatelor**. Pentru a obţine un certificat de la CA local, politica CA trebuie să permită ca CA să emită certificate utilizator.

Pentru a obţine un certificat de la CA local, urmaţi aceşti paşi:
1. Porniţi DCM.
2. În cadrul de navigare, selectaţi **Crearea certificatelor**.
3. Selectaţi **Certificate utilizator** pentru tipul certificatului pe care îl creaţi. Se va afişa un formular în care veţi putea introduce informaţii de identificare pentru certificat.
4. Completaţi formularul şi apăsaţi **Continuare**.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
5. În acest punct, DCM lucrează cu browser-ul pentru a crea cheile private şi publice pentru certificate. Browserul poate afişa mai multe ferestre pentru a vă ghida prin acest proces. Urmaţi instrucţiunile browserului pentru aceste task-uri. După ce browser-ul generează cheile, se va afişa o pagină de confirmare care va indica faptul că DCM-ul a creat certificatele.
6. Instalaţi noul certificat în browser-ul dumneavoastră. Browserul poate afişa mai multe ferestre pentru a vă ghida prin acest proces. Urmaţi instrucţiunile date de browser pentru a termina acest task.
7. Apăsaţi **OK** pentru a încheia taskul.

În timpul procesării, Digital Certificate Manager asociază automat certificatul cu profilul dumneavoastră iSeries de utilizator.

Dacă doriţi ca un certificat de la alt CA pe care un utilizator îl prezintă pentru autentificare client să aibă aceleaşi autorizări ca profilele lor utilizator, utilizatorul poate folosi DCM pentru a asigna certificatul la profilele lor utilizator.

Asignarea unui certificat utilizator: Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă utilizatorii trebuie să prezinte certificate de la o CA (autoritate de certificare) publică Internet, ei pot utiliza DCM (Digital Certificate Manager) pentru a atribui certificatele profilelor lor de utilizator. Acest lucru vă permite dvs. şi utilizatorului să folosească DCM pentru administrarea acestor certificate.

Pentru a folosi task-ul **Atribuirea certificatelor utilizator**, trebuie să aveţi sesiuni sigure cu server-ul HTTP prin care accesaţi DCM-ul (Digital Certificate Manager). Faptul că aveţi sau nu sesiuni sigure este determinat de numărul de port din URL-ul folosit pentru accesarea DCM-ului. Dacă folosiţi portul 2001, care este portul implicit pentru accesarea DCM, atunci nu aveţi o sesiune sigură. De asemenea, Serverul HTTP trebuie configurat să folosească SSL înainte să puteţi comuta pe o conexiune securizată.

Când selectaţi acest task, se va afişa o nouă fereastră pentru browser. Dacă nu aveţi o sesiune sigură, DCM vă cere să efectuaţi un clic pe **Atribuirea unui certificat utilizator** pentru a porni una. Apoi, DCM începe negocierile Secure Sockets Layer (SSL) cu browser-ul.

Ca parte a acestor negocieri, s-ar putea ca browser-ul să vă întrebe dacă aveţi încredere în CA (autoritatea de certificare) care a emis certificaul care identifică server-ul HTTP. De asemenea, browser-ul vă poate întreba dacă acceptaţi sau nu certificatul server.

După ce permiteţi browser-ului să aibă încredere în CA şi să accepte certificatul server, server-ul vă poate cere să prezentaţi un certificat pentru autentificarea client. În funcţie de setările din configurare pentru browser, acesta vă poate cere să selectaţi un certificat pe care să îl folosească pentru autentificare. Dacă browser-ul prezintă un certificat de la o CA pe care sistemul îl acceptă ca fiind de încredere, DCM va afişa informaţiile despre certificat într-o fereastră separată. Dacă nu prezentaţi un certificat acceptabil, server vă poate cere în schimb numele utilizator şi parola pentru autentificare înainte de a vă permite accesul.

După ce s-a stabilit o sesiune sigură, DCM-ul încearcă să ia un certificat bun de la browser pe care să îl poată asocia cu profilul de utilizator. Dacă DCM-ul obţine cu succes unul sau mai multe certificate, puteţi vedea informaţiile despre certificat şi puteţi alege să îl asociaţi cu profilul de utilizator.

Dacă DCM nu afişează informaţia dintr-un certificat, înseamnă că nu aţi putut oferi un certificat pe care DCM-ul să îl poată asocia cu profilul de utilizator. De acest lucru poate fi responsabilă una dintre problemele certificatelor utilizator. De exemplu, certificatele pe care le conţine browser-ul pot fi deja asociate cu profilul de utilizator.

Dacă preferaţi să folosiţi un CA local pentru a emite certificate către utilizatorii dumneavoastră, utilizatorii trebuie să creeze un certificat utilizator în schimb.

Folosiţi API-uri pentru a emite prin programe certificate către utilizatori non-iSeries

Începând cu V5R2, sunt două API-uri noi disponibile pe care le puteţi folosi pentru a emite prin program certificate către utilizatorii non-iSeries. În versiunile anterioare, când foloseaţi CA-ul dvs. Local pentru a emite certificate către utilizatori, aceste certificate erau automat asociate cu profilele lor utilizator iSeries . În consecinţă, pentru a folosi CA local pentru a emite un certificat către un utilizator pentru autentificare client, trebuia să furnizaţi acel utilizator cu un profil utilizator iSeries . De asemenea, când utilizatorii aveau nevoie să obţină un certificat de la un CA local pentru autentificare client, fiecare utilizator trebuia să folosească DCM pentru a crea certificatul necesar. Aşadar, fiecare utilizator trebuie să aibă un profil utilizator pe serverul iSeries care găzduieşte DCM şi o înregistrare validă la acel server iSeries .

Având certificatul asociat cu un profil de utilizator are avantajele sale, mai ales când este vorba de utilizatorii interni. Totuşi, aceste restricţii şi cerinţe au făcut mai puţin practică folosirea CA-ului Local pentru a emite certificate utilizator pentru un număr mare de utilizatori, mai ales când nu doriţi ca acei utilizatori să aibă un profil utilizator iSeries . Pentru a evita furnizarea de profile utilizator acelor utilizatori, ar trebui să cereţi utilizatorilor să plătească pentru un certificat de la un CA bine-cunoscut dacă doriţi să necesite certificate pentru autentificare utilizator pentru aplicaţiile dvs.

Aceste două noi API-uri oferă suportul care vă permite să furnizaţi o interfaţă pentru crearea certificatelor utilizator semnate de certificatul CA local pentru orice nume utilizator. Acest certificat nu va fi asociat cu un profil utilizator. Utilizatorul nu trebuie să existe pe serverul iSeries care găzduieşte DCM şi utilizatorul nu trebuie să folosească DCM pentru a crea certificatul.

Există două API-uri, unul pentru fiecare din programele browser predominante, pe care le puteţi invoca când folosiţi Net.Data pentru a crea un program pentru emiterea certificatelor către utilizatori. Aplicaţia pe care o creaţi trebuie să dispună de codul Interfaţă Utilizator Grafică (GUI) necesar pentru a crea certificatul utilizator şi pentru a apela unul din API-urile corespunzătoare pentru a folosi CA local pentru a semna certificatul.

Pentru mai multe informaţii despre folosirea acestor API-uri, vedeţi aceste pagini:
- Generate and Sign User Certificate Request (QYCUGSUC) API.
- Sign User Certificate Request (QYCUSUC) API.

Obţineţi o copie a certificatului CA privat

Atunci când accesaţi un server care foloseşte o conexiune Secure Sockets Layer (SSL), serverul va prezenta software-ului client un certificat ca dovadă a identităţii sale. Software-ul client trebuie mai apoi să valideze certificatul server-ului înainte ca acesta să poată stabili o sesiune. Pentru a se valida certificatul server, software-ul client trebuie să aibă acces la o copie stocată local a certificatului pentru CA (autoritatea de certificare) care a emis certificatul server. Dacă serverul prezintă un certificat de la un CA Internet public, browserul dumneavoastră sau alt software client ar trebui să aibă deja o copie a certificatului CA. Dacă totuşi, serverul prezintă un certificat de la un CA local privat, trebuie să folosiţi Digital Certificate Manager (DCM) pentru a obţine o copie a certificatului CA local.

Puteţi folosi DCM pentru a descărca certificatul CA local CA direct în browserul dumneavoastră sau puteţi copia certificatul CA local într-un fişier astfel încât alt software client să-l poată şi folosi. Dacă folosiţi atât browserul dumneavoastră cât şi alte aplicaţii pentru comunicaţii securizate, s-ar putea să trebuiască să folosiţi ambele metode pentru a instala certificatul CA local. Dacă folosiţi ambele metode, instalaţi certificatul în browser înainte de a-l copia într-un fişier.

Dacă aplicaţia server vă cere să vă autentificaţi prezentând un certificat de la CA local, trebuie să descărcaţi certificatul CA local în browserul dumneavoastră înainte să cereţi un certificat utilizator de la CA local.

Pentru a folosi DCM să obţineţi o copie a certificatului CA local, urmaţi aceşti paşi:
1. Porniţi DCM.
2. În cadrul de navigare, selectaţi **Instalare certificat CA local pe PC-ul dumneavoastră** pentru a afişa o pagină care vă permite să descărcaţi certificatul CA local în browserul dumneavoastră sau să-l memoraţi într-un fişier pe sistemul dumneavoastră.
3. Selectaţi o metodă pentru obţinerea certificatului CA local.
   a. Selectaţi **Instalare certificat** pentru a descărca certificatul CA local ca o rădăcină de încredere în browserul dumneavoastră. Astfel vă veţi asigura că browser-ul poate stabili sesiuni de comunicaţii sigure cu serverele care folosesc un certificat provenind de la acest CA. Browser-ul va afişa o serie de ferestre care vă vor ajuta să termina instalarea.
   b. Selectaţi **Copiere şi Lipire certificat** pentru a afişa o pagină care conţine o copie codată special a certificatului CA local. Se copiază obiectul text din pagină în clipboard. Mai târziu se va lipi (paste) această informaţie într-un fişier. Acest fişier este utilizat de un program utilitar PC (precum MKKF sau IKEYMAN) la stocarea certificatelor pentru a fi utilizate de programe client pe PC. Înainte ca aplicaţiile dumneavoastră client că poată recunoaşte şi folosi certificatul CA local pentru autentificare, trebuie să configuraţi aplicaţiile să recunoască certificatul ca o rădăcină de încredere. Urmaţi instrucţiunile pe care vi le furnizează aceste aplicaţii pentru a folosi fişierul.
4. Apăsaţi **OK** pentru a reveni la pagina de bază (home) a Digital Certificate Manager.

Gestionare certificate de pe un CA Internet public

După ce v-aţi revăzut atent nevoile şi politicile de securitate, aţi decis că doriţi să folosiţi certificate de la o CA (autoritate de certificare) Internet publică, cum ar fi VeriSign. De exemplu, operaţi un site de web public şi doriţi să folosiţi Secure Sockets Layer (SSL) pentru comunicaţii sigure pentru a asigura confidenţialitatea anumitor tranzacţii de informaţii. Deoarece site-ul de web este accesibil publicului în general, doriţi să folosiţi certificate pe care le pot recunoaşte uşor majoritatea browser-elor.

Sau, dezvoltaţi aplicaţii pentru clienţi externi şi doriţi să folosiţi un certificat public pentru a semna digital pachetele aplicaţiei. Prin semnarea pachetelor aplicaţiei, clienţii vor putea fi siguri de faptul că pachetul provine de la compania dvs. şi că nu a fost alterat de alte părţi neautorizate în timpul tranzitului. Doriţi să folosiţi un certificat public astfel încât clienţii să poată verifica uşor şi necostisitor semnătura digitală a pachetului. De asemenea, puteţi folosi acest certificat pentru a verifica semnătura înainte de a trimite pachetul clenţilor.

Puteţi folosi task-urile asistate din DCM (Digital Certificate Manager) pentru a gestiona centralizat aceste certificate publice şi aplicaţiile care le folosesc pentru a stabili conexiuni SSL, pentru a semna obiecte sau pentru a verifica autenticitatea semnăturilor obiectelor.

Gestionare certificate publice

Atunci când folosiţi DCM pentru a gestiona certificate provenite de la o CA publică Internet, trebuie să creaţi mai întâi un depozit de certificate. Un depozit de certificate este un fişier bază de date de chei special pe care îl foloseşte DCM (Digital Certificate Manager) pentru a stoca certificate digitale şi cheile lor private asociate. DCM vă permite să creaţi şi să gestionaţi mai multe tipuri de depozite de certificate pe baza certificatelor pe care le conţin.

Tipul de depozit de certificate pe care l-aţi creat şi task-urile pe care trebuie să le efectuaţi ulterior pentru gesionarea certificatelor şi a aplicaţiilor care le folosesc, depinde de modul în care doriţi să folosiţi certificatele. Pentru a afla cum să folosiţi DCM pentru a crea depozitul de certificate corespunzător şi pentru a gestiona certificatele Internet necesare aplicaţiilor, revedeţi aceste subiecte:

- Gestionare certificate Internet publice pentru sesiuni de comunicare SSL .
- Gestionare certificate Internet publice pentru semnarea obiectelor.
- Gestionare certificate Internet pentru verificarea semnăturilor obiectelor .

DCM de asemenea vă permite să gestionaţi certificatele pe care le obţineţi dintr-o Infrastructură de Chei Publice pentru Autoritatea de certificare X.509 (PKIX).

Gestionare certificate Internet publice pentru sesiuni de comunicare SSL

Puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele publice Internet pe care aplicaţiile le folosesc pentru a stabili sesiuni de comunicare sigure cu Secure Sockets Layer (SSL). Dacă nu folosiţi DCM pentru a lucra cu Autoritatea de certificare locală (CA) a dumneavoastră, trebuie să creaţi întâi depozitul corespunzător pentru certificate pentru gestionarea certificatelor publice pe care le folosiţi pentru SSL. Aceasta este depozitul de certificate *SYSTEM. Atunci când creaţi un depozit de certificate, DCM vă conduce prin procesul de creare a informaţiilor de cerere a certificatului pe care trebuie să le furnizaţi Autorităţii de certificare publice pentru a obţine un certificat.

Pentru a folosi DCM pentru a administra şi folosi certificate publice Internet pentru ca aplicaţiile să poată stabili sesiuni de comunicare SSL, urmaţi aceşti paşi:

1. Porniţi DCM.

2. În cadrul de navigare al DCM, selectaţi **Crearea unui nou depozit de certificate** pentru a porni task-ul asistat şi pentru a completa o serie de formulare. Aceste formulare vă vor ghida prin procesul de creare a unui depozit de certificate şi a unui certificat pe care aplicaţiile le pot folosi pentru sesiuni SSL.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular în acest task asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Selectaţi ***SYSTEM** ca depozit de certificate pentru a o crea şi apăsaţi **Continuare**.
4. Selectaţi **Da** pentru a crea un certificat ca parte a creării depozitului de certificate *SYSTEM şi apăsaţi **Continuare**.
5. Selectaţi **VeriSign sau altă CA Internet (autoritate de certificare)** ca semnatar al noului certificat şi efectuaţi un clic pe **Continuare** pentru a se afişa un formular care vă va permite să introduceţi informaţii de identificare pentru noul certificat.

   Notă: Dacă iSeries-ul dumneavoastră are un IBM 4758–023 PCI Coprocesor Criptografic instalat, DCM că permite să selectaţi cum să memoraţi cheia privată pentru certificat ca taskul următor. Dacă sistemul nu are un coprocesor, DCM va plasa automat cheia privată în depozitul de certificate *SYSTEM. Dacă aveţi nevoie de ajutor la selectarea modului de depozitare al cheii private, consultaţii ajutorul the online al DCM.
6. Completaţi formularul şi apăsaţi **Continuare** pentru a se afişa pagina de confirmare. Această pagină de confirmare va afişa datele cererii certificatului pe care trebuie să îl furnizaţi autorităţii de certificare (CA) publice care va emite certificatul. Datele CSR (cerere de semnare a certificatului) consistă în cheia publică şi alte informaţii pe care le specificaţi pentru noul certificat.
7. Copiaţi cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fişier separat, pe care îl solicită CA publică pentru cererea unui certificat. Trebuie să folosiţi toate datele CSR, inclusiv liniile Begin şi End New Certificate Request. Atunci când părăsiţi această pagină, datele vor fi pierdute şi nu se vor mai putea recupera. Trimiteţi formularul sau fişierul aplicaţiei către CA aleasă pentru emiterea şi semnarea certificatului.

   Notă: Trebuie să aşteptaţi ca CA să vă returneze certificatul completat şi semnat înainte de a putea încheia procedura.

   Notă: Pentru a folosi certificate cu Serverul HTTP pentru iSeries, trebuie să creaţi şi să vă configuraţi serverul dumneavoastră de web înainte de a lucra cu DCM pentru a lucra cu certificatul complet semnat. Când configuraţi un server web să folosească SSL, este generat un ID aplicaţie pentru server. Trebuie să notaţi acest ID aplicaţie pentru a folosi DCM pentru a specifica ce certificat ar trebui să folosească această aplicaţie păntru SSL.

   Nu terminaţi şi reporniţi serverul până nu folosiţi DCM să asigneze certificatul complet semnat către server. Dacă terminaţi şi reporniţi instanţa *ADMIN a serverului web înainte de asignarea unui certificat către ea, serverul nu va porni şi nu veţi putea să folosiţi DCM să asignaţi un certificat către server.
8. Porniţi DCM după ce CA publică vă întoarce certificatul semnat.
9. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
10. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apăsaţi **Continuare**.
11. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.

12. Din lista de task-uri, selectaţi **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate *SYSTEM. După ce se termină importarea certificatului, puteţi specifica aplicaţiile care ar trebui să îl folosească cu comunicaţiile SSL.
13. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de task-uri.
14. Din lista de task-uri, selectaţi **Actualizarea atribuirii certificatelor** pentru a se afişa o listă de aplicaţii active-SSL pentru care puteţi atribui un certificat.
15. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Actualizarea atribuirii certificatelor**.
16. Selectaţi certificatul pe care l-aţi importat şi efectuaţi un clic pe **Atribuirea noului certificat**. DCM va afişa un mesaj pentru a confirma selecţia certificatului pentru aplicaţie.

    Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. Dacă doriţi ca o aplicaţie cu acest suport să poată să autentifice certificate înainte de a accesa resursele, trebuie să definiţi o listă de încredere CA pentru aplicaţie. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă o aplicaţie utilizator sau client prezintă un certificat care provine de la o CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază a unei autentificări valide.

Atunci când terminaţi task-ul asistat, sunteţi gata să începeţi configurarea aplicaţiilor pentru a folosi SSL pentru comunicaţii sigure. Înainte ca utilizatorii să poată accesa aceste aplicaţii printr-o conexiune SSL, ei trebuie să aibă o copie a certificatului CA care a emis certificatul server. Dacă certificatul este de la o CA Internet binecunoscută, s-ar putea ca software-ul utilizatorilor să aibă deja o copie a certificatului CA necesar. Dacă utilizatorii nu obţin certificatul CA, ei ar trebui să acceseze site-ul de web pentru CA şi să urmeze instrucţiunile oferite de site.

Gestionare certificate Internet publice pentru semnarea obiectelor

Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona certificate Internet publice pentru a semna digital obiectele. Dacă nu folosiţi DCM pentru a opera propria dvs. Autoritate de Certificare (Certificate Authority - CA) Locală, trebuie mai întâi să creaţi un depozit de certificate corespunzător pentru gestionarea certificatelor publice pe care le folosiţi pentru semnarea obiectelor. Acesta este depozitul de certificate *OBJECTSIGNING. Când creaţi un depozit de certificate, DCM vă trece prin procesul creării informaţiilor de cerere a unui certificat pe care trebuie să le furnizaţi către CA-ul Internet public pentru a obţine un certificat.

De asemenea, pentru a folosi certificatul pentru semnarea obiectelor, trebuie să definiţi ID-ul aplicaţiei. Acest ID al aplicaţiei controlează câtă autoritate este necesară pentru ca cineva să semneze obiecte cu un certificat specific şi oferă un alt nivel de control al accesului pe lângă cel oferit de DCM. Implicit, definiţia aplicaţiei cere ca utilizatorul să aibă autoritate specială *ALLOBJ pentru a folosi certificatul în semnarea obiectelor de către aplicaţie. (Oricum, puteţi schimba autorizarea pe care o necesită identificatorul de aplicaţie folosind iSeries Navigator.)

Pentru a folosi DCM pentru a administra şi folosi certificate publice Internet pentru semnarea obiectelor, realizaţi aceste task-uri:

1. Porniţi DCM.
2. În cadrul stâng de navigare al DCM, selectaţi **Crearea unui nou depozit de certificate** pentru a porni task-ul asistat şi pentru a completa o serie de forme. Aceste formulare vă vor ghida prin procesul de creare a unui depozit de certificate şi a unui certificat pe care aplicaţiile le pot folosi pentru semnarea obiectelor.

Notă: Dacă aveţi întrebări despre completarea unui anume formular în acest task asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.

3. Selectaţi ***OBJECTSIGNING** drept depozitul de certificate de creat şi faceţi click pe **Continuare**.
4. Selectaţi **Da** pentru a crea un certificat ca parte a creării depozitului de certificate şi apăsaţi **Continuare**.
5. Selectaţi **VeriSign sau altă CA Internet (autoritate de certificare)** ca semnatar al noului certificat şi efectuaţi un clic pe **Continuare**. Astfel se va afişa un formular care vă va permite să introduceţi informaţii de identificare pentru noul certificat.
6. Completaţi formularul şi apăsaţi **Continuare** pentru a se afişa pagina de confirmare. Această pagină de confirmarea va afişa datele cererii certificatului pe care trebuie să îl furnizaţi Autorităţii de certificare publice care va emite certificatul. Datele CSR (cerere de semnare a certificatului) consistă în cheia publică şi alte informaţii pe care le specificaţi pentru noul certificat.
7. Copiaţi cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fişier separat, pe care îl cere CA publică pentru cererea unui certificat. Trebuie să folosiţi toate datele CSR, inclusiv liniile Begin şi End New Certificate Request. Atunci când părăsiţi această pagină, datele vor fi pierdute şi nu se vor mai putea recupera. Trimiteţi formularul sau fişierul aplicaţiei către CA pe care aţi ales-o pentru emiterea şi semnarea certificatului.

   Notă: Trebuie să aşteptaţi ca CA să vă returneze certificatul completat şi semnat înainte de a putea încheia procedura.
8. Porniţi DCM după ce CA publică vă întoarce certificatul semnat.
9. În cadrul de navigare din stânga, alegeţi **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** în timp ce se deschide certificatul.
10. Când este afişată pagina Depozit de certificate şi Parola, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apoi apăsaţi **Continuare**.
11. În cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a se afişa o listă de task-uri.
12. Din lista de task-uri, selectaţi **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate *OBJECTSIGNING. După ce se termină importarea certificatului, puteţi crea o definiţie de aplicaţie care să folosească certificatul pentru semnarea obiectelor.
13. După ce se reafişează cadrul de navigare din stânga, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de task-uri.
14. Din lista de task-uri, selectaţi **Adăugarea aplicaţiei** pentru a începe procesul de creare a unei definiţii aplicaţie care semnează obiecte pentru a folosi certificatul în semnarea obiectelor.
15. Completaţi formularul pentru a defini aplicaţia care semnează obiecte şi efectuaţi un clic pe **Adăugare**. Această definiţie aplicaţie nu descrie o aplicaţie reală, ci mai degrabă tipul de obiecte pe care doriţi să le formaţi cu un anume certificat. Folosiţi ajutorul online pentru a afla cum să completaţi formularul.
16. Selectaţi **OK** pentru a recunoaşte mesajul de confirmare al definiţiei aplicaţie şi pentru a afişa lista de task-uri Gestionarea aplicaţiilor.
17. Din lista de task-uri, selectaţi **Actualizare asignare certificate** şi apăsaţi **Continuare** pentru a afişa o listă de ID-uri de aplicaţii de semnare obiecte pentru care puteţi asigna un certificat.
18. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Actualizarea atribuirii certificatelor**.

19. Selectaţi certificatul pe care l-aţi importat şi efectuaţi un clic pe **Atribuirea noului certificat**.

Atunci când terminaţi aceste task-uri, puteţi începe semnarea obiectelor pentru a le asigura integritatea.

Când distribuiţi obiecte semnate, cei care primesc obiectele trebuie să folosească o versiune V5R1 sau mai nouă a DCM pentru a valida semnătura de pe obiecte pentru a se asigura că datele sunt nemodificate şi pentru a verifica identitatea expeditorului. Pentru validarea semnăturii, destinatarul trebuie să aibă o copie a certificatului de verificare a semnăturii. Ar trebui să furnizaţi o copie a acestui certificat ca parte a pachetului de obiecte semnate.

De asemenea, destinatarul trebuie să aibă o copie a certificatului CA pentru CA care a emis certificatul server pe care l-aţi folosit pentru semnarea obiectului. Dacă aţi semnat obiectul cu un certificat provenind de la o CA Internet binecunoscută, s-ar putea ca versiunea DCM a destinatarului să aibă deja o copie a certificatului CA necesar. Totuşi, trebuie să furnizaţi o copie a certificatului CA împreună cu obiectele semnate dacă presupuneţi că destinatarul s-ar putea să nu aibă o copie. De exemplu, ar trebui să furnizaţi o copie a certificatului CA-ului Local dacă aţi semnat obiectele cu un certificat de la un CA local private. Din motive de securitate, ar trebui să furnizaţi certificatul CA într-un pachet separat sau să faceţi disponibil public certificatul la cerere celor care au nevoie de el.

Gestionare certificate pentru verificarea semnăturii obiectelor

Puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele de verificare a semnăturilor obiectelor pe care le folosiţi pentru a valida semnăturile digitale ale obiectelor. Pentru a semna un obiect, folosiţi cheia privată a certificatului pentru a crea semnătura. Atunci când trimiteţi altora obiectul semnat, trebuie să includeţi o copie a certificatului care a semnat obiectul. Acest lucru îl puteţi face folosind DCM pentru a exporta certificatul de semnare a obiectelor (fără cheia privată a certificatului) drept certificat de verificare a semnăturii. Puteţi exporta un certificat de verificare a semnăturii într-un fişier pe care puteţi mai apoi să îl distribuiţi. Sau, dacă doriţi să verificaţi semnăturile pe care le-aţi creat, puteţi exporta un certificat de verificare a semnăturilor în depozitul de certificate *SIGNATUREVERIFICATION.

Pentru a valida semnătura unui obiect, trebuie să aveţi o copie a certificatului care a semnat obiectul. Folosiţi cheia publică a certificatului, pe care o conţine acesta, pentru a examina şi verifica semnătura care a fost creată cu cheia privată corespunzătoare. De aceea, înainte de a putea verifica semnătura unui obiect, trebuie să obţineţi o copie a certificatului care l-a semnat de la cel care v-a furnizat obiectele semnate.

De asemenea, trebuie să aveţi o copie a certificatului CA (autoritate de certificare) pentru CA care a emis certificatul care a semnat obiectul. Folosiţi certificatul CA pentru a verifica autenticitatea certificatului care a semnat obiectul. DCM oferă copii de certificate CA de la cele mai cunoscute CA-uri. Dacă, oricum, obiectul a fost semnat de un certificat de la altă AC publică sau de la o CA local privată, trebuie să obţineţi o copie a certificatului AC înainte să puteţi verifica semnătura obiectului.

Pentru a folosi DCM pentru verificarea semnăturilor obiectelor , trebuie să creaţi mai întâi depozitul de certificate necesar pentru gestionarea certificatelor necesării verificării semnăturilor; acesta este depozitul de certificate *SIGNATUREVERIFICATION. Când creaţi acest depozit de certificate, DCM îl populează automat cu copii ale celor mai cunoscute certificate CA publice.

Notă: Dacă doriţi să puteţi verifica semnăturile pe care le-ţi creat cu propriile certificate de semnarea a obiectelor, trebuie să creaţi depozitul de certificate *SIGNATUREVERIFICATION şi să copiaţi certificatele din depozitul de certificate

*OBJECTSIGNING în el. Acest lucru este adevărat chiar dacă vreţi să efectuaţi verificarea semnăturilor din depozitul de certificate *OBJECTSIGNINGe.

Pentru a folosi DCM pentru a administra certificatele de verificare a semnăturilor, realizaţi aceste task-uri:

1. Porniţi DCM.
2. În cadrul stâng de navigare al DCM, selectaţi **Crearea unui nou depozit de certificate** pentru a porni task-ul asistat şi pentru a completa o serie de forme.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular în acest task asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Selectaţi ***SIGNATUREVERIFICATION** drept depozitul de certificate de creat şi faceţi click pe **Continuare**.

   Notă: Dacă există depozitul de certificate *OBJECTSIGNING, DCM vă va cere în acest punct să specificaţi dacă să copieze certificatele care semnează obiecte în noul depozit de certificate ca certificate de verificare a semnăturilor. Dacă doriţi să folosiţi certificatele existente de semnare a obiectelor pentru verificarea semnăturilor, trebuie să selectaţi **Da** şi să alegeţi **Continuare**. Trebuie să cunoaşteţi parola depozitului de certificate *OBJECTSIGNING pentru a copia certificatele din el.
4. Specificaţi o parolă pentru noul depozit de certificate şi apăsaţi **Continuare** pentru a crea depozitul de certificate. Va apare o pagină de confirmare pentru a indica succesul creării depozitului de certificate. Acum puteţi folosi depozitul pentru a gestiona certificatele şi pentru a verifica semnăturile obiectelor.

   Notă: Dacă aţi creat depozitul pentru a putea verifica semnăturile obiectelor pe care le-aţi semnat, vă puteţi opri. În timp ce creaţi noile certificate de semnare a obiectelor, ar trebui să le exportaţi din depozitul de certificate *OBJECTSIGNING în acest depozit de certificate. Dacă nu le exportaţi, nu veţi putea verifica semnăturile pe care le-aţi creat cu ele.

   Notă: Dacă aţi creat depozitul pentru a putea verifica semnăturile obiectelor pe care le-aţi primit din alte surse, trebuie să continuaţi această procedură pentru a putea importa certificatele de care aveţi nevoie în depozitul de certificate.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** în timp ce se deschide depozitul de certificate.
6. Când este afişată pagina Depozit de certificate şi Parola, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apoi apăsaţi **Continuare**.
7. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.
8. Din lista de task-uri, selectaţi **Importare certificate**. Acest task vă îndrumă prin procesul importării certificatelor de care aveţi nevoie în depozitul de certificate pentru a putea verifica semnătura de pe obiectele pe care le-aţi primit.
9. Selectaţi tipul de certificat pe care doriţi să îl importaţi. Selectaţi **Verificare semnături** pentru a importa certificatul pe care l-aţi primit împreună cu obiectele semnate şi pentru a încheia task-ul import.

   Notă: Dacă depozitul de certificate nu conţine deja o copie a certificatului AC pentru AC care a emis certificatul de verificare semnături, trebuie să importaţi certificatul AC *mai întâi*. Aţi putea primi o eroare când importaţi certificatul de verificare semnături dacă nu importaţi certificatul AC înainte de a importa certificatul de verificare semnături.

Puteţi folosi aceste certificate pentru a verifica semnăturile obiectelor.

Capitol 8. Gestionare DCM

După ce aţi configurat DCM, trebuie în timp să mai realizaţi nişte taskuri de gestiune certificate. Pentru a afla cum să folosiţi DCM pentru a vă gestiona certificatele dvs. , revedeţi aceste subiecte:

Folosiţi un CA local pentru a emite certificate pentru alte sisteme iSeries
Aflaţi cum să folosiţi un CA local privat de pe un sistem pentru a emite certificate pentru folosirea pe alte sisteme iSeries .

Gestionarea aplicaţiilor în DCM
Aflaţi cum să folosiţi DCM cu lucrul cu definiţiile de aplicaţii pentru aplicaţiile activate-SSL sau pentru aplicaţiile de semnare obiecte. Acest subiect vă oferă informaţii despre crearea definiţiilor aplicaţie şi cum să gestionaţi o atribuire de certificat a unei aplicaţii. Puteţi afla despre definirea listelor de încredere CS pe care le folosesc aplicaţiile ca bază pentru a accepta certificate pentru autentificarea clienţilor.

Validarea certificatelor şi aplicaţiilor
Aflaţi cum puteţi verifica autenticitatea unui anumit certificat înainte ca o aplicaţie să îl folosească sau să îl accepte.

Asignare certificate
Aflaţi cum puteţi asigna rapid un certificat uneia sau mai multor aplicaţii pentru a-l folosi pentru funcţii sigure.

Gestionarea locaţiilor CRL Aflaţi cum să definiţi şi să folosiţi locaţiile Listei de Revocare Certificate (CRL) pe care aplicaţiile le pot folosi pentru a verifica că certificatele pe care ei le acceptă sunt valide.

Memorarea cheilor de certificate pe Coprocesorul Criptografic IBM 4758
Aflaţi cum să folosiţi un coprocesor instalat pentru a furniza depozite mai sigure pentru cheile private ale certificatelor dvs.

Gestionarea localizării cererii pentru o PKIX CA
Aflaţi cum puteţi folosi DCM pentru a gestiona certificatele pe care le obţineţi de la un CA Internet public care emite certificate sub standardele Public Key Infrastructure for X.509 (PKIX).

Semnare obiecte
Aflaţi cum să folosiţi DCM pentru a gestiona certificatele pe care le folosiţi pentru a semna digital obiecte pentru a le asigura integritatea.

Verificarea semnăturii obiectelor
Aflaţi cum să folosiţi DCM pentru a valida autenticitatea semnăturilor digitale de pe obiecte.

Folosiţi un CA local pentru a emite certificate pentru alte sisteme iSeries

Este posibil să folosiţi deja un CA local privat de pe un sistem iSeries din reţeaua dvs. Acum, doriţi să extindeţi folosirea acestui CA local la alt sistem iSeries din reţeaua dvs. De exemplu, doriţi ca CA-ul dvs. Local curent să emită un certificat server sau client pentru o aplicaţie de pe alt iSeries pentru a îl folosi pentru sesiuni de comunicare SSL. Sau, doriţi să folosiţi certificate de la CA-ul dvs. Local de pe un sistem să semneze obiecte pe care le aveţi memorate pe alt server iSeries.

Acest scop poate fi atins prin folosirea DCM-ului (administratorului de certificate digitale) Realizaţi unele taskuri pe iSeries-ul pe care operaţi cu CA-ul Local şi realizaţi altele pe sistemul secundar iSeries care găzduieşte aplicaţiile pentru care doriţi să emiteţi certificate. Acest sistem secundar este denumit sistemul destinaţie. Taskurile pe care trebuie să le realizaţi pe sistemul destinaţie depind de versiunea acelui sistem.

Notă: Puteţi întâlni o problemă dacă sistemul iSeries pe care operaţi cu CA local foloseşte un produs furnizor de acces criptografic care furnizează o criptare mai puternică decât sistemul destinaţie. (Pentru V5R2 singurul furnizor de acces criptografic disponibil este 5722–AC3, care este cel mai puternic produs disponibil. Totuşi, în versiunile anterioare, puteaţi instala alte produse furnizoare de acces criptografic mai slabe (5722–AC1 sau 5722–AC2) care dispuneau de funcţii de criptare de nivele mai mici.) Atunci când exportaţi certificatul (împreună cu cheia sa privată), sistemul va cripta fişierul pentru a-i proteja conţinutul. Dacă sistemul foloseşte un produs criptografic mai puternic decât sistemul destinaţie, acesta nu va putea decripta fişierul în timpul procesului de import. În consecinţă, importul poate eşua sau s-ar putea ca certificatul să nu poată fi folosit pentru stabilirea de sesiuni SSL. Acest lucru este adevărat chiar dacă folosiţi o dimensiune a cheii pentru noul certificat care este potrivită pentru a fi folosită împreună cu produsul criptografic de pe sistemul destinaţie.

Puteţi folosi CA-ul dvs. Local pentru a emite certificate către alte sisteme, pe care puteţi să le folosiţi apoi pentru semnarea obiectelor sau să puneţi aplicaţiile să le folosească pentru stabilirea sesiunilor SSL. Când folosiţi CA local pentru a crea un certificat pentru a-l folosi pe alt sistem iSeries, fişierele pe care DCM le crează conţin o copie a certificatului CA local, cât şi copii ale certificatelor pentru multe CA-uri Internet publice.

Taskurile pe care trebuie să le realizaţi în DCM diferă puţin în funcţie de tipul de certificat pe care CA-ul dvs. Local îl emite şi de versiunea şi de condiţiile de pe sistemul destinaţie.

Emiteţi certificate private pentru folosirea pe alt sistem V5R2 sau V5R1 iSeries

Pentru a folosi CA local pentru a emite certificate pentru a le folosi pe alt sistem V5R2 sau V5R1 iSeries, realizaţi aceşti paşi pe sistemul care găzduieşte CA-ul Local:

1. Porniţi DCM.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
2. În cadrul de navigare, selectaţi **Creare Certificat** pentru a afişa o listă de tipuri de certificate pe care le puteţi crea folosind CA local.

   Nu trebuie să deschideţi un depozit de certificate pentru a completa acest task. Aceste instrucţiuni presupun fie că nu lucraţi în cadrul unui depozit de certificate specific, fie că lucraţi în depozitul de certificate Autoritate de certificare (CA) local. Un CA local trebuie să existe pe acest sistem înainte să puteţi realiza aceste taskuri.
3. Selectaţi tipul de certificat pe care doriţi să îl emită CA-ul local şi apăsaţi **Continuare** pentru a porni taskul asistat şi completaţi o serie de formulare. Selectaţi să creaţi un **certificat server sau client pentru alt iSeries** (pentru sesiuni SSL) sau un **certificat de semnare obiecte pentru alt iSeries** (pentru folosirea pe alt sistem).

   Notă: Dacă creaţi un certificat de semnare obiecte pentru ca alt sistem să îl folosească, acel sistem trebuie să ruleze o versiune V5R1 sau ulterioară de OS/400 pentru a folosi certificatul. Deoarece sistemul destinaţie trebuie să fie V5R1 sau mai recent, DCM-ul de pe sistemul gazdă nu vă cere să selectaţi un format ediţie destinaţie pentru noul certificat care semnează obiecte.
4. Dacă creaţi un certificat server sau client, selectaţi versiunea sistemului iSeries pentru care creaţi acest certificat. Selectaţi **Continuare** pentru a se afişa un formular care vă va permite să introduceţi informaţii de identificare pentru noul certificat.

   Notă: Nivelul de ediţie pe care îl selectaţi determină formatul folosit de DCM pentru a crea noul certificat. Cantitatea şi tipul de informaţii de identificare din formular

variază în funcţie de nivelul ediţiei pe care l-aţi selectat. Aceasta asigură că fişierele certificatului sunt compatibile cu sistemul iSeries care va folosi certificatul.

5. Completaţi formularul şi apăsaţi **Continuare** pentru a se afişa pagina de confirmare.

   Notă: Dacă există un depozit de certificate *OBJECTSIGNING sau *SYSTEM pe sistemul destinaţie, asiguraţi-vă că aţi specificat o etichetă unică pentru certificat ca şi un nume de fişier unic pentru acesta. Specificarea unei etichete unice şi a unui nume de fişier unic pentru certificat vă asigură de faptul că puteţi importa mai uşor certificatul într-un depozit de certificate de pe sistemul destinaţie.

   Această pagină de confirmare afişează numele fişierelor create de DCM pentru a fi transferate pe sistemul destinaţie. DCM crează aceste fişiere pe baza nivelului de ediţie al sistemului destinaţie pe care l-aţi specificat. DCM pune automat o copie a certificatului CA local în aceste fişiere.

   Notă: DCM crează noul certificat în depozitul de certificate propriu şi generează două fişiere pentru ca dvs. să le transferaţi: un fişier de depozit de certificate (extensia .KDB) şi un fişier cerere (extensia .RDB).

6. Folosiţi Protocolul de transfer al fişierelor în binar (FTP) sau altă metodă pentru a transfera fişierele pe sistemul destinaţie.

Emiteţi certificate private pentru a le folosi pe un sistem V4R4 sau V4R5 iSeries

Pentru a folosi CA local pentru a emite certificate pentru a le folosi pe un sistem V4R4 sau V4R5 iSeries, realizaţi aceşti paşi pe sistemul care găzduieşte CA-ul Local V5R2:

1. Porniţi DCM.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.

2. În cadrul de navigare, selectaţi **Creare Certificat** pentru a afişa o listă de tipuri de certificate pe care le puteţi crea folosind CA local.

   Nu trebuie să deschideţi un depozit de certificate pentru a completa acest task. Aceste instrucţiuni presupun fie că nu lucraţi în cadrul unui depozit de certificate specific, fie că lucraţi în depozitul de certificate Autoritate de certificare (CA) local. Un CA local trebuie să existe pe acest sistem înainte să puteţi realiza aceste taskuri.

3. Selectaţi tipul de certificat pe care doriţi să îl emită CA-ul Local şi apăsaţi **Continuare** pentrua porni taskul asistat şi completaţi o serie de formulare.

   Notă: Deoarece creaţi acest certificat pentru a-l folosi pe un sistem V4R4 sau V4R5 iSeries, trebuie să alegeţi **certificat server sau client pentru alt iSeries**. Sistemele destinaţie cu un nivel de ediţie anterior lui V5R1 nu pot folosi certificate care semnează obiecte.

4. Selectaţi versiunea iSeries pentru care creaţi acest certificat. Selectaţi **Continuare** pentru a se afişa un formular care vă va permite să introduceţi informaţii de identificare pentru noul certificat.

   Notă: Nivelul de ediţie pe care îl selectaţi determină formatul folosit de DCM pentru a crea noul certificat. Cantitatea şi tipul de informaţii de identificare din formular variază în funcţie de nivelul ediţiei pe care l-aţi selectat. Aceasta asigură că fişierele certificatului sunt compatibile cu sistemul iSeries care va folosi certificatul.

5. Completaţi formularul şi apăsaţi **Continuare** pentru a se afişa pagina de confirmare.

Notă: Dacă există un depozit de certificate *SYSTEM pe sistemul destinaţie, asiguraţi-vă că specificaţi o etichetă de certificat unică şi un nume de fişier unic pentru certificat. Specificarea unei etichete unice şi a unui nume de fişier unic pentru certificat vă asigură de faptul că puteţi importa mai uşor certificatul într-un depozit de certificate de pe sistemul destinaţie.

Această pagină de confirmare afişează numele fişierelor create de DCM pentru a fi transferate pe sistemul destinaţie. DCM crează aceste fişiere pe baza nivelului de ediţie al sistemului destinaţie pe care l-aţi specificat. DCM pune automat o copie a certificatului CA local în aceste fişiere.

Notă: DCM crează noul certificat în depozitul de certificate propriu şi generează două fişiere pentru ca dvs. să le transferaţi: un fişier de depozit de certificate (extensia .KDB) şi un fişier cerere (extensia .RDB).

Notă: Dacă aveţi de gând să folosiţi certificatele din aceste fişiere într-un depozit de certificate *SYSTEM existentă de pe un sistem destinaţie V4R4 sau V4R5, nu puteţi importa certificatul CA local direct din fişierele .KDB şi .RDB . Acest lucru se întâmplă deoarece certificatul CA nu se află într-un format pe care îl poate recunoaşte funcţia de import a DCM. În schimb, trebuie să folosiţi sistemul gazdă pentru a exporta o copie a certificatului CA local într-un fişier separat pentru a asigura că certificatul CA este într-un format care va funcţiona cu funcţia de importare pentru versiunile anterioare.

6. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
7. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat pe sistemul gazdă şi apăsaţi **Continuare**.
8. În cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a se afişa o listă de task-uri.
9. Din lista de task-uri, selectaţi **Exportul unui certificat**.
10. Selectaţi **Autoritate de certificare (CA)** ca tip al certificatului care va fi exportat şi efectuaţi un clic pe **Continuare** pentru a se afişa o listă de certificate CA.
11. Din lista de certificate, selectaţi certificatul CA local (de exemplu, LOCAL_CERTIFICATE_AUTHORITY). Apăsaţi **Exportare** pentru a afişa un formular care vă permite să alegeţi destinaţia pentru certificatul CA.
12. Selectaţi **Fişier** şi alegeţi **Continuare**.
13. Specificaţi calea completă calificată şi numele fişierului care va fi exportat şi apăsaţi **Continuare**. Se va afişa o pagină de confirmare care va indica faptul că DCM-ul a exportat cu succes fişierul.

    Notă: Asiguraţi-vă că daţi fişierului un nume şi o extensie unice. De exemplu, puteţi denumi fişierul mycafile.exp. Atunci când denumiţi fişierul, nu folosiţi una din următoarele extensii pentru fişier: .TXT, .KDB, .RDB, sau .KYR. Folosind una din aceste extensii poate genera o problemă când importaţi fişierul pe sistemul destinaţie.
14. Folosiţi Protocolul de Transfer Fişiere binar (FTP) sau altă metodă pentru a transfera fişierele depozitului de certificate pe care le-aţi creat (.KDB şi .RDB) pe sistemul destinaţie V4R4 sau V4R5. Folosiţi modul ASCII FTP pentru a transfera fişierul care conţine certificatul CA local exportat.

Folosiţi fişierele transferate de pe sistemul destinaţie

După ce aţi transferat fişierele, folosiţi DCM pe sistemul destinaţie pentru a lucra cu fişierele certificate transferate. Task-urile DCM pe care le puteţi efectua variază pe baza nivelului de ediţie de pe sistemul destinaţie şi de ce depozite de certificate există pe sistemul destinaţie. De asemenea, tipul certificatului pe care l-aţi creat pe sistemul gazdă afectează task-urile pe care

trebuie să le efectuaţi pe sistemul destinaţie. Pentru a afla cum să folosiţi DCM pe sistemul destinaţie pentru a lucra cu fişierele certificate transferate, revedeţi aceste subiecte:

- Folosiţi un certificat privat pentru sesiuni SSL pe un sistem destinaţie V5R2.
- Folosiţi un certificat privat pentru sesiuni SSL pe un sistem destinaţie V5R1.
- Folosiţi un certificat privat pentru semnarea de obiecte pe un sistem destinaţie V5R2 sau V5R1.
- Folosiţi un certificat privat pentru sesiuni SSL pe un sistem destinaţie V4R5 sau V4R4.

Folosiţi un certificat privat pentru sesiuni SSL pe un sistem destinaţie V5R2

Certificatele folosite de aplicaţii pentru sesiuni SSL din depozitul de certificate *SYSTEM sunt gestionate în DCM (Digital Certificate Manager). Dacă nu aţi mai folosit DCM pe sistemul destinaţie V5R2 pentru a gestiona certificatele pentru SSL, atunci acest depozit de certificate nu ar trebui să existe pe sistemul destinaţie. Taskurile pentru folosirea fişierelor depozitului de certificate transferate pe care le-aţi creat pe sistemul gazdă CA local depind de situaţia dacă depozitul de certificate *SYSTEM există. Dacă depozitul de certificate *SYSTEM nu există , puteţi folosi fişierele certificatelor transferate ca un mijloc de creare a depozitului de certificate *SYSTEM. Dacă depozitul de certificate *SYSTEM există pe sistemul destinaţie V5R2, puteţi folosi fişierele certificatelor transferate în unul din cele două moduri:

- Folosiţi fişierele transferate ca Depozit de certificate de pe alt sistem.
- Importaţi fişierele transferate în depozitul de certificate *SYSTEM existent.

Depozitul de certificate *SYSTEM nu există

Dacă depozitul de certificate *SYSTEM nu există pe sistemul V5R2 pe care doriţi să folosiţi fişierele depozitului de certificate transferate, puteţi folosi fişierele certificatelor transferate ca depozitul de certificate *SYSTEM. Pentru a crea depozitul de certificate *SYSTEM şi folosi fişierele certificatelor pe sistemul dvs. destinaţie V5R2, urmaţi aceşti paşi:

1. Asiguraţi-vă că fişierele depozitului de certificate (două fişiere: unul cu extensia .KDB şi unul cu extensia .RDB) pe care le-aţi creat pe sistemul care găzduieşte CA-ul Local sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER .
2. O dată ce fişierele certificatelor transferate sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , redenumiţi aceste fişiere în DEFAULT.KDB şi DEFAULT.RDB. Redenumind aceste fişiere în catalogul corespunzător, creaţi componentele care conţin depozitul de certificate *SYSTEM pentru sistemul destinaţie. Depozitul de certificate conţine deja copii de certificate pentru multe CA publice Internet. DCM a adăugat acestea, cât şi o copie a certificatului CA local, la fişierele depozitului de certificate când le-aţi creat.

   Atenţie: Dacă sistemul dvs. destinaţie are deja un fişier DEFAULT.KDB şi unul DEFAULT.RDB în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , depozitul de certificate *SYSTEM există pe acest sistem destinaţie. În consecinţă, nu ar trebui să redenumiţi fişierele transferate după cum este sugerat mai sus. Suprascrierea fişierelor implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat şi a conţinutului său. În schimb, trebuie să vă asiguraţi că ele au nume unice şi trebuie să folosească depozitul de certificate transferat ca un **Depozit de certificate de pe alt sistem**. Dacă folosiţi fişierele ca un Depozit de certificate de pe alt sistem, nu puteţi folosi DCM pentru a specifica ce aplicaţii ar trebui să folosească certificatul.
3. Porniţi DCM. Trebuie să schimbaţi acum parola pentru depozitul de certificate *SYSTEM pe care aţi creat-o prin redenumirea fişierelor transferate. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.

4. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
5. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R2 şi apăsaţi **Continuare**.
6. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate. După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el. Apoi puteţi specifica ce aplicaţii ar trebui să folosească certificatul pentru sesiuni SSL.
7. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
8. Când apare pagina Depozit certificate şi Parolă, furnizaţi noua parolă şi apăsaţi **Continuare**.
9. După ce se reafişează cadrul de navigare, selectaţi **Gestionare certificate** din cadrul de navigaţie pentru a afişa o listă de task-uri.
10. Din lista de task-uri, selectaţi **Asignare Certificat** pentru a afişa o listă de certificate din depozitul curent de certificate.
11. Selectaţi certificatul pe care l-aţi creat pe sistemul *gazdă* şi apăsaţi **Asignare la aplicaţii** pentru a afişa o listă de aplicaţii activate-SSL la care puteţi asigna certificatul.
12. Selectaţi aplicaţiile care ar trebui să folosească certificatul pentru sesiunile SSL şi apăsaţi **Continuare**. DCM afişează un mesaj pentru a confirma selecţia certificatului dvs. pentru aplicaţii.

    Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. O aplicaţie cu acest suport trebuie să poată să autentifice certificate înainte de a acorda accesul la resurse. În consecinţă, trebuie să definiţi o listă de încredere CA pentru aplicaţie. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Cu aceste taskuri completate, aplicaţiile de pe sistemul destinaţie pot folosi certificatul emis de CA local de pe alt iSeries. Totuşi, înainte de a putea începe să folosiţi SSL pentru aceste aplicaţii, trebuie să configuraţi aplicaţiile să folosească SSL.

Înainte ca un utilizator să poată accesa aplicaţiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obţine o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA local trebuie să fie copiat într-un fişier de pe PC-ul utilizatorului sau descărcat în browser-ul utilizatorului, în funcţie de cerinţele aplicaţiei activată-SSL.

Depozitul de certificate *SYSTEM există — folosind fişierele ca un Depozit de certificate de pe alt sistem

Dacă sistemul destinaţie V5R2 are deja e meorie de certificate *SYSTEM, trebuie să decideţi cum să lucraţi cu fişierele certificatului. Puteţi alege să folosiţi fişierele certificate transferate ca un **Depozit de certificate de pe alt sistem**. Sau, puteţi alege să importaţi certificatul privat şi certificatul său CA local corespunzător în depozitul de certificate *SYSTEM existent.

Depozitele de certificate de pe alt sistem sunt depozite secundare de certificate definite de utilizatori pentru certificate SSL. Le puteţi crea şi folosi pentru a furniza certificate pentru aplicaţiile activate-SSL scrise de utilizatori care nu folosesc API-uri DCM pentru a înregistra un ID aplicaţie cu opţiunea DCM. Opţiunea Depozit de certificate de pe alt sistem vă permite să gestionaţi certificate pentru aplicaţiile pe care dvs. sau alţii le scrieţi şi care folosesc API SSL_Init pentru a accesa şi a folosi programat un certificat pentru a stabili o sesiune SSL.

Acest API permite unei aplicaţii să folosească mai repede certificatul implicit pentru un depozit de certificate decât certificatul identificat implicit.

Aplicaţiile IBM iSeries (şi multe alte aplicaţii ale dezvoltatorilor de software) sunt scrise pentru a folosi certificate doar în depozitul de certificate *SYSTEM. Dacă alegeţi să folosiţi fişierele transferate ca un Depozit de certificate de pe alt sistem, nu puteţi folosi DCM pentru a specifica ce aplicaţii ar trebui să folosească certificatul pentru sesiuni SSL. În consecinţă, nu puteţi configura aplicaţii standard iSeries activate-SSL pentru a folosi acest certificat. Dacă doriţi să folosiţi certificatul pentru aplicaţii iSeries, trebuie să importaţi certificatul din fişierele transferate ale depozitului dvs. de certificate în depozitul de certificate *SYSTEM.

Pentru a accesa şi a lucra cu fişierele depozit de certificate ca un Depozit de certificate de pe alt sistem, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate (cea cu extensia .KDB) pe care aţi transferat-o de pe sistemul gazdă. De asemenea, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R2 şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el. Mai apoi, puteţi specifica ca certificatul din acest depozit să fie folosit ca certificat implicit.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
6. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate, furnizaţi parola nouă şi apăsaţi **Continuare**.
7. După ce se reafişează cadrul de navigare, selectaţi **Gestionare depozit certificate** şi selectaţi **Setare certificat implicit** din lista de task-uri.

Acum, după ce aţi creat şi configurat Depozit de certificate de pe alt sistem, orice aplicaţii care folosesc API-ul SSL_Init pot folosi certificatul din el pentru a stabili sesiuni SSL.

Depozitul de certificate *SYSTEM există — folosind fişierele din depozitul de certificate *SYSTEM

Puteţi folosi certificatele din fişierele transferate ale depozitului de certificate dintr-un depozit de certificate *SYSTEM existentă de pe un sistem V5R2. Pentru a face acest lucru, trebuie să importaţi certificatele din fişierele depozit de certificate transferate în depozitul de certificate *SYSTEM existent. Totuşi, nu puteţi importa certificatele direct din fişierele .KDB şi .RDB deoarece nu sunt într-un format pe care funcţia de importare a DCM să îl poată recunoaşte şi folosi. Pentru a folosi certificatele transferate într-un depozit de certificate *SYSTEM existentă, trebuie să deschideţi fişierele ca un depozit de certificate de pe alt sistem şi să le exportaţi în depozitul de certificate *SYSTEM.

Pentru a exporta certificatele din fişierele depozitului de certificate în depozitul de certificate *SYSTEM, urmaţi aceşti paşi de pe sistemul destinaţie V5R2:

1. Porniţi DCM.
2. În cadrul de navigare, apăsaţi **Selecţie Depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** ca fiind depozitul de certificate de deschis.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate (cea cu extensia .KDB) pe care aţi transferat-o de pe sistemul gazdă. De asemenea, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R2 şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit. Dacă nu schimbaţi parola şi selectaţi opţiunea Logare Automată, s-ar putea să întâmpinaţi erori când exportaţi certificatele din acest depozit în depozitul de certificate *SYSTEM.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
6. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate, furnizaţi parola nouă şi apăsaţi **Continuare**.
7. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** în cadrul de navigare pentru a se afişa o listă de task-uri şi selectaţi **Exportul certificatului**.
8. Selectaţi **Autoritate certificare (CA)** ca tipul de certificat de exportat şi apăsaţi **Continuare**.

   Notă: Ar trebui să exportaţi certificatul CA local în depozitul de certificate înainte de a exporta certificatul server sau client în depozitul de certificate. Dacă exportaţi întâi certificatul server sau client, s-ar putea să întâlniţi o eroare deoarece certificatul CA local nu există în depozitul de certificate.
9. Selectaţi certificatul CA local care va fi exportat şi alegeţi **Export**.
10. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
11. Introduceţi *SYSTEM ca depozit de certificate destinaţie, introduceţi parola pentru acest depozit de certificate şi alegeţi **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informaţii de eroare dacă exportarea a eşuat.
12. Acum puteţi exporta certificatul server sau client în depozitul de certificate *SYSTEM. Reselectaţi taskul **Exportare certificat**.
13. Selectaţi **Server sau client** ca tipul de certificat de exportat şi apăsaţi **Continuare**.
14. Selectaţi certificatul server sau client corespunzător de exportat şi apăsaţi **Export**.
15. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
16. Introduceţi *SYSTEM ca depozit de certificate destinaţie, introduceţi parola pentru acest depozit de certificate şi alegeţi **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informaţii de eroare dacă exportarea a eşuat.
17. Acum puteţi asigna certificatul către aplicaţii să folosească SSL. Apăsaţi **Selectare depozit de certificate** din cadrul de navigare şi selectaţi ***SYSTEM** ca depozitul de certificate de deschis.
18. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pentru depozitul de certificate *SYSTEM şi apăsaţi **Continuare**.

19. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.
20. Din lista de task-uri, selectaţi **Asignare Certificat** pentru a afişa o listă de certificate din depozitul curent de certificate.
21. Selectaţi certificatul pe care l-aţi creat pe sistemul *gazdă* şi apăsaţi **Asignare la aplicaţii** pentru a afişa o listă de aplicaţii activate-SSL la care puteţi asigna certificatul.
22. Selectaţi aplicaţiile care ar trebui să folosească certificatul pentru sesiunile SSL şi apăsaţi **Continuare**. DCM afişează un mesaj pentru a confirma selecţia certificatului dvs. pentru aplicaţii.

    Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. O aplicaţie cu acest suport trebuie să poată să autentifice certificate înainte de a acorda accesul la resurse. În consecinţă, trebuie să definiţi o listă de încredere CA pentru aplicaţie. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Cu aceste taskuri completate, aplicaţiile de pe sistemul destinaţie pot folosi certificatul emis de CA local de pe alt iSeries. Totuşi, înainte de a putea începe să folosiţi SSL pentru aceste aplicaţii, trebuie să configuraţi aplicaţiile să folosească SSL.

Înainte ca un utilizator să poată accesa aplicaţiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obţine o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA local trebuie să fie copiat într-un fişier de pe PC-ul utilizatorului sau descărcat în browser-ul utilizatorului, în funcţie de cerinţele aplicaţiei activată-SSL.

Folosiţi un certificat privat pentru sesiuni SSL de pe un sistem destinaţie V5R1

Certificatele folosite de aplicaţii pentru sesiuni SSL din depozitul de certificate *SYSTEM sunt gestionate în DCM (Digital Certificate Manager). Dacă nu aţi folosit niciodată DCM pe sistemul destinaţie V5R1 pentru a gestiona certificate pentru SSL, acest depozit de certificate nu ar trebui să existe pe sistemul destinaţie. Taskurile pentru folosirea fişierelor depozitului de certificate transferate pe care le-aţi creat pe sistemul gazdă CA local depind de situaţia dacă depozitul de certificate *SYSTEM există. Dacă depozitul de certificate *SYSTEM nu există , puteţi folosi fişierele certificatelor transferate ca un mijloc de creare a depozitului de certificate *SYSTEM.Dacă certificatul *SYSTEM există pe sistemul destinaţie V5R1, puteţi folosi fişierele certificatelor transferate în unul din cele două moduri:

- Folosiţi fişierele transferate ca Depozit de certificate de pe alt sistem.
- Importaţi fişierele transferate în depozitul de certificate *SYSTEM existent.

Depozitul de certificate *SYSTEM nu există

Dacă depozitul de certificate *SYSTEM nu există pe sistemul V5R1 pe care doriţi să folosiţi fişierele depozit de certificate transferate, le puteţi folosi ca depozit de certificate *SYSTEM. Pentru a folosi fişierele certificatului de pe sistemul dvs. destinaţie V5R1, urmaţi aceşti paşi:

1. Asiguraţi-vă că fişierele depozitului de certificate (două fişiere: unul cu extensia .KDB şi unul cu extensia .RDB) pe care le-aţi creat pe sistemul care găzduieşte CA-ul Local sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER .
2. O dată ce fişierele certificatelor transferate sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , redenumiţi aceste fişiere în DEFAULT.KDB şi DEFAULT.RDB. Redenumind aceste fişiere în catalogul corespunzător, creaţi componentele care conţin depozitul de certificate *SYSTEM pentru sistemul destinaţie. Depozitul de certificate conţine deja copii de certificate

pentru multe CA publice Internet. DCM a adăugat acestea, cât şi o copie a certificatului CA local, la fişierele depozitului de certificate când le-aţi creat.

Atenţie: Dacă sistemul dvs. destinaţie are deja un fişier DEFAULT.KDB şi unul DEFAULT.RDB în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , depozitul de certificate *SYSTEM există pe acest sistem destinaţie. În consecinţă, nu ar trebui să redenumiţi fişierele transferate după cum este sugerat mai sus. Suprascrierea fişierelor implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat şi a conţinutului său. În schimb, trebuie să vă asiguraţi că ele au nume unice şi trebuie să folosească depozitul de certificate transferat ca un **Depozit de certificate de pe alt sistem**. Dacă folosiţi fişierele ca un Depozit de certificate de pe alt sistem, nu puteţi folosi DCM pentru a specifica ce aplicaţii ar trebui să folosească certificatul.

3. Porniţi DCM. Trebuie să schimbaţi acum parola pentru depozitul de certificate *SYSTEM pe care l-aţi creat prin redenumirea fişierelor transferate. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.
4. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
5. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R1 şi apăsaţi **Continuare**.
6. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate. După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el. Apoi puteţi specifica ce aplicaţii ar trebui să folosească certificatul pentru sesiuni SSL.
7. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** în timp ce se deschide depozitul de certificate.
8. Când apare pagina Depozit certificate şi Parolă, furnizaţi noua parolă şi apăsaţi **Continuare**.
9. După ce se reafişează cadrul de navigare, selectaţi **Gestionare Aplicaţii** din cadrul de navigaţie pentru a afişa o listă de task-uri.
10. Din lista de task-uri, selectaţi **Actualizarea atribuirii certificatelor** pentru a se afişa o listă de aplicaţii active-SSL pentru care puteţi atribui un certificat.
11. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Actualizarea atribuirii certificatelor**.
12. Selectaţi certificatul pe care CA local de pe sistemul *gazdă* l-a emis şi apăsaţi **Asignare certificat nou**. DCM va afişa un mesaj pentru a confirma selecţia certificatului pentru aplicaţie.

Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. O aplicaţie cu acest suport trebuie să poată să autentifice certificate înainte de a acorda accesul la resurse. În consecinţă, trebuie să definiţi o listă de încredere CA pentru aplicaţie. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Cu aceste taskuri completate, aplicaţiile de pe sistemul destinaţie pot folosi certificatul emis de CA local de pe alt iSeries. Totuşi, înainte de a putea începe să folosiţi SSL pentru aceste aplicaţii, trebuie să configuraţi aplicaţiile să folosească SSL.

Înainte ca un utilizator să poată accesa aplicaţiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obţine o copie a certificatului CA local de pe sistemul

gazdă. Certificatul CA trebuie copiat într-un fişier pe PC-ul utilizatorului sau transferat în browser-ul utilizatorului, în funcţie de cerinţele aplicaţiei ce foloseşte SSL.

Depozitul de certificate *SYSTEM există — folosind fişierele ca un Depozit de certificate de pe alt sistem

Dacă sistemul destinaţie V5R1 are deja un depozit de certificate *SYSTEM, trebuie să decideţi cum să lucraţi cu fişierele certificate. Puteţi alege să folosiţi fişierele certificate transferate ca un **Depozit de certificate de pe alt sistem**. Sau, puteţi alege să importaţi certificatul privat şi certificatul său CA local corespunzător în depozitul de certificate *SYSTEM existent.

Alte depozite de certificate sistem sunt depozite secundare de certificate definite de utilizatori pentru certificate SSL. Le puteţi crea şi folosi pentru a furniza certificate aplicaţiilor scrise-de-utilizator active-SSL care nu folosesc API-urile DCM pentru a înregistra ID-ul aplicaţiei cu facilitatea DCM. Opţiunea Alte depozite de certificate sistem vă permite să gestionaţi certificate pentru aplicaţiile pe care dvs. sau alţii le scrieţi şi care folosesc API SSL_Init pentru a accesa şi a folosi programat un certificat pentru a stabili o sesiune SSL. Acest API permite unei aplicaţii să folosească mai repede certificatul implicit pentru un depozit de certificate decât certificatul identificat implicit.

Aplicaţiile IBM iSeries (şi multe alte aplicaţii ale dezvoltatorilor de software) sunt scrise pentru a folosi certificate doar în depozitul de certificate *SYSTEM. Dacă alegeţi să folosiţi fişierele transferate ca un Depozit de certificate de pe alt sistem, nu puteţi folosi DCM pentru a specifica ce aplicaţii ar trebui să folosească certificatul pentru sesiuni SSL. În consecinţă, nu puteţi configura aplicaţii standard iSeries activate-SSL pentru a folosi acest certificat. Dacă doriţi să folosiţi certificatul pentru aplicaţii iSeries, trebuie să importaţi certificatul din fişierele transferate ale depozitului dvs. de certificate în depozitul de certificate *SYSTEM.

Pentru a accesa şi a lucra cu fişierele depozit de certificate ca un Depozit de certificate de pe alt sistem, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate (cea cu extensia .KDB) pe care aţi transferat-o de pe sistemul gazdă. De asemenea, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R1 şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el. Mai apoi, puteţi specifica ca certificatul din acest depozit să fie folosit ca certificat implicit.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
6. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate, furnizaţi parola nouă şi apăsaţi **Continuare**.
7. După ce se reafişează cadrul de navigare, selectaţi **Gestionare Depozit certificatee** şi selectaţi **Setare certificat implicit** din lista de task-uri.

Acum, după ce aţi creat şi configurat Depozit de certificate de pe alt sistem, orice aplicaţii care folosesc API-ul SSL_Init pot folosi certificatul din el pentru a stabili sesiuni SSL.

Depozitul de certificate *SYSTEM există — folosind fişierele din depozitul de certificate *SYSTEM

Puteţi folosi certificatele din fişierele depozit de certificate transferate într-un depozit de certificate *SYSTEM existent pe un sistem V5R1. Pentru a face acest lucru, trebuie să importaţi certificatele din fişierele depozit de certificate transferate în depozitul de certificate *SYSTEM existent. Totuşi, nu puteţi importa certificatele direct din fişierele .KDB şi .RDB deoarece nu sunt într-un format pe care funcţia de importare a DCM să îl poată recunoaşte şi folosi. Pentru a folosi certificatele transferate într-un depozit de certificate *SYSTEM existentă, trebuie să deschideţi fişierele ca un depozit de certificate de pe alt sistem şi să le exportaţi în depozitul de certificate *SYSTEM.

Notă: Această procedură descrie cum să folosiţi un depozit de certificate de pe alt sistem de pe sistemul destinaţie pentru a exporta certificatele din fişierele depozitului de certificate originale în depozitul de certificate *SYSTEM. Folosind această metodă pentru a adăuga certificatele la depozitul de certificate *SYSTEM vă poate ajuta să evitaţi posibilele probleme când sistemul destinaţie foloseşte un produs furnizor de acces criptografic mai slab (cum este 5722–AC2) decât sistemul gazdă.

Pentru a exporta certificatele din fişierele depozitului de certificate în depozitul de certificate *SYSTEM, urmaţi aceşti paşi de pe sistemul destinaţie V5R1:

1. Porniţi DCM.
2. În cadrul de navigare, apăsaţi **Selecţie Depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** ca fiind depozitul de certificate de deschis.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate (cea cu extensia .KDB) pe care aţi transferat-o de pe sistemul gazdă. De asemenea, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R1 şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit. Dacă nu schimbaţi parola şi selectaţi opţiunea Logare Automată, s-ar putea să întâmpinaţi erori când exportaţi certificatele din acest depozit în depozitul de certificate *SYSTEM.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
6. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate, furnizaţi parola nouă şi apăsaţi **Continuare**.
7. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** în cadrul de navigare pentru a se afişa o listă de task-uri şi selectaţi **Exportul certificatului**.
8. Selectaţi **Autoritate certificare (CA)** ca tipul de certificat de exportat şi apăsaţi **Continuare**.

   Notă: Ar trebui să exportaţi certificatul CA local în depozitul de certificate înainte de a exporta certificatul server sau client în depozitul de certificate. Dacă exportaţi

întâi certificatul server sau client, s-ar putea să întâlniţi o eroare deoarece certificatul CA local nu există în depozitul de certificate.

9. Selectaţi certificatul CA local care va fi exportat şi alegeţi **Export**.
10. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
11. Introduceţi *SYSTEM ca depozit de certificate destinaţie, introduceţi parola pentru acest depozit de certificate şi alegeţi **Continuare**.
12. Acum puteţi exporta certificatul server sau client în depozitul de certificate *SYSTEM. Reselectaţi taskul **Exportare certificat**.
13. Selectaţi **Server sau client** ca tipul de certificat de exportat şi apăsaţi **Continuare**.
14. Selectaţi certificatul server sau client corespunzător de exportat şi apăsaţi **Export**.
15. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
16. Introduceţi *SYSTEM ca depozit de certificate destinaţie, introduceţi parola pentru acest depozit de certificate şi alegeţi **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informaţii de eroare dacă exportarea a eşuat.
17. Acum puteţi asigna certificatul către aplicaţii să folosească SSL. Apăsaţi **Selectare depozit de certificate** din cadrul de navigare şi selectaţi ***SYSTEM** ca depozitul de certificate de deschis.
18. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pentru depozitul de certificate *SYSTEM şi apăsaţi **Continuare**.
19. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.
20. Din lista de task-uri, selectaţi **Actualizarea atribuirii certificatelor** pentru a se afişa o listă de aplicaţii active-SSL pentru care puteţi atribui un certificat.
21. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Actualizarea atribuirii certificatelor**.
22. Selectaţi certificatul pe care CA local de pe sistemul *gazdă* l-a emis şi apăsaţi **Asignare certificat nou**. DCM va afişa un mesaj pentru a confirma selecţia certificatului pentru aplicaţie.

Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. O aplicaţie cu acest suport trebuie să poată să autentifice certificate înainte de a acorda accesul la resurse. În consecinţă, trebuie să definiţi o listă de încredere CA pentru aplicaţie. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Cu aceste taskuri completate, aplicaţiile de pe sistemul destinaţie pot folosi certificatul emis de CA local de pe alt iSeries. Totuşi, înainte de a folosi SSL pentru aceste aplicaţii, va trebui să configuraţi aplicaţiile pentru a folosi SSL.

Înainte ca un utilizator să poată accesa aplicaţiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obţine o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA trebuie copiat într-un fişier pe PC-ul utilizatorului sau transferat în browser-ul utilizatorului, în funcţie de cerinţele aplicaţiei ce foloseşte SSL.

Folosiţi un certificat privat pentru semnarea obiectelor de pe un sistem destinaţie V5R2 sau V5R1

Certificatele folosite de aplicaţii pentru semnarea obiectelor din depozitul de certificate *OBJECTSIGNING sunt gestionate în DCM (Digital Certificate Manager). Dacă nu aţi folosit niciodată DCM pe sistemul destinaţie pentru a gestiona certificate care semnează

obiecte, atunci acest depozit de certificate nu ar trebui să existe pe sistemul destinaţie. Taskurile pe care trebuie să le realizaţi pentru a folosi fişierele transferate ale depozitului de certificate pe care le-aţi creat pe sistemul gazdă CA local depind de situaţia dacă depozitul de certificate *OBJECTSIGNING există. Dacă depozitul de certificate *OBJECTSIGNING nu există , puteţi folosi fişierele certificatelor transferate ca un mijloc de creare a depozitului de certificate *OBJECTSIGNING. Dacă depozitul de certificate *OBJECTSIGNING există pe sistemul destinaţie, trebuie să importaţi certificatele transferate în ea.

Depozitul de certificate *OBJECTSIGNING nu există

Taskurile pe care le realizaţi pentru a folosi fişierele depozitului de certificate pe care le-aţi creat pe sistemul gazdă CA local depind de situaţia dacă aţi folosit vreodată DCM pe sistemul destinaţie pentru a gestiona certificatele de semnare obiecte.

Dacă depozitul de certificate *OBJECTSIGNING nu există pe sistemul destinaţie V5R2 sau V5R1 cu fişierele transferate ale depozitului de certificate, urmaţi aceşti paşi:

1. Asiguraţi-vă că fişierele depozitului de certificate (două fişiere: unul cu extensia .KDB şi unul cu extensia .RDB) pe care le-aţi creat pe sistemul care găzduieşte CA-ul Local sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SIGNING.
2. O dată ce fişierele certificatelor transferate sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SIGNING , redenumiţi fişierele certificatului în SGNOBJ.KDB şi SGNOBJ.RDB, dacă este necesar. Redenumind aceste fişiere, creaţi componentele care conţin depozitul de certificate *OBJECTSIGNING pentru sistemul destinaţie. Depozitul de certificate conţine deja copii de certificate pentru multe CA publice Internet. DCM a adăugat acestea, cât şi o copie a certificatului CA local, la fişierele depozitului de certificate când le-aţi creat.

   Atenţie: Dacă sistemul dvs. destinaţie are deja un fişier SGNOBJ.KDB şi unul SGNOBJ.RDB în catalogul /QIBM/USERDATA/ICSS/CERT/SIGNING , depozitul de certificate *OBJECTSIGNING există pe acest sistem destinaţie. În consecinţă, nu ar trebui să redenumiţi fişierele transferate după cum este sugerat mai sus. Suprascrierea fişierelor care semnează obiecte implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat şi a conţinutului său. Puteţi obţine certificatele din aceste fişiere în depozitul de certificate existent *OBJECTSIGNING în două moduri. Puteţi exporta certificatele din acest fişier într-un set de fişiere plate din care le puteţi importa în depozitul de certificate *OBJECTSIGNING existent. Sau, puteţi deschide fişierele transferate ca un Depozit de certificate de pe alt sistem şi să exportaţi certificatele direct în depozitul de certificate *OBJECTSIGNING, aşa cum este descris mai jos. În ambele cazuri, trebuie să puneţi certificatele în depozitul de certificate *OBJECTSIGNING dacă doriţi să puteţi gestiona aplicaţiile care le folosesc aşa cum descrie această procedură.
3. Porniţi DCM. Trebuie să modificaţi parola pentru depozitul de certificate *OBJECTSIGNING. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.
4. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** în timp ce se deschide certificatul.
5. Când se afişează pagina parolă, introduceţi parola pe care aţi specificat-o pentru depozitul de certificate atunci când l-aţi creat pe sistemul destinaţie şi alegeţi **Continuare**.
6. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate. După ce modificaţi parola, trebuie să redeschideţi

depozitul de certificate înainte de a putea lucra cu certificatele din el. Apoi, puteţi crea o definiţie de aplicaţie care să folosească certificatul pentru semnarea obiectelor.

7. După ce aţi redeschis depozitul de certificate, selectaţi **Gestionarea aplicaţiilor** din cadrul de navigare pentru a se afişa o listă de task-uri.
8. Din lista de task-uri, selectaţi **Adăugarea aplicaţiei** pentru a începe procesul de creare a unei definiţii aplicaţie care semnează obiecte pentru a folosi certificatul în semnarea obiectelor.
9. Completaţi formularul pentru a defini aplicaţia care semnează obiecte şi efectuaţi un clic pe **Adăugare**. Această definiţie aplicaţie nu descrie o aplicaţie reală, ci mai degrabă tipul de obiecte pe care doriţi să le formaţi cu un anume certificat. Folosiţi ajutorul online pentru a afla cum să completaţi formularul.
10. Selectaţi **OK** pentru a recunoaşte mesajul de confirmare al definiţiei aplicaţie şi pentru a afişa lista de task-uri **Gestionarea aplicaţiilor**.
11. Din lista de task-uri, selectaţi **Actualizare asignare certificate** pentru a afişa o listă de ID-uri de aplicaţii de semnare obiecte pentru care puteţi asigna un certificat.
12. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Actualizarea atribuirii certificatelor**.
13. Selectaţi certificatul pe care CA local de pe sistemul gazdă l-a creat şi apăsaţi **Asignare certificat nou**.

Atunci când terminaţi aceste task-uri, puteţi începe semnarea obiectelor pentru a le asigura integritatea.

Când distribuiţi obiecte semnate, cei care primesc obiectele trebuie să folosească o versiune V5R2 sau V5R1 sau mai nouă a DCM pentru a verifica semnătura de pe obiecte pentru a se asigura că datele sunt nemodificate şi pentru a verifica identitatea expeditorului. Pentru validarea semnăturii, destinatarul trebuie să aibă o copie a certificatului de verificare a semnăturii. Ar trebui să furnizaţi o copie a acestui certificat ca parte a pachetului de obiecte semnate.

De asemenea, destinatarul trebuie să aibă o copie a certificatului CA pentru ca Autoritatea de certificare care a emis certificatul server pe care l-aţi folosit pentru semnarea obiectului. Dacă aţi semnat obiectul cu un certificat provenind de la o CA Internet binecunoscută, s-ar putea ca versiunea de DCM a destinatarului să aibă deja o copie a certificatului CA necesar. Totuşi, trebuie să furnizaţi o copie a certificatului CA, într-un pachet separat, împreună cu obiectele semnate dacă presupuneţi că este necesar. De exemplu, ar trebui să furnizaţi o copie a certificatului CA-ului Local dacă aţi semnat obiectele cu un certificat de la un CA local. Din motive de securitate, ar trebui să furnizaţi certificatul CA într-un pachet separat sau să faceţi disponibil public la cerere certificatul celor care au nevoie de el.

Depozitul de certificate *OBJECTSIGNING există

Puteţi folosi certificatele din fişierele transferate ale depozitului de certificate dintr-un depozit de certificate *OBJECTSIGNING existentă de pe un sistem V5R2 sau V5R1. Pentru a face acest lucru, trebuie să importaţi certificatele din fişierele depozit de certificate transferate în depozitul de certificate *OBJECTSIGNING existent. Totuşi, nu puteţi importa certificatele direct din fişierele .KDB şi .RDB deoarece nu sunt într-un format pe care funcţia de importare a DCM să îl poată recunoaşte şi folosi. Puteţi adăuga certificatele în depozitul de certificate existent *OBJECTSIGNING deschizând fişierele transferate ca depozit de certificate de pe alt sistem de pe sistemul destinaţie V5R2 sau V5R1. Puteţi exporta certificatele direct în depozitul de certificate *OBJECTSIGNING. Trebuie să exportaţi o copie atât a certificatului de semnat obiecte cât şi a certificatului CA local din fişierele transferate.

Pentru a exporta certificatele din fişierele depozitului de certificate direct în depozitul de certificate *OBJECTSIGNING, urmaţi aceşti paşi de pe sistemul destinaţie V5R2 sau V5R1:

1. Porniţi DCM.
2. În cadrul de navigare, apăsaţi **Selecţie Depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** ca fiind depozitul de certificate de deschis.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierelor depozitului de certificate. De asemenea, furnizaţi parola pe care aţi folosit-o când le-aţi creat pe sistemul gazdă apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea depozitelor de certificate** şi selectaţi **Modificarea parolei** din lista de task-uri. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit. Dacă nu schimbaţi parola şi selectaţi opţiunea Logare Automată, s-ar putea să întâmpinaţi erori când exportaţi certificatele din acest depozit în depozitul de certificate *OBJECTSIGNING.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** în timp ce se deschide depozitul de certificate.
6. Când apare pagina Depozit certificate şi Parolă, furnizaţi calea completă şi numele fişierului depozitului de certificate, furnizaţi parola nouă şi apăsaţi **Continuare**.
7. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** în cadrul de navigare pentru a se afişa o listă de task-uri şi selectaţi **Exportul certificatului**.
8. Selectaţi **Autoritate certificare (CA)** ca tipul de certificat de exportat şi apăsaţi **Continuare**.

   Notă: Formularea pentru acest task presupune că atunci când lucraţi cu un Depozit de certificate de pe alt sistem lucraţi cu certificate server sau client. Aceasta este din cauză că acest tip de depozit de certificate este proiectat pentru folosirea ca un depozit de certificate secundar la depozitul de certificate *SYSTEM. Totuşi, folosind taskul export din acest depozit de certificate este cel mai uşor mod de a adăuga certificatele din fişierele transferate în depozitul de certificate *OBJECTSIGNING existent.
9. Selectaţi certificatul CA local care va fi exportat şi alegeţi **Export**.

   Notă: Ar trebui să exportaţi certificatul CA local în depozitul de certificate înainte de a exporta certificatul de semnat obiecte în depozitul de certificate. Dacă exportaţi întâi certificatul de semnat obiecte, s-ar putea să întâlniţi o eroare deoarece certificatul CA local nu există în depozitul de certificate.
10. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
11. Introduceţi *OBJECTSIGNING ca depozitul de certificate destinaţie, introduceţi parola pentru depozitul de certificate şi apăsaţi **Continuare** .
12. Acum puteţi exporta certificatul care semnează obiecte în depozitul de certificate *OBJECTSIGNING. Reselectaţi taskul **Exportare certificat**.
13. Selectaţi **Server sau client** ca tipul de certificat de exportat şi apăsaţi **Continuare**.
14. Selectaţi certificatul corespunzător de exportat şi apăsaţi **Export**.
15. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
16. Introduceţi *OBJECTSIGNING ca depozitul de certificate destinaţie, introduceţi parola pentru depozitul de certificate *OBJECTSIGNING şi apăsaţi **Continuare** . Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informaţii de eroare dacă exportarea a eşuat.

Notă: Pentru a folosi acest certificat pentru a semna obiecte, trebuie acum să asignaţi certificatul către o aplicaţie de semnare obiecte.

Folosiţi un certificat privat pentru sesiuni SSL de pe un sistem destinaţie V4R5 sau V4R4

Certificatele folosite de aplicaţii pentru sesiuni SSL din depozitul de certificate *SYSTEM sunt gestionate în DCM (Digital Certificate Manager). Dacă nu aţi mai folosit DCM pe sistemul destinaţie V4R5 sau V4R4 pentru a gestiona certificatele pentru SSL, atunci acest depozit de certificate nu ar trebui să existe pe sistemul destinaţie. Fişierele transferate ale depozitului de certificate pe care le-aţi creat pe sistemul gazdă CA local conţin două certificate. Aceste fişiere sunt certificatul server sau client pe care l-aţi creat şi certificatul privat CA local pe care l-aţi folosit pentru a-l semna.

Taskurile pe care trebuie să le realizaţi pentru a folosi fişierele transferate ale depozitului de certificate depind de situaţia dacă depozitul de certificate *SYSTEM există. Dacă depozitul de certificate *SYSTEM nu există , puteţi folosi fişierele certificatelor transferate ca un mijloc de creare a depozitului de certificate *SYSTEM.Dacă certificatul *SYSTEM există pe sistemul destinaţie, puteţi folosi fişierele certificatelor transferate în unul din cele două moduri:

- Folosiţi fişierele transferate ca un depozit de certificate de pe alt sistem.
- Importaţi fişierele transferate în depozitul de certificate *SYSTEM existent.

Depozitul de certificate *SYSTEM nu există

Dacă depozitul de certificate *SYSTEM nu există pe sistemul V4R5 sau V4R4 pe care doriţi să folosiţi fişierele transferate ale depozitului de certificate, urmaţi aceşti paşi:

1. Asiguraţi-vă că fişierele depozitului de certificate (două fişiere: unul cu extensia .KDB şi unul cu extensia .RDB) pe care le-aţi creat pe sistemul care găzduieşte CA-ul Local sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER.
2. O dată ce fişierele certificatelor transferate sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , redenumiţi aceste fişiere în DEFAULT.KDB şi DEFAULT.RDB. Redenumind aceste fişiere în catalogul corespunzător, creaţi componentele care conţin depozitul de certificate *SYSTEM pentru sistemul destinaţie. Depozitul de certificate conţine deja copii de certificate pentru multe CA publice Internet. DCM a adăugat acestea, cât şi o copie a certificatului CA local, la fişierele depozitului de certificate când le-aţi creat.

   Atenţie: Dacă sistemul dvs. destinaţie are deja un fişier DEFAULT.KDB şi unul DEFAULT.RDB în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , depozitul de certificate *SYSTEM există pe acest sistem destinaţie. În consecinţă, nu ar trebui să redenumiţi fişierele transferate după cum este sugerat mai sus. Suprascrierea fişierelor implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat şi a conţinutului său. În schimb, trebuie să vă asiguraţi că ele au nume unice şi că foloseasc fişierele depozit de certificate transferate ca un **Alt** depozit de certificate. Dacă folosiţi fişierele ca un Depozit de certificate de pe alt sistem, nu puteţi folosi DCM pentru a specifica ce aplicaţii ar trebui să folosească certificatul.
3. Porniţi DCM. Trebuie să modificaţi parola pentru depozitul de certificate *SYSTEM. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.
4. În cadrul de navigare, asiguraţi-vă că *SYSTEM este arătat ca depozitul de certificate din lista drop-down şi selectaţi **Certificate Sistem** pentru a afişa o listă de taskuri disponibile. Apare fereastra **Depozit de certificate şi parolă**.
5. În câmpurile corespunzătoare, introduceţi *SYSTEM pentru depozitul de certificate de deschis şi parola pe care aţi folosit-o când aţi creat fişerele folosind CA-ul Local de pe sistemul gazdă. Acum puteţi modifica parola depozitului de certificate.

6. Din lista de task-uri din cadrul de navigare, selectaţi **Modificarea parolei**. Completaţi formularul pentru a modifica parola pentru depozitul de certificate. După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el.
7. După ce redeschideţi depozitul de certificate *SYSTEM, selectaţi **Gestionare aplicaţii sigure** din lista de task-uri pentru a se afişa pagina ce vă permite să gestionaţi certificatele asociate cu aplicaţiile specifice.
8. Din lista de aplicaţii, selectaţi-o pe acea care ar trebui să folosească certificatul privat transferat pentru sesiune SSL.
9. Apăsaţi **Lucru cu certificate sistem** şi selectaţi certificatul pe care l-a emis CA local de pe sistemul gazdă.
10. Alegeţi **Atribuirea unui nou certificat** pentru ca aplicaţia specificată să folosească certificatul selectat.

    Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. Folosirea certificatelor pentru autentificarea client asigură faptul că aplicaţia primeşte un certificat valid înainte de a permite accesul la resursele controlate de aceasta. O aplicaţie cu acest suport trebuie să fie configurată să aibă încredere în CA înainte ca aceasta să poată autentifica certificatele emise de o CA specifică. Folosiţi pagina **Lucru cu Autorităţile de certificare** pentru a asigura că certificatul CA are starea de încredere în depozitul de certificate. Apoi, folosiţi pagina **Lucru cu aplicaţii sigure** pentru a asigura că aplicaţiile care folosesc certificatul au încredere în CA local care l-a emis. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificată ca fiind de încredere, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Cu aceste taskuri completate, aplicaţiile de pe sistemul destinaţie V4R5 sau V4R4 pot folosi certificatul emis de CA local V5R2 de pe alt iSeries. Totuşi, înainte de a folosi SSL pentru aceste aplicaţii, va trebui să configuraţi aplicaţiile pentru a folosi SSL.

Înainte ca un utilizator să poată accesa aplicaţiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obţine o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA trebuie copiat într-un fişier pe PC-ul utilizatorului sau transferat în browser-ul utilizatorului, în funcţie de cerinţele aplicaţiei ce foloseşte SSL.

Depozitul de certificate *SYSTEM există — folosind fişierele ca un depozit de certificate de pe alt sistem

Dacă sistemul destinaţie V4R5 sau V4R4 are deja e meorie de certificate *SYSTEM, trebuie să decideţi cum să lucraţi cu fişierele certificatului. Fişierele de certificat transferate conţin două certificate: certificatul server sau client pe care l-aţi creat şi certificatul privat CA local pe care l-aţi folosit pentru a-l semna. Puteţi alege să folosiţi fişierele certificate transferate ca un **Alt** depozit de certificate sistem. Sau, puteţi alege să importaţi certificatul privat şi certificatul CA local corespunzător lui în depozitul de certificate *SYSTEM existent.

Dacă alegeţi să folosiţi fişierele transferate ca un **Alt** depozit de certificate sistem, nu puteţi folosi DCM pentru a specifica ce aplicaţii ar trebui să folosească certificatul pentru sesiuni SSL. Totuşi, puteţi desemna certificatul din acest depozit de certificate care să fie certificatul implicit pentru depozitul de certificate. Opţiunea Depozit de certificate de pe alt sistem vă permite să gestionaţi certificate pentru aplicaţiile pe care dvs. sau alţii le scrieţi şi care folosesc API SSL_Init pentru a accesa şi a folosi programat un certificat pentru a stabili o sesiune SSL. Acest API permite unei aplicaţii să folosească mai degrabă certificatul implicit pentru un depozit de certificate decât certificatul identificat implicit.

Dacă depozitul de certificate *SYSTEM există pe sistemul V4R5 sau V4R4 pe care doriţi să folosiţi fişierele transferate ale depozitului de certificate, urmaţi aceşti paşi:

1. Porniţi DCM. Trebuie să modificaţi parola pentru depozitul de certificate transferat. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.
2. În cadrul de navigare, asiguraţi-vă că OTHER este arătat ca depozitul de certificate din lista drop-down şi selectaţi **Certificate Sistem** pentru a afişa o listă de taskuri disponibile. Apare fereastra **Depozit de certificate şi parolă**.
3. În câmpurile corespunzătoare, introduceţi calea completă şi numele fişierului depozitului de certificate (extensia .KDB) pe care aţi transferat-o de pe sistemul gazdă CA local. Introduceţi parola pe care aţi folosit-o când aţi creat fişierele pe sistemul *gazdă*. Acum puteţi modifica parola depozitului de certificate.
4. În cadrul de navigare, selectaţi **Modificarea parolei** din lista de task-uri Certificate sistem. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el. Mai apoi, puteţi specifica ca certificatul din acest depozit să fie folosit ca certificat implicit.
5. În cadrul de navigare, selectaţi **Gestionare certificate** pentru a se afişa pagina care vă permite să efectuaţi un număr de task-uri care gestionează certificate.
6. Din lista de certificate, selectaţi certificatul pe care doriţi să îl folosiţi ca certificat implicit pentru depozitul curent şi alegeţi **Setare implicit**.

Acum, după ce aţi creat şi configurat Depozitul de certificate de pe alt sistem, orice aplicaţii care folosesc API-ul SSL_Init pot folosi certificatul din el pentru a stabili sesiuni SSL.

Depozitul de certificate *SYSTEM există — Importarea fişierelor într-un depozit de certificate existent *SYSTEM

Înainte de a putea importa certificatele în *SYSTEM de pe un sistem destinaţie V4R5 sau V4R4, trebuie întâi să exportaţi certificatele din depozitul de certificate pe care l-aţi creat într-un format de fişier diferit. Puteţi importa mai apoi certificatele în depozitul de certificate *SYSTEM din noile fişiere. Fişierele de certificat transferate conţin două certificate: certificatul server sau client pe care l-aţi creat şi certificatul privat CA local pe care l-aţi folosit pentru a-l semna. Trebuie să importaţi şi certificatul server sau client pe care l-aţi creat, şi certificatul CA privat local în depozitul de certificate *SYSTEM.

Notă: Funcţiile de export disponibile în DCM pentru V4R5 şi V4R4 nu sunt la fel de bine dezvoltate ca acelea pentru V5R2 şi s-ar putea să experimentaţi probleme dacă folosiţi sistemul destinaţie pentru a exporta certificatul privat CA local. În consecinţă, ar trebui să folosiţi sistemul gazdă V5R2 pentru a exporta o copie *suplimentară* a certificatului CA local într-un fişier separat, decât să folosiţi sistemul destinaţie V4R4 sau V4R5 pentru a o exporta. După ce exportaţi certificatul CA local de pe sistemul gazdă V5R2, puteţi transfera manual fişierul exportat al certificatului CA local pe sistemul destinaţie V4R4 sau V4R5 şi urmaţi paşii furnizaţi mai departe în această procedură pentru a importa certificatul CA local în depozitul de certificate *SYSTEM. Trebuie să importaţi certificatul CA local *înainte* de a importa certificatul privat pe care l-aţi creat cu acesta. Dacă importaţi întâi certificatul privat, s-ar putea să întâlniţi o eroare deoarece certificatul CA local nu există în depozitul de certificate.

Pentru a se exporta certificatele din fişierele depozit de certificate, efectuaţi aceşti paşi pe sistemele destinaţie V4R4 sau V4R5:

1. Porniţi DCM.
2. În cadrul de navigare, asiguraţi-vă că OTHER este arătat ca depozitul de certificate din lista drop-down şi selectaţi **Certificate Sistem** pentru a afişa o listă de taskuri disponibile. Apare fereastra **Depozit de certificate şi parolă**.
3. Specificaţi calea completă şi numele fişierelor transferate ale depozitului de certificate, furnizaţi parola pe care aţi folosit-o când le-aţi creat pe sistemul *gazdă* şi apăsaţi **OK**. Acum puteţi modifica parola depozitului de certificate.
4. În fereastra de navigare, selectaţi **Schimbare parolă** dintr-o listă de taskuri de certificate Sistem. Completaţi formularul pentru a modifica parola pentru depozitul de certificate.

   Notă: Asiguraţi-vă că selectaţi opţiunea **Logare automată** când schimbaţi parola pentru depozitul de certificate. Prin folosirea acestei parole vă veţi asigura că DCM păstrează noua parolă pentru ca dvs. să puteţi folosi toate funcţiile de gestiune a certificatelor ale DCM pentru noul depozit. Dacă nu schimbaţi parola şi selectaţi opţiunea Logare Automată, s-ar putea să întâmpinaţi erori când exportaţi certificatele din acest depozit.

   După ce modificaţi parola, trebuie să redeschideţi depozitul de certificate înainte de a putea lucra cu certificatele din el.
5. În cadrul de navigare, selectaţi **Gestionare certificate** pentru a se afişa o listă de certificate.
6. Selectaţi certificatul privat din listă şi alegeţi **Export** pentru a se afişa pagina Exportul unui certificat.
7. Completaţi formularul Exportare Certificat.

   Notă: Asiguraţi-vă că daţi fişierului un nume şi o extensie unice. De exemplu, puteţi denumi fişierul myfile.exp. Când numiţi fişierul, nu folosiţi una din aceste extensii pentru fişier: .TXT, .KDB, .RDB sau .KYR deoarece folosind una din aceste extensii poate cauza o eroare când importaţi certificatele din fişier. Selectaţi nivelul de ediţie corespunzător pentru sistemul destinaţie care va folosi acest certificat. Ediţia pe care aţi selectat-o afectează formatul pentru certificatul exportat.
8. Selectaţi **OK**. În partea de sus a paginii va fi afişat un mesaj informare despre faptul DCM a exportat în fişier certificatul specificat.

La acest punct, ar trebui să fi folosit DCM pe sistemul gazdă original V5R2 pentru a exporta o copie suplimentară a certificatului CA local şi să-l fi transferat manual pe sistemul destinaţie V4R4 sau V5R5. Ar fi trebuit să fi folosit DCM pe acest sistem destinaţie pentru a exporta certificatul privat server sau client într-un fişier. Acum sunteţi gata să importaţi aceste certificate în depozitul de certificate *SYSTEM. Trebuie să importaţi certificatul CA local *înainte* de a importa certificatul privat pe care l-aţi creat cu acesta. Dacă importaţi întâi certificatul privat, s-ar putea să întâlniţi o eroare deoarece certificatul CA local nu există în depozitul de certificate.

Pentru a se importa certificatele din aceste fişiere de export şi pentru a specifica aplicaţiile active-SSL care să le folosească, urmaţi paşii de mai jos pe sistemele destinaţie V4R4:

1. Porniţi DCM.
2. În cadrul de navigare, asiguraţi-vă că *SYSTEM este arătat ca depozitul de certificate din lista drop-down şi selectaţi **Certificate Sistem** pentru a afişa o listă de taskuri disponibile. Apare fereastra **Depozit de certificate şi parolă**.
3. Alegeţi *SYSTEM ca depozit de certificate de deschis, furnizaţi parola şi selectaţi **Continuare**.
4. Acum trebuie să importaţi certificatul CA local din fişierul exportat pe care l-aţi creat pe sistemul gazdă V5R2. În cadrul de navigare, selectaţi **Primirea unui certificat CA** pentru a se afişa un formular.

5. Completaţi acest formular şi alegeţi **OK** pentru a se afişa pagina Primirea cu succes a certificatului. Când lucraţi cu depozitul de certificate *SYSTEM, această pagină afişează o listă de aplicaţii care se pot seta pentru a avea încredere în certificatul CA importat .

   Notă: Unele aplicaţii active-SSL suportă identificarea clientului pe baza certificatelor. Folosirea certificatelor pentru autentificarea client asigură faptul că aplicaţia primeşte un certificat valid înainte de a permite accesul la resursele controlate de aceasta. O aplicaţie cu acest suport trebuie să fie configurată să aibă încredere în CA înainte ca aceasta să poată autentifica certificatele emise de o CA specifică. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificată ca fiind de încredere, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.
6. Selectaţi aplicaţiile care ar trebui să aibă încredere în certificatul CA şi selectaţi **OK**. Pagina Starea aplicaţiei de securitate vă cere confirmarea că aplicaţiile selectate vor considera de încredere noul certificat.
7. Acum puteţi importa certificatul server. În cadrul de navigare, selectaţi **Gestionare certificate** pentru a se afişa o listă de certificate.
8. Alegeţi **Import** pentru a se afişa pagina Importul unui certificat.
9. Completaţi formularul Import certificat şi apăsaţi **OK** pentru a reveni la pagina Gestionare certificate. Asiguraţi-vă că furnizaţi numele fişierului care conţine certificatul server sau client exportat şi că specificaţi o ediţie destinaţie care se potriveşte cu cea pe care aţi specificat-o la exportarea anterioară a certificatului. În partea de sus a paginii va fi afişat un mesaj informare despre faptul că DCM a adăugat certificatul la depozitul curent de certificate. Certificatul pe care îl veţi importa ar trebui să apară de asemenea în lista certificatelor.
10. Acum trebuie să specificaţi ce aplicaţii ar trebui să folosească certificatul privat importat pentru sesiuni SSL. În cadrul de navigare, selectaţi **Lucru cu aplicaţii sigure** pentru a afişa o pagină care vă permite să gestionaţi certificatele asociate cu anumite aplicaţii.
11. Selectaţi o aplicaţie din listă şi apăsaţi **Lucru cu certificate sistem** pentru a afişa o listă de certificate pe care puteţi specifica că le foloseşte aplicaţia selectată pentru stabilirea de sesiuni SSL.
12. Selectaţi certificatul din listă şi efectuaţi un clic pe **Atribuirea noului certificat** pentru a asigna certificatul selectat aplicaţiei specificate. În partea de sus a ferestrei va fi afişat un mesaj de informare pentru a indica selecţia certificatului.

Cu aceste taskuri completate, aplicaţiile de pe sistemul destinaţie V4R4 sau V4R5 pot folosi certificatul emis de CA local de pe alt iSeries. Totuşi, înainte de a folosi SSL pentru aceste aplicaţii, va trebui să configuraţi aplicaţiile pentru a folosi SSL.

Înainte ca un utilizator să poată accesa aplicaţiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obţine o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA trebuie copiat într-un fişier pe PC-ul utilizatorului sau transferat în browser-ul utilizatorului, în funcţie de cerinţele aplicaţiei ce foloseşte SSL.

Gestionare aplicaţii în DCM

Puteţi folosi DCM (Digital Certificate Manager) pentru a efectua diferite task-uri de gestiune pentru aplicaţiile active-SSL şi pentru aplicaţiile care semnează obiectele. De exemplu, puteţi alege ce certificate folosesc aplicaţiile pentru sesiuni de comunicare Secure Sockets Layer (SSL). Taskurile de gestiune a aplicaţiilor pe care le puteţi realiza variază în funcţie de tipul de aplicaţie şi de depozitul de certificate în care lucraţi. Puteţi gestiona aplicaţii doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

În timp ce majoritatea task-urilor de management furnizate de DCM sunt uşor de înţeles, unele dintre ele s-ar putea să nu vă fie familiare. Pentru mai multe informaţii despre aceste task-uri, revedeţi subiectele:

Crearea unei definiţii de aplicaţie descrie tipurile de aplicaţii pe care le puteţi defini şi cu care puteţi lucra.

Gestionarea asignărilor de certificate descrie cum să asignaţi sau să schimbaţi certificatul pe care îl foloseşte o aplicaţie pentru a stabili o sesiune SSL sau pentru a semna obiecte.

Definirea unui liste de încredere de CA descrie când puteţi şi când trebuie să definiţi în ce Autoritate certificare poate să se încreadă o aplicaţie pentru validarea şi acceptarea certificatelor.

Puteţi găsi informaţii despre alte taskuri DCM în ajutorul online.

Crearea unei definiţii de aplicaţie

Există două tipuri de definiţii aplicaţie cu care puteţi lucra în DCM: definiţii aplicaţie pentru aplicaţii client sau server care folosesc SSL şi definiţii aplicaţie pe care le folosiţi pentru semnarea obiectelor.

Pentru a folosi DCM în lucrul cu definiţii aplicaţie SSL şi certificatele lor, aplicaţia trebuie mai întâi să se înregistreze cu DCM ca o definiţie aplicaţie pentru a avea un ID unic. Cei care au creat aplicaţia înregistrează aplicaţiile active-SSL folosind un API (QSYRGAP, QsyRegisterAppForCertUse) pentru a crea ID-ul aplicaţiei în DCM automat. Toate aplicaţiile IBM iSeries activate prin SSL sunt înregistrate cu DCM aşa că puteţi să folosiţi cu uşurinţă DCM pentru a asigna un certificat către ele astfel încât să poată stabili o sesiune SSL. De asemenea, pentru aplicaţiile pe care le scrieţi sau cumpăraţi, puteţi defini o definiţie aplicaţie şi să creaţi ID-ul aplicaţie pentru el chiar din DCM. Trebuie să lucraţi în depozitul de certificate *SYSTEM pentru a crea o definiţie aplicaţie SSL pentru o aplicaţie server sau client.

Pentru a folosi un certificat pentru semnarea obiectelor, trebuie să definiţi mai întâi o aplicaţie pe care să o folosească certificatul. Spre deosebire de o definiţie aplicaţie SSL, o aplicaţie care semnează obiecte nu descrie o aplicaţie reală. În schimb, o definiţie aplicaţie pe care o creaţi ar trebui să descrie tipul sau grupul de obiecte pe care doriţi să îl semnaţi. Trebuie să lucraţi în depozitul de certificate *OBJECTSIGNING pentru a crea o definiţie aplicaţie care semnează obiecte.

Pentru a crea o definiţie aplicaţie, urmaţi aceşti paşi:

1. Porniţi DCM.
2. Alegeţi **Selectare depozit de certificate** şi selectaţi depozitul de certificate corespunzător. (Acesta este fie depozitul de certificate *SYSTEM, fie *OBJECTSIGNING în funcţie de tipul de definiţie aplicaţie pe care o creaţi.)

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutorul on-line.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de task-uri.
5. Selectaţi **Adăugarea unei aplicaţii** din lista de task-uri pentru a se afişa un formular pentru definirea aplicaţiei.

   Notă: Dacă lucraţi în depozitul de certificate *SYSTEM, DCM vă va cere să alegeţi dacă să adauge o definiţie de aplicaţie server sau o definiţie de aplicaţie client.

6. Completaţi formularul şi apăsaţi **Continuare**. Informaţia pe care o puteţi specifica pentru definiţia aplicaţiei variază pe baza tipului de aplicaţie pe care o definiţi. Dacă definiţi o aplicaţie server, puteţi specifica de asemenea dacă aplicaţia poate folosi certificate pentru autentificarea client şi trebuie să ceară autentificare client. Puteţi specifica de asemenea dacă aplicaţia trebuie să folosească o listă de încredere CA pentru a autentifica certificatele.

Gestionarea asignării de certificate pentru o aplicaţie

Trebuie să folosiţi DCM (administratorul de certificare digitale) pentru a atribui un certificat unei aplicaţii înainte ca aceasta să poată efectua o funcţie sigură, cum ar fi stabilirea unei sesiuni Secure Sockets Layer (SSL) sau semnarea unui obiect. Pentru a atribui un certificat unei aplicaţii sau pentru a modifica atribuirea certificatului pentru o aplicaţie, urmaţi aceşti paşi:

1. Porniţi DCM.
2. Alegeţi **Selectare depozit de certificate** şi selectaţi depozitul de certificate corespunzător. (Acesta este fie depozitul de certificate *SYSTEM, fie *OBJECTSIGNING în funcţie de tipul de aplicaţie căreia îi atribuiţi certificatul.)

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutorul on-line.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de task-uri.
5. Dacă sunteţi în depozitul de certificate *SYSTEM, selectaţi tipul aplicaţiei de gestionat. (Selectaţi fie aplicaţie **Server** fie **Client**, în funcţie de caz.)
6. Din lista de task-uri, selectaţi **Actualizarea atribuirii certificatelor** pentru a se afişa o listă de aplicaţii pentru care puteţi atribui un certificat.
7. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Actualizarea atribuirii certificatelor** pentru a se afişa o listă de certificate pe care le puteţi atribui aplicaţiei.
8. Selectaţi certificatul din listă şi efectuaţi un clic pe **Atribuirea noului certificat**. DCM va afişa un mesaj pentru a confirma selecţia certificatului pentru aplicaţie.

   Notă: Dacă atribuiţi un certificat unei aplicaţii active-SSL care suportă folosirea certificatelor pentru autentificare client, trebuie să definiţi o listă de încredere CA pentru aplicaţie. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificată ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază a unei autentificări valide.

Când modificaţi sau ştergeţi un certificat pentru o aplicaţie, aceasta poate să nu recunoască modificările dacă rulează în momentul modificării atribuirii certificatului. De exemplu, server-ele Client Access Express vor aplica automat modificările pe care le faceţi. Totuşi, s-ar putea să fie nevoie să opriţi şi să porniţi servere Telnet, IBM Serverul HTTP pentru iSeries sau alte aplicaţii înainte ca aceste aplicaţii să poată efectua modificările certificatelor dumneavoastră.

Începând cu V5R2, puteţi utiliza taskul Asignare certificate când doriţi să asignaţi un certificat către mai multe aplicaţii în acelaşi timp.

Definirea unei liste de CA de încredere pentru o aplicaţie

Aplicaţiile care suportă folosirea certificatelor pentru autentificare client în timpul unei sesiuni Secure Sockets Layer (SSL) trebuie să determine dacă vor accepta sau nu un certificat

ca probă validă a identităţii. Unul dintre criteriile pe care le foloseşte o aplicaţie pentru autentificarea unui certificat este dacă aceasta are încredere în CA (autoritatea de certificare) care a emis certificatul.

Puteţi folosi DCM (Digital Certificate Manager) pentru a defini CA-urile în care poate avea încredere o aplicaţie atunci când aceasta efectuează o autentificare client pentru certificate. CA-urile în care are încredere o aplicaţie se gestionează prin intermediul unei liste de încredere CA.

Înainte de a se putea defini o listă de încredere CA pentru o aplicaţie, trebuie să fie îndeplinite mai multe condiţii:
- Aplicaţia trebuie să suporte utilizarea certificatelor pentru autentificare client.
- Definiţia aplicaţiei trebuie să specifice faptul că aceasta foloseşte o listă de încredere CA.

Dacă definiţia pentru o aplicaţie specifică faptul că o aplicaţie foloseşte o listă de încredere CA, trebuie să definiţi lista înainte ca aplicaţia să poată efectua cu succes autentificarea client a certificatului. Acest lucru asigură faptul că aplicaţia poate valida doar acele certificate care provin de la CA-uri pe care le-aţi specificat ca fiind de încredere. Dacă utilizatorii sau o aplicaţie client prezintă un certificat care provine de la o CA care nu este specificată ca fiind de încredere în lista de încredere CA, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

Atunci când adăugaţi o CA listei de încredere a unei aplicaţii, trebuie să vă asiguraţi că acesta este şi el activ.

Pentru a defini o listă de încredere CA pentru o aplicaţie, urmaţi aceşti paşi:
1. Porniţi DCM.
2. Alegeţi **Selectare depozit de certificate** şi selectaţi *SYSTEM în timp ce se deschide depozitul de certificate.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutorul on-line.
3. Când apare pagina Depozit certificate şi Parolă, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi apăsaţi **Continuare**.
4. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Definirea listei de încredere CA**.
6. Selectaţi tipul de aplicaţie (server sau client) pentru care doriţi să definiţi lista şi alegeţi **Continuare**.
7. Selectaţi din listă o aplicaţie şi efectuaţi un clic pe **Continuare** pentru a se afişa o listă de certificate CA pe care le utilizaţi pentru a defini lista de încredere.
8. Selectaţi CA-urile în care ar trebui să aibă încredere aplicaţia şi selectaţi **OK**. DCM va afişa un mesaj pentru a confirma selecţiile pentru lista de încredere.

   Notă: Puteţi selecta fie CA-uri individuale din listă, fie puteţi specifica faptul că aplicaţia ar trebui să aibă încredere în toate sau în nici unul dintre CA-urile din listă. De asemenea, puteţi vizualiza sau valida certificatele CA înainte de a le adăuga listei de încredere.

Validare certificate şi aplicaţii

Puteţi folosi DCM (Digital Certificate Manager) pentru a valida certificate individuale sau aplicaţiile care le folosesc. Lista de lucruri pe care le verifică DCM diferă puţin în funcţie de validarea unui certificat sau a unei aplicaţii.

Validarea aplicaţiilor

Folosirea DCM pentru a se valida o definiţie aplicaţie ajută prevenirea problemelor legate de certificate pentru aplicaţie atunci când efectuează o funcţie care cere certificate. Asemenea probleme nu împiedică aplicaţia de la a participa cu succes la o sesiune Secure Sockets Layer (SSL) sau de la a semna cu succes obiectele.

Atunci când validaţi o aplicaţie, DCM verifică dacă există o atribuire a unui certificat pentru aplicaţie şi se asigură că certificatul atribuit este valid. În plus, DCM se asigură că dacă aplicaţia este configurată pentru a folosi o listă de încredere Autoritate de certificare (CA), atunci lista de încredere conţine cel puţin un certificat CA. DCM verifică mai apoi dacă certificatele CA din lista de încredere CA a aplicaţiei sunt valide. De asemenea, dacă definiţia aplicaţie specifică dacă apare procesarea CRL (lista de revocare a certificatelor) şi dacă este definită o locaţie CRL pentru CA, DCM verifică CRL ca parte a procesului de validare.

Validarea certificatelor

Atunci când validaţi un certificat, DCM verifică un număr de articole aparţinând certificatului pentru a asigura autenticitaţea şi validarea certificatului. Validarea unui certificat se asigură că pentru aplicaţia care foloseşte certificatul pentru comunicaţii sigure sau pentru semnarea obiectelor nu există şanse mari să apară probleme la folosirea certificatului.

Ca parte a procesului de validare, DCM verifică dacă certificatul selectat nu este expirat. De asemenea, DCM verifică dacă certificatul nu se află în CRL (lista de revocare a certificatelor) ca fiind revocat, dacă locaţia CRL există pentru CA care a emis acest certificat. În plus, DCM verifică dacă certificatul CA pentru CA care emite este în depozitul de certificate curent şi dacă certificatul CA este activat şi deci de încredere. Dacă certificatul are o cheie privată (de exemplu, certificate server, client şi care semnează obiecte), atunci DCM validează de asemenea perechea de chei publică-privată pentru a se asigura că aceasta se potriveşte. Cu alte cuvinte, DCM criptează datele cu cheia publică şi apoi se asigură că acestea pot fi decriptate cu cheia privată.

Asignarea unui certificat către aplicaţii

Începând cu V5R2, o nouă îmbunătăţire a DCM vă permite să asignaţi un certificat rapid şi uşor către mai multe aplicaţii. Puteţi asigna un certificat către mai multe aplicaţii doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

Pentru a face o asignare de certificat pentru una sau mai multe aplicaţii, urmaţi aceşti paşi:

1. Porniţi DCM.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular în timp ce folosiţi DCM, selectaţi butonul cu semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
2. În cadrul de navigare, apăsaţi **Selecţie Depozit de certificate** şi selectaţi ***OBJECTSIGNING** sau ***SYSTEM** ca depozitul de certificate de deschis.
3. Introduceţi parola pentru depozitul de certificate şi apăsaţi **Continuare**.
4. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Asignare certificat** pentru a afişa o listă de certificate pentru depozitul de certificate curent.
6. Selectaţi un certificat din listă şi apăsaţi **Asignare către aplicaţii** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate curent.
7. Selectaţi una sau mai multe aplicaţii din listă şi apăsaţi **Continuare**. Apare o pagină fie cu un mesaj de confirmare pentru selecţia dvs. de asignare fie cu un mesaj de eroare dacă a apărut o problemă.

Administrarea locaţiei CRL

Digital Certificate Manager (DCM) vă permite să definiţi şi să administraţi informaţii despre locaţia Listei de Revocare Certificate (Certificate Revocation List - CRL) pentru o Autoritate de Certificare (CA) particulară pentru a o folosi ca parte din procesul de validare a certificatului. DCM sau o aplicaţie care necesită procesare CRL poate folosi CRL pentru a determina dacă Autoritatea de certificare care a emis un certificat specific nu l-a revocat. Când definiţi o locaţie a CRL pentru o CA particulară, aplicaţiile care suportă folosirea de certificate pentru autentificarea clienţilor pot accesa CRL.

Aplicaţiile care suportă folosirea de certificate pentru autentificarea clienţilor pot efectua procesarea CRL pentru a asigura o autentificare mai stringentă pentru certificatele pe care le acceptă ca dovezi valide ale identităţii. Înainte ca o aplicaţie să poată folosi o CRL definită ca parte a procesului de validare a certificatului, definiţia aplicaţie DCM trebuie să ceară aplicaţiei să efectueze procesare CRL.

Cum funcţionează procesarea CRL

Atunci când folosiţi DCM pentru a valida un certificat sau o aplicaţie, DCM efectuează procesarea CRL implicit ca parte a procesului de validare. Dacă nu este definită nici o locaţie CRL pentru CA care a emis certificatul pe care îl validaţi, DCM nu va putea efectua o verificare CRL. Oricum, DCM poate încerca să valideze alte informaţii importante despre certificat, precum aceea că semnătura CA de pe un anume certificat este validă şi că CA care l-a emis este de încredere.

Definiţi o locaţie a CRL

Pentru a defini o locaţie CRL pentru o CA specifică, urmaţi aceşti paşi:

1. Porniţi DCM.
2. În cadrul de navigare, selectaţi **Gestionarea locaţiilor CRL** pentru a se afişa o listă de task-uri.
3. Selectaţi **Adăugarea unei locaţii CRL** din lista de task-uri pentru a se afişa un formular pe care îl puteţi folosi pentru a descrie locaţia CRL şi cum DCM sau altă aplicaţie ar trebui să acceseze această locaţie.
4. Completaţi acest formular şi alegeţi **OK**. Trebuie să daţi un nume unic locaţiei CRL, să identificaţi serverul LDAP care găzduieşte CRL şi să furnizaţi informaţii despre conexiune care să descrie cum se accesează serverul LDAP.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în task-ul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.

   Acum trebuie să asociaţi definiţia locaţiei CRL cu o CA specifică.
5. În fereastra de navigare, selectaţi **Gestionare Certificate** pentru a afişa o listă a task-urilor.
6. Selectaţi **Actualizare asignare locaţie CRL** din lista de task-uri pentru a afişa o listă de certificate CA.
7. Selectaţi din listă certificatul CA cu care vreţi să asignaţi definiţia locaţiei CRL pe care aţi creat-o şi faceţi clic pe **Actualizare Asignare Locaţie CRL**. Va fi afişată o listă a locaţiilor CRL.
8. Selectaţi din listă locaţia CRL pe care vreţi să o asociaţi cu CA şi faceţi clic pe **Actualizare Asignare**. Va fi afişat un mesaj la începutul paginii indicate pentru a indica faptul că locaţia CRL a fost asignată cu certificatul Autorităţii de Certificare (CA).

După ce aţi definit o locaţie pentru o CRL pentru o CA specifică, DCM sau alte aplicaţii pot să o folosească pentru a efectua procesare CRL. Totuşi, înainte ca procesarea CRL să poată

funcţiona, server-ul Directory Services trebuie să conţină CRL corespunzătoare. De asemenea, trebuie să configuraţi şi server-ul Directory Services şi aplicaţiile client pentru a folosi SSL, şi să atribuiţi din DCM un certificat aplicaţiilor.

Pentru a afla mai multe despre configurarea şi folosirea serverului iSeries Directory Services (LDAP), treceţi în revistă aceste subiecte din Centrul de Informaţii:

- Directory Services (LDAP)
  Acest subiect vă spune tot ce trebuie să ştiţi despre configurarea şi folosirea unui server iSeries Directory Services (LDAP).
- Folosirea securităţii Secure Sockets Layer (SSL) împreună cu server-ul LDAP
  Acest articol vă explică despre ce aveţi nevoie pentru a configura server-ul LDAP pentru a folosi comunicaţii sigure SSL.

Depozitarea cheilor de certificate pe IBM Coprocesorul Criptografic 4758

Dacă aţi instalat un IBM Coprocesor Criptografic 4758–023 PCI pe serverul dvs. iSeries, puteţi folosi coprocesorul pentru a vă oferi stocarea mai sigură a cheii private a unui certificat. Puteţi folosi coprocesorul pentru a stoca cheia privată pentru un certificat server, unul client sau pentru un certificat Autoritate de certificare (CA) locală. Totuşi, nu puteţi folosi coprocesorul pentru a depozita cheia privată a unui certificat utilizator deoarece aceasta trebuie să fie stocată pe sistemul utilizatorului. De asemenea, în acest moment nu puteţi folosi coprocesorul pentru a depozita cheia privată pentru un certificat care semnează obiecte.

Puteţi folosi coprocesorul pentru depozitarea cheii private a certificatului în două moduri:
- Depozitarea cheii private a certificatului direct pe coprocesor.
- Folosirea cheii master a coprocesorului pentru a encripta cheia privată a certificatului pentru a o depozita într-un fişier cheie special.

Puteţi selecta această opţiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat. De asemenea, dacă folosiţi coprocesorul pentru a depozita cheia privată a unui certificat, puteţi modifica atribuirea dispozitivului coprocesor pentru acea cheie.

Pentru a folosi coprocesorul pentru depozitarea cheii private, trebuie să vă asiguraţi că acesta este variat înainte de a folosi DCM (Digital Certificate Manager). Altfel, DCM nu va oferi o pagină pentru a se selecta opţiunea pentru depozitare ca parte a procesului de creare sau reînnoire al certificatului.

Dacă dvs. creaţi sau reînnoiţi un certificat server sau client, selectaţi opţiunea de depozitare a cheii private după ce selectaţi tipul de CA care semnează certificatul curent. Dacă dvs. creaţi sau reînnoiţi o CA locală, selectaţi opţiunea de depozitare a cheii private ca prim pas al procesului.

Stocarea cheii private a certificatului direct pe coprocesor

Pentru a proteja mai puternic accesul la şi folosirea unei chei private a unui certificat, puteţi alege să memoraţi cheia direct pe un IBM Coprocesor Criptografic 4758–023 PCI. Puteţi selecta această opţiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat în DCM (administratorul de certificare digitală).

Urmaţi aceşti paşi din pagina **Selecţia unei locaţii de depozitare a cheii** pentru a depozita cheia privată a certificatului direct pe coprocesor:
1. Selectaţi **Hardware** ca opţiune de depozitare.
2. Selectaţi **Continuare**. Acum se va afişa pagina **Selectaţi descrierea unui dispozitiv criptografic**.

3. Din lista de dispozitive, selectaţi-l pe cel pe care doriţi să îl folosiţi pentru depozitarea cheii private a certificatului.
4. Selectaţi **Continuare**. DCM va continua să afişeze pagini pentru task-ul pe care îl realizaţi, cum ar fi informaţii de identificare pentru certificatul pe care îl creaţi sau reînnoiţi.

Folosirea cheii principale (master key) a coprocesorului pentru a cripta cheia privată a certificatului

Pentru a proteja mai puternic accesul la şi folosirea unei chei private a unui certificat, puteţi folosi cheia principală a unui IBM Coprocesor Criptografic 4758–023 PCI pentru a cripta cheia privată şi pentru a memora cheia într-un fişier cheie special. Puteţi selecta această opţiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat în DCM (administratorul de certificare digitală).

Înainte de a putea folosi cu succes această opţiune, trebuie să folosiţi interfaţa web de configurare a IBM Coprocesorului Criptografic 4758–023 PCI pentru a crea un fişier cheie corespunzător. De asemenea, trebuie să folosiţi interfaţa de configurare web a coprocesorului pentru a asocia fişierul care depozitează cheia cu descrierea dispozitiv a coprocesorului pe care doriţi să îl folosiţi. Puteţi accesa interfaţa web de configurare a coprocesorului din pagina de Taskuri iSeries.

Dacă sistemul are mai mult de un dispozitiv coprocesor instalat şi funcţionabil (varied on), puteţi alege să partajaţi cheia privată a certificatului peste mai multe dispozitive. Pentru ca descrierile dispozitiv să partajeze cheia privată, toate dispozitivele trebuie să aibă aceeaşi cheie master. Procesul de distribuire a aceleaşi chei master pentru mai multe dispozitive se numeşte *clonare*. Partajarea de chei peste dispozitive vă permite să folosiţi balansarea muncii Secure Sockets Layer (SSL), care poate îmbunătăţi performanţele pentru sesiuni sigure.

Urmaţi aceşti paşi din pagina **Selecţia unei locaţii de depozitare a cheii** pentru a folosi cheia master a coprocesorului pentru a cripta cheia privată şi pentru a o stoca într-un fişier special de depozitare a cheilor:

1. Selectaţi **Criptare hardware** ca opţiune de depozitare.
2. Selectaţi **Continuare**. Acum se va afişa pagina **Selectaţi descrierea unui dispozitiv criptografic**.
3. Din lista de dispozitive, selectaţi-l pe cel pe care doriţi să îl folosiţi pentru criptarea cheii private a certificatului.
4. Selectaţi **Continuare**. Dacă aveţi mai mult de un coprocesor instalat pornit (varied on), se afişează pagina **Selecţia unor descrieri dispozitiv suplimentare**.

   Notă: Dacă nu aveţi mai multe dispozitive coprocesor disponibile, DCM va continua să afişeze pagini pentru task-ul pe care îl completaţi, cum ar fi informaţii de identificare pentru certificatul pe care îl creaţi sau reînnoiţi.
5. Din lista de dispozitive, selectaţi numele unei sau a mai multor descrieri dispozitiv cu care doriţi să partajaţi cheia privată a certificatului.

   Notă: Descrierile dispozitiv pe care le selectaţi trebuie să aibă aceeaşi cheie master ca şi dispozitivul selectat în pagina precedentă. Pentru a verifica dacă cheia master este aceeaşi pentru dispozitive, folosiţi task-ul Verificarea cheii master din interfaţa web a coprocesorului criptografic 4758. Puteţi accesa interfaţa web de configurare a coprocesorului din pagina de Taskuri iSeries.
6. Selectaţi **Continuare**. DCM va continua să afişeze pagini pentru task-ul pe care îl efectuaţi, cum ar fi informaţii de identificare pentru certificatul pe care îl creaţi sau reînnoiţi.

Gestionarea localizării cererii pentru o PKIX CA

O Autoritate de Certificare (Certificate Authority - CA) de tip Infrastructură de Chei Publice pentru X.509 (Public Key Infrastructure for X.509 - PKIX) este o AC care emite certificate pe baza ultimelelor standarde Internet x.509 pentru implementarea unei infrastructuri de chei publice. Standardele PKIX sunt subliniate în RFC (cereri pentru comentarii) 2560.

O CA PKIX cere o identificare mai bună înainte de a emite un certificat; în general el cere ca un aplicant să furnizeze o dovadă a identităţii prin RA (autoritate de înregistrare). După ce un aplicant furnizează dovada identităţii pe care o cere RA, acesta certifică identitatea aplicantului. Ori RA-ul ori aplicantul, în funcţie de procedura Autorităţii de Certificare, trimite aplicaţia certificată către AC asociată. Pe măsură ce aceste standarde sunt adoptate mai larg, AC-uri compatibile PKIX vor deveni disponibile pe scară mai largă. Ar trebui să încercaţi să folosiţi o CA compatibilă PKIX dacă cerinţele de securitate necesită un control strict al accesului la resursele pe care aplicaţiile active-SSL le furnizează utilizatorilor. De exemplu, Lotus Domino oferă o PKIX CA pentru uzul public.

Dacă aţi ales ca CA PKIX să emită certificate care să fie folosite de aplicaţii, puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona aceste certificate. Folosiţi DCM pentru a configura un URL pentru o CA PKIX. Dacă faceţi acest lucru DCM (Digital Certificate Manager) va fi configurat pentru a furniza o CA PKIX ca o opţiune pentru a se obţine certificate semnate.

Pentru a folosi DCM pentru gestionarea certificatelor provenite de la o CA PKIX, trebuie mai întâi să configuraţi DCM pentru a folosi această locaţie pentru CA urmând paşii:

1. Porniţi DCM.
2. În cadrul de navigare, selectaţi **Gestionarea locaţiei cererii PKIX** pentru a se afişa un formular care vă va permite să specificaţi un URL pentru CA PKIX sau pentru RA-urile asociate.
3. Introduceţi URL-ul complet calificat pentru CA PKIX pe care doriţi să o folosiţi pentru a cere un certificat; de exemplu: http://www.thawte.com şi selectaţi **Adăugare**. Adăugarea unui URL configurează DCM pentru a adăuga CA PKIX ca o opţiune pentru obţinerea de certificate semnate.

După ce adăugaţi o locaţie de cerere PKIX CA, DCM adaăgă PKIX CA ca o opţiune pentru specificarea tipului de CA pe care o alegeţi pentru emiterea unui certificat când folosiţi taskul **Creare Certificat**.

Semnare obiecte

Sunt trei metode pe care le puteţi folosi pentru semnarea obiectelor. Puteţi scrie un program care apelează API-ul Semnare Obiect. Puteţi folosi Digital Certificate Manager (DCM) pentru a semna obiecte. Sau, începând cu V5R2, puteţi folosi opţiunea Navigatorului iSeries Management Central pentru a semna obiecte pe măsură ce le împachetaţi pentru a le distribui către alte sisteme iSeries.

Puteţi folosi certificatele pe care le gestionaţi cu DCM pentru a semna orice obiect pe care îl depozitaţi în sistemul de fişiere integrat al sistemului, cu excepţia obiectelor care sunt depozitate într-o bibliotecă. Puteţi semna doar obiectele care sunt depozitate în sistemul de fişiere QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG şi *FILE (doar salvare fişier). Nou în V5R2, puteţi de asemenea să semnaţi obiecte comandă (*CMD). Nu puteţi semna obiecte care sunt memorate pe alte servere iSeries.

Puteţi semna obiecte cu certificate pe care le cumpăraţi de la o Autoritate certificare Internet publică (CA) sau pe care le creaţi cu un CA local privat în DCM. Procesul de semnare a certificatelor este acelaşi, indiferent dacă folosiţi certificate publice sau private.

Cerinţe anterioare semnării obiectelor

Înainte de a putea folosi DCM (sau Sign Object API) pentru semnarea obiectelor, trebuie să vă asiguraţi că sunt îndeplinite anumite cerinţe necesare anterior:

- Trebuie să fi creat depozitul de certificate *OBJECTSIGNING, fie ca parte a procesului de creare a unui CA local fie ca parte a procesului de gestionare a certificatelor de semnare obiecte de la un CA Internet public.
- Depozitul de certificate *OBJECTSIGNING trebuie să conţină cel puţin un certificat, fie unul pe care l-aţi creat folosind CA local fie unul pe care l-aţi obţinut de la un CA Internet public.
- Trebuie să fi creat o definiţie de aplicaţie de semnare obiecte de folosit pentru semnarea obiectelor.
- Trebuie să fi asignat un certificat către aplicaţia de semnare obiecte pe care aveţi de gând să o folosiţi pentru a semna obiecte.

Folosiţi DCM pentru a semna obiecte

Pentru a folosi DCM pentru a semna unul sau mai multe obiecte, urmaţi aceşti paşi:

1. Porniţi DCM.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular în timp ce folosiţi DCM, selectaţi butonul cu semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** în timp ce se deschide certificatul.
3. Introduceţi parola pentru depozitul de certificate *OBJECTSIGNING şi apăsaţi **Continuare**.
4. După ce cadrul de navigare se reafişează, selectaţi **Gestionarea obiectelor care pot fi semnate** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Semnarea unui obiect** pentru a se afişa o listă de definiţii de aplicaţii pe care le puteţi folosi pentru a semna obiecte.
6. Selectaţi o aplicaţie şi apăsaţi **Semnarea unui obiect** pentru a vizualiza un formular pentru specificarea locaţiei obiectelor pe care doriţi să le semnaţi.

   Notă: Dacă aplicaţia pe care aţi selectat-o nu are atribuit un certificat, nu o puteţi folosi pentru a semna obiectul. Trebuie să folosiţi mai întâi task-ul **Actualizare atribuire certificat** sub **Gestiunea aplicaţiilor** pentru a atribui un certificat definiţiei aplicaţiei.
7. În câmpul furnizat, introduceţi calea complet calificată şi numele de fişier al obiectului sau directorului de obiecte pe care doriţi să îl semnaţi şi apăsaţi **Continuare**. Sau, introduceţi locaţia directorului şi apăsaţi **Răsfoire** pentru a vizualiza conţinutul directorului pentru a selecta obiectele pentru semnare.

   Notă: Trebuie să porniţi numele obiectului cu un slash în faţă, pentru că altfel poate să apară o eroare. De asemenea, puteţi folosi anumite caractere wildcard pentru a descrie partea din director pe care doriţi să o semnaţi. Aceste caractere wildcard sunt asterisc-ul (*****), care specifică ″orice număr de caractere″ şi semnul de întrebare (**?**), care specifică ″un singur caracter (oricare).″ De exemplu, pentru a semna toate obiectele dintr-un director specific, puteţi introduce /directorul_meu/*; pentru a semna toate programele dintr-o bibliotecă specifică, puteţi introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteţi folosi aceste caractere wildcard doar în ultima parte a căii; de exemplu, /directorul_meu*/nume_fişier va produce un mesaj de eroare. Dacă doriţi să folosiţi funcţia Răsfoire pentru a afişa o listă a conţinutului bibliotecilor sau directoarelor, ar trebui să introduceţi caracterele wildcard ca o parte a căii înainte de a efectua clic pe **Răsfoire**.

8. Selectaţi opţiunile de procesare pe care doriţi să le folosiţi pentru semnarea obiectului sau obiectelor selectate şi efectuaţi un clic pe **Continuare**.

   Notă: Dacă alegeţi să aşteptaţi rezultatele job-ului, fişierul cu rezultatele se va afişa chiar în browser. Rezultatele pentru job-ul curent sunt adăugate la sfârşitul fişierului de rezultate. În consecinţă, fişierul poate conţine rezultate de la orice job-uri anterioare, în plus faţă de cele ale job-ului curent. Puteţi folosi câmpul dată din fişier pentru a determina care linii din fişier sunt pentru job-ul curent. Câmpul dată este în format AAAALLZZ. Primul câmp din fişier poate fi fie ID-ul mesajului (dacă a apărut o eroare în timpul procesării obiectului) sau câmpul dată (indicând data la care a fost procesat job-ul).
9. Specificaţi calea completă calificată şi numele fişierului care va fi folosit pentru depozitarea rezultatelor operaţiei de semnare a obiectului şi apăsaţi **Continuare**. Sau, introduceţi locaţia directorului şi apăsaţi **Răsfoire** pentru a vedea conţinutul directorului şi pentru a selecta un fişier care să depoziteze rezultatele job-ului. Se afişează un mesaj pentru a indica dacă job-ul a fost propus pentru a semna obiecte. Pentru a vedea rezultatele job-ului, consultaţi job-ul **QOBJSGNBAT** din istoricul de job-uri.

Verificaţi semnăturile obiectului

Puteţi folosi DCM (Digital Certificate Manager) pentru a verifica autenticitatea semnăturilor digitale pentru obiecte. Când verificaţi semnătura, vă asiguraţi că datele obiectului nu au fost schimbate de când acesta a fost semnat de către proprietar.

Cerinţe anterioare verificării semnăturii

Înainte de a putea folosi DCM pentru verificarea semnăturii obiectelor, trebuie să vă asiguraţi că sunt îndeplinite anumite cerinţe necesare:

- Trebuie să fi creat depozitul de certificate *SIGNATUREVERIFICATION pentru a gestiona certificatele de verificarea semnăturilor.

  Notă: Puteţi efectua verificarea semnăturilor în timp ce lucraţi cu depozitul de certificate *OBJECTSIGNING în cazurile în care verificaţi semnături pentru obiecte care au fost semnate pe acelaşi sistem. Paşii parcurşi în timpul verificării semnăturii în DCM sunt aceaşi ca cei parcurşi pentru orice depozit de certificate. Totuşi, trebuie să existe depozitul de certificate *SIGNATUREVERIFICATION şi acesta trebuie să conţină o copie a certificatului care a semnat obiectul chiar dacă efectuaţi verificarea semnăturii în timp ce lucraţi cu depozitul de certificate *OBJECTSIGNING.
- Depozitul de certificate *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului care a semnat obiectele.
- Depozitul de certificate *SIGNATUREVERIFICATION trebuie să conţină o copie a certificatului CA care a emis certificatul care a semnat obiectele.

Folosiţi DCM pentru a verifica semnăturile de pe obiecte

Pentru a folosi DCM pentru a verificarea semnăturilor obiectelor, urmaţi aceşti paşi:
1. Porniţi DCM.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular în timp ce folosiţi DCM, selectaţi butonul cu semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** în timp ce se deschide depozitul de certificate.

3. Introduceţi parola pentru depozitul de certificate *SIGNATUREVERIFICATION şi apăsaţi **Continuare**.
4. După ce cadrul de navigare se reafişează, selectaţi **Gestionarea obiectelor care pot fi semnate** pentru a afişa o listă de task-uri.
5. Din lista de task-uri, selectaţi **Verificarea semnăturilor obiectelor** pentru a specifica locaţia obiectelor pentru care doriţi să verificaţi semnăturile.
6. În câmpul furnizat, introduceţi calea complet calificată şi numele fişierului pentru obiectul sau directorul de obiecte pentru care doriţi să verificaţi semnăturile şi apăsaţi **Continuare**. Sau, introduceţi locaţia directorului şi apăsaţi **Răsfoire** pentru a vizualiza conţinutul directorului pentru a selecta obiectele pentru verificarea semnăturilor.

   Notă: Puteţi de asemenea să folosiţi anumite caractere joker pentru a descrie partea din catalog pe care doriţi să o verificaţi. Aceste caractere wildcard sunt asterisc-ul (*****), care specifică ″orice număr de caractere″ şi semnul de întrebare (**?**), care specifică ″un singur caracter (oricare).″ De exemplu, pentru a semna toate obiectele dintr-un director specific, puteţi introduce /directorul_meu/*; pentru a semna toate programele dintr-o bibliotecă specifică, puteţi introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteţi folosi aceste caractere wildcard doar în ultima parte a căii; de exemplu, /directorul_meu*/nume_fişier va produce un mesaj de eroare. Dacă doriţi să folosiţi funcţia Răsfoire pentru a afişa o listă a conţinutului bibliotecilor sau directoarelor, ar trebui să introduceţi caracterele wildcard ca o parte a căii înainte de a efectua clic pe **Răsfoire**.
7. Selectaţi opţiunea de procesare pe care doriţi să o folosiţi pentru verificarea semnăturii de pe obiectul sau obiectele selectate şi apăsaţi **Continuare**.

   Notă: Dacă alegeţi să aşteptaţi rezultatele job-ului, fişierul cu rezultatele se va afişa chiar în browser. Rezultatele pentru job-ul curent sunt adăugate la sfârşitul fişierului de rezultate. În consecinţă, fişierul poate conţine rezultate de la orice job-uri anterioare, în plus faţă de cele ale job-ului curent. Puteţi folosi câmpul dată din fişier pentru a determina care linii din fişier sunt pentru job-ul curent. Câmpul dată este în format AAAALLZZ. Primul câmp din fişier poate fi fie ID-ul mesajului (dacă a apărut o eroare în timpul procesării obiectului) sau câmpul dată (indicând data la care a fost procesat job-ul).
8. Specificaţi calea completă calificată şi numele fişierului care va fi folosit pentru depozitarea rezultatelor job-ului pentru operaţia de verficare a semnăturii şi apăsaţi **Continuare**. Sau, introduceţi locaţia directorului şi apăsaţi **Răsfoire** pentru a vedea conţinutul directorului şi pentru a selecta un fişier care să depoziteze rezultatele job-ului. Se afişează un mesaj pentru a indica dacă job-ul a fost propus pentru a se verifica semnătura obiectelor. Pentru a vedea rezultatele job-ului, consultaţi job-ul **QOBJSGNBAT** din istoricul de job-uri.

De asemenea, puteţi folosi DCM pentru a găsi informaţii despre certificatul care a semnat un obiect. Astfel vi se permite să determinaţi dacă obiectul provine de la o sursă în care aveţi încredere înainte de a lucra cu acesta.

Capitol 9. Depanare DCM

Puteţi folosi aceste pagini pentru a găsi informaţii utile care vă pot ajuta să depanaţi unele din cele mai comune probleme pe care le puteţi întâlni în timp ce lucraţi cu Digital Certificate Manager (DCM).

Pentru informaţii despre probleme şi posibile soluţii pentru ele, revedeţi aceste pagini:

Depanare parole şi probleme generale
Folosiţi aceste informaţii pentru a afla mai multe despre problemele comune ale interfeţei DCM pe care le puteţi întâlni şi cum puteţi să le corectaţi.

Depanarea memorării de certificate şi probleme cheie ale bazei de date
Folosiţi aceste informaţii pentru a afla mai multe despre problemele comune ale depozitelor de certificate şi ale bazelor de date de chei şi despre cum puteţi să le corectaţi.

Depanare probleme browser
Folosiţi aceste informaţii pentru a afla mai multe despre problemele comune care pot apare atunci când folosiţi browser-ul pentru a accesa DCM şi despre cum puteţi să le corectaţi.

Depanare probleme ale Serverului HTTP pentru iSeries
Folosiţi aceste informaţii pentru a afla mai multe despre problemele comune ale server-ului HTTP pe care le puteţi întâlni şi despre cum puteţi să le corectaţi.

Erori de migrare şi soluţii de rezolvare
Folosiţi aceste informaţii pentru a afla mai multe despre problemele comune care pot apare atunci când migraţi DCM de la o ediţie anterioară şi despre cum puteţi să le corectaţi.

Depanarea asignării unui certificat utilizator
Folosiţi aceste informaţii pentru a afla mai multe despre problemele comune care pot apare atunci când folosiţi DCM pentru a înregistra un certificat utilizator şi despre cum puteţi să le corectaţi.

Depanarea problemelor generale şi cu parolele

Folosiţi următoarea tabelă pentru a găsi informaţii care să vă ajute să depanaţi unele din cele mai comune probleme cu parolele şi alte probleme generale pe care le puteţi întâlni în timp ce lucraţi cu Digital Certificate Manager (DCM).

Problemă	Soluţie posibilă
Nu puteţi găsi ajutor suplimentar pentru DCM.	În DCM, selectaţi ″**?**″ . Puteţi căuta de asemenea şi în Centrul de informaţii şi site-uri externe pe Internet.
Aţi primit o eroare NET.DATA când aţi încercat să deschideţi un depozit de certificate.	Atunci când doriţi **Selectarea unui depozit de certificate**, folosiţi mai repede mouse-ul pentru a selecta butonul **Continuare** decât tasta **Enter**.
Parola pentru Autoritatea de certificare (CA) locală şi depozitele de certificate *SYSTEM nu funcţionează.	Parolele ţin cont de majuscule. Asiguraţi-vă că tasta Caps Lock este la fel ca la atribuirea parolei.
Încercarea dvs. de a reseta parola când aţi folosit taskul Selectare Depozit de certificate a eşuat.	Funcţia de reset merge doar dacă DCM a păstrat parola. DCM memorează parola automat când creaţi un depozit de certificate. Oricum, dacă modificaţi (sau resetaţi) parola pentru un Depozit de certificate de pe alt sistem, atunci trebuie să selectaţi opţiunea **Automatic login** astfel încât DCM să continue să stocheze parola.

Problemă	Soluţie posibilă
	De asemenea, dacă mutaţi un depozit de certificate de la un sistem la altul, trebuie să schimbaţi parola pentru depozitul de certificate pe noul sistem pentru a vă asigura că DCM o memorează automat. Pentru a schimba parola, trebuie să furnizaţi parola originală pentru depozitul de certificate când îl deschideţi pe noul sistem. Nu puteţi folosi opţiunea reset password până când nu aţi deschis depozitul cu parola originală şi nu aţi modificat parola pentru a fi memorată. Dacă parola nu este schimbată şi memorată, DCM şi SSL nu pot să recupereze automat parola când este nevoie de ea pentru diverse funcţii. Dacă mutaţi un depozit de certificate pe care îl veţi folosi ca un Other System Certificate Store, trebuie să selectaţi opţiunea **Automatic login** când modificaţi parola pentru a vă asigura că DCM memorează noua parolă pentru acest tip de depozit de certificate.
	Verificaţi valoarea asignată atributului ″Allow new digital certificates″ (Permite certificate digitale noi) din opţiunea Lucru cu securitatea sistemului din System Service Tools (SST). Dacă acest atribut este setat la valoarea 2 (No), atunci parola depozitului de certificate nu poate fi resetată. Puteţi vedea sau schimba valoarea acestui atribut folosind comanda STRSST şi introducând ID-ul şi parola utilizator Service Tools. Apoi alegeţi opţiunea ″Work with system security″. ID-ul utilizator Service Tools este probabil ID-ul utilizator QSECOFR.
Nu puteţi găsi o sursă pentru un certificat CA ca să-l primiţi în sistemul dvs. iSeries.	Unele CA-uri nu fac disponibile imediat certificatele CA. Dacă nu puteţi obţine certificatul CA de la CA, contactaţi-vă VAR-ul, dacă VAR-ul a făcut înţelegeri speciale sau monetare cu CA.
Nu puteţi găsi depozitul de certificate *SYSTEM.	Locaţia fişierului certificatului *SYSTEM trebuie să fie /qibm/userdata/icss/cert/server/default.kdb. Dacă acel depozit de certificate nu există, trebuie să folosiţi DCM pentru a crea depozitul de certificate. Folosiţi task-ul **Creare Depozit de Certificate Nou**.
Aţi primit o eroare de la DCM, iar eroarea continuă să apară după ce aţi corectat-o.	Ştergeţi cache-ul browser-ului. Setaţi mărimea cache-ului la 0, iar apoi opriţi şi reporniţi browser-ul.
Puteţi avea o problemă de server LDAP, cum ar fi atribuirea de certificate ce nu este afişată atunci când sunt afişate informaţii despre aplicaţiile securizate imediat după atribuirea unui certificat. Această problemă apare mai des când este folosit iSeries Navigator pentru a ajunge la un browser Netscape Communications. Preferinţa dvs. pentru browser cache este setată să compare documentul din cache cu documentul de pe reţea ″Once per session″. (O dată pe sesiune)	Modificaţi opţiunea implicită pentru a verifica cache-ul de fiecare dată.
Când folosiţi DCM pentru a importa un certificat semnat de o CA externă precum Entrust, primiţi un mesaj de eroare cum că perioada de validitate nu conţine ziua de azi sau că nu cade în perioada de valabilitate a emitentului.	Sistemul foloseşte formatul de timp generalizat pentru perioada de validitate. Aşteptaţi o zi şi reîncercaţi. De asemenea, verificaţi că sistemul dvs. iSeries are valoarea corectă pentru UTC offset (dspsysval qutcoffset). Dacă observaţi Daylight Savings Time, diferenţa poate fi setată incorect.
Aţi primit o eroare base 64 când aţi încercat să importaţi un certificat Entrust.	Certificatul este listat ca având un format specific, cum ar fi PEM. Funcţia de copiere a browser-ului nu funcţionează corect şi s-ar putea să copieze material suplimentar ce nu aparţine de certificat, cum ar fi spaţii la începutul fiecărei linii. Dacă acesta este cazul, atunci certificatul nu va fi în formatul corect când veţi încerca să-l folosiţi pe iSeries. Această problemă este cauzată de formatul unor pagini web. Alte pagini web sunt create pentru a evita această problemă. Asiguraţi-vă că aţi comparat certificatul original faţă de rezultatele copierii (paste) din moment ce aceste informaţii ar trebui să arate la fel.

Problemă	Soluţie posibilă
Când migraţi de la versiunea V4R3 a DCM la versiunea V5R2, migrarea nu găzduieşte certificate sistem expirate.	Certificatul sistem expirat nu mai este bun şi nu poate intra în depozitul de certificate *SYSTEM. Înlăturaţi sau redenumiţi vechile fişiere inel cheie din V4R3 înainte de migrare, ignoraţi indicatorul de eşuare a migrării sau încercaţi din nou migrarea.
Nu puteţi găsi exemplul de cod pentru adăugarea de certificate în lista de validare.	Codul nu este încă disponibil.

Depanarea memorării de certificate şi probleme cheie ale bazei de date

Folosiţi următoarea tabelă pentru a găsi informaţii care să vă ajute să depanaţi unele din cele mai comune probleme de memorare a certificatelor şi probleme cheie a bazelor de date pe care le puteţi întâlni în timp ce lucraţi cu Digital Certificate Manager (DCM).

Problemă	Soluţie posibilă
Sistemul nu a găsit baza de date de chei, sau a găsit-o nevalidă.	Verificaţi parola şi numele fişierului pentru erori. Asiguraţi-vă că este inclusă calea cu numele de fişier, inclusiv slash-ul de la început.
Creare bază de date cheie eşuată.	Verificaţi conflictul numelor de fişiere. Conflictul poate exista la alt fişier decât cel de care întrebaţi.
Sistemul nu acceptă un fişier text CA care a fost transferat în mod binar de pe alt sistem. Acceptă fişiere care sunt transferate ASCII.	Inelele cheie şi bazele de date de chei sunt fişiere binare, deci diferite. Trebuie să folosiţi FTP (protocol de transfer fişiere) în mod ASCII pentru fişierele text CA şi FTP (protocol de transfer fişiere) în mod binar pentru fişierele binare, precum .kdb, .kyr, .sth, .rdb ş.a.m.d.
Nu puteţi modifica parola bazei de date cheie. Un certificat din baza de date cheie nu mai este valid.	Dacă problema nu este o parolă incorectă, găsiţi şi ştergeţi certificatul sau cetificatele invalide din depozitul de certificate şi apoi încercaţi să schimbaţi parola. Dacă aveţi certificate expirate în depozitul de certificate, acestea nu mai sunt valide. Dacă certificatele nu sunt valide, funcţia de shimbare parolă pentru depozitul de certificate poate să nu permită schimbarea parolei şi procesul de criptare nu va cripta cheile private ale certificatului expirat. Aceasta previne schimbarea parolei, iar sistemul poate raporta că unul din motive este coruperea depozitului de certificate. Trebuie să eliminaţi certificatele invalide (expirate) din depozit.
Trebuie să folosiţi certificate de la un utilizator Internet şi de aceea trebuie să folosiţi listele de validare, dar DCM nu furnizează funcţii pentru listele de validare.	Partenerii de afaceri ce scriu aplicaţii pentru utilizarea listelor de validare trebuie să scrie codul pentru a asocia lista de validare cu aplicaţiile lor după cum trebuie. Ei trebuie să scrie şi codul care determină când este validată corect identitatea utilizatorului Internet pentru ca certificatul să poată fi adăugat în lista de validare. Revedeţi subiectul Centrul de informaţii pentru QsyAddVldlCertificate API. Consultaţi Webmaster's Guide pentru ajutor la configurarea instanţei securizate de server pentru a folosi lista de validare.

Depanarea problemelor cu browserul

Folosiţi următoarea tabelă pentru a vă ajuta să depanaţi unele dintre cele mai comune probleme legate de browser pe care le puteţi întâlni când lucraţi cu Digital Certificate Manager (DCM).

Problemă	Soluţie Posibilă
Microsoft Internet Explorer nu vă permite să selectaţi alt certificat până când nu porniţi o nouă sesiune a browserului.	Începeţi o nouă sesiune browser pentru Internet Explorer.

Problemă	Soluţie Posibilă
Internet Explorer nu prezintă toate certificatele client/utilizator selectabile din lista de selecţie a unui browser. Internet Explorer arată doar certificate, emise de o CA de încredere, pe care le puteţi folosi pe un site securizat.	O CA trebuie să fie de încredere în baza de date chei, cât şi pentru aplicaţia securizată. Asiguraţi-vă că aţi semnat pe PC pentru browser-ul Internet Explorer cu acelaşi nume de utilizator ca şi cel ce pune certificatul utilizator în browser. Obţineţi alt certificat utilizator de la sistemul pe care îl accesaţi. Administratorul de sistem trebuie să fie sigur că depozitul de certificate (baza de date) mai are încredere în CA care a semnat certificatele utilizator şi sistem.
Internet Explorer 5 primeşte certificatul CA, dar nu poate deschide fişierul sau să găsească discul pe care aţi salvat certificatul.	Aceasta este o nouă facilitate a browser-ului pentru certificate ce nu sunt încă de încredere pentru browser-ul Internet Explorer. Puteţi alege locaţia pe PC.
Aţi primit o atenţionare browser despre numele sistem şi certificatul sistem ce nu se potrivesc.	Unele browser-e fac diferite lucruri pentru potrivirea numelor în funcţie de litere mari sau mici. Tastaţi URL-ul cu acelaşi tip de caractere ca şi cele prezentate de certificatul sistem. Sau, creaţi certificatul sistem cu tipul de litere pe care cei mai mulţi utilizatori îl vor folosi. Numai dacă ştiţi exact ceea ce faceţi, este mai bine să lasaţi numele de server şi sistem cum sunt. Ar trebui, de asemenea, să verificaţi dacă serverul nume domeniu este setat corect.
Aţi pornit Internet Explorer cu HTTPS în loc de HTTP, şi aţi primit un mesaj de atenţionare despre o combinaţie securizată şi nesecurizată de sesiuni.	Alegeţi accept şi ignoraţi avertismentul; o ediţie viitoare a Internet Explorer va corecta această problemă.
Netscape Communicator 4.04 for Windows a convertit valorile hexazecimale A1 şi B1 în B2 şi 9A în pagina de cod Poloneză.	Acesta este un bug de browser ce afectează NLS. Folosiţi alt browser sau chiar folosiţi aceeaşi versiune a browserului pe o altă platformă, precum Netscape Communicator 4.04 for AIX.
Într-un profil utilizator, Netscape Communicator pentru 4.04 arată majusculele din certificatul utilizator NLS corect, dar literele mici sunt afişate incorect.	Unele caractere specifice limbilor naţionale care au fost introduse corect ca un caracter dar care nu sunt acelaşi caracter atunci când sunt afişate mai târziu. De exemplu, în versiunea pentru Windows a Netscape Communicator 4.04, valorile hexazecimale A1 şi B1 au fost convertite în B2 şi 9A pentru pagina de cod Poloneză, conducând la afişarea unor caractere NLS diferite.
Browser-ul continuă să spună utilizatorului final că CA nu este încă de încredere.	Folosiţi DCM pentru a seta **starea CA** pentru a o activa pentru a seta Autoritatea de certificare ca fiind de încredere.
Cererile Internet Explorer resping conexiunea pentru HTTPS.	Aceasta este o problemă a funcţiei browser-ului sau a configuraţiei sale. Browser-ul alege să nu se conecteze la un site care foloseşte un certificat sistem ce poate fi autosemnat sau poate să nu fie valid din anumite motive.
Browser-ul Netscape Communicator şi produsele server folosesc certificate rădăcină de la companii, incluzând, dar nu limitându-se la, VeriSign, ca o facilitate ce se poate activa a comunicaţiilor SSL— mai specific, autentificare. Toate certificatele rădăcină expiră în mod periodic. Unele certificate browser Netscape şi rădăcină server expiră între 25 Decembrie 1999 şi 31 Decenbrie 1999. Dacă nu aţi corectat această problemă înainte de 14 Decembrie 1999, veţi primi un mesaj de eroare.	Versiunile mai vechi ale browser-ului (Netscape Communicator 4.05 sau mai vechi) au certificate care expiră. Trebuie să actualizaţi browser-ul la versiunea curentă a Netscape Communicator. Informaţii despre certificate rădăcină browser sunt disponibile în multe site-uri, cum ar fi http://home.netscape.com/security/ şi http://www.verisign.com/server/cus/rootcert/webmaster.html. Download-ari gratuite ale browser-ului sunt disponibile la http://www.netcenter.com.

Depanarea problemelor Serverului HTTP pentru iSeries

Folosiţi următoarea tabelă pentru a găsi informaţii care să vă ajute să depanaţi unele din cele mai comune probleme ale Serverului HTTP pentru iSeries pe care le puteţi întâlni în timp ce lucraţi cu Digital Certificate Manager (DCM).

Problemă	Soluţie posibilă
Hypertext Transfer Protocol Secure (HTTPS) nu funcţionează.	Asiguraţi-vă că serverul HTTP este setat corect pentru folosirea SSL. În V5R1 sau versiuni ulterioare fişierul de configurare trebuie să aibe **SSLAppName** setat folosind interfaţa grafică (GUI) a Serverului HTTP. De asemenea, configuraţia trebuie să aibe configurată o gazdă virtuală (virtual host) care să folosească portul SSL, cu **SSLEnable** în interiorul gazdei virtuale. De asemenea trebuie să existe două directive listen care să specifice două porturi diferite, unul pentru SSL şi celălalt nu pentru SSL. Asiguraţi-vă că instanţa server este creată şi că certificatul serverului este semnat.
Procesul pentru înregistrarea unei instanţe server HTTP ca o aplicaţie securizată are nevoie de clarificări.	Pe sistemul dvs. iSeries, mergeţi la interfaţa web a Serverului dvs. HTTP pentru a seta configuraţia pentru Serverul dvs. HTTP. Trebuie ca mai întâi să definiţi o gazdă virtuală pentru a activa SSL. Aceasta se face din ecranul Context Management. Gazda virtuală trebuie să fie definită să folosească portul SSL definit anterior în directiva Listen. Apoi, trebuie să folosiţi ecranul Setări Generale SSL pentru a activa SSL în gazda virtuală configurată anterior. Toate schimbările trebuie să fie aplicate fişierului de configurare. Notaţi că înregistrarea instanţei dvs. nu alege automat care certificate trebuie să folosească instanţa. Trebuie să folosiţi DCM pentru a asigna un certificat anume cu aplicaţia dvs. înainte de a încerca să închideţi şi apoi să restartaţi instanţa serverului dvs.
Dacă aveţi dificultăţi la setarea serverului HTTP pentru liste validarea listelor şi autentificării opţionale a clientului.	Consultaţi HTTP Server Webmaster's Guide pentru opţiuni la setarea instanţei. Aceste informaţii sunt disponibile de asemenea în cadrul subiectului Web serving din Centrul de Informaţii.
Netscape Communicator aşteaptă expirarea directivei de configurare din codul server HTTP înainte de a vă permite să selectaţi un alt certificat.	O valoare mare de certificat face dificilă înregistrarea unui al doilea certificat, dacă browser-ul îl mai foloseşte încă pe primul.
Încercaţi ca browser-ul să prezinte certificatul X.509 server-ului HTTP pentru a putea folosi certificatul ca intrare pentru API-urile QsyAddVldlCertificate.	Trebuie să folosiţi **SSLEnable** şi **SSLClientAuth ON** pentru a face ca Serverul HTTP să încarce variabila de mediu HTTPS_CLIENT_CERTIFICATE. Puteţi găsi aceste API-uri în subiectul OS/400 API-uri din Centrul de Informaţii. Puteţi să consultaţi şi aceste liste de validare sau API-uri legate de certificate: • QsyListVldlCertificates şi QSYLSTVC • QsyRemoveVldlCertificate şi QRMVVC • QsyCheckVldlCertificate şi QSYCHKVC • QsyParseCertificate şi QSYPARSC ş.a.m.d.
Nu puteţi găsi fişierul cerere ce este creat la instalarea serverului HTTP. Sistemul foloseşte acest fişier pentru a indica inelele cheie valide găsite pentru directiva KEYFILE din fişierele de configurare din directorul său.	Vedeţi Migrarea la DCM dintr-o ediţie anterioară pentru informaţii suplimentare. Pentru Serverul HTTP fişierul corect este /qibm/userdata/httpsvr/keyring/keymreq.crt. Pentru LDAP fişierul corect este /qibm/userdata/os400/dirsrv/qdirsrv.crt.
Server-ului HTTP îi ia foarte mult timp să se întoarcă sau expiră dacă cereţi o listă de certificate din lista de validare şi sunt mai mult de 10.000 de elemente.	Creaţi un job batch ce caută şi şterge certificate ce corespund unui anumit criteriu, cum ar fi cele ce expirat sau formează un anumit CA.
Aţi observat o problemă cu depozitele dvs. de certificate după instalarea V5R2 peste ediţia V4R3 şi acum există fişierul /qibm/userdata/httpsvr/keyring/keymreq.crt sau /qibm/usedata/os400/dirsrv/qdirsrv.crt. Sistemul nu poate completa migrarea automată de la inel cheie la bază de date cheie.	Specificaţi vechile fişiere inel cheie ca depozit de certificate, apoi găsiţi şi ştergeţi certificatele invalide din fişierele inele cheie înainte de a apela qicss/qyepmgrt pentru a reîncerca migrarea. Sau, ignoraţi sau ştergeţi fişierul .crt dacă activitatea de migrarea a mutat toate certificatele importante.

Problemă	Soluţie posibilă
Serverul HTTP nu va porni cu succes cu **SSLEnable** setat şi va apare mesajul de eroare HTP8351 în jurnalul de joburi. Jurnalul de erori pentru serverul *ADMIN arată o eroare că operaţia de iniţializare SSL a eşuat cu un cod de retur de eroare 107 când Serverul HTTP a eşuat.	Eroarea 107 înseamnă că certificatul a expirat. Dacă instanţa server este serverul *ADMIN, atunci setaţi temporar **SSLDisable** astfel încât să puteţi folosi DCM pe serverul *ADMIN. Folosiţi DCM pentru a asigna un alt certificat aplicaţiei; de exemplu, QIBM_HTTP_SERVER_ADMIN dacă instanţa server este serverul *ADMIN.

Erori de migrare şi soluţii de rezolvare

Erori şi recuperări din eroare

Următorii indicatori vă informează despre erori ce pot apărea în timpul migrării:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
Prezenţa acestui indicator după ce aţi instalat cu succes ambele opţiuni 34 şi 5722-DG1 înseamnă că migrarea inel cheie încercată de 5722-DG1 nu a avut succes. Este posibil să trebuiască să efectuaţi migrarea inel cheie în depozitul de certificate *SYSTEM.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
Prezenţa acestui indicator după ce aţi instalat cu succes opţiunea 34 înseamnă că migrarea inelului de chei pentru serverul LDAP nu a avut succes.

Pe lângă erorile indicate, există erori de migrare posibile pe care sistemul nu le indică. De exemplu, când sistemul găseşte fişiere inel cheie de care are nevoie pentru a migra în depozitul de certificate *SYSTEM, pot apărea şi conflicte cu fişiere de date pentru utilizator integrate în sistemul de fişiere. În acest caz, sistemul poate să nu încheie migrarea fişierului inel cheie, deşi aţi încheiat cu succes instalarea.

Într-un scenariu puţin probabil, este posibil să aveţi realizată migrarea fişierului inel cheie cu o atribuire parţială de certificat sistem, înainte ca o eroare să împiedice încheierea migrării. Aceasta poate avea ca rezultat erori când porniţi instanţa *ADMIN a Serverului HTTP IBM dacă SSLMODE este ON. Explicaţiile posibile sunt:

- Un fişier inel cheie migrat are un certificat sistem invalid setat ca implicit.
- DCM a oprit migrarea pentru a păstra datele utilizator ce existau deja într-un nume critic de fişier.
- A apărut o eroare imprevizibilă în codul de migrare.

Puteţi porni IBM Serverul HTTP fără SSLMODE setat pe ON prin punerea temporară a SSLMODE pe OFF pentru instanţa *ADMIN înainte de pornirea instanţei *ADMIN. Aceasta vă permite să investigaţi depozitul de certificate cu DCM şi să rezolvaţi problema înainte de oprirea instanţei *ADMIN. După ce opriţi instanţa *ADMIN, puteţi reveni la SSLMODE ON (pornit) şi să porniţi instanţa *ADMIN pentru a iniţializa SSL corect.

După migrarea opţiunii 34, pot apărea erori în timpul cererilor DCM normale ce folosesc depozite de certificate. Aceste erori apar în browser. Exemple de astfel de erori:

```
Eroare la baza de date
Eroare la citirea din baza de date
Eroare la scriere în baza de date
Coruperea bazei de date
Tabela bazei de date este coruptă
```

În continuare, sistemul poate avea un fişier ce nu este un depozit de certificate valid, numit default.kdb în acelaşi director ca şi /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR sau

/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. În acest caz, trebuie să efectuaţi următoarele migrări manuale înainte de a folosi DCM pentru a crea certificate noi:

Notă: Dacă alegeţi să nu migraţi fişierele inel cheie, iar, în schimb, să creaţi un certificat sistem şi o CA noi, treceţi peste următoarea procedură de migrare manuală.

- Dacă aveţi de gând să instalaţi Serverul HTTP pentru iSeries (5722-DG1), instalaţi-l acum înainte de a continua.

  Note:

  1. Codul de instalare 572–SS12 opţiunea 34 nu încearcă din nou migrarea după ce instalaţi opţiunea 34. Simpla reinstalarea a opţiunii 34 nu vă ajută cu nimic.
  2. Fişierele corespunzătoare sunt localizate în directoarele pentru date utilizator ce au fost create cu autorizare PUBLIC *EXCLUDE. Asiguraţi-vă că le-aţi autorizat corect.

- Verificaţi dacă următoarele fişiere există:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Dacă există, folosiţi comandaWRKLNK pentru a le redenumi pentru a crea copii de siguranţă.
- Dintr-un profil utilizator ce are autorizare *ALLOBJ, apelaţi programul QICSS/QYEPMGRT în linia de comandă, după cum urmează:

  ```
  CALL QICSS/QYEPMGRT
  ```

  Dacă rezultatul este bun, asiguraţi-vă că nici unul din următoarele fişiere nu există în sistemul dvs:
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

DCM păstrează în mod normal o copie de siguranţă a datelor utilizator pe care le salvaţi în fişierele ale căror nume sunt în conflict cu cele folosite de DCM. Dacă următoarele fişiere nu există:

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

Dacă acestea există:

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

Apoi, sistemul încearcă să le redenumească, adăugând extensia .OLD. Dacă şi aceste fişiere există, sistemul nu crează copii de siguranţă. În schimb, şterge fişierele .STH.

Diverse

Dacă încercările dvs. de a crea o CA şi un certificat sistem continuă să eşueze datorită conflictelor legate de nume, puteţi întâlni una din următoarele:

- **Conflict de nume fişiere diferite** – DCM încearcă să protejeze datele utilizator din directoarele pe care le crează, chiar dacă acele fişiere împiedică DCM să creeze fişierele de care are nevoie. Rezolvaţi această problemă copiind toate fişierele ce provoacă conflictul în alt director şi, dacă este posibil, folosiţi funcţii DCM pentru a şterge fişierele corespunzătoare. Dacă nu puteţi folosi DCM pentru a realiza aceasta, ştergeţi manual fişierele din directorul original integrat în sistemul de fişiere unde acestea se află în conflict cu DCM. Asiguraţi-vă că aţi înregistrat exact ce fişiere le mutaţi şi unde le-aţi mutat. Aceste copii vă permit să recuperaţi fişierele dacă veţi mai avea nevoie de ele. Va trebui să creaţi o nouă CA după mutarea acestor fişiere:

```
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT
```

Va trebui să creaţi un nou depozit de certificate *SYSTEM şi certificat sistem după ce aţi mutat următoarele fişiere:

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

- **Precerinţe lipsă** – Asiguraţi-vă că aţi instalat corect LPP-urile (programele licenţiate necesare înainte) necesare.
- **Problemă de cod** – Contactaţi reprezentantul dvs. pentru service.

Depanarea asignării unui certificat utilizator

Când folosiţi taskul **Asignarea unui certificat utilizator**, Digital Certificate Manager (DCM) afişează informaţii despre certificat ca dumneavoastră să le aprobaţi înainte de a înregistra certificatul. Dacă DCM nu poate afişa certificatul, problema poate fi una din următoarele:

1. Browserul nu a cerut să se selecteze un certificat pentru a fi prezentat serverului. Aceasta poate apare dacă browserul a memorat un certificat anterior (din accesarea unui alt server). Se poate încerca ştergerea memoriei browserului şi apoi executarea din nou a procesului. Browserul ar trebui să vă ceară selectarea unui certificat.
2. Certificatul care se doreşte a fi înregistrat este deja înregistrat cu DCM.
3. Autoritatea de certificat care a emis certificatul, nu este desemnată ca root de încredere în sisitem. De aceea certificatul pe care îl prezentaţi nu este este nevalid. Contactaţi-vă administratorul de sistem pentru a determina dacă CA care a emis certificatul este corect. Dacă CA este corectă, administratorul de sistem ar putea avea nevoie să **Importe** certificatul CA în depozitul de certificate *SYSTEM. Sau, este posibil ca administratorul să aibă nevoie să folosească taskul **Gestionare certificatele CA** pentru a activa CA ca o rădăcină de încredere pe sistem pentru a corecta problema.

4. Nu există un certificat pentru înregistrare. Se pot verifica certificatele client în browser pentru a vedea dacă este vreo problemă.
5. Certificatul care se doreşte a fi înregistrat este expirat sau incomplet. Trebuie fie să reînnoiţi certificatul sau să contactaţi CA care la emis, în vederea rezolvării problemei.
6. IBM Serverul HTTP pentru iSeries nu este setat corect pentru a face înregistrări de certificate folosind SSL şi autentificare client pe instanţa securizată a serverului *ADMIN. Dacă nu funcţionează nici unul dintre sfaturile de depanare propuse, contactaţi administratorul de sistem pentru a raporta problema.

Pentru a **Atribui un certificat utilizator**, trebuie să vă conectaţi la un DCM (administrator de certificate digitale) folosind o sesiune SSL. Dacă nu folosiţi SSL când selectaţi task-ul **Atribuirea unui certificat utilizator**, DCM va afişa un mesaj în care vă va spune că trebuie să folosiţi SSL. Acest mesaj este însoţit de un buton prin care se poate face conectarea la DCM folosind SSL. Dacă butonul respectiv nu apare, informaţi administratorul în legătură cu această problemă. Server-ul Web ar trebui să fie repornit pentru a se confirma dacă directivele de configurare pentru folosirea SSL sunt activate.

Capitol 10. Informaţii înrudite pentru DCM

Cum folosirea certificatelor digitale a devenit mai răspândită, resursele informaţionale au devenit de asemenea mai disponibile. Iată o listă scurtă cu alte resurse pe care le puteţi trece în revistă pentru a afla mai multe despre certificate digitale şi despre cum le puteţi folosi pentru a vă extinde politica de securitate iSeries:

- **VeriSign Help Desk web site**
  Site-ul de web VeriSign oferă o librărie extensibilă de articole despre certificatele digitale, ca şi un număr de alte subiecte legate de securitatea pe Internet.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM şi Îmbunătăţiri Criptografice SG24-6168**
  Această IBM carte roşie se concentrează asupra îmbunătăţirilor securităţii în reţea din V5R1. Cartea acoperă multe subiecte incluzând cum se folosesc capabilităţile iSeries de semnare a obiectelor, Digital Certificate Manager (DCM), suportul pentru SSL al Coprocesorului Criptografic 4758 ş.a.m.d.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  Această carte descrie ce puteţi face cu certificatele digitale pe un server iSeries. Explică cum se setează diferitele servere şi clienţi care folosesc certificate. Mai departe oferă informaţii şi exemple de cod sursă despre cum să folosiţi API-urile OS/400 pentru a administra şi folosi certificate digitale în aplicaţii utilizator.
- **Căutare în Indexul RFC-urilor**
  Acest site web oferă un depozit al Cererilor pentru Comentarii (Request for Comments - RFC). RFC-urile descriu standardele pentru protocoale Internet, cum ar fi SSL, PKIX şi altele care sunt înrudite cu folosirea certificatelor digitale.

Tipărit în S.U.A.