System i

Digital Certificate Manager

Versiunea 6 Ediţia 1

System i

Digital Certificate Manager

Versiunea 6 Ediţia 1

Notă

Înainte de a folosi aceste informaţii şi produsul la care se referă, aveţi grijă să citiţi informaţiile din "Observaţii", la pagina 87.

Această ediţie este valabilă pentru IBM i5/OS (număr de produs 5761-SS1) versiunea 6, ediţia 1, modificarea 0 şi pentru toate ediţiile şi modificările ulterioare până se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

Digital Certificate Manager (DCM)

Digital Certificate Manager (DCM) vă permite să gestionaţi certificate digitale pentru reţeaua dumneavoastră şi să utilizaţi Secure Sockets Layer (SSL) pentru a activa comunicaţii sigure pentru multe aplicaţii.

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 îmbunătăţite de securitate în reţea. De exemplu, certificatele digitale sunt esenţiale pentru configurarea şi utilizarea SSL. Folosirea SSL vă permite să creaţi conexiuni sigure între utilizatori şi aplicaţii server peste o reţea ce nu este de încredere, cum ar fi Internet. SSL oferă una dintre cele mai bune soluţii pentru protecţia în Internet a caracterului privat al datelor sensibile, cum ar fi numele de utilizator şi parolele. Multe platforme System i şi aplicaţii, ca FTP, Telnet, server HTTP furnizează suport SSL pentru a asigura confidenţialitatea datelor.

System i 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 utiliza 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 obiectelor, pentru a le asigura integritatea.

Caracteristica gratuită Digital Certificate Manager vă permite să beneficiaţi cu uşurinţă de suportul System i pentru certificate, asigurând gestionarea centrală a certificatelor pentru aplicaţiile dumneavoastră. DCM vă permite să gestionaţi certificatele pe care le obţineţi de la orice CA (autoritate de certificare). De asemenea, puteţi utiliza DCM-ul să creaţi şi opera propriul dumneavoastră CA local să emite certificate private la aplicaţii şi utilizatori în organizaţia dumneavoastră.

Cheile folosirii efective a certificatelor pentru beneficiile lor în ceea ce priveşte securitatea sunt planificarea şi evaluarea corectă. Aţi putea să revedeţi 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:

Informaţii înrudite

Secure Sockets Layer (SSL)

Semnare obiect şi verificare semnătură

Ce este nou în V6R1

Citiţi despre informaţiile modificate semnificativ sau noi pentru colecţia de subiecte refritoare la Digital Certificate Manager (DCM) for i5/OS.

Noi informaţii pentru gestionarea certificatelor prin expirare

Aceste noi informaţii explică cum se gestionează certificatele de server sau client, certificatele de semnare obiecte, certificatele CA şi certificatele de utilizator prin expirearea pe sistemul local.

- “Gestionarea certificatelor prin expirare” la pagina 68

Noi informaţii pentru pornirea DCM

Aceste noi informaţii explică pas cu pas procesul pentru pornirea DCM pe sistemul dumneavoastră. Noul proces implică utilizarea pe portul 2001 a unei noi interfeţe de consolă Web, numită IBM Systems Director Navigator for i5/OS.

- “Pornirea DCM” la pagina 41

Cum puteţi vedea ce este nou sau modificat

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

- Imaginea » pentru marcarea locului unde încep informaţiile noi sau cele modificate.
- Imaginea « pentru marcarea locului unde se termină informaţiile noi sau cele modificate.

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

Fişierul PDF pentru DCM

Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

Pentru a vizualiza sau descărca versiunea PDF a acestui subiect, selectaţi Digital Certificate Manager (aproximativ 1100 KB).

Salvarea fişierelor PDF

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

1. Faceţi clic dreapta pe legătura PDF în browser-ul dumneavoastră.
2. Faceţi clic pe opţiunea de salvare locală a PDF-ului.
3. Navigaţi la directorul în care doriţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

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

Concepte privind DCM

Un certificat digital este o acreditare digitală care validează identitatea proprietarului certificatului, foarte asemănător modului în care 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:

Extensiile de certificat

Extensiile de certificat 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 (Certificate Authority) care emit certificate.

De exemplu, CA-ul local pe care managerul de certificat digital (DCM) îl furnizează, vă permite să utilizaţi numai extensiile 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 in intenţionaţi să folosiţi certificatul pentru a identifica un punct final de conexiune System i VPN (Virtual Private Network), trebuie să oferiţi informaţii pentru aceste extensii.

Concepte înrudite

"Numele distinctiv"
Numele distinctiv (DN) este un termen pentru informaţiile de identificare dintr-un certificat, fiind parte a certificatului propriu-zis. Un certificat conţine informaţii DN atât pentru proprietarul sau solicitantul certificatului (numite DN subiect), cât şi pentru CA-ul care emite certificatul (numite DN emitent). În funcţie de politica de identificare a CA-ului care emite certificatul, numele distinctiv poate include o varietate de informaţii.

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 utilizaţi CA-ul local pentru a semna certificatul reînnoit, DCM utilizează informaţiile pe care le furnizaţi pentru a crea un nou certificat în depozitul de certificate curent 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 construit din cheia publică 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 altă CA publică. 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

Numele distinctiv (DN) este un termen pentru informaţiile de identificare dintr-un certificat, fiind parte a certificatului propriu-zis. Un certificat conţine informaţii DN atât pentru proprietarul sau solicitantul certificatului (numite DN subiect), cât şi pentru CA-ul care emite certificatul (numite DN emitent). În funcţie de politica de identificare a CA-ului care emite certificatul, numele distinctiv poate include o varietate de informaţii.

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 şi 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 standardele PKIX (schimb de infrastructură a cheilor), pot cere ca solicitantul 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.

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:

- Adrese IP versiunea 4 sau 6
- Numele complet calificat al domeniului
- Adresa de e-mail

Concepte înrudite

“Extensiile de certificat” la pagina 2
Extensiile de certificat sunt câmpuri de informaţii care furnizează informaţii suplimentare despre certificat.

Semnăturile digitale

O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme de criptografie, fiind echivalentă cu o semnătură personală de 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 conţin e 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 pretind 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.

Concepte înrudite

"Autoritatea de certificare"
Autoritatea de certificare (CA) este o entitate administrativă centrală de încredere care poate emite certificate digitale utilizatorilor şi serverelor.

"Criptografia" la pagina 8
Cheile partajate şi cheile publice sunt două tipuri diferite de funcţii criptografice pe care certificatele digitale le utilizează pentru securitate.

"Perechea de chei publice-private"
Fiecare certificat digital are o pereche de chei criptografice asociate.

Perechea de chei publice-private

Fiecare certificat digital are o pereche de chei criptografice asociate.

Notă: Certificatele care verifică semnătura sunt o excepţie de la această regulă şi au asociată 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, documentele 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.

Concepte înrudite

"Semnăturile digitale" la pagina 4
O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme de criptografie, fiind echivalentă cu o semnătură personală de pe un document scris.

"Autoritatea de certificare"
Autoritatea de certificare (CA) este o entitate administrativă centrală de încredere care poate emite certificate digitale utilizatorilor şi serverelor.

Autoritatea de certificare

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 utiliza DCM pentru a opera propriul dumneavoastră CA local privat pentru a emite certificate private la sisteme şi utilizatori. Când CA-ul local emite un certificat utilizator, DCM asociază automat certificatul cu profilul utilizator al utilizatorului System i sau alte identităţi 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 şi autorizările pentru certificat sunt aceleaşi ca ale deţinătorului 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 o autoritate de certificare locală (CA) cu DCM, puteţi specifica politica datelor pentru CA-ul local. Politica datelor pentru un CA local descrie privilegiile de semnare pe care le are. Datele politicii determină:

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

Concepte înrudite

“Semnăturile digitale” la pagina 4
O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme de criptografie, fiind echivalentă cu o semnătură personală de pe un document scris.

“Perechea de chei publice-private” la pagina 5
Fiecare certificat digital are o pereche de chei criptografice asociate.

Locaţiile listei de revocare a certificatelor

O listă de revocare a certificatelor (CRL) este un fişier care conţine informaţii despre toate certificatele nevalide 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 Uniform Resource Identifier (URI - 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.

Când vă conectaţi la un server LDAP trebuie să furnizaţi un DN şi o parolă pentru a evita o conexiune anonimă Legarea anonimă la server nu asigură nivelul de autoritate pentru a accesa un atribut ″critical″, cum ar fi CRL. Într-un asemenea caz, DCM ar putea valida un certificat cu o stare revocată deoarece DCM nu are posibilitatea să obţină starea corectă din CRL. Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiţi unealta Administrare Web

pentru Directory Server şi selectaţi taskul ″Gestionare schemă″ pentru a schimba clasa de securitate (de asemenea numit şi ″clasă de acces″) a atributelor **certificateRevocationList** şi **authorityRevocationList** din ″critical″ în ″normal″.

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 realiza procesarea CRL pentru autentificarea certificatelor sunt: conexiunile VPN (Virtual Private Networking), serverul IKE (Internet Key Exchange), aplicaţiile activate pentru SSL (Secure Sockets Layer) şi procesul de semnare a obiectelor. 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. .

Concepte înrudite

“Validarea certificatelor şi aplicaţiilor” la pagina 69
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.

Operaţii înrudite

“Gestionarea locaţiilor CRL” la pagina 70
Digital Certificate Manager (DCM) vă permite să definiţi şi să administraţi informaţii despre locaţia CRL (Certificate Revocation List) pentru o Autoritate de certificare (CA) particulară pentru a o folosi ca parte din procesul de validare a certificatului.

Depozitele de certificate

Un depozit de certificate este un fişier special de bază de date de chei, pe care DCM îl foloseşte pentru a memora certificatele digitale.

Depozitul de certificate conţine de asemenea cheia privată a certificatului, exceptând cazul în care alegeţi să folosiţi un IBM Cryptographic Coprocessor pentru a memora cheia. DCM vă permite să creaţi şi să gestionaţi mai multe tipuri de depozite de certificate. DCM controlează accesul la depozitele de certificate prin parole 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. Taskurile 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:

Autoritate de certificare local (CA)
DCM utilizează acest depozit de certificate pentru a memora certificatul CA local şi cheile sale private dacă creaţi un CA local. Puteţi utiliza certificatul în acest depozit de certificate pentru a semna certificate pe care le utilizează CA-ul local să le emită. Când CA-ul local emite un certificat, DCM pune o copie a certificatelor 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 SSL (Secure Sockets Layer). Aplicaţiile System i (şi multe alte aplicaţii ale dezvoltatorilor de software) sunt scrise pentru a utiliza certificate numai din depozitul de certificate *SYSTEM. Când utilizaţi 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, taskurile din acest depozit de certificate vă permit să creaţi semnături digitale pe obiecte, cât şi să vizualizaţi şi să verificaţi semnăturile de pe obiecte. Când utilizaţi DCM pentru a crea un CA local, DCM creează acest depozit de certificate ca parte din proces. Când alegeţi să obţineţi certificate de la un CA public, cum sunt VeriSign, pentru semnarea obiectelor, trebuie să creaţi acest depozit de certificate.

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

Alt depozit de certificate sistem
Acest depozit de certificate oferă o locaţie alternativă de depozitare a certificatelor client sau server pe care le folosiţi pentru sesiuni SSL. Depozitele de certificate de pe alt 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. Autoritatea de certificare locală (CA), depozitele de certificate*SYSTEM, *OBJECTSIGNING, şi *SIGNATUREVERIFICATION trebuie să fie localizate în căile specifice în sistemul de fişiere integrat, alte depozite de certificate pot fi localizate oriunde în sistemul de fişiere integrat.

Concepte înrudite

“Tipurile de certificate digitale” la pagina 32
Când utilizaţi DCM la gestionarea certificatelor dumneavoastră, acesta le organizează şi le stochează (împreună cu cheile private asociate) într-un depozit de certificate, în funcţie de tipul certificatului.

Criptografia

Cheile partajate şi cheile publice sunt două tipuri diferite de funcţii criptografice pe care certificatele digitale le utilizează pentru securitate.

Criptografia este ştiinţa păstrării datelor în siguranţă. Criptograpfia vă permite să stocaţi informaţii sau să comunicaţi cu alte părţi fără ca părţile neimplicate să înţeleagă informaţiile sau comunicaţia. Criptarea 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).

Există două tipuri de criptografie:

- 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.

Concepte înrudite

“Semnăturile digitale” la pagina 4
O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme de criptografie, fiind echivalentă cu o semnătură personală de pe un document scris.

“Secure Sockets Layer”
Secure Sockets Layer (SSL) este standardul industrial pentru criptarea sesiunii între clienţi şi servere.

IBM Cryptographic Coprocessors for System i

Coprocesorul criptografic furnizează servicii criptografice dovedite, asigurând protecţie şi integritate, pentru a dezvolta aplicaţii e-business sigure.

Folosirea unui coprocesor criptografic IBM pentru platforma System i adaugă sistemului dumneavoastră capabilitatea de procesare criptografică de înaltă securitate. 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.

Concepte înrudite

“Stocarea cheilor de certificat pe IBM Cryptographic Coprocessor” la pagina 72
Dacă aţi instalat un coprocesor criptografic IBM pe sistemul dumneavoastră, puteţi utiliza coprocesorul să furnizeze spaţiu de stocare mai sigur pentru cheia privată a unui certificat. Puteţi folosi coprocesorul pentru a stoca cheia privată pentru un certificat server, unul client sau pentru un certificat CA local.

Secure Sockets Layer

Secure Sockets Layer (SSL) este standardul industrial pentru criptarea sesiunii 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 creează 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.

Concepte înrudite

“Criptografia” la pagina 8
Cheile partajate şi cheile publice sunt două tipuri diferite de funcţii criptografice pe care certificatele digitale le utilizează pentru securitate.

"Tipurile de certificate digitale" la pagina 32
Când utilizaţi DCM la gestionarea certificatelor dumneavoastră, acesta le organizează şi le stochează (împreună cu cheile private asociate) într-un depozit de certificate, în funcţie de tipul certificatului.

Definiţiile de aplicaţie

DCM vă permite să gestionaţi definiţii aplicaţiilor care vor lucra cu configuraţii SSL şi semnarea obiectelor.

Există două tipuri de definiţii de aplicaţie pe care le puteţi gestiona în DCM:

- 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 System i activate pentru SSL sunt înregistrate în DCM, aşa că puteţi să folosiţi cu uşurinţă DCM pentru a le aloca 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 obiectelor pe care intenţionaţi să le semnaţi. Trebuie să lucraţi în depozitul de certificate *OBJECTSIGNING pentru a crea o definiţie aplicaţie care semnează obiecte.

Concepte înrudite

"Gestionarea aplicaţiilor în DCM" la pagina 65
DCM vă permite să creaţi definiţii de aplicaţie şi să gestionaţi alocarea certificatelor pentru o aplicaţie. Puteţi de asemenea defini lista de încredere CA pe care o utilizează aplicaţiile ca bază a acceptării certificatelor pentru autentificarea clientului.

Operaţii înrudite

"Creare definiţie aplicaţie" la pagina 66
În Digital Certificate Manager (DCM) puteţi crea şi lucra cu aceste două tipuri de definiţii de aplicaţie: aplicaţii server sau client care utilizează SSL şi definiţii de aplicaţie pe care le utilizaţi pentru semnarea obiectelor.

Validarea

DCM (Digital Certificate Manager) furnizează taskuri care vă permit să validaţi un certificat sau o aplicaţie pentru a verifica diferite proprietăţi 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.

În cazul în care configuraţi maparea LDAP (Lightweight Directory Access Protocol) pentru a folosi CRL, DCM verifică lista CRL când validează certificatul, pentru a se asigura că certificatul nu este listat în CRL. Totuşi, validarea procesului pentru verificarea cu acurateţe CRL, serverul director (LDAP) configurat pentru maparea LDAP trebuie să conţină un CRL corespunzător. În caz contrar, luaţi legătura cu Microsoft pentru a obţine cea mai recentă actualizare.

Trebuie să furnizaţi un DN şi o parolă pentru a evita validarea unui certificat cu starea revocat. De asemenea, dacă nu specificaţi un DN şi o parolă când configuraţi maparea LDAP, veţi fi legat ca anonim la serverul LDAP. O legare anonimă la serverul LDAP nu furnizează nivelul necesar de autoritate pentru a accesa ″atributele critice″, iar CRL este un atribut ″critic″. Într-un asemenea caz, DCM ar putea valida un certificat cu o stare revocată deoarece DCM nu are posibilitatea să obţină starea corectă din CRL. Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiţi unealta Administrare Web pentru Directory Server şi selectaţi taskul ″Gestionare schemă″ pentru a schimba clasa de securitate (de asemenea numit şi ca ″clasă de acces″) a atributelor **certificateRevocationList** şi **authorityRevocationList** din ″critical″ în ″normal″.

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 alocare de certificat pentru aplicaţie şi asigură că certificatul alocat 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 despre 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.

Concepte înrudite

“Validarea certificatelor şi aplicaţiilor” la pagina 69
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.

Scenarii: DCM

Aceste scenarii ilustrează scheme tipice de implementat certificate pentru a vă ajuta să planificaţi propriile implementări de certificat ca parte din politica dumneavoastră de securitate System i. Fiecare scenariu de asemenea furnizează toate taskurile de configurare necesare pentru a realiza lansarea scenariului.

DCM vă permite să utilizaţi certificate pentru a îmbunătăţi politica de securitate în diverse 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 SSL (Secure Sockets Layer) pentru acces sigur la pagini 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) System i. 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 taskurile de configurare pe care trebuie să le realizaţi pentru a implementa scenariul.

Informaţii înrudite

Cerinţe preliminarii pentru semnarea obiectelor

Scenariu: Folosirea certificatelor pentru autentificarea externă

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

Situaţia

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 ratei care permite ca sute de agenţi independenţi să genereze baremuri pentru clienţii lor. Deoarece informaţia pe care această aplicaţie o furnizează este oarecum sensibilă, doriţi să vă asiguraţi că doar agenţii înregistraţi o pot folosi. Mai mult, 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 introduse 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) pentru utilizatorii 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 bine cunoscute.

Obiective

În acest scenariu, MyCo, Inc. vrea să folosească certificate digitale pentru a proteja informaţiile de calculare rată pe care aplicaţia lor o furnizează utilizatorilor 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:

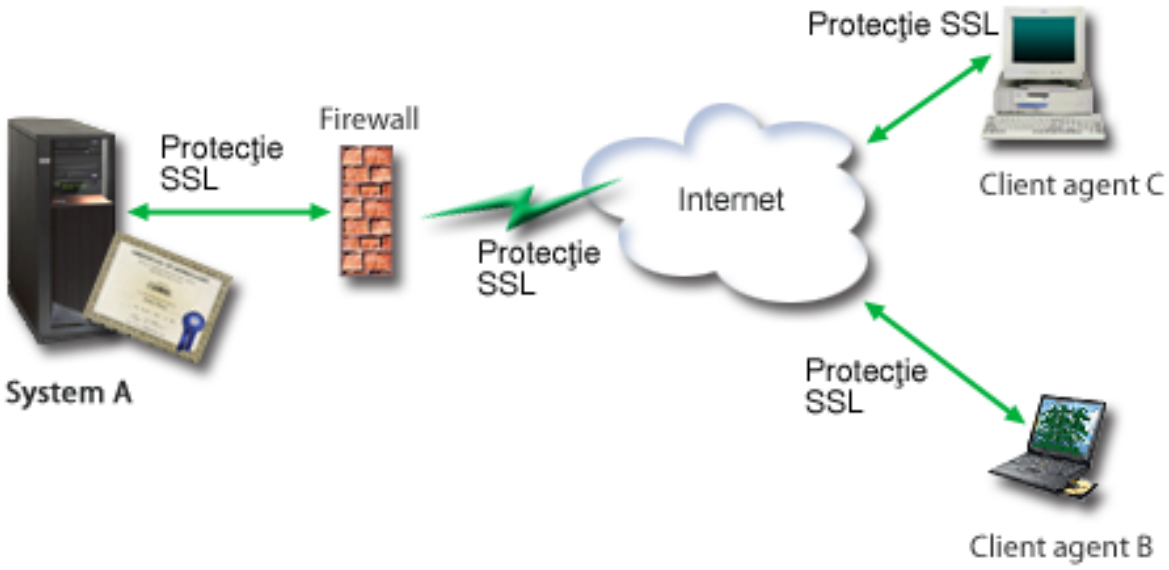

Figura ilustrează următoarele informaţii despre situaţia pentru acest scenariu:

Server companie public – System A

- System A este serverul care găzduieşte aplicaţia de calcul a ratei companiei.
- System A rulează i5/OS versiunea 5 ediţia 4 (V5R4) sau ulterior.
- System A are Digital Certificate Manager şi IBM HTTP Server for i5/OS instalat şi configurat.
- System A rulează aplicaţia de calculat rata, 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.

- System A prezintă certificatele sale pentru a iniţia o sesiune SSL când clienţii B şi C accesează aplicaţia de calculat rata.
- După iniţializarea sesiunii SSL, System A cere clienţilor B şi C să furnizeze un nume de utilizator şi o parolă valide înainte de a permite accesul la aplicaţia de calculat rata.

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 calculat rata pe System A, care îşi prezintă certificatele la software-ul clientului pentru a autentifica identitatea sa şi iniţia o sesiune SSL.
- Software-ul client pe clienţii B şi C este configurat să accepte certificatul din System A în scopul iniţializării unei sesiuni SSL.
- După ce sesiunea SSL începe, clienţii B şi C trebuie să furnizeze nume utilizator şi parolă valide înainte ca System A să acorde acces la aplicaţie.

Cerinţele preliminare şi presupuneri

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:

- Aplicaţia de calcul a ratei de pe System A este o aplicaţie generică, ce poate fi configurată pentru utilizarea SSL. Cele mai multe aplicaţii, inclusiv multe aplicaţii System i 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.
- 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.
- System A îndeplineşte “Cerinţe de setare DCM” la pagina 31 pentru instalarea şi utilizarea Managerului de certificate digitale (DCM)
- Nimeni nu a mai configurat sau utilizat DCM pe System A.
- Oricine foloseşte DCM pentru a realiza taskurile din acest scenariu trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilurile lor de utilizator.
- System A nu are un IBM coprocesor criptografic instalat.

Taskurile de configurare

Operaţii înrudite

“Pornirea DCM” la pagina 41
Înainte de a putea utiliza orice caracteristică din Digital Certificate Manager (DCM), trebuie să îl porniţi pe sistem.

Finalizarea fişelor de planificare

Următoarele fişe 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 articolele cerinţelor preliminare şi aveţi nevoie să aveţi adunate toate informaţiile cerute înainte să realizaţi orice task de configurare.

Tabela 1. Fişa de planificare a cerinţelor preliminare pentru implementarea certificatelor

Fişă cu cerinţe preliminare	Răspunsuri
Sistemul dumneavoastră rulează i5/OS V5R4 sau mai târziu?	Da

Tabela 1. Fişa de planificare a cerinţelor preliminare pentru implementarea certificatelor (continuare)

Fişă cu cerinţe preliminare	**Răspunsuri**
Aveţi DCM instalat pe sistemul dumneavoastră?	Da
Este IBM HTTP Server for i5/OS instalat pe sistemul dumneavoastră şi instanţa server administrativ pornită?	Da
Este configurat TCP pentru sistemul dumneavoastră astfel încât să puteţi folosi un browser Web şi instanţa serverului administrativ server 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 taskurile necesare de configurare pentru a termina implementarea:

Tabela 2. Fişa de planificare a configuraţiei pentru implementarea certificatelor

Fişa de planificare pentru System A	**Răspunsuri**
Veţi opera propriul dumneavoastră CA local sau obţine certificate pentru aplicaţia dumneavoastră de la un CA public?	Obţineţi certificate de la un CA public
System A găzduieşte aplicaţiile pe care vreţi să le 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 de organizare**: identifică secţiunea sau zona de organizare pentru aplicaţia care va folosi acest certificat. • **Nume organizaţie**: identifică compania dumneavoastră sau secţiunea divizionară 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.	**Mărime cheie**: 1024**Etichetă certificat**: Myco_public_cert**Nume comun**: myco_rate_server@myco.com**Unitate de organizare**: Rate dept**Nume organizaţie**: myco**Localitate sau oraş**: Any_city**Provincie sau oraş**: Any**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

Crearea unei cereri de certificat client sau server

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigare al DCM, selectaţi **Creare depozit de certificate nou** pentru a porni operaţia ghidată şi pentru a completa o serie de formulare. Aceste formulare vă 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 modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.

3. Selectaţi ***SYSTEM** ca depozit de certificate 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 Autoritare de certificare Internet (CA)** ca semnatar al noului certificat şi faceţi clic pe **Continuare** pentru a afişa un formular care vă permite să furnizaţi informaţii de identificare pentru noul certificat.
6. Completaţi formularul şi faceţi clic pe **Continuare** pentru a afişa o pagină de confirmare. Această pagină de confirmare afişează datele cererii pe care trebuie să le furnizaţi Autorităţii de certificare (CA) care vă va emite certificatul. Datele CSR (Certificate Signing Request) sunt constituite din cheia publică, numele distinctiv şi alte informaţii pe care le-aţi specificat pentru certificatul nou.
7. Copiaţi şi lipiţi cu atenţie datele CSR în formularul de cerere a certificatului, sau într-un fişier separat, pe care CA publică îl cere pentru solicitarea unui certificat. Trebuie să utilizaţi toate datele CSR, inclusiv liniile Început şi Sfârşit cerere certificat nou.

   Notă: Când ieşiţi din această pagină, datele se pierd şi nu le mai puteţi recupera.
8. Când ieşiţi din această pagină, datele se pierd şi nu le mai puteţi recupera.
9. Aşteptaţi ca Autoritatea de certificare (CA) să trimită înapoi certificatul semnat şi completat înainte de a continua cu următorul pas de operaţie pentru scenariu.

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

Configurarea aplicaţiilor pentru a utiliza SSL

Când vă primiţi înapoi certificatul semnat de la CA publică, puteţi continua procesul de activare a comunicaţiilor SSL pentru aplicaţia dumneavoastră publică. Trebuie să configuraţi aplicaţia să folosească SSL înainte să lucreze cu certificatele dumneavoastră semnate. Unele aplicaţii, ca de exemplu IBM HTTP Server for i5/OS generează o aplicaţie ID unică şi înregistrează ID-ul cu DCM când configuraţi aplicaţia să utilizeze SSL. Trebuie să ştiţi ID-ul aplicaţiei înainte de a putea folosi DCM pentru a aloca 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. Când terminaţi configurarea SSL pentru aplicaţia dumneavoastră, puteţi configura certificatul public semnat pentru aplicaţie astfel încât să poată iniţializa sesiuni SSL.

Informaţii înrudite

Aplicaţie securitate cu SSL

Importul şi alocarea certificatului public semnat

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

Pentru a importa şi aloca certificatul dumneavoastră către aplicaţia dumneavoastră pentru a completa procesul de configurare SSL, urmaţi aceşti paşi:

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** pentru ca să se deschidă 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 împrospătarea cadrului de navigare, selectaţi **Gestionare certificate** pentru afişarea unei liste de taskuri.
5. Din lista de taskuri, selectaţi **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate *SYSTEM.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
6. Apoi, selectaţi **Alocare certificat** din lista de taskuri **Gestionare certificate** pentru a afişa o listă de certificate pentru depozitul de certificate curent.
7. Selectaţi certificatul dumneavoastră din listă şi faceţi clic pe **Alocare la aplicaţii** pentru a afişa o listă de definiţii de aplicaţii pentru depozitul de certificate curent.
8. Selectaţi aplicaţia dumneavoastră din listă şi faceţi clic pe **Continuare**. Se afişează o pagină fie cu un mesaj de confirmare pentru alocarea selecţiei dumneavoastră sau o eroare dacă a apărut o problemă.

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

Pornirea aplicaţiilor în modul SSL

După ce terminaţi procesul de importare şi alocare 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 alocarea certificatului există în timp ce aplicaţia se execută. Revedeţi documentaţia pentru aplicaţia dumneavoastră pentru a determina dacă necesită să reporniţi aplicaţia sau pentru alte informaţii specifice 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.

(Opţional): Definirea unei liste de încredere CA pentru o aplicaţie care necesită

Aplicaţiile care suportă folosirea certificatelor pentru autentificare client în timpul unei sesiuni SSL (Secure Sockets Layer) 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 certificatul de autentificare a clientului ca fundament pentru a vă configura aplicaţia să folosească 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. Vedeţi Pornirea DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** pentru ca să se deschidă 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 împrospătarea cadrului de navigare, selectaţi **Gestionare certificate** pentru afişarea unei liste de taskuri.
5. Din lista de taskuri, selectaţi **Setare stare CA** pentru a afişa o listă de certificate CA.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
6. Selectaţi 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: Folosirea certificatelor pentru autentificarea internă

Acest scenariu descrie cum să folosiţi certificatele ca un mecanism de autentificare pentru a proteja şi restricţiona care resurse şi aplicaţii pot fi accesate din servere interne.

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 for i5/OS (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 SSL (Secure Sockets Layer) pentru a proteja transmisia datelor. În plus, puteţi folosi certificate în locul parolelor pentru autentificarea mai sigură a utilizatorilor şi pentru limitarea informaţiilor despre resurse umane pe care le pot accesa ei.

De aceea, dumneavoastră decideţi să setaţi o autoritate de certificare local privată (CA) şi emite certificate către toţi angajaţii şi ca angajaţii să asocieze certificatele lor cu System i profilele 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 dumneavoastră au deja profiluri de utilizator System i 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 System i. 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.
- Configuraţia SSL trebuie să fie realizată cu certificate private dintr-o autoritate de certificare (CA) local internă.
- 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:

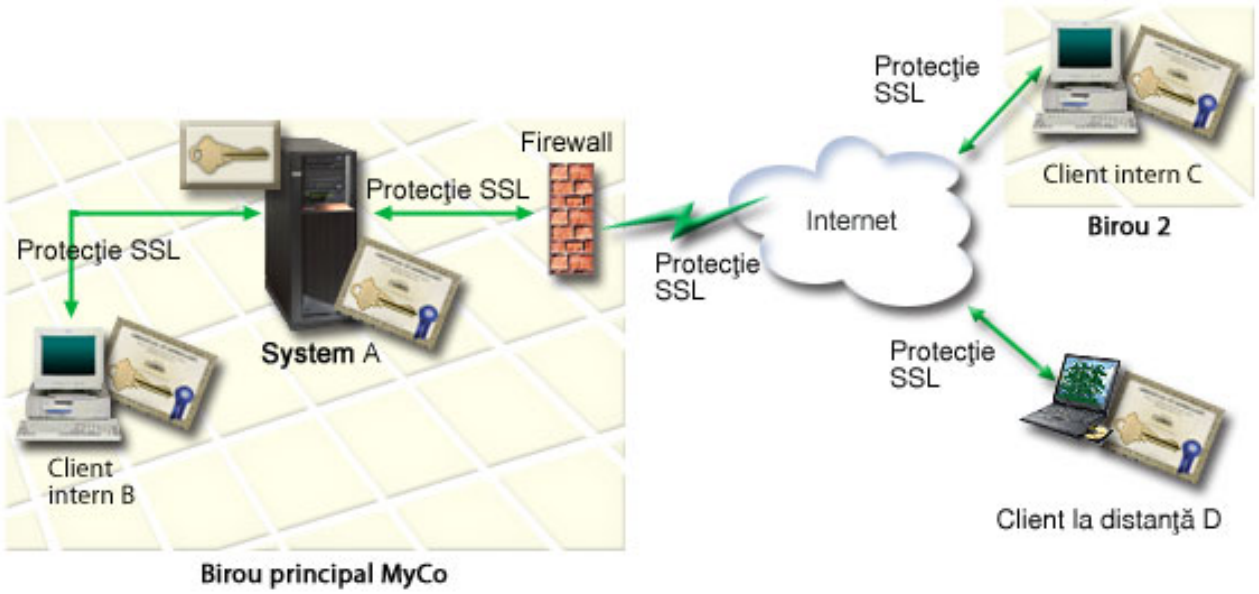

Figura ilustrează următoarele informaţii despre situaţia pentru acest scenariu:

Serverul public al companiei – System A

- System A este serverul care găzduieşte aplicaţia companiei de calculat rata.
- System A rulează i5/OS versiunea 5 ediţia 4 (V5R4) sau ulterioară.
- System A are Digital Certificate Manager şi IBM HTTP Server for i5/OS instalat şi configurat.
- System A rulează aplicaţia de calculat rata, 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.
- System A prezintă certificatele sale pentru a iniţia o sesiune SSL când clienţii B şi C accesează aplicaţia de calculat rata.
- După iniţializarea sesiunii SSL, System A cere clienţilor B şi C să furnizeze un nume de utilizator şi o parolă valide înainte de a permite accesul la aplicaţia de calculat rata.

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 calculat rata pe System A, care îşi prezintă certificatele la software-ul clientului pentru a autentifica identitatea saşi iniţia o sesiune SSL.
- Software-ul client pe clienţii B şi C este configurat să accepte certificatul din System A în scopul iniţializării unei sesiuni SSL.
- După ce sesiunea SSL începe, clienţii B şi C trebuie să furnizeze nume utilizator şi parolă valide înainte ca System A să acorde acces la aplicaţie.

Cerinţele preliminare şi presupuneri

Acest scenariu depinde de următoarele cerinţe preliminare şi supoziţii:

- IBM HTTP Server for i5/OS-ul (motorizat de Apache) rulează aplicaţia resurse umane pe System A. Acest scenariu nu furnizează instrucţiuni specifice pentru configurarea serverului HTTP spre utilizarea SSL. Acest scenariu furnizează instrucţiuni pentru configurarea şi gestionarea certificatelor care sunt necesare pentru ca orice aplicaţie să folosească SSL.
- Serverul HTTP poate avea capabilitatea de a cere certificate pentru autentificarea unui client. Acest scenariu furnizează instrucţiuni pentru utilizarea DCM pentru a configura cerinţele gestiunii certificatului pentru acest scenariu. Totuşi, acest scenariu nu furnizează anumiţi paşi de configurare pentru configurarea autentificării unui client prin certificate pentru Serverul HTTP.
- Serverul HTTP de resurse umane pe System A deja utilizează autentificarea parolelor.
- System A îndeplineşte cerinţele pentru instalarea şi utilizarea DCM.
- Nimeni nu a configurat sau utilizat anterior DCM pe System A.
- Oricine foloseşte DCM pentru a realiza taskurile din acest scenariu trebuie să aibă autorizările speciale *SECADM şi *ALLOBJ pentru profilurile lor de utilizator.
- System A nu are un coprocesor criptografic IBM instalat.

Taskurile de configurare

Finalizarea fişelor de planificare

Următoarele fişe 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 articolele cerinţelor preliminare şi aveţi nevoie să aveţi adunate toate informaţiile cerute înainte să realizaţi orice task de configurare.

Tabela 3. Fişa de planificare a cerinţelor preliminare pentru implementarea certificatelor

Fişă cu cerinţe preliminare	**Răspunsuri**
Sistemul dumneavoastră rulează i5/OS V5R4 sau mai târziu?	Da
Aveţi DCM instalat pe sistemul dumneavoastră?	Da
Este IBM HTTP Server for i5/OS instalat pe sistemul dumneavoastră şi instanţa server administrativ pornită?	Da
Este configurat TCP pentru sistemul dumneavoastră astfel încât să puteţi folosi un browser Web şi instanţa serverului administrativ server 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 taskurile necesare de configurare pentru a termina implementarea:

Tabela 4. Fişa de planificare a configuraţiei pentru implementarea certificatelor

Fişa de planificare pentru System A	**Răspunsuri**
Veţi opera propriul dumneavoastră CA local sau obţine certificate pentru aplicaţia dumneavoastră de la un CA public?	Creare CA local pentru a emite certificate
System A găzduieşte aplicaţiile pe care vreţi să le activaţi pentru SSL?	Da
Ce informaţii nume distinctive veţi utiliza 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 divizionară 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	**Mărime cheie**: 1024**Nume CA (Certificate Authority)**: Myco_CA@myco.com**Unitate de organizare**: Rate dept**Nume organizaţie**: myco**Localitate sau oraş**: Any_city**Stat sau provincie**: Any**Ţară sau regiune**: ZZ**Perioada de validitate a CA**: 1095
Doriţi să setaţi datele de politică pentru CA-ul local pentru a-i permite să emită certificate utilizator pentru autentificare client?	Da

Tabela 4. Fişa de planificare a configuraţiei pentru implementarea certificatelor (continuare)

Fişa de planificare pentru System A	Răspunsuri
Ce informaţii nume distinctive veţi utiliza pentru certificatul server pe care CA-ul local îl emite? • **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 de organizare**: identifică secţiunea sau zona de organizare pentru aplicaţia care va folosi acest certificat. • **Nume organizaţie**: identifică compania dumneavoastră sau secţiunea divizionară 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.	**Mărime cheie**: 1024**Etichetă certificat**: Myco_public_cert**Nume comun**: myco_rate_server@myco.com**Unitate de organizare**: Rate dept**Nume organizaţie**: myco**Localitate sau oraş**: Any_city**Provincie sau oraş**: Any**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?	DaMyco_CA@myco.com

Configurarea serverului HTTP de resurse umane pentru a utiliza SSL

Configuraţia SSL pentru serverul HTTP (motorizat de Apache) de resurse umane pe System A implică un număr de taskuri care variază în funcţie de configuraţia curentă a serverului dumneavoastră.

Pentru a configura 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 câmpul **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 selectaţi din nou în DCM.

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.

Informaţii înrudite

IBM HTTP Server for i5/OS

Crearea şi operarea unui CA local

După ce aţi configurat Serverul HTTP de resurse umane să folosească SSL, trebuie să configuraţi un certificat pe care să îl folosească serverul pentru a iniţia SSL. Conform obiectivelor pentru acest scenariu, aţi ales să creaţi şi să opera o autoritate de certificare locală (CA), care să emită un certificat pentru server.

Când utilizaţi Manager certificat digital (DCM) pentru a crea un CA local, sunteţi ghidat printr-un proces care asigură că dumneavoastră configuraţi tot ce aveţi nevoie pentru a activa SSL pentru aplicaţia dumneavoastră. Aceasta include alocarea certificatului pe care CA-ul local îţ emite la aplicaţia server web. De asemenea, adăugaţi CA-ul local la serverul web lista de încredere CA a aplicaţiilor. Având CA-ul local în lista de încredere a aplicaţiilor vă asigură că aplicaţia poate recunoaşte şi autentifica utilizatori car e prezintă certificate pe care CA-ul local le emite.

Pentru a utiliza DCM la crearea şi operarea unui CA local şi emite un certificat la aplicaţia server resurse umane,finalizaţi aceşti paşi:

1. Porniţi DCM. Vedeţi Pornirea 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 de creare a unui CA local şi finalizare alte taskuri necesare pentru începerea utilizării certificatelor digitale pentru SSL, semnare obiect,şi verificare semnătură.

   Notă: Dacă aveţi întrebări despre modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
3. Completaţi formularele pentru acest task asistat. În utilizarea acestor formulare pentru realizarea tuturor taskurilor necesare pentru a seta o autoritate de certificare (CA) funcţională, realizaţi următorii paşi:
   a. Furnizaţi informaţii identificatoare pentru CA-ul local.
   b. Instalaţi certificatul CA local pe PC-ul dumneavoastră sau în browser în aşa fel încât software-ul dumneavoastră poate recunoaşte CA-ul local şi valida certificate pe care le emite CA-ul local.
   c. Alegeţi datele politicii pentru CA-ul dumneavoastră local.

      Notă: Fiţi sigur să selectaţi că CA-ul local poate emite certificate utilizator.
   d. Utilizaţi noul CA local pentru a emite un certificat server sau client pe care aplicaţiile dumneavoastră îl poate 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. Utilizaţi noul CA local pentru emiterea unui certificat de semnare obiect pe care aplicaţiile îl pot folosi pentru semnarea digitală a obiectelor. Acest subtask creează 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 utilizează certificate de semnare obiecte, asiguraţi-vă că aţi parcurs acest pas. Dacă anulaţi la acest moment al taskului, el se opreşte şi trebuie să realizaţi taskuri separate pentru a efectua configurarea certificatului SSL.
   g. Selectaţi aplicaţiile care vor avea încredere în CA-ul local.

      Notă: Fiţi sigur să selectaţi aplicaţia ID serverul HTTP de resurse umane, de exemplu, QIBM_HTTP_SERVER_MYCOTEST, ca unul din aplicaţiile care are 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.

Configurarea autentificării clientului pentru server 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. Deschideţi un browser web şi introduceţi http://numele_sistemului_dumneavoastră:2001 ca să încărcaţi pagina de bun venit IBM Systems Director Navigator for i5/OS.
3. Din pagina de bun venit faceţi clic pe legătura **i5/OS Pagina de taskuri**.
4. Selectaţi **IBM Web Administration pentru i5/OS**.
5. 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.
6. Selectaţi serverul corespunzător din listă şi faceţi clic pe **Gestionare detalii**.
7. În cadrul de navigaţie, selectaţi **Securitate**.
8. Selectaţi fişa **SSL cu Autentificare certificat** din formular.
9. Selectaţi **Folosire profil i5/OS al clientului**.
10. În câmpul **Nume sau regiune autentificare**, specificaţi un nume pentru regiunea de autentificare.
11. Selectaţi Activat pentru câmpul **Procesare cereri folosind autorizarea client** şi faceţi clic pe **Aplicare**.
12. Selectaţi fişa **Controlare acces** din formular.
13. Selectaţi **Toţi utilizatorii autentificaţi (nume utilizator şi parolă valide)** şi faceţi clic pe **Aplicare**.
14. Selectaţi câmpul **SSL cu autentificare certificat** din formular.
15. Asiguraţi-vă că Activat este valoarea selectată în câmpul **SSL**.
16. În câmpul **Nume aplicaţie certificat server**, asiguraţi-vă că este specificată valoarea corectă, de exemplu, QIBM_HTTP_SERVER_MYCOTEST.
17. Selectaţi **Acceptare certificat client dacă este disponibil înainte de a face conexiunea**. Apăsaţi **OK**.

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

Informaţii înrudite

IBM HTTP Server for i5/OS

Pornirea serverului 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 alocarea 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 System i expandaţi **sistemul dumneavoastră → Network → Servere → TCP/IP → Administrare HTTP**
2. Faceţi clic pe **Pornire** pentru a porni interfaţa Administrare server HTTP.
3. Faceţi clic pe fişa **Gestionare** pentru a vedea o listă a tuturor serverelor HTTP configurate.
4. Selectaţi serverul corespunzător din listă şi faceţi clic pe **Oprire** dacă serverul rulează.
5. Faceţi clic pe **Pornire** pentru a reporni serverul. Consultaţi ajutorul online pentru informaţii suplimentare despre parametrii de pornire.

Înainte ca utilizatorii să poată accesa aplicaţia web de resurse umane, trebuie mai întâi să instaleze o copie a certificatului CA local în software-ul browser al lor.

Informaţii înrudite

Server HTTP - Privire generală centru de informare

Instalarea în browser a copiei unui certificat CA local

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. Atunci când, ca în scenatiul acesta, serverul prezintă un certificat de la un CA local, fiecare utilizator trebuie să utilizeze DCM pentru a instala o copie a certificatului CA local.

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

1. Porniţi DCM. Vedeţi Pornirea 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 îl memoraţi într-un fişier de 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 acest CA. Browser-ul va afişa o serie de ferestre care vă vor ajuta să terminaţi instalarea.
4. Apăsaţi **OK** pentru a reveni la pagina de bază (home) a Digital Certificate Manager.

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, trebuie să obţină un certificat utilizator de la CA-ul local.

Cererea unui certificat de la CA-ul local

În paşii anteriori, aţi configurat serverul Web de resurse umane să ceară certificate pentru autentificarea utilizatorilor. Acum utilizatorii prezintă un certificat valid de la CA-ul local înainte să le fie permis să acceseze serverul Web. Fiecare utilizator trebuie să folosească DCM pentru a obţine un certificat folosind taskul **Creare certificat**. Pentru a obţine un certificat de la CA-ul local, politica CA-ului local trebuie să permită CA-ului să emită certificate de utilizator.

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

1. Porniţi DCM. Vedeţi Pornirea 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 modul de completare a unui anumit formular din această operaţie ghidată, selectaţi butonul cu semnul de întrebare (**?**) din partea de sus a paginii pentru a accesa ajutorul online.
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 taskuri. 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 taskul.

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

Cu aceste taskuri 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.

Scenariu: Setarea autorităţii de certificare cu Digital Certificate Manager

Înainte de a seta o autoritate de certificare (CA), administratorul pentru ramura de birouri trebuie să se asigure că sunt finalizate câteva tascuri de planificare. Asiguraţi-vă că toate cerinţele preliminare pentru acest scenariu au fost finalizate înainte de realizarea acestor taskuri.

Completarea fişelor de planificare pentru Digital Certificate Manager

MyCo, Inc. finalizează fişele de lucru de planificare pentru ajutorul setării certificatelor digitale pentru a emite la partnerul lor de afaceri.

Tabela 5. Fişele de planificare pentru crearea unei autorităţi de certificare (CA) cu Digital Certificate Manager (DCM)

Întrebări	**Răspunsuri**
Ce dimensiune a cheii plănuiţi să utilizaţi pentru generarea cheilor private şi publice pentru certificat?	1024
Care este parola depozitului de certificate?	secret **Important:** Toate parolele care sunt utilizate în acest scenariu sunt numai pentru scopul de a exemplifica. Nu utilizaţi aceste parole în orice configuraţie actuală.
Care este numele autorităţii de certificare?	mycoca
Care este numele organizaţiei dumneavoastră?	myco
Câte zile doriţi ca autoritatea de certificare să fie validă?	1095 (3 ani)
Care este browser-ul dumneavoastră?	Windows Internet Explorer versiunea 6.0
Veţi emite certificate la utilizatori de pe reţea?	Nu

Tabela 6. Fişa de planificare pentru certificatul digital pentru System A

Întrebări	**Răspunsuri**
Ce dimensiune a cheii plănuiţi să utilizaţi pentru generarea cheilor private şi publice pentru certificat?	1024
Care este parola depozitului de certificate?	secret **Important:** Toate parolele care sunt utilizate în acest scenariu sunt numai pentru scopul de a exemplifica. Nu utilizaţi aceste parole în orice configuraţie actuală.
Care este numele etichetei certificatului?	mycocert
Care este numele obişnuit pentru certificatul dumneavoastră?	mycocert
Care este numele organizaţiei dumneavoastră?	MyCo, Inc
care este adresa IP a sistemului dumneavoastră?	192.168.1.2 (2001:DB8::2 in IPv6) **Important:** Adresele IP utilizate în acest scenariu sunt menite numai în scop exemplificator. Ele nu reflectă o schemă de adresă IP şi nu ar trebui utilizate în nici o configuraţie actuală. Ar trebui să utilizaţi propria adresă IP când finalizaţi aceste taskuri.
Care este numele de domeniu complet calificat al sistemului dumneavoastră?	systema.myco.min.com

Tabela 7. Fişa de planificare pentru certificatele digitale pentru System B

Întrebări	Răspunsuri
Ce dimensiune a cheii plănuiţi să utilizaţi pentru generarea cheilor private şi publice pentru certificat?	1024
Care este numele etichetei certificatului?	corporatecert
Care este numele obişnuit pentru certificatul dumneavoastră?	corporatecert
Care este calea depozitului de certificate şi parola?	/tmp/systemb.kdb
Care este parola depozitului de certificate?	secret2 **Important:** Toate parolele care sunt utilizate în acest scenariu sunt numai pentru scopul de a exemplifica. Nu utilizaţi aceste parole în orice configuraţie actuală.
Care este numele comun al certificatului digital?	corporatecert
Care este numele organizaţional care posedă acest certificat?	MyCo, Inc
Care este adresa IP a sistemului dumneavoastră?	172.16.1.3 (2002:DD8::3 in IPv6) **Important:** Adresele IP utilizate în acest sc enariu sunt menite numai în scop exemplificator. Ele nu reflectă o schemă de adresă IP şi nu ar trebui utilizate în nici o configuraţie actuală. Ar trebui să utilizaţi propria adresă IP când finalizaţi aceste taskuri.
Care este numele gazdă complet calificatal sistemului dumneavoastră?	systemb.myco.wis.com

Pornirea IBM HTTP Server for i5/OS pe System A

Utilizaţi această procedură pentru a porni IBM HTTP Server for i5/OS pe System A.

Pentru a accesa interfaţa DCM, trebuie să porniţi instanţa administrativă a serverului HTTP prin finalizarea următoarelor taskuri.

1. Din System A, semnaţi-vă la o interfaţă bazată pe caractere.
2. La linia de comandă, tastaţi strtcpsvr server(*HTTP) httpsvr(*admin). Aceasta porneşte sistemul de administrare a serverului HTTP.

Configurarea System A ca o autoritate de certificare

Utilizaţi această procedură pentru a configura System A ca o Autoritate de certificare (CA).

1. Deschideţi un browser web şi introduceţi http://numele_sistemului_dumneavoastră:2001 ca să încărcaţi pagina de bun venit IBM Systems Director Navigator for i5/OS.
2. Logaţi-vă cu numele profilului de utilizator System A şi parola dumneavoastră.
3. Din pagina de bun venit faceţi clic pe **i5/OS legătura Pagina de taskuri**.
4. Selectaţi **Digital Certificate Manager**.
5. Din panoul de navigaţie din stânga, selectaţi **Creare Autoritate de certificare (CA)**.
6. Pe pagina Creare Autoritate de certificare (CA), umpleţi următoarele câmpuri necesare cu informaţiile din fişa de lucru de planificare DCM:
   - **Dimensiunea cheii:** 1024
   - **Parolă depozit de certificate:** secretă
   - **Confirmare parolă:** secretă

Important: Toate parolele care sunt utilizate în acest scenariu sunt numai în scop de exemple. Nu utilizaţi aceste parole în orice configuraţie actuală.

- **Nume Autoritate de certificare:** mycoca
- **Nume organizaţie:** MyCo, Inc
- **Stat sau provincie:** min
- **Ţară sau regiune:** us
- **Perioadă de validitate Autoritate de certificare (2-7300):** 1095

7. Selectaţi **Continuare**.
8. Pe **pagina Instalare certificat local CA**, faceţi clic pe **Continuare**.
9. Pe pagina **Date politică Autoritate de certificare (CA)**, selectaţi următoarele opţiuni:
   - **Permisiune creare de certificate utilizator:** Da
   - **Perioada de validitate a certificatelor care sunt emise de această autoritate de certificare(1-2000):** 365
10. Pe pagina Date politică acceptate, citiţi mesajele care sunt afişate şi faceţi clic pe **Continuare** pentru a crea depozitul de certificate implicit al serverului (*SYSTEM) şi un certificat server semnat de CA-ul dumneavoastră. Citiţi mesajul de confirmare şi faceţi clic pe **Continuare**.
11. Pe pagina Creare certificat server sau client, introduceţi următoarele informaţii:
    - **Dimensiune control:** 1024
    - **Etichetă certificat:** mycocert
    - **Parolă depozit de certificate:** secret
    - **Confirmare parolă:** secret

    Important: Toate parolele care sunt utilizate în acest scenariu sunt numai pentru scopul de a exemplifica. Nu utilizaţi aceste parole în orice cpnfiguraţie actuală.

    - **Nume obişnuit:** mycocert
    - **Nume organizaţie:** myco
    - **Stat sau provincie:** min
    - **Ţară sau regiuni:** us
    - **Adresă IP versiunea 4:** 192.168.1.2
    - **Adresă IP versiunea 6:** 2001:DB8::3

    Notă: Adresele IP utilizate în acest scenariu sunt menite numai în scop exemplificator. Ele nu reflectă o schemă de adresă IP şi nu ar trebui utilizate în nici o configuraţie actuală. Ar trebui să utilizaţi propria adresă IP când finalizaţi aceste taskuri.

    - **Nume domeniu complet calificat:** systema.myco.min.com
    - **Adresă poştă electronică:** administrator@myco.min.com
12. Selectaţi **Continuare**.
13. Pe pagina Selectare aplicaţie, faceţi clic pe **Continuare**.

    Indiciu: Vrăjitorul VPN de conexiune nouă alocă automat certificatul pe care l-aţi creat la aplicaţia manager de chei VPN i5/OS. Dacă aveţi alte aplicaţii care ar putea utiliza acest certificat, le puteţi selecta pe această pagină. Pentru că acest scenariu utilizează numai certificate pentru conexiuni VPN, nu este nevoie să selectaţi aplicaţii suplimentare.
14. Pe pagina Stare aplicaţie, citiţi mesajele care sunt afişate şi faceţi clic pe **Anulare**. Aceasta acceptă modificările pe care le-aţi creat.

    Notă: Dacă doriţi să creaţi un depozit de certificate care să conţină certificate care sunt utilizate la semnarea obiectelor, selectaţi **Continuare**.
15. Când interfaţa DCM este reîmprospătată, selectaţi **Selectare depozit de certificate**.
16. Pe pagina Selectare depozit de certificate, selectaţi ***SYSTEM**. Selectaţi **Continuare**.

17. Pe pagina Depozit de certificate şi parolă, introduceţi secret. Selectaţi **Continuare**.
18. În cadrul de navigare stâng, selectaţi **Gestiune aplicaţii**.
19. Pe pagina Gestiune aplicaţii, selectaţi **Definire listă de încredere CA**. Selectaţi **Continuare**.
20. Pe pagina Definire listă de încredere CA, selectaţi **Server**. Selectaţi **Continuare**.
21. Selectaţi **Manager de chei VPN i5/OS** . Facţi clic pe **Definire listă de încredere CA**.
22. Pe pagina Definire listă de încredere CA, selectaţi **LOCAL_CERTIFICATE_AUTHORITY**. Apăsaţi **OK**.

Crearea certificatului digital pentru System B

Utilizaţi această procedură pentru a crea un certificat digital pentru System B.

1. În panoul de navigaţie stâng, faceţi clic pe **Creare certificat** şi selectaţi **Certificat server sau client pentru alt System i**.
2. Selectaţi **Continuare**.
3. Pe Creare certificat server sau client Certificate pentru altă pagină System i, selectaţi **V5R3**. Acesta este nivelul ediţiei pentru System B. Faceţi clic pe **Continuare**.
4. Pe pagina Creare certificat server sau client, introduceţi următoarele informaţii:
   - **Dimensiune cheie:** 1024
   - **Etichetă certificat:** corporatecert
   - **Cale depozit de certificate şi nume fişier:** /tmp/systemb.kdb
   - **Parolă depozit de certificate:** secret2
   - **Confirmare parolă:** secret2

     Notă: Toate parolele care sunt utilizate în acest scenariu sunt numai pentru scopul de a exemplifica. Nu utilizaţi aceste parole în orice configuraţie actuală.
   - **Nume obişnuit:** corporatecert
   - **Nume organizaţie:** MyCo, Inc
   - **Stat sau provincie:** wis
   - **Ţară sau regiune:** us
   - **Adresă IP versiunea 4:** 172.16.1.3
   - **Adresă IP versiunea 6:** 2002:DD8::3

     Important: Adresele IP utilizate în acest scenariu sunt menite numai în scop exemplificator. Ele nu reflectă o schemă de adresă IP şi nu ar trebui utilizate în nici o configuraţie actuală. Ar trebui să utilizaţi propria adresă IP când finalizaţi aceste taskuri.
   - **Nume gazdă complet calificat:** systemb.myco.wis.com
   - **Adresă poştă electronică:** administrator@myco.wis.com
5. Selectaţi **Continuare**. Veţi primi un mesaj de confirmare pentru a verifica dacă un certi ficat de server a fost creat pe System A pentru System B. Ca administrator al reţelei pentru ramura biroului de vânzări, trimiteţi aceste fişiere la administrator la biroul corporativprin poştă electronică criptată. Administratorul de la biroul corporativ trebuie acum să mute şi să redunemească depozit de certificate fişierul (.KDB) şi cererea fişier (.RDB) la System B. Administratorul de biroul corporativ va trebui să mute aceste fişiere la directorul /QIBM/USERDATA/ICSS/CERT/SERVER în sistemul de fişiere integrat folosind FTP binar. După aceasta este finalizată, administratorul trebuie să redenumească aceste fişiere în directorul corespunzător.

Redenumirea fişierelor .KDB şi .RDB pe System B

Utilizaţi această procedură pentru redenumirea fişierelor .KDB şi .RDB pe System B.

Deoarece depozitul de certificate *SYSTEM nu există pe System B, administratorul reţelei corporative trebuie să redenumească fişierele systemb.kdb şi systemb.RDB cu DEFAULT.KDB şi DEFAULT.RDB, utilizând aceste fişiere transferate ca depozitul de certificate *SYSTEM pe System B.

1. În Navigator System i, expandaţi **System B → Sisteme de fişiere → Sistem de fişiere integrat → Qibm → UserData → ICSS → Cert → Server**, şi verificaţi că fişierele systemb.kdb şi systemb.RDB sunt listate în acest director.
2. Într-o linie de comandă, tastaţi wrklnk ('/qibm/userdata/icss/cert/server').
3. Pe pagina Lucrul cu obiecte legătură, selectaţi 7 (Redenumire) pentru a redenumi fişierul systemb.kdb. Apăsaţi Enter.
4. În pagina Redenumire obiect, introduceţi DEFAULT.KDB în câmpul **Obiect nou**. Apăsaţi Enter.
5. Repetaţi Pas 3 şi Pas 4 pentru a redenumi fişierul systemb.RDB cu DEFAULT.RDB.
6. Verificaţi că aceste fişiere au fost modificate reîmprospătând Navigator System i şi expandând ***System B →* Sisteme de fişiere → sistem de fişiere integrat → Qibm → UserData → ICSS → Cert → Server**. Fişierele DEFAULT.KDB şi DEFAULT.RDB trebuiesc listate în director.

Schimbarea parolei de depozit de certificate pe System B

Utilizaţi această procedură pentru a modifica parola de depozit de certificate pe System B.

Acum administratorul de reţea pentru biroul corporativ trebuie să modifice parola pentru noul *SYSTEM depozit de certificate care a fost creat când fişierele DEFAULT.KDB şi DEFAULT.RDB au fost create.

Notă: Trebuie să modificaţi parola depozitului de certificate *SYSTEM. Când modificaţi parola, este ascunsă în aşa fel încât aplicaţia o poate recupera automat şi deschide depozitul de certificate pentru a accesa certificatele.

1. Deschideţi un browser web şi introduceţi http://numele_sistemului_dumneavoastră:2001 ca să încărcaţi pagina de bun venit IBM Systems Director Navigator for i5/OS.
2. Din pagina de bun venit faceţi clic pe **i5/OS legătura Pagina de taskuri**.
3. Selectaţi **Digital Certificate Manager**.
4. Din stânga panoului de navigaţie faceţi clic pe**Selectare depozit de certificate**
5. Selectare ***SYSTEM depozit de certificate** şi introduceţi secret2 pentru parolă. Aceasta este parola pe care administratorul ramurei biroului de vânzări a specificat-o când a creat certificatul serverului pentru System B. Faceţi clic pe **Continuare**.
6. În cadrul de navigare din stânga, selectaţi **Gestiune depozit de certificate** şi selectaţi **Schimbare parolă** şi faceţi clic pe **Continuare**.
7. Pe pagina modificare depozit de certificate, introduceţi corporatepwd în câmpurile **Parolă nouă** şi **Confirmare parolă**.
8. Selectaţi **Parola nu expiră** pentru politica de expirare. Selectaţi **Continuare**. O pagină de confirmare este încărcată. Apăsaţi **OK**.
9. Pe pagina de confirmare Schimbare parolă depozit de certificate, citiţi mesajulde pe acel ecran şi faceţi clic pe **OK**.
10. Pe pagina Depozit de certificate şi parolă care este reîncărcată, introduceţi coporatepwd în câmpul**Parolă depozit de certificate**. Selectaţi **Continuare**.

Definirea încrederii CA pentru mangerul de chei VPN i5/OS pe System B

Utilizaţi această procedură pentru a defini încrederea CA pentru manager de chei VPN pe System B.

1. În stânga cadrului de navigaţie, selectaţi **Gestionare aplicaţii**.
2. Pe pagina Gestiune aplicaţii, selectaţi **Definire listă de încredere CA**. Selectaţi **Continuare**.
3. Pe pagina Definire listă de încredere CA, selectaţi **Server**. Selectaţi **Continuare**.
4. Selectaţi **Manager de chei VPN i5/OS** . Facţi clic pe **Definire listă de încredere CA**.
5. Pe pagina Definire listă de încredere CA, selectaţi **LOCAL_CERTIFICATE_AUTHORITY**. Apăsaţi **OK**.

Acum administratorii pentru ramura de birouri vânzări şi birou corporativ pot începe configuraţia VPN.

Planificarea 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 de setare DCM

Pentru ca Managerul certificat digital (DCM) să funcţioneze corespunzător trebuie să aveţi anumite produse instalate şi aplicaţii configurate.

DCM (Digital Certificate Manager) este o caracteristică gratuită System i care vă permite să gestionaţi central certificatele digitale pentru aplicaţiile dumneavoastră. Pentru a folosi cu succes DCM, aveţi grijă să faceţi următoarele:

- Instalaţi Digital Certificate Manager. Aceasta este caracteristica DCM bazată pe browser.
- Instalaţi IBM HTTP Server for i5/OS şi porniţi instanţa Server administrativ.
- 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 privind salvarea de rezervă şi recuperarea datelor DCM

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

Un exemplu de asemenea circumstanţă este când utilizaţi DCM pentru a crea un certificat pentru un model System i şi alegeţi să folosiţi fişierele certificat pe sistemul ţintă pentru a crea un nou depozit de certificate. În această situaţie, trebuie să deschideţi noul depozit de certificate creat şi să utilizaţi taskul **Schimbare parolă** pentru a modifica parola pentru depozitul de certificate de pe sistemul destinaţie, care asigură faptul că DCM păstrează noua parolă. Dacă depozitul de certificate este alt depozit de certificate sistem, ar trebui de asemenea să specificaţi că vreţi să folosiţi opţiunea **Logare automată** când modificaţi parola.

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 taskul **Schimbare 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 sincronizate. 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.

Operaţii înrudite

"Folosirea unui CA local la emiterea certificatelor pentru alte modele System i" la pagina 58
Folosind DCM, puteţi configura un CA local privat pe un sistem care să emită certificate pentru utilizarea pe alte platforme System i.

Tipurile de certificate digitale

Când utilizaţi DCM la gestionarea certificatelor dumneavoastră, acesta le organizează şi le stochează (împreună cu cheile private asociate) într-un depozit de certificate, în funcţie de tipul certificatului.

Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona următoarele tipuri de certificate:

Certificate ale Autorităţii de Certificare (CA - Certificate Authority)
Un certificat CA este o acreditare digitală care validează identitatea Autorităţii de certificare care este proprietara certificatului. Certificatul CA 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 le semnează CA-ul. Un certificat Autoritate de certificare poate fi semnat de alt CA, cum ar fi VeriSign sau poate fi autosemnat în cazul în care este o entitate independentă. CA-ul local pe care îl creaţi şi operaţi cu DCM 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 le semnează CA-ul. Pentru a folosi un certificat pentru SSL, semnarea obiectelor sau verificarea semnăturilor obiectelor, trebuie să aveţi o copie a certificatului CA-ului emitent.

Certificate server sau client
Un certificat client sau server este o acreditare digitală 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 SSL (Secure Sockets Layer) 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 criptate SSL 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 o acreditare digitală 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 System i. De asemenea, puteţi folosi DCM pentru a asocia profilului de utilizator certificatele pe care le emite alt CA System i.

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.

Concepte înrudite

"Secure Sockets Layer" la pagina 9
Secure Sockets Layer (SSL) este standardul industrial pentru criptarea sesiunii între clienţi şi servere.

"Depozitele de certificate" la pagina 7
Un depozit de certificate este un fişier special de bază de date de chei, pe care DCM îl foloseşte pentru a memora certificatele digitale.

Certificatele publice şi certificatele private

Puteţi folosi certificate de la un CA publică 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.

O dată ce vă decideţi să folosiţi certificate, trebuie să alegeţi tipul implementării certificatelor care se potriveşte cel mai bine nevoilor dumneavoastră de securitate. Opţiunile pe care le aveţi pentru obţinerea certificatelor includ:

- Obţinerea certificatelor de la o Autoritate de certificare (CA) publică.
- Operarea propriului dumneavoastră CA local pentru a emite certificate private pentru aplicaţiile şi utilizatorii dumneavoastră.
- Folosirea unei combinaţii de certificate de la CA-ul public internet şi CA-ul dumneavoastră local.

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 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 să aibă încredere în certificatele pe care un binecunoscut CA public le emite mai mult decât CA-ul tău local le emite.

Folosirea certificatelor private

Dacă creaţi propria dumneavoastră CA locală, puteţi emite certificate la sisteme şi utilizatori într-un domeniu mai limitat, ca de exemplu în compania sau organizaţia dumneavoastră. Crearea şi menţinerea propriei CA a dumneavoastră vă permite să emiteţi certificate numai la acei utilizatori care sunt membrii de încredere a 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 dumneavoastră CA locală este durata şi resursele pe care trebuie să le investiţi. Oricum, Digital Certificate Manager (DCM) face acest proces mai uşor pentru dumneavoastră.

Când utilizaţi o CA locală pentru a emite certificate la utilizatori pentru autentificare client,trebuie să vă decideţi unde doriţi să memoraţi certificatele utilizator. C ând utilizatorii îşi obţin certificatele de la CA-ul local prin DCM certificatele lorsunt memorate cu un profil utilizator 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. Dacă preferaţi să nu aveţi certificate utilizator asociate cu un profil utilizator sau memorat cu un profil utilizator în orice manieră, puteţi utiliza API-uri să emită certificate programaticla utilizatori alţii decât utilizatorii System i.

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.

Taskuri 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 taskurile pe care trebuie să le realizaţi dacă alegeţi să operaţi un CA local să emită certificate private.
- Gestionarea certificatelor de la un CA public din Internet descrie taskurile 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 modele System i descrie taskurile pe care tr ebuie să le realizaţi dacă doriţi să utilizaţi certificatede la un CA privat local pe mai mult de un sistem.

Concepte înrudite

“Gestionarea certificatelor de la un CA public din Internet” la pagina 50
Când utilizaţi DCM la gestionarea certificatelor de la un CA public din Internet, trebuie mai întâi să creaţi un depozit de certificate. Un depozit de certificate este un fişier special de bază de date de chei, pe care îl foloseşte DCM (Digital Certificate Manager) pentru a stoca certificate digitale şi cheile lor private asociate.

“Certificatele publice şi certificatele private” la pagina 33
Puteţi folosi certificate de la un CA publică 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.

"Setarea certificatelor pentru prima dată" la pagina 41
Cadrul stâng al DCM (administrator de certificate digitale) este cadrul de navigare task. Puteţi folosi acest cadru pentru a selecta o varietate largă de taskuri pentru gestionarea certificatelor şi a aplicaţiilor care le folosesc.

"Certificatele digitale pentru semnarea obiectelor" la pagina 39
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.

Operaţii înrudite

"Certificatele digitale şi EIM" la pagina 37
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.

"Crearea certificatului de utilizator" la pagina 45
Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă utilizaţi DCM pentru a opera o autoritate de certificare local privată (CA), puteţi utiliza CA-ul local pentru emite certificate la fiecare utilizator.

"Crearea şi operarea unui CA local" la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

"Folosirea unui CA local la emiterea certificatelor pentru alte modele System i" la pagina 58
Folosind DCM, puteţi configura un CA local privat pe un sistem care să emită certificate pentru utilizarea pe alte platforme System i.

Referinţe înrudite

"Folosirea API-urilor pentru a emite programatic certificate altor utilizatori decât utilizatorii System i" la pagina 48
CA-ul local al dumneavoastră poate emite certificate private pentru utilizatori fără să asocieze certificatul cu un profil de utilizator System i.

Certificatele digitale pentru comunicaţiile sigure SSL

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 dumneavoastră este autentic, furnizând o sesiune de comunicaţii criptată pentru a asigura că datele care trec peste 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.

Concepte înrudite

"Certificatele digitale pentru autentificarea utilizatorului" la pagina 36
Tradiţional, utilizatorii primesc acces la resurse de la o aplicaţie sau sistem pe baza numelui de utilizator şi a parolei. Se poate creşte securitatea sistemului prin utilizarea certificatelor digitale (în locul numelor de utilizatori şi a parolelor) pentru a autentifica şi autoriza sesiunile dintre mai multe aplicaţii server utilizatori.

Certificatele digitale pentru autentificarea utilizatorului

Tradiţional, utilizatorii primesc acces la resurse de la o aplicaţie sau sistem pe baza numelui de utilizator şi a parolei. Se poate creşte securitatea sistemului prin utilizarea certificatelor digitale (în locul numelor de utilizatori şi a parolelor) pentru a autentifica şi autoriza sesiunile dintre mai multe aplicaţii server utilizatori.

Puteţi utiliza DCM pentru a asocia un certificat de utilizator cu acel profil utilizator System i sau altă identitate de utilizator. Apoi certificatul are aceleaşi autorizări şi pemisiuni ca şi identitatea sau profilul de utilizator asociat. Alternativ,puteţi utiliza API-uri să utilizaţi programatic autoritatea de certificare privată locală (CA) pentru a emite certificate pentru utilizatori alţii decât System i utilizatori. Aceste API-uri văî furnizează abilitatea de a emite certificate private la utilizatoricând nu doriţi aceşti utilizatori să aibă System i profil utilizator sau alte identitatăţi utilizator intern.

Un certificat digital se comportă ca o acreditare electronică 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 număr unic în scopul identificării şi au o autoritate de emitere ce poate fi recunoscută, care permite verificarea autenticităţii acreditării. În cazul unui certificat, o funcţie CA de încredere, a treia parte care emite certificatul şi verifică este o acreditare autentică.

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. Actualmente,aceste aplicaţiiSystem i furnizează suport autentificare certificat client:

- Server Telnet
- IBM HTTP Server for i5/OS (monitorizat de Apache)
- IBM Tivoli Directory Server for i5/OS
- System i Access pentru Windows (inclusiv NavigatorulNavigator System i)
- 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 SSL (Secure Sockets Layer) pentru a cripta sesiuni de comunicare.

Concepte înrudite

"Certificatele digitale pentru comunicaţiile sigure SSL" la pagina 35
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.

Referinţe înrudite

"Folosirea API-urilor pentru a emite programatic certificate altor utilizatori decât utilizatorii System i" la pagina 48
CA-ul local al dumneavoastră poate emite certificate private pentru utilizatori fără să asocieze certificatul cu un profil de utilizator System i.

Certificatele digitale şi EIM

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.

EIM vă permite să gestionaţi identităţi utilizator în întreprinderea dumneavoastră, incluzând profile 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 identitatea utilizator necesară. Realizaţi asta în EIM prin definirea unei asociaţii între o identitatea 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 utilizator 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 taskuri de configurare EIM înainte de a realiza orice taskuri de configurare DCM:

1. Folosiţi vrăjitorul **Configurare EIM** din **Navigator System i** 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 utilizatori i5/OS local, astfel încât orice certificat de utilizator pe care utilizatorul îl alocă 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 utilizatori **i5/OS** local pe care l-aţi specificat în vrăjitorul **Configurare EIM**.

După ce realizaţi taskurile de configurare EIM necesare, trebuie să folosiţi taskul **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, taskul **Creare certificat** pentru certificate utilizator şi taskul **Alocare certificat utilizator** procesează certificatele pentru utilizare EIM mai degrabă decât să aloce 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 împreuna puteţi folosi DCM pentru a verifica expirarea certificatelor utilizator la nivel de întreprindere mai degrabă decât la nivel de sistem.

Concepte înrudite

"Certificatele publice şi certificatele private" la pagina 33
Puteţi folosi certificate de la un CA publică 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.

Operaţii înrudite

"Gestionarea certificatelor pe baza expirării" la pagina 47
DCM oferă suport de gestionare a expirării certificatelor, pentru a permite administratorilor să verifice datele de expirare a certificatelor utilizatorilor pe modelul System i local. Suportul de gestionare a expirării certificatelor DCM poate fi utilizat împreună cu EIM astfel încât administratorii să poată utiliza DCM să verifice expirarea certificatelor de utilizator la nivel de întreprindere.

"Gestionarea locaţiei LDAP pentru certificate utilizator" la pagina 74
Puteţi folosi Digital Certificate Manager (DCM) pentru stocarea certificatelor de utilizator într-o locaţie de director a serverului LDAP, extinzând Enterprise Identity Mapping pentru a lucra cu certificate de utilizator.

Informaţii înrudite

Subiectul pentru Centrul de Informare EIM DNS

Certificatele digitale pentru conexiuni VPN

Puteţi folosi certificate digitale ca un mijloc de a stabili o System i conexiune VPN. Ambele capete ale unei conexiuni dinamice VPN trebuie să poată comunica pentru a se autentifica una alteia înainte de a se activa conexiunea.

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 utilizaţi CA-ul local în DCM la emiterea unui certificat puteţi specifica alternativ numele subiectului informaţiei pentru certificat. Specificând aceste informaţii, vă asiguraţi că aveţi o conexiune VPN compatibilă cu alte implementări VPN care au nevoie de ele pentru autentificare.

Concepte înrudite

"Gestionarea certificatelor de la un CA public din Internet" la pagina 50
Când utilizaţi DCM la gestionarea certificatelor de la un CA public din Internet, trebuie mai întâi să creaţi un depozit de certificate. Un depozit de certificate este un fişier special de bază de date de chei, pe care îl foloseşte DCM (Digital Certificate Manager) pentru a stoca certificate digitale şi cheile lor private asociate.

Operaţii înrudite

"Crearea şi operarea unui CA local" la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

"Definire listă de încredere CA pentru o aplicaţie" la pagina 67
Aplicaţiile care suportă folosirea certificatelor pentru autentificare client în timpul unei sesiuni SSL (Secure Sockets Layer) 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.

Informaţii înrudite

Configurarea unei conexiuni 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 semnare obiect sporeşte tradiţionalele System i modele de unelte care pot modifica obiecte. Elementele de control tradiţionale nu pot proteja un obiect de amestecare neautorizată în timp c e obiectul este în tranzit peste Internet sau altă reţea lipsită de încredere sau cât timp obiectul este memorat pe un sistem altul decât platforma System i. De asemenea, controalele tradiţionale nu pot determina întotdeauna 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, totuşi, intenţionaţi să distribuiţi obiecte doar în organizaţia dumneavoastră, s-ar putea să preferaţi DCM la operarea propriului dumneavoastră CA la emiterea de certificate pentru semnare obiecte. Utilizând certificate private de la un CA local pentru a semna obiecte este mai puţin scump decât a cumpăra certificate de la un binecunoscut CA public.

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. Deasemenea, puteţi folosi DCM pentru a semna obiecte şi pentru a verifica semnăturile obiectelor.

Concepte înrudite

“Certificatele publice şi certificatele private” la pagina 33
Puteţi folosi certificate de la un CA publică 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.

“Certificatele digitale pentru verificarea semnăturii obiectelor” la pagina 40
i5/OS oferă 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.

Operaţii înrudite

“Verificarea semnăturii obiectelor” la pagina 77
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.

“Gestionarea certificatelor publice din Internet pentru semnarea obiectelor” la pagina 52
Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona certificate Internet publice pentru a semna digital obiectele.

“Gestionarea certificatelor pentru verificarea semnăturii obiectelor” la pagina 54
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.

Certificatele digitale pentru verificarea semnăturii obiectelor

i5/OS oferă 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.

Există anumite valori pe care le puteţi utiliza pentru variabila sistem QVFYOBJRST, de la ignorarea tuturor semnăturilor la necesitatea semnăturilor valide pentru toate obiectele pe care sistemul le restaurează. Această valoare de sistem afectează doar obiectele executabile care sunt restaurate, nu fişierele salvare sau fişierele sistemului de fişiere integrat. Pentru a învăţa mai mult despre utilizarea acestuia şi alte valori de sistem, vedeţi Detector valori de sistem în Centrul de informare i5/OS.

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

Concepte înrudite

“Certificatele digitale pentru semnarea obiectelor” la pagina 39
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.

Informaţii înrudite

Detector valoare sistem

Valoare sistem QVFYOBJRST

Configurarea DCM

DCM furnizează o interfaţă de utilizator bazată pe Web pe care o puteţi folosi pentru a gestiona şi configura certificatele 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 taskurile care să administreze certificatele sau aplicaţiile care le folosesc. În timp ce unele taskuri individuale apar direct în cadrul principal de navigare, majoritatea taskurilor din cadrul de navigare sunt organizate în categorii. De exemplu, **Gestionare certificate** este o categorie de taskuri care conţine o varietate de taskuri 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 taskuri, asfel încât să puteţi alege taskul 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 taskul 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 taskuri înrudite dintr-un singur set central de pagini.

Taskurile care sunt disponibile în cadrul de navigare variază pe baza depozitului de certificate în care lucraţi. De asemenea, categoria şi numărul de taskuri pe care le vedeţi în cadrul de navigaţie variază în funcţie de autorizaţiile pe care le are profilul dumneavoastră de utilizator System i. Toate taskurile pentru operarea unui CA, pentru administrarea certificatelor pe care le folosesc aplicaţiile şi alte taskuri la nivelul de sistem sunt disponibile numai pentru System i responsabilii cu securitatea sau administratori. Responsabilul cu securitate sau administratorul trebuie să deţină autorizările speciale *SECADM şi *ALLOBJ pentru a vizualiza şi utiliza aceste procese. Utilizatorii fără aceste autorizări speciale au acces doar la funcţiile de certificare utilizator.

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

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 .

Pornirea DCM

Înainte de a putea utiliza orice caracteristică din Digital Certificate Manager (DCM), trebuie să îl porniţi pe sistem.

Finalizaţi următoarele taskuri pentru a vă asigura că puteţi porni DCM cu succes:

1. Instalaţi Digital Certificate Manager.
2. Instalaţi IBM HTTP Server for i5/OS.
3. Folosiţi Navigator System i pentru a porni serverul administrativ server HTTP:
   a. În Navigator System i, expandaţi **sistemul dumneavoastră → Reţea → Servere → TCP/IP**.
   b. Efectuaţi un clic dreapta pe **Administrare HTTP**.
   c. Selectaţi **Pornire**.
4. Deschideţi un browser web şi introduceţi http://numele_sistemului_dumneavoastră:2001 ca să încărcaţi consola web IBM Systems Director Navigator for i5/OS.
5. Din pagina de bun venit faceţi clic pe legătura **Pagina Taskuri i5/OS**.
6. Selectaţi **Digital Certificate Manager** din lista de produse din pagina Taskuri i5/OS pentru a accesa interfaţa de utilizator DCM.

Concepte înrudite

“Scenariu: Folosirea certificatelor pentru autentificarea externă” la pagina 12
Acest scenariu descrie când şi cum să folosiţi certificate ca un mecanism de autentificare pentru a proteja şi limita accesul utilizatorilor publici la resurse publice sau din afara reţelei şi la aplicaţii.

Setarea certificatelor 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 taskuri pentru gestionarea certificatelor şi a aplicaţiilor care le folosesc.

Care taskuri sunt disponibile depinde de ce depozit de certificate (dacă există unul) cu care lucraţi şi de autorizările speciale ale profilului utilizator. Majoritatea taskurilor 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 un depozit de certificate. În consecinţă, când accesaţi iniţial DCM, panoul de navigaţie afişează doar aceste taskuri 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 utilizaţi 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.
- Întoarcere la i5/OS pagina Taskuri.

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 taskuri sau categorii de taskuri în cadrul de navigaţie stâng. Care taskuri sau categorii DCM afişează variaţii bazate pe depozitul de certificate care este deschis şi autorizaţiile speciale pentru profilul utilizator al dumneavoastră.

Trebuie să accesaţi mai întâi depozitul necesar de certificate înainte de a putea începe lucrul cu majoritatea taskurilor 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 IBM HTTP Server for i5/OS 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 creţi să folosiţi certificate private sau emiterea de certificate private.

Concepte înrudite

“Certificatele publice şi certificatele private” la pagina 33
Puteţi folosi certificate de la un CA publică 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.

Crearea şi operarea unui CA local

Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

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 taskului 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 IBM HTTP Server for i5/OS, 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 aloce un certificat către server. Dacă opriţi şi reporniţi instanţa *ADMIN a serverului Web înainte de a-i aloca un certificat, serverul nu va porni şi nu veţi putea folosi DCM pentru a aloca un certificat serverului.

Pentru a utiliza DCM la crearea şi operareaunui CA local, urmăriţi aceşti paşi:

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigare al DCM, selectaţi Crearea unui CA pentru a se afişa o serie de formulare. Aceste formulare vă ghidează prin procesul de creare a unui CA local şi finalizarea altor taskuri necesare pentru a începe utilizarea certificatelor digitale pentru SSL, semnare obiect şi verificare semnătură.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în taskul asistat, selectaţi semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.
3. Completaţi toate formularele pentru acest task. În utilizarea acestor formulare pentru a realiza toate taskurile care vă trebuiesc pentru a seta o autoritate de certificare locală (CA) funcţională, dumneavoastră:
   a. Alegeţi cum să memoraţi cheia privată pentru certificatul CA local. (Acest pas este furnizat doar dacă aveţi un IBM Cryptographic Coprocessor instalat pe sistemul dumneavoastră Dacă sistemul dumneavoastră nu are un coprocesor criptografic, automatDCM memorează certificatul şi cheia sa privată în depozitul de certificate al autorităţii de certificare local.)
   b. Furnizaţi informaţii identificatoare pentru CA-ul local.
   c. Instalaţi certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră în aşa fel încât software-ul dumneavo astră să poată recunoaşte CA-ul local şi să valideze certificate pe care CA-ul le emite.
   d. Alegeţi datele politicii pentru propriul CA local.
   e. Utilizaţi noul CA local la emiterea unui certificat server sau client pe care aplicaţiile dumneavoastră îl poate folosi pentru conexiunile SSL. (Dacă sistemul dumneavoastră are un IBM Cryptographic Coprocessor 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 creează 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 publică din Internet, nu efectuaţi acest lucru sau pasul anterior.
   g. Utilizaţi noul CA local pentru emiterea unui certificat de semnare obiect pe care aplicaţiile îl pot folosi pentru semnarea digitală a obiectelor. Acest subtask creează 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 publică din Internet, nu efectuaţi acest lucru sau pasul anterior.
   i. Selectaţi aplicaţiile pe care le veţi încrede CA-ului local al dumneavoastră.

Când sfârşiţi taskul îndrumat, aveţi tot ce vă trebuie să începeţin configurarea aplicaţiilor dumneavoastră la utiliza rea SSL pentru comunicaţii în siguranţă.

După ce configuraţi aplicaţiile dumneavoastră, utilizatorii care accesează apli caţiile printr-o conexiue SSL trebuie să utilizeze 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 utiliza DCM fie pentru a copia certificatul CA local la un fişier sau pentru a descărca certificatul în browser-ul lor. Cum utilizatorii memorează certificatul CA local depinde de software-ul client pe care îl utilize ază pentru a stabili o conexiune SSL la o aplicaţie .

De asemenea, puteţi utiliza CA local pentru a emite certificate la aplicaţii pe alte modele System i în reţeaua dumneavoastră.

Pentru a învăţa mai mult despre utilizarea DCM la gestionarea certificatelor utilizator şi cum utilizatoriipot obţine o copie a CA-ului local pentru a autentfica certificatele emise de CA-ul local, revedeţi aceste subiecte:

Concepte înrudite

"Certificatele publice şi certificatele private" la pagina 33
Puteţi folosi certificate de la un CA publică 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.

"Certificatele digitale pentru conexiuni VPN" la pagina 38
Puteţi folosi certificate digitale ca un mijloc de a stabili o System i conexiune VPN. Ambele capete ale unei conexiuni dinamice VPN trebuie să poată comunica pentru a se autentifica una alteia înainte de a se activa conexiunea.

"Gestionarea certificatelor de utilizator"
Puteţi folosi DCM (Digital Certificate Manager) pentru a obţine certificate cu SSL sau asocierea certificatelor existente cu profilurile de utilizator System i.

Operaţii înrudite

"Folosirea unui CA local la emiterea certificatelor pentru alte modele System i" la pagina 58
Folosind DCM, puteţi configura un CA local privat pe un sistem care să emită certificate pentru utilizarea pe alte platforme System i.

"Obţinerea unei copii de certificat CA privat" la pagina 49
Atunci când accesaţi un server care foloseşte o conexiune SSL (Secure Sockets Layer), 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.

"Semnarea obiectelor" la pagina 75
Sunt trei tipuri diferite de metode pe care le puteţi utiliza pentru semnarea obiectelor. Pentru a semna un obiect puteţi scrie un program care apelează Semnare obiect API, utilizaţi DCM sau utiliza caracteristica Navigator System i Administrare centrală pentru pachetele pe care le distribuiţi la alte sisteme.

Referinţe înrudite

"Folosirea API-urilor pentru a emite programatic certificate altor utilizatori decât utilizatorii System i" la pagina 48
CA-ul local al dumneavoastră poate emite certificate private pentru utilizatori fără să asocieze certificatul cu un profil de utilizator System i.

Gestionarea certificatelor de utilizator:

Puteţi folosi DCM (Digital Certificate Manager) pentru a obţine certificate cu SSL sau asocierea certificatelor existente cu profilurile de utilizator System i.

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 publică, 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 utilizează un certificat de la un CA local privat, utilizatorii dumneavoastră trebuie să obţină o copie a certificatului CA local înainte ca ei să poată stabili o seseiune 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. Depinzând de cerinţele sistemului dumneavoastră,utilizatorii prezintă un certificat de la un CA internet public sau unul pe care îl obţin de la un CA pe care operaţi. Dacă aplicaţia server a dumneavoastră furnizează acces la resurse pentru utilizatorii interni care au în acest moment System i 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 alocate unui profil de utilizator System i. 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 nici un depozit de certificate nu este deschis, sau când depozitul de certificate al autorităţii de certificare (CA) este deschis, puteţi selecta **Gestionare certificate utilizator** din cadrul de navigaţie pentru a accesataskurile apropiate. Dacă este deschis un depozit de certificate diferit, taskurile certificat utilizator sunt integrate în taskuri sub **Gestionarea certificatelor**.

Utilizatorii fără autorizările speciale de profil de utilizator *SECADM şi *ALLOBJ îşi pot gestiona doar propriile alocări de certificate. Ei pot selecta **Gestionare certificate Utilizator** pentru a accesa taskuri care le permit să vizualizeze certificatele asociate cu profilurile lor de utilizator, să şteargă un certificat din profilurile lor de utilizator sau să aloce un certificat de la un CA diferit la profilurile lor de utilizator. Utilizatorii, în ciuda autorităţiilor speciale pentru profilele lor utilizator, pot obţine un certificat utilizator de la CA-ul local selectând taskul **Creare certificat** în cadrul principal de navigaţie.

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

Operaţii înrudite

“Crearea şi operarea unui CA local” la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

“Obţinerea unei copii de certificat CA privat” la pagina 49
Atunci când accesaţi un server care foloseşte o conexiune SSL (Secure Sockets Layer), 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.

Crearea certificatului de utilizator:

Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă utilizaţi DCM pentru a opera o autoritate de certificare local privată (CA), puteţi utiliza CA-ul local pentru emite certificate la fiecare utilizator.

Fiecare utilizator trebuie să acceseze DCM pentru a obţine un certificat folosind taskul **Crearea certificatelor.**. Pentru a obţine un certificat de la CA-ul local, politica CA trebuie să permite CA-ului să emită certificate de utilizator.

Pentru a obţine un certificat de la CA-ul local, finalizaţi aceşti paşi:

1. Porniţi DCM. Vedeţi Pornirea 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 taskul 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 taskuri. 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 taskul.

În timpul procesării, DCM (Digital Certificate Manager) asociază automat certificatul cu System i profilul dumneavoastră 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 alocarea certificatului la profilurile lor utilizator.

Concepte înrudite

"Certificatele publice şi certificatele private" la pagina 33
Puteţi folosi certificate de la un CA publică 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.

Operaţii înrudite

"Alocarea unui certificat de utilizator"
Puteţi să alocaţi un certificat pe care îl deţineţi la profilul utilizator i5/OS sau la altă identitate de utilizator. Certificatul poate fi de la un CA local privat pe alt sistem sau de la un bine cunoscut internet CA. Pentru a aloca 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.

"Obţinerea unei copii de certificat CA privat" la pagina 49
Atunci când accesaţi un server care foloseşte o conexiune SSL (Secure Sockets Layer), 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.

Alocarea unui certificat de utilizator:

Puteţi să alocaţi un certificat pe care îl deţineţi la profilul utilizator i5/OS sau la altă identitate de utilizator. Certificatul poate fi de la un CA local privat pe alt sistem sau de la un bine cunoscut internet CA. Pentru a aloca 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.

Unii utilizatori pot avea certificate de la o autoritate de certificare (CA) exterioară sau o CA locală pe un sistemdiferit iSeries pa care dumneavoastră, ca administrator, vreţi să le faceţi disponibile la DCM. Asta vă permite dumneavoastră şi utilizatorului să folosiţi DCM pentru a gestiona aceste certificate, care sunt cel mai adesea folosite pentru autentificarea client. Taskul **Alocare certificat utilizator** furnizează un mecanism pentru a permite unui utilizator să creeze o alocare DCM pentru un certificat obţinut dintr-un CA din afară.

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

- Memorare certificat local pe System i cu profilul utilizator al acestuia. Când o locaţie LDAP nu este definită pentru DCM, taskul **Alocare un certificat utilizator** ermite unui utilizator să aloce un certificat din afară unui i5/OS profil utilizator. Alocarea 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 o locaţie definită LDAP şi modelul System i este configurat să participe în EIM, atunci taskul **Alocare certificat utilizator** permite unui utilizator să memoreze o copie of ana unui certificat exterior în directorul LDAP specificat. DCM creează de asemenea o asociere sursă în EIM pentru certificat. Memorarea certificatul în această 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 aloca 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 a folosi taskul **Alocare 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 **Alocare 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 taskul. (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 aloca 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.

   Operaţii înrudite

   “Crearea certificatului de utilizator” la pagina 45
   Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă utilizaţi DCM pentru a opera o autoritate de certificare local privată (CA), puteţi utiliza CA-ul local pentru emite certificate la fiecare utilizator.

   “Depanarea alocării unui certificat de utilizator” la pagina 84
   Utilizaţi următorii paşi pentru a vă ajuta să depanaţi orice probleme pe care le puteţi întâmpina în timp ce încercaţi să alocaţi un certificat utilizator cu DCM.

   Informaţii înrudite

   Subiectul pentru Centrul de Informare EIM

Gestionarea certificatelor pe baza expirării:

DCM oferă suport de gestionare a expirării certificatelor, pentru a permite administratorilor să verifice datele de expirare a certificatelor utilizatorilor pe modelul System i local. Suportul de gestionare a expirării certificatelor DCM poate fi utilizat împreună cu EIM astfel încât administratorii să poată utiliza DCM să verifice expirarea certificatelor de 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. Vedeţi Pornirea DCM.

Notă: Dacă aveţi întrebări despre completarea unui anume formular în timp ce folosiţi DCM, selectaţi butonul cu semnul de întrebare (**?**) 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 taskuri.

   Notă: Dacă lucraţi curent cu un depozit de certificate, selectaţi **Gestionare certificate** pentru a afişa o listă de taskuri, 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 alocate un profil utilizator i5/OS 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.

Operaţii înrudite

"Certificatele digitale şi EIM" la pagina 37
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.

"Gestionarea certificatelor prin expirare" la pagina 68
DCM oferă suport de gestionare a expirării certificatelor, pentru a permite administratorilor să gestioneze certificate server sau client, certificate de semnare obiect, certificare CA şi certificate de utilizator prin data de expirare de pe sistemul local.

Informaţii înrudite

Subiectul pentru Centrul de Informare EIM

Folosirea API-urilor pentru a emite programatic certificate altor utilizatori decât utilizatorii System i:

CA-ul local al dumneavoastră poate emite certificate private pentru utilizatori fără să asocieze certificatul cu un profil de utilizator System i.

| API-ul de generare şi cerere certificat (QYCUGSUC) şi API-ul de cerere certificat semnare utilizator (QYCUSUC) vă
| permit să emiteţi programatic certificate pentru alţi utilizatori decât utilizatorii System i. Asocierea certificatului cu un
| profil de utilizator System i are avantajele sale, în special când este vorba de utilizatori interni. Însă aceste restricţii şi
| cerinţe au făcut mai puţin practică utilizarea CA-ului local pentru a emite certificate de utilizator pentru un număr mare
| de utilizatori, în special când nu vreţi ca aceşti utilizatori să aibă un profil de utilizator System i. Pentru a nu le da
| acestor utilizatori profiluri de utilizator, le-aţi putea cere să plătească pentru un certificat de la un CA binecunoscut,
| dacă doriţi să cereţi certificate pentru autentificarea utilizatorilor aplicaţiilor dumneavoastră.

Aceste două API-uri vă permit să furnizaţi o interfaţă pentru crearea certificatelor de utilizator semnate de certificatul CA local pentru orice nume de utilizator. Acest certificat nu va fi asociat cu un profil de utilizator. Utilizatorul nu trebuie să existe pe sistemul care găzduieşte DCM şi nu trebuie să utilizeze DCM pentru a crea certificatul.

Există 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 furnizeze codul interfeţei grafice de utilizator necesare pentru a crea certificatul de utilizator şi a apela unul dintre API-urile corespunzătoare pentru a utiliza CA-ul local la semnarea certificatului.

Concepte înrudite

"Certificatele publice şi certificatele private" la pagina 33
Puteţi folosi certificate de la un CA publică 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.

"Certificatele digitale pentru autentificarea utilizatorului" la pagina 36
Tradiţional, utilizatorii primesc acces la resurse de la o aplicaţie sau sistem pe baza numelui de utilizator şi a parolei. Se poate creşte securitatea sistemului prin utilizarea certificatelor digitale (în locul numelor de utilizatori şi a parolelor) pentru a autentifica şi autoriza sesiunile dintre mai multe aplicaţii server utilizatori.

Operaţii înrudite

"Crearea şi operarea unui CA local" la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

Informaţii înrudite

API-ul de generare şi cerere a certificatului de semnare utilizator (QYCUGSUC)

API-ul de cerere certificat desemnare utilizator (QYCUSUC)

Obţinerea unei copii de certificat CA privat:

Atunci când accesaţi un server care foloseşte o conexiune SSL (Secure Sockets Layer), 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. Dacă, totuşi, server-ul prezintă un certificat de la un CA local privat, trebuie să utilizaţi DCM pentru a obţine o copie a certificatului CA local.

Când utilizaţi DCM pentru a descărca certificatul local CA direct în browser-ul dumneavoastră, sau puteţi copia certificatul local CA într-un fişier pentru ca alt software client il poate accesa şi utiliza. Dacă utilizaţi atât browser-ul cât şi alte aplicaţii comunicaţii sigure, s-ar putea să aveţi nevoie să utilizaţi 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 prin prezentarea unui certificat de la CA-ul local, trebuie să descărcaţi certificatull CA local în browser-ul dumneavoastră înainte să cereţi un certificat utilizator din CA-ul local.

Pentru a utiliza DCM la obţinereaunei copii a unui certificat CA local, finalizaţi aceşti paşi:

1. Porniţi DCM. Vedeţi Pornirea 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 îl memoraţi într-un fişier de 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 client să poată recunoaşte şi utiliza certificatul CA local pentru autentificare, trebuie să c onfiguraţi 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.

Concepte înrudite

"Gestionarea certificatelor de utilizator" la pagina 44
Puteţi folosi DCM (Digital Certificate Manager) pentru a obţine certificate cu SSL sau asocierea certificatelor existente cu profilurile de utilizator System i.

Operaţii înrudite

"Crearea şi operarea unui CA local" la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

"Crearea certificatului de utilizator" la pagina 45
Dacă doriţi să folosiţi certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să deţină certificate. Dacă utilizaţi DCM pentru a opera o autoritate de certificare local privată (CA), puteţi utiliza CA-ul local pentru emite certificate la fiecare utilizator.

Gestionarea certificatelor de la un CA public din Internet

Când utilizaţi DCM la gestionarea certificatelor de la un CA public din Internet, trebuie mai întâi să creaţi un depozit de certificate. Un depozit de certificate este un fişier special de bază de date de chei, pe care îl foloseşte DCM (Digital Certificate Manager) pentru a stoca certificate digitale şi cheile lor private asociate.

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 clienţilor.

Puteţi utiliza taskurile ghidate din DCM la gestionare centrală a acestor certificate publice şi a aplicaţiilor care le utilizează pentru stabilirea conexiunilor SSL, semnarea obiectelor sau verificarea autenticităţii semnăturilor digitale pe obiecte.

Gestionarea certificatelor 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 taskurile pe care trebuie să le efectuaţi ulterior pentru gestionarea certificatelor şi a aplicaţiilor care le folosesc, depinde de modul în care doriţi să folosiţi certificatele.

Notă: 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).

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:

Concepte înrudite

"Certificatele publice şi certificatele private" la pagina 33
Puteţi folosi certificate de la un CA publică 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.

"Certificatele digitale pentru conexiuni VPN" la pagina 38
Puteţi folosi certificate digitale ca un mijloc de a stabili o System i conexiune VPN. Ambele capete ale unei conexiuni dinamice VPN trebuie să poată comunica pentru a se autentifica una alteia înainte de a se activa conexiunea.

Operaţii înrudite

"Gestionarea locaţiei cererii pentru un PKIX CA" la pagina 73
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.

Gestionarea certificatelor publice din Internet 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 SSL (Secure Sockets Layer).

Dacă nu utilizaţi DCM pentru a opera propria dumneavoastră Autoritate de certificare (CA), trebuie mai întâi să creaţi depozitul de certificate corespunzător pentru gestionarea certificatelor publice 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. Vedeţi Pornirea DCM.
2. În cadrul de navigare al DCM, selectaţi **Crearea unui nou depozit de certificate** pentru a porni taskul 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 taskul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Selectaţi ***SYSTEM** ca depozit de certificate 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.

   Notă: Dacă pe server este instalat IBM Cryptographic Coprocessor, DCM vă permite să selectaţi cum să memoraţi cheia privată pentru certificat ca taskul următor. Dacă sistemul nu are un coprocesor, DCM va plasa automat cheia privată în depozitul de certificate *SYSTEM. Dacă aveţi nevoie de ajutor la selectarea modului de depozitare al cheii private, consultaţi ajutorul online al DCM.
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 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.

Pentru a folosi certificate cu serverul HTTP pentru sistemul dumneavoastră, 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 aloce certificatul complet semnat către server. Dacă opriţi şi reporniţi instanţa *ADMIN a serverului Web înainte de a-i aloca un certificat, serverul nu va porni şi nu veţi putea folosi DCM pentru a aloca un certificat serverului.

8. Porniţi DCM după ce CA publică vă întoarce certificatul semnat.
9. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SYSTEM** pentru ca să se deschidă depozitul de certificate.
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. După ce se reafişează cadrul de navigare, selectaţi **Gestionarea certificatelor** pentru a afişa o listă de taskuri.
12. Din lista de taskuri, 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 taskuri.
14. Din lista de taskuri, selectaţi **Actualizarea atribuirii certificatelor** pentru a se afişa o listă de aplicaţii activate-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 activate-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.

Când finalizaţi operaţia ghidată, aveţi tot ce vă trebuie pentru a începe configurarea aplicaţiilor dumneavoastră pentru a utiliza 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 publice din Internet pentru semnarea obiectelor:

Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona certificate Internet publice pentru a semna digital obiectele.

Dacă nu utilizaţi DCM pentru a opera supra propriei autorităţi de certificare (CA), trebuie ca mai întâi să creaţi d epozitul de certificate corespunzător pentru gestionare certificatelor corespunzătoare pe care le utilizaţi 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 Navigator System i.)

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

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigaţie stâng al DCM, selectaţi **Creare depozit de certificate nou** pentru a porni taskul 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 care este în taskul 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 clic 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 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.
8. Porniţi DCM după ce CA publică vă întoarce certificatul semnat.
9. În cadrul de navigaţie 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 fereastra de navigare, selectaţi **Gestionare certificate** pentru a afişa o listă a taskurilor.
12. Din lista de taskuri, 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 reîmprospătează, selectaţi **Gestionare aplicaţii** pentru a afişa o listă a taskurilor.
14. Din lista de taskuri, 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 taskuri Gestionarea aplicaţiilor.
17. Din lista de taskuri, selectaţi **Actualizare alocare certificate** şi apăsaţi **Continuare** pentru a afişa o listă de ID-uri de aplicaţii de semnare obiecte pentru care puteţi aloca 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 taskuri, 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 utilizeze OS/400 V5R1 sau versiuni ulterioare ale DCM-ului pentru a valida semnătura pe obiecte pentru a se asigura că datele sunt nemodificate şi să verifice identificarea celui care a trimis. 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, 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 local CA dacă aţi semnat obiectele cu un certificat de la un CA privat 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.

Concepte înrudite

“Certificatele digitale pentru semnarea obiectelor” la pagina 39
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.

Operaţii înrudite

“Verificarea semnăturii obiectelor” la pagina 77
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.

“Semnarea obiectelor” la pagina 75
Sunt trei tipuri diferite de metode pe care le puteţi utiliza pentru semnarea obiectelor. Pentru a semna un obiect puteţi scrie un program care apelează Semnare obiect API, utilizaţi DCM sau utiliza caracteristica Navigator System i Administrare centrală pentru pachetele pe care le distribuiţi la alte sisteme.

Gestionarea certificatelor pentru verificarea semnăturii 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, totuşi,obiectul a fost semnat de un certificat de alt CA local sau privat, trebuie să obţineţi o copie a certificatu lui CA înainte să puteţi verificasemnătura obiectului.

Pentru a folosi DCM pentru verificarea semnăturilor obiectelor , trebuie să creaţi mai întâi depozitul de certificate necesar pentru gestionarea certificatelor necesare 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 taskuri:

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigaţie stâng al DCM, selectaţi **Creare depozit de certificate nou** pentru a porni taskul ghidat şi a efectua o serie de formulare.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în taskul 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 clic 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. 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** pentru ca să se deschidă 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 taskuri.
8. Din lista de taskuri, selectaţi **Import certificat**. 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 taskul 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.

Concepte înrudite

“Certificatele digitale pentru semnarea obiectelor” la pagina 39
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.

Operaţii înrudite

“Verificarea semnăturii obiectelor” la pagina 77
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.

Reînnoirea unui certificat existent

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

Puteţi reînnoi un certificat cu CA-ul local sau cu un CA Internet.

Reînnoirea unui certificat de la CA-ul local

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

Pentru a reînnoi un certficat cu CA urmaţi aceşti paşi:

1. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate**, şi selectaţi depozit de certificate pe care să-l deschideţi.
2. În cadrul de navigare, selectaţi **Gestionare certificate**.
3. În cadrul de navigare, selectaţi **Reînnoire certificate**.
4. Selectaţi certificatul pe care doriţi să îl reînnoiţi şi selectaţi **Reînnoire**.
5. Selectaţi **Autoritate de certificare locală (CA)** şi faceţi clic pe **Continuare**.
6. Completaţi formularul identificare certificat. Trebuie să schimbaţi câmpul **Etichetă de certificat nouă** dar orice alte câmpuri pot rămâne la fel.
7. Selectaţi orice aplicaţie căruia doriţi să îi reînnoiţi certificatul şi faceţi clic pe **Continuare** pentru a termina reînnoirea certificatului.

   Notă: Nu trebuie să selectaţi o aplicaţie pentru a folosi certificatul.

Reînnoirea unui certificat de la un CA din Internet

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.

Puteţi reînnoi un certificat direct cu CA-ul Internet şi apoi să importaţi certificatul reînnoit din fişierul pe care l-aţi primit de la CA-ul de semnare. Altă cale prin care puteţi reînnoi certificatul este să utilizaţi DCM pentru a crea o nouă pereche de chei public- private şi Cerere semnare certificat (CSR) pentru certificat şi apoi trimiteţi această informaţi la CA-ul internet pentru a obţine un nou certificat. Când primiţi înapoi certificatul de la CA, atunci puteţi termina procesul de reînnoire.

Importarea şi reînnoirea unui certificat obţinut direct de la CA-ul de internet:
Pentru importarea şi reînnoirea unui certificat obţinut direct de la Internet CA, urmăriţi paşi:

1. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate** şi selectaţi depozitul de certificate pe care să-l deschideţi.

   Notă: Faceţi clic pe butonul ?. pentru orice panou de răspuns la orice panou de întrebări, aveţi despre completarea panourilor.
2. În cadrul de navigare, selectaţi **Gestionare certificate**.
3. În cadrul de navigare, selectaţi **Reînnoire certificate**.
4. Selectaţi certificatul pe care doriţi să îl reînnoiţi şi selectaţi **Reînnoire**.
5. Selectaţi **VeriSign** alt **CA Internet** şi efectuaţi un clic pe **Continuare**.
6. Selectaţi **Nu - Imporaţi certificatul nou semnat din fişierul existent**.
7. Completaţi ghidurile pentru a importa certificatul. Când alegeţi să reînnoiţi certificatul direct cu CA emis, CA reutnează certificatul reînnoit într-un fişier. Fiţi sigur că aţi specificat calea absolut corectă unde certificatul este memorat pe server. Fişierul care conţine certificatul reînnoit poate fi memorat într-un director IFS (integrated file system).
8. Apăsaţi **OK** pentru a termina taskul.

Reînnoirea unui certificat prin crearea unei noi chei publice-private şi CSR pentru certificat:

Pentru a reînnoi un certificat cu un CA Internet prin crearea unei noi perechi cheie publică-privată şi CSR pentru certificat, urmaţi aceşti paşi:

1. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate**, şi selectaţi depozit de certificate pe care să-l reînnoiţi.

   Notă: Faceţi clic pe butonul ?. pentru orice panou de răspuns la orice panou de întrebări, aveţi despre completarea panourilor.
2. În cadrul de navigare, selectaţi **Gestionare certificate**.
3. În cadrul de navigaţie, selectaţi **Reînnoire certificat**
4. Selectaţi certificatul pe care doriţi să îl reînnoiţi şi selectaţi **Reînnoire**.
5. Selectaţi **VeriSign** alt **CA Internet** şi efectuaţi un clic pe **Continuare**.
6. Faceţi clic pe **Da - Creează o nouă pereche cheie pentru acest certificat şi apăsaţi Continuare**.
7. Completaţi formularul identificare certificat. Trebuie să schimbaţi eticheta Certificat Nou, dar celelalte câmpuri pot rămâne la fel. Notă: Faceţi clic pe butonul ?. pentru orice panou de răspuns la orice panou de întrebări, aveţi despre completarea panourilor.
8. Apăsaţi **OK** pentru a termina taskul.

Importarea unui certificat

Puteţi folosi Digital Certificate Manager (DCM) pentru a importa certificate care sunt localizate în fişiere de pe sistemul dumneavoastră. Puteţi de asemenea să importaţi un certificat din alt server în loc să recreaţi certificatul pe serverul curent.

De exemplu, pe System A aţi utilizat CA-ul local pentru a crea un certificat pentru aplicaţia web cu bucata pentru a utiliza iniţierea conexiunilor SSL. Afacerea dumneavoastră a crescut recent şi aţi instalat un nou model System i (System B) pentru a găzdui mai multe instanţe ale acestei aplicaţii cu bucata foarte ocupată. Dumneavoastră doriţi ca toate instanţele aplicaţiei retail să folosească certificate identice pentru identificarea lor şi să iniţieze conexiuni SSL. În consecinţă, aţi putea decide să importaţi ambele certificate locale CA şi certificatul server din System A la System B mai degrabă decât să utilizaţi CA-ul local pe System A pentru a crea un certificat nou, diferit pentru System B să îl utilizeze.

Parcurgeţi următorii paşi pentru a utiliza DCM:

1. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate** şi selectaţi depozitul de certificate pe care să-l deschideţi. Certificatul memorat în care importaţi trebuie să conţină certificate de acelaşi tip ca şi certificatele exportate pe alte sisteme. De exemplu, daca importaţi un certificat de server atunci importaţi-l într-un depozit de certificate care conţine certificate de server cum ar fi *SYSTEM sau Alt depozit sistem de certificate.
2. În cadrul de navigare, selectaţi **Gestionare certificate**.
3. În cadrul de navigare, selectaţi **Import certificate**.
4. Selectaţi tipul de certificat pe care doriţi să-l importaţi şi apăsaţi **Continuare**. Tipul de certificat pe care îl importaţi trebui să fie de acelaşi tip cu certificatul exportat. De exemplu, dacă aţi exportat un certificat server selectaţi să importaţi un certificat server.

   Notă: Când DCM exportă un certificat în format pkcs12, CA emitent este inclus în lanţul de certificatele exportate şi este, deci, automat importat când însuşi certificatul este importat de DCM în depozitul de certificate. Totuşi, dacă certificatul nu este exportat în format pkcs12 şi nu doriţi să aveţi în depozitul de certificate un certificat CA, trebuie să importaţi certificatul CA-ului emitent înainte de a importa certificatul.
5. Completaţi taskurile asistate pentru a importa certificatul. Când importaţi certificatul fiţi sigur că aţi specificat calea absolut corect unde certificatul este depozitat pe server.

Gestionarea DCM

După ce aţi configurat DCM, trebuie în timp să mai realizaţi nişte taskuri de gestiune certificate.

Pentru a afla cum să folosiţi DCM pentru a vă gestiona certificatele dumneavoastră , revedeţi aceste subiecte:

Folosirea unui CA local la emiterea certificatelor pentru alte modele System i

Folosind DCM, puteţi configura un CA local privat pe un sistem care să emită certificate pentru utilizarea pe alte platforme System i.

Puteţi deja să utilizaţi o autoritate de certificare privat locală (CA) pe un sistem din reţeaua dumneavoastră. Acum, doriţi să extindeţi folosinţa acestui CA local la alt sistem în reţeaua dumneavoastră. De exemplu, doriţi ca CA-ul dumneavoastră să emită un certificat client sau server pentru o aplicaţie pe alt sistem la utilizarea pentru sesiuni de comunicaţii SSL. Sau doriţi să utilizaţi certificate din CA-ul local pe un sistem pentru s emnare obiecte pe care le memoraţi pe alt server.

Puteţi realiza această ţintă folosind DCM. Realizaţi unele dintre taskuri pe sistemul pe care operaţi CA-ul local şi realizaţi altele pe sistemul secundar care găzduieşte aplicaţiile pentru care doriţi să emiteţi certificate. Acest sistem secundar este denumit sistemul destinaţie. Taskurile pe care trebuie să le realizaţi pe sistemul destinaţie depind de versiunea acelui sistem.

Notă: Puteţi întâlni o problemă dacă sistemul pe care operaţi CA-ul local utilizează un produs furnizor de acces criptografic care furnizează criptare mai puternică decât sistemul ţintă. Când exportaţi certificatul (cu cheia sa privată), sistemul criptează conţinutul fişierului de protejat. 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.

Put eţi utiliza CA-ul dumneavoastră local pentru a emite certificate la alte sisteme, pe care le puteţi apoi utiliza pentru semnat obiecte sau avea folosirea aplicaţiilor pentru stabilirea sesiunilor SSL. Când utilizaţi CA-ul local pentru a crea un certificat pentru utilizarea pe alt sistem, fişierele pe care DCM le creează conţin o copie a certificatului CA local, ca şi copiile certificatelor pentru multe CA-uri publice internet.

Taskurile pe care trebuie să le realizaţi în DCM variază foarte puţin depinzând de fiecare tip de certificat pe care CA-ul local al dumneavoastră îl emite şi nivelul ediţiei şi condiţiile pe sistemul ţintă.

E mitere certificate private pentru utilizarea pe un alt model System i

Pentru a utiliza CA-ul dumneavoastră local să emită certificate pentru utilizarea pe alt sistem, realizaţi aceşti paşi pe sistemul care găzduieşte CA-ul local:

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigare, selectaţi **Creare certificat** pentru a afişa o listă de tipuri de certificat pe care le puteţi utiliza CA-ul local la creare.

   Notă: Nu este nevoie să deschideţi un depozit de certificate pentru a realiza acest task. Aceste instrucţiuni presupun fie că nu lucraţi într-un depozit de certificate specific sau că lucraţi în depozitul de certificate al autorităţii de certificare (CA) locale. Un CA local trebuie să existe pe acest sistem înainte să puteţi realiza aceste taskuri. Dacă aveţi întrebări despre completarea unui anume formular care este în taskul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Selectaţi tipul de certificat pe care vreţi ca CA-ul local să îl emită şi faceţi clic pe **Continuare** pentru a începet taskul îndrumat şi completaţi un număr de formulare.
4. Selectaţi fie să creeze un **certificat server sau client pentru alt System i** (pentru sesiuni SSL) sau o **certificat semnare obiect pentru alt System i** (pentru utilizarea pe alt sistem).
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 creează aceste fişiere pe baza nivelului de ediţie al sistemului destinaţie pe care l-aţi specificat. DCM pune automat o copie a certif icatului CA local în acele fişiere.

DCM creează 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.

Concepte înrudite

"Considerente privind salvarea de rezervă şi recuperarea datelor DCM" la pagina 31
Parolele bazei de date de chei de criptare pe care le folosiţi ca să accesaţi depozitele de certificate în Digital Certificate Manager (DCM) sunt memorate (ascunse), într-un fişier de securitate special de pe sistemul dumneavoastră. Când folosiţi DCM pentru a crea un depozit de certificate pe sistemul dumneavoastră, DCM păstrează automat parola pentru dumneavoastră. Totuşi, trebuie să vă asiguraţi manual că DCM păstrează parolele de depozite de certificate în anumite circumstanţe.

"Certificatele publice şi certificatele private" la pagina 33
Puteţi folosi certificate de la un CA publică 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.

Operaţii înrudite

"Crearea şi operarea unui CA local" la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

Folosirea unui certificat privat pentru SSL

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.

Taskurile pentru utilizarea fişierelor depozit de certificate transferate pe care le-aţi creat pe sistemul gazdăautoritate de certificare locală (CA) variază bazat pe 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 puteţi ori să folosiţi fişierele transferate ca Depozit de certificate pe alt sistem sau importaţi fişierele transferate în depozitul de certificate *SYSTEM.

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 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 depozit de certificate (două fişiere: unul cu o extensie .KDB şi unul cu o extensie.RDB)pe care le-aţi creat pe sistemul care găzduieşte CA-ul local sunt în directorul /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, ca şi o copie a certificatului CA local, la fişierele depozit 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. Schimbarea 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** pentru ca să se deschidă depozitul de certificate.
5. Când pagina Depozit de certificate şi parolă se afişează, furnizaţi parola pe care aţi specificat-o pe sistemul gazdă pentru depozitul de certificat pentru sistemul ţintă şi faceţi clic pe **Continuare**.
6. În cadrul de navigare, selectaţi **Gestionare depozite de certificate** şi selectaţi **Schimbare parolă** din lista de taskuri. 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** pentru ca să se deschidă 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 taskuri.
10. Din lista de taskuri, selectaţi **Alocare 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 **Alocare la aplicaţii** pentru a afişa o listă de aplicaţii activate-SSL la care puteţi aloca 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 activate-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 taskuri finalizate, aplicaţii de pe sistemul ţintă pot utiliza certificatul utilizat de CA-ul local pe alt sistem. 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 utilizeze DCM pentru a obţineo copie a certificatului CA local de la sistemul gazdă. Certificatul CA local trebuie copiat la un fişier de pe PC-ul utilizatorului sau descărcat în browser-ul web, depinzând de necesităţile aplicaţiei activate 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. Puteţi alege să folosiţi fişierele certificate transferate ca un **Depozit de certificate de pe alt sistem**. Sau, puteţi alege săimportaţi certificatul privat şi certificatul corespondent CA-ului local 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 System i (şi, probabil, şi multe aplicaţii ale altor dezvoltatori de software) sunt scrise pentru a folosi certificate numai din 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 System i standard activate pentru SSL să folosească acest certificat. Dacă doriţi să folosiţi certificatul pentru aplicaţii System i, 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, 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 **Gestionare depozite de certificate** şi selectaţi **Schimbare parolă** din lista de taskuri. 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** pentru ca să se deschidă 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 taskuri.

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 sistemul dumneavoastră. 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:

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 **Gestionare depozite de certificate** şi selectaţi **Schimbare parolă** din lista de taskuri. 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.

   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.
5. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi **Depozit de certificate de pe alt sistem** pentru ca să se deschidă 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 taskuri 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 server sau client în depozitul de certificate. Dacă exportaţi certificatul server sau client primul, puteţi întâmpina o eroare deoarece certificatul CA local nu există în de pozitul de certificate.
9. Selectaţi certificatul local CA pentru a exporta şi face clic pe **Exportare**.
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 taskul **Exportare certificat**.
13. Selectaţi **Server sau client** ca tipul de certificat de exportat şi apăsaţi **Continuare**.
14. Selectaţi certificatul server sau client corespunzător de exportat şi apăsaţi **Export**.
15. Selectaţi **Depozit de certificate** ca destinaţie pentru certificatul exportat şi alegeţi **Continuare**.
16. Introduceţi *SYSTEM ca depozit de certificate destinaţie, introduceţi parola pentru acest depozit de certificate şi alegeţi **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informaţii de eroare dacă exportarea a eşuat.
17. Acum puteţi aloca 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 taskuri.
20. Din lista de taskuri, selectaţi **Alocare 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 **Alocare la aplicaţii** pentru a afişa o listă de aplicaţii activate-SSL la care puteţi aloca 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 activate-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 taskuri finalizate, aplicaţii de pe sistemul ţintă pot utiliza certificatul utilizat de CA-ul local pe alt sistem. 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 utilizeze DCM pentru a obţineo copie a certificatului CA local de la sistemul gazdă. Certificatul CA local trebuie copiat la un fişier de pe PC-ul utilizatorului sau descărcat în browser-ul web, depinzând de necesităţile aplicaţiei activate SSL.

Folosirea certificatului privat pentru semnarea obiectelor pe un sistem ţintă

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.

Taskurile pe care trebuie să le realizaţi pentru a utiliza fişierele depozit de certificate transferate pe care le creaţi pe sistemul gazdă local CA variază în funcţie de existenţa depozitului de certificate *OBJECTSIGNING. 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 el.

Depozitul de certificate *OBJECTSIGNING nu există:

Taskurile pe care trebuie să le realizaţi pentru a utiliza fişierele depozit de certificate transferate pe care le creaţi pe sistemul gazdă local CA variază în funcţie de faptul că aţi utilizat vreodată DCM pe sistemul ţintă pentru a gestiona certificate 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. Asguraţi-vă că fişierele depozit de certificate (două fişiere: unul cu extensia .KDB şi unul cu extensia .RDB) pe care le-aţi creat pe sistemul care găszduieşte CA-ul local se află în directorul /QIBM/USERDATA/ICSS/CERT/SIGNING.
2. După ce fişierele certificatelor transferate se află 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. Acestea au fost adăugate de DCM, împreună cu o copie a certificatului CA local, în fişierele depozit de certificat, 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. Schimbarea 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** pentru ca să se deschidă depozitul de certificate.
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 **Gestionare depozite de certificate** şi selectaţi **Schimbare parolă** din lista de taskuri. 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 taskuri.
8. Din lista de taskuri, 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 taskuri **Gestionarea aplicaţiilor**.
11. Din lista de taskuri, selectaţi **Actualizare alocare certificate** pentru a afişa o listă de ID-uri de aplicaţii de semnare obiecte pentru care puteţi aloca 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 faceţi clic pe **Alocare nou certificat**.

Când terminaţi aceste taskuri, 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 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, tre să furnizaţi o copie a crtificatului CA local dacă aţi semnat obiecte 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 depozit de certificate transferate într-un depozit de certificate *OBJECTSIGNING existent pe un sistem 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 a ambelor certificate de semnare obiecte şi certificatul CA local de la fişierele transferate.

Pentru a exporta certificatele din fişierele depozitului de certificate în depozitul de certificate *OBJECTSIGNING, 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 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 **Gestionare depozite de certificate** şi selectaţi **Schimbare parolă** din lista de taskuri. 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** pentru ca să se deschidă 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 taskuri şi selectaţi **Exportul certificatului**.
8. Selectaţi **Autoritate certificare (CA)** ca tipul de certificat de exportat şi apăsaţi **Continuare**.

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

   Notă: Trebuie să exportaţi certificatul local CA în depozitul de certificate înainte să exportaţi certificatul de semnare alobiectului în depozitul de certificate. Dacă exportaţi primul certificatul de semnare al obiectului, puteţi întâmpina o eroare p entru că certificatul local CA 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 taskul **Exportare certificat** task.
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 alocaţi certificatul către o aplicaţie de semnare obiecte.

Gestionarea aplicaţiilor în DCM

DCM vă permite să creaţi definiţii de aplicaţie şi să gestionaţi alocarea certificatelor pentru o aplicaţie. Puteţi de asemenea defini lista de încredere CA pe care o utilizează aplicaţiile ca bază a acceptării certificatelor pentru autentificarea clientului.

Puteţi folosi DCM pentru a realiza diverse taskuri de gestionare pentru aplicaţiile activate pentru SSL şi aplicaţiile de semnare a obiectelor. De exemplu, puteţi gestiona care certificate le vor utiliza aplicaţiile dumneavoastră pentru sesiuni

de comunicaţii SSL. Taskurile de gestiune a aplicaţiilor pe care le puteţi realiza variază în funcţie de tipul de aplicaţie şi de depozitul de certificate în care lucraţi. Puteţi gestiona aplicaţii doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

În timp ce majoritatea taskurilor 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 taskuri, revedeţi subiectele:

Concepte înrudite

“Definiţiile de aplicaţie” la pagina 10
DCM vă permite să gestionaţi definiţii aplicaţiilor care vor lucra cu configuraţii SSL şi semnarea obiectelor.

Creare definiţie aplicaţie

În Digital Certificate Manager (DCM) puteţi crea şi lucra cu aceste două tipuri de definiţii de aplicaţie: aplicaţii server sau client care utilizează SSL şi definiţii de aplicaţie pe care le utilizaţi 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. 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 System i activate pentru SSL sunt înregistrate în DCM, aşa că puteţi să folosiţi cu uşurinţă DCM pentru a le aloca 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 obiectelor 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. Vedeţi Pornirea 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 taskul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. 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**.
4. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de taskuri.
5. Selectaţi **Adăugarea unei aplicaţii** din lista de taskuri 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 autentificarea certificatelor.

Concepte înrudite

“Definiţiile de aplicaţie” la pagina 10
DCM vă permite să gestionaţi definiţii aplicaţiilor care vor lucra cu configuraţii SSL şi semnarea obiectelor.

Informaţii înrudite

QSYRGAP, QsyRegisterAppForCertUse API

Gestionarea alocării certificatului pentru o aplicaţie

Trebuie să folosiţi DCM pentru a atribui un certificat unei aplicaţii înainte ca aceasta să poată efectua o funcţie sigură, cum ar fi stabilirea unei sesiuni SSL (Secure Sockets Layer) 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. Vedeţi Pornirea 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 taskul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. 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**.
4. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de taskuri.
5. Dacă sunteţi în depozitul de certificate *SYSTEM, selectaţi tipul aplicaţiei de gestionat. (Selectaţi aplicaţia corespunzătoare a **Serverului** sau a **Clientului**.)
6. Din lista de taskuri, 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 nespecificat 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 System i Access pentru Windows vor aplica automat orice modificare de certificat. Totuşi, poate sunteţi nevoiţi să opriţi şi să reporniţi serverele Telnet, IBM HTTP Server for i5/OS sau alte aplicaţii înainte de aceste aplicaţii pot aplica modificările certificatelor dumneavoastră.

Operaţii înrudite

“Gestionarea locaţiilor CRL” la pagina 70
Digital Certificate Manager (DCM) vă permite să definiţi şi să administraţi informaţii despre locaţia CRL (Certificate Revocation List) pentru o Autoritate de certificare (CA) particulară pentru a o folosi ca parte din procesul de validare a certificatului.

“Alocarea unui certificat la aplicaţii” la pagina 70
Digital Certificate Manager (DCM) vă permite să alocaţi un certificat uşor şi rapid pentru multiplicat aplicaţii. Puteţi aloca un certificat către mai multe aplicaţii doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

Definire listă de încredere CA pentru o aplicaţie

Aplicaţiile care suportă folosirea certificatelor pentru autentificare client în timpul unei sesiuni SSL (Secure Sockets Layer) 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 nespecificat 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. Vedeţi Pornirea DCM.
2. În cadrul de navigare, faceţi clic pe **Selectare depozit de certificate** şi selectaţi ***SYSTEM** ca depozit de certificate pe care să-l deschideţi.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în taskul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. 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**.
4. În cadrul de navigare, selectaţi **Gestionarea aplicaţiilor** pentru a afişa o listă de taskuri.
5. Din lista de taskuri, 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.

Concepte înrudite

“Certificatele digitale pentru conexiuni VPN” la pagina 38
Puteţi folosi certificate digitale ca un mijloc de a stabili o System i conexiune VPN. Ambele capete ale unei conexiuni dinamice VPN trebuie să poată comunica pentru a se autentifica una alteia înainte de a se activa conexiunea.

Gestionarea certificatelor prin expirare

DCM oferă suport de gestionare a expirării certificatelor, pentru a permite administratorilor să gestioneze certificate server sau client, certificate de semnare obiect, certificare CA şi certificate de utilizator prin data de expirare de pe sistemul local.

Notă: Dacă configuraţi DCM să lucreze cu mapare identitate întreprindere (EIM), puteţi gestiona certificate utilizator pe baza datei de expirare dincolo de 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. Vedeţi Pornirea DCM, dacă DCM nu este deja pornit.
2. În cadrul de navigare, apăsaţi **Selecţie Depozit de certificate** şi selectaţi ***OBJECTSIGNING** sau ***SYSTEM** ca depozitul de certificate de deschis.

   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.
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 taskuri.
5. Din lista de taskuri, selectaţi **Verificare expirare**.
6. Selectaţi tipul certificatului pe care vreţi să-l verificaţi.

   Notă: Pentru a verifica expirarea pentru certificate server sau client trebuie să fiţi în *SYSTEM sau alt sistem de depozitare de certificate. Pentru a verifica expirarea pentru certificate semnare obiecte trebuie să fiţi în depozitul de certificate *OBJECTSIGNING. Certificatele autoritate de certificare pot fi verificate de expirare în toate depozitele de certificate cu excepţia depozitului de certificate local Autoritate de certificare. Puteţi verifica expirarea pentru certificate utilizator în orice depozit de certificate. Trebuie să vizualizaţi singurul certificat CA local pentru a determina aplicaţia sa.
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.

Operaţii înrudite

“Gestionarea certificatelor pe baza expirării” la pagina 47
DCM oferă suport de gestionare a expirării certificatelor, pentru a permite administratorilor să verifice datele de expirare a certificatelor utilizatorilor pe modelul System i local. Suportul de gestionare a expirării certificatelor DCM poate fi utilizat împreună cu EIM astfel încât administratorii să poată utiliza DCM să verifice expirarea certificatelor de utilizator la nivel de întreprindere.

Validarea 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 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 certificatelor

Atunci când validaţi un certificat, DCM verifică un număr de articole aparţinând certificatului pentru a asigura autenticitatea 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.

Concepte înrudite

"Locaţiile listei de revocare a certificatelor" la pagina 6
O listă de revocare a certificatelor (CRL) este un fişier care conţine informaţii despre toate certificatele nevalide şi revocate pentru o Autoritate de certificare (CA) specifică.

"Validarea" la pagina 10
DCM (Digital Certificate Manager) furnizează taskuri care vă permit să validaţi un certificat sau o aplicaţie pentru a verifica diferite proprietăţi pe care fiecare trebuie să le aibă.

Alocarea unui certificat la aplicaţii

Digital Certificate Manager (DCM) vă permite să alocaţi un certificat uşor şi rapid pentru multiplicat aplicaţii. Puteţi aloca un certificat către mai multe aplicaţii doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

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

1. Porniţi DCM. Vedeţi Pornirea DCM.
2. În cadrul de navigare, apăsaţi **Selecţie Depozit de certificate** şi selectaţi ***OBJECTSIGNING** sau ***SYSTEM** ca depozitul de certificate de deschis.

   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.
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 taskuri.
5. Din lista de taskuri, selectaţi **Alocare certificat** pentru a afişa o listă de certificate pentru depozitul de certificate curent.
6. Selectaţi un certificat din listă şi apăsaţi **Alocare 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 alocare fie cu un mesaj de eroare dacă a apărut o problemă.

Operaţii înrudite

"Gestionarea alocării certificatului pentru o aplicaţie" la pagina 67
Trebuie să folosiţi DCM pentru a atribui un certificat unei aplicaţii înainte ca aceasta să poată efectua o funcţie sigură, cum ar fi stabilirea unei sesiuni SSL (Secure Sockets Layer) sau semnarea unui obiect.

Gestionarea locaţiilor CRL

Digital Certificate Manager (DCM) vă permite să definiţi şi să administraţi informaţii despre locaţia CRL (Certificate Revocation List) 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. Vedeţi Pornirea DCM.
2. În cadrul de navigare, selectaţi **Gestionarea locaţiilor CRL** pentru a se afişa o listă de taskuri.

   Notă: Dacă aveţi întrebări despre completarea unui anume formular care este în taskul asistat, selectaţi semnul întrebării (**?**) din partea de sus a paginii pentru a accesa ajutor online.
3. Selectaţi **Adăugare locaţie CRL** din lista de taskuri 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. 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 taskurilor.
6. Selectaţi **Actualizare alocare locaţie CRL** din lista de taskuri pentru a afişa o listă de certificate CA.
7. Selectaţi din listă certificatul CA cu care vreţi să alocaţi definiţia locaţiei CRL pe care aţi creat-o şi faceţi clic pe **Actualizare Alocare 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 Alocare**. Va fi afişat un mesaj la începutul paginii indicate pentru a indica faptul că locaţia CRL a fost alocată cu certificatul Autorităţii de Certificare (CA).

Notă: Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiţi unealta Administrarea server Web Directory Server şi să selectaţi taskul ″Gestionare schemă″ pentru a schimba clasa de securitate (de asemenea numită şi ″clasă de acces″) a atributelor certificateRevocationList şi authorityRevocationList din ″critical″ şi ″normal″ şi lăsaţi goale câmpurile **Nume distinctiv logare** şi **Parolă**.

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 de director (LDAP) şi aplicaţii client pentru a utiliza SSL, şi a aloca un certi ficat la aplicaţiile din DCM.

Concepte înrudite

“Locaţiile listei de revocare a certificatelor” la pagina 6
O listă de revocare a certificatelor (CRL) este un fişier care conţine informaţii despre toate certificatele nevalide şi revocate pentru o Autoritate de certificare (CA) specifică.

Operaţii înrudite

"Gestionarea alocării certificatului pentru o aplicaţie" la pagina 67
Trebuie să folosiţi DCM pentru a atribui un certificat unei aplicaţii înainte ca aceasta să poată efectua o funcţie sigură, cum ar fi stabilirea unei sesiuni SSL (Secure Sockets Layer) sau semnarea unui obiect.

Informaţii înrudite

Server director IBM pentru iSeries (LDAP)

Activare SSL pe Directory Server

Stocarea cheilor de certificat pe IBM Cryptographic Coprocessor

Dacă aţi instalat un coprocesor criptografic IBM pe sistemul dumneavoastră, puteţi utiliza coprocesorul să furnizeze spaţiu de stocare mai sigur pentru cheia privată a unui certificat. Puteţi folosi coprocesorul pentru a stoca cheia privată pentru un certificat server, unul client sau pentru un certificat CA local.

Nu puteţi utiliza coprocesorul pentru memorarea cheii private 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 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 cripta 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.

Concepte înrudite

"IBM Cryptographic Coprocessors for System i" la pagina 9
Coprocesorul criptografic furnizează servicii criptografice dovedite, asigurând protecţie şi integritate, pentru a dezvolta aplicaţii e-business sigure.

Informaţii înrudite

Privire generală criptografie

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 IBM Cryptographic Coprocessor pentru a cripta cheia privată şi a o memora într-un fişier de chei special. Puteţi selecta această opţiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat în DCM.

Înainte de a putea utiliza această opţiune cu succes, trebuie să utilizaţi interfaţa web de configurare acoprocesorului criptografic IBM penru a crea un fişier depozit de chei 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 Taskuri System i.

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 SSL (Secure Sockets Layer), 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 taskul pe care îl completaţi, cum ar fi informaţii de identificare pentru certificatul pe care îl creaţi sau reînnoiţi.
5. Din lista de dispozitive, selectaţi numele unei sau a mai multor descrieri dispozitiv cu care doriţi să partajaţi cheia privată a certificatului.

   Notă: Descrierile dispozitiv pe care le selectaţi trebuie să aibă aceeaşi cheie master ca şi dispozitivul selectat în pagina precedentă. Pentru a verifica dacă cheia master este aceeaşi pe dispozitive, folosiţi taskul de verificare a cheii master din interfaţa de configurare Web a coprocesorului criptografic 4758. Puteţi accesa interfaţa web de configurare a coprocesorului criptografic din consola web IBM Systems Director Navigator for i5/OS.
6. Selectaţi **Continuare**. DCM va continua să afişeze pagini pentru taskul pe care îl efectuaţi, cum ar fi informaţii de identificare pentru certificatul pe care îl creaţi sau reînnoiţi.

Informaţii înrudite

Privire generală criptografie

Lucrul cu Navigator director de sisteme IBM pentru i5/OS

Gestionarea locaţiei cererii pentru un PKIX CA

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.

Un CA PKIX cere o identificare mai bună înainte de a emite un certificat; în general el cere ca un solicitant 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 o PKIX CA pentru uzul public.

Dacă aţi ales ca CA PKIX să emită certificate care să fie folosite de aplicaţii, puteţi folosi DCM (Digital Certificate Manager) pentru a gestiona aceste certificate. Folosiţi DCM pentru a configura un URL pentru 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. Vedeţi Pornirea 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 adaugă PKIX CA ca o opţiune pentru specificarea tipului de CA pe care o alegeţi pentru emiterea unui certificat când folosiţi taskul **Creare Certificat**.

Notă: Standardele PKIX sunt subliniate în RFC (cereri pentru comentarii) 2560.

Concepte înrudite

"Gestionarea certificatelor de la un CA public din Internet" la pagina 50
Când utilizaţi DCM la gestionarea certificatelor de la un CA public din Internet, trebuie mai întâi să creaţi un depozit de certificate. Un depozit de certificate este un fişier special de bază de date de chei, pe care îl foloseşte DCM (Digital Certificate Manager) pentru a stoca certificate digitale şi cheile lor private asociate.

Gestionarea locaţiei LDAP pentru certificate utilizator

Puteţi folosi Digital Certificate Manager (DCM) pentru stocarea certificatelor de utilizator într-o locaţie de director a serverului LDAP, extinzând Enterprise Identity Mapping pentru a lucra cu certificate de utilizator.

Implicit, DCM memorează certificatele de utilizator pe care le emite autoritatea de certificare (CA) locală cu profilurile de utilizator i5/OS. Însă puteţi configura DCM împreună cu EIM astfel încât atunci când Autoritatea de certificare (CA) locală emite certificate utilizator, copia publică a certificatului să fie memorată într-o locaţie de director a serverului LDAP. O configuraţie combinată de EIM cu DCM vă permite să stocaţi certificatele de utilizator într-o locaţie de director LDAP, pentru a face certificatele 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 taskul **Alocare certificat utilizator** .

EIM este o tehnologieServer care vă permite să gestionaţi identităţiile de utilizator în întreprinderea dumneavoastră, inclusiv profilurile de utilizator şi certificate utilizator i5/OS. Dacă vreţi să folosiţi EIM pentru a gestiona certificate utilizato, este nevoie să realizaţi aceste taskuri de configurare EIM înainte de a realiza orice taskuri de configurare:

1. Folosiţi vrăjitorul **Configurare EIM** din Navigator System i pentru a configura EIM.
2. Creaţi registrul X.509 în domeniul EIM pentru a fi folosit în asocierea certificatelor
3. Selectaţi meniul de proprietăţi pentru configuraţia folder în domeniul EIM şi introduceţi numele de registru X.509.
4. Creaţi un identificator EIM pentru fiecare utilizator care vreţi să participe la EIM.
5. Creaţi o asociere destinaţie între fiecare identificator EIM şi profilul de utilizator al acelui utilizator în registrul de utilizator al acelui utilizator în registrul de utilizator locali5/OS. Folosiţi numele de definiţie din registrul EIM pentru registrul de utilizatori i5/OS local pe care l-aţi specificat în vrăjitorul **Configurare EIM**.

După ce realizaţi taskurile de configurare EIM necesare, trebuie să efectuaţi următoarele taskuri pentru a termina configurarea generală pentru folosirea EIM şi DCM împreună:

1. În DCM, utilizaţi taskul **Gestionare locaţie LDAP** pentru a specifica directorul LDAP pe care DCM îl va folosi să memoreze un certificat utilizator pe care CA-ul local îl creează. Locaţia LDAP nu necesită să fie pe modelulSystem i local, nici nu necesită să fie acelaşi server LDAP pe care EIM îl utilizează. Când configuraţi locaţia LDAP în DCM, DCM utilizează directorul specificat LDAP pentru a memora toate certificatele de utilizator pe care CA-ul local le emite. DCM utilizează de asemenea locaţie LDAP pentru a memora certificate utilizator procesate de taskul **Alocare certificat utilizator**în loc să memoreze certificatul cu un profil utilizator.
2. Rulează **Converiret certificate utilizator** comanda (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 creează 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.

Notă: Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiţi unealta Administrarea server Web Directory Server şi să selectaţi taskul Gestionare schemă pentru a schimba clasa de securitate (de asemenea numită şi ″clasă de acces″) a atributelor certificateRevocationList şi authorityRevocationList din ″critical″ şi ″normal″ şi lăsaţi goale câmpurile **Nume distinctiv logare** şi **Parolă**.

Operaţii înrudite

“Certificatele digitale şi EIM” la pagina 37
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.

Informaţii înrudite

Convertire comandă certificat utilizator (CVTUSRCERT)

Enterprise Identity Mapping (EIM)

Semnarea obiectelor

Sunt trei tipuri diferite de metode pe care le puteţi utiliza pentru semnarea obiectelor. Pentru a semna un obiect puteţi scrie un program care apelează Semnare obiect API, utilizaţi DCM sau utiliza caracteristica Navigator System i Administrare centrală pentru pachetele pe care le distribuiţi la alte sisteme.

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

Puteţi semna obiecte cu certificate pe care l e cumpăraţi de la o autoritate de certificare publică internet (CA) sau să 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 aveţi creat depozitul *OBJECTSIGNING , fie ca parte a proesului de creare a CA-ului local sau ca parte a procesului de gestionare certificate semnare obiecte de la un CA public internet.
- Depozitul de certificate *OBJECTSIGNING trebuie să conţină cel puţin un certificat, fie unul pe care l-aţi creat utilizând CA-ul local sau unul pe care l-aţi obţinut de la un CA public internet.
- Pentru semnarea obiectelor, trebuie să fi creat o definiţie de aplicaţie pentru semnarea obiectelor.
- Trebuie să fi alocat 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. Vedeţi Pornirea DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***OBJECTSIGNING** pentru ca să se deschidă depozitul de certificate.

   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.
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 taskuri.
5. Din lista de taskuri, 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 taskul **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 cu conţinutul 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.

Operaţii înrudite

“Crearea şi operarea unui CA local” la pagina 42
Puteţi utiliza DCM pentru a crea şi opera propriul dumneavoastră CA local, pentru a emite certificate private pentru aplicaţiile dumneavoastră.

“Gestionarea certificatelor publice din Internet pentru semnarea obiectelor” la pagina 52
Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona certificate Internet publice pentru a semna digital obiectele.

Informaţii înrudite

API-ul de semnare obiecte

Scenariu: Folosirea Administrare centrală din Navigator System i pentru a semna obiecte

Scenariu: Folosirea DCM pentru a semna obiecte şi a verifica semnăturile

Verificarea semnăturii 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:

- Trebuia să fi creat depozitul de certificate *SIGNATUREVERIFICATION pentru a gestionacertificatele de verificare a semnăturii.

  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 aceeaşi 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. Vedeţi Pornirea DCM.
2. În cadrul de navigare, alegeţi **Selectare depozit de certificate** şi selectaţi ***SIGNATUREVERIFICATION** pentru ca să se deschidă depozitul de certificate.

   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.
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 taskuri.
5. Din lista de taskuri, 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 cu conţinutul 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 verificare 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.

Concepte înrudite

"Certificatele digitale pentru semnarea obiectelor" la pagina 39
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.

Operaţii înrudite

"Gestionarea certificatelor publice din Internet pentru semnarea obiectelor" la pagina 52
Puteţi folosi Digital Certificate Manager (DCM) pentru a gestiona certificate Internet publice pentru a semna digital obiectele.

"Gestionarea certificatelor pentru verificarea semnăturii obiectelor" la pagina 54
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.

Depanarea DCM

Utilizaţi următoarele metode de depanare pentru a soluţiona unele dintre problemele de bază pe care le-aţi putea expe rimenta în timp ce configuraţi şi utilizaţi DCM.

Când lucraţi cu DCM şi certificate, aţi putea întâlni erori care vă împiedică de la realizarea taskurilor şi ţelurilor dumneavoastră. Multe din erorile şi problemele comune pe care le-aţi putea întâlni cad într-un număr de categorii, cum ar fi următoarele:

Depanarea problemelor generale şi de parole

Utilizaţi următoarea tabelă pentru a vă ajuta să depanaţi unele dintre cele mai comune probleme legate de parolă şi alte probleme generale pe care le puteţi întâlni cât timp lucraţi cu DCM.

Problemă	Soluţie posibilă
Nu puteţi găsi ajutor suplimentar pentru DCM.	În DCM, selectaţi ″**?**″ . Puteţi căuta de asemenea Centrul de informare i5/OS şi extern IBM site-uri web de pe internet.
Parola dumneavoastră pentru autoritatea de certificare locală (CA) 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.
Aţi primit un mesaj de eroare că parola dumneavoastră a expirat când aţi încercat să deschideţi depozitul de certificate.	Trebuie să modificaţi parola pentru depozitul de certificate transferat. Faceţi clic pe butonul **OK** pentru a schimba parola.
Încercarea dumneavoastră de resetare a parolei când aţi folosit taskul **Selectare depozit de certificate** a eşuat.	Funcţia reset funcţionează doar dacă DCM a memorat 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 **Logare automată**, astfel încât DCM să continue să stocheze parola.

Problemă	Soluţie posibilă
	De asemenea, dacă mutaţi un depozit de certificate de la un sistem la altul, trebuie să schimbaţi parola pentru depozitul de certificate pe noul sistem pentru a vă asigura că DCM o memorează automat. Pentru a schimba parola, trebuie să furnizaţi parola originală pentru depozitul de certificate când îl deschideţi pe noul sistem. Nu puteţi folosi opţiunea de resetare parolă 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 **Logare automată** când modificaţi parola pentru a vă asigura că DCM memorează noua parolă pentru acest tip de depozit de certificate.
	Verificaţi valoarea alocată 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 de unelte de service 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 financiare 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 taskul **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 alocarea certificatului nu este afişată când informaţiile despre aplicaţia sigură este afişată imediat după alocarea unui certificat. Această problemă apare mai des când este folosit Navigator System i 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 sistem. 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 problemelor de depozit de certificate şi bază de date de chei

Utilizaţi următoarea tabelă pentru a vă ajuta la depanarea unora dintre cele mai comune probleme ale depozitului de certificate şi bază de date de chei pe care le puteţi întâlni în timp ce lucraţi, cu 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

Creare bază de date de chei eşuată sau Creare un CA locală 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 creează, 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. Trebuie să creaţi un nou CA local 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 program cu licenţă (LPP) pe care DCM îl cere instalat. Verificaţi lista de “Cerinţe de setare DCM” la pagina 31 şi asiguraţi-vă că toate programele cu licenţă sunt instalate corespunzător.

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 certificatele nevalide 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 schimbare 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 nevalide (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. Pentru informaţii suplimentare revedeţi Centrul de informare i5/OS subiectul Api QsyAddVldlCertificate. Consultaţi server IBM HTTP pentru documentaţie i5/OS pentru ajut or la configurarea unei instanţe server HTTP sigure pentru a folosi lista de validare.

Depanarea problemelor de browser

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 lăsaţi 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’ (eroare) 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 Decembrie 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. Descărcarea gratuită a browser-ului este disponibilă la http://www.netcenter.com.

Depanarea problemelor HTTP Server for i5/OS

Utilizaţi următoarea tabelă pentru a vă ajuta să depanaţi problemele serverului HTTP pe care le puteţi întâmpina cât timp lucraţi cu DCM.

Problemă	Soluţie posibilă
HTTPS (Hypertext Transfer Protocol Secure) 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** setat la **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 aloca 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 IBM server HTTP pentru i5/OS documentaţiepentru opţiuni despre setarea 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 localiza informaţii despre aceste API-uri cu Detector API subiect înCentrul de informare i5/OS. Aţi putea de asemenea să vreţi să vă uitaţi la aceste API-uri legate de liste de validare sau 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 au expirat sau sunt de la 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 aloca 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 aloca un certificat diferit aplicaţiei QIBM_HTTP_SERVER_ADMIN şi încercaţi să setaţi **SSL** pe **Activat** din nou.

Depanarea alocării unui certificat de utilizator

Utilizaţi următorii paşi pentru a vă ajuta să depanaţi orice probleme pe care le puteţi întâmpina în timp ce încercaţi să alocaţi un certificat utilizator cu DCM.

Când folosiţi taskul **Alocarea 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 cache a 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 aloca un certificat. Contactaţi 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-ul 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 taskul **Setare stare CA** pentru a activa CA drept de încredere pentru a corecta problema.
5. Nu există un certificat pentru înregistrare. Puteţi să verificaţi 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 for i5/OS nu este configurat corect pentru înregistrarea certificatelor folosind SSL şi autentificarea clientului pe instanţa securizată Admin a serverului. Dacă nu funcţionează nici unul dintre sfaturile de depanare propuse, contactaţi administratorul de sistem pentru a-i raporta problema.

Pentru **Atribuirea unui certificat utilizator**, trebuie să vă conectaţi la un DCM, folosind o sesiune SSL. Dacă nu folosiţi SSL când selectaţi taskul **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. Serverul Web ar trebui să fie repornit pentru a se confirma dacă directivele de configurare pentru folosirea SSL sunt activate.

Operaţii înrudite

"Alocarea unui certificat de utilizator" la pagina 46
Puteţi să alocaţi un certificat pe care îl deţineţi la profilul utilizator i5/OS sau la altă identitate de utilizator. Certificatul poate fi de la un CA local privat pe alt sistem sau de la un bine cunoscut internet CA. Pentru a aloca 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.

Informaţii înrudite pentru DCM

Siturile IBM şi publicaţiile Redbooks conţin informaţii care au legătură cu colecţia de subiecte Digital Certificate Manager (DCM). Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

IBM Redbooks

- IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements
- AS/400 Internet Security: Developing a Digital Certificate Infrastructure

Situri web

- **Situl Web VeriSign Help Desk** Acest sit Web oferă o bibliotecă extinsă de subiecte referitoare la certificatele digitale, precum şi alte câteva subiecte privind securitatea în Internet.
- **RFC Index Search** Aceste sit Web oferă o magazie pentru căutarea RFC-urilor. 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. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau 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. Prin furnizarea acestui document nu vi se acordă nicio licenţă pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

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

Pentru întrebări privind licenţa pentru informaţiile DBCS (pe doi octeţi), contactaţi departamentul IBM de proprietate intelectuală din ţara dumneavoastră sau trimiteţi întrebările în scris la:

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

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

Aceste informaţii pot conţine greşeli tehnice sau erori de tipar. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) descris în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe 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 pentru dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să obţină 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, trebuie să contacteze:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu respectarea termenilor şi condiţiilor corespunzătoare, iar în unele cazuri cu plata unei taxe.

Programul licenţiat la care se referă acest document şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM în conformitate cu termenii din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau din alt acord echivalent încheiat între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Este posibil ca unele măsurători să fi fost realizate pe sisteme de nivel evoluat şi nu există nici o garanţie că aceste măsurători vor fi identice pe sisteme general disponibile. Mai mult, unele măsurători pot fi estimări obţinute prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

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

Toate preţurile IBM prezentate sunt preţurile cu amănuntul sugerate de IBM, sunt actuale şi pot fi modificate fără notificare. Preţurile dealer-ului pot fi diferite.

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

LICENŢĂ COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără ca IBM să pretindă vreo plată, când o faceţi în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform cu interfaţa de programare a aplicaţiilor pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate amănunţit în toate condiţiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

Fiecare copie sau porţiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Unele porţiuni din acest cod sunt derivate din programele exemplu oferite de IBM Corp. © Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vizualizaţi aceste informaţii în format electronic, este posibil să nu apară fotografiile şi ilustraţiile color.

Informaţii despre interfaţa de programare

Această publicaţie, Digital Certificate Manager, conţine informaţii despre interfeţele de programare menite să permită beneficiarului să scrie programe pentru a obţine serviciile IBM i5/OS.

Mărci comerciale

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

AIX
AS/400

| Domino
| eServer
| i5/OS
| IBM
| iSeries
| Lotus
| Net.Data
| OS/400
| Redbooks
| System i

| Adobe, logo-ul Adobe, PostScript şi logo-ul PostScript sunt mărci comerciale înregistrate sau mărci comerciale
| deţinute de Adobe Systems Incorporated în Statele Unite şi/sau alte ţări.

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

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

Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru Publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţinută în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.