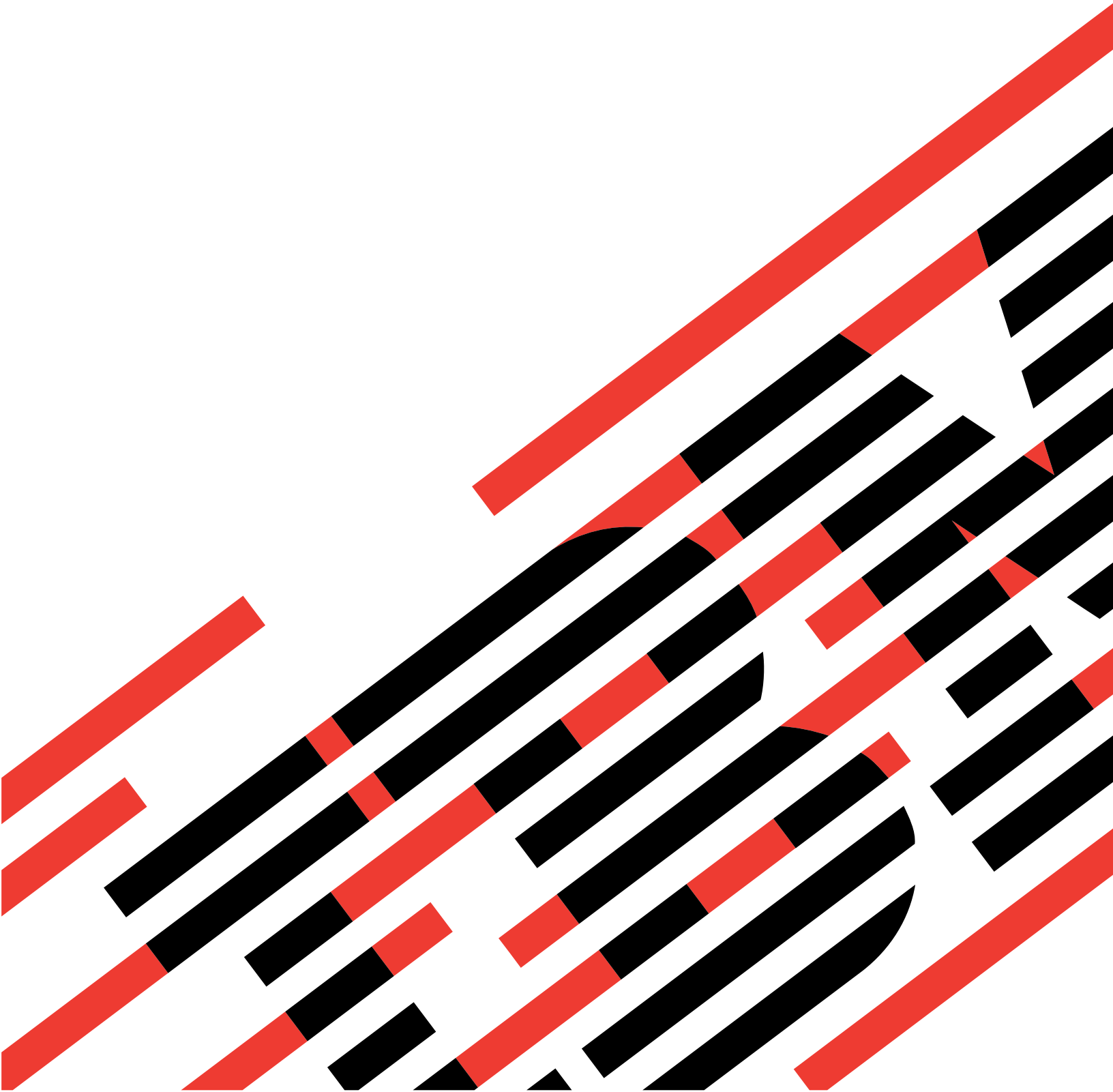
IBM

eserver

iSeries

Digital Certificate Manager

Versiunea 5 ediţia 3



IBM

@server

iSeries

Digital Certificate Manager

Versiunea 5 ediţia 3

Notă

Înainte de a folosi aceste informaţii şi produsul pe care îl suportă, asiguraţi-vă că aţi citit informaţiile din “Observaţii”, la pagina 93.

Ediţia a opta (august, 2005)

Această ediţie este valabilă pentru IBM Operating System/400 (număr produs 5722–SS1) versiunea 5, ediţia 3, modificarea 0 şi pentru toate ediţiile şi modificările ulterioare, până când se specifică altfel în noile ediţii. Această versiune nu rulează pe toate modelele de calculatoare RISC şi nici pe modelele CISC.

Cuprins

Capitolul 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 internetul. SSL oferă una dintre cele mai bune soluţii pentru protecţia în Internet a caracterului privat al datelor sensibile, cum ar fi numele de utilizator şi parolele. Multe servicii şi aplicaţii, cum ar fi FTP, Telnet, HTTP Server pentru iSeries şi multe altele, oferă suport SSL pentru a asigura protecţia datelor.

IBM asigură un suport extins pentru certificatele digitale, care vă permite să folosiţi certificate digitale drept acreditări în mai multe 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.

DCM (Digital Certificate Manager), o caracteristică gratuită, vă simplifică folosirea suportului pentru certificate, permiţându-vă să gestionaţi centralizat certificatele pentru aplicaţiile dumneavoastră. DCM vă permite să gestionaţi certificatele 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. Aţi putea să treceţi în revistă aceste subiecte pentru a învăţa mai multe despre modul în care funcţionează certificatele şi cum puteţi folosi DCM pentru a gestiona certificatele şi aplicaţiile care le folosesc:

Ce este nou pentru V5R3
Folosiţi aceste informaţii pentru a învăţa despre îmbunătăţirile şi modificările subiectului informaţii ale Digiral Certificate Manager pentru această ediţie.

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

Scenarii DCM
Folosiţi aceste informaţii pentru a examina 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. Fiecare scenariu furnizează de asemenea toate task-urile 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 aceaste informaţii pentru a vă ajuta să decideţi cum şi când aţi putea utiliza certificate digitale pentru a vă îndeplini ţelurile de securitate. Folosiţi aceste informaţii 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 aceste informaţii 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.

Capitolul 2. Ce este nou pentru V5R3

Printre îmbunătăţirile pe care le oferă V5R3 pentru DCM (Digital Certificate Manager) şi capabilităţile certificatelor digitale se numără:

- **Gestionare locaţie LDAP**
  Noul task Gestionare locaţie LDAP în task-ul DCM vă permite să memoraţi certificatele utilizator pe care le emite CA-ul local într-o locaţie LDAP (Lightweight Directory Access Protocol). Când configuraţi DCM să utilizeze această opţiune, puteţi folosi certificatele utilizator care sunt memorate în această locaţie LDAP cu EIM (Enterprise Identity Mapping). Accesaţi acest task din meniul de navigaţie principal al DCM.
- **Asignare îmbunătăţiri task unui certificat utilizator pentru EIM**
  Când configuraţi DCM să lucreze cu EIM (Enterprise Identity Mapping), task-ul Asignare certificat utilizator memorează certificatele asignate într-o locaţie LDAP (Lightweight Directory Access Protocol) mai degrabă decât cu un profil utilizator. Cum tratează DCM asignarea certificatelor depinde dacă aveţi configurat DCM să utilizeze o locaţie LDAP (Lightweight Directory Access Protocol) pentru a memora certificate în conjuncţie cu utilizarea EIM (Enterprise Identity Mapping).
- **Verificare expirare certificate**
  Această nouă funcţie vă permite să vedeţi şi să gestionaţi rapid şi uşor certificate pe baza datei de expirare a certificatului. Puteţi verifica expirarea certificatelor pentru certificatele server sau client şi pentru certificatele de semnare a obiectului pe sistemul local. De asemenea, puteţi verifica expirarea certificatelor utilizator. Puteţi verifica expirarea certificatului utilizator fie pentru un profil utilizator specific, fie pentru toate certificatele utilizator din sistem, fie pentru toate certificatele utilizator într-o întreprindere când EIM este configurat pe sistem.

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

Cum să vedeţi ce este nou sau modificat

Pentru a vă ajuta să vedeţi unde au fost făcute modificări tehnice, aceste informaţii folosesc:

- Imaginea » de marcat unde încep informaţiile noi sau modificate.
- Imaginea « de marcat unde se termină informaţiile noi sau modificate.

Capitolul 3. Tipărirea acestui articol

Pentru a vedea sau descărca versiunea PDF a acestui subiect, selectaţi Digital Certificate Manager  (dimensiunea fişierului este de aporximativ 600 KB sau aproximativ 116 pagini).

Salvare fişiere PDF:

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

1. Faceţi clic dreapta pe PDF în browser-ul dumneavoastră (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe **Save Target As...** dacă folosiţi Internet Explorer. Faceţi clic pe **Save Link As...** dacă folosiţi Netscape Communicator.
3. Navigaţi în directorul în care doriţi să salvaţi fişierul PDF.
4. Selectaţi **Save**.

Descărcare Adobe Acrobat Reader

Aveţi nevoie de Adobe Acrobat Reader pentru a vedea sau tipări aceste PDF-uri. Puteţi descărca o copie de la situl Web al Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Capitolul 4. Scenarii DCM

DCM (Digital Certificate Manager) şi suportul sistemului pentru certificate digitale vă permit să folosiţi certificate pentru a vă îmbunătăţi politica de securitate în mai multe feluri. Alegerea modului în care folosiţi certificatele depinde atât de obiectivele dumneavoastră de afaceri, cât şi de nevoile dumneavoastră 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, în funcţie de cum configuraţi DCM, puteţi folosi DCM pentru a asocia un certificat de utilizator profilului său de utilizator sau identificatorului EIM (Enterprise Identity Mapping). Certificatul apoi are aceleaşi autorizări şi permisiuni ca profilul utilizator asociat.

În consecinţă, cum alegeţi să folosiţi certificatele poate fi complicat şi depinde de o multitudine de factori. Scenariile furnizate în acest subiect descriu unele din cele mai comune obiective de securitate cu certificate digitale pentru comunicaţii sigure în contextele tipice de afaceri. Fiecare scenariu descrie de asemenea toate cerinţele de sistem şi software preliminare necesare şi toate task-urile de configurare pe care trebuie să le realizaţi pentru a implementa scenariul. **Notă:** Vedeţi Scenarii semnare obiect în Centrul de informare iSeries pentru exemple detaliate despre cum să folosiţi certificate digitale pentru a semna obiecte pentru a le proteja integritatea.

Citiţi aceste scenarii pentru a vă ajuta să determinaţi în ce fel folosirea certificatelor pentru securitate se potriveşte mai bine nevoilor dumneavoastră:

Scenariu: Folosire certificate pentru autentificare externă
Acest scenariu descrie când şi cum să folosiţi certificate ca un mecanism de autentificare pentru a proteja şi a limita accesul utilizatorilor publici la resurse publice sau din afara reţelei şi la aplicaţii.

Scenariu: Folosire certificate pentru autentificare internă
Acest scenariu descrie când şi cum să folosiţi certificate ca un mecanism de autentificare pentru a proteja şi a restricţiona care resurse şi aplicaţii pot fi accesate din serverele interne.

Scenariu: Folosire certificate pentru autentificare externă

Situaţie

Lucraţi pentru compania de asigurări MyCo, Inc şi sunteţi responsabil pentru menţinerea diferitelor aplicaţii de pe siturile reţelei interne şi externe a companiei dumneavoastră. O anumită aplicaţie pentru care sunteţi responsabil este o aplicaţie de calculare a ratelor de asigurare 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, vreţi să furnizaţi în final o metodă mai sigură de autentificare utilizator la aplicaţie decât metoda curentă cu nume utilizator şi parolă. Sunteţi îngrijorat suplimentar că utilizatori neautorizaţi ar putea captura aceste informaţii când sunt transmise printr-o reţea în care nu aveţi încredere. De asemenea, sunteţi îngrijorat că diferiţi agenţi ar putea împărţi aceste informaţii cu fiecare care nu are autorizare să facă asta.

După unele cercetări, decideţi că folosirea certificatelor digitale vă poate oferi securitatea de care aveţi nevoie pentru a proteja informaţiile sensibile întroduse în şi extrase din această aplicaţie. Folosirea certificatelor vă permite să folosiţi SSL (Secure Sockets Layer) pentru a proteja transmisia datelor 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 dumneavoastră să aibă nevoie de ceva timp înainte ca acest scop să fie realizat. În plus la folosirea autentificării client prin certificat, plănuiţi să continuaţi folosirea curentă a autentificării prin nume utilizator şi parolă deoarece SSL protejează intimitatea acestor date sensibile la transmisie.

Pe baza tipului de aplicaţie şi a utilizatorilor ei şi a scopului dumneavoastră viitor de autentificare a certificatelor pentru toţi utilizatorii, decideţi să folosiţi un certificat public de la un CA binecunoscut pentru a configura SSL pentru aplicaţia dumneavoastră.

Avantajele scenariului

Acest scenariu are următoarele avantaje:
- Folosirea certificatelor digitale pentru a configura accesul SSL la aplicaţia dumneavoastră 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 unde folosirea certificatelor digitale nu este posibilă, autentificarea client prin intermediul autentificării cu nume utilizator şi parolă este protejată şi menţinută privată de către sesiunea SSL, făcând schimbul de astfel de date sensibile mai sigur.
- Folosirea certificatelor digitale *publice* pentru a autentifica utilizatori la aplicaţiile şi datele dumneavoastră în maniera pe care o descrie acest scenariu este o alegere practică pentru aceste condiţii sau unele similare:
  - Datele şi aplicaţiile dumneavoastră 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 sit Web Internet sau o aplicaţie din afara reţelei.
  - Nu vreţi să operaţi propria Autoritate de certificare (CA) pe baza motivelor administrative, cum ar fi un număr mare de utilizatori din afară care vă accesează aplicaţiile şi resursele.
- Folosirea unui certificat public pentru a configura aplicaţia de calculare rate pentru SSL din acest scenariu scade cantitatea de configurare pe care utilizatorii trebuie să o realizeze pentru a accesa aplicaţia sigur. Majoritatea software-ului client conţine certificate CA pentru majoritatea CA-urilor binecunoscute.

Obiective

În acest scenariu, MyCo, Inc. vrea să folosească certificate digitale pentru a proteja informaţiile de calculare rată pe care aplicaţia lor o furnizează utilzatorilor publici autorizaţi. Compania vrea de asemenea o metodă mai sigură de autentificare a acelor utilizatori cărora le este permis să acceseze această aplicaţie când este posibil.

Obiectivele acestui scenariu sunt următoarele:
- Aplicaţia de calculare a ratei publice a companiei trebuie să folosească SSL pentru a proteja izolarea datelor pe care le furnizează şi le primesc de la utilizatori.
- Configurarea SSL trebuie realizată cu certificate publice de la un CA public binecunoscut din Internet.
- 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 să prezinte fie un certificat digital public de la un CA binecunoscut, fie un nume de utilizator şi o parolă valide, în cazul în care certificatul nu este disponibil.

Detalii

Următoarea figură ilustrează configuraţia reţelei în acest scenariu:

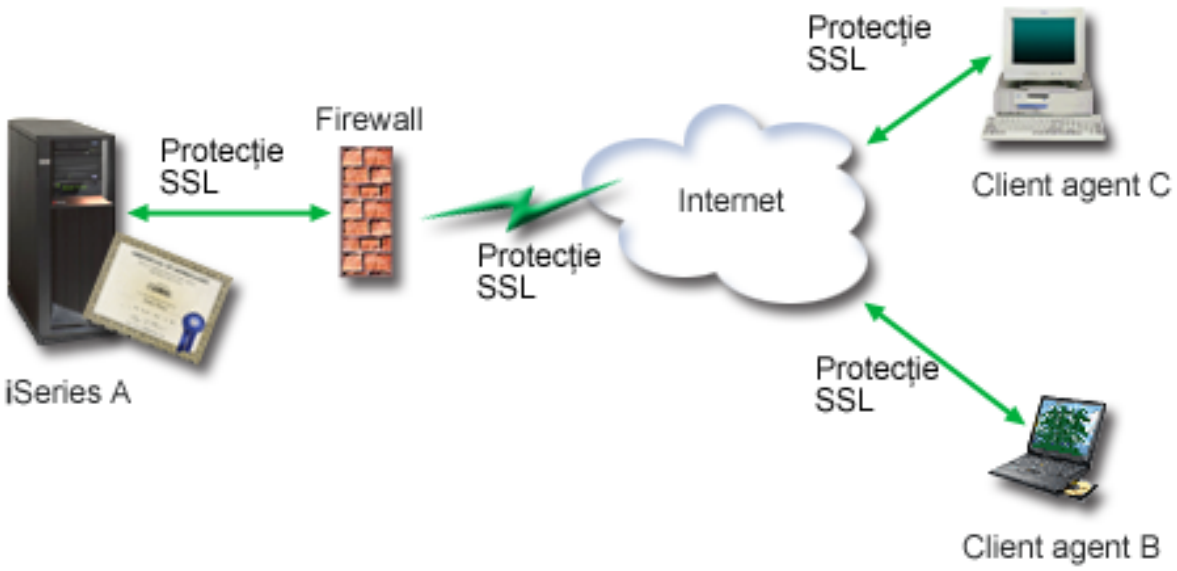


Figura ilustrează următoarele informaţii despre situaţia pentru acest scenariu:

Serverul public al companiei – A
- Serverul A este serverul care găzduieşte aplicaţia companiei de calculare a ratei.
- Pe Serverul A rulează OS/400 Versiunea 5 Ediţia 2 (V5R2) sau mai recentă.
- Serverul A are instalat un furnizor de acces criptografic (5722–AC3).
- Pe Serverul A sunt instalate şi configurate Digital Certificate Manager (OS/400 opţiunea 34) şi IBM HTTP Server pentru iSeries (5722–DG1).
- Serverul A rulează aplicaţia de calculare a ratei, care este configurată în aşa fel încât:
  - Necesită modul SSL.
  - Foloseşte un certificat public de la un CA binecunoscut pentru a se autentifica pe sine pentru a iniţializa o sesiune SSL.
  - Necesită autentificarea utilizatorului prin nume utilizator şi parolă.
- Serverul A îşi prezintă certificatul pentru a iniţia o sesiune SSL când clienţii B şi C accesează aplicaţia de calculare a ratei.
- După iniţializarea sesiunii SSL, Serverul A cere clienţilor B şi C să furnizeze un nume de utilizator şi o parolă valide înainte de a permite accesul la aplicaţia de calculare a ratei.

Sistemele client agent – Client B şi Client C
- Clienţii B şi C sunt agenţi independenţi care accesează aplicaţia de calcul a ratei.
- Software-ul client al clienţilor B şi C are o copie instalată a certificatului CA binecunoscut care a emis certificatul aplicaţiei.
- Clienţii B şi C accesează aplicaţia de calculare a ratei de pe Serverul A, care îşi prezintă certificatul către software-ul de client pentru autentificarea identităţii sale şi iniţierea unei sesiuni SSL.
- Software-ul client de pe Clientul B şi Clientul C este configurat să accepte certificatul de la Serverul A pentru iniţializarea unei sesiuni SSL.
- După ce începe sesiunea SSL, clienţii B şi C trebuie să furnizeze un de nume utilizator şi o parolă valide pentru ca Serverul A să le acorde acces la aplicaţie.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:
1. Aplicaţia de calculare a ratei de pe Serverul A este o aplicaţie generică, ce poate fi configurată să folosească SSL. Cele mai multe aplicaţii, inclusiv multe aplicaţii server, asigură suportul 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 calculare rată 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 DCM (Digital Certificate Manager) pentru a configura încrederea în certificate pentru acele aplicaţii care oferă 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. Serverul A îndeplineşte cerinţele pentru instalarea şi folosirea DCM (Digital Certificate Manager).
4. Nimeni nu a configurat sau folosit anterior DCM pe Serverul A.
5. Oricine foloseşte DCM pentru a realiza task-urile din acest scenariu trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilurile lor de utilizator.
6. Pe Serverul A nu este instalat IBM Cryptographic Coprocessor.

Paşi de configurare

Pentru a implementa acest scenariu, trebuie să executaţi aceste task-uri pe Serverul A:

1. Finalizaţi foile de lucru pentru planificare
2. Finalizaţi toţi paşii preliminari pentru instalarea şi configurarea tuturor produselor necesare
3. Folosiţi DCM (Digital Certificate Manager) pentru a crea o cerere de certificat de la server
4. Configuraţi aplicaţia să folosească SSL (Secure Sockets Layer)
5. Folosiţi DCM pentru a importa şi asigna serverul semnat sau certificatul client ID-ului aplicaţiei dumneavoastră
6. Porniţi aplicaţia în mod SSL, dacă este necesar
7. **Opţional**. Folosiţi DCM pentru a defini o listă de CA-uri de încredere pentru a activa autentificarea client pe baza certificatelor pentru aplicaţii care furnizează acest suport

Notă: Situaţia pe care o descrie acest scnearіu nu necesită ca aplicaţia de calculare rată să folosească certificate pentru autentificarea clientului. 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 task-ului pentru a folosi certificatele pentru configurarea accesului public protejat la aplicaţii şi resurse după cum descrie acest scenariu.

Pasul 1: Completaţi foile de lucru de planificare

Următoarele foi de lucru demonstrează informaţiile pe care trebuie să le adunaţi şi deciziile pe care este nevoie să le faceţi pentru a pregăti implementarea certificatelor digitale pe care o descrie acest scenariu. Pentru a asigura o implementare cu succes, este nevoie să fiţi capabil să răspundeţi Da la toate elementele de cerinţe preliminare şi aveţi nevoie să aveţi adunate toate informaţiile cerute înainte să realizaţi orice task de configurare.

Tabela 1. Foaie de lucru de planificare a cerinţelor preliminare de implementare certificat

Foaie de lucru cerinţe preliminare	Răspunsuri
Versiunea dumneavoastră de OS/400 este V5R2 (5722-SS1) sau mai mare?	Da
Este instalat pe sistem Cryptographic Access Provider (5722-AC3)?	Da
Este instalată pe sistemul dumneavoastră opţiunea 34 a OS/400?	Da

Tabela 1. Foaie de lucru de planificare a cerinţelor preliminare de implementare certificat (continuare)

Foaie de lucru cerinţe preliminare	Răspunsuri
Este instalat serverul HTTP IBM pentru iSeries (5722–DG1) pe sistemul dumneavoastră şi este pornită instanţa de server pentru administrare?	Da
Este configurat TCP pentru sistemul dumneavoastră astfel încât să puteţi folosi un browser Web şi instanţa de server Administrative a serverului HTTP pentru a accesa DCM?	Da
Aveţi autorizările speciale *SECADM şi *ALLOBJ?	Da

Trebuie să adunaţi următoarele informaţii despre implementarea dumneavoastră de certificate digitale pentru a realiza task-urile necesare de configurare pentru a termina implementarea:

Tabela 2. Foaie de lucru de planificare a configuraţiei de implementare certificat

Foaie de lucru de planificare pentru Serverul A	Răspunsuri
Veţi opera propria dumneavoastră CA locacă sau veţi obţine certificate pentru aplicaţia dumneavoastră de la un CA public?	Obţineţi certificate de la un CA public
Serverul A găzduieşte aplicaţia pe care vreţi să o activaţi pentru SSL?	Da
Ce informaţii despre nume distinctiv veţi folosi pentru cererea de semnare certificat (CSR) pe care o creaţi cu DCM? • **Dimensiune cheie**: determină puterea cheilor criptografice pentru certificat. • **Etichetă certificat**: identifică certificatul cu un şir unic de caractere. • **Nume comun**: identifică proprietarul certificatului, cum ar fi o persoană, entitate sau aplicaţie; parte a DN-ului subiect pentru certificat. • **Unitate organizaţie**: identifică secţiunea sau zona de organizare pentru aplicaţia care va folosi acest certificat. • **Nume organizaţie**: identifică compania dumneavoastră sau secţiunea divizională pentru aplicaţia care va folosi acest certificat. • **Localitate sau oraş**: identifică oraşul sau o desemnare a localităţii pentru organizaţia dumneavoastră. • **Stat sau provincie**: identifică statul sau provincia în care veţi folosi acest certificat. • **Ţară sau regiune**: identifică, cu o desemnare din două litere, ţara sau regiunea în care veţi folosi acest certificat.	**Dimensiune cheie**: 1024 **Etichetă certificat**: Myco_public_cert **Nume comun**: myco_rate_server@myco.com **Unitate organizaţie**: Rate dept **Nume organizaţie**: myco **Localitate sau oraş**: Orice_oraş **Stat sau provincie**: Orice **Ţară sau regiune**: ZZ
Care este ID-ul aplicaţiei DCM pentru aplicaţia pe care vreţi să o configuraţi să folosească SSL?	mcyo_agent_rate_app
Veţi configura aplicaţia cu SSL aplicat să folosească certificate pentru autentificarea client? Dacă da, care CA-uri vreţi să le adăugaţi la lista de CA-uri de încredere a aplicaţiei?	Nu

Pasul 2: Finalizarea task-urilor preliminare pentru a instala toate produsele necesare

Trebuie să finalizaţi toate task-urile preliminare pentru a instala şi configura toate produsele necesare înainte de a putea executa orice task de configurare specific pentru implementarea acestui scenariu.

Pasul 3: Crearea unei cereri de certificate 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 public pentru emiterea unui certificat.

Pentru a începe procesul de obţinere a certificatului dumneavoastră, 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 (Certificate Signing Request) sunt constituite din cheia publică, numele distinctiv şi alte informaţii pe care le-aţi specificat pentru certificatul nou.
7. Copiaţi cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fişier separat, pe care îl cere CA public pentru cererea unui certificat. Trebuie să folosiţi toate datele CSR, inclusiv liniile Begin şi End New Certificate Request. **Notă:** Când ieşiţi din această pagina, datele sunt pierdute şi nu le puteţi 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 task-ului pentru scenariu.

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

Pasul 4: Configurare aplicaţie să folosească SSL

Când vă primiţi înapoi certificatul semnat de la CA public, puteţi continua procesul de actviare a comunicaţiilor SSL pentru aplicaţia dumneavoastră publică. Trebuie să configuraţi aplicaţia să folosească SSL înainte să lucreze cu certificatele dumneavoastră semnate. Unele aplicaţii, cum ar fi serverul HTTP pentru iSeries generează un ID aplicaţie unic şi îl înregistrează cu DCM (Digital Certificate Manager) când configuraţi aplicaţia să folosească SSL. Trebuie să ştiţi ID-ul aplicaţiei înainte de a putea folosi DCM pentru a asigna la ea certificatul dumneavoastră semnat şi să terminaţi procesul de configurare SSL.

Cum vă configuraţi aplicaţia să folosească SSL depinde de aplicaţie. Acest scenariu nu presupune o sursă specifică pentru aplicaţia de calculare rată pe care o descrie deoarece sunt un număr de căi prin care MyCo, Inc. ar putea furniza această aplicaţie agenţilor săi.

| Pentru a vă configura aplicaţia să folosească SSL, urmaţi instrucţiunile pe care le furnizează documentaţia aplicaţiei
| dumneavoastră. De asemenea, puteţi învăţa mai multe despre configurarea multor aplicaţii IBM comune să folosească
| SSL prin revederea SSL (Secure Sockets Layer) din Centrul de informare iSeries.

| Când terminaţi configurarea SSL pentru aplicaţia dumneavoastră, puteţi configura certificatul public semnat pentru
| aplicaţie astfel încât să poată iniţializa sesiuni SSL.

Pasul 5: Importare şi asignare certificat public semnat

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

Pentru a importa şi asigna certificatul dumneavoastră către aplicaţia dumneavoastră 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 este afişată pagina **Depozit de certificate şi parolă**, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi faceţi clic pe **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 task-uri **Gestionare certificate** pentru a afişa o listă de certificate pentru depozitul de certificate curent.
7. Selectaţi certificatul dumneavoastră din listă şi faceţi clic pe **Asignare la aplicaţii** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate curent.
8. Selectaţi aplicaţia dumneavoastră din listă şi apăsaţi **Continuare** . Apare o pagină fie cu un mesaj de confirmare pentru selecţia dumneavoastră de asignare fie cu un mesaj de eroare dacă a apărut o problemă.

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

Pasul 6: Pornire aplicaţie în mod SSL

După ce terminaţi procesul de importare şi asignare a certificatului către aplicaţia dumneavoastră, s-ar putea să trebuiască să terminaţi şi să reporniţi aplicaţia în modul SSL. Acest lucru este 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 dumneavoastră pentru a determina dacă aveţi nevoie să restartaţi aplicaţia sau pentru alte informaţii despre pornirea aplicaţiei în modul SSL.

| Dacă vreţi să folosiţi certificate pentru autentificarea clientului, puteţi defini acum o listă de CA-uri de încredere pentru
| aplicaţie.

Pasul 7 (Opţional): Definire listă de CA-uri de încredere pentru o aplicaţie care necesită certificate pentru autentificarea clientului

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 calculare rată să folosească certificate pentru
| autentificarea client, dar aplicaţia va fi capabilă să accepte certificate pentru autentificare atunci când sunt disponibile.
| Multe aplicaţii furnizează suport pentru certificate de autentificare client; cum configuraţi acest suport variază mult în
| cadrul aplicaţiilor. 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 un 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 dumneavoastră, 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 este afişată pagina **Depozit de certificate şi parolă**, furnizaţi parola pe care aţi specificat-o pentru depozitul de certificate când l-aţi creat şi faceţi clic pe **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 unul sau mai multe certificate CA din lista în care aplicaţia dumneavoastră va avea încredere şi faceţi clic pe **Activare** pentru a afişa o listă a aplicaţiilor care folosesc o listă de CA-uri de încredere.
7. Selectaţi aplicaţia din listă care are nevoie să adauge CA selectată la lista ei de încredere şi faceţi clic pe **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 dumneavoastră.

Scenariu: Folosire certificate pentru autentificare internă

Situaţie

Sunteţi administrator 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 sit Web intern pentru a furniza aceste informaţii angajaţilor. Sunteţi responsabil pentru administrarea acestui sit Web intern, care rulează pe IBM HTTP Server pentru iSeries (motorizat de Apache).

Deoarece angajaţii sunt situaţi în două birouri separate geografic şi unii angajaţi călătoresc frecvent, dumneavoastră sunteţi preocupat de păstrarea acestor informaţii private la transportul lor prin Internet. De asemenea, autentificaţi suplimentar utilizatorii prin intermediul unui nume utilizator şi parolă pentru a limita accesul la datele companiei. Din cauza naturii sensibile şi private a acestor date, realizaţi că limitarea accesului la ele pe baza autentificării prin parolă s-ar putea să nu fie suficientă. La urma urmei, oamenii pot partaja, pot uita şi chiar fura parole.

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. 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.

Ca urmare, decideţi să setaţi un CA local şi să emiteţi certificate pentru toţi angajaţii şi să asociaţi certificatele tuturor angajaţilor cu profilurile de utilizator. 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 dumneavoastră 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 certificatelor digitale pentru a configura accesul SSL la serverul Web de resurse umane asigură că informaţiile transmise între server şi client sunt protejate şi private.
- Folosirea de certificate digitale pentru autentificarea clienţilor furnizează o metodă mai sigură de identificare a utilizatorilor autorizaţi.
- Folosirea certificatelor digitale *publice* pentru a autentifica utilizatori la aplicaţiile şi datele dumneavoastră este o alegere practică pentru aceste condiţii sau unele 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 dumneavostră au deja profiluri de utilizator care le controlează accesul la aplicaţii şi date.
  - Doriţi să operaţi asupra propriului Certificate Authority (CA).
- Folosirea certificatelor private pentru autentificarea client vă permite să asociaţi mai uşor certificatul cu profilul de utilizator 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 se poate schimba pe el şi poate să ruleze sub acel profil utilizator sau să realizeze acţiuni pentru a acel utilizator pe baza informaţiile din profilul utilizator.

Obiective

În acest scenariu, MyCo, Inc. vrea să folosească certificate digitale pentru a proteja informaţiile sensibile despre personal pe care situl lor Web intern de resurse umane le furnizează angajaţilor. Compania vrea de asemenea o metodă mai sigură de autentificare a acelor utilizatori cărora le este permis să acceseze acest sit Web.

Obiectivele acestui scenariu sunt următoarele:
- Situl Web intern de resurse umane trebuie să utilizeze SSL pentru a proteja izolarea datelor pe care le oferă utilizatorilor.
- Configurarea SSL trebuie să fie realizată cu certificate private de la un CA local intern.
- Utilizatorii autorizaţi trebuie să ofere un certificat valid pentru a accesa situl Web de resurse umane în mod SSL.

Detalii

Următoarea figură ilustrează configuraţia reţelei pentru acest scenariu:

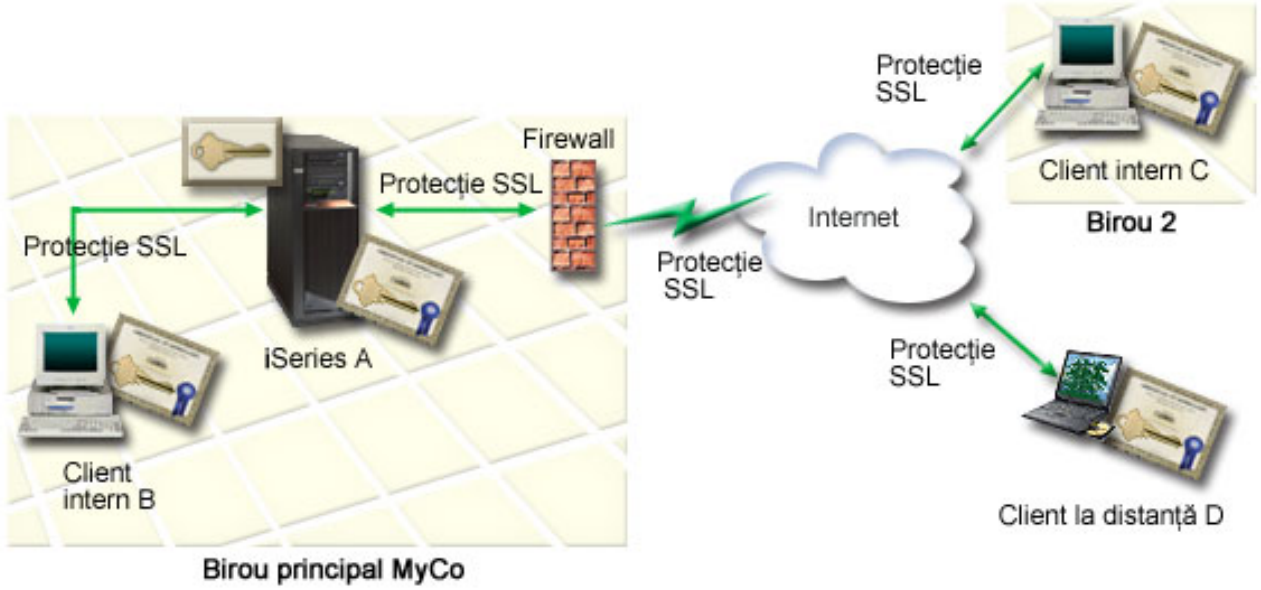


Figura ilustrează următoarele informaţii despre situaţia pentru acest scenariu:

Serverul de Web pentru resursele umane ale companiei – Serverul A
- Serverul A este serverul care găzduieşte aplicaţia de resurse umane bazată pe Web.
- Pe Serverul A rulează OS/400 Versiunea 5 Ediţia 2 (V5R2) sau o versiune ulterioară.

- Serverul A are instalat furnizorul de acces criptografic (5722–AC3).
- Pe Serverul A sunt instalate şi configurate Digital Certificate Manager (OS/400 opţiunea 34) şi IBM HTTP Server pentru iSeries (5722–DG1).
- Serverul A rulează aplicaţia de resurse umane, care este configurată în aşa fel încât:
  - Necesită modul SSL.
  - Foloseşte un certificat privat de la un CA binecunoscut pentru configurarea SSL.
  - Necesită certificate pentru autentificarea clienţilor.
- Serverul A îşi prezintă certificatul pentru a iniţia o sesiune SSL atunci când clienţii B, C şi D accesează aplicaţia.
- După iniţializarea sesiunii SSL, Serverul A cere clienţilor 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
- Clientul B este un angajat care lucrează în biroul principal al companiei MyCo, unde se află Serverul A.
- Clientul C este un angajat care lucrează în biroul secundar din MyCo, care este separat geografic de biroul principal.
- Clientul D este un angajat care lucrează la distanţă şi călătoreşte frecvent pentru afacerile companieie şi trebuie să fie în stare să acceseze în siguranţă situl 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 Serverul A, care îşi prezintă certificatul software-ului 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 Serverul A şi începe sesiunea SSL.
- După ce începe sesiunea SSL, clienţii B, C şi D trebuie să furnizeze un certificat valid înainte ca Serverul A să le acorde acces la aplicaţie şi la resursele sale.

Cerinţe preliminare şi supoziţii

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:
1. IBM HTTP Server pentru iSeries (motorizat de Apache) rulează aplicaţia de resurse umane pe Serverul A. Acest scenariu nu furnizează instrucţiuni *specifice* pentru a configura serverul HTTP Server 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 folosirea DCM (Digital Certificate Manager) pentru a configura cerinţele de gestionare certificat 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 Serverul A foloseşte deja autentificarea prin parolă.
4. Serverul A îndeplineşte cerinţele pentru instalarea şi folosirea DCM (Digital Certificate Manager).
5. Nimeni nu a configurat sau folosit anterior DCM pe Serverul A.
6. Oricine foloseşte DCM pentru a realiza task-urile din acest scenariu trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilurile lor de utilizator.
7. Pe Serverul A nu este instalat IBM Cryptographic Coprocessor.

Paşi de configurare

Sunt două seturi de task-uri pe care trebuie să le efecuaţi pentru a implementa acest scenariu: Un set vă permite să setaţi aplicaţia de resurse umane pe Serverul A astfel încât să folosească SSL şi să ceară certificate pentru autentificarea utilizatorului. Celălalt set de task-uri permite utilizatorilor dumneavoastră de pe Clienţii B, C şi D să participe în sesiunile SSL cu aplicaţia de resurse umane şi să obţină certificate pentru autentificarea utilizatorilor.

Paşi ai task-ului aplicaţie server Web de resurse umane

Pentru a implementa acest scenariu, trebuie să executaţi aceste task-uri pe Serverul A:
1. Completaţi foile de lucru de planificare a scenariului

2. Finalizaţi toţi paşii preliminari pentru instalarea şi configurarea tuturor produselor necesare
3. Configuraţi serverul HTTP de resurse umane să folosească SSL şi notaţi ID-ului aplicaţiei pentru instanţa server
4. Folosiţi DCM (Digital Certificate Manager) pentru a crea şi opera un CA local
5. Configuraţi autentificarea client pentru serverul Web de resurse umane.
6. Porniţi serverul HTTP de resurse umane în mod SSL .

Paşii task-ului de configurare a clientului

Pentru a implementa acest scenariu, fiecare client (clienţii B, C şi D) care va accesa serverul Web de resurse umane de pe Serverul A trebuie să realizeze aceste task-uri:
7. Să instaleze o copie a certificatului CA local în browser
8. Să ceară un certificat de la CA-ul local

Detalii de configurare

Efectuaţi următorii paşi ai task-ului pentru a folosi certificatele pentru a configura acces SSL protejat la aplicaţiile şi resursele interne şi pentru a autentifica utilizatorii aşa cum descrie acest scenariu.

Pasul 1: Completaţi foile de lucru de planificare

Următoarele foi de lucru demonstrează informaţiile pe care trebuie să le adunaţi şi deciziile pe care este nevoie să le faceţi pentru a pregăti implementarea certificatelor digitale pe care o descrie acest scenariu. Pentru a asigura o implementare cu succes, este nevoie să fiţi capabil să răspundeţi Da la toate elementele de cerinţe preliminare şi aveţi nevoie să aveţi adunate toate informaţiile cerute înainte să realizaţi orice task de configurare.

Tabela 3. Foaie de lucru de planificare a cerinţelor preliminare de implementare certificat

Foaie de lucru cerinţe preliminare	**Răspunsuri**
Versiunea dumneavoastră de OS/400 este V5R2 (5722-SS1) sau mai mare?	Da
Este instalat pe sistem Cryptographic Access Provider (5722-AC3)?	Da
Este instalată pe sistemul dumneavoastră opţiunea 34 a OS/400?	Da
Este instalat serverul HTTP IBM pentru iSeries (5722–DG1) pe sistemul dumneavoastră şi este pornită instanţa Administrative a serverului?	Da
Este configurat TCP pentru sistemul dumneavoastră astfel încât să puteţi folosi un browser Web şi instanţa Administrative a serverului HTTP pentru a accesa DCM?	Da
Aveţi autorizările speciale *SECADM şi *ALLOBJ?	Da

Trebuie să adunaţi următoarele informaţii despre implementarea dumneavoastră de certificate digitale pentru a realiza task-urile necesare de configurare pentru a termina implementarea:

Tabela 4. Foaie de lucru de planificare a configuraţiei de implementare certificat

Foaie de lucru de planificare pentru Serverul A	**Răspunsuri**
Veţi opera propriul dumneavoastră CA local sau veţi obţine certificate pentru aplicaţia dumneavoastră de la un CA public?	Creaţi CA-ul local pentru a emite certificate
Serverul A găzduieşte aplicaţia pe care vreţi să o activaţi pentru SSL?	Da

Tabela 4. Foaie de lucru de planificare a configuraţiei de implementare certificat (continuare)

Foaie de lucru de planificare pentru Serverul A	Răspunsuri
Ce informaţii de nume distinctiv veţi folosi pentru CA-ul local? • **Dimensiune cheie**: determină puterea cheilor criptografice pentru certificat. • **Nume CA**: identifică CA-ul şi devine numele comun pentru certificatul CA şi DN-ul emitentului pentru certificatele pe care le emite CA. • **Unitate de organizare**: identifică secţiunea sau zona de organizare pentru aplicaţia care va folosi acest certificat. • **Nume organizaţie**: identifică compania dumneavoastră sau secţiunea divizională pentru aplicaţia care va folosi acest certificat. • **Localitate sau oraş**: identifică oraşul sau o desemnare a localităţii pentru organizaţia dumneavoastră. • **Stat sau provincie**: identifică statul sau provincia în care veţi folosi acest certificat. • **Ţară sau regiune**: identifică, cu o desemnare din două litere, ţara sau regiunea în care veţi folosi acest certificat. • **Perioadă de validitate a Autorităţii de certificare**: specifică numărul de zile pentru care certificatul Autorităţii de certificare este valid	**Dimensiune cheie**: 1024 **Nume Autoritate de certificare (CA)**: Myco_CA@myco.com **Unitate organizaţie**: Rate dept **Nume organizaţie**: myco **Localitate sau oraş**: Orice_oraş **Stat sau provincie**: Orice **Ţară sau regiune**: ZZ **Perioadă de validitate a Autorităţii de certificare**: 1095
Vreţi să setaţi datele politicii pentru a permite CA-ului local să emită certificate de utilizator pentru autentificarea clientului?	Da
Ce informaţii despre numele distinctiv veţi folosi pentru certificatul de server pe care îl emite CA-ul local? • **Dimensiune cheie**: determină puterea cheilor criptografice pentru certificat. • **Etichetă certificat**: identifică certificatul cu un şir unic de caractere. • **Nume comun**: identifică proprietarul certificatului, cum ar fi o persoană, entitate sau aplicaţie; parte a DN-ului subiect pentru certificat. • **Unitate organizaţie**: identifică secţiunea sau zona de organizare pentru aplicaţia care va folosi acest certificat. • **Nume organizaţie**: identifică compania dumneavoastră sau secţiunea divizională pentru aplicaţia care va folosi acest certificat. • **Localitate sau oraş**: identifică oraşul sau o desemnare a localităţii pentru organizaţia dumneavoastră. • **Stat sau provincie**: identifică statul sau provincia în care veţi folosi acest certificat. • **Ţară sau regiune**: identifică, cu o desemnare din două litere, ţara sau regiunea în care veţi folosi acest certificat.	**Dimensiune cheie**: 1024 **Etichetă certificat**: Myco_public_cert **Nume comun**: myco_rate_server@myco.com **Unitate organizaţie**: Rate dept **Nume organizaţie**: myco **Localitate sau oraş**: Orice_oraş **Stat sau provincie**: Orice **Ţară sau regiune**: ZZ
Care este ID-ul aplicaţiei DCM pentru aplicaţia pe care vreţi să o configuraţi să folosească SSL?	mcyo_agent_rate_app
Veţi configura aplicaţia cu SSL aplicat să folosească certificate pentru autentificarea client? Dacă da, care CA-uri vreţi să le adăugaţi la lista de CA-uri de încredere a aplicaţiei?	Da Myco_CA@myco.com

Pasul 2: Finalizarea task-urilor preliminare pentru a instala toate produsele necesare

Trebuie să finalizaţi toate task-urile preliminare pentru a instala şi configura toate produsele necesare înainte de a putea executa orice task de configurare specific pentru implementarea acestui scenariu.

Pasul 3: Configurare server HTTP de resurse umane pentru a folosi SSL

| Configuraţia SSL (Secure Sockets Layer) pentru serverul HTTP de resurse umane (monitorizat de Apache) de pe
| Serverul A implică un număr de task-uri care variază în funcţie de cum este configurat curent serverul dumneavoastră.

| Pentru a cofigura serverul să folosească SSL, urmaţi aceşti paşi:
| 1. Porniţi interfaţa Administrare server HTTP.
| 2. Pentru a lucra cu un server HTTP specific, selectaţi aceste fişe de pagini **Gestionare —> Toate serverele —> Toate serverele HTTP** pentru a vedea o listă a tuturor serverelor HTTP configurate.
| 3. Selectaţi serverul corespunzător din listă şi faceţi clic pe **Gestionare detalii**.
| 4. În cadrul de navigaţie, selectaţi **Securitate**.
| 5. Selectaţi fişa **SSL cu Autentificare certificat** din formular.
| 6. În câmpul **SSL**, selectaţi Activat.
| 7. În câmpul **Nume aplicaţie certificat server**, specificaţi un ID de aplicaţie prin care este cunoscută această instanţă server. Sau, puteţi selecta unul din listă. Acest ID aplicaţie este în forma QIBM_HTTP_SERVER_[nume_server], de exemplu, QIBM_HTTP_SERVER_MYCOTEST. **Notă:** Memoraţi acest ID aplicaţie. Va fi nevoie să-l selecatţi din nou în DCM.

| Puteţi afla mai multe despre configuraţia generală necesară pentru serverul dumneavoastră HTTP la folosirea SSL în
| subiectul Informaţii HTTP Server for iSeries, în special într-un exemplu numit Scenariu: JKL activează protecţia SSL
| (Secure Sockets Layer) pe serverul lor HTTP (monitorizat de Apache). Acest scenariu furnizează toţi paşii task-urilor
| pentru crearea unei gazde virtuale şi configurarea ei pentru folosirea SSL, inclusiv următoarele task-uri:
| 1. Stare gazdă virtuală bazată pe nume.
| 2. Setare directivă Ascultare pentru gazdă virtuală.
| 3. Setare directoare gazdă virtuală.
| 4. Setare protecţie parolă via autentificare de bază.
| 5. Activare SSL pentru gazda virtuală

Pentru informaţii suplimentare despre configurarea atât a versiunilor curente cât şi a celor viitoare ale serverului HTTP pentru iSeries, vedeţi subiectul Server HTTP pentru iSeries.

| Când terminaţi configurarea pentru ca serverul HTTP să folosească SSL, puteţi utiliza DCM pentru a configura
| suportul de certificat de care aveţi nevoie pentru SSL şi autentificare client.

Pasul 4: Crearea şi operarea CA-ului 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 ceea ce este necesar pentru a activa SSL pentru aplicaţia dumneavoastră. Asta include asignarea certificatului pe care îl emite CA-ul local pentru aplicaţia dumneavoastră de server Web. De asemnea, adăugaţi CA-ul local la lista de CA-uri de încredere pentru aplicaţia serverului 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-ul local.

Pentru a folosi DCM pentru a crea şi opera un CA local şi emite un certificat către aplicaţia de pe serverul dumneavoastră de resurse umane, urmaţi aceşti paşi:
1. Porniţi DCM.
2. În cadrul de navigare din DCM, selectaţi **Crearea unui CA** pentru a se afişa o serie de formulare. Aceste formulare vă îndrumă prin procesul creării unui CA local şi completării altor task-uri necesare pentru a începe folosirea certificatelor 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. Când folosiţi aceste formulare pentru a realiza toate task-urile de care aveţi nevoie pentru a seta un CA local funcţional, parcurgeţi paşii următori:
   a. Furnizaţi informaţiile de identificare pentru CA-ul local.
   b. Instalaţi certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaşte CA-ul local şi să valideze certificatele pe care le emite CA-ul local.
   c. Alegeţi datele politicii pentru CA-ul dumneavoastră local.

      Notă: Asiguraţi-vă că selectaţi opţiunea care permite CA-ului local să emită certificate de utilizator.
   d. Folosiţi noul CA local pentru a emite un certificat server sau client pe care aplicaţiile dumneavoastră 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 dumneavoastră.
   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 la acest moment al task-ului, el se opreşte şi trebuie să realizaţi task-uri separate pentru a efectua configurarea certificatului SSL.
   g. Selectaţi aplicaţiile care vor avea încredere în CA-ul local.

      Notă: Aveţi grijă să selectaţi ID-ul aplicaţiei pentru serverul dumneavoastră HTTP de resurse umane, de exemplu, QIBM_HTTP_SERVER_MYCOTEST, ca una dintre aplicaţiile care au încredere în CA-ul local.

Când terminaţi configuraţia certificatului pe care aplicaţia server Web o cere pentru a folosi SSL, puteţi configura serverul Web să necesite certificate pentru autentificarea utilizatorilor.

Pasul 5: Configurare autentificare client pentru serverul Web de resurse umane

Trebuie să configuraţi setările generale de autentificare pentru serverul HTTP când specificaţi că serverul HTTP necesită certificate pentru autentificare. Configuraţi aceste setări în acelaşi formular de securitate pe care l-aţi folosit pentru a configura serverul să folosească SSL (Secure Sockets Layer).

Pentru a configura serverul să necesite certificate pentru autentificarea client, urmaţi aceşti paşi:

1. Porniţi interfaţa Administrare server HTTP.
2. Pentru a lucra cu un server HTTP specific, selectaţi aceste fişe de pagini **Gestionare —> Toate serverele —> Toate serverele HTTP** pentru a vedea o listă a tuturor serverelor HTTP configurate.
3. Selectaţi serverul corespunzător din listă şi faceţi clic pe **Gestionare detalii**.
4. În cadrul de navigaţie, selectaţi **Securitate**.
5. Selectaţi fişa **SSL cu Autentificare certificat** din formular.
6. Selectaţi **Folosire profil OS/400 al clientului**.
7. În câmpul **Nume sau regiune autentificare**, specificaţi un nume pentru regiunea de autentificare.
8. Selectaţi Activat pentru câmpul **Procesare cereri folosind autorizarea client** şi faceţi clic pe **Aplicare**.
9. Selectaţi fişa **Controlare acces** din formular.
10. Selectaţi **Toţi utilizatorii autentificaţi (nume utilizator şi parolă valide)** şi faceţi clic pe **Aplicare**.
11. Selectaţi câmpul **SSL cu autentificare certificat** din formular.
12. Asiguraţi-vă că Activat este valoarea selectată în câmpul **SSL**.
13. În câmpul **Nume aplicaţie certificat server**, asiguraţi-vă că este specificată valoarea corectă, de exemplu, QIBM_HTTP_SERVER_MYCOTEST.
14. Selectaţi **Acceptare certificat client dacă este disponibil înainte de a face conexiunea**. Faceţi clic pe OK.

Puteţi afla mai multe despre configuraţia generală necesară pentru serverul dumneavoastră HTTP la folosirea SSL în subiectul Informaţii HTTP Server for iSeries, în special într-un exemplu numit Scenariu: JKL activează protecţia SSL (Secure Sockets Layer) pe serverul lor HTTP (monitorizat de Apache). Acest scenariu furnizează toţi paşii task-ului pentru crearea unei gazde virtuale şi configurarea ei să folosească SSL.

Când terminaţi configurarea autentificării client, puteţi să reporniţi serverul HTTP în mod SSL şi să începeţi să protejaţi securitatea datelor aplicaţiei de resurse umane.

Pasul 6: Pornire server Web de resurse umane în mod SSL

S-ar putea să fie nevoie să opriţi şi să reporniţi Serverul dumneavoastră 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 reporni serverul HTTP (monitorizat de Apache) urmaţi aceşti paşi:
1. În Navigator **iSeries**, expandaţi-vă serverul.
2. Expandaţi **Reţea > Servere > TCP/IP > Administrare HTTP**.
3. Faceţi clic pe **Pornire** pentru a porni interfaţa Administrare server HTTP.
4. Faceţi clic pe fişa **Gestionare** pentru a vedea o listă a tuturor serverelor HTTP configurate.
5. Selectaţi serverul corespunzător din listă şi faceţi clic pe **Oprire** dacă serverul rulează.
6. Faceţi clic pe **Pornire** pentru a reporni serverul. Consultaţi ajutorul online pentru informaţii suplimentare despre parametrii de pornire.

Pentru informaţii suplimentare despre gestionarea atât a versiunilor curente cât şi a celor viitoare ale serverului HTTP pentru iSeries (original sau monitorizat de Apache), vedeţi subiectul Server HTTP pentru iSeries.

Pentru ca utilizatorii să poată accesa aplicaţia Web de resurse umane, ei trebuie mai întâi să instaleze o copie a certificatului CA local în browser.

Pasul 7: Faceţi utilizatorii să instaleze o copie a certificatului CA local în browser

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 public din Internet, browser-ul utilizatorului sau alt software client trebuie 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 DCM (Digital Certificate Manager) 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. 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 browser-ul 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 dumneavoastră. Asta asigură că browser-ul dumneavoastră poate stabili sesiuni de comunicaţie sigure cu serverele Web care folosesc un certificat de la acestă 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.

Acum că utilizatorii pot accesa serverul Web de resurse umane în mod SSL, aceştia trebuie să fie capabili să prezinte un certificat corespunzător pentru a se autentifica la server. În consecinţă, ei trebuie să obţină un certificat de la CA-ul local.

Pasul 8: Faceţi ca fiecare utilizator să ceară un certificat de la CA-ul 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-ul local pentru a li se permite să acceseze serverul Web. Fiecare utilizator trebuie să folosească DCM pentru a obţine un certificat folosind task-ul **Creare certificat**. Pentru a obţine un certificat de la CA-ul local, politica de CA local trebuie să-i permită să emită certificate utilizator.

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

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. Browser-ul poate afişa mai multe ferestre pentru a vă ghida prin acest proces. Se urmează instrucţiunile browser-ului 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. Browser-ul 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 task-ul.

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

Cu aceste task-uri terminate, doar utilizatorii autorizaţi cu un certificat valid pot accesa date de la serverul Web de resurse umane şi datele respective sunt protejate în timpul transmisiei de către SSL.

Capitolul 5. Concepte de certificate digitale

Înainte să începeţi să folosiţi certificate digitale pentru a îmbunătăţi sistemul dumneavoastră şi politica de securitate a reţelei, trebuie să înţelegeţi ce sunt ele şi ce avantaje de securitate oferă.

Un certificat digital este un credential digital care validează identitatea proprietarului certificatului, cum o face un paşaport. Informaţiile de identificare pe care un certificat digital le oferă sunt cunoscute ca numele distinctiv al subiectului. O parte de încredere, numită Autoritate de certificare (CA) emite certificate digitale către utilizatori sau organizaţii. Încrederea în CA stă la baza încrederii în certificat ca o scrisoare de acreditare validă.

Un certificat digital conţine de asemenea o cheie publică care este parte dintr-o pereche de chei publice-private. O varietate de funcţii de securitate se bazează pe utilizarea certificatelor digitale şi a perechilor de chei asociate. Puteţi folosi certificate digitale pentru a configura sesiuni SSL (Secure Sockets Layer) pentru a asigura sesiuni de comunicaţii private, sigure între utilizatori şi aplicaţiile dumneavoastră server. Puteţi extinde această securitate prin configurarea multor aplicaţii cu SSL activat pentru a necesita certificate în loc de nume utilizator şi parole pentru o autentificare mai sigură a utilizatorului.

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

Extensii certificat
Citiţi aceste informaţii pentru a învăţa care câmpuri de extensie certificat sunt şi cum sunt folosite.

Reînnoire certificat
Citiţi aceste informaţii pentru a învăţa despre procesul pe care îl foloseşte DCM pentru a reînnoi certificatele server şi client şi certificatele de semnare a obiectelor.

Numele distinctiv
Citiţi aceste informaţii pentru a învăţa despre caracteristicile de identificare ale certificatelor digitale.

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

Perechea de chei publică-privată
Citiţi aceste informaţii pentru a învăţa despre cheile de securitate asociate cu certificate digitale.

Autoritate de certificare (CA)
Citiţi aceste informaţii pentru a învaţa despre CA-uri, entităţile care emit certificate digitale.

Locaţii CRL (Certificate Revocation List)
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 afla 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.

Coprocesor criptografic IBM pentru iSeries
Citiţi aceste informaţii pentru a învăţa cum să folosiţi DCM şi coprocesoarele criptografice IBM pentru o memorare mai sigură a cheii.

Secure Sockets Layer (SSL)
Citiţi aceste informaţii pentru o descriere scurtă a SSL.

Definiţii aplicaţii
Citiţi aceste informaţii pentru a învăţa ce aplicaţii DCM sunt şi cum să lucraţi cu ele pentru configurare SSL şi semnare obiect.

Validare
Citiţi aceste informaţii pentru a învăţa cum funcţionează procesul de validare pentru aplicaţii şi certificate în DCM.

Extensii certificate

Extensiile certificatelor sunt câmpuri de informaţii care furnizează informaţii suplimentare despre certificat. Extensiile certificatelor furnizează un mijloc de expandare a standardelor de informaţii certificat X.509. În timp ce informaţiile pentru unele extensii sunt furnizate pentru a extinde informaţiile de identificare pentru certificat, alte extensii furnizează informaţii despre capabilităţile criptografice ale certificatului.

Nu toate certificatele folosesc câmpurile extensie pentru a extinde numele distinctiv şi alte informaţii. Numărul şi tipul câmpurilor extensie pe care le foloseşte un certificat variază între entităţile CA care emit certificate.

De exemplu, CA-ul local pe care îl furnizează DCM (Digital Certificate Manager), vă permite să folosiţi doar extensiile pentru certificat Nume alternativ subiect. Aceste extensii vă permit să asociaţi un certificat cu o adresă IP specifică, un nume domeniu complet calificat, sau o adresă de email. Dacă intenţionaţi să folosiţi certificatul pentru a identifica un punct final de conexiune VPN (Virtual Private Network), trebuie să oferiţi informaţii pentru aceste extensii.

Reînnoirea certificatelor

Procesul de reînnoire a certificatelor pe care îl foloseşte DCM (Digital Certificate Manager) variază în funcţie de tipului CA-ului care a emis certificatul.

Dacă folosiţi CA-ul local pentru a semna certificatul reînnoit, DCM foloseşte informaţiile pe care le furnizaţi pentru a crea un nou certificat în depozitul curent de certificate şi reţine certificatul anterior.

Dacă utilizaţi un CA din Internet binecunoscut pentru a emite certificatul, puteţi trata reînnoirea certificatului în unul din cele două moduri: să importaţi certificatul reînnoit dintr-un fişier pe care îl primiţi de la CA de semnare sau să puneţi DCM-ul să creeze o nouă pereche de chei publică-privată pentru certificat. DCM furnizează prima opţiune în caz că preferaţi să reînnoiţi certificatul direct cu CA-ul care l-a emis.

Dacă alegeţi să creaţi o nouă pereche de chei, DCM tratează reînnoirea în acelaşi mod în care a tratat crearea certificatului. DCM creează o nouă pereche de chei publică-privată pentru certificatul reînnoit şi generează un CSR (Certificate Signing Request) care este constuită din cheia puclică şi alte informaţii pe care le specificaţi pentru noul certificat. Puteţi folosi CSR-ul pentru a cere un nou certificat de la VeriSign sau orice alt CA public. O dată ce primiţi certificatul semnat de la CA, folosiţi DCM pentru a-l importa în depozitul corespunzător de certificate. Depozitul de certificate apoi conţine ambele copii ale certificatului, originalul şi certificatul reînnoit emis recent.

Dacă alegeţi să nu genereze DCM o nouă pereche de chei, DCM vă ghidează prin procesul de importare a certificatului reînnoit, semnat în depozitul de certificate dintr-un fişier existent pe care l-aţi primit de la CA. Certificatul importat, reînnoit înlocuieşte apoi certificatul anterior.

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 plănuiţi să acceptaţi şi să utilizaţi certificatele drept acreditări, trebuie să revedeţi cererile de identificare pentru un CA pentru a determina dacă cererile lor se potrivesc nevoilor dumneavoastră de securitate.

Nume distinctiv (DN) este un termen care descrie informaţiile de identificare dintr-un certificat şi este parte a certicatului în sine. Un certificat conţine informaţii DN atât pentru proprietar sau solicitant al certificatului (numit DN-ul subiect) cât şi pentru CA care emite certificatul (numit DN emitent). 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 un CA
| public din Internet îl emite pentru organizaţia dumneavoastră. Informaţiile DN pe care le puteţi furniza pentru unul
| dintre tipurile de certificate includ:
| • Numele comun al deţinătorului certificatului.
| • Organizaţia
| • Unitatea organizaţională
| • Localitate sau oraş
| • Stat sau provincie
| • Ţară sau regiune

| Când folosiţi DCM pentru a emite certificate private, puteţi utiliza extensii pentru certificat pentru a furniza informaţii
| suplimentare despre DN pentru certificat, inclusiv:
| • Adresă de IP versiuna 4
| • Numele complet calificat al domeniului
| • Adresa de e-mail

| Aceaste informaţii suplimentare sunt folositoare dacă plănuiţi să utilizaţi certificatul pentru a configura o conexiune
| VPN (virtual private network).

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 dumneavoastră 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 cheii de semnare) cu 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 software a creat o aplicaţie i5/OS pe care vrea să o distribuie prin Internet, ca o măsură comodă şi ieftină pentru clienţii săi. Totuşi, el ştie că respectivii clienţi sunt, pe bună dreptate, îngrijoraţi de descărcarea programului din Internet, datorită crescândelor probleme privind obiectele 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 binecunoscut 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 este 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. Digital Certificate Manager (DCM) vă permite să gestionaţi certificate atât de la CA-uri publice cât şi de la cele private.

De asemenea, puteţi folosi DCM pentru a opera propriul dumneavoastră CA local pentru a emite certificate private către sisteme şi utilizatori. Când CA-ul local emite un certificat de utilizator, DCM îl asociază automat certificatul cu profilul de utilizator de pe sistemul utilizatorului sau altă identitate de utilizator. Dacă DCM asociază certificatul cu un profil utilizator sau cu o identitate diferită pentru utilizator depinde dacă configuraţi DCM să lucreze cu EIM (Enterprise Identity Mapping). 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 un CA special.

Puteţi folosi DCM pentru a activa sau dezactiva starea de încredere pentru un certificat CA (Certificate Authority). 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 un CA (Certificate Authority) local cu Digital Certificate Manager, puteţi specifica datele de politică pentru CA-ul local. Datele de politică pentru un CA local descriu privilegiile de semnare pe care le are acesta. Datele politicii determină:

- Dacă CA-ul local poate emite şi semna certificate de utilizator.
- Cât timp sunt valide certificatele pe care le emite CA-ul local.

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 un CA îşi publică propria listă CRL, certificatul indică acest lucru incluzând o extensie punct distribuţie CRL în formularul URI (Uniform Resource Identifier - identificator resursă uniform).

DCM (Digital Certificate Manager) 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 un CA specific 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-ul specificat. .

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 conţine de asemenea cheia privată a certificatului doar dacă nu alegeţi să folosiţi un coprocesor criptografic IBM pentru a memora cheia în schimb. DCM vă permite să creaţi şi să gestionaţi mai multe tipuri de depozite de certificate. DCM controlează accesul la depozitele de certificate prin parole în conjuncţie cu controlul accesului la directorul sistemului de fişiere şi la fişierele 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:

CA local
DCM foloseşte acest depozit de certificate pentru a memora certificatul CA local şi cheia sa primară în cazul în care creaţi un CA local. Puteţi folosi certificatul din acest depozit pentru a semna certificate pentru care folosiţi CA-ul local pentru a le emite. Când CA-ul local emite un certificat, DCM pune o copie a certificatului CA (fără cheia privată) în depozitul de certificate corespunzător (de exemplu, *SYSTEM) pentru scopuri de autentificare. Aplicaţiile folosesc 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 (şi, probabil, şi multe aplicaţii ale altor dezvoltatori de software) sunt scrise pentru a folosi certificate numai din depozitul de certificate *SYSTEM. Când folosiţi DCM pentru a crea un CA local, DCM creează acest depozit de certificate ca parte a procesului. Când alegeţi să obţineţi certificate de la un CA public, cum sunt VeriSign, pentru ca aplicaţia dumneavoastră 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, task-urile 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 creează 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 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 dumneavoastră 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 pe server este instalat IBM Cryptographic Coprocessor, puteţi alege alte opţiuni de memorare a cheii private pentru certificate (cu excepţia certificatelor de semnare pentru obiecte). 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 CA local, *SYSTEM, *OBJECTSIGNING şi *SIGNATUREVERIFICATION trebuie să fie localizate în căi specifice ale sistemului de fişiere integrat, iar depozitele Alte certificate sistem (Other System Certificate) 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. Un grup are o pereche de chei compusă dintr-o cheie publică şi una privată. Cheia publică se distribuie liber, tipic într-un certificat digital, în timp ce cheia privată este păstrată în siguranţă de către 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. .

IBM Cryptographic Coprocessors pentru iSeries

Dacă se foloseşte IBM Cryptographic Coprocessors se adaugă serverului capacitatea de procesare criptografică de înaltă siguranţă. Coprocesorul criptografic furnizează servicii criptografice dovedite, asigurând protecţie şi integritate, pentru a dezvolta aplicaţii e-business sigure.

Dacă aveţi un coprocesor criptografic instalat şi variat pe sistemul dumneavoastră, îl puteţi utiliza pentru a oferi memorare mai sigură a cheii pentru cheile private ale certificatului.

Puteţi folosi coprocesorul criptografic pentru a memora cheia privată pentru un certificat server sau client şi pentru un certificat Autoritate de certificare (CA). Totuşi, nu puteţi folosi coprocesorul criptografic pentru a memora cheia primară a unui certificat utilizator deoarece această cheie trebuie să fie memorată pe sistemul utilizatorului. De asemenea, în acest moment nu puteţi folosi coprocesorul pentru a depozita cheia privată pentru un certificat care semnează obiecte.

Puteţi fie să memoraţi cheia privată a unui certificat direct în coprocesorul criptografic, fie puteţi folosi cheia master a coprocesorului criptografic pentru a cripta cheia şi să o memoraţi într-un fişier cheie special. Puteţi selecta aceste opţiuni de memorare a cheii ca parte a procesului de creare sau 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 utiliza coprocesorul criptografic pentru memorarea cheii private, trebuie să vă asiguraţi că aceste este activat înainte să folosiţi DCM (Digital Certificate Manager). Altfel, DCM nu furnizează opţiunea de selectare a unei locaţii de memorare ca parte a procesului de creare sau reînnoire a certificatului.

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.

Definiţii aplicaţie

Sunt două tipuri de definiţii de aplicaţie pe care le puteţi gestiona în DCM (Digital Certificate Manager):

- Definiţii de aplicaţii client sau server care folosesc sesiuni de comunicaţii SSL (Secure Sockets Layer).
- Definiţii de aplicaţii de semnare obiecte care semnează obiecte pentru a asigura integritatea obiectului.

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. Dezvoltatorii de aplicaţii înregistrează aplicaţiile cu SSL activat utilizând un API (QSYRGAP, QsyRegisterAppForCertUse) pentru a crea ID-ul aplicaţiei în DCM automat. Toate aplicaţiile IBM activate pentru SSL sunt înregistrate în DCM, aşa că puteţi să folosiţi cu uşurinţă DCM pentru a le asigna un certificat astfel încât să poată stabili o sesiune SSL. De asemenea, pentru aplicaţii pe care le scrieţi sau le cumpăraţi, puteţi să definiţi o definiţie de aplicaţie şi să creaţi un ID aplicaţie pentru ea în interiorul 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, definiţia aplicaţiei pe care o creaţi ar putea descrie tipul sau grupul obiectelor pe care intenţionaţi să le semnaţi. Trebuie să lucraţi în depozitul de certificate *OBJECTSIGNING pentru a crea o definiţie aplicaţie care semnează obiecte.

Validare

DCM (Digital Certificate Manager) furnizează task-uri care vă permit să validaţi un certificat sau o aplicaţie pentru a verifica diferite proprieităţi pe care fiecare trebuie să le aibă.

Validarea certificatelor

Când validaţi un certificat, DCM (Digital Certificate Manager) verifică un număr de articole care aparţin certificatului pentru a asigura autenticitatea şi validitatea sa. 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. DCM verifică de asemenea că certificatul CA pentru CA emiţătoare este depozitul de certificate curent şi că certificatul CA este marcat ca fiind de încredere. Dacă certificatul are o cheie privată (de exemplu, certificate de semnare client sau server sau obiect), atunci DCM validează de asemenea perechea de chei publică-privată pentru a se asigura că se potriveşte. Cu alte cuvinte, DCM criptează datele cu cheia publică şi apoi se asigură că acestea pot fi decriptate cu cheia privată.

Validarea aplicaţiilor

Când validaţi o aplicaţie, DCM (Digital Certificate Manager) verifică că există o asignare de certificat pentru aplicaţie şi asigură că certificatul asignat 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 aplicaţiei specifică că apare procesarea CRL (Certificate Revocation List) şi că există o locaţie CRL definită pentru CA, DCM verifică CRL-ul ca parte a procesului de validare.

Validarea unui aplicaţii poate să vă ajute să vă alerteze depre problemele potenţiale pe care le-ar putea avea aplicaţia când realizează o funcţie care necesită certificate. Asemenea probleme ar putea împiedica o aplicaţie fie de la participarea cu succes la o sesiune SSL (Secure Sockets Layer) fie de la semnarea cu succes a obiectelor.

Capitolul 6. Plan pentru DCM

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

Considerente despre salvare de rezervă şi recuperare pentru date DCM
Citiţi acesta pentru a învăţa cum să asiguraţi ca datele DCM importante sunt adăugate la salvarea de rezervă şi planul de recuperare pentru sistemul dumneavoastră.

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 dumneavoastră după ce decideţi cum doriţi să folosiţi certificatele pentru a profita de securitatea adiţională pe care o oferă. Puteţi folosi certificate de la un CA public sau puteţi crea şi opera un CA privat 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 şi EIM (Enterprise Identity Mapping)
Folosiţi aceste informaţii pentru a învăţa despre folosirea DCM în conjuncţie cu EIM.

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

DCM (Digital Certificate Manager) este o caracteristică gratuită care vă permite să gestionaţi central certificatele digitale pentru aplicaţiile dumneavoastră. Pentru a folosi cu succes DCM, aveţi grijă să 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 din i5/OS. Aceasta este facilitatea DCM bazată pe browser.
- Instalaţi serverul HTTP IBM pentru iSeries (5722–DG1) şi porniţi instanţa server Administrativă.
- Asiguraţi-vă că TCP este configurat pentru sistemul dumneavoastră astfel încât să puteţi folosi un browser Web şi instanţa server Server HTTP administrativ pentru a accesa 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.

Considerente despre salvare de rezervă şi recuperare pentru date DCM

Parolele bazei de date de chei codate pe care le folosiţi pentru a accesa depozitele de certificate din DCM (Digital Certificate Manager) sunt memorate, sau *ascunse*, într-un fişier special de securitate de pe server. Când folosiţi DCM pentru a crea un depozit de certificate pe sistemul dumneavoastră, DCM păstrează automat parola penru dumneavoastră. Totuşi, trebuie să vă asiguraţi manual că DCM păstrează parole de depozite de certificate în anumite circumstanţe.

Un exemplu este situaţia în care folosiţi DCM pentru a crea un certificat pentru alt server şi alegeţi să utilizaţi fişierele de certificat de pe sistemul destinaţie pentru a crea un nou depozit de certificate. În acest caz, trebuie să deschideţi noul depozit de certificate creat şi să utilizaţi task-ul **Modificare parolă** pentru a modifica parola pentru depozitul de certificate de pe sistemul destinaţie, care asigură faptul că DCM păstrează noua parolă. Dacă depotizul de certificate este alt depozit de certificate sistem, ar trebui de asemenea să specificaţi că vreţi să folosiţi opţiunea **Logare automată** când modificaţi parola. Pentru a afla mai multe despre folosirea DCM pentru a crea certificate pentru alte sisteme, vedeţi Folosirea unui CA local pentru a emite certificate pentru alte servere.

Suplimentar, trebuie să specificaţi opţiunea **Logare automată** când modificaţi sau resetaţi parola pentru alt depozit de certificate sistem.

Pentru a vă asigura că aveţi o copie de rezervă completă a datelor DCM critice, trebuie să faceţi următoarele:

- Utilizaţi comanda SAV (Save - Salvare) pentru a salva toate fişierele .KDB şi .RDB. Fiecare depozit de certificate DCM este compus din două fişiere, unul cu extensia .KDB şi unul cu extensia .RDB.
- Folosiţi comanda SAVSYS (Save system - Salvare sistem) şi SAVSECDATA (save security data - Salvare date securitate) pentru a salva fişierul special de securitate care conţine parolele bazei de date de chei pentru acces la depozitul de certificate. Pentru a restaura fişierul de securitate parole DCM, folosiţi comanda RSTUSRPRF (restore user profiles - restaurare profiluri utilizator) şi specificaţi *ALL pentru opţiunea profil utilizator (USRPRF).

O alt considerent de recuperare se referă la utilizarea operaţiei SAVSECDATA şi la posibilitatea ca parolele curente ale depozitivului de certificate să devină nesincronizate cu parolele din fişierul de securitate parolă DCM salvat. Dacă modificaţi parole pentru un depozit de certificate după ce faceţi o operaţie SAVSECDTA, dar înainte să restauraţi detele din acea operaţie, parola curentă a depozitului de certificate nu va fi sincronizată cu cea din fişierul restaurat.

Pentru a evita această situaţie, trebuie să folosiţi task-ul **Modificare parolă** (sub **Gestionare depozit certificare** în cadrul de navigaţie) în DCM pentru a modifica parolele depozitului de certificate după ce restauraţi datele de la o operaţie SAVSECDTA pentru a vă asigura că primiţi parolele înapoi sincronzate. Totuşi, în această situaţie nu folosi butonul **Resetare parolă** care este afişat când selectaţi un depozit de certificate pentru deschidere. Când încercaţi să resetaţi parola, DCM încearcă să extragă parola păstrată. Dacă parola păstrată nu este sincronizată cu parola curentă, operaţia de resetare va eşua. Dacă nu modificaţi parolele depozitului de certificate des, ar putea să consideraţi să faceţi o SAVSECDTA de fiecare dată când modificaţi aceste parole pentru a vă asigura că mereu aveţi versiunea păstrată cea mai curentă a parolelor salvate în caz că veţi avea nevoie vreodată să restauraţi aceste date.

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. CA local pe care îl creaţi şi cu care operaţi cu 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, semnarea obiectelor sau verificarea semnăturilor obiectelor, trebuie să aveţi o copie a certificatului CA emitent.

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 de fişiere integrat 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. DCM (Digital Certificate Manager) asociază automat profilului de utilizator certificatele de utilizator pe care le emite CA-ul dumneavoastră privat. De asemenea, puteţi folosi DCM pentru a asocia profilului de utilizator certificatele pe care le emite alt CA.

Când folosiţi DCM (Digital Certificate Manager) pentru a vă gestiona certificatele, DCM le organizează şi le memorează pe ele şi cheile private asociate într-un depozit de certificate pe baza acestor clasificări .

Notă: Dacă pe server este instalat IBM Cryptographic Coprocessor, puteţi alege alte opţiuni de memorare a cheii private pentru certificate (cu excepţia certificatelor de semnare pentru obiecte). Puteţi alege să memoraţi cheia privată chiar pe coprocesorul criptografic. Sau, puteţi folosi coprocesorul criptografic pentru a cripta cheia privată şi să o memoraţi într-un fişier cheie special în locul unui depozit 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

O dată ce vă decideţi să folosiţi certificate, trebuie să alegeţi tipul implementării certificatelor care se potriveşte cel mai bine nevoilor dumneavoatră de securitate. Opţiunile pe care le aveţi pentru obţinerea certificatelor includ:
- Obţinerea certificatelor de la o Autoritate de certificare (CA) publică.
- Operarea unui CA local pentru a emite certificate private pentru utilizatorii şi aplicaţiile dumneavoastră.
- Utilizarea unei combinaţii de certificate de la CA-uri Internet publice şi CA-urile dumneavoastră locale.

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 dumneavoastră de afacere şi de securitate.

Folosirea certificatelor publice

CA-urile publice Internet lansează certificate către oricine plăteşte taxa corespunzătoare. Însă un CA din 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. Trebuie să evaluaţi dacă stringenţa politicii de identificare a CA se potriveşte nevoilor nevoilor dumneavoastră de securitate înainte de a decide să obţineţi certificate de la CA sau de a avea încredere în certificatele pe care ea le emite. Cum standardele PKIX (Public Key Infrastructure for X.509) au evoluat, unele CA-uri publice acum furnizează standarde de identificare mult mai stringente 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 unui CA public pentru a emite certificate. Dacă aveţi nevoie de certificate pentru un număr limitat de aplicaţii client sau server şi clienţi, costul s-ar putea să nu fie un factor important pentru dumneavoastră. 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, trebuie să consideraţi de asemenea efortul administrativ şi de programare necesar pentru a configura aplicaţiile server să accepte doar un subset specific de certificate pe care le emite un CA public.

Folosirea certificatelor provenite de la un CA public vă poate economisi timp şi resurse, deoarece multe aplicaţii server, client şi de utilizator sunt configurate pentru a recunoaşte majoritatea dintre CA-uri publice binecunoscute. De asemenea, alte companii şi utilizatori pot recunoaşte şi avea încredere în certificatele pe care le emite un CA public binecunoscut mai mult decât în cele emise de CA-ul dumneavoastră local.

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 dumneavoastră. Crearea şi menţinerea CA-ului dumneavoastră local vă permite să emiteţi certificate doar acelor utilizatori care sunt membri de încredere ai grupului dumneavoastră. Aceasta oferă o securitate mai bună, deoarece puteţi controla mai strâns cine are acces la certificate şi de aceea cine are acces la resursele dumneavoastră. Un potenţial dezavantaj al menţinerii propriei CA locale este cantitatea de timp şi resurse pe care trebuie să le investiţi. Oricum, Digital Certificate Manager (DCM) face acest proces mai uşor pentru dumneavoastră.

| Când folosiţi un CA local pentru a emite certificate utilizatorilor pentru autentificarea client, trebuie să decideţi unde
| vreţi să memoraţi certificatele utilizator. Când utilizatorii obţin certificatele lor de la CA-ul local prin intermediul
| DCM, acestea sunt memorate cu un profil utilizator în mod implicit. Totuşi, puteţi configura DCM să lucreze cu EIM
| (Enterprise Identity Mapping) astfel ca certificatele lor să fie memorate într-o locaţie LDAP (Lightweight Directory
| Access Protocol) în schimb. (Vedeţi Certificate digitale şi EIM (Enterprise Identity Mapping) pentru informaţii
| suplimentare despre cum lucrează împreună DCM şi EIM.) Dacă preferaţi să nu aveţi certificatele utilizator asociate
| sau memorate cu un profil utilizator de nici un fel, puteţi folosi API-uri pentru a emite programabil certificate către
| utilizatori non-iSeries.

Notă: Nu contează ce CA folosiţi pentru a emite certificate, administratorul de sistem controlează în care CA-uri vor avea încredere aplicaţiile pe sistemul său. Dacă o copie a unui certificat pentru un CA binecunoscut poate fi găsită în browser-ul dumneavoastră, acesta poate fi setat să aibă încredere în certificate server ce au fost emise de acel CA. Administratorii setează încrederea pentru certificate CA în depozitul de certificate corespunzător, care conţine copii ale certificatelor CA publice binecunoscute. Totuşi, dacă un certificat CA nu este în depozitul dumneavoastră de certificate, serverul dumneavoastră nu poate avea încredere în certificatele utilizator sau client care au fost emise de acel CA până nu obţineţi şi importaţi o copie a certificatului CA. Certificatul CA trebuie să fie în formatul corect de fişier şi trebuie să-l adăugaţi la 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 dumneavoastră 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 unui CA privat descrie task-urile pe care trebuie să le realizaţi dacă alegeţi să operaţi un CA local pentru a trimite certificate.
- Gestionarea certificatelor de la un CA public din Internet descrie task-urile pe care trebuie să le efectuaţi pentru a folosi certificatele de la un CA public binecunoscut, incluzând CA PKIX.
- Folosirea unui CA local pe alte servere prezintă task-urile pe care trebuie să le realizaţi dacă vreţi să folosiţi certificate de la un CA local privat pe mai multe sisteme.

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 dumneavoastră 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 situl 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 serverului cu o copie a certificatului emis de Autoritatea de certificare (CA). (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 SSL iniţiale pentru a negocia o cheie simetrică care este folosită ulterior pentru criptarea şi decriptarea datelor aplicaţiei pentru o sesiune SSL particulară. Aceasta înseamnă că serverul dumneavoastră 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 şi utilizatori. De asemenea, puteţi folosi DCM (Digital Certificate Manager) pentru a asocia certificatul unui utilizator cu profilul său de utilizator sau cu altă identitate

de utilizator. Apoi certificatul are aceleaşi autorizări şi permisiuni ca şi identitatea sau profilul de utilizator asociat. Alternativ, puteţi folosi API-uri pentru a utiliza autoritatea de certificare locală pentru a emite certificate utilizatorilor non-iSeries. Aceste API-uri vă dau posibilitatea să emiteţi certificate private pentru utilizatori când nu vreţi ca aceştia să aibă un profil de utilizator sau altă identitate de utilizator internă.

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 oferă suport pentru certificate de autentificare client:
- Server Telnet
- Server HTTP IBM(monitorizat de Apache)
- Server director IBM
- Acces iSeries pentru Windows (inclusiv Navigatorul iSeries)
- 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 învăţa mai multe despre configurarea aplicaţiilor server pentru folosirea certificatelor pentru autentificarea client în timpul unei sesiuni SSL, vedeţi subiectul SSL (Secure Sockets Layer) din Centrul de informare iSeries.

Certificate digitale şi EIM (Enterprise Identity Mapping)

Enterprise Identity Mapping (EIM) este o tehnologie eServer care vă permite să gestionaţi identităţile utilizator din întreprinderea dumneavoastră, inclusiv profiluri utilizator şi certificate utilizator. Un nume utilizator şi parolă sunt cea mai comună formă de identitate utilizator; certificatele sunt altă formă de identitate utilizator. Unele aplicaţii sunt configurate să permită utilizatorilor să fie autentificaţi prin intermediul unui certificat utilizator mai degrabă decât un nume utilizator şi parolă.

Puteţi folosi EIM pentru a crea mapări între identităţi utilizator, care permite unui utilizator să se autentifice cu o identitate utilizator şi să acceseze resursele altei identităţi utilizator fără ca utilizatorul să fie nevoit prezinte identiatea utilizator necesară. Realizaţi asta în EIM prin definirea unei asociaţii între o identitate utilizator şi altă identitate utilizator. Identităţile utilizator pot fi în diverse forme, inclusiv certificate utilizator. Puteţi fie să creaţi asociaţii individuale între un identificator EIM şi diferitele identităţi utilizator care aparţin unui utilizator reprezentat de acel identificator EIM. Sau puteţi crea asocieri de politică, care mapează un grup de identităţi utilizator la o singură identitate utilizator destinaţie. Identităţile utilizator pot fi în diverse forme, inclusiv certificate utilizator. Când creaţi aceste asociaţii, certificatele utilitor pot fi mapate pe identificatorii EIM corespunzători astfel făcând mai uşoară folosirea certificatelor pentru autentificare.

Pentru a profita de această caracteristică EIM pentru a gestiona certificate utilizator, trebuie să realizaţi aceste task-uri de configurare EIM înainte de a realiza orice task-uri de configurare DCM:

1. Folosiţi vrăjitorul **Configuraţie EIM** din Navigatorul **iSeries** pentru a configura EIM.
2. Creaţi un identificator EIM pentru fiecare utilizator care vreţi să participe la EIM.
3. Creaţi o asociere destinaţie între fiecare identificator EIM şi profilul de utilizator al utilizatorului respectiv din registrul de utilizatorii5/OS local, astfel încât orice certificat de utilizator pe care utilizatorul îl asignează prin DCM sau îl creează în DCM să poată fi mapat la profilul de utilizator. Folosiţi numele de definiţie din registrul EIM pentru registrul de utilizatorii5/OS local pe care l-aţi specificat în vrăjitorul **Configurare EIM**. **Notă:** Pentru informaţii suplimentare despre configurarea EIM, vedeţi subiectul EIM.

După ce realizaţi task-urile de configurare EIM necesare, trebuie să folosiţi task-ul **Gestionare locaţie LDAP** pentru a configura DCM (Digital Certificate Manager) să memoreze certificate utilizator într-o locaţie LDAP (Lightweight Directory Access Protocol) în locul unui profil utilizator. Când configuraţi EIM sau DCM să lucreze împreună, task-ul **Creare certificat** pentru certificate utilizator şi task-ul **Asignare certificat utilizator** procesează certificatele pentru utilizare EIM mai degrabă decât să asigneze certificatul unui profil utilizator. DCM memorează certificatul în directorul LDAP configurat şi foloseşte informaţiile din DN-ul certificatului pentru a crea o asociaţie sursă pentru identificatorul EIM corespunzător. Aceasta permite sistemelor de operare şi aplicaţiilor să folosească certificatul ca sursă a unei operaţii de căutare EIM pentru a mapa de la certificat la o identitate utilizator destinaţie asociată cu acelaşi identificator EIM.

Suplimentar, când configuraţi EIM şi DCM să lucreze împreună puteţi folosi DCM pentru a verifica expirarea certificatelor utilizator la nivel de întreprindere mai degrabă decât la nivel de sistem.

Certificatele digitale pentru conexiuni VPN

Puteţi folosi certificate digitale ca un mijloc de a stabili o conexiune VPN. 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.

O metodă pe care serverele IKE o pot folosi pentru a se autentifica unul pe altul este o cheie pre-partajată. Totuşi, folosirea unei chei pre-partajate este mai puţin sigură deoarece trebuie să comunicaţi această cheie manual administratorului de la celălalt capăt al VPN-ului dumneavoastră. 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. Când folosiţi CA-ul local în DCM pentru a emite un certificat, puteţi specifica informaţii alternative privind numele subiectului certificatului. Specificând aceste informaţii, vă asiguraţi că aveţi o conexiune VPN compatibilă cu alte implementări VPN care au nevoie de ele 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:
  - Crearea şi operarea unui CA local, privat vă arată cum să folosiţi DCM pentru a emite certificate private pentru aplicaţiile dumneavoastră.
  - Gestionarea certificatelor de la un CA public din Internet descrie cum să utilizaţi DCM pentru a lucra cu certificatele provenite de la un CA public.
- 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

i5/OS oferă 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 capacitatea uneltelor tradiţionale de sistem de a controla cine poate modifica obiectele. 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 îndeplineşte nevoile şi politicile dumneavoastră de securitate, este nevoie să evaluaţi dacă aveţi nevoie să folosiţi certificate publice versus emitere de certificate private. Dacă intenţionaţi să distribuiţi obiecte către utilizatori din publicul general, aţi putea considera folosirea certificatelor de la un CA public binecunoscut pentru a semna obiecte. 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 însă itenţionaţi să distribuiţi obiecte doar în cadrul organizaţiei dumneavoastră, aţi putea prefera să folosiţi DCM (Digital Certificate Manager)

pentru a opera propriul dumneavoastră CA local, cu care să emiteţi 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 un CA public binecunoscut.

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 DCM pentru a gestiona certificatele pe care le folosiţi pentru a semna obiecte şi 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

i5/OS furnizează suport pentru utilizarea certificatelor pentru a verifica semnături digitale pe obiecte. Oricine doreşte să se asigure că un obiect semnat nu a fost modificat la transfer 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. Când alegeţi să aveţi încredere într-un CA (Certificate Authority), puteţi să alegeţi dacă să aveţi încredere în semnăturile pe care le creează altcineva folosind un certificat emis de CA-ul de încredere. Când alegeţi să nu aveţi încredere într-un 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 dumneavoastră Controlaţi aceasta cu o valoare de sistem numită QVFYOBJRST (Verify object signatures during restore). 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 de sistem afectează doar obiectele executabile care sunt restaurate, nu fişierele salvare sau fişierele sistemului de fişiere integrat. Pentru a învăţa mai multe despre utilizarea ei şi a altor valori de sistem, vedeţi Căutătorul de valori sistem din Centrul de informare iSeries.

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

Capitolul 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 cadrul de navigaţie variază în funcţie de autorizaţiile pe care le are profilul dumneavoastră de utilizator i5/OS. Toate task-urile pentru operarea unui CA, pentru administrarea certificatelor pe care le folosesc aplicaţiile şi alte task-uri la nivelul de sistem sunt disponibile numai pentru responsabilii cu securitatea sau administratori. Responsabilul cu securitatea 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 cum se accesează caracteristica DCM (Digital Certificate Manager) pe server.

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 un CA (Certificate Authority - Autoritate de certificare) din Internet sau cum să creaţi şi să operaţi un CA local, privat pentru a emite certificate.

Dacă vreţi mai multe informaţii educaţionale despre folosirea certificatelor digitale într-un mediu Internet pentru a vă îmbunătăţi securitatea sistemului şi a reţelei dumneavoastră, situl Web VeriSign este o resursă excelentă. Situl Web VeriSign furnizează o bibliotecă extinsă despre subiecte de certificate digitale, precum şi un număr de alte subiecte legate de securitatea 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 priptografic pe care îl foloseşte DCM pentru a genera o pereche de chei publică-privată pentru certificate, pentru a cripta fişiere certificat exportate şi a decripta fişiere certificat importate.

2. Folosiţi Navigatorul iSeries pentru a porni serverul administrativ server HTTP:
   a. Porniţi **iSeries Navigator**.
   b. Faceţi dublu clic pe serverul dumneavoastră în vizualizarea arbore principală.
   c. Expandaţi **Reţea > Servere > TCP/IP**.
   d. Efectuaţi un clic dreapta pe **Administrare HTTP**.
   e. Selectaţi **Pornire**.
3. Porniţi-vă browser-ul Web.
4. Folosind browser-ul, mergeţi la pagina Task-uri de pe sistemul dumneavoastră, la http://*numele_sistemului_dvs*:2001.
5. Selectaţi **Digital Certificate Manager** din lista de produse din pagina Task-uri pentru a accesa interfaţa de utilizator DCM.

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. Care task-uri sunt disponibile depinde de memoria certificat (dacă există una) cu care lucraţi şi de autorizările speciale ale profilului utilizator. Majoritatea task-urilor sunt disponibile doar dacă aveţi autorizaţii speciale *ALLOBJ şi *SECADM. Pentru a utiliza DCM pentru a verifica semnături ale obiectelor, profilul dumneavoastră utilizator trebuie să aibă autorizarea specială *AUDIT.

Când folosiţi DCM (Digital Certificate Manager) pentru prima dată, nu există nici o memorie certificat. În consecinţă, când accesaţi iniţial DCM, panoul de navigaţie afişează doar aceste task-uri şi doar când aveţi autorizările speciale necesare:

- Gestionarea certificatelor utilizator.
- Crearea unui nou Depozit de certificate.
- Crearea unui CA (Certificate Authority - Autoritate de certificare). (Notă: După ce folosiţi acest task pentru a crea un CA local privat, acest task nu mai apare în listă.)
- Gestionarea locaţiilor CRL.
- Gestionare locaţie LDAP.
- Gestionarea locaţiei cererii PKIX.
- Revenirea în pagina Task-uri.

Chiar dacă depozitul de certificate există deja pe sistemul dumneavoastră (de exemplu, migraţi de la o versiune anterioară a DCM), DCM afişează doar un număr limitat de task-uri sau categorii de task-uri în cadrul de navigaţie stâng. Task-urile sau categoriile pe care DCM le afişează variază în funcţie de depozitul de certificate (dacă există unul) care este deschis şi autorizările speciale pentru profilul dumneavoastră utilizator.

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 afişa o a doua fereastră de browser pentru a iniţia o conexiune sigură folosind SSL (Secure Sockets Layer). 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 browser-ul 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 dumneavoastră.

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

Crearea şi operarea cu unui CA local

După ce revedeţi cu atenţie necesităţile şi politicile dumneavoastră de securitate, vă decideţi să operaţi cu un CA local pentru a emite certificate private pentru aplicaţiile dumneavoastră. Puteţi folosi DCM ca să creaţi şi să operaţi cu propriul dumneavoastră CA local. DCM vă oferă un task ghidat, care vă poartă prin acest proces de creare a unui CA şi de folosire a lui pentru a emite certificate pentru aplicaţii. Calea task-ului ghidat vă asigură că aveţi tot ce este necesar pentru a începe să folosiţi certificatele 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 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 faceţi o notă a acestui ID aplicaţie astfel încât să puteţi folosi DCM pentru a specifica care certificat va fi utilizat de această aplicaţie pentru SSL.

Nu terminaţi şi reporniţi serverul până nu folosiţi DCM să asigneze un certificat către server. Dacă opriţi şi reporniţi instanţa *ADMIN a serverului Web înainte de a-i asigna un certificat, serverul nu va porni şi nu veţi putea folosi DCM pentru a asigna un certificat serverului.

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 unui CA** pentru a se afişa o serie de formulare. Aceste formulare vă îndrumă prin procesul creării unui CA local şi completării altor task-uri necesare pentru a începe folosirea certificatelor 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. Când folosiţi aceste formulare pentru a realiza toate task-urile de care aveţi nevoie pentru a seta un CA local operaţional:
   a. Alegeţi cum să memoraţi cheia privată pentru certificatul CA local. (Acest pas este furnizat doar dacă aveţi un coprocesor criptografic IBM instalat pe iSeries-ul dumneavoastră. Dacă sistemul nu are un coprocesor criptografic, DCM va plasa automat certificatul şi cheia privată în CA-ul local.)
   b. Furnizaţi informaţiile de identificare pentru CA-ul local.
   c. Instalaţi certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaşte CA local şi să valideze certificatele pe care le emite CA.
   d. Alegeţi datele politicii pentru CA-ul dumneavoastră local.
   e. Folosiţi noul CA local pentru a emite un certificat server sau client pe care aplicaţiile dumneavoastră să îl poată folosi pentru conexiuni SSL. (Dacă iSeries-ul dumneavoastră are un coprocesor criptografic IBM 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 un CA public din 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 un CA public din Internet, nu efectuaţi acest lucru sau pasul anterior.

i. Selectaţi aplicaţiile care vor avea încrederea în CA-ul 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 folosească DCM pentru a obţine o copie a certificatului CA local. Fiecare utilizator trebuie să aibă o copie a certificatului astfel încât sofware-ul client al utilizatorului să-l poată utiliza 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 dumneavoastră.

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-ul local, revedeţi aceste subiecte:

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

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

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

Gestionarea certificatelor utilizator

Dumneavoastră şi utilizatorii dumneavoastră puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele pe care dumneavoastră şi utilizatorii dumneavoastră 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 serverul dumneavoastră foloseşte un certificat dintr-un CA public, software-ul utilizatorilor dumneavoastră ar putea poseda deja o copie a certificatului CA. În consecinţă, nici dumneavoastră ca administrator al DCM, nici utilizatorii dumneavoastră 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 emis de CA-ul 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 de utilizator acceptat pentru a accesa resursele pe care le furnizează serverul. În funcţie de nevoile dumneavoastră de securitate, utilizatorii pot prezenta un certificat de la un CA public din Internet sau unul pe care îl obţin de la CA-ul local pe care îl folosiţi dumneavoastră. Dacă aplicaţia server a dumneavoastră furnizează acces la resurse pentru utilizatorii interni care au în acest moment iSeries profiluri utilizator, puteţi folosi DCM pentru a le adăuga certificatele lor la profilurile 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 dumneavoastră ca şi pentru alţi utilizatori. Când nu este deschis nici un depozit de certificate sau când depozitul de certificate CA (autoritate de certificare) local 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 task-uri care le permit să vizualizeze certificatele asociate cu profilurile lor de utilizator, să şteargă un certificat din profilurile lor de utilizator sau să asigneze un certificat de la un CA diferit la profilurile lor de utilizator. Utilizatorii, indiferent de autorizările speciale pentru profilurile lor de utilizator, pot obţine un certificat de utilizator de la CA-ul local prin selectarea task-ului **Creare certificate** din cadrul de navigare principal.

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

Crearea unui certificat utilizator
Folosiţi aceste informaţii pentru a afla cum pot utilizatorii să folosească CA-ul local pentru a emite un certificat pentru autentificarea clientului.

Asignarea unui certificat utilizator
Utilizaţi aceste informaţii pentru a învăţa cum să asignaţi un certificat pe care îl deţineţi la profilul utilizator OS/400 sau altă identitate utilizator. Certificatul poate fi de la un CA local privat de pe alt sistem sau de la un CA din Internet binecunoscut. Pentru a asigna un certificat unei identităţi de utilizator, CA-ul emitent trebuie să fie de încredere pentru server şi certificatul trebuie să nu fie deja asociat cu un profil de utilizator sau altă identitate de utilizator din sistem.

Gestionare certificate utilizator prin expirare
Folosiţi aceste informaţii pentru a învăţa cum să vedeţi şi să gestionaţi certificate utilizator pe baza datelor lor de expirare.

Crearea unui certificat utilizator: Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă folosiţi DCM (Digital Certificate Manager) pentru a lucra cu un CA local privat, puteţi folosi CA-ul 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-ul local, politica de CA trebuie să permită CA-ului să emită certificate de utilizator.

Pentru a obţine un certificat de la un CA local, parcurgeţi paşii următori:
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. Browser-ul poate afişa mai multe ferestre pentru a vă ghida prin acest proces. Urmaţi instrucţiunile browser-ului 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. Browser-ul 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 task-ul.

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 profilurile lor utilizator, utilizatorul poate folosi DCM pentru a asigna certificatul la profilurile lor utilizator.

Asignarea unui certificat utilizator: Unii utilizator pot avea certificate de la un CA (Certificate Authority) din afară sau de la un CA local pe un sistem iSeries pe care dumneavoastră, ca administrator, vreţi să le faceţi disponibile pentru DCM (Digital Certificate Manager). Asta vă permite dumneavoastră şi utilizatorului să folosiţi DCM pentru a gestiona aceste certificate, care sunt cel mai adesea folosite pentru autentificarea client. Task-ul **Asignare certificat utilizator** furnizează un mecanism pentru a permite unui utilizator să creeze o asignare DCM pentru un certificat obţinut dintr-un CA din afară.

Când un utilizator asignează un certificat, DCM are una din două căi de a trata certificatul asignat:

- Memorare certificat local pe iSeries cu profilul utilizator al acestuia.
  Când o locaţie LDAP nu este definită pentru DCM, task-ul **Asignare un certificat utilizator** permite unui utilizator să asigneze un certificat din afară unui OS/400 profil utilizator. Asignarea certificatului la un profil utilizator asigură că certificatul poate fi folosit cu aplicaţii din sistem care necesită certificate pentru autentificarea client.
- Memorare certificat în locaţie LDAP (Lightweight Directory Access Protocol) pentru utilizare cu EIM (Enterprise Identity Mapping).
  Când este definită o locaţie LDAP şi sistemul iSeries este configurat să participe în EIM, task-ul **Asignare certificat utilizator** permite unui utilizator să memoreze o copie a unui certificat din afară în directorul LDAP specificat. DCM crează de asemenea o asociere sursă în EIM pentru certificat. Memorarea certificatul în acestă manieră permite unui administrator EIM să-l recunoască ca o identitate utilizator validă care poate participa în EIM.

  Notă: Înainte ca un utilizator să poată asigna un certificat la o identitate utilizator într-o configuraţie EIM, EIM trebuie să fie configurat în mod corespunzător pentru utilizator. Această configuraţie EIM implică creaţia unui identificator EIM pentru utilizator şi creaţia unei asocieri destinaţie între acel identificator EIM şi profilul utilizator. Altfel, DCM nu poate crea o asociaţie sursă corespunzătoare cu identificatorul EIM pentru certificat. Pentru informaţii suplimentare despre configurarea EIM, vedeţi Centrul de informareEIM topic in the iSeries.

Pentru a folosi task-ul **Asignare certificat utilizator**, un utilizator trebuie să îndeplinească următoarele cerinţe:

1. Să aibă o sesiune sigură cu serverul HTTP prin care să acceseze DCM.

   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 utilizatorul selectează acest task, se afişează o nouă fereastră de browser. Dacă utilizatorul nu are o sesiune sigură, DCM îl promptează să facă clic pe **Asignare certificat utilizator** pentru a porni una. DCM iniţiază apoi negocieri SSL (Secure Sockets Layer) cu browser-ul utilizatorului. Ca parte a acestor negocieri, browser-ul ar putea cere utilizatorului dacă să aibă încredere în Autoritatea de certificare (CA) care a emis certificatul care identifică serverul HTTP. De asemenea, browser-ul ar putea cere utilizatorului dacă să accepte certificatul serverului însuşi.
2. Să prezinte un certificat pentru autentificare 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 un 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.
3. Să aibă un certificat în browser care nu este asociat deja cu identitatea utilizatorului pentru cel care realizează task-ul. (Sau, dacă DCM este configurat pentru a lucra în conjuncţie cu EIM, utilizatorul trebuie să aibă un certificat în browser care nu este deja memorat în locaţia LDAP pentru DCM.)

   O dată ce stabiliţi o sesiune sigură, DCM încearcă să extragă un certificat corespunzător de la browser-ul dumneavoastră pentru a-l asocia cu identitatea dumneavoastră 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 informaţii de la un certificat, nu aţi putut să furnizaţi un certificat pe care DCM să-l poată asigna identităţii utilizator a dumneavoastră. De acest lucru poate fi responsabilă una dintre problemele certificatelor utilizator. De exemplu, certificatele pe care le conţine browser-ul dumneavoastră pot fi asociate deja cu identitatea utilizator a dumneavoastră.

Gestionarea certificatelor prin expirare: DCM (Digital Certificate Manager) furnizează suport pentru gestiunea expirării certificatelor pentru a permite administratorilor să verifice datele de expirare ale certificatelor utilizator din sistemul local iSeries. Suportul DCM pentru gestiunea expirării certificatelor poate fi folosit în conjuncţie cu Enterprise Identity Mapping (EIM) astfel încât administratorii pot folosi DCM pentru a verifica expirarea certificatelor utilizator la nivel de întreprindere.

Pentru a profita de suportul de gestiune al expirării pentru certificate utilizator la nivel de întreprindere, EIM trebuie să fie configurat în întreprindere şi trebuie să conţină informaţiile de mapare corespunzătoare pentru certificate utilizator. Pentru a verifica expirarea certificatelor utilizator altele decât cele asociate cu profilul dumneavoastră utilizator, trebuie să aveţi autorizările speciale *ALLOBJ şi *SECADM.

Folosirea DCM pentru a vedea certificate pe baza expirării vă permite să determinaţi rapid şi uşor care certificate sunt aproape de expirare astfel încât certificatele să poată fi reînnoite într-o manieră temporală.

Pentru a vedea şi a gestiona certificatele utilizator pe baza datelor de expirare, 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 navigaţie, selectaţi **Gestionare certificate utilizator** pentru a afişa o listă de task-uri. **Notă:** Dacă lucraţi curent cu un depozit de certificate, selectaţi **Gestionare certificate** pentru a afişa o listă de task-uri, apoi selectaţi **Verificare expirare** şi selectaţi **Utilizator**.
3. Dacă profilul utilizator al dumneavoastră are autorizările speciale *ALLOBJ şi *SECADM, puteţi selecta o metodă pentru a alege care certificate utilizator să le vedeţi şi să le gestionaţi pe baza datelor lor de expirare. (Dacă profilul utilizator al dumneavoastră nu are aceste autorizări speciale, DCM vă cere să specificaţi intervalul datei de expirare aşa cum este descris în pasul următor.) Puteţi selecta unul din următoarele:
   - **Profil utilizator** pentru a vedea şi gestiona certificatele utilizator care sunt asignate un profil utilizator OS/400 specific. Specificaţi un **Nume profil utilizator** şi faceţi clic pe **Continuare**. **Notă:** Puteţi specifica un profil utilizator altul decât al dumneavoastră dacă aveţi autorizările speciale *ALLOBJ şi *SECADM.
   - **Toate certificatele utilizator** pentru a vedea şi a gestiona certificatele pentru toate identităţile utilizator.
4. În câmpul **Interval dată expirare în zile (1-365)**, introduceţi numărul de zile pentru care să vedeţi certificatele utilizator pe baza datei lor de expirare şi faceţi clic pe **Continuare**. DCM afişează toate certificatele utilizator pentru profilul utilizator specificat care expiră între data de astăzi şi data care se potriveşte numărului de zile specificat. DCM afişează de asemenea toate certificatele utilizator care au datele de expirare înainte de data de astăzi.
5. Selectaţi un certificat utilizator pentru gestionare. Puteţi alege să vedeţi detalii despre informaţiile certificatului sau să-l înlăturaţi din identitatea utilizator asociată.
6. Când terminaţi de lucrat cu certificatele din listă, faceţi clic pe **Anulare** pentru a ieşi din task.

Folosirea API-urilor 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 dumneavoastră. Local pentru a emite certificate către utilizatori, aceste certificate erau automat asociate cu profilurile lor utilizator iSeries . În consecinţă, pentru a folosi CA-ul 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 Locale 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 profilurilor de utilizator către aceşti utilizatori, aţi putea cere acestora să plătească pentru un certificat de la un CA binecunoscut dacă aţi dorit să cereţi certificate pentru autentificarea utilizatorului pentru aplicaţiile dumneavoastră.

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.

Sunt două API-uri, câte unul pentru fiecare program browser predominant, pe care le puteţi apela la folosirea Net.Data pentru a crea un program pentru emiterea certificatelor către utilizatori. Aplicaţia pe care o creaţi trebuie să dispună de codul GUI (interfaţă utilizator grafică) necesar pentru a crea certificatul utilizator şi pentru a apela unul din API-urile corespunzătoare pentru a folosi CA-ul 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 public din Internet, browser-ul dumneavoastră sau alt software client ar putea avea deja o copie a certificatului CA. Însă dacă 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 direct în browser-ul dumneavoastră sau puteţi copia certificatul CA local într-un fişier astfel încât alt software client să-l poată accesa şi folosi. Dacă folosiţi atât browser-ul 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 necesită să vă autentificaţi prezentând un certificat de la CA-ul local, trebuie să descărcaţi certificatul CA local în browser-ul dumneavoastră înainte de a cere un certificat de utilizator de la CA-ul local.

Pentru a folosi DCM ca să obţineţi o copie a certificatului CA local, urmaţi aceşti paşi:
1. Porniţi DCM.
2. În cadrul de navigare, selectaţi **Instalarea certificatului CA local pe PC-ul dumneavoastră** pentru a afişa o pagină care vă permite să descărcaţi certificatul CA local în browser-ul 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 browser-ul 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 trebuie să lipiţi (paste) aceste informaţii 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.

Gestionarea certificatelor 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 un CA public din Internet, cum ar fi VeriSign. De exemplu, operaţi un sit Web public şi vreţi să folosiţi SSL (Secure Sockets Layer) pentru sesiuni de comunicaţie sigure pentru a asigura protejarea anumitor tranzacţii de informaţii. Din cauză că situl Web este disponibil publicului larg, vreţi să folosiţi certificate pe care majoritatea browser-elor Web le recunosc la citire.

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 dumneavoastră 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 un CA public din 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).

Gestionarea certificatelor 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 CA-ul dumneavoastră local, 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 alt CA din Internet** ca semnatar al noului certificat şi faceţi clic pe **Continuare** pentru a afişa un formular care vă permite să introduceţi informaţiile de identificare pentru noul certificat.

   Notă: Dacă pe server este instalat IBM Cryptographic Coprocessor, DCM vă permite să selectaţi cum să memoraţi cheia privată pentru certificat ca task-ul 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 public 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 configuraţi serverul dumneavoastră Web înainte de a gestiona 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 faceţi o notă a acestui ID aplicaţie astfel încât să folosiţi DCM pentru a specifica care certificat trebuie să fie utilizat de această aplicaţie pentru SSL.

   Nu terminaţi şi reporniţi serverul până nu folosiţi DCM să asigneze certificatul complet semnat către server. Dacă opriţi şi reporniţi instanţa *ADMIN a serverului Web înainte de a-i asigna un certificat, serverul nu va porni şi nu veţi putea folosi DCM pentru a asigna un certificat serverului.
8. Porniţi DCM după ce CA public 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 terminaţi de importat certificatul, puteţi specifica aplicaţiile care trebuie să-l folosească pentru comunicaţii 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 un 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 un CA din Internet binecunoscut, s-ar putea ca software-ul utilizatorilor să aibă deja o copie a certificatului CA necesar. Dacă utilizatorii trebuie să obţină certificatul CA, trebuie să acceseze situl Web pentru CA şi să urmeze instrucţiunile pe care acesta le furnizează.

Gestionarea certificatelor 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 propriul dumneavoastră CA (Certificate Authority) local, 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 Internet publică 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 de navigaţie stâng al DCM, selectaţi **Creare depozit de certificate nou** pentru a porni task-ul ghidat şi a efectua 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 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 public 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 public vă întoarce certificatul semnat.
9. În cadrul de nevigaţie stâng, faceţi clic pe **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** ca depozitul de certificate care va fi deschis.
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 cadrul de navigare din stânga se reîmrospătează, selectaţi **Gestionare aplicaţii** pentru a afişa o listă a task-urilor.
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**.

Când terminaţi aceste task-uri, aveţi tot ce vă trebuie pentru a 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. Trebuie să furnizaţi o copie a acestui certificat ca parte a pachetului obiectelor 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 obiectele cu un certificat de la un CA binecunoscut, versiunea DCM a receptorului ar putea avea deja o copie a certificatului CA necesar. Totuşi, aţi putea furniza o copie a certificatului CA împreună cu obiectele semnate dacă vă gândiţi că receptorul s-ar putea să nu aibă o copie. De exemplu, trebuie să furnizaţi o copie a certificatului CA local dacă aţi semnat obiectele cu un certificat de la un CA local privat. Din motive de securitate, trebuie să furnizaţi certificatul CA într-un pachet separat sau să faceţi public certificatul CA disponibil la cererea tuturor celor care au nevoie de el.

Gestionarea certificatelor 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 însă obiectul a fost semnat de un certificat de la alt CA public sau de la un CA local privat, trebuie să obţineţi o copie a certificatului CA 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 de navigaţie stâng al DCM, selectaţi **Creare depozit de certificate nou** pentru a porni task-ul ghidat şi a efectua o serie de formulare.

   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 vreţi să folosiţi certificatele de semnare obiect existente pentru a verifica semnăturile, selectaţi **Da** şi faceţi clic pe **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. Pe măsură ce creaţi certificate noi de semnare obiecte, trebuie să le exportaţi din depozitul de certificate *OBJECTSIGNING în acest depozit. Dacă nu le exportaţi, nu veţi putea verifica semnăturile pe care le-aţi creat cu ele.

   Notă: Dacă aţi creat acest depozit de certificate astfel încât să puteţi verifica semnăturile de pe obiecte pe care le-aţi primit din alte surse, trebuie să continuaţi cu această procedură astfel încât să puteţi importa certificatele de care aveţi nevoie în depozit.
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 CA pentru CA-ul care a emis certificatul de verificare semnături, trebuie să importaţi certificatul CA *mai întâi*. Aţi putea primi o eroare dacă nu importaţi certificatul CA înainte de importarea certificatului de verificare a semnăturii.

Puteţi folosi aceste certificate pentru a verifica semnăturile obiectelor.

Capitolul 8. Gestionare DCM

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

Utilizare CA local pentru a emite certificate pentru alte sisteme iSeries
Aflaţi cum se foloseşte un CA local privat de pe un sistem pentru a emite certificate folosite pe alte sisteme.

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.

Gestionare certificate după expirare
Învăţaţi cum să folosiţi DCM pentru a vedea şi gestiona certificate pe baza detei lor de expirare.

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.

Memorare chei certificate pe un coprocesor criptografic IBM
Aflaţi cum să folosiţi un coprocesor instalat pentru a furniza depozite mai sigure pentru cheile private ale certificatelor dumneavoastră.

Gestionarea localizării cererii pentru un CA PKIX
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).

Gestionare locaţie LDAP pentru certificate utilizator
Învăţaţi cum să configuraţi DCM să memoreze certificate utilizator într-o locaţie director a serverului LDAP (Lightweight Directory Access Protocol) pentru a extinde Enterprise Identity Mapping să lucreze cu certificate utilizator.

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.

Folosirea unui CA local pentru a emite certificate pentru alte sisteme iSeries

Este posibil să folosiţi deja un CA local privat pe un server din reţea. Acum, doriţi să extindeţi folosirea acestui CA local la alt server din reţeaua dumneavoastră. De exemplu, doriţi să faceţi CA-ul local curent să emită certificate de server sau de client pentru ca o aplicaţie de pe alt server să folosească sesiuni de comunicaţie SSL. Sau doriţi să folosiţi certificate de la CA-ul dumneavoastră local de pe un sistem pentru semnarea obiectelor pe care le aveţi stocate pe alt server.

Acest obiectiv poate fi atins folosind DCM. Executaţi unele task-uri pe serverul pe care operează CA-ul local şi executaţi altele pe serverul secundar, care găzduieşte aplicaţiile pentru care doriţi să emiteţi certificate. Acest sistem secundar este denumit sistemul destinaţie. Task-urile pe care trebuie să le realizaţi pe sistemul destinaţie depind de versiunea acelui sistem.

Notă: Pot apărea probleme dacă serverul pe care operează CA-ul local foloseşte un produs Cryptographic Access Provider care asigură o criptare mai puternică decât sistemul destinaţie. Pentru V5R2 sau versiunile ulterioare de OS/400 sau i5/OS, singurul furnizor de acces criptografic este 5722–AC3, care este cel mai puternic produs disponibil. Totuşi, în ediţiile anterioare, puteaţi instala alte produse de furnizare de acces criptografic mai slabe (5722–AC1 sau 5722–AC2) care furnizau funcţii criptografice de nivel mai slab. Când exportaţi certificatul (cu cheia sa privată), sistemul criptează 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 dumneavoastră 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-ul local pentru a crea un certificat ce este folosit pe alt server, fişierele pe care le creează DCM conţin o copie a certificatului CA local, precum şi copii ale certificatelor pentru numeroase CA-uri publice din Internet.

Task-urile pe care trebuie să le realizaţi în DCM diferă puţin în funcţie de tipul de certificat pe care CA-ul dumneavoastră local îl emite şi de versiunea şi de condiţiile de pe sistemul destinaţie.

Emiterea certificatelor private pentru utilizarea pe alt sistem V5R3, V5R2 sau V5R1

Pentru a folosi CA-ul local la emiterea certificatelor folosite pe alt sistem V5R3, V5R2 sau V5R1, parcurgeţi paşii următori pe sistemul V5R3 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-ul local.

   Nu este nevoie să deschideţi un depozit de certificate pentru a realiza acest task. Aceste instrucţiuni presupun fie că nu lucraţi în cadrul unui depozit de certificate specific, fie că lucraţi în depozitul de certificate CA local. Pentru a realiza aceste task-uri, trebuie să existe un CA local pe acest sistem.
3. Selectaţi tipul de certificat pe care doriţi să îl emită CA-ul local şi apăsaţi **Continuare** pentru a porni task-ul asistat şi completaţi o serie de formulare. Selectaţi crearea unui **certificat de server sau de client pentru alt sistem** (pentru sesiuni SSL) sau a unui **certificat de semnare a obiectelor pentru alt sistem**.

   Notă: Când creaţi un certificat de semnare a obiectelor pentru a fi folosit de alt sistem, pe sistemul respectiv trebuie să ruleze V5R1 sau o versiune ulterioară de OS/400 sau i5/OS pentru a folosi certificatul. Deoarece sistemul destinaţie trebuie să aibă V5R1 sau mai recentă, DCM de pe sistemul gazdă local nu vă cere să selectaţi un format de eliberare destinaţie pentru noul certificat de semnare obiecte.
4. Când creaţi un certificat de server sau de client, selectaţi nivelul de ediţie al serverului pentru care creaţi certificatul respectiv. 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 vă asigură că fişierele certificatului sunt compatibile cu serverul 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 dumneavoastră 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.

Emiterea certificatelor private pentru utilizarea pe un server V4R5

Pentru a folosi CA-ul local la emiterea certificatelor folosite pe un server V4R5, parcurgeţi paşii următori pe sistemul V5R3 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-ul local.

   Nu este nevoie să deschideţi un depozit de certificate pentru a realiza 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. Pentru a realiza aceste task-uri, trebuie să existe un CA local pe acest sistem.

3. Selectaţi **Certificat de server sau de client pentru alt server** pentru tipul de certificat pe care doriţi să-l emită CA-ul local şi faceţi clic pe **Continuare** pentru a porni task-ul ghidat şi a completa o serie de formulare.

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

4. Selectaţi nivelul de ediţie al serverului pentru care creaţi certificatul. 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 vă asigură că fişierele certificatului sunt compatibile cu serverul 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 dumneavoastră să le transferaţi: un fişier de depozit de certificate (extensia .KDB) şi un fişier cerere (extensia .RDB).

   Notă: Dacă plănuiţi să folosiţi certificatele din aceste fişiere într-un depozit de certificate *SYSTEM existent pe un sistem destinaţie 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, aţi putea numi 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. Utilizaţi FTP (File Transfer Protocol) sau altă metodă pentru a transfera fişierele depozitului de certificate pe care le-aţi creat (.KDB and .RDB) la ssitemul destinaţie V4R5. Folosiţi modul ASCII FTP pentru a transfera fişierul care conţine certificatul CA local exportat.

Folosire fişiere transferate 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:

- Folosire certificat privat pentru sesiuni SSL pe un sistem destinaţie V5R3 sau V5R2
- Folosiţi un certificat privat pentru sesiuni SSL de pe un sistem destinaţie V5R1
- Folosire certificat privat pentru semnare obiecte pe un sistem destinaţie V5R3, V5R2 sau V5R1
- Folosire certificat privat pentru sesiuni SSL pe un sistem destinaţie V4R5

Folosirea certificatului privat pentru sesiuni SSL pe un sistem destinaţie V5R3 sau V5R2

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 V5R3 sau V5R2 pentru a gestiona certificate pentru SSL, atunci acest depozit de certificate nu va exista pe sistemul destinaţie. Task-urile 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 nu există pe sistemul destinaţie V5R3 sau V5R2, puteţi folosi fişierele certificat tranferate în unul din 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 V5R3 sau V5R2 pe care vreţi să utilizaţi fişierele depozitului de certificate transferate, le puteţi folosi ca depozitul de certificate *SYSTEM. Pentru a crea depozitul de certificate *SYSTEM şi a folosi fişierele certificate pe sistemul dumneavoastră destinaţie V5R3 sau 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 dumneavoastră 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 trebuie să redenumiţi fişierele transferate aşa cum a fost sugerat. 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 au nume unice şi trebuie să utilizaţi depozitul de certificate transferat ca un **alt depozit de certificate sistem**. Dacă folosiţi fişierele ca un alt depozit de certificate sistem, nu puteţi utiliza DCM pentru a specifica care aplicaţii vor folosi 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 dumneavoastră 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 este afişată pagina Depozit de certificate şi parolă, furnizaţi parola pe care aţi specificat-o pe sistemul *gazdă* pentru depozitul de certificate când aţi creat certificatul pentru sistemul destinaţie V5R3 sau V5R2 şi faceţi clic pe **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 care aplicaţii vor folosi 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 este afişată pagina **Depozit de certificate şi parolă**, furnizaţi noua parolă şi faceţi clic pe **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 vor folosi certificatul pentru sesiuni SSL şi faceţi clic pe **Continuare**. DCM afişează un mesaj pentru a confirma selecţia certificatului dumneavoastră 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 un 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 task-uri completate, aplicaţiile de pe sistemul destinaţie pot folosi certificatul emis de CA-ul local pe alt server. 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 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 alt depozit de certificate sistem

Dacă sistemul destinaţie V5R3 sau V5R2 are deja un depozit de certificate *SYSTEM, trebuie să decideţi cum să lucraţi cu fişierele certificat pe care le-aţi transferat pe sistemul destinaţie. 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 Alte depozite de certificate sistem vă permite să gestionaţi certificate pentru aplicaţiile pe care dumneavoastră 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 alt depozit de certificate sistem, nu puteţi folosi DCM pentru a specifica care aplicaţii vor folosi certificatul pentru sesiuni SSL. În consecinţă, nu puteţi configura aplicaţiile standard activate pentru SSL să folosească acest certificat. Dacă doriţi să folosiţi certificatul pentru aplicaţii iSeries, trebuie să importaţi certificatul din fişierele transferate ale depozitului dumneavoastră 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 dumneavoastră 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 este afişată pagina **Depozit de certificate şi parolă**, furnizaţi numele cale şi numele fişier complet calificate fişierului depozit de certificate, furnizaţi noua parolă şi faceţi clic pe **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 certificatele din depozitul de certificate *SYSTEM existent

| Puteţi folosi certificatele din fişierele depozitului de certificate într-un depozit *SYSTEM existent pe un sistem V5R3
| sau 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 dumneavoastră 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 este afişată pagina **Depozit de certificate şi parolă**, furnizaţi numele cale şi numele fişier complet calificate fişierului depozit de certificate, furnizaţi noua parolă şi faceţi clic pe **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: Trebuie să exportaţi certificatul CA local în depozitul de certificate înainte să exportaţi certificatul client sau server în depozit. 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. Re-selectaţi task-ul**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 vor folosi certificatul pentru sesiuni SSL şi faceţi clic pe **Continuare**. DCM afişează un mesaj pentru a confirma selecţia certificatului dumneavoastră 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 un 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 task-uri 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.

Folosirea unui 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, atunci acest depozit de certificate nu va exista pe sistemul destinaţie. Task-urile 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 dumneavoastră 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 dumneavoastră 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 trebuie să redenumiţi fişierele transferate aşa cum a fost sugerat. 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 au nume unice şi trebuie să utilizaţi depozitul de certificate transferat ca un **alt depozit de certificate sistem**. Dacă folosiţi fişierele ca un alt depozit de certificate sistem, nu puteţi utiliza DCM pentru a specifica care aplicaţii vor folosi 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 dumneavoastră 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 care aplicaţii vor folosi 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-ul 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 un 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 task-uri completate, aplicaţiile de pe sistemul destinaţie pot folosi certificatul emis de CA-ul 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 alt depozit de certificate 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.

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 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 dumneavoastră 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 alt depozit de certificate sistem, nu puteţi folosi DCM pentru a specifica care aplicaţii vor folosi 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 dumneavoastră 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 dumneavoastră 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 certificatele din depozitul de certificate *SYSTEM existent

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 dumneavoastră 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: Trebuie să exportaţi certificatul CA local în depozitul de certificate înainte să exportaţi certificatul client sau server în depozit. 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. Re-selectaţi task-ul**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 un 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 task-uri 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.

Folosirea certificat primar pentru semnarea obiectelor pe un sistem destinaţie V5R3, 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 V5R1 pentru a gestiona certificate pentru semnarea obiectelor, atunci acest depozit de certificate nu va exista pe sistemul destinaţie. Task-urile 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

Task-urile 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 în sistemul destinaţie V5R3, V5R2 sau V5R1 cu fişierele depozitului de certificate transferat, 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 dumneavoastră 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 trebuie să redenumiţi fişierele transferate aşa cum a fost sugerat. Suprascrierea fişierelor care semnează obiecte implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat şi a conţinutului său. Când depozitul de certificate *OBJECTSIGNING există deja,, trebuie să folosiţi un proces diferit pentru a obţine certificatele în depozitul de certificate existent.
3. Porniţi DCM. Trebuie să modificaţi parola pentru depozitul de certificate *OBJECTSIGNING. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dumneavoastră 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-ul 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 V5R3, V5R2 sau V5R1 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. Trebuie 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 obiectele cu un certificat de la un CA binecunoscut din Internet, versiunea de DCM a primitorului va avea 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 este necesar. De exemplu, trebuie să furnizaţi o copie a certificatului CA local dacă aţi semnat obiectele cu un certificat de la un CA local. Din motive de securitate, trebuie să furnizaţi certificatul CA într-un pachet separat sau să faceţi public certificatul CA disponibil la cererea tuturor celor care au nevoie de el.

Depozitul de certificate *OBJECTSIGNING există

| Puteţi folosi certificatele din fişierele depozitului de certificate într-un depozit *OBJECTSIGNING existent pe un
| sistem V5R3, 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 *OBJECTSIGNING existent deschizând
| fişierele transferate ca un alt depozit de certificate sistem pe sistemul destinaţie V5R3, 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, efectuaţi aceşti paşi pe sistemul destinaţie V5R3, 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 dumneavoastră 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 task-ul 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: Trebuie să exportaţi certificatul CA local în depozitul de certificate înainte să exportaţi certificatul semnare obiect în depozit. 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 depozit de certificate destinaţie, introduceţi parola pentru depozitul de certificate *OBJECTSIGNING şi faceţi clic pe **Continuare**.
12. Acum puteţi exporta certificatul care semnează obiecte în depozitul de certificate *OBJECTSIGNING. Re-selectaţi task-ul**Exportare certificat**.
13. Selectaţi **Server sau client** ca tipul de certificat de exportat şi apăsaţi **Continuare**.
14. Selectaţi certificatul corespunzător pentru export şi faceţi clic pe **Exportare**.
15. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
16. Introduceţi *OBJECTSIGNING ca depozit de certificate destinaţie, introduceţi parola pentru depozitul de certificate *OBJECTSIGNING şi faceţi clic pe **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.

Utilizarea certificatului privat pentru sesiuni SSL pe un sistem destinaţie V4R5

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 V4R5 pentru a gestiona certificate pentru SSL, atunci acest depozit de certificate nu va exista 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.

Task-urile 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 pe care doriţi să folosiţi fişierele depozit de certificate transferate, 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 dumneavoastră 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 trebuie să redenumiţi fişierele transferate aşa cum a fost sugerat. 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 au nume unice şi trebuie să utilizaţi depozitul de certificate transferat ca un **alt** depozit de certificate sistem. Dacă folosiţi fişierele ca un alt depozit de certificate sistem, nu puteţi utiliza DCM pentru a specifica care aplicaţii vor folosi certificatul.

3. Porniţi DCM. Trebuie să modificaţi parola pentru depozitul de certificate *SYSTEM. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dumneavoastră 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 task-uri 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. Dintr-o listă de aplicaţii, selectaţi aplicaţia care va folosi certificatul privat transferat pentru sesiuni SSL.
9. Apăsaţi **Lucru cu certificate sistem** şi selectaţi certificatul pe care l-a emis CA-ul 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 un anumit CA. 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-ul 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 un CA care nu este specificat ca fiind de încredere, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.

| Cu aceste task-uri efectuate, aplicaţiile pe sistemul destinaţie V4R5 pot folosi certificatul emis de CA-ul local V5R3 pe
| un 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 alt depozit de certificate sistem

| Dacă sistemul destinaţie V4R5 sau V5R2 are deja un depozit de certificate *SYSTEM, trebuie să decideţi cum să
| lucraţi cu fişierele certificat pe care le-aţi transferat pe sistemul destinaţie. 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 specfiica care aplicaţii vor utiliza 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 dumneavoastră 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 pe care doriţi să folosiţi fişierele depozit de certificate
| transferate, 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 dumneavoastră 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 task-uri 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 dumneavoastră 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 — importând fişierele într-un depozitul de certificate *SYSTEM existent

| Înainte să puteţi importa certificatele în *SYSTEM pe un sistem destinaţie V4R5, trebuie mai întâi să exportaţi
| certificatele din depozitul 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 nu sunt la fel de bine dezvoltate ca cele pentru V5R3 şi aţi
| putea avea probleme dacă folosiţi sistemul destinaţie pentru a exporta certificatul CA local. În consecinţă,
| trebuie să folosiţi sistemul gazdă V5R3 pentru a exporta o copie *suplimentară* a certificatului CA local într-un
| fişier separat mai degrabă decât să folosiţi sistemul destinaţie V4R5 pentru a-l exporta. După ce exportaţi
| certificatul CA local pe sistemul gazdă V5R3, puteţi să transferaţi manual fişierul de export al certificatului CA
| local pe sistemul destinaţie V4R5 şi să urmaţi paşii furnizaţi mai departe în această procedură pentru a importa
| certificatul CA local în depozitul *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 exporta certificatul din fişierele depozitului de certificate, efectuaţi aceşti paşi pe sistemul destinaţie 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 task-uri 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 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 dumneavoastră 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, aţi putea numi 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 moment, trebuie să fi folosit DCM pe sistemul gazdă V5R3 original pentru a exporta orice copie suplimentară
| a certificatului CA local şi aţi transferat-o manual în mod ASCII la sistemul destinaţie V4R5. De asemenea trebuie să fi
| folosit DCM pe acest sistem destinaţie pentru a exporta certificatul server sau client privat 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 importa certificatele din aceste fişiere export şi pentru a specifica că le folosesc aplicaţii activate SSL,
| efectuaţi aceşti paşi pe sistemul ţintă V4R5:

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 task-uri 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 crea pe sistemul gazdă V5R3. 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 un anumit CA. 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 un CA care nu este specificat ca fiind de încredere, aplicaţia nu îl va accepta ca bază pentru o autentificare validă.
6. Selectaţi aplicaţiile care vor avea încredere în certificatul CA şi faceţi clic pe **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 Importare certificat şi faceţi clic pe **OK** pentru a vă întoarce la pagina **Lucrul cu 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 l-aţi importat va apărea şi în lista de certificate.

10. Acum trebuie să specificaţi care aplicaţii vor folosi certificatul privat importat pentru 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 task-uri completate, aplicaţiile de pe sistemul destinaţie V4R5 pot folosi certificatul emis de CA-ul local pe alt server. 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.

Gestionarea aplicaţiilor 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). Task-urile 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.

Gestionare asignare certificat pentru o aplicaţie descrie cum să asignaţi sau să modificaţi certificatul pe care îl foloseşte o aplicaţie pentru a stabili o sesiune SSL sau pentru a semna obiecte.

Definite listă CA de încredere pentru o aplicaţie descrie când puteţi şi este nevoie să definiţi în care Autorităţi certificate poate avea încredere o aplicaţie pentru validarea şi acceptarea certificatelor.

Puteţi găsi informaţii despre alte task-uri 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 activate pentru SSL sunt înregistrate în DCM, aşa că puteţi să folosiţi cu uşurinţă DCM pentru a le asigna un certificat 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, definiţia aplicaţiei pe care o creaţi ar putea descrie tipul sau grupul de obiecte pe care intenţionaţi să le 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 ajutor online.
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 ajutor online.
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 un 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.

Când modificaţi sau ştergeţi un certificat pentru o aplicaţie, aceasta poate să nu recunoască modificările dacă rulează în momentul modificării atribuirii certificatului. De exemplu, serverele iSeries Acces pentru Windows vor aplica orice modificări faceţi automat. 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 task-ul 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 un 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.

Atunci când adăugaţi un 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 ajutor online.
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 aplicaţia va avea încredere şi faceţi clic pe **OK**. DCM va afişa un mesaj pentru a confirma selecţiile pentru lista de încredere.

   Notă: Puteţi fie să selectaţi CA-uri individuale din listă sau să specificaţi că aplicaţia va avea încredere în toate sau în nici unul din CA-urile din listă. De asemenea, puteţi vizualiza sau valida certificatele CA înainte de a le adăuga listei de încredere.

Gestionarea certificatelor prin expirare

DCM (Digital Certificate Manager) oferă suport pentru gestionarea expirării certificatelor, pentru a permite administratorilor să gestioneze certificatele de server sau de client, certificatele de semnare a obiectelor şi certificatele de utilizator în funcţie de data expirării pe serverul local. În plus, dacă configuraţi DCM să lucreze cu EIM (Enterprise Identity Mapping), puteţi gestiona certificate utilizator după data expirării în întreprindere.

Folosirea DCM pentru a vedea certificate pe baza expirării vă permite să determinaţi rapid şi uşor care certificate sunt aproape de expirare astfel încât certificatele să poată fi reînnoite într-o manieră temporală.

Notă: Deoarece puteţi folosi un certificat de verificare a semnăturii pentru a verifica semnăturile obiectelor chiar şi când certificatul este expirat, DCM nu furnizează suport pentru verificarea expirării acestor certificate.

Pentru a vedea şi a gestiona certificatele server şi client sau certificate semnare obiecte pe baza datelor lor de expirare, 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 **Verificare expirare**.
6. Selectaţi tipul certificatului pe care vreţi să-l verificaţi. Dacă sunteţi în depozitul de certificate *SYSTEM, selectaţi **Server sau client**; dacă sunteţi în depozitul de certificate *OBJECTSIGNING, selectaţi **Semnare obiect**.
7. În câmpul **Interval dată expirare în zile (1-365)**, introduceţi numărul de zile pentru care să vedeţi certificatele pe baza datei lor de expirare şi faceţi clic pe **Continuare**. DCM afişează toate certificatele care expiră între data de astăzi şi data care se potriveşte numărului de zile specificat. DCM afişează de asemenea toate certificatele care au datele de expirare înainte de data de astăzi.
8. Selectaţi un certificat pe care vreţi să-l gestionaţi. Puteţi alege să vedeţi detalii despre informaţiile certificatului,să-l ştergeţi sau să-l reînnoiţi.
9. Când terminaţi de lucrat cu certificatele din listă, faceţi clic pe **Anulare** pentru a ieşi.

Validare certificatelor şi aplicaţiilor

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 ar putea împiedica o aplicaţie de la participarea cu succes într-o sesiune SSL (Secure Sockets Layer) sau de la semnarea cu succes a obiectelor.

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 dumneavoastră 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 un anumit CA, 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 un anumit CA, 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 **Adăugare locaţie CRL** din lista de task-uri pentru a afişa un formular pe care îl puteţi folosi pentru a descrie locaţia CRL şi cum DCM sau aplicaţia vor accesa locaţia.

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 un anumit CA.
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 un anumit CA, 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 atât serverul director (LDAP) şi aplicaţiile client să utilizeze SSL cât şi să asignaţi un certificat aplicaţiilor din DCM.

Pentru a învăţa mai multe despre configurarea şi utilizarea serverului director (LDAP) iSeries, revedeţi aceste subiecte din Centrul de informare:

- Server director IBM pentru iSeries (LDAP)
  Acest subiect vă spune tot ce aveţi nevoie să ştiţi despre configurarea şi utilizarea unui server director iSeries.
- Activare SSL pe serverul director
  Acest subiect expică ce trebuie să faceţi pentru a configura serverul dumneavoastră director să utilizeze SSL pentru comunicaţii sigure.

Memorarea cheilor certificatului pe un coprocesor criptografic IBM

Dacă aveţi un coprocesor criptografic IBM instalat pe iSeries-uldumneavoastră, îl puteţi folosi pentru a furniza o memorare mai sigură pentru o cheie privată a certificatului. Puteţi folosi coprocesorul pentru a stoca cheia privată pentru un certificat server, unul client sau pentru un certificat CA local. 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 memorarea cheii private, trebuie să vă asiguraţi că coprocesorul este activ 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 dumneavoastră 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 dumneavoastră creaţi sau reînnoiţi un CA local, selectaţi opţiunea de depozitare a cheii private ca prim pas al procesului.

Stocarea cheii private a certificatului direct pe coprocesor

Pentru a proteja mai mult accesul la şi utilizarea unei chei private a certificatului, puteţi alege să memoraţi cheia direct pe un coprocesor criptografic IBM. 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 master a coprocesorului pentru a cripta cheia privată a certificatului

Pentru a proteja mai mult accesul la şi utilizarea unei chei private a certificatului, puteţi folosi cheia master a unui coprocesor criptografic IBM pentru a cripta cheia privată şi a o memora 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 această opţiune cu succes, trebuie să folosiţi interfaţa de configurare Web a coprocesorului criptografic IBM pentru a crea un fişier de memorare a cheii corespunzător. De asemenea, trebuie să folosiţi interfaţa de configurare Web a coprocesorului pentru a asocia fişierul de stocare al cheii cu descrierea dispozitivului pe care doriţi să îl folosiţi. Puteţi accesa interfaţa de configurare Web a coprocesorului din pagina Task-uri 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 că cheia master este aceeaşi pe dispozitive, folosiţi task-ul de verificare a cheii master din interfaţa de configurare Web a coprocesorului criptografic 4758. Puteţi accesa interfaţa de configurare Web a coprocesorului din pagina Task-uri 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 un CA PKIX

O Autoritate de certificare PKIX (Public Key Infrastructure for X.509) este un CA care emite certificate pe baza celor mai noi standarde Internet X.509 pentru implementarea unei infrastructuri cheie publică. Standardele PKIX sunt subliniate în RFC (cereri pentru comentarii) 2560.

Un 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 solicitant furnizează dovada identităţii pe care o cere RA, acesta certifică identitatea solicitantului. Ori RA-ul ori solicitantul, în funcţie de procedura autorităţii de certificare, trimite aplicaţia certificată către CA-ul asociat. Pe măsură ce aceste standarde sunt adoptate mai larg, CA-uri compatibile PKIX vor deveni disponibile pe scară mai largă. Aţi putea să investigaţi folosirea unui CA flexibil PKIX dacă nevoile dumneavoastră de securitate cer control strict al accesului la resurse pe care aplicaţiile activate SSL le furnizează utilizatorilor. De exemplu, Lotus Domino oferă un CA PKIX 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 un CA PKIX. Dacă faceţi acest lucru DCM (Digital Certificate Manager) va fi configurat pentru a furniza un CA PKIX ca o opţiune pentru a se obţine certificate semnate.

Pentru a folosi DCM pentru gestionarea certificatelor provenite de la un 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 task-ul **Creare Certificat**.

Gestionarea locaţiei LDAP pentru certificate utilizator

Implicit, DCM (Digital Certificate Manager) stochează certificatele de utilizator pe care le emite CA-ul local împreună cu profilurile de utilizator i5/OS. Totuşi, puteţi configura DCM (Digital Certificate Manager) în conjuncţie cu EIM (Enterprise Identity Mapping) astfel încât când Autoritatea de certificare (CA) emite certificate utilizator, copia publică a certificatului este memorată într-o locaţie director specifică a serverului LDAP (Lightweight Directory Access Protocol). O configuraţie combinată de EIM cu DCM vă permite să memoraţi certifiate utilizator într-o locaţie director LDAP pentru a face certificatele mai disponibile la citire pentru alte aplicaţii. Configuraţia combinată vă permite de asemenea să folosiţi EIM pentru a gestiona certificate utilizator ca un tip de identitate utilizator în interiorul întreprinderii dumneavoastră.

Notă: Dacă vreţi ca un utilizator să memoreze un certificat de la un CA diferit în locaţia LDAP, utilizatorul trebuie să efectueze task-ul **Asignare certificat utilizator**.

EIM este o tehnologie eServer care vă permite să gestionaţi identităţile de utilizator în întrepinderea dumneavoastră, inclusiv profilurile de utilizator i5/OS şi certificatele de utilizator. Dacă vreţi să folosiţi EIM pentru a gestiona certificate utilizato, este nevoie să realizaţi aceste task-uri de configurare EIM înainte de a realiza orice task-uri de configurare:

1. Folosiţi vrăjitorul **Configuraţie EIM** din Navigatorul **iSeries** pentru a configura EIM.
2. Creaţi un identificator EIM pentru fiecare utilizator care vreţi să participe la EIM.
3. Creaţi o asociaţie destinaţie între fiecare identificator EIM şi profilul de utilizator al acelui utilizator în registrul de utilizatorilocal i5/OS. Folosiţi numele de definiţie din registrul EIM pentru registrul de utilizatorii5/OS local pe care l-aţi specificat în vrăjitorul **Configurare EIM**. **Notă:** Pentru informaţii suplimentare despre configurarea EIM, vedeţi subiectul EIM din Centrul de informare iSeries.

După ce realizaţi task-urile de configurare EIM necesare, trebuie să efectuaţi următoarele task-uri pentru a termina configurarea generală pentru folosirea EIM şi DCM împreună:

1. În DCM, folosiţi task-ul **Gestionare locaţie LDAP** pentru a specifica directorul LDAP pe care DCM îl va folosi automat pentru a memora un certificat utilizator pe care îl creează CA-ul local. Nu este necesar ca locaţia LDAP să fie pe serverul local şi nici să fie pe serverul LDAP pe care îl foloseşte EIM. Când configuraţi locaţia LDAP în DCM, acesta foloseşte directorul LDAP specificat pentru a memora toate certificatele utilizator pe care le emite CA-ul local. DCM utilizează de asemenea locaţie LDAP pentru a memora certificate utilizator procesate de task-ul **Asignare certificat utilizator** în loc să memoreze certificatul cu un profil utilizator.
2. Rulaţi comanda **Convertire certificate utilizator** (CVTUSRCERT). Această comandă copiază certificatele utilizator existente în locaţia director LDAP corespunzătoare. Totuşi, comanda doar copiază certificatele pentru un utilizator care a avut o asociaţie destinaţie creată între un identificator EIM şi profilul utilizator. Comanda crează apoi o asociaţie sursă între fiecare certificat şi identificatorul EIM asociat. Comanda foloseşte numele distinctiv (DN) al subiectului certificatului , DN emitent şi un hash al acestor DN-uri împreună cu cheia publică a certificatului pentru a defini numele identităţii utilizator pentru asociaţia sursă.

Semnarea obiectelor

Sunt trei metode pe care le puteţi folosi pentru semnarea obiectelor. Puteţi scrie un program care apelează API-ul de semnare obiect. Puteţi folosi Digital Certificate Manager (DCM) pentru a semna obiecte. Sau, începând cu V5R2, puteţi folosi din Navigator iSeries caracteristica Administrare centrală pentru a semna obiectele pe măsură ce le împachetaţi pentru a le distribui pe alte servere.

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 fişier salvare). Nou în V5R2, puteţi de asemenea să semnaţi obiecte comandă (*CMD). Nu puteţi semna obiecte care sunt stocate pe alte servere.

Puteţi semna obiecte cu certificate pe care le cumpăraţi de la un CA public 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 preliminarii pentru semnarea 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 public din Internet.
- Depozitul de certificate *OBJECTSIGNING trebuie să conţină cel puţin un certificat, fie unul pe care l-aţi creat folosind CA-ul local, fie unul pe care l-aţi obţinut de la un CA public din Internet.
- Pentru semnarea obiectelor, trebuie să fi creat o definiţie de aplicaţie pentru semnarea obiectelor.
- Trebuie să fi asignat un certificat către aplicaţia de semnare a obiectelor pe care intenţionaţi 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. Puteţi de asemenea să folosiţi anumite caractere de înlocuire pentru a descrie partea din catalog pe care doriţi să o semnaţi. Aceste caractere de înlocuire 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 /mydirectory/*; pentru a semna toate programele dintr-o bibliotecă specifică, aţi putea introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteţi folosi aceste caractere de înlocuire doar în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă vreţi să folosiţi funcţia Răsfoire pentru a vedea o listă de conţinut al bibliotecii sau directorului, trebuie să introduceţi caracterul de înlocuire ca parte al numelui căii înainte de a face 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.

Verificarea semnăturilor obiectelor

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 de înlocuire pentru a descrie partea din catalog pe care doriţi să o verificaţi. Aceste caractere de înlocuire 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, aţi putea introduce /mydirectory/*; pentru a semna toate programele dintr-o bibliotecă specifică, aţi putea introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteţi folosi aceste caractere de înlocuire doar în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă vreţi să folosiţi funcţia Răsfoire pentru a vedea o listă de conţinut al bibliotecii sau directorului, trebuie să introduceţi caracterul de înlocuire ca parte al numelui căii înainte de a face 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.

Capitolul 9. Depanarea DCM

Când lucraţi cu DCM (Digital Certificate Manager) şi certificate, aţi putea întâlni erori care vă împiedică să realizaţi task-urile şi ţelurile dumneavoastră. Multe din erorile şi problemele comune pe care le-aţi putea întâlni cad într-un număr de categorii, cum ar fi următoarele:

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.

Depanarea problemelor serverului HTTP
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.

Depanare task Asignare 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 de asemenea să căutaţi în Centrul de informare şi pe siturile Web IBM de pe Internet.
Parola pentru CA-ul local 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 dumneavoastră de resetare a parolei când aţi folosit task-ul **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.
	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 Alt depozit de certificate sistem, 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.

Problemă	Soluţie posibilă
	Verificaţi valoarea asignată atributului **Permitere certificate digitale noi** sub opţiunea **Gestionare securitate sistem** a SST (System Service Tools). Dacă acest atribut este setat la valoarea 2 (No), atunci parola depozitului de certificate nu poate fi resetată. Puteţi vedea sau modifica valoarea pentru acest atribut folosind comanda STRSST şi introducând ID-ul utilizator şi parola pentru Uneltele de service . Apoi alegeţi opţiunea **Gestionare securitate sistem**. ID-ul utilizator Service Tools este probabil ID-ul utilizator QSECOFR.
Nu puteţi găsi o sursă pentru un certificat CA ca să-l primiţi pe sistemul dumneavoastră.	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.
Aveţi o problemă cu serverul director (LDAP) cu ar fi asignarea certificatului nu este afişată când informaţiile despre aplicaţia sigură este afişată imediat după asignarea unui certificat. Această problemă apare mai des când este folosit iSeries Navigator pentru a ajunge la un browser Netscape Communications. Preferinţa pentru cache-ul browser-ului este setată să compare documentul din cache cu documentul din reţea **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 un CA extern, 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 serverul dumneavoastră are valoarea corectă pentru offset-ul UTC (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 server. Unele design-uri ale paginilor Web cauzează această problemă. Alte pagini Web sunt proiectate pentru a evita această problemă. Fiţi sigur că comparaţi aspectul certificatului original cu rezultatele lipirii, din moment ce informaţiile lipite trebuie să arate la fel.

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.

Problemă	Soluţie posibilă

Crearea bazei de date de chei a eşuat sau crearea CA-ului local a eşuat.	Verificaţi conflictul numelor de fişiere. Conflictul poate exista la alt fişier decât cel de care întrebaţi. DCM încearcă să protejeze datele utilizator din directoarele pe care le crează, chiar dacă acele fişiere împiedică DCM să creeze cu succes fişiere când 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. E nevoie să creaţi un CA local nou după ce mutaţi următoarele 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`

	S-ar putea să vă lipsească un LPP (prerequisite licensed program) pe care DCM îl cere instalat. Verificaţi lista de cerinţe preliminare DCM şi asiguraţi-vă că toate programele licenţiate sunt instalate corect.

Problemă	Soluţie posibilă
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 serverul HTTP pentru documentaţie iSeries pentru ajutor la configurarea unei instanţe de server HTTP sigure pentru a folosi lista de validare.

Depanarea problemelor cu browser-ul

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 browser-ului.	Începeţi o nouă sesiune browser pentru Internet Explorer.
Internet Explorer nu prezintă toate certificatele client/utilizator selectabile din lista de selecţie a unui browser. Internet Explorer arată doar certificate, emise de un CA de încredere, pe care le puteţi folosi pe un sit securizat.	Un CA trebuie să fie de încredere atât 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 de chei) încă 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. Trebuie de asemenea să verificaţi că 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.

Problemă	Soluţie Posibilă
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 browser-ului 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-i spună utilizatorului că CA nu este încă de încredere.	Folosiţi DCM pentru a seta **starea CA** pe **activă** pentru a marca CA drept 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 sit 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 situri, 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 dintre cele mai comune probleme ale serverului HTTP pe care le-aţi putea întâlni în timp ce lucraţi cu DCM (Digital Certificate Manager).

Problemă	Soluţie posibilă
Hypertext Transfer Protocol Secure (HTTPS) nu funcţionează.	Asiguraţi-vă că serverul HTTP este setat corect pentru folosirea SSL. În versiunile mai mari de V5R1 fişierul de configurare trebuie să aibă **SSLAppName** setat prin folosirea interfeţei de administrare a serverului HTTP. De asemenea, configuraţia trebuie să aibă o gazdă virtuală configurată care foloseşte portul SSL, cu **SSL** set to **Activat** pentru gazda virtuală. Trebuie de asemenea să fie două directive **Ascultare** specificând două porturi diferite, unul pentru SSL şi unul nu pentru SSL. Acestea sunt setate în pagina **Setări generale**. 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 serverul dumneavoastră, mergeţi la interfaţa Administrare server HTTP pentru a seta configuraţia serverului dumneavoastră HTTP. Mai întâi trebuie să definiţi o gazdă virtuală pentru a activa SSL. După ce definiţi o gazdă virtuală, trebuie să specificaţi că gazda virtuală foloseşte portul SSL definit anterior în directiva **Ascultare** (în pagina **Setări generale**. Apoi, trebuie să folosiţi pagina **SSL cu autentificare certificat** sub **Securitate** pentru a activa SSL în gazda virtuală configurată anterior. Toate schimbările trebuie să fie aplicate fişierului de configurare. Luaţi aminte că înregistrarea instanţei dumneavoastră nu alege automat care certificate vor fi folosite de instanţă. Trebuie să folosiţi DCM pentru a asigna un certificat specific aplicaţiei dumneavoastră înainte să încercaţi să opriţi şi apoi să reporniţi instanţa server a dumneavoastră.

Problemă	Soluţie posibilă
Dacă aveţi dificultăţi la setarea serverului HTTP pentru liste validarea listelor şi autentificării opţionale a clientului.	Vedeţi documentaţia serverului HTTP pentru iSeries pentru opţiuni de setare a instanţei.
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 API-urile i5/OS din Centrul de informare. Aţi putea de asemenea să vreţi să vă uitaţi la 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.
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.
Serverul HTTP nu va porni cu succes cu **SSL** setat pe **Activat** şi mesajul de eroare HTP8351 apare în istoricul jobului. Istoricul erorii pentru serverul HTTP arată o eroare că operaţia de iniţializare SSL a eşuat cu o eroare cod de returnare de 107 când serverul HTTP eşuează.	Eroarea 107 înseamnă că certificatul a expirat. Folosiţi DCM pentru a asigna un certificat diferit aplicaţiei; de exemplu, QIBM_HTTP_SERVER_MY_SERVER. Dacă instanţa server care eşuează la pornire este serverul *ADMIN, atunci setaţi temporar **SSL** pe **Dezactivat** astfel încât să folosiţi DCM pe serverul *ADMIN. Apoi folosiţi DCM pentru a asigna un certificat diferit aplicaţiei QIBM_HTTP_SERVER_ADMIN şi încercaţi să setaţi **SSL** pe **Activat** din nou.

Depanarea asignării unui certificat utilizator

Când folosiţi task-ul **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 să afişeze un certificat, problema ar putea fi cauzată de una din următoarele situaţii:

1. Browser-ul nu a cerut să se selecteze un certificat pentru a fi prezentat serverului. Aceasta poate apare dacă browser-ul a memorat un certificat anterior (din accesarea unui alt server). Se poate încerca ştergerea memoriei browser-ului şi apoi executarea din nou a procesului. Browser-ul vă va prompta să selectaţi un certificat.
2. Asta s-ar putea întâmpla de asemenea dacă configuraţi browser-ul dumneavoastră astfel încât să nu afişeze o listă de selecţie şi browser-ul conţine doar un certificat de la o Autoritate de certificare din lista de CA-uri în care are încredere serverul. Verificaţi setările de configurare ale browser-ului şi modificaţi-le dacă este necesar. Browser-ul dumneavoastră vă va prompta să selectaţi un certificat. Dacă nu puteţi prezenta un certificat de la un CA pentru care serverul este setat să aibă încredere, nu puteţi asigna un certificat. Contactactaţi administratorul dumneavoastră DCM.
3. Certificatul care se doreşte a fi înregistrat este deja înregistrat cu DCM.
4. Autoritatea de certificare care a emis certificatul nu este desemnată drept de încredere pentru sistemul sau aplicaţia în cauză. De aceea certificatul pe care îl prezentaţi nu este valid. 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, administratorul ar putea avea nevoie să folosească task-ul **Setare stare CA** pentru a activa CA drept de încredere pentru a corecta problema.
5. Nu există un certificat pentru înregistrare. Se pot verifica certificatele client în browser pentru a vedea dacă este vreo problemă.
6. 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.

7. Produsul IBM HTTP Server nu este setat corect pentru înregistrarea certificatelor folosind SSL şi autorizarea client pe instanţa serverului administrativ. 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.

Capitolul 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 certificatele digitale şi despre cum le puteţi folosi pentru a vă îmbunătăţi politica de securitate:

- **Site Web VeriSign Help Desk**
  Situl Web VeriSign furnizează o bibliotecă extinsă cu subiecte despre certificatele digitale, precum şi un număr de alte subiecte despre securitatea Internet.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Această carte IBM Redbook se concentrează asupra îmbunătăţirilor securităţii în reţea la V5R1. Cartea acoperă multe subiecte, cum ar fi modalitatea de a folosi capabilităţile de semnare a obiectelor, DCM (Digital Certificate Manager), suportul pentru SSL al coprocesorului criptografic 4758 şi aşa mai departe.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  Această carte arată ce puteţi face cu certificatele digitale pe serverul dumneavoastră. Explică cum se setează diferitele servere şi clienţi care folosesc certificate. De asemenea, oferă informaţii şi exemple de cod sursă pentru modul în care se folosesc API-urile i5/OS pentru a gestiona şi folosi certificatele digitale în aplicaţiile de utilizator.
- **RFC Index Search**
  Acest sit Web furnizează o magazie în care puteţi căuta RFC-uri (Request for Comments). RFC-urile descriu standardele pentru protocoale Internet, cum ar fi SSL, PKIX şi altele care sunt înrudite cu folosirea certificatelor digitale.

Anexa. Observaţii

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

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Consultaţi-vă reprezentatntul IBM local pentru informaţii despre produsele şi serviciile disponibile curent în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licenţa pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

| IBM Director of Licensing
| IBM Corporation
| 500 Columbus Avenue
| Thornwood, NY 10594-1785
| U.S.A.

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte character set), contactaţi departamentul de Proprietate intelectuală al IBM-ului din ţara dumneavoastră sau trimiteţi întrebările în scris la:

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

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

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modifcări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment fără vreun avertisment.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

| IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca
| aceasta să implice vreo obligaţie faţă de dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

| IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile, să fie supuse unor termeni şi condiţii, inclusiv în unele cazuri, plata unor taxe.

Programul licenţiat descris în această publicaţie şi toate materialele licenţiate disponibile pentru el sunt furnizate de către IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement sau din orice acord echivalent încheiat între noi.

Orice date de performaţe conţinute aici au fost determinate într-un mediu controlat. Aşasar, rezultatele obţiunte în alte medii de operare pot varia semnificativ. Unele măsurători ar fi putu fi făcute pe sisteme la nivel de dezvoltare şi nu este nici o garanţie că aceste măsurători vor fi aceleaşi pe sistemele generale disponibile. Mai mult, unele măsurători ar fi putut fi făcute prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice datele aplicate pentru mediul lor specific.

Toate declaraţiile referitoare la direcţia sau intenţiile viitoare ale IBM sunt subiectul modificării sau a retragerii fără aviz şi reprezintă doar ţeluri şi obiective.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile zilnice de afaceri. Pentru a le ilustra cât mai bine posibil, exemplele includ nume de indivizi, companii, mărci şi produse. Toate aceste nume sunt fictive şi orice asemnănare cu numele şi adresele folosite de o întreprindere de afaceri reală este pur întâmplătoare.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale corporaţiei International Business Machines din Statele Unite, din alte ţări sau ambele:

AIX
Application System/400
AS/400
Domino
e (logo)
eServer
i5/OS
IBM
iSeries
Net.Data
Operating System/400
OS/400
400

Lotus, Freelance şi WordPro sunt mărci comerciale ale corporaţiei International Business Machines şi ale corporaţiei Lotus Development din Statele Unite, din alte ţări sau ambele.

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale ale corporaţiei Microsoft din Statele Unite, din alte ţări sau ambele.

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

Termeni şi condiţii pentru descărcarea şi tipărirea publicaţiilor

Permisiunile pentru utilizarea publicaţiilor pe care le-aţi selectat pentru descărcare sunt acordate cu condiţia respectării următorilor termeni şi condiţii şi a confirmării că le acceptaţi.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru uzul personal, fără caracter comercial, cu condiţia să fie păstrate toate observaţiile privitoare la proprietate. Nu puteţi să distribuiţi aceste publicaţii, să le afişaţi sau să produceţi lucrări derivate pe baza lor sau a unei porţiuni din ele, fără consimţământul expres al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii numai în cadrul firmei dumneavoastră, cu condiţia să fie păstrate toate observaţiile privitoare la proprietate. Nu puteţi să produceţi lucrări derivate pe baza acestor publicaţii sau să reproduceţi, să distribuiţi sau să afişaţi publicaţiile sau porţiuni din ele fără consimţământul expres al IBM.

Cu excepţia celor menţionate în această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, exprese sau implicite, pentru publicaţii sau pentru informaţii, date, software sau alte proprietăţi intelectuale conţinute de acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate de fiecare dată când consideră că utilizarea acestor publicaţii este în detrimentul intereselor sale, aşa cum sunt determinate de IBM, sau atunci când constată că instrucţiuile de mai sus nu au fost respectate.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât respectând integral legile şi reglementările în vigoare, precum şi legile şi reglementările din Statele Unite privind exportul. IBM NU OFERĂ NICI O GARANŢIE REFERITOARE LA CONŢINUTUL ACESTOR PUBLICAŢII. PUBLICAŢIILE SUNT OFERITE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRIMATĂ SAU IMPLICITĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP.

Descărcând sau tipărind o publicaţie de pe acest sit, confirmaţi că sunteţi de acord cu aceşti termeni şi condiţii.

Tipărit în S.U.A.