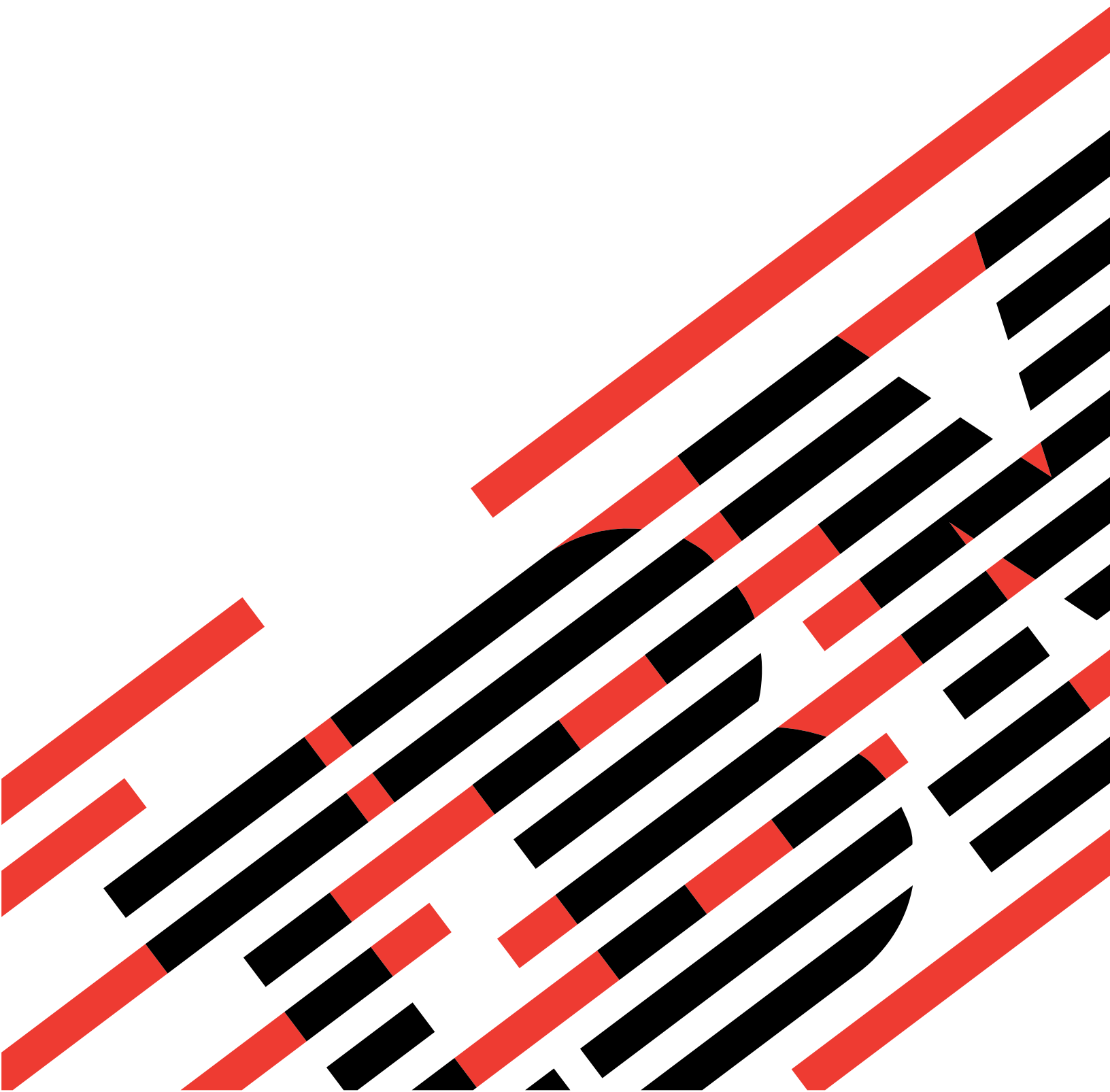




IBM Systems - iSeries
Digital Certificate Manager

Versiunea 5 Ediția 4





IBM Systems - iSeries
Digital Certificate Manager

Versiunea 5 Ediția 4

Notă

Înainte de a folosi aceste informații și produsul pe care îl suportă, asigurați-vă că ați citit informațiile din “Observații”, la pagina 81.

Ediția a cincea (Februarie 2006)

Această ediție se aplică versiunilor 5, ediția 4, modificarea 0 IBM i5/OS (număr produs 5722-SS1) și tuturor următoarelor modificări și ediții până la edițiile următoare indicate. Această versiune nu rulează pe toate modelele de calculatoare RISC și nici pe modelele CISC.

© Copyright International Business Machines Corporation 1999, 2006. Toate drepturile rezervate.

Cuprins

DCM - Manager certificate digitale. . . . 1

Ce este nou pentru V5R4	1
PDF tipăribil	2
Conceptele DCM	2
Extensii certificat	3
Reînnoire certificat	3
Nume distinctiv	3
Semnături digitale	4
Perechea de chei publice-private	5
CA (autoritate de certificare)	5
Locații CRL (listă de revocare certificate)	6
Depozite de certificate	7
Criptografie	8
IBM Cryptographic Coprocessors for iSeries	9
SSL (Secure Sockets Layer)	9
Definiții aplicație	10
Validarea	10
Scenarii DCM	11
Scenariu: Folosirea certificatelor pentru autentificări externe	12
Scenariu: Folosirea certificatelor pentru autentificări interne	18
Plan pentru DCM	26
Cerințe de setare DCM	26
Considerentele despre salvarea de rezervă și recuperarea datelor DCM.	27
Tipuri de certificate digitale	28
Certificate publice contra certificate private	29
Certificatele digitale pentru comunicațiile sigure SSL	31
Certificatele digitale pentru autentificarea utilizatorului	31
Certificate digitale și EIM (Enterprise Identity Mapping)	33
Certificatele digitale pentru conexiuni VPN	34
Certificatele digitale pentru semnarea obiectelor	35

Certificate digitale pentru verificarea semnăturii obiectelor	36
Configurarea DCM	37
Pornirea Digital Certificate Manager	37
Setarea certificatelor pentru prima dată	38
Reînnoirea unui certificat existent	52
Importarea unui certificat.	53
Gestionarea DCM	54
Utilizarea CA local pentru a emite certificate pentru alte sisteme iSeries	54
Gestionarea aplicațiilor în DCM.	62
Gestionarea certificatelor prin expirare.	64
Validarea certificatelor și aplicațiilor	65
Alocarea unui certificat la aplicații	66
Gestionarea locațiilor CRL	66
Memorarea cheilor certificatului pe un IBM Cryptographic Coprocessor	67
Gestionarea locației cerute pentru un PKIX CA	69
Gestionarea locației LDAP pentru certificatele utilizator	70
Semnarea obiectelor	71
Verificarea semnăturii obiecte	72
Depanarea DCM	74
Depanarea parolelor și problemelor generale	74
Depanarea problemelor cu depozitul de certificate și cu bazele de date de chei.	75
Depanarea problemelor browser-ului	77
Depanarea problemelor serverului iSeries	78
Depanarea alocării unui certificat utilizator	79
Informații înrudite pentru DCM.	80

Anexa. Observații 81

Mărci comerciale	82
Termenii și condițiile	83

DCM - Manager certificate digitale

Un certificat digital este o acreditare electronică pe care o puteți folosi pentru a vă demonstra identitatea pentru o tranzacție electronică. Există un număr din ce în ce mai mare de modalități de folosire a certificatelor digitale pentru a se asigura măsuri de securitate crescând în rețea. De exemplu, certificatele digitale sunt esențiale pentru configurarea și folosirea SSL (Secure Sockets Layer). Utilizarea SSL vă permite să creați conexiuni sigure între utilizatori și aplicații server peste o rețea ce nu este de încredere, cum ar fi Internet. SSL oferă una dintre cele mai bune soluții pentru protecția în Internet a caracterului privat al datelor sensibile, cum ar fi numele de utilizator și parolele. Multe iSeries servicii și aplicații, cum ar fi FTP, Telnet, HTTP Server pentru iSeries și multe altele, oferă suport SSL pentru a asigura protecția datelor.

iSeries IBM asigură un suport extins pentru certificatele digitale, care vă permite să folosiți certificate digitale drept acreditări în mai multe aplicații de securitate. În plus față de folosirea certificatelor pentru configurarea SSL, le puteți folosi și drept credite în autentificarea clienților pentru tranzacții SSL și VPN (rețele private virtuale). De asemenea, puteți folosi certificatele digitale și cheile de securitate asociate lor pentru a semna obiecte. Semnarea obiectelor vă permite să detectați modificările sau posibilele deteriorări ale conținutului obiectelor prin verificarea semnăturilor asupra obiectelor pentru a le asigura integritatea.

DCM (Digital Certificate Manager), o caracteristică gratuită, vă simplifică folosirea suportului iSeries pentru certificate, permițându-vă să gestionați centralizat certificatele pentru aplicațiile dumneavoastră. DCM vă permite să gestionați certificatele pe care le obțineți de la orice CA (autoritate de certificare). De asemenea, puteți folosi DCM pentru a crea și lucra cu propriul dumneavoastră CA local pentru a emite certificate private către aplicațiile și utilizatorii din organizația dumneavoastră.

Cheile folosirii efective a certificatelor pentru beneficiile lor în ceea ce privește securitatea sunt planificarea și evaluarea corectă. Ați putea să revedeți aceste subiecte pentru a învăța mai multe despre modul în care funcționează certificatele și cum puteți folosi DCM pentru a gestiona certificatele și aplicațiile care le folosesc:

Ce este nou pentru V5R4

Această informație descrie ce informație este nouă și schimbată în mod semnificativ în această ediție.

Noi informații pentru reînnoirea certificatelor

Aceste noi informații explică pas cu pas procesul de reînnoire a certificatelor existente cu CA local sau CA Internet

- “Reînnoirea unui certificat existent” la pagina 52

Noi informații pentru reînnoirea certificatelor

Aceste noi informații vă explică pas cu pas procesul de importare ale certificatelor în fișierele de pe serverul dumneavoastră sau de pe alt server

- “Importarea unui certificat” la pagina 53



Îmbunătățiri ale informațiilor despre CRL (Certificate Revocation List) și LDAP (Lightweight Directory Access Protocol)

Aceste informații au fost actualizate pentru a include informații despre cum să vă legați anonim la un server LDAP pentru procesare CRL.

- “Gestionarea locațiilor CRL” la pagina 66
- “Gestionarea locației LDAP pentru certificatele utilizator” la pagina 70
- “Locații CRL (listă de revocare certificate)” la pagina 6

Cum puteți vedea ce este nou sau modificat


Pentru a vă ajuta să vedeți unde au fost făcute modificări tehnice, aceste informații folosesc:

- Imaginea  de marcat unde încep informațiile noi sau modificate.
- Imaginea  de marcat unde se termină informațiile noi sau modificate.

Pentru a găsi alte informații despre ce este nou sau modificat în această ediție, vedeți Memo către utilizatori.

PDF tipăribil

Folosiți această pagină pentru a afla cum să tipăriți întregul subiect ca un fișier PDF.


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

Salvarea fișierelor PDF

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

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

Descărcarea programului Adobe Acrobat Reader

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

Conceptele DCM

Folosiți aceste informații pentru a înțelege mai bine ce sunt certificatele digitale și cum lucrează ele. Aflați despre diferitele tipuri de certificate și cum le puteți folosi ca parte a politicii de securitate a dumneavoastră.

Înainte să începeți să folosiți certificate digitale pentru a îmbunătăți sistemul dumneavoastră și politica de securitate a rețelei, trebuie să înțelegeți ce sunt ele și ce avantaje de securitate oferă.

Un certificat digital este un credential digital care validează identitatea proprietarului certificatului, cum o face un pașaport. Informațiile 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 organizații. Încrederea în CA stă la baza încrederii în certificat ca o scrisoare de acreditare validă.

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

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

Extensii certificat

Extensiile certificatelor sunt câmpuri de informații care furnizează informații suplimentare despre certificat.

Extensiile certificatelor furnizează un mijloc de expandare a standardelor de informații certificat X.509. În timp ce informațiile pentru unele extensii sunt furnizate pentru a extinde informațiile de identificare pentru certificat, alte extensii furnizează informații despre capabilitățile criptografice ale certificatului.

Nu toate certificatele folosesc câmpurile extensie pentru a extinde numele distinctiv și alte informații. Numărul și tipul câmpurilor extensie pe care le folosește un certificat variază între entitățile CA (Certificate Authority) care emit certificate.

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

Concepte înrudite

“Nume distinctiv”

Folosiți aceste informații pentru a învăța despre caracteristicile de identificare ale certificatelor digitale.

Reînnoire certificat

Procesul de reînnoire a certificatelor pe care îl folosește DCM (Digital Certificate Manager) variază în funcție de tipul CA-ului care a emis certificatul.

Dacă folosiți CA-ul local pentru a semna certificatul reînnoit, DCM folosește informațiile pe care le furnizați pentru a crea un nou certificat în depozitul curent de certificate și reține certificatul anterior.

Dacă utilizați un CA din Internet binecunoscut pentru a emite certificatul, puteți trata reînnoirea certificatului în unul din cele două moduri: să importați certificatul reînnoit dintr-un fișier pe care îl primiți de la CA de semnare sau să puneți DCM-ul să creeze o nouă pereche de chei publică-privată pentru certificat. DCM furnizează prima opțiune în caz că preferați să reînnoiți certificatul direct cu CA-ul care l-a emis.

Dacă alegeți să creați o nouă pereche de chei, DCM tratează reînnoirea în același mod în care a tratat crearea certificatului. DCM creează o nouă pereche de chei publică-privată pentru certificatul reînnoit și generează un CSR (Certificate Signing Request) care este construit din cheia publică și alte informații pe care le specificați pentru noul certificat. Puteți folosi CSR-ul pentru a cere un nou certificat de la VeriSign sau orice altă CA publică. O dată ce primiți certificatul semnat de la CA, folosiți DCM pentru a-l importa în depozitul corespunzător de certificate. Depozitul de certificate apoi conține ambele copii ale certificatului, originalul și certificatul reînnoit emis recent.

Dacă alegeți 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 fișier existent pe care l-ați primit de la CA. Certificatul importat, reînnoit înlocuiește apoi certificatul anterior.

Nume distinctiv

Folosiți aceste informații pentru a învăța despre caracteristicile de identificare ale certificatelor digitale.

Fiecare CA are o politică pentru a hotărî informațiile de identificare pe care le solicita CA pentru a emite un certificat. Anumite Autorități de certificare Internet pot cere puține informații, cum ar fi un nume și o adresă de mail. Alte CA-uri publice pot cere mai multe informații și să necesite o dovadă mai strictă decât informațiile de identificare înainte de a emite un certificat. De exemplu, CA-urile care suportă standardele PKIX (schimb de infrastructură a cheilor), pot cere ca cel care cere să își verifice identitatea printr-un RA (autoritate de înregistrare) înainte de a emite certificatul. În consecință, dacă plănuți să acceptați și să utilizați certificatele drept acreditări, trebuie să revedeți cererile de identificare pentru un CA pentru a determina dacă cererile lor se potrivesc nevoilor dumneavoastră de securitate.

Nume distinctiv (DN) este un termen care descrie informațiile de identificare dintr-un certificat și este parte a certificatului în sine. Un certificat conține informații DN atât pentru proprietar sau solicitant al certificatului (numit DN-ul subiect) cât și pentru CA care emite certificatul (numit DN emitent). În funcție de politica de identificare a CA care emite certificatul, DN-ul (numele distinct) poate include o varietate de informații. Puteți folosi DCM (Digital Certificate Manager) pentru a opera o Autoritate de certificare privată și pentru a emite certificate private. De asemenea, puteți folosi DCM pentru a genera informațiile DN și perechea de chei pentru certificatul pe care un CA public din Internet îl emite pentru organizația dumneavoastră. Informațiile DN pe care le puteți furniza pentru unul dintre tipurile de certificate includ:

- Numele comun al deținătorului certificatului.
- Organizația
- Unitatea organizațională
- Localitate sau oraș
- Stat sau provincie
- Țară sau regiune

Când folosiți DCM pentru a emite certificate private, puteți utiliza extensii pentru certificat pentru a furniza informații suplimentare despre DN pentru certificat, inclusiv:

- Adresă de IP versiunea 4
- Numele complet calificat al domeniului
- Adresa de e-mail

Concepte înrudite

“Extensii certificat” la pagina 3

Extensiile certificatelor sunt câmpuri de informații care furnizează informații suplimentare despre certificat.

Semnături digitale

O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme criptografie și este echivalent cu o semnătură personală pe un document scris.

O semnătură digitală furnizează dovada originii obiectului și 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 folosește cheia publică corespunzătoare a certificatului pentru a decripta semnătura, care verifică integritatea obiectului semnat ca și emitentul ca sursă.

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

O semnătură digitală este o semnătură electronică pe care dumneavoastră sau o aplicație o creați pe un obiect prin folosirea unei chei private a unui certificat digital. Semnătura digitală pe un obiect furnizează o legare electronică unică a identității semnatarului (proprietarul cheii de semnare) cu originea obiectului. Când accesați un obiect care conține o semnătură digitală, puteți verifica semnătura de pe obiect pentru a verifica sursa obiectului ca validă (de exemplu, că o aplicație pe care o descărcați chiar vine de la o sursă autorizată cum este IBM). Acest proces de verificare vă permite de asemenea să determinați dacă au fost făcute modificări neautorizate asupra obiectului de când a fost semnat.

Un exemplu de cum funcționează o semnătură digitală

Un dezvoltator software a creat o aplicație i5/OS pe care vrea să o distribuie prin Internet, ca o măsură comodă și ieftină pentru clienții săi. Totuși, el știe că respectivii clienți sunt, pe bună dreptate, îngrijorați de descărcarea programului din Internet, datorită crescândelor probleme privind obiectele care se dau drept programe legitime, dar de fapt conțin programe distructive, cum sunt virușii.

În consecință, el decide să semneze digital aplicația astfel încât clienții săi să poată face verificarea că compania lui este sursa legitimă a aplicației. El folosește cheia privată de la un certificat digital pe care l-a obținut de la un CA public

binecunoscut pentru a semna aplicația. Apoi îl face disponibil de descărcat pentru clienții 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 aplicația, clientul poate folosi cheia publică a certificatului pentru a verifica semnătura de pe aplicație. Acest proces permite clientului să identifice și să verifice sursa aplicației, cât și să se asigure că conținutul obiectului aplicație nu a fost alterat de când a fost semnat.

Concepte înrudite

“CA (autoritate de certificare)”

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

“Criptografie” la pagina 8

Citiți aceste informații pentru a afla ce este criptografia și cum folosesc certificatele digitale funcțiile criptografice pentru a oferi 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 excepție de la această regulă și au asociată doar o cheie publică.

O cheie publică este o parte a certificatului digital al proprietarului și este disponibilă pentru ca oricine să o folosească. Totuși, o cheie privată este protejată și este doar la îndemâna proprietarului acesteia. Acest acces limitat asigură siguranța 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” și cripta datele trimise între utilizatori și servere, cum sunt mesajele, documentele și obiectele codate. Receptorul obiectului semnat poate apoi să folosească cheia publică conținută în certificatul semnatarului pentru a decripta semnătura. Asemenea semnături digitale asigură încrederea originii unui obiect și furnizează un mijloc de verificare a integrității obiectului.

Concepte înrudite

“Semnături digitale” la pagina 4

O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme criptografie și este echivalent cu o semnătură personală pe un document scris.

“CA (autoritate de certificare)”

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

CA (autoritate de certificare)

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

Încrederea în CA stă la baza încrederii în certificat ca o scrisoare de acreditare validă. O CA folosește 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 alții pentru a se verifica autenticitatea certificatelor pe care le emite și semnează CA.

O CA poate fi o entitate comercială publică, așa cum este VeriSign, sau poate fi o entitate privată pe care operează o organizație în scopuri interne. Anumite firme furnizează servicii de Certificate Authority pentru utilizatorii Internet. Digital Certificate Manager (DCM) vă permite să gestionați certificate atât de la CA-uri publice cât și de la cele private.

De asemenea, puteți folosi DCM pentru a opera propriul dumneavoastră CA local pentru a emite certificate private către sisteme și utilizatori. Când CA-ul local emite un certificat de utilizator, DCM îl asociază automat certificatul cu

iSeries profilul de utilizator de pe sistemul utilizatorului sau altă identitate de utilizator. Dacă DCM asociază certificatul cu un profil utilizator sau cu o identitate diferită pentru utilizator depinde dacă configurați DCM să lucreze cu EIM (Enterprise Identity Mapping). Aceasta asigură că drepturile de acces și autorizările pentru certificat sunt aceleași ca ale deținătorului 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 aplicații să autentifice și să accepte certificate emise de CA (autoritate de certificare).

Când se procură un certificat al Autorității de certificare în propriul browser, acesta vă permite să îl desemnați drept rădăcină de încredere. Alte aplicații care suportă folosirea certificatelor trebuie să fie de asemenea configurate să aibă încredere în CA înainte ca această aplicație să poată autentifica și să aibă încredere în certificatele emise de un CA special.

Puteți folosi DCM pentru a activa sau dezactiva starea de încredere pentru un certificat CA (Certificate Authority). Atunci când activați un certificat CA, puteți specifica faptul că aplicațiile îl pot utiliza pentru a autentifica și accepta certificatele emise de CA. Când dezactivați un certificat CA, nu puteți specifica faptul că aplicațiile îl pot utiliza pentru a autentifica și accepta certificatele emise de CA.

Date de politică Autoritate de certificare

Când creați un CA (Certificate Authority) local cu Digital Certificate Manager, puteți specifica datele de politică pentru CA-ul local. Datele de politică pentru un CA local descriu privilegiile de semnare pe care le are acesta. Datele politicii determină:

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

Concepte înrudite

“Semnături digitale” la pagina 4

O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme criptografie și este echivalent cu o semnătură personală pe un document scris.

“Perechea de chei publice-private” la pagina 5

Fiecare certificat digital are o pereche de chei criptografice asociate.

Locații CRL (listă de revocare certificate)

O listă de revocare a certificatelor (CRL) este un fișier care conține informații despre toate certificatele invalide și revocate pentru o Autoritate de certificare (CA) specifică.

CA-urile actualizează periodic CRL-urile lor și le fac disponibile și altora pentru ca aceștia să le publice în directoarele Lightweight Directory Access Protocol (LDAP). Puține CA-uri, cum ar fi SSH în Finlanda, își publică singure CRL-urile în directoarele LDAP pe care le puteți accesa direct. Dacă un CA își publică propria listă CRL, certificatul indică acest lucru incluzând o extensie punct distribuție CRL în formularul Uniform Resource Identifier (URI - identificator resursă uniform).

DCM (Digital Certificate Manager) vă permite să definiți și să gestionați informațiile despre locațiile CRL pentru a asigura o autentificare mai stringentă pentru certificatele pe care le folosiți sau le acceptați de la alții. O definiție locație CRL descrie locația unui, și informațiile de acces pentru server-ul Lightweight Directory Access Protocol (LDAP) care păstrează CRL-ul.

- | Când vă conectați la un server LDAP trebuie să furnizați un DN și 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 obțină starea corectă
- | din CRL. Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiți unealta Administrare Web

l pentru Directory Server și selectați task-ul "Gestionare schemă" pentru a schimba clasa de securitate (de asemenea
l numit și "clasă de acces") a atributelor **certificateRevocationList** și **authorityRevocationList** din "critical" în
l "normal".

Aplicațiile care efectuează autentificarea certificatelor accesează locația CRL, dacă este definită una, pentru un CA specific pentru a se asigura că aceasta nu a revocat un anumit certificat. DCM vă permite să definiți și să gestionați informațiile despre locația CRL de care au nevoie aplicațiile pentru a efectua procesare CRL în timpul autentificării certificatului. Exemple de aplicații și procese care pot efectua procesare CRL pentru autentificarea certificatelor: serverul VPN (rețea privată virtuală) IKE (Internet Key Exchange), aplicațiile activate SSL (Secure Sockets Layer) și procesele care semnează aplicații. De asemenea, atunci când definiți locații CRL și le asociați 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 și aplicațiilor" la pagina 65

Puteți folosi DCM (Digital Certificate Manager) pentru a valida certificate individuale sau aplicațiile care le folosesc. Lista de lucruri pe care le verifică DCM diferă puțin în funcție de validarea unui certificat sau a unei aplicații.

Operații înrudite

"Gestionarea locațiilor CRL" la pagina 66

Digital Certificate Manager (DCM) vă permite să definiți și să administrați informații despre locația CRL (Certificate Revocation List) pentru o Autoritate de certificare (CA) particulară pentru a o folosi ca parte din procesul de validare a certificatului.

Depozite de certificate

Un depozit de certificate este un fișier bază de date cheie special pe care DCM îl folosește pentru a memora certificatele digitale.

Depozitul de certificate conține de asemenea cheia privată a certificatului doar dacă nu alegeți să folosiți un IBM Cryptographic Coprocessor pentru a memora cheia în schimb. DCM vă permite să creați și să gestionați mai multe tipuri de depozite de certificate. DCM controlează accesul la depozitele de certificate prin parole în conjuncție cu controlul accesului la directorul sistemului de fișiere și la fișierele care constituie depozitul de certificate.

Depozitele de certificate sunt clasificate pe baza tipurilor de certificate pe care le conțin. Task-urile de management pe care le puteți efectua pentru fiecare depozit de certificate variază în funcție de tipul certificatului pe care îl conține depozitul de certificate. DCM furnizează următoarele depozite de certificate predefinite pe care le puteți crea și gestiona:

Autoritate de certificare (CA)

DCM folosește acest depozit de certificate pentru a memora certificatul CA local și cheia sa primară în cazul în care creați un CA local. Puteți folosi certificatul din acest depozit pentru a semna certificate pentru care folosiți CA-ul local pentru a le emite. Când CA-ul local emite un certificat, DCM pune o copie a certificatului CA (fără cheia privată) în depozitul de certificate corespunzător (de exemplu, *SYSTEM) pentru scopuri de autentificare. Aplicațiile folosesc certificate CA pentru a verifica originea certificatelor pe care trebuie să le valideze ca parte a negocierilor SSL pentru a garanta autorizații pentru resurse.

***SYSTEM**

DCM furnizează depozitul de certificate pentru gestionarea certificatelor server sau client pe care le folosesc aplicațiile pentru a participa la sesiuni de comunicare SSL (Secure Sockets Layer). Aplicațiile IBM iSeries (și, probabil, și multe aplicații ale altor dezvoltatori de software) sunt scrise pentru a folosi certificate numai din depozitul de certificate *SYSTEM. Când folosiți DCM pentru a crea un CA local, DCM creează acest depozit de certificate ca parte a procesului. Când alegeți să obțineți certificate de la un CA public, cum sunt VeriSign, pentru ca aplicația dumneavoastră server sau client să le folosească, trebuie să creați acest depozit de certificate.

***OBJECTSIGNING**

DCM furnizează acest depozit de certificate pentru gestionarea certificatelor pe care le folosiți pentru a semna

digital obiecte. De asemenea, task-urile din acest depozit de certificate vă permit să creați semnături digitale pe obiecte, cât și să vizualizați și să verificați semnăturile de pe obiecte. Când folosiți DCM pentru a crea un CA local, DCM creează acest depozit de certificate ca parte a procesului. Când alegeți să obțineți certificate de la un CA public, cum sunt VeriSign, pentru semnarea obiectelor, trebuie să creați acest depozit de certificate.

*SIGNATUREVERIFICATION

DVM furnizează acest depozit de certificate pentru gestionarea certificatelor pe care le folosiți pentru a verifica autenticitatea semnăturilor digitale de pe obiecte. Pentru a verifica o semnătură digitală, acest depozit de certificate trebuie să conțină o copie a certificatului care a semnat obiectul. Depozitul de certificate trebuie să conțină de asemenea o copie a certificatului CA pentru CA care a emis certificatul de semnat obiecte. Obțineți aceste certificate fie exportând certificatele de semnat obiecte de pe sistemul curent în depozit, fie importând certificatele pe care le primiți de la semnatarul obiectului.

Alt depozit de certificate sistem

Acest depozit de certificate oferă o locație alternativă de depozitare a certificatelor client sau server pe care le folosiți pentru sesiuni SSL. Depozitele de certificate de pe alt sistem sunt depozite secundare de certificate definite de utilizatori pentru certificate SSL. Opțiunea Alte depozite de certificate sistem vă permite să gestionați certificate pentru aplicațiile pe care dumneavoastră sau alții le scrieți și care folosesc API SSL_Init pentru a accesa și a folosi programat un certificat pentru a stabili o sesiune SSL. Acest API permite unei aplicații să folosească mai repede certificatul implicit pentru un depozit de certificate decât certificatul identificat implicit. Mai des, folosiți acest depozit de certificate atunci când transferați certificate de la o ediție anterioară a DCM, sau când creați un subset special de certificate folosite pentru SSL.

Notă: acă pe server este instalat IBM Cryptographic Coprocessor, puteți alege alte opțiuni de memorare a cheii private pentru certificate (cu excepția certificatelor de semnare pentru obiecte). Puteți alege să păstrați cheia privată chiar pe coprocesor sau să îl folosiți pe acesta pentru a cripta cheia privată și să o păstrați într-un fișier special cheie privată în loc de depozitul de certificate.

DCM controlează accesul la depozitele de certificate prin parole. De asemenea, DCM menține controlul accesului la directoarele și fișierele sistemului de fișiere integrat care constituie depozitele de certificate. Depozitele de certificate CA local, *SYSTEM, *OBJECTSIGNING și *SIGNATUREVERIFICATION trebuie să fie localizate în căi specifice ale sistemului de fișiere integrat, iar Alte depozite de certificate sistem pot fi localizate oriunde în sistemul de fișiere integrat.

Concepte înrudite

“Tipuri de certificate digitale” la pagina 28

Folosiți aceste informații pentru a învăța diferitele tipuri de certificate pentru administrarea cărora puteți folosi DCM.

Criptografie

Citiți aceste informații pentru a afla ce este criptografia și cum folosesc certificatele digitale funcțiile criptografice pentru a oferi securitate.

Criptografia este știința de a ține datele în siguranță. Criptografia vă permite stocarea de informații sau comunicarea cu terți în timp ce împiedicați ca părțile neimplicate să înțeleagă informațiile stocate sau să înțeleagă comunicația. Criptarea transformă textul inteligibil într-unul neinteligibil (ciphertext). Decriptarea reface textul inteligibil din date cifrate. Ambele procese presupun o formulă matematică sau un algoritm și o secvență secretă de date (cheia).

Sunt două tipuri de criptografieri:

- În criptografia **partajată sau cu cheie secretă (simetrică)**, o cheie este un secret partajat între două părți în comunicare. Criptarea și decriptarea folosesc aceeași cheie.
- În criptografia **cu cheie publică (asimetrică)**, criptarea și decriptarea folosesc fiecare chei diferite. Un grup are o pereche de chei compusă dintr-o cheie publică și una privată. Cheia publică se distribuie liber, tipic într-un certificat digital, în timp ce cheia privată este păstrată în siguranță de către proprietar. Cele două chei sunt matematice, dar este virtual imposibil să derivați 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 și receptorul poate folosi cheia privată corespunzătoare pentru decriptarea acestei semnături digitale.

Concepte înrudite

"Semnături digitale" la pagina 4

O semnătură digitală pe un document electronic sau pe alt obiect este creată prin folosirea unei forme criptografie și este echivalent cu o semnătură personală pe un document scris.

"SSL (Secure Sockets Layer)"

Original creat de Netscape, SSL (Secure Sockets Layer) este standardul industrial pentru criptarea sesiunilor între clienți și servere.

IBM Cryptographic Coprocessors for iSeries

Coprocessorul criptografic furnizează servicii criptografice dovedite, asigurând protecție și integritate, pentru a dezvolta aplicații e-business sigure.

Dacă se folosește IBM Cryptographic Coprocessor for iSeries se adaugă serverului capacitatea de procesare criptografică de înaltă siguranță. Dacă aveți un coprocessor criptografic instalat și variat pe sistemul dumneavoastră, îl puteți utiliza pentru a oferi memorare mai sigură a cheii pentru cheile private ale certificatului.

Puteți folosi coprocessorul criptografic pentru a memora cheia privată pentru un certificat server sau client și pentru un certificat Autoritate de certificare (CA). Totuși, nu puteți folosi coprocessorul 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 puteți folosi coprocessorul pentru a depozita cheia privată pentru un certificat care semnează obiecte.

Puteți fie să memorați cheia privată a unui certificat direct în coprocessorul criptografic, fie puteți folosi cheia master a coprocessorului criptografic pentru a cripta cheia și să o memorați într-un fișier cheie special. Puteți selecta aceste opțiuni de memorare a cheii ca parte a procesului de creare sau reînnoire a unui certificat. De asemenea, dacă folosiți coprocessorul pentru a depozita cheia privată a unui certificat, puteți modifica atribuirea dispozitivului coprocessor pentru acea cheie.

Pentru a utiliza coprocessorul criptografic pentru memorarea cheii private, trebuie să vă asigurați că acesta este activat înainte să folosiți DCM (Digital Certificate Manager). Altfel, DCM nu furnizează opțiunea de selectare a unei locații de memorare ca parte a procesului de creare sau reînnoire a certificatului.

Concepte înrudite

"Memorarea cheilor certificatului pe un IBM Cryptographic Coprocessor" la pagina 67

Aflați cum să folosiți un coprocessor instalat pentru a furniza depozite mai sigure pentru cheile private ale certificatelor dumneavoastră.

SSL (Secure Sockets Layer)

Original creat de Netscape, SSL (Secure Sockets Layer) este standardul industrial pentru criptarea sesiunilor între clienți și servere.

SSL folosește criptografie cu chei asimetrice sau publice pentru a cripta sesiuni între server și client. Aplicațiile client și server negociază această cheie sesiune în timpul unui schimb de certificate digitale. Cheia expiră automat după 24 de ore și procesul SSL creează o cheie diferită pentru fiecare conexiune server și fiecare client. Astfel, chiar dacă utilizatorii neautorizați interceptează și 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

"Criptografie" la pagina 8

Citiți aceste informații pentru a afla ce este criptografia și cum folosesc certificatele digitale funcțiile criptografice pentru a oferi securitate.

“Tipuri de certificate digitale” la pagina 28

Folosiți aceste informații pentru a învăța diferitele tipuri de certificate pentru administrarea cărora puteți folosi DCM.

Definiții aplicație

Citiți aceste informații pentru a învăța ce aplicații DCM sunt și cum să lucrați cu ele pentru configurare SSL și semnare obiect.

Sunt două tipuri de definiții de aplicație pe care le puteți gestiona în DCM(Digital Certificate Manager):

- Definiții de aplicații client sau server care folosesc sesiuni de comunicații SSL (Secure Sockets Layer).
- Definiții de aplicații de semnare obiecte care semnează obiecte pentru a asigura integritatea obiectului.

Pentru a folosi DCM în lucrul cu definiții aplicație SSL și certificatele lor, aplicația trebuie mai întâi să se înregistreze cu DCM ca o definiție aplicație pentru a avea un ID unic. Dezvoltatorii de aplicații înregistrează aplicațiile cu SSL activat utilizând un API (QSYRGAP, QsyRegisterAppForCertUse) pentru a crea ID-ul aplicației în DCM automat. Toate aplicațiile IBM iSeries activate pentru SSL sunt înregistrate în DCM, așa că puteți să folosiți cu ușurință DCM pentru a le aloca un certificat astfel încât să poată stabili o sesiune SSL. De asemenea, pentru aplicațiile pe care le scrieți sau cumpărați, puteți defini o definiție aplicație și să creați ID-ul aplicație pentru el chiar din DCM. Trebuie să lucrați în depozitul de certificate *SYSTEM pentru a crea o definiție aplicație SSL pentru o aplicație server sau client.

Pentru a folosi un certificat pentru semnarea obiectelor, trebuie să definiți mai întâi o aplicație pe care să o folosească certificatul. Spre deosebire de o definiție aplicație SSL, o aplicație care semnează obiecte nu descrie o aplicație reală. În schimb, definiția aplicației pe care o creați ar putea descrie tipul sau grupul obiectelor pe care intenționați să le semnați. Trebuie să lucrați în depozitul de certificate *OBJECTSIGNING pentru a crea o definiție aplicație care semnează obiecte.

Concepte înrudite

“Gestionarea aplicațiilor în DCM” la pagina 62

Acest subiect vă oferă informații despre crearea definițiilor aplicație și cum să gestionați o atribuire de certificat a unei aplicații. Puteți afla despre definirea listelor de încredere CS pe care le folosesc aplicațiile ca bază pentru a accepta certificate pentru autentificarea clienților.

Operații înrudite

“Crearea unei definiții de aplicație” la pagina 62

Examinați acest subiect pentru a învăța cum două tipuri de aplicații pe care le puteți defini și lucra cu ele.

Validarea

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

Validarea certificatelor

Când validați un certificat, DCM (Digital Certificate Manager) verifică un număr de articole care aparțin certificatului pentru a asigura autenticitatea și validitatea sa. Validarea unui certificat se asigură că pentru aplicația care folosește certificatul pentru comunicații sigure sau pentru semnarea obiectelor nu există șanse 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 locația CRL există pentru CA care a emis acest certificat.

| Dacă configurați maparea LDAP (Lightweight Directory Access Protocol) pentru a folosi CRL, DCM verifică CRL-ul
| când validează certificatul pentru a fi sigur că certificatul nu este listat în CRL. Toruși, validarea procesului pentru
| verificarea cu acuratețe CRL, serverul director (LDAP) configurat pentru maparea LDAP trebuie să conțină un CRL
| corespunzător. În caz contrar, luați legătura cu Microsoft pentru a obține cea mai recentă actualizare. Trebuie să

furnizați un DN și o parolă pentru a evita revocarea validării unui certificat . De asemenea, dacă nu specificați un DN și o parolă când configurați maparea LDAP veți 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 obțină starea corectă din CRL. Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiți unealta Administrare Web pentru Directory Server și selectați task-ul "Gestionare schemă" pentru a schimba clasa de securitate (de asemenea numit și ca "clasă de acces") a atributelor **certificateRevocationList** și **authorityRevocationList** din "critical" în "normal".

DCM verifică de asemenea că certificatul CA pentru CA emițătoare este depozitul de certificate curent și 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 potrivește. Cu alte cuvinte, DCM criptează datele cu cheia publică și apoi se asigură că acestea pot fi decriptate cu cheia privată.

Validarea aplicațiilor

Când validați o aplicație, DCM (Digital Certificate Manager) verifică că există o alocare de certificat pentru aplicație și asigură că certificatul alocat este valid. În plus, DCM se asigură că dacă aplicația este configurată pentru a folosi o listă de încredere Autoritate de certificare (CA), atunci lista de încredere conține cel puțin un certificat CA. DCM verifică mai apoi dacă certificatele CA din lista de încredere CA a aplicației sunt valide. De asemenea, dacă definiția aplicației specifică că apare procesarea CRL (Certificate Revocation List) și că există o locație CRL definită pentru CA, DCM verifică CRL-ul ca parte a procesului de validare.

Validarea unui aplicații poate să vă ajute să vă alerteze despre problemele potențiale pe care le-ar putea avea aplicația când realizează o funcție care necesită certificate. Asemenea probleme ar putea împiedica o aplicație 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 și aplicațiilor” la pagina 65

Puteți folosi DCM (Digital Certificate Manager) pentru a valida certificate individuale sau aplicațiile care le folosesc. Lista de lucruri pe care le verifică DCM diferă puțin în funcție de validarea unui certificat sau a unei aplicații.

Scenarii DCM

Folosiți aceste informații pentru a examina două scenarii care ilustrează scheme tipice de implementare a certificatelor, pentru a vă ajuta să vă planificați propria iSeries ca parte a politicii de securitate. Fiecare scenariu furnizează de asemenea toate task-urile de configurare necesare pe care trebuie să le realizați pentru a face scenariul după descriere.

DCM (Digital Certificate Manager) și iSeries certificate digitale care permit utilizatorilor să perfecționeze polița de securitate în nenumărate moduri. Alegerea modului în care folosiți certificatele depinde atât de obiectivele dumneavoastră de afaceri, cât și de nevoile dumneavoastră de securitate.

Folosirea certificatelor digitale vă poate ajuta să vă îmbunătățiți securitatea în mai multe moduri. Certificatele digitale permit folosirea SSL (Secure Sockets Layer) pentru acces sigur la pagini Web și alte servicii Internet. Puteți folosi certificate digitale pentru a configura conexiuni VPN (rețea privată virtuală). De asemenea, puteți 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 și protejează integritatea obiectului.

Securitatea sistemului poate fi îmbunătățită atunci când se utilizează certificate digitale (în locul numelor de utilizatori și a parolilor) pentru a autentifica și autoriza sesiunile dintre utilizatori și servere. De asemenea, în funcție de cum configurați DCM, puteți folosi DCM pentru a asocia un certificat de utilizator profilului său de utilizator sau identificatorului EIM (Enterprise Identity Mapping) iSeries. Certificatul apoi are aceleași autorizări și permisiuni ca profilul utilizator asociat.

În consecință, cum alegeți să folosiți certificatele poate fi complicat și depinde de o multitudine de factori. Scenariile furnizate în acest subiect descriu unele din cele mai comune obiective de securitate cu certificate digitale pentru comunicații sigure în contextele tipice de afaceri. Fiecare scenariu descrie de asemenea toate cerințele de sistem și software preliminară necesare și toate task-urile de configurare pe care trebuie să le realizați pentru a implementa scenariul.

Informații înrudite

Cerințe preliminare pentru semnarea obiectelor

Scenariu: Folosirea certificatelor pentru autentificări externe

Acest scenariu descrie când și cum să folosiți certificate ca un mecanism de autentificare pentru a proteja și limita accesul utilizatorilor publici la resurse publice sau din afara rețelei și la aplicații.

Situație:

Lucrați pentru compania de asigurări MyCo, Inc și sunteți responsabil pentru menținerea diferitelor aplicații de pe siturile rețelei interne și externe a companiei dumneavoastră. O anumită aplicație pentru care sunteți responsabil este o aplicație de calculare a ratei care permite ca sute de agenți independenți să genereze baremuri pentru clienții lor. Deoarece informația pe care această aplicație o furnizează este oarecum sensibilă, doriți să vă asigurați că doar agenții înregistrați o pot folosi. Mai mult, vreți să furnizați în final o metodă mai sigură de autentificare utilizator la aplicație decât metoda curentă cu nume utilizator și parolă. Sunteți îngrijorat suplimentar că utilizatori neautorizați ar putea captura aceste informații când sunt transmise printr-o rețea în care nu aveți încredere. De asemenea, sunteți îngrijorat că diferiți agenți ar putea împărtăși aceste informații cu fiecare care nu are autorizare să facă asta.

După unele cercetări, decideți că folosirea certificatelor digitale vă poate oferi securitatea de care aveți nevoie pentru a proteja informațiile sensibile introduse în și extrase din această aplicație. Folosirea certificatelor vă permite să folosiți SSL (Secure Sockets Layer) pentru a proteja transmisia datelor rată. Deși doriți ca în final toți agenții să folosească un certificat pentru a accesa aplicația, știți că s-ar putea ca agenții și compania dumneavoastră să aibă nevoie de ceva timp înainte ca acest scop să fie realizat. În plus la folosirea autentificării client prin certificat, plănuți să continuați folosirea curentă a autentificării prin nume utilizator și parolă deoarece SSL protejează intimitatea acestor date sensibile la transmisie.

Pe baza tipului de aplicație și a utilizatorilor ei și a scopului dumneavoastră viitor de autentificare a certificatelor pentru toți utilizatorii, decideți să folosiți un certificat public de la un CA binecunoscut pentru a configura SSL pentru aplicația dumneavoastră.

Avantajele scenariului

Acest scenariu are următoarele avantaje:

- Folosirea certificatelor digitale pentru a configura accesul SSL la aplicația dumneavoastră de calculare a ratei asigură că informația transmisă între server și client este protejată și privată.
- Folosirea certificatelor digitale de fiecare dată când este posibilă pentru autentificarea clientului furnizează o metodă mai sigură de identificare a utilizatorilor autorizați. Chiar unde folosirea certificatelor digitale nu este posibilă, autentificarea client prin intermediul autentificării cu nume utilizator și parolă este protejată și menținută privată de către sesiunea SSL, făcând schimbul de astfel de date sensibile mai sigur.
- Folosirea certificatelor digitale *publice* pentru a autentifica utilizatori la aplicațiile și datele dumneavoastră în maniera pe care o descrie acest scenariu este o alegere practică pentru aceste condiții sau unele similare:
 - Datele și aplicațiile dumneavoastră necesită diferite nivele de securitate.
 - Există o rată înaltă de modificări (turnover) între utilizatorii de încredere.
 - Furnizați acces public la aplicații și date, cum ar fi un sit Web Internet sau o aplicație din afara rețelei.
 - Nu vreți să operați propria Autoritate de certificare (CA) pe baza motivelor administrative, cum ar fi un număr mare de utilizatori din afară care vă accesează aplicațiile și resursele.

- Folosirea unui certificat public pentru a configura aplicația de calculare rate pentru SSL din acest scenariu scade cantitatea de configurare pe care utilizatorii trebuie să o realizeze pentru a accesa aplicația sigur. Majoritatea software-ului client conține certificate CA pentru majoritatea CA-urilor bine cunoscute.

Obiective

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

Obiectivele acestui scenariu sunt următoarele:

- Aplicația de calculare a ratei publice a companiei trebuie să folosească SSL pentru a proteja izolarea datelor pe care le furnizează și le primesc de la utilizatori.
- Configurarea SSL trebuie realizată cu certificate publice de la un CA public binecunoscut din Internet.
- Utilizatorii autorizați trebuie să furnizeze un nume utilizator și parolă valide pentru a accesa aplicația în modul SSL. În cele din urmă, utilizatorii autorizați trebuie să poată folosi una din cele două metode de autentificare sigură pentru a li se permite accesul la aplicație. Agenții trebuie să prezinte fie un certificat digital public de la un CA binecunoscut, fie un nume de utilizator și o parolă valide, în cazul în care certificatul nu este disponibil.

Detalii

Următoarea figură ilustrează configurația rețelei în acest scenariu:

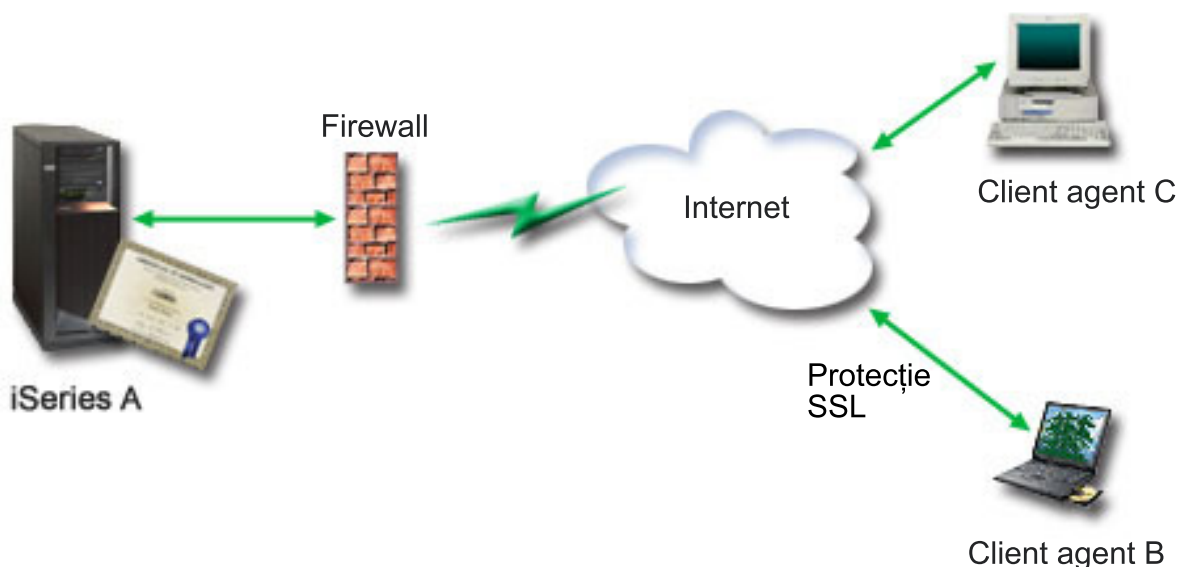


Figura ilustrează următoarele informații despre situația pentru acest scenariu:

Serverul public al companiei iSeries A

- iSeriesServerul A este serverul care găzduiește aplicația companiei de calculare a ratei.
- iSeries A folosește i5/OS Versiunea 5 Ediția 4 (V5R4).
- iSeries Pe serverul A sunt instalate și configurate Digital Certificate Manager (i5/OS opțiunea 34) și IBM HTTP Server for i5/OS (5722-DG1).
- iSeries Serverul A rulează aplicația de calculare a ratei, care este configurată în așa fel încât:
 - Necesită modul SSL.
 - Folosește un certificat public de la un CA binecunoscut pentru a se autentifica pe sine pentru a inițializa o sesiune SSL.

- Necesită autentificarea utilizatorului prin nume utilizator și parolă.
- iSeries A își prezintă certificatul pentru a iniția o sesiune SSL când clienții B și C accesează aplicația de calculare a ratei.
- După inițializarea sesiunii SSL, iSeries A cere clienților B și C să furnizeze un nume de utilizator și o parolă valide înainte de a permite accesul la aplicația de calculare a ratei.

Sistemele client agent Client B și Client C

- Clienții B și C sunt agenți independenți care accesează aplicația de calcul a ratei.
- Software-ul client al clienților B și C are o copie instalată a certificatului CA binecunoscut care a emis certificatul aplicației.
- Clienții B și C accesează aplicația de calculare a ratei de pe iSeries A, care își prezintă certificatul către software-ul de client pentru autentificarea identității sale și inițierea unei sesiuni SSL.
- Software-ul client de pe Clientul B și C este configurat să accepte certificatul de la iSeries A pentru inițializarea unei sesiuni SSL.
- După ce începe sesiunea SSL, clienții B și C trebuie să furnizeze un nume de utilizator și o parolă valide pentru ca iSeries A să le acorde acces la aplicație.

Cerințele preliminare și presupuneri

Acest scenariu depinde de următoarele cerințe preliminare și supoziții:

- Aplicația de calculare a ratei de pe iSeries A este o aplicație generică, ce poate fi configurată să folosească SSL. Cele mai multe aplicații, inclusiv multe aplicații iSeries asigură suportul SSL. Pașii de configurare SSL variază foarte mult de la aplicație la aplicație. În consecință, acest scenariu nu furnizează instrucțiuni specifice pentru configurarea aplicației de calculare rată să folosească SSL. Acest scenariu furnizează instrucțiuni pentru configurarea și gestionarea certificatelor care sunt necesare pentru ca orice aplicație să folosească SSL.
- Aplicația de calcul a ratei poate avea capabilitatea de a cere certificate pentru autentificarea unui client. Acest scenariu furnizează instrucțiuni despre cum să folosiți DCM (Digital Certificate Manager) pentru a configura încrederea în certificate pentru acele aplicații care oferă acest suport. Deoarece pașii de configurare pentru autentificarea unui client diferă de la aplicație la aplicație, acest scenariu nu dă instrucțiuni specifice pentru configurarea unui certificat de autentificare a unui client pentru aplicația de calcul a ratei.
- iSeries A îndeplinește cerințele pentru instalarea și folosirea DCM (Digital Certificate Manager).
- Nimeni nu a configurat sau folosit anterior DCM pe iSeries A.
- Oricine folosește DCM pentru a realiza task-urile din acest scenariu trebuie să aibă autorizările speciale *SECADM și *ALLOBJ pentru profilurile lor de utilizator.
- Pe iSeries A nu este instalat IBM Cryptographic Coprocessor.

Task-urile de configurare

Operații înrudite

“Pornirea Digital Certificate Manager” la pagina 37

Folosiți aceste informații pentru a afla cum se accesează caracteristica DCM (Digital Certificate Manager) pe sistem.

Finalizarea foilor de lucru pentru planificare

Următoarele work sheet-uri demonstrează informațiile pe care trebuie să le adunați și deciziile pe care este nevoie să le faceți pentru a pregăti implementarea certificatelor digitale pe care o descrie acest scenariu. Pentru a asigura o implementare cu succes, este nevoie să fiți capabil să răspundeți Da la toate articolele cerințelor preliminare și aveți nevoie să aveți adunate toate informațiile cerute înainte să realizați orice task de configurare.

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

Foaie de lucru cerințe preliminare	Răspunsuri
i5/OS al dumneavoastră este V5R42 (5722-SS1)?	Da

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

Foaie de lucru cerințe preliminare	Răspunsuri
Este instalată pe sistemul dumneavoastră opțiunea 34 a i5/OS?	Da
Este instalat IBM HTTP Server for i5/OS(5722–DG1) pe sistemul dumneavoastră și este pornită instanța Admin a serverului?	Da
Este configurat TCP pentru sistemul dumneavoastră astfel încât să puteți folosi un browser Web și instanța serverului administrativ server HTTP pentru a accesa DCM?	Da
Aveți autorizările speciale *SECADM și *ALLOBJ?	Da

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

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

Foaie de lucru de planificare pentru serverul iSeries A	Răspunsuri
Veți opera propriul dumneavoastră CA local sau veți obține certificate pentru aplicația dumneavoastră de la un CA public?	Obțineți certificate de la un CA public
Serverul iSeries A găzduiește aplicația pe care vreți să o activați pentru SSL?	Da
Ce informații despre nume distinctiv veți folosi pentru cererea de semnare certificat (CSR) pe care o creați cu DCM? <ul style="list-style-type: none"> • Dimensiune cheie: determină puterea cheilor criptografice pentru certificat. • Etichetă certificat: identifică certificatul cu un șir unic de caractere. • Nume comun: identifică proprietarul certificatului, cum ar fi o persoană, entitate sau aplicație; parte a DN-ului subiect pentru certificat. • Unitate de organizare: identifică secțiunea sau zona de organizare pentru aplicația care va folosi acest certificat. • Nume organizație: identifică compania dumneavoastră sau secțiunea divizionară pentru aplicația care va folosi acest certificat. • Localitate sau oraș: identifică orașul sau o desemnare a localității pentru organizația dumneavoastră. • Stat sau provincie: identifică statul sau provincia în care veți folosi acest certificat. • Țară sau regiune: identifică, cu o desemnare din două litere, țara sau regiunea în care veți folosi acest certificat. 	Mărime cheie: 1024 Etichetă certificat: Myco_public_cert nume comun: myco_rate_server@myco.com Unitate de organizare: Rate dept Nume organizație: myco Localitate sau oraș: Any_city Province sau stat: Any Țara sau regiune: ZZ
Care este ID-ul aplicației DCM pentru aplicația pe care vreți să o configurați să folosească SSL?	mcyo_agent_rate_app
Veți configura aplicația cu SSL aplicat să folosească certificate pentru autentificarea client? Dacă da, care CA-uri vreți să le adăugați la lista de CA-uri de încredere a aplicației?	Nu

Crearea unei cereri de certificate server sau client

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

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

3. Selectați ***SYSTEM** ca depozit de certificate pentru creare și apăsați **Continuare**.
4. Selectați **Da** pentru a crea un certificat ca parte a creării depozitului de certificate ***SYSTEM** și apăsați **Continuare**.
5. Selectați **VeriSign sau altă CA Internet (autoritate de certificare)** ca semnatar al noului certificat și efectuați un clic pe **Continuare** pentru a se afișa un formular care vă va permite să introduceți informații de identificare pentru noul certificat.
6. Completați formularul și apăsați **Continuare** pentru a se afișa pagina de confirmare. Această pagină de confirmare va afișa datele cererii certificatului pe care trebuie să îl furnizați Autorității de certificare publice care va emite certificatul. Datele CSR (Certificate Signing Request) sunt constituite din cheia publică, numele distinctiv și alte informații pe care le-ați specificat pentru certificatul nou.
7. Copiați cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fișier separat, pe care îl solicitați CA public pentru cererea unui certificat. Trebuie să folosiți toate datele CSR, inclusiv liniile Begin și End New Certificate Request.

Notă: Atunci când părăsiți această pagină, datele vor fi pierdute și nu se vor mai putea recupera.

8. Atunci când părăsiți această pagină, datele vor fi pierdute și nu se vor mai putea recupera.
9. Așteptați ca CA să returneze certificatul complet, semnat înainte de a continua cu pasul următor al task-ului pentru scenariu.

După ce CA returnează certificatul complet semnat, puteți configura aplicația dumneavoastră să folosească SSL, importați certificatul în depozitul de certificate ***SYSTEM** și alocați-l aplicației dumneavoastră să îl folosească pentru SSL.

Configurarea aplicației să folosească SSL

Când vă primiți înapoi certificatul semnat de la CA publică, puteți continua procesul de activare a comunicațiilor SSL pentru aplicația dumneavoastră publică. Trebuie să configurați aplicația să folosească SSL înainte să lucreze cu certificatele dumneavoastră semnate. Unele aplicații, cum ar fi serverul HTTP pentru iSeries generează un ID aplicație unic și îl înregistrează cu DCM (Digital Certificate Manager) când configurați aplicația să folosească SSL. Trebuie să știți ID-ul aplicației înainte de a putea folosi DCM pentru a aloca la ea certificatul dumneavoastră semnat și să terminați procesul de configurare SSL.

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

Pentru a vă configura aplicația să folosească SSL, urmați instrucțiunile pe care le furnizează documentația aplicației dumneavoastră. De asemenea, puteți învăța mai multe despre configurarea multor aplicații IBM comune să folosească SSL prin revederea, SSL (Secure Sockets Layer) din Centrul de informare Centrul de informare iSeries.

Când terminați configurarea SSL pentru aplicația dumneavoastră, puteți configura certificatul public semnat pentru aplicație astfel încât să poată inițializa sesiuni SSL.

Importarea și alocarea certificatului public semnat

După ce vă configurați aplicația să folosească SSL, puteți folosi DCM pentru a importa certificatul dumneavoastră semnat și să-l alocați aplicației dumneavoastră.

Pentru a importa și aloca certificatul dumneavoastră către aplicația dumneavoastră pentru a completa procesul de configurare SSL, urmați acești pași:

1. Porniți DCM.

2. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați ***SYSTEM** pentru ca să se deschidă depozitul de certificate.
3. Când este afișată pagina **Depozit de certificate și parolă**, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și faceți clic pe **Continuare**.
4. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate ***SYSTEM**.

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

6. Apoi, selectați **Alocare certificat** din lista de task-uri **Gestionare certificate** pentru a afișa o listă de certificate pentru depozitul de certificate curent.
7. Selectați certificatul dumneavoastră din listă și faceți clic pe **Alocare la aplicații** pentru a afișa o listă de definiții de aplicații pentru depozitul de certificate curent.
8. Selectați aplicația dumneavoastră din listă și apăsați **Continuare**. Apare o pagină fie cu un mesaj de confirmare pentru selecția dumneavoastră de alocare fie cu un mesaj de eroare dacă a apărut o problemă.

Cu aceste task-uri completate, vă puteți porni aplicația în modul SSL și puteți începe protejarea securității datelor pe care le furnizează.

Pornirea aplicației în mod SSL

După ce terminați procesul de importare și alocare a certificatului către aplicația dumneavoastră, s-ar putea să trebuiască să terminați și să reporniți aplicația în modul SSL. Acest lucru este necesar în unele cazuri deoarece s-ar putea ca aplicația să nu poată să determine că alocarea certificatului există în timp ce aplicația se execută. Revedeți documentația pentru aplicația dumneavoastră pentru a determina dacă aveți nevoie să reporniți aplicația sau pentru alte informații despre pornirea aplicației în modul SSL.

Dacă vreți să folosiți certificate pentru autentificarea clientului, puteți defini acum o listă de CA-uri de încredere pentru aplicație.

(Opțional): Definirea listei de CA-uri de încredere pentru o aplicație care necesită certificate pentru autentificarea clientului

Aplicațiile 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 identității. Unul dintre criteriile pe care le folosește o aplicație pentru autentificarea unui certificat este dacă aceasta are încredere în CA (autoritatea de certificare) care a emis certificatul.

Situația pe care o descrie acest scenariu nu necesită ca aplicația de calculare rată să folosească certificate pentru autentificarea client, dar aplicația va fi capabilă să accepte certificate pentru autentificare atunci când sunt disponibile. Multe aplicații furnizează suport pentru certificate de autentificare client; cum configurați acest suport variază mult în cadrul aplicațiilor. Acest task opțional este furnizat pentru a vă ajuta să înțelegeți cum să folosiți DCM pentru a activa încrederea în use pentru autentificarea clientului ca un fundament pentru configurarea suportului aplicației dumneavoastră pentru certificate de autentificare a clientului.

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

- Aplicația trebuie să suporte utilizarea certificatelor pentru autentificare client.
- Definiția DCM pentru aplicație trebuie să specifice că aplicația folosește o listă de încredere CA.

Dacă definiția pentru o aplicație specifică faptul că o aplicație folosește o listă de încredere CA, trebuie să definiți lista înainte ca aplicația să poată efectua cu succes autentificarea client a certificatului. Acest lucru asigură faptul că aplicația poate valida doar acele certificate care provin de la CA-uri pe care le-ați specificat ca fiind de încredere. Dacă

utilizatorii sau o aplicație client prezintă un certificat care provine de la un CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicația nu îl va accepta ca bază pentru o autentificare validă.

Pentru a folosi DCM să definiți o listă de încredere CA pentru aplicația dumneavoastră, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați ***SYSTEM** pentru ca să se deschidă depozitul de certificate.
3. Când este afișată pagina **Depozit de certificate și parolă**, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și faceți clic pe **Continuare**.
4. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Setare stare CA** pentru a afișa o listă de certificate CA.

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

6. Selectați unul sau mai multe certificate CA din lista în care aplicația dumneavoastră va avea încredere și faceți clic pe **Activare** pentru a afișa o listă a aplicațiilor care folosesc o listă de CA-uri de încredere.
7. Selectați aplicația din listă care are nevoie să adauge CA selectată la lista ei de încredere și faceți clic pe **OK**. Apare un mesaj la începutul paginii pentru a indica faptul că aplicațiile pe care le-ați selectat vor avea încredere în CA și în certificatele pe care le emite.

Acum puteți să vă configurați aplicația să ceară certificate pentru autentificarea unui client. Urmăriți instrucțiunile furnizate de documentație pentru aplicația dumneavoastră.

Scenariu: Folosirea certificatelor pentru autentificări interne

Acest scenariu descrie cum să folosiți certificatele ca un mecanism de autentificare pentru a proteja și restricționa care resurse și aplicații pot fi accesate din servere interne.

Situație

Sunteți administrator de rețea pentru o companie (MyCo, Inc.) al cărei departament de resurse umane este preocupat cu probleme precum chestiuni legale și securitatea înregistrărilor. Angajații companiei au cerut să poată accesa online informațiile despre beneficiile lor personale și sănătate. Compania a răspuns la această cerere prin crearea unui sit Web intern pentru a furniza aceste informații angajaților. Sunteți responsabil pentru administrarea acestui sit Web intern, care rulează pe IBM HTTP Server for i5/OS (motorizat de Apache).

Deoarece angajații sunt situați în două birouri separate geografic și unii angajați călătoresc frecvent, dumneavoastră sunteți preocupat de păstrarea acestor informații private la transportul lor prin Internet. De asemenea, autentificați suplimentar utilizatorii prin intermediul unui nume utilizator și parolă pentru a limita accesul la datele companiei. Din cauza naturii sensibile și private a acestor date, realizați 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 și chiar fura parole.

După cercetare, decideți că folosirea certificatelor digitale vă poate furniza securitatea de care aveți nevoie. Folosirea certificatelor vă permite să folosiți SSL (Secure Sockets Layer) pentru a proteja transmisia datelor. În plus, puteți folosi certificate în locul parolelor pentru autentificarea mai sigură a utilizatorilor și pentru limitarea informațiilor despre resurse umane pe care le pot accesa ei.

Ca urmare, decideți să setați un CA local și emiteți certificate pentru toți angajații și să asociați certificatele tuturor angajaților cu iSeries profilurile de utilizator. Acest tip de implementare a certificatelor private vă permite să controlați mai strâns accesul la date sensibile, precum și să controlați securitatea datelor prin folosirea SSL. În ultimă instanță, prin emiterea de către dumneavoastră a certificatelor, măriți probabilitatea ca datele să rămână sigure și 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 informațiile transmise între server și client sunt protejate și private.
- Folosirea de certificate digitale pentru autentificarea clienților furnizează o metodă mai sigură de identificare a utilizatorilor autorizați.
- Folosirea certificatelor digitale *publice* pentru a autentifica utilizatori la aplicațiile și datele dumneavoastră este o alegere practică pentru aceste condiții sau unele similare:
 - Necesități un grad înalt de securitate, în special în ceea ce privește autentificarea utilizatorilor.
 - Aveți încredere în persoanele către care acordați (lansați) certificate.
 - Utilizatorii dumneavoastră au deja profiluri de utilizator iSeries care le controlează accesul la aplicații și date.
 - Doriți să operați asupra propriului Certificate Authority (CA).
- Folosirea certificatelor private pentru autentificarea client vă permite să asociați mai ușor certificatul cu profilul de utilizator autorizat iSeries. 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 și poate să ruleze sub acel profil utilizator sau să realizeze acțiuni pentru a acel utilizator pe baza informațiile din profilul utilizator.

Obiective

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

Obiectivele acestui scenariu sunt următoarele:

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

Detalii

Următoarea figură ilustrează configurația rețelei pentru acest scenariu:

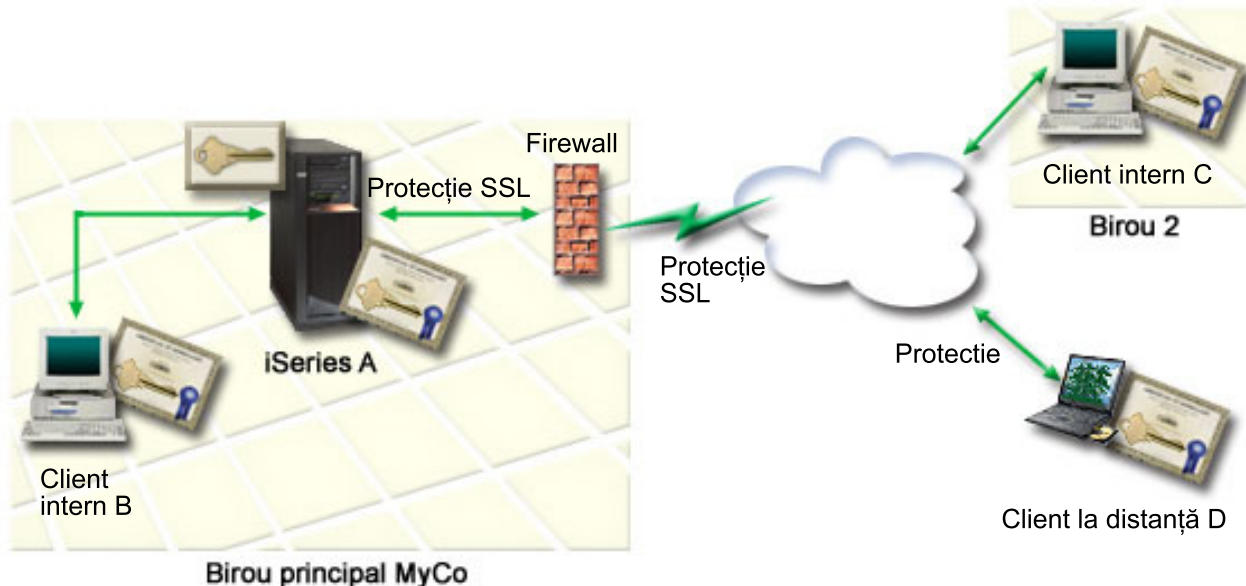


Figura ilustrează următoarele informații despre situația pentru acest scenariu:

Serverul public al companiei iSeries A

- iSeries A este serverul care găzduiește aplicația companiei de calculare a ratei.
- iSeries A folosește i5/OS Versiunea 5 Ediția 4 (V5R4).
- iSeries Pe serverul A sunt instalate și configurate Digital Certificate Manager (i5/OS opțiunea 34) și IBM HTTP Server for i5/OS (5722–DG1).
- iSeries A rulează aplicația de calculare a ratei, care este configurată în așa fel încât:
 - Necesită modul SSL.
 - Folosește un certificat public de la un CA binecunoscut pentru a se autentifica pe sine pentru a inițiază o sesiune SSL.
 - Necesită autentificarea utilizatorului prin nume utilizator și parolă.
- iSeries A își prezintă certificatul pentru a inițiază o sesiune SSL când clienții B și C accesează aplicația de calculare a ratei.
- După inițializarea sesiunii SSL, iSeries A cere clienților B și C să furnizeze un nume de utilizator și o parolă valide înainte de a permite accesul la aplicația de calculare a ratei.

Sistemele client agent – Client B și Client C

- Clienții B și C sunt agenți independenți care accesează aplicația de calcul a ratei.
- Software-ul client al clienților B și C are o copie instalată a certificatului CA binecunoscut care a emis certificatul aplicației.
- Clienții B și C accesează aplicația de calculare a ratei de pe iSeries A, care își prezintă certificatul către software-ul de client pentru autentificarea identității sale și inițierea unei sesiuni SSL.
- Software-ul client de pe Clientul B și C este configurat să accepte certificatul de la iSeries A pentru inițializarea unei sesiuni SSL.
- După ce începe sesiunea SSL, clienții B și C trebuie să furnizeze un nume de utilizator și o parolă valide pentru ca iSeries A să le acorde acces la aplicație.

Cerințele preliminare și presupuneri

Acest scenariu depinde de următoarele cerințe preliminare și supoziții:

- IBM HTTP Server for i5/OS (motorizat de Apache) folosește aplicații de resursele umane pe iSeries A. Acest scenariu nu furnizează instrucțiuni specifice pentru configurare serverului HTTP să folosească SSL. Acest scenariu furnizează instrucțiuni pentru configurarea și gestionarea certificatelor care sunt necesare pentru ca orice aplicație să folosească SSL.
- Serverul HTTP poate avea capacitatea de a cere certificate pentru autentificarea unui client. Acest scenariu furnizează instrucțiuni despre folosirea DCM (Digital Certificate Manager) pentru a configura cerințele de gestionare certificat pentru acest scenariu. Totuși, acest scenariu nu furnizează anumiți pași de configurare pentru configurarea autentificării unui client prin certificate pentru Serverul HTTP.
- Serverul HTTP de resurse umane de pe iSeries A folosește deja autentificarea prin parolă.
- iSeries A îndeplinește cerințele pentru instalarea și folosirea DCM (Digital Certificate Manager).
- Nimeni nu a configurat sau folosit anterior DCM pe iSeries A.
- Oricine folosește DCM pentru a realiza task-urile din acest scenariu trebuie să aibă autorizările speciale *SECADM și *ALLOBJ pentru profilurile lor de utilizator.
- Pe iSeries A nu este instalat IBM Cryptographic Coprocessor.

Task-urile de configurare

Finalizarea foilor de lucru pentru planificare

Următoarele work sheet-uri demonstrează informațiile pe care trebuie să le adunați și deciziile pe care este nevoie să le faceți pentru a pregăti implementarea certificatelor digitale pe care o descrie acest scenariu. Pentru a asigura o implementare cu succes, este nevoie să fiți capabil să răspundeți **Da** la toate articolele cerințelor preliminare și aveți nevoie să aveți adunate toate informațiile cerute înainte să realizați orice task de configurare.

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

Foaie de lucru cerințe preliminare	Răspunsuri
i5/OS al dumneavoastră este V5R4 (5722-SS1)?	Da
Este instalată pe sistemul dumneavoastră opțiunea 34 a i5/OS?	Da
Este instalat IBM HTTP Server for i5/OS (5722-DG1) pe sistemul dumneavoastră și este pornită instanța Admin a serverului?	Da
Este configurat TCP pentru sistemul dumneavoastră astfel încât să puteți folosi un browser Web și instanța serverului administrativ server HTTP pentru a accesa DCM?	Da
Aveți autorizările speciale *SECADM și *ALLOBJ?	Da

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

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

Foaie de lucru de planificare pentru Serverul iSeries A	Răspunsuri
Veți opera propriul dumneavoastră CA local sau veți obține certificate pentru aplicația dumneavoastră de la un CA public?	Creați CA-ul local pentru a emite certificate
Serverul iSeries A găzduiește aplicația pe care vreți să o activați pentru SSL?	Da

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

Foaie de lucru de planificare pentru Serverul iSeries A	Răspunsuri
<p>Ce informații de nume distinctiv veți folosi pentru CA-ul local?</p> <ul style="list-style-type: none"> • Dimensiune cheie: determină puterea cheilor criptografice pentru certificat. • Nume CA: identifică CA-ul și devine numele comun pentru certificatul CA și DN-ul emitentului pentru certificatele pe care le emite CA. • Unitate de organizare: identifică secțiunea sau zona de organizare pentru aplicația care va folosi acest certificat. • Nume organizație: identifică compania dumneavoastră sau secțiunea divizionară pentru aplicația care va folosi acest certificat. • Localitate sau oraș: identifică orașul sau o desemnare a localității pentru organizația dumneavoastră. • Stat sau provincie: identifică statul sau provincia în care veți folosi acest certificat. • Țară sau regiune: identifică, cu o desemnare din două litere, țara sau regiunea în care veți folosi acest certificat. • Perioadă de validitate a Autorității de certificare: specifică numărul de zile pentru care certificatul Autorității de certificare este valid 	<p>Mărime cheie: 1024 Nume CA (Certificate Authority): Myco_CA@myco.com Unitate de organizare: Rate dept Nume organizație: myco Localitate sau oraș: Any_city Stat sau provincie: Any Țară sau regiune: ZZ Perioada de validitate a CA: 1095</p>
<p>Vreți să setați datele politicii pentru a permite CA-ului local să emită certificate de utilizator pentru autentificarea clientului?</p>	<p>Da</p>
<p>Ce informații despre numele distinctiv veți folosi pentru certificatul de server pe care îl emite CA-ul local?</p> <ul style="list-style-type: none"> • Dimensiune cheie: determină puterea cheilor criptografice pentru certificat. • Etichetă certificat: identifică certificatul cu un șir unic de caractere. • Nume comun: identifică proprietarul certificatului, cum ar fi o persoană, entitate sau aplicație; parte a DN-ului subiect pentru certificat. • Unitate de organizare: identifică secțiunea sau zona de organizare pentru aplicația care va folosi acest certificat. • Nume organizație: identifică compania dumneavoastră sau secțiunea divizionară pentru aplicația care va folosi acest certificat. • Localitate sau oraș: identifică orașul sau o desemnare a localității pentru organizația dumneavoastră. • Stat sau provincie: identifică statul sau provincia în care veți folosi acest certificat. • Țară sau regiune: identifică, cu o desemnare din două litere, țara sau regiunea în care veți folosi acest certificat. 	<p>Mărime cheie: 1024 Etichetă certificat: Myco_public_cert Nume comun: myco_rate_server@myco.com Unitate de organizare: Rate dept Nume organizație: myco Localitate sau oraș: Any_city Provincie sau oraș: Any Țară sau regiune: ZZ</p>
<p>Care este ID-ul aplicației DCM pentru aplicația pe care vreți să o configurați să folosească SSL?</p>	<p>mcyo_agent_rate_app</p>
<p>Veți configura aplicația cu SSL aplicat să folosească certificate pentru autentificarea client? Dacă da, care CA-uri vreți să le adăugați la lista de CA-uri de încredere a aplicației?</p>	<p>Da Myco_CA@myco.com</p>

Configurarea serverului HTTP de resurse umane pentru a folosi SSL

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

Pentru a configura serverul să folosească SSL, urmați acești pași:

1. Porniți interfața Administrare server HTTP.
2. Pentru a lucra cu un server HTTP specific, selectați aceste fișe de pagini **Gestionare** → **Toate serverele** → **Toate serverele HTTP** pentru a vedea o listă a tuturor serverelor HTTP configurate.
3. Selectați serverul corespunzător din listă și faceți clic pe **Gestionare detalii**.
4. În cadrul de navigație, selectați **Securitate**.
5. Selectați câmpul **SSL cu autentificare certificat** din formular.
6. În câmpul **SSL**, selectați **Activat**.
7. În câmpul **Nume aplicație certificat server**, specificați un ID de aplicație prin care este cunoscută această instanță server. Sau, puteți selecta unul din listă. Acest ID aplicație este în forma **QIBM_HTTP_SERVER_[nume_server]**, de exemplu, **QIBM_HTTP_SERVER_MYCOTEST**. **Notă:** Memorați acest ID aplicație. Va fi nevoie să-l selectați din nou în DCM.

uteți afla mai multe despre configurația generală necesară pentru serverul dumneavoastră HTTP la folosirea SSL în subiectul Informații HTTP Server pentru iSeries, în special într-un exemplu numit Scenariu: JKL activează protecția SSL (Secure Sockets Layer) pe serverul lor HTTP (monitorizat de Apache). Acest scenariu furnizează toți pașii task-urilor pentru crearea unei gazde virtuale și configurarea ei pentru folosirea SSL, inclusiv următoarele task-uri:

1. Stare gazdă virtuală bazată pe nume.
2. Setare directivă Ascultare pentru gazdă virtuală.
3. Setare directoare gazdă virtuală.
4. Setare protecție parolă via autentificare de bază.
5. Activare SSL pentru gazda virtuală

Pentru informații suplimentare despre configurarea atât a versiunilor curente, cât și a celor viitoare ale serverului HTTP pentru iSeries, vedeți HTTP Server pentru iSeries.

Când terminați configurarea pentru ca serverul HTTP să folosească SSL, puteți utiliza DCM pentru a configura suportul de certificat de care aveți nevoie pentru SSL și autentificare client.

Crearea și lucrul cu un CA local

După ce ați configurat Serverul HTTP de resurse umane să folosească SSL, trebuie să configurați un certificat pe care să îl folosească serverul pentru a iniția SSL. În funcție de obiectivele pentru acest scenariu, ați ales să creați și să operați un CA local să emită un certificat către server.

Când folosiți DCM pentru a crea un CA local, sunteți îndrumat printr-un proces care se asigură că configurați tot ceea ce este necesar pentru a activa SSL pentru aplicația dumneavoastră. Asta include alocarea certificatului pe care îl emite CA-ul local pentru aplicația dumneavoastră de server Web. De asemenea, adăugați CA-ul local la lista de CA-uri de încredere a aplicației de server Web. Având un CA local în lista de încredere a aplicației asigură că aplicația poate recunoaște și autentifica utilizatori care prezintă certificate pe care le emite CA-ul local.

Pentru a folosi DCM pentru a crea și opera un CA local și emite un certificat către aplicația de pe serverul dumneavoastră de resurse umane, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare din DCM, selectați **Crearea unui CA** pentru a se afișa o serie de formulare. Aceste formulare vă îndrumă prin procesul creării unui CA local și completării altor task-uri necesare pentru a începe folosirea certificatelor digitale pentru SSL, semnarea obiectelor și verificarea semnăturii.

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

3. Completați formularele pentru acest task asistat. Când folosiți aceste formulare pentru a realiza toate task-urile de care aveți nevoie pentru a seta un CA local funcțional, parcurgeți pașii următori:
 - a. Furnizați informațiile de identificare pentru CA-ul local.
 - b. Instalați certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaște CA-ul local și să valideze certificatele pe care le emite CA-ul local.
 - c. Alegeți datele politicii pentru CA-ul dumneavoastră local.

Notă: Asigurați-vă că selectați opțiunea care permite CA-ului local să emită certificate de utilizator.

- d. Folosiți noul CA local pentru a emite un certificat server sau client pe care aplicațiile dumneavoastră să îl poată folosi pentru conexiuni SSL.
- e. Selectați aplicațiile care pot folosi certificatul client sau server pentru conexiuni SSL.

Notă: Asigurați-vă că selectați ID-ul aplicației pentru Serverul HTTP de resurse umane al dumneavoastră.

- f. Folosiți noul CA local pentru a emite un certificat de semnare obiect pe care aplicațiile să îl poată folosi pentru a semna digital obiecte. Acest subtask creează depozitul de certificate *OBJECTSIGNING; acesta este depozitul de certificate pe care îl folosiți pentru a gestiona certificate care semnează obiecte.

Notă: Deși acest scenariu nu folosește certificate de semnare obiect, asigurați-vă că realizați acest pas. Dacă anulați la acest moment al task-ului, el se oprește și trebuie să realizați task-uri separate pentru a efectua configurarea certificatului SSL.

- g. Selectați aplicațiile care vor avea încredere în CA-ul local.

Notă: Aveți grijă să selectați ID-ul aplicației pentru serverul dumneavoastră HTTP de resurse umane, de exemplu, QIBM_HTTP_SERVER_MYCOTEST, ca una dintre aplicațiile care au încredere în CA-ul local.

Când terminați configurația certificatului pe care aplicația server Web o cere pentru a folosi SSL, puteți configura serverul Web să necesite certificate pentru autentificarea utilizatorilor.

Configurarea autentificării clientului pentru serverul Web de resurse umane

Trebuie să configurați setările generale de autentificare pentru serverul HTTP când specificați că serverul HTTP necesită certificate pentru autentificare. Configurați aceste setări în același formular de securitate pe care l-ați folosit pentru a configura serverul să folosească SSL (Secure Sockets Layer).

Pentru a configura serverul să necesite certificate pentru autentificarea client, urmați acești pași:

1. Porniți interfața Administrare server HTTP.
2. Folosind browser-ul, mergeți la pagina Task-uri de pe sistemul i5/OS dumneavoastră, la http://numele_sistemului_dvs:2001.
3. Selectați **IBM Web Administration pentru i5/OS**.
4. Pentru a lucra cu un server HTTP specific, selectați aceste fișe de pagini **Gestionare** → **Toate serverele** → **Toate serverele HTTP** pentru a vedea o listă a tuturor serverelor HTTP configurate.
5. Selectați serverul corespunzător din listă și faceți clic pe **Gestionare detalii**.
6. În cadrul de navigație, selectați **Securitate**.
7. Selectați fișa **SSL cu Autentificare certificat** din formular.
8. Selectați **Folosire profil i5/OS al clientului**.
9. În câmpul **Nume sau regiune autentificare**, specificați un nume pentru regiunea de autentificare.
10. Selectați **Activat** pentru câmpul **Procesare cereri folosind autorizarea client** și faceți clic pe **Aplicare**.
11. Selectați fișa **Controlare acces** din formular.

12. Selectați **Toți utilizatorii autentificați (nume utilizator și parolă valide)** și faceți clic pe **Aplicare**.
13. Selectați câmpul **SSL cu autentificare certificat** din formular.
14. Asigurați-vă că **Activat** este valoarea selectată în câmpul **SSL**.
15. În câmpul **Nume aplicație certificat server**, asigurați-vă că este specificată valoarea corectă, de exemplu, **QIBM_HTTP_SERVER_MYCOTEST**.
16. Selectați **Acceptare certificat client dacă este disponibil înainte de a face conexiunea**. Selectați **OK**.

Puteți afla mai multe despre configurația generală necesară pentru serverul dumneavoastră HTTP la folosirea SSL în subiectul Informații HTTP Server pentru iSeries în special într-un exemplu numit Scenariu: JKL activează protecția SSL (Secure Sockets Layer) pe serverul lor HTTP (monitorizat de Apache). Acest scenariu furnizează toți pașii task-ului pentru crearea unei gazde virtuale și configurarea ei să folosească SSL.

Când terminați configurarea autentificării client, puteți să reporniți serverul HTTP în mod SSL și să începeți să protejați securitatea datelor aplicației de resurse umane.

Pornirea serverului Web de resurse umane în mod SSL

S-ar putea să fie nevoie să opriți și să reporniți Serverul dumneavoastră HTTP pentru a asigura că serverul poate să determine că alocarea certificatului există și să îl folosească pentru a iniția sesiuni SSL.

Pentru a opri și reporni serverul HTTP (monitorizat de Apache) urmați acești pași:

1. În Navigator iSeries extindeți serverul dumneavoastră .
2. Expandați **Rețea** → **Servere** → **TCP/IP** → **Administrare HTTP**.
3. Faceți clic pe **Pornire** pentru a porni interfața Administrare server HTTP.
4. Faceți clic pe fișa **Gestionare** pentru a vedea o listă a tuturor serverelor HTTP configurate.
5. Selectați serverul corespunzător din listă și faceți clic pe **Oprire** dacă serverul rulează.
6. Faceți clic pe **Pornire** pentru a reporni serverul. Consultați ajutorul online pentru informații suplimentare despre parametrii de pornire.

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

Informații înrudite

Server HTTP - Privire generală centru de informare

Faceți utilizatorii să instaleze o copie a certificatului CA local în browser

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

Fiecare utilizator (Clienții B, C și D) trebuie să facă acești pași pentru a obține o copie a certificatului CA local:

1. Porniți DCM.
2. În cadrul de navigare, selectați **Instalare certificat CA local pe PC-ul dumneavoastră** pentru a afișa o pagină care vă permite să descărcați certificatul CA local în browser-ul dumneavoastră sau să-l memorați într-un fișier pe sistemul dumneavoastră.
3. Selectați opțiunea de instalare a certificatului. Această opțiune descarcă certificatul CA local ca o rădăcină de încredere în browser-ul dumneavoastră. Asta asigură că browser-ul dumneavoastră poate stabili sesiuni de comunicație sigure cu serverele Web care folosesc un certificat de la acest CA. Browser-ul va afișa o serie de ferestre care vă vor ajuta să terminați instalarea.

4. Apăsați **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, aceștia trebuie să fie capabili să prezinte un certificat corespunzător pentru a se autentifica la server. În consecință, ei trebuie să obțină un certificat de la CA-ul local.

Faceți ca fiecare utilizator să ceară un certificat de la CA-ul local

În pașii anteriori, ați configurat serverul Web de resurse umane să ceară certificate pentru autentificarea utilizatorilor. Acum utilizatorii trebuie să prezinte un certificat valid de la CA-ul local pentru a li se permite să acceseze serverul Web. Fiecare utilizator trebuie să folosească DCM pentru a obține un certificat folosind task-ul **Creare certificat**. Pentru a obține un certificat de la CA-ul local, politica de CA local trebuie să-i permită să emită certificate utilizator.

Fiecare utilizator (Clienții B, C și D) trebuie să urmeze acești pași pentru a obține un certificat:

1. Porniți DCM.
2. În cadrul de navigare, selectați **Crearea certificatelor**.
3. Selectați **Certificate utilizator** pentru tipul certificatului pe care îl creați. Se va afișa un formular în care veți putea introduce informații de identificare pentru certificat.
4. Completați formularul și apăsați **Continuare**.

Notă: Dacă aveți întrebări despre completarea unui anume formular care este în task-ul asistat, selectați 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 și publice pentru certificate. Browser-ul poate afișa mai multe ferestre pentru a vă ghida prin acest proces. Urmați instrucțiunile browser-ului pentru aceste task-uri. După ce browser-ul generează cheile, se va afișa o pagină de confirmare care va indica faptul că DCM-ul a creat certificatele.
6. Instalați noul certificat în browser-ul dumneavoastră. Browser-ul poate afișa mai multe ferestre pentru a vă ghida prin acest proces. Urmați instrucțiunile date de browser pentru a termina acest task.
7. Apăsați **OK** pentru a termina task-ul.

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

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

Plan pentru DCM

Folosiți aceste informații pentru a vă ajuta să decideți cum și când ați putea utiliza certificate digitale pentru a vă îndeplini țelurile de securitate. Folosiți aceste informații pentru a afla despre orice cerințe preliminare de care aveți nevoie pentru instalare, ca și de alte cerințe de care trebuie să țineți cont înainte de folosirea DCM.

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

Pentru a afla mai multe despre cum să plănuieți utilizarea DCM și pentru a înțelege mai bine cum pot fi incluse certificatele digitale în politica dumneavoastră de securitate, revedeți aceste subiecte:

Cerințe de setare DCM

Folosiți acest subiect pentru a vă asigura că aveți opțiunile necesare pentru a folosi DCM (Digital Certificate Manager).

DCM (Digital Certificate Manager) este o caracteristică gratuită iSeries care vă permite să gestionați central certificatele digitale pentru aplicațiile dumneavoastră. Pentru a folosi cu succes DCM, aveți grijă să faceți următoarele:

- Instalați opțiunea 34 din i5/OS. Aceasta este facilitatea DCM bazată pe browser.
- Instalați serverul IBM HTTP Server for i5/OS (5722–DG1) și porniți instanța server Administrativă.
- Asigurați-vă că TCP este configurat pentru sistemul dumneavoastră astfel încât să puteți folosi un browser Web și instanța server Server HTTP administrativ pentru a accesa DCM.

Notă: Nu veți putea crea certificate decât dacă ați instalat toate produsele necesare. Dacă un produs cerut nu este instalat, DCM va afișa un mesaj de eroare spunându-vă să instalați componenta care lipsește.

Considerentele despre salvarea de rezervă și recuperarea datelor DCM

Folosiți aceste informații pentru a afla cum să asigurați că datele DCM importante sunt adăugate la salvarea de rezervă și planul de recuperare pentru sistemul dumneavoastră.

Parolele bazei de date de chei codate pe care le folosiți pentru a accesa depozitele de certificate din DCM (Digital Certificate Manager) sunt memorate, sau *ascunse*, într-un fișier special de securitate de pe sistem. Când folosiți DCM pentru a crea un depozit de certificate pe sistemul dumneavoastră, DCM păstrează automat parola pentru dumneavoastră. Totuși, trebuie să vă asigurați manual că DCM păstrează parole de depozite de certificate în anumite circumstanțe.

Un exemplu este situația în care folosiți DCM pentru a crea un certificat pentru alt server **iSeries** și alegeți să utilizați fișierele de certificat de pe sistemul destinație pentru a crea un nou depozit de certificate. În această situație, trebuie să deschideți noul depozit de certificate creat și să utilizați task-ul **Modificare parolă** pentru a modifica parola pentru depozitul de certificate de pe sistemul destinație, care asigură faptul că DCM păstrează noua parolă. Dacă depozitul de certificate este alt depozit de certificate sistem, ar trebui de asemenea să specificați că vreți să folosiți opțiunea **Logare automată** când modificați parola. Pentru a afla mai multe despre folosirea DCM pentru a crea certificate pentru alte iSeries sisteme, vedeți Folosirea unui CA local pentru a emite certificate pentru alte iSeries sisteme.

Suplimentar, trebuie să specificați opțiunea **Logare automată** când modificați sau resetați parola pentru alt depozit de certificate sistem.

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

- Utilizați comanda SAV (Save - Salvare) pentru a salva toate fișierele .KDB și .RDB. Fiecare depozit de certificate DCM este compus din două fișiere, unul cu extensia .KDB și unul cu extensia .RDB.
- Folosiți comanda SAVSYS (Save system - Salvare sistem) și SAVSECDATA (save security data - Salvare date securitate) pentru a salva fișierul special de securitate care conține parolele bazei de date de chei pentru acces la depozitul de certificate. Pentru a restaura fișierul de securitate parole DCM, folosiți comanda RSTUSRPRF (restore user profiles - restaurare profiluri utilizator) și specificați *ALL pentru opțiunea profil utilizator (USRPRF).

O alt considerent de recuperare se referă la utilizarea operației SAVSECDATA și la posibilitatea ca parolele curente ale depozitivului de certificate să devină nesincronizate cu parolele din fișierul de securitate parolă DCM salvat. Dacă modificați parole pentru un depozit de certificate după ce faceți o operație SAVSECDTA, dar înainte să restaurați detele din acea operație, parola curentă a depozitivului de certificate nu va fi sincronizată cu cea din fișierul restaurat.

Pentru a evita această situație, trebuie să folosiți task-ul **Modificare parolă** (sub **Gestionare depozit certificate** în cadrul de navigație) în DCM pentru a modifica parolele depozitivului de certificate după ce restaurați datele de la o operație SAVSECDTA pentru a vă asigura că primiți parolele înapoi sincronizate. Totuși, în această situație nu folosiți butonul **Resetare parolă** care este afișat când selectați un depozit de certificate pentru deschidere. Când încercați să resetați parola, DCM încearcă să extragă parola păstrată. Dacă parola păstrată nu este sincronizată cu parola curentă, operația de resetare va eșua. Dacă nu modificați parolele depozitivului de certificate des, ar putea să considerați să faceți o SAVSECDTA de fiecare dată când modificați aceste parole pentru a vă asigura că mereu aveți versiunea păstrată cea mai curentă a parolelor salvate în caz că veți avea nevoie vreodată să restaurați aceste date.

Operații înrudite

“Utilizarea CA local pentru a emite certificate pentru alte sisteme iSeries” la pagina 54

Aflați cum se folosește un CA local privat de pe un sistem pentru a emite certificate folosite pe alte sisteme. iSeries.

Tipuri de certificate digitale

Folosiți aceste informații pentru a învăța diferitele tipuri de certificate pentru administrarea cărora puteți folosi DCM.

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

Certificate ale Autorității de Certificare (CA - Certificate Authority)

Un certificat CA este o acreditare digitală care validează identitatea Autorității de certificare care este proprietara certificatului. Certificatul CA conține informații de identificare despre Autoritatea de certificare, precum și cheia publică a acesteia. Cheia publică a certificatului CA poate fi utilizată de alții pentru a se verifica autenticitatea certificatelor pe care le emite și 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 local pe care îl creați și cu care operați cu Digital Certificate Manager este o entitate independentă. Cheia publică a certificatului CA poate fi utilizată de alții pentru a se verifica autenticitatea certificatelor pe care le emite și le semnează CA-ul. Pentru a folosi un certificat pentru SSL, semnarea obiectelor sau verificarea semnăturilor obiectelor, trebuie să aveți o copie a certificatului CA-ului emitent.

Certificate server sau client

Un certificat client sau server este o acreditare digitală care identifică aplicația server sau client care folosește certificatul pentru comunicații sigure. Certificatele server sau client conțin informații de identificare despre organizația proprietară a aplicației, cum ar fi numele distinct al sistemului. Certificatul conține de asemenea cheia publică a sistemului. Un server trebuie să aibă un certificat digital pentru a folosi SSL (Secure Sockets Layer) pentru comunicații sigure. Aplicațiile care suportă certificatele digitale pot examina certificatul server-ului pentru a verifica identitatea acestuia când clienții accesează serverul. Aplicația poate folosi mai apoi autentificarea certificatului ca bază pentru inițializarea unei sesiuni criptate SSL între client și server. Puteți 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, furnizați un mijloc prin care puteți verifica atât integritatea obiectului cât și originea sau proprietarul obiectului. Puteți folosi certificatul pentru a semna o varietate de obiecte, inclusiv majoritatea obiectelor din sistemul de fișiere integrat și obiectele *CMD. Puteți găsi o listă completă a obiectelor ce pot fi semnate în capitolul despre Semnarea obiectelor și verificarea semnăturilor. Atunci când se folosește 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. Puteți 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. Folosiți cheia publică a certificatului pentru verificarea semnăturii pentru a autentifica semnătura digitală creată cu un certificat pentru semnarea obiectelor. Verificarea semnăturii vă permite să determinați originea obiectului și dacă a fost modificat de când a fost semnat. Puteți 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 deține certificatul. În prezent, multe aplicații furnizează un suport care vă permite să folosiți certificatele pentru a autentifica utilizatori pentru resurse în loc de a se folosi nume de utilizatori și parole. DCM (Digital Certificate Manager) asociază automat profilului de utilizator certificatele de utilizator pe care le emite CA-ul dumneavoastră privat iSeries. De asemenea, puteți folosi DCM pentru a asocia profilului de utilizator certificatele pe care le emite alt CA iSeries.

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

Notă: Dacă pe server este instalat IBM Cryptographic Coprocessor, puteți alege alte opțiuni de memorare a cheii private pentru certificate (cu excepția certificatelor de semnare pentru obiecte). Puteți alege să memorați cheia privată chiar pe coprocesorul criptografic. Sau, puteți folosi coprocesorul criptografic pentru a cripta cheia

privată și să o memorați într-un fișier cheie special în locul unui depozit de certificate. Totuși, certificatele utilizator și cheile lor private sunt depozitate în sistemul utilizatorului, sau în software-ul browser-ului sau într-un fișier care să fie folosit de alte pachete software client.

Concepte înrudite

“SSL (Secure Sockets Layer)” la pagina 9

Original creat de Netscape, SSL (Secure Sockets Layer) este standardul industrial pentru criptarea sesiunilor între clienți și servere.

“Depozite de certificate” la pagina 7

Un depozit de certificate este un fișier bază de date cheie special pe care DCM îl folosește pentru a memora certificatele digitale.

Certificate publice contra certificate private

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

Puteți folosi certificate de la un CA publică sau puteți crea și opera un CA privat pentru a emite certificate. Alegerea modului în care obțineți certificatele depinde de modul în care intenționați să le utilizați. O dată ce vă decideți să folosiți certificate, trebuie să alegeți tipul implementării certificatelor care se potrivește cel mai bine nevoilor dumneavoastră de securitate. Opțiunile pe care le aveți pentru obținerea certificatelor includ:

- Obținerea certificatelor de la o Autoritate de certificare (CA) publică.
- Operarea unui CA local pentru a emite certificate private pentru utilizatorii și aplicațiile dumneavoastră.
- Utilizarea unei combinații de certificate de la CA-uri Internet publice și CA-urile dumneavoastră locale.

Alegerea uneia dintre aceste opțiuni de implementare depinde de un număr de factori, unul dintre cei mai importanți fiind mediul în care sunt folosite certificatele. Mai jos sunt niște informații care vă vor ajuta să determinați mai bine care opțiune de implementare este potrivită pentru cerințele dumneavoastră de afaceri și de securitate.

Folosirea certificatelor publice

CA-urile publice Internet lansează certificate către oricine plătește taxa corespunzătoare. Însă un CA din Internet necesită încă o dovadă a identității înainte să poată lansa un certificat. Acest nivel al dovezii variază, în funcție de politica de identificare a CA. Trebuie să evaluați dacă stringența politicii de identificare a CA se potrivește nevoilor dumneavoastră de securitate înainte de a decide să obțineți 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 obținere a certificatelor de la un asemenea CA PKIX este mai evoluat, certificatele emise de CA oferă o mai bună asigurare a securității accesului la aplicații prin utilizatori specifici. Digital Certificate Manager (DCM) vă permite să folosiți și să gestionați certificatele provenite de la CA-uri PKIX care folosesc aceste noi standarde pentru certificate.

Trebuie să considerați de asemenea costul asociat cu folosirea unui CA public pentru a emite certificate. Dacă aveți nevoie de certificate pentru un număr limitat de aplicații client sau server și clienți, costul s-ar putea să nu fie un factor important pentru dumneavoastră. Totuși, costul poate fi foarte important dacă aveți un număr mare de utilizatori *privați* care au nevoie de certificate publice pentru autentificare client. În acest caz, trebuie să considerați de asemenea efortul administrativ și de programare necesar pentru a configura aplicațiile 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 și resurse, deoarece multe aplicații server, client și de utilizator sunt configurate pentru a recunoaște majoritatea dintre CA-uri publice binecunoscute. De asemenea, alte companii și utilizatori pot recunoaște și avea încredere în certificatele pe care le emite un CA public binecunoscut mai mult decât în cele emise de CA-ul dumneavoastră local.

Folosirea certificatelor private

Dacă vă creați propriul CA local, puteți emite certificate către sisteme și utilizatori într-un domeniu mult mai limitat, precum în interiorul companiei sau organizației dumneavoastră. Crearea și menținerea CA-ului dumneavoastră local vă permite să emiteți certificate doar acelor utilizatori care sunt membri de încredere ai grupului dumneavoastră. Aceasta oferă o securitate mai bună, deoarece puteți controla mai strâns cine are acces la certificate și de aceea cine are acces la resursele dumneavoastră. Un potențial dezavantaj al menținerii propriei CA locale este cantitatea de timp și resurse pe care trebuie să le investiți. Oricum, Digital Certificate Manager (DCM) face acest proces mai ușor pentru dumneavoastră.

Când folosiți un CA local pentru a emite certificate utilizatorilor pentru autentificarea client, trebuie să decideți unde vreți să memorați certificatele utilizator. Când utilizatorii obțin certificatele lor de la CA-ul local prin intermediul DCM, acestea sunt memorate cu un profil utilizator în mod implicit. Totuși, puteți configura DCM să lucreze cu EIM (Enterprise Identity Mapping) astfel ca certificatele lor să fie memorate într-o locație LDAP (Lightweight Directory Access Protocol) în schimb. Dacă preferați să nu aveți certificatele utilizator asociate sau memorate cu un profil utilizator de nici un fel, puteți folosi API-uri pentru a emite programabil certificate către utilizatori non-iSeries.

Notă: Nu contează ce CA folosiți pentru a emite certificate, administratorul de sistem controlează în care CA-uri vor avea încredere aplicațiile 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 conține copii ale certificatelor CA publice binecunoscute. Totuși, 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 obțineți și importați o copie a certificatului CA. Certificatul CA trebuie să fie în formatul corect de fișier și trebuie să-l adăugați la depozitul de certificate DCM.

Ați putea găsi folositor să treceți în revistă unele scenarii comune de folosire a certificatelor pentru a vă ajuta să alegeți dacă folosirea de certificate publice sau private se potrivește cel mai bine cu afacerea dumneavoastră și cu necesitățile de securitate.

Task-uri înrudite

După ce decideți cum doriți să folosiți certificatele și ce tip să folosiți, revedeți aceste proceduri pentru a afla mai multe despre cum să folosiți DCM (Digital Certificate Manager) pentru a vă pune planul în acțiune:

- Crearea și operarea unui CA privat descrie task-urile pe care trebuie să le realizați dacă alegeți să operați un CA local pentru a trimite certificate.
- Gestionarea certificatelor de la un CA public din Internet descrie task-urile pe care trebuie să le efectuați pentru a folosi certificatele de la un CA public binecunoscut, incluzând CA PKIX.
- Folosirea unui CA local pe alte iSeries servere prezintă task-urile pe care trebuie să le realizați dacă vreți să folosiți certificate de la un CA local privat pe mai multe sisteme.

Concepte înrudite

“Gestionarea certificatelor de pe un CA Internet public” la pagina 46

Folosiți această informație pentru a gestiona certificate provenite de la un CA public din Internet, trebuie să creați mai întâi un depozit de certificate.

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

“Setarea certificatelor pentru prima dată” la pagina 38

Învățați cum să faceți primii pași în administrarea certificatelor de la un CA (Certificate Authority - Autoritate de certificare) din Internet sau cum să creați și să operați un CA local privat pentru a emite certificate..

“Certificatele digitale pentru semnarea obiectelor” la pagina 35

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticității sale.

Operații înrudite

“CertIFICATE digitale și EIM (Enterprise Identity Mapping)” la pagina 33

Aceasta permite sistemelor de operare și aplicațiilor să folosească certificatul ca sursă a unei operații de căutare EIM pentru a mapa de la certificat la o identitate utilizator destinație asociată cu același identificator EIM.

“Crearea unui certificat utilizator” la pagina 41

Folosiți aceste informații pentru a afla cum pot utilizatorii să folosească CA-ul local pentru a emite un certificat pentru autentificarea clientului.

“Crearea și lucrul cu un CA local” la pagina 39

Folosiți această informație pentru a învăța cum să creați și operați CA pentru a emite certificate private pentru aplicații.

“Utilizarea CA local pentru a emite certificate pentru alte sisteme iSeries” la pagina 54

Aflați cum se folosește un CA local privat de pe un sistem pentru a emite certificate folosite pe alte sisteme. iSeries.

Referințe înrudite

“Folosirea API-urilor pentru a emite prin programe certificate către utilizatorii non-iSeries” la pagina 44

Folosiți aceste informații pentru a emite cerțificate către utilizatorii fără a asocia certificatul cu un profil de utilizator iSeries.

Certificatele digitale pentru comunicațiile sigure SSL

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru ca aplicațiile să poată stabili sesiuni de comunicare sigure.

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

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

Aplicațiile client și server lucrează împreună pentru a asigura securizarea datelor după cum urmează.

1. Aplicația server prezintă certificatul către aplicația client (utilizator) ca dovadă a identității server-ului.
2. Aplicația client verifică identitatea serverului cu o copie a certificatului emis de Autoritatea de certificare (CA). (Aplicația client trebuie să aibă acces la copia stocată local a certificatului CA relevant.)
3. Aplicațiile server și client se pun de acord cu o cheie simetrică pentru criptare și o folosesc pentru a cripta sesiunea de comunicare.
4. Opțional, server-ul poate cere client-ului să furnizeze o dovadă a identității înainte de a permite accesul la resursele cerute. Pentru a se folosi certificate ca dovadă a identității, aplicațiile care comunică trebuie să suporte folosirea certificatelor pentru autentificarea utilizatorilor.

SSL folosește algoritmi cu cheie asimetrică (cheie publică) în timpul procesării SSL inițiale pentru a negocia o cheie simetrică care este folosită ulterior pentru criptarea și decriptarea datelor aplicației pentru o sesiune SSL particulară. Aceasta înseamnă că serverul dumneavoastră și clientul folosesc chei-sesiune diferite, ce expiră automat după un timp stabilit anterior, pentru fiecare conexiune. Este un fenomen neobișnuit ca cineva să intercepteze și 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”

Folosiți aceste informații pentru a afla despre cum să folosiți certificate pentru a furniza un mijloc pentru o autentificare mai puternică a utilizatorilor care accesează resurse de pe un server iSeries.

Certificatele digitale pentru autentificarea utilizatorului

Folosiți aceste informații pentru a afla despre cum să folosiți certificate pentru a furniza un mijloc pentru o autentificare mai puternică a utilizatorilor care accesează resurse de pe un server iSeries.

Tradițional, utilizatorii primesc acces la resurse de la o aplicație sau sistem pe baza numelui de utilizator și a parolei. Se poate crește securitatea sistemului prin utilizarea certificatelor digitale (în locul numelor de utilizatori și a parolelor)

pentru a autentifica și autoriza sesiunile dintre mai multe aplicații server utilizatori. De asemenea, puteți folosi DCM (Digital Certificate Manager) pentru a asocia certificatul unui utilizator cu profilul său de utilizator sau cu altă identitate de utilizator iSeries. Apoi certificatul are aceleași autorizări și permisiuni ca și identitatea sau profilul de utilizator asociat. Alternativ, puteți folosi API-uri pentru a utiliza autoritatea de certificare locală pentru a emite certificate utilizatorilor non-iSeries. Aceste API-uri vă dau posibilitatea să emiteți certificate private pentru utilizatori când nu vreți ca aceștia să aibă un profil de utilizator sau altă identitate de utilizator internă iSeries.

Un certificat digital se comportă ca un credential electronic și verifică dacă persoana ce se prezintă este cea care se pretinde a fi. Astfel, un certificat este similar unui pașaport. Ambele stabilesc o identitate individuală, și ambele conțin un unic număr în scopul identificării și au autorități de emiter care pot recunoaște dacă este autentic credentialul. În cazul unui certificat, funcțiile unei Autorități de certificare (CA) fiind a treia parte, de încredere, care emite certificatul și îl verifică dacă este un credential autentic.

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

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

- Server Telnet
- IBM HTTP Server for i5/OS (monitorizat de Apache)
- Server director IBM
- iSeries Access pentru Windows (inclusiv Navigatorul Navigator iSeries)
- Server FTP

De-a lungul timpului, aplicații adiționale pot furniza suport pentru certificate de autentificare a clienților; citiți documentația pentru aplicații 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 își înregistreze numele de utilizator și parola pentru a se asigura că le țin minte. Ca rezultat, utilizatori neautorizați pot obține mai ușor nume și parole de la utilizatori autorizați. Deoarece depozitele de certificate sunt depozitate într-un fișier sau altă locație electronică, aplicațiile client (mai repede decât cele utilizator) manevrează accesul și prezentarea certificatului pentru autentificare. Acest lucru asigură faptul că este mai puțin probabil ca utilizatorii să împartă certificate cu utilizatori neautorizați, cu excepția cazului în care utilizatorii neautorizați 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 conține 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 și decriptare. Ceilalți 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 comparație cu parolele.
- Cheile certificatelor digitale oferă câteva moduri potențiale de utilizare pe care nu le oferă parolele, cum ar fi integritatea datelor și intimitatea. Puteți folosi certificatele și cheile lor asociate pentru a:
 - Asigura integritatea datelor prin detectarea modificărilor aduse lor.
 - Dovedi faptul că o anume acțiune a fost realizată. Acest proces este numit nerepudiare.
 - Asigura intimitatea transferurilor de date folosind SSL (Secure Sockets Layer) pentru a cripta sesiuni de comunicare.

Pentru a învăța mai multe despre configurarea aplicațiilor iSeries server pentru folosirea certificatelor pentru autentificarea client în timpul unei sesiuni SSL, vedeți subiectul SSL (Secure Sockets Layer) din Centrul de informare Centrul de informare iSeries.

Concepte înrudite

“CertIFICATELE digitale pentru comunicațiile sigure SSL” la pagina 31

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru ca aplicațiile să poată stabili sesiuni de comunicare sigure.


Referințe înrudite

“Folosirea API-urilor pentru a emite prin programe certificate către utilizatorii non-iSeries” la pagina 44

Folosiți aceste informații pentru a emite certificate către utilizatorii fără a asocia certificatul cu un profil de utilizator iSeries.

Certificate digitale și EIM (Enterprise Identity Mapping)

Aceasta permite sistemelor de operare și aplicațiilor să folosească certificatul ca sursă a unei operații de căutare EIM pentru a mapa de la certificat la o identitate utilizator destinație asociată cu același identificator EIM.

EIM este o tehnologie  care vă permite să gestionați identitățile de utilizator în întreprinderea dumneavoastră, inclusiv profilurile de utilizator și certificate utilizator. Un nume utilizator și parolă sunt cea mai comună formă de identitate utilizator; certificatele sunt altă formă de identitate utilizator. Unele aplicații sunt configurate să permită utilizatorilor să fie autentificați prin intermediul unui certificat utilizator mai degrabă decât un nume utilizator și parolă.

Puteți folosi EIM pentru a crea mapări între identități utilizator, care permite unui utilizator să se autentifice cu o identitate utilizator și să acceseze resursele altei identități utilizator fără ca utilizatorul să fie nevoit prezinte identitatea utilizator necesară. Realizați asta în EIM prin definirea unei asociații între o identitate utilizator și altă identitate utilizator. Identitățile utilizator pot fi în diverse forme, inclusiv certificate utilizator. Puteți fie să creați asociații individuale între un identificator EIM și diferitele identități utilizator care aparțin unui utilizator reprezentat de acel identificator EIM. Sau puteți crea asocieri de politică, care mapează un grup de identități utilizator la o singură identitate utilizator destinație. Identitățile utilizator pot fi în diverse forme, inclusiv certificate utilizator. Când creați aceste asociații, certificatele utilizator pot fi mapate pe identificatorii EIM corespunzători astfel făcând mai ușoară folosirea certificatelor pentru autentificare.

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

1. Folosiți vrăjitorul **Configurare EIM** din **Navigație iSeries** pentru a configura EIM.
2. Creați un identificator EIM pentru fiecare utilizator care vreți să participe la EIM.
3. Creați o asociere destinație între fiecare identificator EIM și 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. Folosiți numele de definiție din registrul EIM pentru registrul de utilizatori i5/OS local pe care l-ați specificat în vrăjitorul **Configurare EIM**.

După ce realizați task-urile de configurare EIM necesare, trebuie să folosiți task-ul **Gestionare locație LDAP** pentru a configura DCM (Digital Certificate Manager) să memoreze certificate utilizator într-o locație LDAP (Lightweight Directory Access Protocol) în locul unui profil utilizator. Când configurați EIM sau DCM să lucreze împreună, task-ul **Creare certificat** pentru certificate utilizator și task-ul **Alocare certificat utilizator** procesează certificatele pentru utilizare EIM mai degrabă decât să aloce certificatul unui profil utilizator. DCM memorează certificatul în directorul LDAP configurat și folosește informațiile din DN-ul certificatului pentru a crea o asociație sursă pentru identificatorul EIM corespunzător. Aceasta permite sistemelor de operare și aplicațiilor să folosească certificatul ca sursă a unei operații de căutare EIM pentru a mapa de la certificat la o identitate utilizator destinație asociată cu același identificator EIM.

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

Concepte înrudite

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

Operații înrudite

“Gestionarea certificatelor utilizator prin expirare” la pagina 43

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

“Gestionarea locației LDAP pentru certificatele utilizator” la pagina 70

Învățați cum să configurați DCM să memoreze certificate utilizator într-o locație director a serverului LDAP (lightweight Directory Access protocol) pentru a extinde Enterprise Identity Mapping să lucreze cu certificatele utilizator.

Informații înrudite

Subiectul pentru Centrul de Informare EIM DNS

Certificatele digitale pentru conexiuni VPN

Folosiți aceste informații pentru a învăța cum să folosiți certificate ca parte a configurării unei conexiuni VPN.

Puteți folosi certificate digitale ca un mijloc de a stabili o iSeries conexiune VPN. Ambele capete ale unei conexiuni dinamice VPN trebuie să poată comunica pentru a se autentifica una altele 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 și 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. Totuși, folosirea unei chei pre-partajate este mai puțin sigură deoarece trebuie să comunicați această cheie manual administratorului de la celălalt capăt al VPN-ului dumneavoastră. În consecință, este posibil ca aceasta să fie văzută de alții în timpul procesului de comunicare al ei.

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

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

Unele implementări VPN cer ca certificatul să conțină informații nume subiect alternative, cum ar fi un nume domeniu sau o adresă de mail, suplimentare față de informația standard legată de numele distinct. Când folosiți CA-ul local în DCM pentru a emite un certificat, puteți specifica informații alternative privind numele subiectului certificatului. Specificând aceste informații, vă asigurați că aveți o conexiune VPN compatibilă cu alte implementări VPN care au nevoie de ele pentru autentificare.

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

- Dacă nu ați folosit niciodată DCM pentru a gestiona certificate, aceste articole vă vor ajuta să începeți:
 - Crearea și operarea unui CA local, privat vă arată cum să folosiți DCM pentru a emite certificate private pentru aplicațiile dumneavoastră.
 - Gestionarea certificatelor de la un CA public din Internet descrie cum să utilizați DCM pentru a lucra cu certificatele provenite de la un CA public.

- Dacă nu folosiți în curent DCM pentru a gestiona certificate pentru alte aplicații, revedeți aceste surse pentru a afla cum să specificați dacă o aplicație folosește un certificat existent și ce certificate poate accepta și autentifica aplicația:
 - Gestionarea atribuirii certificatului pentru o aplicație vă descrie cum să folosiți DCM pentru a atribui un certificat existent unei aplicații, cum ar fi server-ul IKE.
 - Definirea listei de încredere CA pentru o aplicație vă descrie cum să specificați în care CA-uri poate avea încredere o aplicație atunci când aceasta acceptă certificate pentru autentificare client (sau VPN).

Informații înrudite

Configurarea unei conexiuni VPN

Certificatele digitale pentru semnarea obiectelor

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticității sale.

IBM i5/OS oferă suport pentru folosirea certificatelor pentru a "semna" digital obiecte.. Semnarea digitală a obiectelor furnizează un mod de a verifica atât integritatea conținutului obiectului cât și originea lui. Suportul pentru semnarea obiectelor îmbunătățește capacitatea uneltelor tradiționale iSeries de sistem de a controla cine poate modifica obiectele. Controlul tradițional nu poate proteja un obiect de atacurile neautorizate în timp ce obiectul este în tranzit peste Internet sau alte rețele care nu sunt de încredere, sau în timp ce obiectul este depozitat pe un sistem non-iSeries. De asemenea, controalele tradiționale 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 și conținutul său nu sunt criptate și nu sunt făcute private de semnătura digitală; totuși, 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 și 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 și poate în schimb să-l contacteze pe semnatar și să obțină altă copie a obiectului semnat.

Dacă decideți că folosirea semnăturilor digitale îndeplinește nevoile și politicile dumneavoastră de securitate, este nevoie să evaluați dacă aveți nevoie să folosiți certificate publice versus emitere de certificate private. Dacă intenționați să distribuiți obiecte către utilizatori din publicul general, ați putea considera folosirea certificatelor de la un CA public binecunoscut pentru a semna obiecte. Folosirea certificatelor publice asigură faptul că ceilalți pot verifica ușor și necostisitor semnăturile pe care le-ați plasat pe obiectele pe care le-ați distribuit. Dacă însă intenționați să distribuiți obiecte doar în cadrul organizației dumneavoastră, ați putea prefera să folosiți DCM (Digital Certificate Manager) pentru a opera propriul dumneavoastră CA local, cu care să emiteți certificate pentru semnarea obiectelor. Folosirea certificatelor private de la un CA local pentru a semna obiecte este mai puțin costisitoare decât cumpărarea de certificate de la un CA public binecunoscut.

Semnătura de pe un obiect reprezintă sistemul care a semnat obiectul, nu un utilizator specific de pe acel sistem (deși utilizatorul trebuie să aibă autoritatea necesară pentru a folosi certificatul pentru a semna obiecte). Folosiți DCM pentru a gestiona certificatele pe care le folosiți pentru a semna obiecte și a verifica semnăturile obiectelor. Deasemenea, puteți folosi DCM pentru a semna obiecte și pentru a verifica semnăturile obiectelor.

Concepte înrudite

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

“Certificate digitale pentru verificarea semnăturii obiectelor” la pagina 36

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a verifica semnătura digitală a unui obiect pentru a verifica autenticitatea acestuia.

Operații înrudite

“Verificarea semnăturii obiecte” la pagina 72

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

“Gestionarea certificatelor Internet publice pentru semnarea obiectelor” la pagina 48

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

“Gestionarea certificatelor pentru verificarea semnăturii obiectelor” la pagina 50

Puteți folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele de verificare a semnăturilor obiectelor pe care le folosiți pentru a valida semnăturile digitale ale obiectelor.

Certificate digitale pentru verificarea semnăturii obiectelor

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a verifica semnătura digitală a unui obiect pentru a verifica autenticitatea acestuia.

IBM i5/OS oferă suport pentru utilizarea certificatelor pentru a verifica semnături digitale pe obiecte. Oricine dorește să se asigure că un obiect semnat nu a fost modificat la transfer și că obiectul provine de la o sursă acceptată și legitimă poate folosi cheia publică a certificatului 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 și poate în schimb să-l contacteze pe semnat și să obțină 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 decideți în care Autorități de certificare aveți încredere și în care certificate aveți încredere pentru a semna obiecte. Când alegeți să aveți încredere într-un CA (Certificate Authority), puteți să alegeți dacă să aveți încredere în semnăturile pe care le creează altcineva folosind un certificat emis de CA-ul de încredere. Când alegeți să nu aveți încredere într-un CA, alegeți și să nu aveți încredere în certificatele emise de CA sau în semnăturile create de cineva folosind aceste certificate.

Verificarea valorii sistem restaurare obiect (QVfyOBJRST)

Dacă vă decideți să efectuați verificarea semnăturilor, una dintre primele decizii importante pe care trebuie să le luați este să determinați cât de importante sunt semnăturile pentru obiectele restaurate pe sistemul dumneavoastră Controlați 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 definește 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 și îl tratează ca și când nu ar fi semnat.

Sunt mai multe valori pe care le puteți folosi pentru valoarea sistem QVfyOBJRST, care variază între ignorarea tuturor semnăturilor și necesitatea de semnături valide pentru toate obiectele pe care le restaurează sistemul. Această valoare de sistem afectează doar obiectele executabile care sunt restaurate, nu fișierele salvare sau fișierele sistemului de fișiere integrat. Pentru a învăța mai multe despre utilizarea ei și a altor valori de sistem, vedeți Centrul de informare iSeries.

Folosiți DCM pentru a implementa certificatul dumneavoastră și deciziile de încredere CA cât și pentru a gestiona certificatele pe care le folosiți pentru a verifica semnăturile obiectelor. Deasemenea, puteți folosi DCM pentru a semna obiecte și pentru a verifica semnăturile obiectelor.

Concepte înrudite

“Certificatele digitale pentru semnarea obiectelor” la pagina 35

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticității sale.

Informații înrudite

Căutător de valori de sistem

Configurarea DCM

Folosiți aceste informații pentru a afla cum să configurați tot ce vă trebuie pentru a vă asigura că puteți folosi DCM pentru a vă gestiona certificatele dumneavoastră și cheile lor.


DCM (Digital Certificate Manager) furnizează o interfață cu utilizatorul bazată pe browser pe care o puteți folosi pentru a gestiona certificate digitale pentru aplicații și utilizatori. Interfața cu utilizatorul este divizată în două cadre principale: un cadru de navigare și un cadru de task.

Puteți folosi cadrul de navigare pentru a selecta task-urile care să administreze certificatele sau aplicațiile care le folosesc. În timp ce unele task-uri individuale apar direct în cadrul principal de navigare, majoritatea task-urilor din cadrul de navigare sunt organizate în categorii. De exemplu, **Gestionare certificate** este o categorie de task-uri care conține o varietate de task-uri individuale asistate, cum ar fi Vizualizare certificate, Reînnoire certificat, Import certificat și așa 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 veți selecta legătura categorie, va fi afișată o listă extinsă de task-uri, astfel încât să puteți alege task-ul dorit pentru executare.

Cu excepția categoriei **Cale rapidă**, fiecare task din cadrul de navigare este un task asistat care vă trece printr-o serie de pași pentru a se efectua task-ul ușor și rapid. Categoria Cale rapidă oferă un grup de funcții de gestionare a certificatelor și aplicațiilor care permit utilizatorilor experimentați ai DCM să acceseze rapid o varietate de task-uri înrudite dintr-un singur set central de pagini.

Task-urile care sunt disponibile în cadrul de navigare variază pe baza depozitului de certificate în care lucrați. De asemenea, categoria și numărul de task-uri pe care le vedeți în cadrul de navigare variază în funcție de autorizațiile pe care le are profilul dumneavoastră de utilizator i5/OS. Toate task-urile pentru operarea unui CA, pentru administrarea certificatelor pe care le folosesc aplicațiile și alte task-uri la nivelul de sistem sunt disponibile numai pentru iSeries responsabilii cu securitatea sau administratori. Responsabilul cu securitate sau administratorul trebuie să dețină autorizările speciale *SECADM și *ALLOBJ pentru a vizualiza și utiliza aceste procese. Utilizatorii fără aceste autorizări speciale au acces doar la funcțiile de certificare utilizator.

Pentru a învăța cum să configurați DCM și să începeți să-l folosiți pentru administrarea certificatelor, revedeți aceste subiecte:

Dacă vreți mai multe informații educaționale despre folosirea certificatelor digitale într-un mediu Internet pentru a vă îmbunătăți securitatea sistemului și a rețelei dumneavoastră, situl Web VeriSign este o resursă excelentă. Situl Web VeriSign furnizează o bibliotecă extinsă despre subiecte de certificate digitale, precum și un număr de alte subiecte legate de securitatea Internet. Puteți accesa biblioteca lor la VeriSign Help Desk .

Pornirea Digital Certificate Manager

Folosiți aceste informații pentru a afla cum se accesează caracteristica DCM (Digital Certificate Manager) pe sistem.

Înainte de a folosi oricare din aceste funcții DCM, va trebui să-l porniți. Efectuați aceste task-uri pentru a vă asigura că ați pornit cu succes DCM:

1. Instalați 5722 SS1 Opțiunea 34. Acesta este Digital Certificate Manager - DCM.
2. Instalați 5722 DG1. Acesta este IBM HTTP Server for i5/OS.
3. Folosiți Navigator iSeries pentru a porni serverul administrativ server HTTP:
 - a. Porniți **Navigator iSeries**.
 - b. Faceți dublu clic pe serverul dumneavoastră în vizualizarea arbore principală.
 - c. Expandați **Rețea > Servere > TCP/IP**.
 - d. Efectuați un clic dreapta pe **Administrare HTTP**.
 - e. Selectați **Pornire**.
4. Porniți-vă browser-ul Web.

5. Folosind browser-ul, mergeți la pagina Task-uri de pe sistemul iSeries dumneavoastră, la http://numele_sistemului_dvs:2001.
6. Selectați **Digital Certificate Manager** din lista de produse din pagina Task-uri iSeries pentru a accesa interfața de utilizator DCM.

Concepte înrudite

“Scenariu: Folosirea certificatelor pentru autentificări externe” la pagina 12

Acest scenariu descrie când și cum să folosiți certificate ca un mecanism de autentificare pentru a proteja și limita accesul utilizatorilor publici la resurse publice sau din afara rețelei și la aplicații.

Setarea certificatelor pentru prima dată

Învățați cum să faceți primii pași în administrarea certificatelor de la un CA (Certificate Authority - Autoritate de certificare) din Internet sau cum să creați și să operați un CA local privat pentru a emite certificate..

Cadrul stâng al DCM (administrator de certificate digitale) este cadrul de navigare task. Puteți folosi acest cadru pentru a selecta o varietate largă de task-uri pentru gestionarea certificatelor și a aplicațiilor care le folosesc. Care task-uri sunt disponibile depinde de ce depozit de certificate (dacă există unul) cu care lucrați și de autorizările speciale ale profilului utilizator. Majoritatea task-urilor sunt disponibile doar dacă aveți autorizații speciale *ALLOBJ și *SECADM. Pentru a utiliza DCM pentru a verifica semnături ale obiectelor, profilul dumneavoastră utilizator trebuie să aibă autorizarea specială *AUDIT.

Când folosiți DCM (Digital Certificate Manager) pentru prima dată, nu există nici un depozit de certificate. În consecință, când accesați inițial DCM, panoul de navigație afișează doar aceste task-uri și doar când aveți autorizările speciale necesare:

- Gestionarea certificatelor utilizator.
- Crearea unui nou Depozit de certificate.
- Crearea unui CA (Certificate Authority - Autoritate de certificare). (Notă: După ce folosiți acest task pentru a crea un CA local privat, acest task nu mai apare în listă.)
- Gestionarea locațiilor CRL.
- Gestionare locație LDAP.
- Gestionarea locației cererii PKIX.
- Consultați iSeries.

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

Trebuie să accesați mai întâi depozitul necesar de certificate înainte de a putea începe lucrul cu majoritatea task-urilor de gestiune a certificatelor și a aplicațiilor. Pentru a deschide un depozit de certificate specific, alegeți în cadrul de navigare **Selectare depozit de certificate**.

Cadrul de navigare al DCM oferă de asemenea un buton **Conexiune sigură**. Puteți folosi acest buton pentru a afișa o a doua fereastră de browser pentru a iniția o conexiune sigură folosind SSL (Secure Sockets Layer). Pentru a folosi cu succes această funcție, trebuie să configurați mai întâi IBM HTTP Server for i5/OS pentru a folosi SSL să operați în modul securizat. Trebuie să porniți apoi Serverul HTTP în modul securizat. Dacă nu ați configurat și pornit Serverul HTTP pentru operare SSL, veți vedea un mesaj de eroare și browser-ul nu va deschide o sesiune securizată.

Pornirea

Deși s-ar putea să doriți să folosiți certificate pentru a realiza un număr de cerințe legate de securitate, ceea ce veți face mai întâi depinde de cum veți planifica să vă obțineți certificatele. Există două căi primare pe care le puteți urma atunci când folosiți pentru prima oară DCM, diferind dacă creți să folosiți certificate private sau emiterea de certificate private.

Concepte înrudite

“CertIFICATE publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

Crearea și lucrul cu un CA local

Folosiți această informație pentru a învăța cum să creați și operați CA pentru a emite certificate private pentru aplicații.

După ce revedeți cu atenție necesitățile și politicile dumneavoastră de securitate, vă decideți să operați cu un CA local pentru a emite certificate private pentru aplicațiile dumneavoastră. Puteți folosi DCM ca să creați și să operați cu propriul dumneavoastră CA local. DCM vă oferă un task ghidat, care vă poartă prin acest proces de creare a unui CA și de folosire a lui pentru a emite certificate pentru aplicații. Calea task-ului ghidat vă asigură că aveți tot ce este necesar pentru a începe să folosiți certificatele digitale pentru a configura aplicațiile să folosească SSL și să semneze obiecte și să verifice semnătura obiectelor.

Notă: Pentru a folosi certificate cu IBM HTTP Server for i5/OS, trebuie să creați și să configurați serverul dumneavoastră Web înainte de a lucra cu DCM. Când configurați un server Web să folosească SSL, este generat un ID aplicație pentru server. Trebuie să faceți o notă a acestui ID aplicație astfel încât să puteți folosi DCM pentru a specifica care certificat va fi utilizat de această aplicație pentru SSL.

Nu terminați și reporniți serverul până nu folosiți DCM să aloce un certificat către server. Dacă opriți și reporniți instanța *ADMIN a serverului Web înainte de a-i aloca un certificat, serverul nu va porni și nu veți putea folosi DCM pentru a aloca un certificat serverului.

Pentru a folosi DCM să creeze și să opereze cu un CA local, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare al DCM, selectați Crearea unui CA pentru a se afișa o serie de formulare. Aceste formulare vă îndrumă prin procesul creării unui CA local și completării altor task-uri necesare pentru a începe folosirea certificatelor digitale pentru SSL, semnarea obiectelor și verificarea semnăturii.

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

3. Completați toate formularele pentru acest task. Când folosiți aceste formulare pentru a realiza toate task-urile de care aveți nevoie pentru a seta un CA local operațional:
 - a. Alegeți cum să memorați cheia privată pentru certificatul CA local. (Acest pas este furnizat doar dacă aveți un IBM Cryptographic Coprocessor instalat pe sistemul dumneavoastră. Dacă sistemul nu are un coprocesor criptografic, DCM va plasa automat certificatul și cheia privată în CA-ul local.)
 - b. Furnizați informațiile de identificare pentru CA-ul local.
 - c. Instalați certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră astfel încât software-ul dumneavoastră să poată recunoaște CA local și să valideze certificatele pe care le emite CA.
 - d. Alegeți datele politicii pentru CA-ul dumneavoastră local.
 - e. Folosiți noul CA local pentru a emite un certificat server sau client pe care aplicațiile dumneavoastră să îl poată folosi pentru conexiuni SSL. (Dacă sistemul dumneavoastră are un IBM Cryptographic Coprocessor instalat, acest pas vă permite să selectați cum să memorați cheia privată pentru certificatul server sau client. Dacă sistemul nu are un coprocesor, DCM va plasa automat certificatul și cheia privată în depozitul de certificate *SYSTEM. DCM creează depozitul de certificate *SYSTEM ca parte a acestui subtask.)
 - f. Selectați aplicațiile care pot folosi certificatul client sau server pentru conexiuni SSL.

Notă: Dacă ați folosit DCM pentru a crea anterior depozitul de certificate *SYSTEM pentru a gestiona certificate pentru SSL de la un CA publică din Internet, nu efectuați acest lucru sau pasul anterior.

- g. Folosiți noul CA local pentru a emite un certificat de semnare obiect pe care aplicațiile să îl poată folosi pentru a semna digital obiecte. Acest subtask creează depozitul de certificate *OBJECTSIGNING; acesta este depozitul de certificate pe care îl folosiți pentru a gestiona certificate care semnează obiecte.
- h. Selectați aplicațiile care pot folosi certificatul care semnează obiecte pentru a plasa semnături digitale pe obiecte.

Notă: Dacă ați 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 efectuați acest lucru sau pasul anterior.

- i. Selectați aplicațiile care vor avea încrederea în CA-ul local.

Atunci când terminați task-ul asistat, sunteți gata să începeți configurarea aplicației dumneavoastră pentru a folosi SSL pentru comunicații securizate.

După ce vă configurați aplicațiile, utilizatorii care accesează aplicațiile printr-o conexiune SSL trebuie să folosească DCM pentru a obține o copie a certificatului CA local. Fiecare utilizator trebuie să aibă o copie a certificatului astfel încât software-ul client al utilizatorului să-l poată utiliza pentru a autentifica identitatea serverului ca parte a procesului de negociere SSL. Utilizatorii pot folosi DCM fie pentru a copia certificatul CA local într-un fișier, fie pentru a descărca certificatul în browser-ul lor. Cum memorează utilizatorii certificatul CA local depinde de software-ul client pe care îl folosesc pentru a stabili o conexiune SSL la o aplicație.

De asemenea, puteți folosi acest CA local pentru a emite certificate către aplicații de pe alte sisteme iSeries din rețeaua dumneavoastră.

Pentru a afla mai multe despre folosirea DCM pentru gestionarea certificatelor utilizator și cum pot obține utilizatorii o copie a certificatului CA local pentru a autentifica certificatele pe care le emite CA-ul local, revedeți aceste subiecte:

Concepte înrudite

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

“Gestionarea certificatelor utilizator”

Puteți folosi DCM (Digital Certificate Manager) pentru a obține certificate cu SSL sau asocierea certificatelor existente cu profilurile de utilizator iSeries.

Operații înrudite

“Utilizarea CA local pentru a emite certificate pentru alte sisteme iSeries” la pagina 54

Aflați cum se folosește un CA local privat de pe un sistem pentru a emite certificate folosite pe alte sisteme. iSeries.

“Obținerea unei copii a certificatului CA privat” la pagina 45

Aflați cum să obțineți o copie a certificatului CA privat și instalați-l pe PC-ul dumneavoastră astfel încât să puteți autentifica orice certificate server pe care le emite CA.

Referințe înrudite

“Folosirea API-urilor pentru a emite prin programe certificate către utilizatorii non-iSeries” la pagina 44

Folosiți aceste informații pentru a emite certificate către utilizatorii fără a asocia certificatul cu un profil de utilizator iSeries.

Gestionarea certificatelor utilizator:

Puteți folosi DCM (Digital Certificate Manager) pentru a obține certificate cu SSL sau asocierea certificatelor existente cu profilurile de utilizator iSeries.

Dacă utilizatorii accesează serverele publice sau interne printr-o conexiune SSL, aceștia 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 folosește un certificat dintr-un CA publică, software-ul utilizatorilor dumneavoastră ar putea poseda

deja o copie a certificatului CA. În consecință, nici dumneavoastră ca administrator al DCM, nici utilizatorii dumneavoastră nu trebuie să luați nici o acțiune înainte de a participa într-o sesiune SSL. Totuși, dacă serverul dumneavoastră folosește un certificat de la un CA local privat, utilizatorii dumneavoastră trebuie să obțină o copie a certificatului emis de CA-ul local înainte să poată stabili o sesiune SSL cu serverul.

În plus, dacă aplicația server suportă și cere autentificarea clienților prin certificate, utilizatorii trebuie să prezinte un certificat de utilizator acceptat pentru a accesa resursele pe care le furnizează serverul. În funcție de nevoile dumneavoastră de securitate, utilizatorii pot prezenta un certificat de la un CA public din Internet sau unul pe care îl obțin de la CA-ul local pe care îl folosiți dumneavoastră. Dacă aplicația server a dumneavoastră furnizează acces la resurse pentru utilizatorii interni care au în acest moment iSeries profiluri utilizator, puteți folosi DCM pentru a le adăuga certificatele lor la profilurile lor de utilizator. Această asociere asigură faptul că utilizatorii au același acces și aceleași restricții pentru resurse când prezintă certificate ca și cele garantate de profilul lor de utilizator.

Digital Certificate Manager (DCM) vă permite să gestionați certificate care sunt alocate unui profil de utilizator iSeries. Dacă aveți un profil de utilizator cu autorizații speciale *ALLOBJ, puteți gestiona atribuirea de certificate profil de utilizator pentru dumneavoastră ca și pentru alți utilizatori. Când nu este deschis nici un depozit de certificate sau când depozitul de certificate CA (autoritate de certificare) local este deschis, puteți selecta **Gestionarea certificatelor utilizator** din cadrul de navigare pentru a accesa task-urile necesare. Dacă este deschis un depozit de certificate diferit, task-urile certificat utilizator sunt integrate în task-uri sub **Gestionarea certificatelor**.

Utilizatorii fără autorizările speciale de profil de utilizator *SECADM și *ALLOBJ își pot gestiona doar propriile alocări de certificate. Ei pot selecta **Gestionare certificate Utilizator** pentru a accesa task-uri care le permit să vizualizeze certificatele asociate cu profilurile lor de utilizator, să șteargă un certificat din profilurile lor de utilizator sau să alocă un certificat de la un CA diferit la profilurile lor de utilizator. Utilizatorii, indiferent de autorizările speciale pentru profilurile lor de utilizator, pot obține un certificat de utilizator de la CA-ul local prin selectarea task-ului **Creare certificate** din cadrul de navigare principal.

Pentru a afla mai multe despre cum să folosiți DCM pentru a gestiona și crea certificate de utilizator, revedeți aceste subiecte:

Operații înrudite

“Crearea și lucrul cu un CA local” la pagina 39

Folosiți această informație pentru a învăța cum să creați și operați CA pentru a emite certificate private pentru aplicații.

“Obținerea unei copii a certificatului CA privat” la pagina 45

Aflați cum să obțineți o copie a certificatului CA privat și instalați-l pe PC-ul dumneavoastră astfel încât să puteți autentifica orice certificate server pe care le emite CA.

Crearea unui certificat utilizator:

Folosiți aceste informații pentru a afla cum pot utilizatorii să folosească CA-ul local pentru a emite un certificat pentru autentificarea clientului.

Dacă doriți să folosiți certificate digitale pentru autentificarea utilizatorului, utilizatorii trebuie să dețină certificate. Dacă folosiți DCM (Digital Certificate Manager) pentru a lucra cu un CA local privat, puteți folosi CA-ul local pentru a emite certificate către fiecare utilizator. Fiecare utilizator trebuie să acceseze DCM pentru a obține un certificat folosind task-ul **Crearea certificatelor**. Pentru a obține un certificat de la CA-ul local, politica de CA trebuie să permită CA-ului să emită certificate de utilizator.

Pentru a obține un certificat de la un CA local, parcurgeți pașii următori:

1. Porniți DCM.
2. În cadrul de navigare, selectați **Crearea certificatelor**.
3. Selectați **Certificate utilizator** pentru tipul certificatului pe care îl creați. Se va afișa un formular în care veți putea introduce informații de identificare pentru certificat.
4. Completați formularul și apăsați **Continuare**.

Notă: Dacă aveți întrebări despre completarea unui anume formular care este în task-ul asistat, selectați 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 și publice pentru certificate. Browser-ul poate afișa mai multe ferestre pentru a vă ghida prin acest proces. Urmați instrucțiunile browser-ului pentru aceste task-uri. După ce browser-ul generează cheile, se va afișa o pagină de confirmare care va indica faptul că DCM-ul a creat certificatele.
6. Instalați noul certificat în browser-ul dumneavoastră. Browser-ul poate afișa mai multe ferestre pentru a vă ghida prin acest proces. Urmați instrucțiunile date de browser pentru a termina acest task.
7. Apăsați **OK** pentru a încheia task-ul.

În timpul procesării, DCM (Digital Certificate Manager) asociază automat certificatul cu iSeries

Dacă doriți ca un certificat de la alt CA pe care un utilizator îl prezintă pentru autentificare client să aibă aceleași autorizări ca profilurile lor utilizator, utilizatorul poate folosi DCM pentru a alocă certificatul la profilurile lor utilizator.

Concepte înrudite

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

Operații înrudite

“Alocarea unui certificat utilizator”

Puteți să alocați un certificat pe care îl dețineți la profilul utilizator i5/OS sau la altă identitate de utilizator.

Certificatul poate fi de la un CA local privat de pe alt sistem sau de la un CA din Internet binecunoscut. Pentru a alocă un certificat unei identități de utilizator, CA-ul emitent trebuie să fie de încredere pentru server și certificatul trebuie să nu fie deja asociat cu un profil de utilizator sau altă identitate de utilizator din sistem.

“Obținerea unei copii a certificatului CA privat” la pagina 45

Aflați cum să obțineți o copie a certificatului CA privat și instalați-l pe PC-ul dumneavoastră astfel încât să puteți autentifica orice certificate server pe care le emite CA.

Alocarea unui certificat utilizator:

Puteți să alocați un certificat pe care îl dețineți la profilul utilizator i5/OS sau la altă identitate de utilizator. Certificatul poate fi de la un CA local privat de pe alt sistem sau de la un CA din Internet binecunoscut. Pentru a alocă un certificat unei identități de utilizator, CA-ul emitent trebuie să fie de încredere pentru server și certificatul trebuie să nu fie deja asociat cu un profil de utilizator sau altă identitate de utilizator din sistem.

Unii utilizator pot avea certificate de la un CA (Certificate Authority) din afară sau de la un CA local pe un sistem iSeries pe care dumneavoastră, ca administrator, vreți să le faceți disponibile pentru DCM (Digital Certificate Manager). Asta vă permite dumneavoastră și utilizatorului să folosiți DCM pentru a gestiona aceste certificate, care sunt cel mai adesea folosite pentru autentificarea client. Task-ul **Alocare certificat utilizator** furnizează un mecanism pentru a permite unui utilizator să creeze o alocare DCM pentru un certificat obținut 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 iSeries cu profilul utilizator al acestuia. Când o locație LDAP nu este definită pentru DCM, task-ul **Alocare un certificat utilizator** permite unui utilizator să alocă un certificat din afară unui i5/OS profil utilizator. Alocarea certificatului la un profil utilizator asigură că certificatul poate fi folosit cu aplicații din sistem care necesită certificate pentru autentificarea client.
- Memorare certificat în locație LDAP (Lightweight Directory Access Protocol) pentru utilizare cu EIM (Enterprise Identity Mapping). Când este definită o locație LDAP și sistemul iSeries este configurat să participe în EIM, task-ul **Alocare certificat utilizator** permite unui utilizator să memoreze o copie a unui certificat din afară în directorul LDAP specificat. DCM creează de asemenea o asociere sursă în EIM pentru certificat. Memorarea certificatului 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 alocă un certificat la o identitate utilizator într-o configurație EIM, EIM trebuie să fie configurat în mod corespunzător pentru utilizator. Această configurație EIM implică crearea unui identificator EIM pentru utilizator și crearea unei asocieri destinație între acel identificator EIM și profilul utilizator. Altfel, DCM nu poate crea o asociație sursă corespunzătoare cu identificatorul EIM pentru certificat.

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

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

Faptul că aveți sau nu sesiuni sigure este determinat de numărul de port din URL-ul folosit pentru accesarea DCM-ului. Dacă folosiți portul 2001, care este portul implicit pentru accesarea DCM, atunci nu aveți o sesiune sigură. De asemenea, Serverul HTTP trebuie configurat să folosească SSL înainte să puteți comuta pe o conexiune securizată.

Când utilizatorul selectează acest task, se afișează 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 inițiază 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 însuși.

2. Să prezinte un certificat pentru autentificare client.

În funcție de setările din configurare pentru browser, acesta vă poate cere să selectați 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 afișa informațiile despre certificat într-o fereastră separată. Dacă nu prezentați un certificat acceptabil, server vă poate cere în schimb numele utilizator și parola pentru autentificare înainte de a vă permite accesul.

3. Să aibă un certificat în browser care nu este asociat deja cu identitatea utilizatorului pentru cel care realizează task-ul. (Sau, dacă DCM este configurat pentru a lucra în conjuncție cu EIM, utilizatorul trebuie să aibă un certificat în browser care nu este deja memorat în locația LDAP pentru DCM.)

O dată ce stabiliți 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 obține cu succes unul sau mai multe certificate, puteți vedea informațiile despre certificat și puteți alege să îl asociați cu profilul de utilizator.

Dacă DCM nu afișează informații de la un certificat, nu ați putut să furnizați un certificat pe care DCM să-l poată alocă identității utilizator a dumneavoastră. De acest lucru poate fi responsabilă una dintre problemele certificatelor utilizator. De exemplu, certificatele pe care le conține browser-ul dumneavoastră pot fi asociate deja cu identitatea utilizator a dumneavoastră.

Operații înrudite

“Crearea unui certificat utilizator” la pagina 41

Folosiți aceste informații pentru a afla cum pot utilizatorii să folosească CA-ul local pentru a emite un certificat pentru autentificarea clientului.

“Depanarea alocării unui certificat utilizator” la pagina 79

Informații înrudite

Subiectul pentru Centrul de Informare EIM

Gestionarea certificatelor utilizator prin expirare:

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

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

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

Pentru a vedea și a gestiona certificatele utilizator pe baza datelor de expirare, urmați acești pași:

1. Porniți DCM.

Notă: Dacă aveți întrebări despre completarea unui anume formular în timp ce folosiți DCM, selectați butonul cu semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.

2. În cadrul de navigație, selectați **Gestionare certificate utilizator** pentru a afișa o listă de task-uri.

Notă: Dacă lucrați curent cu un depozit de certificate, selectați **Gestionare certificate** pentru a afișa o listă de task-uri, apoi selectați **Verificare expirare** și selectați **Utilizator**.

3. Dacă profilul utilizator al dumneavoastră are autorizările speciale *ALLOBJ și *SECADM, puteți selecta o metodă pentru a alege care certificate utilizator să le vedeți și să le gestionați pe baza datelor lor de expirare. (Dacă profilul utilizator al dumneavoastră nu are aceste autorizări speciale, DCM vă cere să specificați intervalul datei de expirare așa cum este descris în pasul următor.) Puteți selecta unul din următoarele:

- **Profil utilizator** pentru a vedea și gestiona certificatele utilizator care sunt alocate un profil utilizator i5/OS specific. Specificați un **Nume profil utilizator** și faceți clic pe **Continuare**.

Notă: Puteți specifica un profil utilizator altul decât al dumneavoastră dacă aveți autorizările speciale *ALLOBJ și *SECADM.

- **Toate certificatele utilizator** pentru a vedea și a gestiona certificatele pentru toate identitățile utilizator.

4. În câmpul **Interval dată expirare în zile (1-365)**, introduceți numărul de zile pentru care să vedeți certificatele utilizator pe baza datei lor de expirare și faceți clic pe **Continuare**. DCM afișează toate certificatele utilizator pentru profilul utilizator specificat care expiră între data de astăzi și data care se potrivește numărului de zile specificat. DCM afișează de asemenea toate certificatele utilizator care au datele de expirare înainte de data de astăzi.

5. Selectați un certificat utilizator pentru gestionare. Puteți alege să vedeți detalii despre informațiile certificatului sau să-l înlăturați din identitatea utilizator asociată.

6. Când terminați de lucrat cu certificatele din listă, faceți clic pe **Anulare** pentru a ieși din task.

Operații înrudite

“Certificate digitale și EIM (Enterprise Identity Mapping)” la pagina 33

Aceasta permite sistemelor de operare și aplicațiilor să folosească certificatul ca sursă a unei operații de căutare EIM pentru a mapa de la certificat la o identitate utilizator destinație asociată cu același identificator EIM.

Informații înrudite

EIM - Privire generală centru de informare

Folosirea API-urilor pentru a emite prin programe certificate către utilizatorii non-iSeries:

Folosiți aceste informații pentru a emite ceritfcate către utilizatorii fără a asocia certificatul cu un profil de utilizator iSeries.

Începând cu i5/OS V5R3, sunt două API-uri noi disponibile pe care le puteți folosi pentru a emite prin program certificate către utilizatorii non-iSeries. În versiunile anterioare, când foloseați CA-ul dumneavoastră local pentru a emite certificate către utilizatori, aceste certificate erau automat asociate cu profilurile lor utilizator iSeries. În consecință, pentru a folosi CA-ul local pentru a emite un certificat către utilizator pentru autentificare client, trebuia să furnizați acel utilizator cu un profil de utilizator iSeries. De asemenea, când utilizatorii aveau nevoie să obțină un certificat de la un CA local pentru autentificare client, fiecare utilizator trebuia să folosească DCM pentru a crea certificatul necesar. Așadar, fiecare utilizator trebuie să aibă un profil utilizator pe serverul iSeries care găzduiește DCM și o semnare validă la acel server iSeries.

Având certificatul asociat cu un profil de utilizator are avantajele sale, mai ales când este vorba de utilizatorii interni. Totuși, aceste restricții și cerințe au făcut mai puțin practică folosirea CA-ului local pentru a emite certificate utilizator

pentru un număr mare de utilizatori, mai ales când nu doriți ca acei utilizatori să aibă un profil utilizator iSeries. Pentru a evita furnizarea profilurilor de utilizator către acești utilizatori, ați putea cere acestora să plătească pentru un certificat de la un CA binecunoscut dacă ați dorit să cereți certificate pentru autentificarea utilizatorului pentru aplicațiile dumneavoastră.

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

Sunt două API-uri, câte unul pentru fiecare program browser predominant, pe care le puteți apela la folosirea Net.Data pentru a crea un program pentru emiterea certificatelor către utilizatori. Aplicația pe care o creați trebuie să dispună de codul Interfață Utilizator Grafică (GUI) necesar pentru a crea certificatul utilizator și pentru a apela unul din API-urile corespunzătoare pentru a folosi CA-ul local pentru a semna certificatul.

Pentru mai multe informații despre folosirea acestor API-uri, vedeți aceste pagini:

- API Generate and Sign User Certificate Request (QYUCGSUC).
- API Sign User Certificate Request (QYCUSUC).

Concepte înrudite

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

“Certificatele digitale pentru autentificarea utilizatorului” la pagina 31

Folosiți aceste informații pentru a afla despre cum să folosiți certificate pentru a furniza un mijloc pentru o autentificare mai puternică a utilizatorilor care accesează resurse de pe un server iSeries.

Operații înrudite

“Crearea și lucrul cu un CA local” la pagina 39

Folosiți această informație pentru a învăța cum să creați și operați CA pentru a emite certificate private pentru aplicații.

Obținerea unei copii a certificatului CA privat:

Aflați cum să obțineți o copie a certificatului CA privat și instalați-l pe PC-ul dumneavoastră astfel încât să puteți autentifica orice certificate server pe care le emite CA.

Atunci când accesați un server care folosește o conexiune SSL (Secure Sockets Layer), serverul va prezenta software-ului client un certificat ca dovadă a identității sale. Software-ul client trebuie mai apoi să valideze certificatul server-ului înainte ca acesta să poată stabili o sesiune. Pentru a se valida certificatul server, software-ul client trebuie să aibă acces la o copie stocată local a certificatului pentru CA (autoritatea de certificare) care a emis certificatul server. Dacă serverul prezintă un certificat de la un CA public din Internet, browser-ul dumneavoastră sau alt software client ar putea avea deja o copie a certificatului CA. Însă dacă serverul prezintă un certificat de la un CA local privat, trebuie să folosiți Digital Certificate Manager (DCM) pentru a obține o copie a certificatului CA local.

Puteți folosi DCM pentru a descărca certificatul CA local direct în browser-ul dumneavoastră sau puteți copia certificatul CA local într-un fișier astfel încât alt software client să-l poată și folosi. Dacă folosiți atât browser-ul dumneavoastră cât și alte aplicații pentru comunicații securizate, s-ar putea să trebuiască să folosiți ambele metode pentru a instala certificatul CA local. Dacă folosiți ambele metode, instalați certificatul în browser înainte de a-l copia într-un fișier.

Aflați cum să obțineți o copie a certificatului CA privat și instalați-l pe PC-ul dumneavoastră astfel încât să puteți autentifica orice certificate server pe care le emite CA.

Pentru a folosi DCM ca să obțineți o copie a certificatului CA local, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, selectați **Instalare certificat CA local pe PC-ul dumneavoastră** pentru a afișa o pagină care vă permite să descărcați certificatul CA local în browser-ul dumneavoastră sau să-l memorați într-un fișier pe sistemul dumneavoastră.
3. Selectați o metodă pentru obținerea certificatului CA local.
 - a. Selectați **Instalare certificat** pentru a descărca certificatul CA local ca o rădăcină de încredere în browser-ul dumneavoastră. Astfel vă veți asigura că browser-ul poate stabili sesiuni de comunicații sigure cu serverele care folosesc un certificat provenind de la acest CA. Browser-ul va afișa o serie de ferestre care vă vor ajuta să termina instalarea.
 - b. Selectați **Copiere și lipire certificat** pentru a afișa o pagină care conține o copie codată special a certificatului CA local. Se copiază obiectul text din pagină în clipboard. Mai târziu trebuie să lipiți (paste) aceste informații într-un fișier. Acest fișier 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 aplicațiile dumneavoastră client să poată recunoaște și folosi certificatul CA local pentru autentificare, trebuie să configurați aplicațiile să recunoască certificatul ca o rădăcină de încredere. Urmați instrucțiunile pe care vi le furnizează aceste aplicații pentru a folosi fișierul.
4. Apăsați **OK** pentru a reveni la pagina de bază (home) a Digital Certificate Manager.

Concepte înrudite

“Gestionarea certificatelor utilizator” la pagina 40

Puteți folosi DCM (Digital Certificate Manager) pentru a obține certificate cu SSL sau asocierea certificatelor existente cu profilurile de utilizator iSeries.

Operații înrudite

“Crearea și lucrul cu un CA local” la pagina 39

Folosiți această informație pentru a învăța cum să creați și operați CA pentru a emite certificate private pentru aplicații.

“Crearea unui certificat utilizator” la pagina 41

Folosiți aceste informații pentru a afla cum pot utilizatorii să folosească CA-ul local pentru a emite un certificat pentru autentificarea clientului.

Gestionarea certificatelor de pe un CA Internet public

Folosiți această informație pentru a gestiona certificate provenite de la un CA public din Internet, trebuie să creați mai întâi un depozit de certificate.

După ce v-ați revăzut atent nevoile și politicile de securitate, ați decis că doriți să folosiți certificate de la un CA public din Internet, cum ar fi VeriSign. De exemplu, operați un sit Web public și vreți să folosiți SSL (Secure Sockets Layer) pentru sesiuni de comunicație sigure pentru a asigura protejarea anumitor tranzacții de informații. Din cauză că situl Web este disponibil publicului larg, vreți să folosiți certificate pe care majoritatea browser-elor Web le recunosc la citire.

Sau, dezvoltați aplicații pentru clienți externi și doriți să folosiți un certificat public pentru a semna digital pachetele aplicației. Prin semnarea pachetelor aplicației, clienții vor putea fi siguri de faptul că pachetul provine de la compania dumneavoastră și că nu a fost alterat de alte părți neautorizate în timpul tranzitului. Doriți să folosiți un certificat public astfel încât clienții să poată verifica ușor și necostisitor semnătura digitală a pachetului. De asemenea, puteți folosi acest certificat pentru a verifica semnătura înainte de a trimite pachetul clienților.

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

Gestionare certificate publice

Atunci când folosiți DCM pentru a gestiona certificate provenite de la un CA public din Internet, trebuie să creați mai întâi un depozit de certificate. Un depozit de certificate este un fișier bază de date de chei special pe care îl folosește

DCM (Digital Certificate Manager) pentru a stoca certificate digitale și cheile lor private asociate. DCM vă permite să creați și să gestionați mai multe tipuri de depozite de certificate pe baza certificatelor pe care le conțin.

Tipul de depozit de certificate pe care l-ați creat și task-urile pe care trebuie să le efectuați ulterior pentru gestionarea certificatelor și a aplicațiilor care le folosesc, depinde de modul în care doriți să folosiți certificatele.

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

Pentru a afla cum să folosiți DCM pentru a crea depozitul de certificate corespunzător și pentru a gestiona certificatele Internet necesare aplicațiilor, revedeți aceste subiecte:

Concepte înrudite

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

Operații înrudite

“Gestionarea locației cerute pentru un PKIX CA” la pagina 69

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 Internet publice pentru sesiunile de comunicare SSL:

Puteți folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele publice Internet pe care aplicațiile le folosesc pentru a stabili sesiuni de comunicare sigure cu SSL (Secure Sockets Layer).

Dacă nu folosiți DCM pentru a lucra cu CA-ul dumneavoastră local, trebuie să creați întâi depozitul corespunzător pentru certificate pentru gestionarea certificatelor publice pe care le folosiți pentru SSL. Aceasta este depozitul de certificate *SYSTEM. Atunci când creați un depozit de certificate, DCM vă conduce prin procesul de creare a informațiilor de cerere a certificatului pe care trebuie să le furnizați Autorității de certificare publice pentru a obține un certificat.

Pentru a folosi DCM pentru a administra și folosi certificate publice Internet pentru ca aplicațiile să poată stabili sesiuni de comunicare SSL, urmați acești pași:

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

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

3. Selectați ***SYSTEM** ca depozit de certificate pentru creare și apăsați **Continuare**.
4. Selectați **Da** pentru a crea un certificat ca parte a creării depozitului de certificate *SYSTEM și apăsați **Continuare**.
5. Selectați **VeriSign sau altă CA Internet (autoritate de certificare)** ca semnatar al noului certificat și efectuați un clic pe **Continuare** pentru a se afișa un formular care vă va permite să introduceți informații de identificare pentru noul certificat.

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

6. Completați formularul și apăsați **Continuare** pentru a se afișa pagina de confirmare. Această pagină de confirmare va afișa datele cererii certificatului pe care trebuie să îl furnizați Autorității de certificare publice care va emite certificatul. Datele CSR (cerere de semnare a certificatului) consistă în cheia publică și alte informații pe care le specificați pentru noul certificat.
7. Copiați cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fișier separat, pe care îl solicitați CA public pentru cererea unui certificat. Trebuie să folosiți toate datele CSR, inclusiv liniile Begin și End New Certificate Request. Atunci când părăsiți această pagină, datele vor fi pierdute și nu se vor mai putea recupera. Trimiteți formularul sau fișierul aplicației către CA aleasă pentru emiterea și semnarea certificatului.

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

Pentru a folosi certificate cu serverul HTTP pentru sistemul dumneavoastră, trebuie să creați și să configurați serverul dumneavoastră Web înainte de a gestiona DCM pentru a lucra cu certificatul complet semnat. Când configurați un server Web să folosească SSL, este generat un ID aplicație pentru server. Trebuie să faceți o notă a acestui ID aplicație astfel încât să folosiți DCM pentru a specifica care certificat trebuie să fie utilizat de această aplicație pentru SSL.

Nu terminați și reporniți serverul până nu folosiți DCM să aloce certificatul complet semnat către server. Dacă opriți și reporniți instanța *ADMIN a serverului Web înainte de a-i aloca un certificat, serverul nu va porni și nu veți putea folosi DCM pentru a aloca un certificat serverului.

8. Porniți DCM după ce CA publică vă întoarce certificatul semnat.
9. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați *SYSTEM pentru ca să se deschidă depozitul de certificate.
10. Când este afișată pagina Depozit de certificate și Parola, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și apoi apăsați **Continuare**.
11. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
12. Din lista de task-uri, selectați **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate *SYSTEM. După ce terminați de importat certificatul, puteți specifica aplicațiile care trebuie să-l folosească pentru comunicații SSL.
13. În cadrul de navigare, selectați **Gestionarea aplicațiilor** pentru a afișa o listă de task-uri.
14. Din lista de task-uri, selectați **Actualizarea atribuirii certificatelor** pentru a se afișa o listă de aplicații activate-SSL pentru care puteți atribui un certificat.
15. Selectați din listă o aplicație și efectuați un clic pe **Actualizarea atribuirii certificatelor**.
16. Selectați certificatul pe care l-ați importat și efectuați un clic pe **Atribuirea noului certificat**. DCM va afișa un mesaj pentru a confirma selecția certificatului pentru aplicație.

Notă: Unele aplicații activate-SSL suportă identificarea clientului pe baza certificatelor. Dacă doriți ca o aplicație cu acest suport să poată să autentifice certificate înainte de a accesa resursele, trebuie să definiți o listă de încredere CA pentru aplicație. Acest lucru asigură faptul că aplicația poate valida doar acele certificate care provin de la CA-uri pe care le-ați specificat ca fiind de încredere. Dacă o aplicație 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, aplicația nu îl va accepta ca bază a unei autentificări valide.

Atunci când terminați task-ul asistat, sunteți gata să începeți configurarea aplicațiilor pentru a folosi SSL pentru comunicațiile securizate. Înainte ca utilizatorii să poată accesa aceste aplicații 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 obțină certificatul CA, trebuie să acceseze situl Web pentru CA și să urmeze instrucțiunile pe care acesta le furnizează.

Gestionarea certificatelor Internet publice pentru semnarea obiectelor:

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

Dacă nu folosiți DCM pentru a opera propriul dumneavoastră CA (Certificate Authority) local, trebuie mai întâi să creați un depozit de certificate corespunzător pentru gestionarea certificatelor publice pe care le folosiți pentru semnarea obiectelor. Acesta este depozitul de certificate *OBJECTSIGNING. Când creați un depozit de certificate, DCM vă trece prin procesul creării informațiilor de cerere a unui certificat pe care trebuie să le furnizați către CA Internet publică pentru a obține un certificat.

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

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

1. Porniți DCM.
2. În cadrul de navigație stâng al DCM, selectați **Creare depozit de certificate nou** pentru a porni task-ul ghidat și a efectua o serie de formulare. Aceste formulare vă vor ghida prin procesul de creare a unui depozit de certificate și a unui certificat pe care aplicațiile le pot folosi pentru semnarea obiectelor.

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

3. Selectați ***OBJECTSIGNING** drept depozitul de certificate de creat și faceți clic pe **Continuare**.
4. Selectați **Da** pentru a crea un certificat ca parte a creării depozitului de certificate și apăsați **Continuare**.
5. Selectați **VeriSign sau altă CA Internet (autoritate de certificare)** ca semnatar al noului certificat și efectuați un clic pe **Continuare**. Astfel se va afișa un formular care vă va permite să introduceți informații de identificare pentru noul certificat.
6. Completați formularul și apăsați **Continuare** pentru a se afișa pagina de confirmare. Această pagină de confirmare va afișa datele cererii certificatului pe care trebuie să îl furnizați Autorității de certificare publice care va emite certificatul. Datele CSR (cerere de semnare a certificatului) consistă în cheia publică și alte informații pe care le specificați pentru noul certificat.
7. Copiați cu grijă datele CSR în formularul de aplicare al certificatului, sau într-un fișier separat, pe care îl solicita CA public pentru cererea unui certificat. Trebuie să folosiți toate datele CSR, inclusiv liniile Begin și End New Certificate Request. Atunci când părăsiți această pagină, datele vor fi pierdute și nu se vor mai putea recupera. Trimiteți formularul sau fișierul aplicației către CA aleasă pentru emiterea și semnarea certificatului.

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

8. Porniți DCM după ce CA publică vă întoarce certificatul semnat.
9. În cadrul de navigație stâng, faceți clic pe **Selectare depozit de certificate** și selectați ***OBJECTSIGNING** ca depozitul de certificate care va fi deschis.
10. Când este afișată pagina Depozit de certificate și Parola, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și apoi apăsați **Continuare**.
11. În fereastra de navigare, selectați **Gestionare certificate** pentru a afișa o listă a task-urilor.
12. Din lista de task-uri, selectați **Importarea unui certificat** pentru a începe procesul de importare a certificatului semnat în depozitul de certificate ***OBJECTSIGNING**. După ce se termină importarea certificatului, puteți crea o definiție de aplicație care să folosească certificatul pentru semnarea obiectelor.
13. După ce cadrul de navigare din stânga se reîmprospătează, selectați **Gestionare aplicații** pentru a afișa o listă a task-urilor.
14. Din lista de task-uri, selectați **Adăugarea aplicației** pentru a începe procesul de creare a unei definiții aplicație care semnează obiecte pentru a folosi certificatul în semnarea obiectelor.

15. Completați formularul pentru a defini aplicația care semnează obiecte și efectuați un clic pe **Adăugare..** Această definiție aplicație nu descrie o aplicație reală, ci mai degrabă tipul de obiecte pe care doriți să le formați cu un anume certificat. Folosiți ajutorul online pentru a afla cum să completați formularul.
16. Selectați **OK** pentru a recunoaște mesajul de confirmare al definiției aplicație și pentru a afișa lista de task-uri Gestionarea aplicațiilor.
17. Din lista de task-uri, selectați **Actualizare alocare certificate** și apăsați **Continuare** pentru a afișa o listă de ID-uri de aplicații de semnare obiecte pentru care puteți alocă un certificat.
18. Selectați din listă o aplicație și efectuați un clic pe **Actualizarea atribuirii certificatelor**.
19. Selectați certificatul pe care l-ați importat și efectuați un clic pe **Atribuirea noului certificat**.

Când terminați aceste task-uri, aveți tot ce vă trebuie pentru a începe semnarea obiectelor pentru a le asigura integritatea.

Când distribuiți 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 și pentru a verifica identitatea expeditorului. Pentru validarea semnăturii, destinatarul trebuie să aibă o copie a certificatului de verificare a semnăturii. Trebuie să furnizați 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-ați folosit pentru semnarea obiectului. Dacă ați semnat obiectele cu un certificat de la un CA binecunoscut, versiunea DCM a receptorului ar putea avea deja o copie a certificatului CA necesar. Totuși, ați putea furniza o copie a certificatului CA împreună cu obiectele semnate dacă vă gândiți că receptorul s-ar putea să nu aibă o copie. De exemplu, trebuie să furnizați o copie a certificatului CA local dacă ați semnat obiectele cu un certificat de la un CA local privat. Din motive de securitate, trebuie să furnizați certificatul CA într-un pachet separat sau să faceți public certificatul CA disponibil la cererea tuturor celor care au nevoie de el.

Concepte înrudite

“CertIFICATELE digitale pentru semnarea obiectelor” la pagina 35

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticității sale.

Gestionarea certificatelor pentru verificarea semnăturii obiectelor:

Puteți folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele de verificare a semnăturilor obiectelor pe care le folosiți pentru a valida semnăturile digitale ale obiectelor.

Pentru a semna un obiect, folosiți cheia privată a certificatului pentru a crea semnătura. Atunci când trimiteți altora obiectul semnat, trebuie să includeți o copie a certificatului care a semnat obiectul. Acest lucru îl puteți face folosind DCM pentru a exporta certificatul de semnare a obiectelor (fără cheia privată a certificatului) drept certificat de verificare a semnăturii. Puteți exporta un certificat de verificare a semnăturii într-un fișier pe care puteți mai apoi să îl distribuiți. Sau, dacă doriți să verificați semnăturile pe care le-ați creat, puteți exporta un certificat de verificare a semnăturilor în depozitul de certificate *SIGNATUREVERIFICATION.

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

De asemenea, trebuie să aveți o copie a certificatului CA (autoritate de certificare) pentru CA care a emis certificatul care a semnat obiectul. Folosiți certificatul CA pentru a verifica autenticitatea certificatului care a semnat obiectul. DCM oferă copii de certificate CA de la cele mai cunoscute CA-uri. Dacă însă obiectul a fost semnat de un certificat de la alt CA public sau de la un CA local privat, trebuie să obțineți o copie a certificatului CA înainte să puteți verifica semnătura obiectului.

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

Notă: Dacă doriți să puteți verifica semnăturile pe care le-ți creat cu propriile certificate de semnarea a obiectelor, trebuie să creați depozitul de certificate *SIGNATUREVERIFICATION și să copiați certificatele din depozitul de certificate *OBJECTSIGNING în el. Acest lucru este adevărat chiar dacă vreți să efectuați verificarea semnăturilor din depozitul de certificate *OBJECTSIGNINGe.

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

1. Porniți DCM.
2. În cadrul de navigație stâng al DCM, selectați **Creare depozit de certificate nou** pentru a porni task-ul ghidat și a efectua o serie de formulare.

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

3. Selectați *SIGNATUREVERIFICATION drept depozitul de certificate de creat și faceți clic pe **Continuare**.

Notă: Dacă există depozitul de certificate *OBJECTSIGNING, DCM vă va cere în acest punct să specificați dacă să copieze certificatele care semnează obiecte în noul depozit de certificate ca certificate de verificare a semnăturilor. Dacă vreți să folosiți certificatele de semnare obiect existente pentru a verifica semnăturile, selectați **Da** și faceți clic pe **Continuare**. Trebuie să cunoașteți parola depozitului de certificate *OBJECTSIGNING pentru a copia certificatele din el.

4. Specificați o parolă pentru noul depozit de certificate și apăsați **Continuare** pentru a crea depozitul de certificate. Va apare o pagină de confirmare pentru a indica succesul creării depozitului de certificate. Acum puteți folosi depozitul pentru a gestiona certificatele și pentru a verifica semnăturile obiectelor.

Notă: Dacă ați creat depozitul pentru a putea verifica semnăturile obiectelor pe care le-ați semnat, vă puteți opri. Pe măsură ce creați certificate noi de semnare obiecte, trebuie să le exportați din depozitul de certificate *OBJECTSIGNING în acest depozit. Dacă nu le exportați, nu veți putea verifica semnăturile pe care le-ați creat cu ele. Dacă ați creat acest depozit de certificate astfel încât să puteți verifica semnăturile de pe obiecte pe care le-ați primit din alte surse, trebuie să continuați cu această procedură astfel încât să puteți importa certificatele de care aveți nevoie în depozit.

5. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați *SIGNATUREVERIFICATION pentru ca să se deschidă depozitul de certificate.
6. Când este afișată pagina Depozit de certificate și Parola, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și apoi apăsați **Continuare**.
7. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
8. Din lista de task-uri, selectați **Importare certificate**. Acest task vă îndrumă prin procesul importării certificatelor de care aveți nevoie în depozitul de certificate pentru a putea verifica semnătura de pe obiectele pe care le-ați primit.
9. Selectați tipul de certificat pe care doriți să îl importați. Selectați **Verificare semnături** pentru a importa certificatul pe care l-ați primit împreună cu obiectele semnate și pentru a încheia task-ul import.

Notă: Dacă depozitul de certificate nu conține deja o copie a certificatului CA pentru CA-ul care a emis certificatul de verificare semnături, trebuie să importați certificatul CA mai *întâi*. Ați putea primi o eroare dacă nu importați certificatul CA înainte de importarea certificatului de verificare a semnăturii.

Puteți folosi aceste certificate pentru a verifica semnăturile obiectelor.

Concepte înrudite

“CertIFICATELE DIGITALE PENTRU SEMNAREA OBIECTELOR” LA PAGINA 35

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticității sale.

Operații înrudite

“Verificarea semnăturii obiecte” la pagina 72

Puteți folosi DCM (Digital Certificate Manager) pentru a verifica autenticitatea semnăturilor digitale pentru obiecte.

Când verificați semnătura, vă asigurați 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 folosește DCM (Digital Certificate Manager) variază în funcție de tipul CA-ului care a emis certificatul.

Puteți reînnoi un certificat cu un CA local sau cu un CA Internet.

Reînnoirea unui certificat din CA-ul local

Dacă folosiți CA-ul local pentru a semna certificatul reînnoit, DCM folosește informațiile pe care le furnizați pentru a crea un nou certificat în depozitul curent de certificate și reține certificatul anterior.

Pentru reînnoirea unui certificat cu un CA local urmăriți pașii:

1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate**, și selectați depozit de certificate pe care să-l deschideți.
2. În cadrul de navigare, selectați **Gestionare certificate**.
3. În cadrul de navigare, selectați **Reînnoire certificate**.
4. Selectați certificatul pe care doriți să îl reînnoiți și selectați **Reînnoire**.
5. Selectați **CA local** și faceți clic pe **Continuare**.
6. Completați formularul identificare certificat. Trebuie să schimbați câmpul **Etichetă de certificat nouă** dar orice alte câmpuri pot rămâne la fel.
7. Selectați orice aplicație căruia doriți să îi reînnoiți certificatul și faceți clic pe **Continuare** pentru a termina reînnoirea certificatului.

Notă: Nu trebuie să selectați o aplicație pentru a folosi certificatul.

Reînnoirea unui certificat din CA-ul Internet

Dacă utilizați un CA din Internet binecunoscut pentru a emite certificatul, puteți trata reînnoirea certificatului în unul din cele două moduri: să importați certificatul reînnoit dintr-un fișier pe care îl primiți de la CA de semnare sau să puneți DCM-ul să creeze o nouă pereche de chei publică-privată pentru certificat.

Puteți reînnoi un certificat direct cu CA-ul Internet și apoi să importați certificatul reînnoit din fișierul pe care l-ați primit de la CA-ul de semnare. Sau puteți folosi DCM pentru a crea o pereche noua cheie publică-privată și CSR pentru certificate și apoi trimiteți această informație la CA de Internet pentru a obține un nou certificat. Când primiți înapoi certificatul de la CA, atunci puteți termina procesul de reînnoire.

Importarea și reînnoirea unui certificat obținut direct de la CA-ul de internet:

Pentru importarea și reînnoirea unui certificat obținut direct de la Internet CA, urmăriți pași:

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

Notă: Faceți clic pe butonul ? pentru orice panou de răspuns la orice panou de întrebări, aveți despre completarea panourilor.

2. În cadrul de navigare, selectați **Gestionare certificate**.
3. În cadrul de navigare, selectați **Reînnoire certificate**.

- | 4. Selectați certificatul pe care doriți să îl reînnoiți și selectați **Reînnoire**.
- | 5. Selectați **VeriSign** alt **CA Internet** și efectuați un clic pe **Continuare**.
- | 6. Selectați **Nu - Importați certificatul nou semnat din fișierul existent**.
- | 7. Completați ghidurile pentru a importa certificatul. Când alegeți să reînnoiți certificatul direct cu CA emis, CA reutnează certificatul reînnoit într-un fișier. Fiți siguri că ați specificat calea absolut corectă unde certificatul este memorat pe server. Fișierul care conține certificatul reînnoit poate fi memorat într-un director IFS (integrated file system).
- | 8. Apăsați **OK** pentru a termina task-ul.

| **Reînnoiți certificatul prin crearea unei chei publice-privată și CSR pentru certificat:**

| Pentru a reînnoi un certificat cu un CA Internet prin crearea unei noi perechi cheie publică-privată și CSR pentru certificat, urmați acești pași:

- | 1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate**, și selectați depozit de certificate pe care să-l reînnoiți.

| **Notă:** Faceți clic pe butonul ? pentru orice panou de răspuns la orice panou de întrebări, aveți despre completarea panourilor.

- | 2. În cadrul de navigare, selectați **Gestionare Certificate**.
- | 3. În cadrul de navigație, selectați **Reînnoire certificat**
- | 4. Selectați certificatul pe care doriți să îl reînnoiți și selectați **Reînnoire**.
- | 5. Selectați **VeriSign** altă **CA Internet (autoritate de certificare)** și efectuați un clic pe **Continuare**.
- | 6. Faceți clic pe **Da - Creează o nouă pereche cheie pentru acest certificat și apăsați Continuare**.
- | 7. Completați formularul identificare certificat. Trebuie să schimbați eticheta Certificat Nou, dar celelalte câmpuri pot rămâne la fel. **Notă:** Faceți clic pe butonul ? pentru orice panou de răspuns la orice panou de întrebări, aveți despre completarea panourilor.
- | 8. Apăsați **OK** pentru a termina task-ul.

| **Importarea unui certificat**

| Citiți aceste informații pentru a învăța cum să folosiți DCM pentru a importa certificate care sunt localizate pe serverul dumneavoastră.

| Puteți de asemenea să importați un certificat din alt server în loc să recreați certificatul pe serverul curent. De exemplu, pe iSeries A ați folosit CA-ul local pentru a crea certificate pentru aplicația web de retail pentru a le folosi la inițierea conexiunilor SSL. Afacerea dumneavoastră a crescut recent și ați instalat un nou server iSeries (iSeries B) pentru a găzdui mai multe instanțe a acestei aplicații de retail foarte solicitate. Dumneavoastră doriți ca toate instanțele aplicației retail să folosească certificate identice pentru identificarea lor și să inițieze conexiuni SSL. După aceea ați putea decide să importați atât certificatul CA local, cât și certificatul server de la iSeries A la iSeries B, în loc să folosiți CA local de pe iSeries A pentru a crea un nou certificat diferit pentru iSeries B.

| Parcurgeți următorii pași pentru a utiliza DCM:

- | 1. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați depozitul de certificate pe care să-l deschideți. Certificatul memorat în care importați trebuie să conțină certificate de același tip ca certificatele exportate pe alte sisteme. De exemplu, dacă importați un certificat de server atunci importați-l într-un depozit de certificate care conține certificate de server cum ar fi *SYSTEM sau Alt depozit sistem de certificate.
- | 2. În cadrul de navigare, selectați **Gestionare certificate**.
- | 3. În cadrul de navigare, selectați **Import certificate**.
- | 4. Selectați tipul de certificat pe care doriți să-l importați și apăsați **Continuare**. Tipul de certificat pe care îl importați trebuie să fie de același tip cu certificatul exportat. De exemplu, dacă ați exportat un certificat server selectați să importați un certificat server.

- | **Notă:** Când DCM exportă un certificat în format pkcs12, CA emitent este inclus în lanțul de certificatele exportate
| și este, deci, automat importat când însuși certificatul este importat de DCM în depozitul de certificate.
| Totuși, dacă certificatul nu este exportat în format pkcs12 și nu doriți să aveți în depozitul de certificate un
| certificat CA, trebuie să importați certificatul CA-ului emitent înainte de a importa certificatul.
- | 5. Completați task-urile asistate pentru a importa certificatul. Când importați certificatul fiți sigur că ați specificat
| calea absolut corect unde certificatul este depozitat pe server.

Gestionarea DCM

Folosiți aceste informații pentru a învăța să folosiți DCM pentru gestionarea certificatelor și a aplicațiilor care le folosesc. De asemenea, puteți învăța cum să semnați digital obiecte și cum să creați și să operați propriile Autorități de certificare.

După ce ați configurat DCM, trebuie în timp să mai realizați niște task-uri de gestiune certificate. Pentru a afla cum să folosiți DCM pentru a vă gestiona certificatele dumneavoastră, revedeți aceste subiecte:

Utilizarea CA local pentru a emite certificate pentru alte sisteme iSeries

Aflați cum se folosește un CA local privat de pe un sistem pentru a emite certificate folosite pe alte sisteme. iSeries.

Este posibil să folosiți deja un CA local privat pe un sistem din rețea. Acum, doriți să extindeți folosirea acestui CA local la alt sistem din rețeaua dumneavoastră. De exemplu, doriți să faceți CA-ul local curent să emită certificate de server sau de client pentru ca o aplicație de pe alt sistem să folosească sesiuni de comunicație SSL. Sau doriți să folosiți certificate de la CA-ul dumneavoastră local de pe un sistem pentru semnarea obiectelor pe care le aveți stocate pe alt server.

Acest obiectiv poate fi atins folosind DCM (administratorului de certificate digitale) Executați unele task-uri pe serverul pe care operează CA-ul local și executați altele pe serverul secundar, care găzduiește aplicațiile pentru care doriți să emiteți certificate. Acest sistem secundar este denumit sistemul destinație. Task-urile pe care trebuie să le realizați pe sistemul destinație depind de versiunea acelu sistem.

Notă: Pot apărea probleme dacă serverul pe care operează CA-ul local folosește un produs Cryptographic Access Provider care asigură o criptare mai puternică decât sistemul destinație. Pentru OS/400 V5R2 și OS/400 V5R3 singurul furnizor de acces criptografic este 5722-AC3, care este cel mai puternic produs disponibil. Totuși, în edițiile anterioare, puteați instala alte produse de furnizare de acces criptografic mai slabe (5722-AC1 sau 5722-AC2) care furnizau funcții criptografice de nivel mai slab. Când exportați certificatul (cu cheia sa privată), sistemul criptează fișierul pentru a-i proteja conținutul. Dacă sistemul folosește un produs criptografic mai puternic decât sistemul destinație, acesta nu va putea decodifica fișierul în timpul procesului de import. În consecință, importul poate eșua sau s-ar putea ca certificatul să nu poată fi folosit pentru stabilirea de sesiuni SSL. Acest lucru este adevărat chiar dacă folosiți o dimensiune a cheii pentru noul certificat care este potrivită pentru a fi folosită împreună cu produsul criptografic de pe sistemul destinație.

Puteți folosi CA-ul dumneavoastră local pentru a emite certificate către alte sisteme, pe care puteți să le folosiți apoi pentru semnarea obiectelor sau să puneți aplicațiile să le folosească pentru stabilirea sesiunilor SSL. Când folosiți CA-ul local pentru a crea un certificat ce este folosit pe alt sistem, fișierele pe care le creează DCM conțin o copie a certificatului CA local, precum și copii ale certificatelor pentru numeroase CA-uri publice din Internet.

Task-urile pe care trebuie să le realizați în DCM diferă puțin în funcție de tipul de certificat pe care CA-ul dumneavoastră local îl emite și de versiunea și de condițiile de pe sistemul destinație.

Emiterea certificatelor private pentru utilizarea pe alt sistem iSeries

Pentru a folosi CA-ul local la emiterea certificatelor folosite pe un alt sistem, parcurgeți pașii următori pe sistemul care găzduiește CA-ul local:

1. Pornire DCM

2. În cadrul de navigare, selectați **Creare certificat** pentru a afișa o listă de tipuri de certificate pe care le puteți crea folosind CA-ul local.

Notă: Nu este nevoie să deschideți un depozit de certificate pentru a realiza acest task. Aceste instrucțiuni presupun fie că nu lucrați în cadrul unui depozit de certificate specific, fie că lucrați în depozitul de certificate Autoritate de certificare (CA) local. Pentru a realiza aceste task-uri, trebuie să existe un CA local pe acest sistem. Dacă aveți întrebări despre completarea unui anume formular care este în task-ul asistat, selectați semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.

3. Selectați tipul de certificat pe care doriți să îl emiți CA-ul local și apăsați **Continuare** pentru a porni task-ul asistat și completați o serie de formulare.
4. Selectați crearea unui **certificat de server sau de client pentru alt sistem iSeries** (pentru sesiuni SSL), sau a unui **certificat de semnare a obiectelor iSeries** pentru alt sistem.

Notă: Când creați un certificat de semnare a obiectelor pentru a fi folosit de alt sistem, pe sistemul respectiv trebuie să ruleze OS/400 V5R1 sau o versiune ulterioară de a folosi certificatul. Deoarece sistemul destinație trebuie să aibă OS/400 V5R1 sau mai recentă, DCM de pe sistemul gazdă local nu vă cere să selectați un format de eliberare destinație pentru noul certificat de semnare obiecte.

5. Completați formularul și apăsați **Continuare** pentru a se afișa pagina de confirmare.

Notă: Dacă există un depozit de certificate *OBJECTSIGNING sau *SYSTEM pe sistemul destinație, asigurați-vă că ați specificat o etichetă unică pentru certificat ca și un nume de fișier unic pentru acesta. Specificarea unei etichete unice și a unui nume de fișier unic pentru certificat vă asigură de faptul că puteți importa mai ușor certificatul într-un depozit de certificate de pe sistemul destinație. Această pagină de confirmare afișează numele fișierelor create de DCM pentru a fi transferate pe sistemul destinație. DCM creează aceste fișiere pe baza nivelului de ediție al sistemului destinație pe care l-ați specificat. DCM pune automat o copie a certificatului CA local în aceste fișiere.

DCM creează noul certificat în depozitul de certificate propriu și generează două fișiere pentru ca dumneavoastră să le transferați: un fișier de depozit de certificate (extensia (.KDB și un fișier cerere (extensia .RDB).

6. Folosiți Protocolul de transfer al fișierelor în binar (FTP) sau altă metodă pentru a transfera fișierele pe sistemul destinație.

Concepte înrudite

“Considerentele despre salvarea de rezervă și recuperarea datelor DCM” la pagina 27

Folosiți aceste informații pentru a afla cum să asigurați că datele DCM importante sunt adăugate la salvarea de rezervă și planul de recuperare pentru sistemul dumneavoastră.

“Certificate publice contra certificate private” la pagina 29

Folosiți aceste informații pentru a învăța cum să determinați ce tip de certificate se potrivește cel mai bine cu nevoile dumneavoastră după ce decideți cum doriți să folosiți certificatele pentru a profita de securitatea adițională pe care o oferă.

Operații înrudite

“Crearea și lucrul cu un CA local” la pagina 39

Folosiți această informație pentru a învăța cum să creați și operați CA pentru a emite certificate private pentru aplicații.

Folosirea certificatului privat pentru sesiuni SSL

Certificatele folosite de aplicații pentru sesiuni SSL din depozitul de certificate *SYSTEM sunt gestionate în DCM (Digital Certificate Manager). Dacă nu ați folosit niciodată DCM pe sistemul destinație V5R1 pentru a gestiona certificate pentru SSL, atunci acest depozit de certificate nu va exista pe sistemul destinație.

Task-urile pentru folosirea fișierelor depozitului de certificate transferate pe care le-ați creat pe sistemul gazdă CA local depind de situația dacă depozitul de certificate *SYSTEM există. Dacă depozitul de certificate *SYSTEM nu există, puteți folosi fișierele certificatelor transferate ca un mijloc de creare a depozitului de certificate *SYSTEM. Dacă

depozitul de certificate *SYSTEM nu există pe sistemul destinație puteți ori să folosiți fișierele transferate ca Depozit de certificate pe alt sistem sau importați fișierele transferate în depozitul de certificate *SYSTEM.

Depozitul de certificate *SYSTEM nu există:

Dacă depozitul de certificate *SYSTEM nu există pe sistemul V5R1 pe care doriți să folosiți fișierele depozit de certificate transferate, le puteți folosi ca depozit de certificate *SYSTEM. Pentru a crea depozitul de certificate *SYSTEM și a folosi fișierele certificate pe sistemul dumneavoastră destinație V5R3 sau V5R2, urmați acești pași:

1. Asigurați-vă că fișierele depozitului de certificate (două fișiere: unul cu extensia .KDB și unul cu extensia .RDB) pe care le-ați creat pe sistemul care găzduiește CA-ul local sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER.
2. O dată ce fișierele certificatelor transferate sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , redenumiți aceste fișiere în DEFAULT.KDB și DEFAULT.RDB. Redenumind aceste fișiere în catalogul corespunzător, creați componentele care conțin depozitul de certificate *SYSTEM pentru sistemul destinație. Depozitul de certificate conține deja copii de certificate pentru multe CA publice Internet. DCM a adăugat acestea, cât și o copie a certificatului CA local, la fișierele depozitului de certificate când le-ați creat.

Atenție: Dacă sistemul dumneavoastră destinație are deja un fișier DEFAULT.KDB și unul DEFAULT.RDB în catalogul /QIBM/USERDATA/ICSS/CERT/SERVER , depozitul de certificate *SYSTEM există pe acest sistem destinație. În consecință, nu trebuie să redenumiți fișierele transferate așa cum a fost sugerat. Suprascierea fișierelor implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat și a conținutului său. În schimb, trebuie să vă asigurați că au nume unice și trebuie să utilizați depozitul de certificate transferat ca un **alt depozit de certificate sistem**. Dacă folosiți fișierele ca un alt depozit de certificate sistem, nu puteți utiliza DCM pentru a specifica care aplicații vor folosi certificatul.

3. Porniți DCM. Trebuie să schimbați acum parola pentru depozitul de certificate *SYSTEM pe care l-ați creat prin redenumirea fișierelor transferate. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dumneavoastră să puteți folosi toate funcțiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.
4. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați *SYSTEM pentru ca să se deschidă depozitul de certificate.
5. Când este afișată pagina Depozit de certificate și parolă, furnizați parola pe care ați specificat-o pe sistemul *gazdă* pentru depozitul de certificate când ați creat certificatul pentru sistemul destinație V5R3 sau V5R2 și faceți clic pe **Continuare**.
6. În cadrul de navigare, selectați **Gestionarea depozitelor de certificate** și selectați **Modificarea parolei** din lista de task-uri. Completați formularul pentru a modifica parola pentru depozitul de certificate. După ce modificați parola, trebuie să redeschideți depozitul de certificate înainte de a putea lucra cu certificatele din el. Apoi puteți specifica care aplicații vor folosi certificatul pentru sesiuni SSL.
7. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați *SYSTEM pentru ca să se deschidă depozitul de certificate.
8. Când este afișată pagina **Depozit de certificate și parolă**, furnizați noua parolă și faceți clic pe **Continuare**.
9. După ce se reafixează cadrul de navigare, selectați **Gestionare certificate** din cadrul de navigație pentru a afișa o listă de task-uri.
10. Din lista de task-uri, selectați **Alocare Certificat** pentru a afișa o listă de certificate din depozitul curent de certificate.
11. Selectați certificatul pe care l-ați creat pe sistemul *gazdă* și apăsați **Alocare la aplicații** pentru a afișa o listă de aplicații activate-SSL la care puteți alocă certificatul.
12. Selectați aplicațiile care vor folosi certificatul pentru sesiuni SSL și faceți clic pe **Continuare**. DCM afișează un mesaj pentru a confirma selecția certificatului dumneavoastră pentru aplicații.

Notă: Unele aplicații activate-SSL suportă identificarea clientului pe baza certificatelor. O aplicație cu acest suport trebuie să poată să autentifice certificate înainte de a acorda accesul la resurse. În consecință, trebuie să definiți o listă de încredere CA pentru aplicație. Acest lucru asigură faptul că aplicația poate valida doar acele certificate care provin de la CA-uri pe care le-ați specificat ca fiind de încredere. Dacă utilizatorii sau

o aplicație client prezintă un certificat care provine de la un CA care nu este specificat ca fiind de încredere în lista de încredere CA, aplicația nu îl va accepta ca bază pentru o autentificare validă.

Cu aceste task-uri completate, aplicațiile de pe sistemul destinație pot folosi certificatul emis de CA local de pe alt sistem. Totuși, înainte de a folosi SSL pentru aceste aplicații, va trebui să configurați aplicațiile pentru a folosi SSL.

Înainte ca un utilizator să poată accesa aplicațiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obține o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA local trebuie să fie copiat într-un fișier de pe PC-ul utilizatorului sau descărcat în browser-ul utilizatorului, în funcție de cerințele aplicației activate-SSL.

Depozitul de certificate *SYSTEM există folosind fișierele ca un alt depozit de certificate sistem:

Dacă sistemul destinație V4R5 sau V5R2 are deja un depozit de certificate *SYSTEM, trebuie să decideți cum să lucrați cu fișierele certificat pe care le-ați transferat pe sistemul destinație. Puteți alege să folosiți fișierele certificate transferate ca un **Depozit de certificate de pe alt sistem**. Sau, puteți alege să importați certificatul privat și certificatul său CA local corespunzător în depozitul de certificate *SYSTEM existent.

Depozitele de certificate de pe alt sistem sunt depozite secundare de certificate definite de utilizatori pentru certificate SSL. Le puteți crea și folosi pentru a furniza certificate pentru aplicațiile activate-SSL scrise de utilizatori care nu folosesc API-uri DCM pentru a înregistra un ID aplicație cu opțiunea DCM. Opțiunea Alte depozite de certificate sistem vă permite să gestionați certificate pentru aplicațiile pe care dumneavoastră sau alții le scrieți și care folosesc API SSL_Init pentru a accesa și a folosi programat un certificat pentru a stabili o sesiune SSL. Acest API permite unei aplicații să folosească mai repede certificatul implicit pentru un depozit de certificate decât certificatul identificat implicit.

Aplicațiile IBM iSeries (și, probabil, și multe aplicații ale altor dezvoltatori de software) sunt scrise pentru a folosi certificate numai din depozitul de certificate *SYSTEM. Dacă alegeți să folosiți fișierele transferate ca un alt depozit de certificate sistem, nu puteți folosi DCM pentru a specifica care aplicații vor folosi certificatul pentru sesiuni SSL. În consecință, nu puteți configura aplicațiile iSeries standard activate pentru SSL să folosească acest certificat. Dacă doriți să folosiți certificatul pentru aplicații iSeries, trebuie să importați certificatul din fișierele transferate ale depozitului dumneavoastră de certificate în depozitul de certificate *SYSTEM.

Pentru a accesa și a lucra cu fișierele depozit de certificate ca un Depozit de certificate de pe alt sistem, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, apăsați **Selecție Depozit de certificate** și selectați **Depozit de certificate de pe alt sistem** ca fiind depozitul de certificate de deschis.
3. Când apare pagina Depozit certificate și Parolă, furnizați calea completă și numele fișierului depozitului de certificate (cea cu extensia .KDB) pe care ați transferat-o de pe sistemul gazdă. De asemenea, furnizați parola pe care ați specificat-o pe sistemul *gazdă* pentru depozitul de certificate când ați creat certificatul pentru sistemul destinație V5R2 și apăsați **Continuare**.
4. În cadrul de navigare, selectați **Gestionarea depozitelor de certificate** și selectați **Modificarea parolei** din lista de task-uri. Completați formularul pentru a modifica parola pentru depozitul de certificate.

Notă: Asigurați-vă că selectați opțiunea **Logare automată** când schimbați parola pentru depozitul de certificate.

Prin folosirea acestei parole vă veți asigura că DCM păstrează noua parolă pentru ca dumneavoastră să puteți folosi toate funcțiile de gestiune a certificatelor ale DCM pentru noul depozit.

După ce modificați parola, trebuie să redeschideți depozitul de certificate înainte de a putea lucra cu certificatele din el. Mai apoi, puteți specifica ca certificatul din acest depozit să fie folosit ca certificat implicit.

5. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați **Depozit de certificate de pe alt sistem** pentru ca să se deschidă depozitul de certificate.
6. Când este afișată pagina **Depozit de certificate și parolă**, furnizați numele cale și numele fișier complet calificate fișierului depozit de certificate, furnizați noua parolă și faceți clic pe **Continuare**.

7. După ce se reafixează cadrul de navigare, selectați **Gestionare depozit certificate** și selectați **Setare certificat implicit** din lista de task-uri.

Acum, după ce ați creat și configurat Depozit de certificate de pe alt sistem, orice aplicații 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:*

Puteți folosi certificatele din fișierele depozit de certificate transferate într-un depozit de certificate *SYSTEM existent pe un sistemul dumneavoastră. Pentru a face acest lucru, trebuie să importați certificatele din fișierele depozit de certificate transferate în depozitul de certificate *SYSTEM existent. Totuși, nu puteți importa certificatele direct din fișierele .KDB și .RDB deoarece nu sunt într-un format pe care funcția de importare a DCM să îl poată recunoaște și folosi. Pentru a folosi certificatele transferate într-un depozit de certificate *SYSTEM existentă, trebuie să deschideți fișierele ca un depozit de certificate de pe alt sistem și să le exportați în depozitul de certificate *SYSTEM.

Pentru a exporta certificatele din fișierele depozitului de certificate în depozitul de certificate *SYSTEM, urmați acești pași de pe sistemul destinație:

1. Porniți DCM.
2. În cadrul de navigare, apăsați **Selectie Depozit de certificate** și selectați **Depozit de certificate de pe alt sistem** ca fiind depozitul de certificate de deschis.
3. Când apare pagina Depozit certificate și Parolă, furnizați calea completă și numele fișierului depozitului de certificate (cea cu extensia .KDB) pe care ați transferat-o de pe sistemul gazdă. De asemenea, furnizați parola pe care ați specificat-o pe sistemul *gazdă* pentru depozitul de certificate când ați creat certificatul pentru sistemul destinație V5R2 și apăsați **Continuare**.
4. În cadrul de navigare, selectați **Gestionarea depozitelor de certificate** și selectați **Modificarea parolei** din lista de task-uri. Completați formularul pentru a modifica parola pentru depozitul de certificate. După ce modificați parola, trebuie să redeschideți depozitul de certificate înainte de a putea lucra cu certificatele din el.

Notă: Asigurați-vă că selectați opțiunea **Logare automată** când schimbați parola pentru depozitul de certificate. Prin folosirea acestei parole vă veți asigura că DCM păstrează noua parolă pentru ca dumneavoastră să puteți folosi toate funcțiile de gestiune a certificatelor ale DCM pentru noul depozit. Dacă nu schimbați parola și selectați opțiunea Logare automată, s-ar putea să întâmpinați erori când exportați certificatele din acest depozit în depozitul de certificate *SYSTEM.

5. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați **Depozit de certificate de pe alt sistem** pentru ca să se deschidă depozitul de certificate.
6. Când este afișată pagina **Depozit de certificate și parolă**, furnizați numele cale și numele fișier complet calificate fișierului depozit de certificate, furnizați noua parolă și faceți clic pe **Continuare**.
7. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** în cadrul de navigare pentru a se afișa o listă de task-uri și selectați **Exportul certificatului**.
8. Selectați **Autoritate certificare (CA)** ca tipul de certificat de exportat și apăsați **Continuare**.

Notă: Trebuie să exportați certificatul CA local în depozitul de certificate înainte să exportați certificatul client sau server în depozit. Dacă exportați întâi certificatul server sau client, s-ar putea să întâlniți o eroare deoarece certificatul CA local nu există în depozitul de certificate.

9. Selectați certificatul CA local care va fi exportat și alegeți **Export**.
10. Selectați **Depozit de certificate** ca destinație pentru certificatul exportat și alegeți **Continuare**.
11. Introduceți *SYSTEM ca depozit de certificate destinație, introduceți parola pentru acest depozit de certificate și alegeți **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informații de eroare dacă exportarea a eșuat.
12. Acum puteți exporta certificatul server sau client în depozitul de certificate *SYSTEM. Re-selectați task-ul **Exportare certificat**.
13. Selectați **Server sau client** ca tipul de certificat de exportat și apăsați **Continuare**.
14. Selectați certificatul server sau client corespunzător de exportat și apăsați **Export**.

15. Selectați **Depozit de certificate** ca destinație pentru certificatul exportat și alegeți **Continuare**.
16. Introduceți ***SYSTEM** ca depozit de certificate destinație, introduceți parola pentru acest depozit de certificate și alegeți **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informații de eroare dacă exportarea a eșuat.
17. Acum puteți alocă certificatul către aplicații să folosească SSL. Apăsați **Selectare depozit de certificate** din cadrul de navigare și selectați ***SYSTEM** ca depozitul de certificate de deschis.
18. Când apare pagina Depozit certificate și Parolă, furnizați parola pentru depozitul de certificate ***SYSTEM** și apăsați **Continuare**.
19. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
20. Din lista de task-uri, selectați **Alocare Certificat** pentru a afișa o listă de certificate din depozitul curent de certificate.
21. Selectați certificatul pe care l-ați creat pe sistemul *gazdă* și apăsați **Alocare la aplicații** pentru a afișa o listă de aplicații activate-SSL la care puteți alocă certificatul.
22. Selectați aplicațiile care vor folosi certificatul pentru sesiuni SSL și faceți clic pe **Continuare**. DCM afișează un mesaj pentru a confirma selecția certificatului dumneavoastră pentru aplicații.

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

Cu aceste task-uri completate, aplicațiile de pe sistemul destinație pot folosi certificatul emis de CA local de pe alt sistem. Totuși, înainte de a folosi SSL pentru aceste aplicații, va trebui să configurați aplicațiile pentru a folosi SSL.

Înainte ca un utilizator să poată accesa aplicațiile selectate printr-o conexiune SSL, utilizatorul trebuie să folosească DCM pentru a obține o copie a certificatului CA local de pe sistemul gazdă. Certificatul CA local trebuie să fie copiat într-un fișier de pe PC-ul utilizatorului sau descărcat în browser-ul utilizatorului, în funcție de cerințele aplicației activate-SSL.

Folosirea unui certificat privat pentru înscrierea obiectelor pe un sistem țintă

Certificatele folosite de aplicații pentru semnarea obiectelor din depozitul de certificate ***OBJECTSIGNING** sunt gestionate în DCM (Digital Certificate Manager). Dacă nu ați folosit niciodată DCM pe sistemul destinație V5R1 pentru a gestiona certificate pentru semnarea obiectelor, atunci acest depozit de certificate nu va exista pe sistemul destinație.

Task-urile pe care trebuie să le realizați pentru a folosi fișierele transferate ale depozitului de certificate pe care le-ați creat pe sistemul gazdă CA local depind de situația dacă depozitul de certificate ***OBJECTSIGNING** există. Dacă depozitul de certificate ***OBJECTSIGNING** nu există, puteți folosi fișierele certificatelor transferate ca un mijloc de creare a depozitului de certificate ***OBJECTSIGNING**. Dacă depozitul de certificate ***OBJECTSIGNING** există pe sistemul destinație, trebuie să importați certificatele transferate în el.

Depozitul de certificate ***OBJECTSIGNING** nu există:

Task-urile pe care le realizați pentru a folosi fișierele depozitului de certificate pe care le-ați creat pe sistemul gazdă CA local depind de situația dacă ați folosit vreodată DCM pe sistemul destinație pentru a gestiona certificatele de semnare obiecte.

Dacă depozitul de certificate ***OBJECTSIGNING** nu există în sistemul destinație V5R3, V5R2 sau V5R1 cu fișierele depozitului de certificate transferat, urmați acești pași:

1. Asigurați-vă că fișierele depozitului de certificate (două fișiere: unul cu extensia **.KDB** și unul cu extensia **.RDB**) pe care le-ați creat pe sistemul care găzduiește CA-ul local sunt în catalogul **/QIBM/USERDATA/ICSS/CERT/SIGNING**.

2. O dată ce fișierele certificatelor transferate sunt în catalogul /QIBM/USERDATA/ICSS/CERT/SIGNING , redenumiți fișierele certificatului în SGNOBJ.KDB și SGNOBJ.RDB, dacă este necesar. Redenumind aceste fișiere, creați componentele care conțin depozitul de certificate *OBJECTSIGNING pentru sistemul destinație. Depozitul de certificate conține deja copii de certificate pentru multe CA publice Internet. DCM a adăugat acestea, cât și o copie a certificatului CA local, la fișierele depozitului de certificate când le-ați creat.

Atenție: Dacă sistemul dumneavoastră destinație are deja un fișier SGNOBJ.KDB și unul SGNOBJ.RDB în catalogul /QIBM/USERDATA/ICSS/CERT/SIGNING , depozitul de certificate *OBJECTSIGNING există pe acest sistem destinație. În consecință, nu trebuie să redenumiți fișierele transferate așa cum a fost sugerat. Suprascrierea fișierelor care semnează obiecte implicite va crea probleme la folosirea DCM, a depozitului de certificate transferat și a conținutului său. Când depozitul de certificate *OBJECTSIGNING există deja,, trebuie să folosiți un proces diferit pentru a obține certificatele în depozitul de certificate existent.

3. Porniți DCM. Trebuie să modificați parola pentru depozitul de certificate *OBJECTSIGNING. Modificarea parolei va permite DCM să păstreze noua parolă pentru ca dumneavoastră să puteți folosi toate funcțiile de gestiune a certificatelor ale DCM pentru depozitul de certificate.
4. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați ***OBJECTSIGNING** pentru ca să se deschidă depozitul de certificate.
5. Când se afișează pagina parolă, introduceți parola pe care ați specificat-o pentru depozitul de certificate atunci când l-ați creat pe sistemul destinație și alegeți **Continuare**.
6. În cadrul de navigare, selectați **Gestionarea depozitelor de certificate** și selectați **Modificarea parolei** din lista de task-uri. Completați formularul pentru a modifica parola pentru depozitul de certificate. După ce modificați parola, trebuie să redeschideți depozitul de certificate înainte de a putea lucra cu certificatele din el. Apoi, puteți crea o definiție de aplicație care să folosească certificatul pentru semnarea obiectelor.
7. După ce ați redeschis depozitul de certificate, selectați **Gestionarea aplicațiilor** din cadrul de navigare pentru a se afișa o listă de task-uri.
8. Din lista de task-uri, selectați **Adăugarea aplicației** pentru a începe procesul de creare a unei definiții aplicație care semnează obiecte pentru a folosi certificatul în semnarea obiectelor.
9. Completați formularul pentru a defini aplicația care semnează obiecte și efectuați un clic pe **Adăugare..** Această definiție aplicație nu descrie o aplicație reală, ci mai degrabă tipul de obiecte pe care doriți să le formați cu un anume certificat. Folosiți ajutorul online pentru a afla cum să completați formularul.
10. Selectați **OK** pentru a recunoaște mesajul de confirmare al definiției aplicație și pentru a afișa lista de task-uri **Gestionarea aplicațiilor**.
11. Din lista de task-uri, selectați **Actualizare alocare certificate** pentru a afișa o listă de ID-uri de aplicații de semnare obiecte pentru care puteți alocă un certificat.
12. Selectați din listă o aplicație și efectuați un clic pe **Actualizarea atribuirii certificatelor**.
13. Selectați certificatul pe care CA-ul local de pe sistemul gazdă l-a creat și apăsați **Alocare certificat nou**.

Când terminați aceste task-uri, aveți tot ce vă trebuie pentru a începe semnarea obiectelor pentru a le asigura integritatea.

Când distribuiți 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 și pentru a verifica identitatea expeditorului. Pentru validarea semnăturii, destinatarul trebuie să aibă o copie a certificatului de verificare a semnăturii. Trebuie să furnizați 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-ați folosit pentru semnarea obiectului. Dacă ați semnat obiectele cu un certificat de la un CA binecunoscut din Internet, versiunea de DCM a primitivului va avea deja o copie a certificatului CA necesar. Totuși, trebuie să furnizați o copie a certificatului CA, într-un pachet separat, împreună cu obiectele semnate dacă este necesar. De exemplu, trebuie să furnizați o copie a certificatului CA local dacă ați semnat obiectele cu un certificat de la un CA local. Din motive de securitate, trebuie să furnizați certificatul CA într-un pachet separat sau să faceți public certificatul CA disponibil la cererea tuturor celor care au nevoie de el.

Depozitul de certificate *OBJECTSIGNING există:

Puteți folosi certificatele din fișierele depozit de certificate transferate într-un depozit de certificate *OBJECTSIGNING existent pe un sistem V5R1. Pentru a face acest lucru, trebuie să importați certificatele din fișierele depozit de certificate transferate în depozitul de certificate *OBJECTSIGNING existent. Totuși, nu puteți importa certificatele direct din fișierele .KDB și .RDB deoarece nu sunt într-un format pe care funcția de importare a DCM să îl poată recunoaște și folosi. Puteți adăuga certificatele în depozitul de certificate *OBJECTSIGNING existent deschizând fișierele transferate ca un alt depozit de certificate sistem pe sistemul destinație V5R3, V5R2 sau V5R1. Puteți exporta certificatele direct în depozitul de certificate *OBJECTSIGNING. Trebuie să exportați o copie atât a certificatului de semnat obiecte cât și a certificatului CA local din fișierele transferate.

Pentru a exporta certificatele din fișierele depozitului de certificate în depozitul de certificate *OBJECTSIGNING, urmați acești pași de pe sistemul destinație V5R2:

1. Porniți DCM.
2. În cadrul de navigare, apăsați **Selecție Depozit de certificate** și selectați **Depozit de certificate de pe alt sistem** ca fiind depozitul de certificate de deschis.
3. Când apare pagina Depozit certificate și Parolă, furnizați calea completă și numele fișierelor depozitului de certificate. De asemenea, furnizați parola pe care ați folosit-o când le-ați creat pe sistemul gazdă apăsați **Continuare..**
4. În cadrul de navigare, selectați **Gestionarea depozitelor de certificate** și selectați **Modificarea parolei** din lista de task-uri. Completați formularul pentru a modifica parola pentru depozitul de certificate.

Notă: Asigurați-vă că selectați opțiunea **Logare automată** când schimbați parola pentru depozitul de certificate. Prin folosirea acestei parole vă veți asigura că DCM păstrează noua parolă pentru ca dumneavoastră să puteți folosi toate funcțiile de gestiune a certificatelor ale DCM pentru noul depozit. Dacă nu schimbați parola și selectați opțiunea Logare automată, s-ar putea să întâmpinați erori când exportați certificatele din acest depozit în depozitul de certificate *OBJECTSIGNING.

După ce modificați parola, trebuie să redeschideți depozitul de certificate înainte de a putea lucra cu certificatele din el.

5. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați **Depozit de certificate de pe alt sistem** pentru ca să se deschidă depozitul de certificate.
6. Când apare pagina Depozit certificate și Parolă, furnizați calea completă și numele fișierului depozitului de certificate, furnizați parola nouă și apăsați **Continuare**.
7. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** în cadrul de navigare pentru a se afișa o listă de task-uri și selectați **Exportul certificatului**.
8. Selectați **Autoritate certificare (CA)** ca tipul de certificat de exportat și apăsați **Continuare**.

Notă: Formularea pentru acest task presupune că atunci când lucrați cu un Depozit de certificate de pe alt sistem lucrați 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. Totuși, folosind task-ul export din acest depozit de certificate este cel mai ușor mod de a adăuga certificatele din fișierele transferate în depozitul de certificate *OBJECTSIGNING existent.

9. Selectați certificatul CA local care va fi exportat și alegeți **Export**.

Notă: Trebuie să exportați certificatul CA local în depozitul de certificate înainte să exportați certificatul semnare obiect în depozit. Dacă exportați întâi certificatul de semnat obiecte, s-ar putea să întâlniți o eroare deoarece certificatul CA local nu există în depozitul de certificate.

10. Selectați **Depozit de certificate** ca destinație pentru certificatul exportat și alegeți **Continuare**.
11. Introduceți *OBJECTSIGNING ca depozit de certificate destinație, introduceți parola pentru depozitul de certificate *OBJECTSIGNING și faceți clic pe **Continuare**.
12. Acum puteți exporta certificatul care semnează obiecte în depozitul de certificate *OBJECTSIGNING. Re-selectați task-ul **Exportare certificat** task.

13. Selectați **Server sau client** ca tipul de certificat de exportat și apăsați **Continuare**.
14. Selectați certificatul corespunzător pentru export și faceți clic pe **Exportare**.
15. Selectați **Depozit de certificate** ca destinație pentru certificatul exportat și alegeți **Continuare**
16. Introduceți *OBJECTSIGNING ca depozit de certificate destinație, introduceți parola pentru depozitul de certificate *OBJECTSIGNING și faceți clic pe **Continuare**. Apare un mesaj pentru a indica faptul că certificatul a fost exportat cu succes sau pentru a da informații de eroare dacă exportarea a eșuat.

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

Gestionarea aplicațiilor în DCM

Acest subiect vă oferă informații despre crearea definițiilor aplicație și cum să gestionați o atribuire de certificat a unei aplicații. Puteți afla despre definirea listelor de încredere CS pe care le folosesc aplicațiile ca bază pentru a accepta certificate pentru autentificarea clienților.

Puteți folosi DCM (Digital Certificate Manager) pentru a efectua diferite task-uri de gestiune pentru aplicațiile activate-SSL și pentru aplicațiile care semnează obiectele. De exemplu, puteți alege ce certificate folosesc aplicațiile pentru sesiuni de comunicare SSL (Secure Sockets Layer). Task-urile de gestiune a aplicațiilor pe care le puteți realiza variază în funcție de tipul de aplicație și de depozitul de certificate în care lucrați. Puteți gestiona aplicații doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

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

Concepte înrudite

“Definiții aplicație” la pagina 10

Citiți aceste informații pentru a învăța ce aplicații DCM sunt și cum să lucrați cu ele pentru configurare SSL și semnare obiect.

Crearea unei definiții de aplicație

Examinați acest subiect pentru a învăța cum două tipuri de aplicații pe care le puteți defini și lucra cu ele.

Există două tipuri de definiții aplicație cu care puteți lucra în DCM: definiții aplicație pentru aplicații client sau server care folosesc SSL și definiții aplicație pe care le folosiți pentru semnarea obiectelor.

Pentru a folosi DCM în lucrul cu definiții aplicație SSL și certificatele lor, aplicația trebuie mai întâi să se înregistreze cu DCM ca o definiție aplicație pentru a avea un ID unic. Cei care au creat aplicația înregistrează aplicațiile active-SSL folosind un API (QSYRGAP, QsyRegisterAppForCertUse) pentru a crea ID-ul aplicației în DCM automat. Toate aplicațiile IBM iSeries activate pentru SSL sunt înregistrate în DCM, așa că puteți să folosiți cu ușurință DCM pentru a le aloca un certificat astfel încât să poată stabili o sesiune SSL. De asemenea, pentru aplicațiile pe care le scrieți sau cumpărați, puteți defini o definiție aplicație și să creați ID-ul aplicație pentru el chiar din DCM. Trebuie să lucrați în depozitul de certificate *SYSTEM pentru a crea o definiție aplicație SSL pentru o aplicație server sau client.

Pentru a folosi un certificat pentru semnarea obiectelor, trebuie să definiți mai întâi o aplicație pe care să o folosească certificatul. Spre deosebire de o definiție aplicație SSL, o aplicație care semnează obiecte nu descrie o aplicație reală. În schimb definiția aplicației pe care o creați ar putea descrie tipul sau grupul obiectelor pe care intenționați să le semnați. Trebuie să lucrați în depozitul de certificate *OBJECTSIGNING pentru a crea o definiție aplicație care semnează obiecte.

Pentru a crea o definiție aplicație, urmați acești pași:

1. Porniți DCM.
2. Alegeți **Selectare depozit de certificate** și selectați depozitul de certificate corespunzător. (Acesta este fie depozitul de certificate *SYSTEM, fie *OBJECTSIGNING în funcție de tipul de definiție aplicație pe care o creați.)

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

3. Când este afișată pagina Depozit de certificate și Parola, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și apoi apăsați **Continuare**.
4. În cadrul de navigare, selectați **Gestionarea aplicațiilor** pentru a afișa o listă de task-uri.
5. Selectați **Adăugarea unei aplicații** din lista de task-uri pentru a se afișa un formular pentru definirea aplicației.

Notă: Dacă lucrați în depozitul de certificate *SYSTEM, DCM vă va cere să alegeți dacă să adauge o definiție de aplicație server sau o definiție de aplicație client.

6. Completați formularul și apăsați **Continuare**. Informația pe care o puteți specifica pentru definiția aplicației variază pe baza tipului de aplicație pe care o definiți. Dacă definiți o aplicație server, puteți specifica de asemenea dacă aplicația poate folosi certificate pentru autentificarea client și trebuie să ceară autentificare client. Puteți specifica de asemenea dacă aplicația trebuie să folosească o listă de încredere CA pentru a autentifica certificatele.

Concepte înrudite

“Definiții aplicație” la pagina 10

Citiți aceste informații pentru a învăța ce aplicații DCM sunt și cum să lucrați cu ele pentru configurare SSL și semnare obiect.

Gestionarea alocării de certificate pentru o aplicație

Trebuie să folosiți DCM pentru a atribui un certificat unei aplicații înainte ca aceasta să poată efectua o funcție sigură, cum ar fi stabilirea unei sesiuni SSL (Secure Sockets Layer) sau semnarea unui obiect.

Pentru a atribui un certificat unei aplicații sau pentru a modifica atribuirea certificatului pentru o aplicație, urmați acești pași:

1. Porniți DCM.
2. Alegeți **Selectare depozit de certificate** și selectați depozitul de certificate corespunzător. (Acesta este fie depozitul de certificate *SYSTEM, fie *OBJECTSIGNING în funcție de tipul de aplicație căreia îi atribuiți certificatul.)

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

3. Când este afișată pagina Depozit de certificate și Parola, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și apoi apăsați **Continuare**.
4. În cadrul de navigare, selectați **Gestionarea aplicațiilor** pentru a afișa o listă de task-uri.
5. Dacă sunteți în depozitul de certificate *SYSTEM, selectați tipul aplicației de gestionat. (Selectați aplicația corespunzătoare a **Serverului** sau a **Clientului**.)
6. Din lista de task-uri, selectați **Actualizarea atribuirii certificatelor** pentru a se afișa o listă de aplicații pentru care puteți atribui un certificat.
7. Selectați din listă o aplicație și efectuați un clic pe **Actualizarea atribuirii certificatelor** pentru a se afișa o listă de certificate pe care le puteți atribui aplicației.
8. Selectați certificatul din listă și efectuați un clic pe **Atribuirea noului certificat**. DCM va afișa un mesaj pentru a confirma selecția certificatului pentru aplicație.

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

Când modificați sau ștergeți un certificat pentru o aplicație, aceasta poate să nu recunoască modificările dacă rulează în momentul modificării atribuirii certificatului. De exemplu, serverele iSeries Access pentru Windows vor aplica automat orice modificare de certificat. Totuși, poate sunteți nevoiți să opriți și să reporniți serverele Telnet, IBM HTTP Server for i5/OS sau alte aplicații înainte de aceste aplicații pot aplica modificările certificatelor dumneavoastră.

În OS/400 V5R2 sau mai târziu, puteți folosi task-ul Alocare certificat când doriți să alocați certificate mai multor aplicații certificate.

Definirea unei liste de încredere CA pentru o aplicație

Aplicațiile 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 identității. Unul dintre criteriile pe care le folosește o aplicație pentru autentificarea unui certificat este dacă aceasta are încredere în CA (autoritatea de certificare) care a emis certificatul.

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

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

- Aplicația trebuie să suporte utilizarea certificatelor pentru autentificare client.
- Definiția aplicației trebuie să specifice faptul că aceasta folosește o listă de încredere CA.

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

Atunci când adăugați un CA listei de încredere a unei aplicații, trebuie să vă asigurați că acesta este și el activ.

Pentru a defini o listă de încredere CA pentru o aplicație, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, faceți clic pe **Selectare depozit de certificate** și selectați ***SYSTEM** ca depozit de certificate pe care să-l deschideți.

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

3. Când este afișată pagina Depozit de certificate și Parola, furnizați parola pe care ați specificat-o pentru depozitul de certificate când l-ați creat și apoi apăsați **Continuare**.
4. În cadrul de navigare, selectați **Gestionarea aplicațiilor** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Definirea listei de încredere CA**.
6. Selectați tipul de aplicație (server sau client) pentru care doriți să definiți lista și alegeți **Continuare**.
7. Selectați din listă o aplicație și efectuați un clic pe **Continuare** pentru a se afișa o listă de certificate CA pe care le utilizați pentru a defini lista de încredere.
8. Selectați CA-urile în care aplicația va avea încredere și faceți clic pe **OK**. DCM va afișa un mesaj pentru a confirma selecțiile pentru lista de încredere.

Notă: Puteți fie să selectați CA-uri individuale din listă sau să specificați că aplicația va avea încredere în toate sau în nici unul din CA-urile din listă. De asemenea, puteți vizualiza sau valida certificatele CA înainte de a le adăuga listei de încredere.

Gestionarea certificatelor prin expirare

DCM (Digital Certificate Manager) oferă suport pentru gestionarea expirării certificatelor, pentru a permite administratorilor să gestioneze certificatele de server sau de client, certificatele de semnare a obiectelor și certificatele de utilizator în funcție de data expirării pe serverul local.

Notă: Dacă configurați DCM să lucreze cu EIM (Enterprise Identity Mapping), puteți gestiona certificate utilizator după data expirării în întreprindere.

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

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

Pentru a vedea și a gestiona certificatele server și client sau certificate semnare obiecte pe baza datelor lor de expirare, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, apăsați **Selecție Depozit de certificate** și selectați ***OBJECTSIGNING** sau ***SYSTEM** ca depozitul de certificate de deschis.

Notă: Dacă aveți întrebări despre completarea unui anume formular în timp ce folosiți DCM, selectați butonul cu semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.

3. Introduceți parola pentru depozitul de certificate și apăsați **Continuare**.
4. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Verificare expirare**.
6. Selectați tipul certificatului pe care vreți să-l verificați. Dacă sunteți în depozitul de certificate ***SYSTEM**, selectați **Server sau client**; dacă sunteți în depozitul de certificate ***OBJECTSIGNING**, selectați **Semnare obiect**.
7. În câmpul **Interval dată expirare în zile (1-365)**, introduceți numărul de zile pentru care să vedeți certificatele pe baza datei lor de expirare și faceți clic pe **Continuare**. DCM afișează toate certificatele care expiră între data de astăzi și data care se potrivește numărului de zile specificat. DCM afișează de asemenea toate certificatele care au datele de expirare înainte de data de astăzi.
8. Selectați un certificat pe care vreți să-l gestionați. Puteți alege să vedeți detalii despre informațiile certificatului, să-l ștergeți sau să-l reînnoiți.
9. Când terminați de lucrat cu certificatele din listă, faceți clic pe **Anulare** pentru a ieși.

Validarea certificatelor și aplicațiilor

Puteți folosi DCM (Digital Certificate Manager) pentru a valida certificate individuale sau aplicațiile care le folosesc. Lista de lucruri pe care le verifică DCM diferă puțin în funcție de validarea unui certificat sau a unei aplicații.

Validarea aplicațiilor

Folosirea DCM pentru a se valida o definiție aplicație ajută prevenirea problemelor legate de certificate pentru aplicație atunci când efectuează o funcție care cere certificate. Asemenea probleme ar putea împiedica o aplicație de la participarea cu succes într-o sesiune SSL (Secure Sockets Layer) sau de la semnarea cu succes a obiectelor.

Atunci când validați o aplicație, DCM verifică dacă există o atribuire a unui certificat pentru aplicație și se asigură că certificatul atribuit este valid. În plus, DCM se asigură că dacă aplicația este configurată pentru a folosi o listă de încredere Autoritate de certificare (CA), atunci lista de încredere conține cel puțin un certificat CA. DCM verifică mai apoi dacă certificatele CA din lista de încredere CA a aplicației sunt valide. De asemenea, dacă definiția aplicației specifică că apare procesarea CRL (Certificate Revocation List) și că există o locație CRL definită pentru CA, DCM verifică CRL-ul ca parte a procesului de validare.

Validarea certificatelor

Atunci când validați un certificat, DCM verifică un număr de articole aparținând certificatului pentru a asigura autenticitatea și validarea certificatului. Validarea unui certificat se asigură că pentru aplicația care folosește certificatul pentru comunicații sigure sau pentru semnarea obiectelor nu există șanse 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 locația 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 și dacă certificatul CA este activat și deci de încredere. Dacă certificatul are o cheie privată (de exemplu, certificate server, client și care semnează obiecte), atunci DCM validează de asemenea perechea de chei publică-privată pentru a se asigura că aceasta se potrivește. Cu alte cuvinte, DCM criptează datele cu cheia publică și apoi se asigură că acestea pot fi decriptate cu cheia privată.

Concepte înrudite

“Locații CRL (listă de revocare certificate)” la pagina 6

O listă de revocare a certificatelor (CRL) este un fișier care conține informații despre toate certificatele invalide și revocate pentru o Autoritate de certificare (CA) specifică.

“Validarea” la pagina 10

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

Alocarea unui certificat la aplicații

Digital Certificate Manager (DCM) vă permite să alocați un certificat ușor și rapid pentru multiplicat aplicații. Puteți aloca un certificat către mai multe aplicații doar din depozitele de certificate *SYSTEM sau *OBJECTSIGNING.

Pentru a face o alocare de certificat pentru una sau mai multe aplicații, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, apăsați **Selecție Depozit de certificate** și selectați ***OBJECTSIGNING** sau ***SYSTEM** ca depozitul de certificate de deschis.

Notă: Dacă aveți întrebări despre completarea unui anume formular în timp ce folosiți DCM, selectați butonul cu semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.

3. Introduceți parola pentru depozitul de certificate și apăsați **Continuare**.
4. După ce se reafixează cadrul de navigare, selectați **Gestionarea certificatelor** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Alocare certificat** pentru a afișa o listă de certificate pentru depozitul de certificate curent.
6. Selectați un certificat din listă și apăsați **Alocare către aplicații** pentru a afișa o listă de definiții de aplicații pentru depozitul de certificate curent.
7. Selectați una sau mai multe aplicații din listă și apăsați **Continuare**. Apare o pagină fie cu un mesaj de confirmare pentru selecția dumneavoastră de alocare fie cu un mesaj de eroare dacă a apărut o problemă.

Gestionarea locațiilor CRL

Digital Certificate Manager (DCM) vă permite să definiți și să administrați informații despre locația 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 aplicație 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 definiți o locație a CRL pentru un anumit CA, aplicațiile care suportă folosirea de certificate pentru autentificarea clienților pot accesa CRL.

Aplicațiile care suportă folosirea de certificate pentru autentificarea clienților pot efectua procesarea CRL pentru a asigura o autentificare mai stringentă pentru certificatele pe care le acceptă ca dovezi valide ale identității. Înainte ca o aplicație să poată folosi o CRL definită ca parte a procesului de validare a certificatului, definiția aplicație DCM trebuie să ceară aplicației să efectueze procesare CRL.

Cum funcționează procesarea CRL

Atunci când folosiți DCM pentru a valida un certificat sau o aplicație, DCM efectuează procesarea CRL implicit ca parte a procesului de validare. Dacă nu este definită nici o locație CRL pentru CA care a emis certificatul pe care îl

validați, DCM nu va putea efectua o verificare CRL. Oricum, DCM poate încerca să valideze alte informații importante despre certificat, precum aceea că semnătura CA de pe un anumit certificat este validă și că CA care l-a emis este de încredere.

Definiți o locație a CRL

Pentru a defini o locație CRL pentru un anumit CA, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, selectați **Gestionarea locațiilor CRL** pentru a se afișa o listă de task-uri.

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

3. Selectați **Adăugare locație CRL** din lista de task-uri pentru a afișa un formular pe care îl puteți folosi pentru a descrie locația CRL și cum DCM sau aplicația vor accesa locația.
4. Completați acest formular și alegeți **OK**. Trebuie să dați un nume unic locației CRL, să identificați serverul LDAP care găzduiește CRL și să furnizați informații despre conexiune care să descrie cum se accesează serverul LDAP. Acum trebuie să asociați definiția locației CRL cu un anumit CA.
5. În fereastra de navigare, selectați **Gestionare certificate** pentru a afișa o listă a task-urilor.
6. Selectați **Actualizare alocare locație CRL** din lista de task-uri pentru a afișa o listă de certificate CA.
7. Selectați din listă certificatul CA cu care vreți să alocați definiția locației CRL pe care ați creat-o și faceți clic pe **Actualizare Alocare Locație CRL**. Va fi afișată o listă a locațiilor CRL.
8. Selectați din listă locația CRL pe care vreți să o asociați cu CA și faceți clic pe **Actualizare Alocare**. Va fi afișat un mesaj la începutul paginii indicate pentru a indica faptul că locația CRL a fost alocată cu certificatul Autorității de Certificare (CA).

Notă: Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiți unealta Administrarea server Web Directory Server și să selectați task-ul "Gestionare schemă" pentru a schimba clasa de securitate (de asemenea numită și "clasă de acces") a atributelor certificateRevocationList și authorityRevocationList din "critical" și "normal" și lăsați goale câmpurile **Nume distinctiv logare** și **Parolă**.

După ce ați definit o locație pentru o CRL pentru un anumit CA, DCM sau alte aplicații pot să o folosească pentru a efectua procesare CRL. Totuși, înainte ca procesarea CRL să poată funcționa, server-ul Directory Services trebuie să conțină CRL corespunzătoare. De asemenea, trebuie să configurați atât serverul director (LDAP) și aplicațiile client să utilizeze SSL cât și să alocați un certificat aplicațiilor din DCM.

Concepte înrudite

"Locații CRL (listă de revocare certificate)" la pagina 6

O listă de revocare a certificatelor (CRL) este un fișier care conține informații despre toate certificatele invalide și revocate pentru o Autoritate de certificare (CA) specifică.

Informații înrudite

Server director IBM pentru iSeries (LDAP)

Activare SSL pe Directory Server

Memorarea cheilor certificatului pe un IBM Cryptographic Coprocessor

Aflați cum să folosiți un coprocesor instalat pentru a furniza depozite mai sigure pentru cheile private ale certificatelor dumneavoastră.

Dacă aveți un IBM Cryptographic Coprocessor pe sistemul dumneavoastră, îl puteți folosi pentru a furniza o memorare mai sigură pentru o cheie privată a certificatului. Puteți folosi coprocesorul pentru a stoca cheia privată pentru un certificat server, unul client sau pentru un certificat CA local. Totuși, nu puteți folosi coprocesorul pentru a depozita cheia privată a unui certificat utilizator deoarece aceasta trebuie să fie stocată pe sistemul utilizatorului. De asemenea, în acest moment nu puteți folosi coprocesorul pentru a depozita cheia privată pentru un certificat care semnează obiecte.

Puteți 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 fișier cheie special.

Puteți selecta această opțiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat. De asemenea, dacă folosiți coprocesorul pentru a depozita cheia privată a unui certificat, puteți modifica atribuirea dispozitivului coprocesor pentru acea cheie.

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

Dacă dumneavoastră creați sau reînnoiți un certificat server sau client, selectați opțiunea de depozitare a cheii private după ce selectați tipul de CA care semnează certificatul curent. Dacă dumneavoastră creați sau reînnoiți un CA local, selectați opțiunea de depozitare a cheii private ca prim pas al procesului.

Concepte înrudite

“IBM Cryptographic Coprocessors for iSeries” la pagina 9

Coprocesorul criptografic furnizează servicii criptografice dovedite, asigurând protecție și integritate, pentru a dezvolta aplicații e-business sigure.

Memorarea cheii certificat private direct pe coprocesor

Pentru a proteja mai mult accesul la și utilizarea unei chei private a certificatului, puteți alege să memorați cheia direct pe un IBM Cryptographic Coprocessor. Puteți selecta această opțiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat în DCM.

Urmați acești pași din pagina **Selecția unei locații de depozitare a cheii** pentru a depozita cheia privată a certificatului direct pe coprocesor:

1. Selectați **Hardware** ca opțiune de depozitare.
2. Selectați **Continuare**. Acum se va afișa pagina **Selecția descrierea unui dispozitiv criptografic**.
3. Din lista de dispozitive, selectați-l pe cel pe care doriți să îl folosiți pentru depozitarea cheii private a certificatului.
4. Selectați **Continuare**. DCM va continua să afișeze pagini pentru task-ul pe care îl realizați, cum ar fi informații de identificare pentru certificatul pe care îl creați sau reînnoiți.

Folosirea cheii master a coprocesorului pentru a cripta cheia certificat privată

Pentru a proteja mai mult accesul la și utilizarea unei chei private a certificatului, puteți folosi cheia master a unui IBM Cryptographic Coprocessor pentru a cripta cheia privată și a o memora într-un fișier de chei special. Puteți selecta această opțiune de depozitare a cheii ca parte a procesului de creare sau de reînnoire a unui certificat în DCM.

Înainte de a putea folosi această opțiune cu succes, trebuie să folosiți interfața de configurare Web a IBM Cryptographic Coprocessor pentru a crea un fișier depozit de chei corespunzător. De asemenea, trebuie să folosiți interfața de configurare Web a coprocesorului pentru a asocia fișierul de stocare al cheii cu descrierea dispozitivului pe care doriți să îl folosiți. Puteți accesa interfața de configurare Web a coprocesorului din pagina Task-uri iSeries.

Dacă sistemul are mai mult de un dispozitiv coprocesor instalat și funcționabil (varied on), puteți alege să partajați cheia privată a certificatului peste mai multe dispozitive. Pentru ca descrierile dispozitiv să partajeze cheia privată, toate dispozitivele trebuie să aibă aceeași cheie master. Procesul de distribuire a aceleași chei master pentru mai multe dispozitive se numește *clonare*. Partajarea de chei peste dispozitive vă permite să folosiți balansarea muncii SSL (Secure Sockets Layer), care poate îmbunătăți performanțele pentru sesiuni sigure.

Urmați acești pași din pagina **Selecția unei locații de depozitare a cheii** pentru a folosi cheia master a coprocesorului pentru a cripta cheia privată și pentru a o stoca într-un fișier special de depozitare a cheilor:

1. Selectați **Criptare hardware** ca opțiune de depozitare.
2. Selectați **Continuare**. Acum se va afișa pagina **Selecția descrierea unui dispozitiv criptografic**.

3. Din lista de dispozitive, selectați-l pe cel pe care doriți să îl folosiți pentru criptarea cheii private a certificatului.
4. Selectați **Continuare**. Dacă aveți mai mult de un coprocesor instalat pornit (varied on), se afișează pagina **Selecția unor descrieri dispozitiv suplimentare**.

Notă: Dacă nu aveți mai multe dispozitive coprocesor disponibile, DCM va continua să afișeze pagini pentru task-ul pe care îl completați, cum ar fi informații de identificare pentru certificatul pe care îl creați sau reînnoiți.

5. Din lista de dispozitive, selectați numele unei sau a mai multor descrieri dispozitiv cu care doriți să partajați cheia privată a certificatului.

Notă: Descrierile dispozitiv pe care le selectați trebuie să aibă aceeași cheie master ca și dispozitivul selectat în pagina precedentă. Pentru a verifica că cheia master este aceeași pe dispozitive, folosiți task-ul de verificare a cheii master din interfața de configurare Web a coprocesorului criptografic 4758. Puteți accesa interfața de configurare Web a coprocesorului din pagina Task-uri iSeries.

6. Selectați **Continuare**. DCM va continua să afișeze pagini pentru task-ul pe care îl efectuați, cum ar fi informații de identificare pentru certificatul pe care îl creați sau reînnoiți.

Gestionarea locației cerute 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 identității prin RA (autoritate de înregistrare). După ce un solicitant furnizează dovada identității pe care o cere RA, acesta certifică identitatea solicitantului. Ori RA-ul ori solicitantul, în funcție de procedura autorității de certificare, trimite aplicația 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. Ați putea să investigați folosirea unui CA flexibil PKIX dacă nevoile dumneavoastră de securitate cer control strict al accesului la resurse pe care aplicațiile activate SSL le furnizează utilizatorilor. De exemplu, Lotus Domino oferă o PKIX CA pentru uzul public.

Dacă ați ales ca CA PKIX să emită certificate care să fie folosite de aplicații, puteți folosi DCM (Digital Certificate Manager) pentru a gestiona aceste certificate. Folosiți DCM pentru a configura un URL pentru un CA PKIX. Dacă faceți acest lucru DCM (Digital Certificate Manager) va fi configurat pentru a furniza un CA PKIX ca o opțiune pentru a se obține certificate semnate.

Pentru a folosi DCM pentru gestionarea certificatelor provenite de la un CA PKIX, trebuie mai întâi să configurați DCM pentru a folosi această locație pentru CA urmând pașii:

1. Porniți DCM.
2. În cadrul de navigare, selectați **Gestionarea locației cererii PKIX** pentru a se afișa un formular care vă va permite să specificați un URL pentru CA PKIX sau pentru RA-urile asociate.
3. Introduceți URL-ul complet calificat pentru CA PKIX pe care doriți să o folosiți pentru a cere un certificat; de exemplu: <http://www.thawte.com> și selectați **Adăugare**. Adăugarea unui URL configurează DCM pentru a adăuga CA PKIX ca o opțiune pentru obținerea de certificate semnate.

După ce adăugați o locație de cerere PKIX CA, DCM adaugă PKIX CA ca o opțiune pentru specificarea tipului de CA pe care o alegeți pentru emiterea unui certificat când folosiți task-ul **Creare Certificat**.

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

Concepte înrudite

“Gestionarea certificatelor de pe un CA Internet public” la pagina 46

Folosiți această informație pentru a gestiona certificate provenite de la un CA public din Internet, trebuie să creați mai întâi un depozit de certificate.

Gestionarea locației LDAP pentru certificatele utilizator

Învățați cum să configurați DCM să memoreze certificate utilizator într-o locație director a serverului LDAP (lightweight Directory Access protocol) pentru a extinde Enterprise Identity Mapping să lucreze cu certificatele utilizator.

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

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

EIM este o tehnologie **@ server** care vă permite să gestionați identitățile de utilizator în întreprinderea dumneavoastră, inclusiv profilurile de utilizator și certificate utilizator i5/OS. Dacă vreți să folosiți EIM pentru a gestiona certificate utilizator, este nevoie să realizați aceste task-uri de configurare EIM înainte de a realiza orice task-uri de configurare:

1. Folosiți vrăjitorul **Configurare EIM** din Navigator iSeries pentru a configura EIM.
2. Creați registrul X.509 în domeniul EIM pentru a fi folosit în asocierea certificatelor
3. Selectați meniul de proprietăți pentru configurația folder în domeniul EIM și introduceți numele de registru X.509.
4. Creați un identificator EIM pentru fiecare utilizator care vreți să participe la EIM.
5. Creați o asociere destinație între fiecare identificator EIM și profilul de utilizator al aceluși utilizator în registrul de utilizator al aceluși utilizator în registrul de utilizator local i5/OS. Folosiți numele de definiție din registrul EIM pentru registrul de utilizatori i5/OS local pe care l-ați specificat în vrăjitorul **Configurare EIM**.

Notă: Pentru informații suplimentare despre configurarea EIM, vedeți subiectul EIM.

După ce realizați task-urile de configurare EIM necesare, trebuie să efectuați următoarele task-uri pentru a termina configurarea generală pentru folosirea EIM și DCM împreună:

1. În DCM, folosiți task-ul **Gestionare locație LDAP** pentru a specifica directorul LDAP pe care DCM îl va folosi automat pentru a memora un certificat utilizator pe care îl creează CA-ul local. Nu este necesar ca locația LDAP să fie pe serverul iSeries local și nici să fie pe serverul LDAP pe care îl folosește EIM. Când configurați locația LDAP în DCM, acesta folosește directorul LDAP specificat pentru a memora toate certificatele utilizator pe care le emite CA-ul local. DCM utilizează de asemenea locație LDAP pentru a memora certificate utilizator procesate de task-ul **Alocare certificat utilizator** în loc să memoreze certificatul cu un profil utilizator.
2. Rulați comanda **Convertire certificate utilizator** (CVTUSRCERT). Această comandă copiază certificatele utilizator existente în locația director LDAP corespunzătoare. Totuși, comanda doar copiază certificatele pentru un utilizator care a avut o asociație destinație creată între un identificator EIM și profilul utilizator. Comanda creează apoi o asociație sursă între fiecare certificat și identificatorul EIM asociat. Comanda folosește numele distinctiv (DN) al subiectului certificatului, DN emitent și un hash al acestor DN-uri împreună cu cheia publică a certificatului pentru a defini numele identității utilizator pentru asociația sursă.

Notă: Pentru a lega anonim la un server LDAP pentru procesare CRL, trebuie să folosiți unealta Administrarea server Web Directory Server și să selectați task-ul Gestionare schemă pentru a schimba clasa de securitate (de asemenea numită și "clasă de acces") a atributelor certificateRevocationList și authorityRevocationList din "critical" și "normal" și lăsați goale câmpurile **Nume distinctiv logare** și **Parolă**.

Operații înrudite

“Certificate digitale și EIM (Enterprise Identity Mapping)” la pagina 33

Aceasta permite sistemelor de operare și aplicațiilor să folosească certificatul ca sursă a unei operații de căutare EIM pentru a mapa de la certificat la o identitate utilizator destinație asociată cu același identificator EIM.

Semnarea obiectelor

Aflați cum să folosiți DCM pentru a gestiona certificatele pe care le folosiți pentru a semna digital obiecte pentru a le asigura integritatea.

Sunt trei metode pe care le puteți folosi pentru semnarea obiectelor. Puteți scrie un program care apelează API-ul Sign Object. Puteți folosi Digital Certificate Manager (DCM) pentru a semna obiecte. Începând cu OS/400 V5R2, puteți folosi caracteristica Navigator iSeries Administrare centrală pentru a semna obiecte când le împachetați pentru a le distribui pe alte sisteme.

Puteți folosi certificatele pe care le gestionați cu DCM pentru a semna orice obiect pe care îl depozitați în sistemul de fișiere integrat al sistemului, cu excepția obiectelor care sunt depozitate într-o bibliotecă. Puteți semna doar obiectele care sunt depozitate în sistemul de fișiere QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG și *FILE (doar salvare fișier). În OS/400 începând cu V5R3, puteți de asemenea să semnați obiecte comandă (*CMD). Nu puteți semna obiecte care sunt stocate pe alte servere.

Puteți semna obiecte cu certificate pe care le cumpărați de la un CA public sau pe care le creați cu un CA local privat în DCM. Procesul de semnare a certificatelor este același, indiferent dacă folosiți certificate publice sau private.

Cerințe preliminare pentru semnarea obiectelor

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

- Trebuie să fi creat depozitul de certificate *OBJECTSIGNING, fie ca parte a procesului de creare a unui CA local, fie ca parte a procesului de gestionare a certificatelor de semnare obiecte de la un CA public din Internet.
- Depozitul de certificate *OBJECTSIGNING trebuie să conțină cel puțin un certificat, fie unul pe care l-ați creat folosind CA-ul local, fie unul pe care l-ați obținut de la un CA public din Internet.
- Pentru semnarea obiectelor, trebuie să fi creat o definiție de aplicație pentru semnarea obiectelor.
- Trebuie să fi alocat un certificat către aplicația de semnare a obiectelor pe care intenționați să o folosiți pentru a semna obiecte.

Folosiți DCM pentru a semna obiecte

Pentru a folosi DCM pentru a semna unul sau mai multe obiecte, urmați acești pași:

1. Pornire DCM
2. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați *OBJECTSIGNING pentru ca să se deschidă depozitul de certificate.

Notă: Dacă aveți întrebări despre completarea unui anume formular în timp ce folosiți DCM, selectați butonul cu semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.

3. Introduceți parola pentru depozitul de certificate *OBJECTSIGNING și apăsați **Continuare**.
4. După ce cadrul de navigare se reafișează, selectați **Gestionarea obiectelor care pot fi semnate** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Semnarea unui obiect** pentru a se afișa o listă de definiții de aplicații pe care le puteți folosi pentru a semna obiecte.
6. Selectați o aplicație și apăsați **Semnarea unui obiect** pentru a vizualiza un formular pentru specificarea locației obiectelor pe care doriți să le semnați.

Notă: Dacă aplicația pe care ați selectat-o nu are atribuit un certificat, nu o puteți folosi pentru a semna obiectul. Trebuie să folosiți mai întâi task-ul **Actualizare atribuire certificat** sub **Gestiunea aplicațiilor** pentru a atribui un certificat definiției aplicației.

7. În câmpul furnizat, introduceți calea complet calificată și numele de fișier al obiectului sau directorului de obiecte pe care doriți să îl semnați și apăsați **Continuare**. Sau, introduceți locația directorului și apăsați **Răsfoire** pentru a vizualiza conținutul directorului pentru a selecta obiectele pentru semnare.

Notă: Trebuie să porniți numele obiectului cu un slash în față, pentru că altfel poate să apară o eroare. Puteți de asemenea să folosiți anumite caractere de înlocuire pentru a descrie partea din catalog pe care doriți să o semnați. Aceste caractere de înlocuire sunt asterisc-ul (*), care specifică "orice număr de caractere" și semnul de întrebare (?), care specifică "un singur caracter (oricare)." De exemplu, pentru a semna toate obiectele dintr-un director specific, puteți introduce /mydirectory/*; pentru a semna toate programele dintr-o bibliotecă specifică, ați putea introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteți folosi aceste caractere de înlocuire doar în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă vreți să folosiți funcția Răsfoire pentru a vedea o listă cu conținutul bibliotecii sau directorului, trebuie să introduceți caracterul de înlocuire ca parte al numelui căii înainte de a face clic pe **Răsfoire**.

8. Selectați opțiunile de procesare pe care doriți să le folosiți pentru semnarea obiectului sau obiectelor selectate și efectuați un clic pe **Continuare**.

Notă: Dacă alegeți să așteptați rezultatele job-ului, fișierul cu rezultatele se va afișa chiar în browser. Rezultatele pentru job-ul curent sunt adăugate la sfârșitul fișierului de rezultate. În consecință, fișierul poate conține rezultate de la orice job-uri anterioare, în plus față de cele ale job-ului curent. Puteți folosi câmpul dată din fișier pentru a determina care linii din fișier sunt pentru job-ul curent. Câmpul dată este în format AAAALLZZ. Primul câmp din fișier 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. Specificați calea completă calificată și numele fișierului care va fi folosit pentru depozitarea rezultatelor operației de semnare a obiectului și apăsați **Continuare**. Sau, introduceți locația directorului și apăsați **Răsfoire** pentru a vedea conținutul directorului și pentru a selecta un fișier care să depoziteze rezultatele job-ului. Se afișează un mesaj pentru a indica dacă job-ul a fost propus pentru a semna obiecte. Pentru a vedea rezultatele job-ului, consultați job-ul **QOJSGNBAT** din istoricul de job-uri.

Verificarea semnăturii obiecte

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

Cerințe anterioare verificării semnăturii

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

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

Notă: Puteți efectua verificarea semnăturilor în timp ce lucrați cu depozitul de certificate *OBJECTSIGNING în cazurile în care verificați semnături pentru obiecte care au fost semnate pe același sistem. Pașii parcurși în timpul verificării semnăturii în DCM sunt aceiași ca cei parcurși pentru orice depozit de certificate. Totuși, trebuie să existe depozitul de certificate *SIGNATUREVERIFICATION și acesta trebuie să conțină o copie a certificatului care a semnat obiectul chiar dacă efectuați verificarea semnăturii în timp ce lucrați cu depozitul de certificate *OBJECTSIGNING.

- Depozitul de certificate *SIGNATUREVERIFICATION trebuie să conțină o copie a certificatului care a semnat obiectele.
- Depozitul de certificate *SIGNATUREVERIFICATION trebuie să conțină o copie a certificatului CA care a emis certificatul care a semnat obiectele.

Folosiți DCM pentru a verifica semnăturile de pe obiecte

Pentru a folosi DCM pentru a verifica semnăturilor obiectelor, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare, alegeți **Selectare depozit de certificate** și selectați ***SIGNATUREVERIFICATION** pentru ca să se deschidă depozitul de certificate.

Notă: Dacă aveți întrebări despre completarea unui anume formular în timp ce folosiți DCM, selectați butonul cu semnul întrebării (?) din partea de sus a paginii pentru a accesa ajutor online.

3. Introduceți parola pentru depozitul de certificate ***SIGNATUREVERIFICATION** și apăsați **Continuare**.
4. După ce cadrul de navigare se reafixează, selectați **Gestionarea obiectelor care pot fi semnate** pentru a afișa o listă de task-uri.
5. Din lista de task-uri, selectați **Verificarea semnăturilor obiectelor** pentru a specifica locația obiectelor pentru care doriți să verificați semnăturile.
6. În câmpul furnizat, introduceți calea complet calificată și numele fișierului pentru obiectul sau directorul de obiecte pentru care doriți să verificați semnăturile și apăsați **Continuare**. Sau, introduceți locația directorului și apăsați **Răfoire** pentru a vizualiza conținutul directorului pentru a selecta obiectele pentru verificarea semnăturilor.

Notă: Puteți de asemenea să folosiți anumite caractere de înlocuire pentru a descrie partea din catalog pe care doriți să o verificați. Aceste caractere de înlocuire sunt asterisc-ul (*), care specifică "orice număr de caractere" și semnul de întrebare (?), care specifică "un singur caracter (oricare)." De exemplu, pentru a semna toate obiectele dintr-un director specific, ați putea introduce /mydirectory/*; pentru a semna toate programele dintr-o bibliotecă specifică, ați putea introduce /QSYS.LIB/QGPL.LIB/*.PGM. Puteți folosi aceste caractere de înlocuire doar în ultima parte a numelui căii; de exemplu, /mydirectory*/filename dă un mesaj de eroare. Dacă vreți să folosiți funcția Răfoire pentru a vedea o listă cu conținutul bibliotecii sau directorului, trebuie să introduceți caracterul de înlocuire ca parte al numelui căii înainte de a face clic pe **Răfoire**.

7. Selectați opțiunea de procesare pe care doriți să o folosiți pentru verificarea semnăturii de pe obiectul sau obiectele selectate și apăsați **Continuare**.

Notă: Dacă alegeți să așteptați rezultatele job-ului, fișierul cu rezultatele se va afișa chiar în browser. Rezultatele pentru job-ul curent sunt adăugate la sfârșitul fișierului de rezultate. În consecință, fișierul poate conține rezultate de la orice job-uri anterioare, în plus față de cele ale job-ului curent. Puteți folosi câmpul dată din fișier pentru a determina care linii din fișier sunt pentru job-ul curent. Câmpul dată este în format AAAALLZZ. Primul câmp din fișier 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. Specificați calea completă calificată și numele fișierului care va fi folosit pentru depozitarea rezultatelor job-ului pentru operația de verificare a semnăturii și apăsați **Continuare**. Sau, introduceți locația directorului și apăsați **Răfoire** pentru a vedea conținutul directorului și pentru a selecta un fișier care să depoziteze rezultatele job-ului. Se afișează un mesaj pentru a indica dacă job-ul a fost propus pentru a se verifica semnătura obiectelor. Pentru a vedea rezultatele job-ului, consultați job-ul **QOJSGNBAT** din istoricul de job-uri.

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

Concepte înrudite

"CertIFICATELE DIGITALE PENTRU SEMNAREA OBIECTELOR" la pagina 35

Folosiți aceste informații pentru a învăța cum să folosiți certificate pentru a asigura integritatea unui obiect sau pentru a verifica semnătura digitală a unui obiect pentru verificarea autenticității sale.

Operații înrudite

"GESTIONAREA CERTIFICATELOR PENTRU VERIFICAREA SEMNĂTURII OBIECTELOR" la pagina 50

Puteți folosi DCM (Digital Certificate Manager) pentru a gestiona certificatele de verificare a semnăturilor obiectelor pe care le folosiți pentru a valida semnăturile digitale ale obiectelor.

Depanarea DCM

Folosiți aceste informații pentru a învăța cum să rezolvați unele dintre cele mai comune erori pe care le puteți întâlni când folosiți DCM.

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

Depanarea parolelor și problemelor generale

Folosiți următoarea tabelă pentru a găsi informații care să vă ajute să depanați unele din cele mai comune probleme cu parolele și alte probleme generale pe care le puteți întâlni în timp ce lucrați cu Digital Certificate Manager (DCM).

Problemă	Soluție posibilă
Nu puteți găsi ajutor suplimentar pentru DCM.	În DCM, selectați "?" . Puteți de asemenea să căutați în Centrul de informare și pe site-urile Web IBM de pe Internet.
Parola pentru CA-ul local și depozitele de certificate *SYSTEM nu funcționează.	Parolele țin cont de majuscule. Asigurați-vă că tasta Caps Lock este la fel ca la atribuirea parolei.
Ați primit un mesaj de eroare că parola dumneavoastră a expirat când ați încercat să deschideți depozitul de certificate.	Trebuie să modificați parola pentru depozitul de certificate transferat. Faceți clic pe butonul OK pentru a schimba parola.
Încercarea dumneavoastră de resetare a parolei când ați folosit task-ul Selectare depozit de certificate a eșuat.	Funcția reset funcționează doar dacă DCM a memorat parola. DCM memorează parola automat când creați un depozit de certificate. Oricum, dacă modificați (sau resetați) parola pentru un Depozit de certificate de pe alt sistem, atunci trebuie să selectați opțiunea Logare automată , astfel încât DCM să continue să stocheze parola.
	De asemenea, dacă mutați un depozit de certificate de la un sistem la altul, trebuie să schimbați parola pentru depozitul de certificate pe noul sistem pentru a vă asigura că DCM o memorează automat. Pentru a schimba parola, trebuie să furnizați parola originală pentru depozitul de certificate când îl deschideți pe noul sistem. Nu puteți folosi opțiunea de resetare parolă până când nu ați deschis depozitul cu parola originală și nu ați modificat parola pentru a fi memorată. Dacă parola nu este schimbată și memorată, DCM și SSL nu pot să recupereze automat parola când este nevoie de ea pentru diverse funcții. Dacă mutați un depozit de certificate pe care îl veți folosi ca un Alt depozit de certificate sistem, trebuie să selectați opțiunea Logare automată când modificați parola pentru a vă asigura că DCM memorează noua parolă pentru acest tip de depozit de certificate.
	Verificați valoarea alocată atributului Permitere certificate digitale noi sub opțiunea 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. Puteți vedea sau modifica valoarea pentru acest atribut folosind comanda STRSST și introducând ID-ul utilizator și parola pentru Uneltele de service . Apoi alegeți opțiunea Gestionare securitate sistem . ID-ul utilizator de unelte de service este probabil ID-ul utilizator QSECOFR.
Nu puteți găsi o sursă pentru un certificat CA ca să-l primiți pe sistemul dumneavoastră.	Unele CA-uri nu fac disponibile imediat certificatele CA. Dacă nu puteți obține certificatul CA de la CA, contactați-vă VAR-ul, dacă VAR-ul a făcut înțelegeri speciale sau financiare cu CA.

Problemă	Soluție posibilă
Nu puteți găsi depozitul de certificate *SYSTEM.	Locația fișierului certificatului *SYSTEM trebuie să fie /qibm/userdata/icss/cert/server/default.kdb. Dacă acel depozit de certificate nu există, trebuie să folosiți DCM pentru a crea depozitul de certificate. Folosiți task-ul Creare depozit de certificate nou .
Ați primit o eroare de la DCM, iar eroarea continuă să apară după ce ați corectat-o.	Ștergeți cache-ul browser-ului. Setati mărimea cache-ului la 0, iar apoi opriți și reporniți browser-ul.
Aveți o problemă cu serverul director (LDAP) cu ar fi alocarea certificatului nu este afișată când informațiile despre aplicația sigură este afișată imediat după alocarea unui certificat. Această problemă apare mai des când este folosit Navigator iSeries pentru a ajunge la un browser Netscape Communications. Preferința pentru cache-ul browser-ului este setată să compare documentul din cache cu documentul din rețea O dată pe sesiune .	Modificați opțiunea implicită pentru a verifica cache-ul de fiecare dată.
Când folosiți DCM pentru a importa un certificat semnat de un CA extern, precum Entrust, primiți un mesaj de eroare cum că perioada de validitate nu conține ziua de azi sau că nu cade în perioada de valabilitate a emitentului.	Sistemul folosește formatul de timp generalizat pentru perioada de validitate. Așteptați o zi și reîncercați. De asemenea, verificați că serverul dumneavoastră are valoarea corectă pentru offset-ul UTC (dspsysval qutcoffset). Dacă observați Daylight Savings Time, diferența poate fi setată incorect.
Ați primit o eroare base 64 când ați încercat să importați un certificat Entrust.	Certificatul este listat ca având un format specific, cum ar fi PEM. Funcția de copiere a browser-ului nu funcționează corect și s-ar putea să copieze material suplimentar ce nu aparține de certificat, cum ar fi spații la începutul fiecărei linii. Dacă acesta este cazul, atunci certificatul nu va fi în formatul corect când veți încerca să-l folosiți pe sistem. Unele design-uri ale paginilor Web cauzează această problemă. Alte pagini Web sunt proiectate pentru a evita această problemă. Fiți siguri că comparați aspectul certificatului original cu rezultatele lipirii, din moment ce informațiile lipite trebuie să arate la fel.

Depanarea problemelor cu depozitul de certificate și cu bazele de date de chei

Folosiți următoarea tabelă pentru a găsi informații care să vă ajute să depanați unele din cele mai comune probleme de memorare a certificatelor și probleme cheie a bazelor de date pe care le puteți întâlni în timp ce lucrați cu Digital Certificate Manager (DCM).

Problemă	Soluție posibilă
Sistemul nu a găsit baza de date de chei, sau a găsit-o nevalidă.	Verificați parola și numele fișierului pentru erori. Asigurați-vă că este inclusă calea cu numele de fișier, inclusiv slash-ul de la început.

Problemă	Soluție posibilă
<p>Crearea bazei de date de chei a eşuat sau crearea CA-ului local a eşuat.</p>	<p>Verificați conflictul numelor de fișiere. Conflictul poate exista la alt fișier decât cel de care întrebați. DCM încearcă să protejeze datele utilizator din directoarele pe care le creează, chiar dacă acele fișiere împiedică DCM să creeze cu succes fișiere când are nevoie.</p> <p>Rezolvați această problemă copiind toate fișierele ce provoacă conflictul în alt director și, dacă este posibil, folosiți funcții DCM pentru a șterge fișierele corespunzătoare. Dacă nu puteți folosi DCM pentru a realiza aceasta, ștergeți manual fișierele din directorul original integrat în sistemul de fișiere unde acestea se află în conflict cu DCM. Asigurați-vă că ați înregistrat exact ce fișiere le mutați și unde le-ați mutat. Aceste copii vă permit să recuperați fișierele dacă veți mai avea nevoie de ele. E nevoie să creați un CA local nou după ce mutați următoarele fișiere:</p> <pre data-bbox="773 632 1377 1157"> /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 </pre> <p>Va trebui să creați un nou depozit de certificate *SYSTEM și certificat sistem după ce ați mutat următoarele fișiere:</p> <pre data-bbox="773 1255 1344 1675"> /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 </pre>
	<p>S-ar putea să vă lipsească un program cu licență (LPP) pe care DCM îl cere instalat. Verificați lista de cerințe preliminară DCM și asigurați-vă că toate programele licențiate sunt instalate corect.</p>
<p>Sistemul nu acceptă un fișier text CA care a fost transferat în mod binar de pe alt sistem. Acceptă fișiere care sunt transferate ASCII.</p>	<p>Inelele cheie și bazele de date de chei sunt fișiere binare, deci diferite. Trebuie să folosiți FTP (protocol de transfer fișiere) în mod ASCII pentru fișierele text CA și FTP (protocol de transfer fișiere) în mod binar pentru fișierele binare, precum .kdb, .kyr, .sth, .rdb ș.a.m.d.</p>

Problemă	Soluție posibilă
Nu puteți modifica parola bazei de date cheie. Un certificat din baza de date cheie nu mai este valid.	Dacă problema nu este o parolă incorectă, găsiți și ștergeți certificatul sau certificatele invalide din depozitul de certificate și apoi încercați să schimbați parola. Dacă aveți certificate expirate în depozitul de certificate, acestea nu mai sunt valide. Dacă certificatele nu sunt valide, funcția de schimbare parolă pentru depozitul de certificate poate să nu permită schimbarea parolei și 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 eliminați certificatele invalide (expirate) din depozit.
Trebuie să folosiți certificate de la un utilizator Internet și de aceea trebuie să folosiți listele de validare, dar DCM nu furnizează funcții pentru listele de validare.	Partenerii de afaceri ce scriu aplicații pentru utilizarea listelor de validare trebuie să scrie codul pentru a asocia lista de validare cu aplicațiile lor după cum trebuie. Ei trebuie să scrie și codul care determină când este validată corect identitatea utilizatorului Internet pentru ca certificatul să poată fi adăugat în lista de validare. Revedeți subiectul din Centrul de informare pentru API-ul QsyAddVldCertificate. Consultați serverul HTTP pentru documentație iSeries pentru ajutor la configurarea unei instanțe de server HTTP sigure pentru a folosi lista de validare.

Depanarea problemelor browser-ului

Folosiți următoarea tabelă pentru a vă ajuta să depanați unele dintre cele mai comune probleme legate de browser pe care le puteți întâlni când lucrați cu Digital Certificate Manager (DCM).

Problemă	Soluție posibilă
Microsoft Internet Explorer nu vă permite să selectați alt certificat până când nu porniți o nouă sesiune a browser-ului.	Începeți o nouă sesiune browser pentru Internet Explorer.
Internet Explorer nu prezintă toate certificatele client/utilizator selectabile din lista de selecție a unui browser. Internet Explorer arată doar certificate, emise de un CA de încredere, pe care le puteți folosi pe un sit securizat.	Un CA trebuie să fie de încredere atât în baza de date chei, cât și pentru aplicația securizată. Asigurați-vă că ați semnat pe PC pentru browser-ul Internet Explorer cu același nume de utilizator ca și cel ce pune certificatul utilizator în browser. Obțineți alt certificat utilizator de la sistemul pe care îl accesați. 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 și sistem.
Internet Explorer 5 primește certificatul CA, dar nu poate deschide fișierul sau să găsească discul pe care ați salvat certificatul.	Aceasta este o nouă facilitate a browser-ului pentru certificate ce nu sunt încă de încredere pentru browser-ul Internet Explorer. Puteți alege locația pe PC.
Ați primit o atenționare browser despre numele sistem și certificatul sistem ce nu se potrivesc.	Unele browser-e fac diferite lucruri pentru potrivirea numelor în funcție de litere mari sau mici. Tastați URL-ul cu același tip de caractere ca și cele prezentate de certificatul sistem. Sau, creați certificatul sistem cu tipul de litere pe care cei mai mulți utilizatori îl vor folosi. Numai dacă știți exact ceea ce faceți, este mai bine să lăsați numele de server și sistem cum sunt. Trebuie de asemenea să verificați că serverul nume domeniu este setat corect.
Ați pornit Internet Explorer cu HTTPS în loc de HTTP, și ați primit un mesaj de atenționare despre o combinație securizată și nesecurizată de sesiuni.	Alegeți accept și ignorați avertismentul; o ediție viitoare a Internet Explorer va corecta această problemă.
Netscape Communicator 4.04 for Windows a convertit valorile hexazecimale A1 și B1 în B2 și 9A în pagina de cod Poloneză.	Acesta este un 'bug' (eroare) de browser ce afectează NLS. Folosiți alt browser sau chiar folosiți aceeași versiune a browser-ului pe o altă platformă, precum Netscape Communicator 4.04 for AIX.

Problemă	Soluție posibilă
Într-un profil utilizator, Netscape Communicator pentru 4.04 arată majusculele din certificatul utilizator NLS corect, dar literele mici sunt afișate incorect.	Unele caractere specifice limbilor naționale care au fost introduse corect ca un caracter dar care nu sunt același caracter atunci când sunt afișate mai târziu. De exemplu, în versiunea pentru Windows a Netscape Communicator 4.04, valorile hexazecimale A1 și B1 au fost convertite în B2 și 9A pentru pagina de cod Poloneză, conducând la afișarea unor caractere NLS diferite.
Browser-ul continuă să-i spună utilizatorului că CA nu este încă de încredere.	Folosiți 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 funcției browser-ului sau a configurației sale. Browser-ul alege să nu se conecteze la un sit care folosește un certificat sistem ce poate fi autosemnat sau poate să nu fie valid din anumite motive.
Browser-ul Netscape Communicator și produsele server folosesc certificate rădăcină de la companii, incluzând, dar nu limitându-se la, VeriSign, ca o facilitare ce se poate activa a comunicațiilor SSL mai specific, autentificare. Toate certificatele rădăcină expiră în mod periodic. Unele certificate browser Netscape și rădăcină server expiră între 25 Decembrie 1999 și 31 Decembrie 1999. Dacă nu ați corectat această problemă înainte de 14 Decembrie 1999, veți primi un mesaj de eroare.	Versiunile mai vechi ale browser-ului (Netscape Communicator 4.05 sau mai vechi) au certificate care expiră. Trebuie să actualizați browser-ul la versiunea curentă a Netscape Communicator. Informații despre certificate rădăcină browser sunt disponibile în multe surse, cum ar fi http://home.netscape.com/security/ și http://www.verisign.com/server/cus/rootcert/webmaster.html . Descărcarea gratuită a browser-ului este disponibilă la http://www.netcenter.com .

Depanarea problemelor serverului iSeries

Problemă	Soluție posibilă
HTTPS (Hypertext Transfer Protocol Secure) nu funcționează.	Asigurați-vă că serverul HTTP este setat corect pentru folosirea SSL. În versiunile mai mari de V5R1 fișierul de configurare trebuie să aibă SSLAppName setat prin folosirea interfeței de administrare a serverului HTTP. De asemenea, configurația trebuie să aibă o gazdă virtuală configurată care folosește 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 și unul nu pentru SSL. Acestea sunt setate în pagina Setări generale . Asigurați-vă că instanța server este creată și că certificatul serverului este semnat.
Procesul pentru înregistrarea unei instanțe server HTTP ca o aplicație securizată are nevoie de clarificări.	Pe serverul dumneavoastră, mergeți la interfața Administrare server HTTP pentru a seta configurația serverului dumneavoastră HTTP. Mai întâi trebuie să definiți o gazdă virtuală pentru a activa SSL. După ce definiți o gazdă virtuală, trebuie să specificați că gazda virtuală folosește portul SSL definit anterior în directiva Ascultare (în pagina Setări generale). Apoi, trebuie să folosiți pagina SSL cu autentificare certificat sub Securitate pentru a activa SSL în gazda virtuală configurată anterior. Toate schimbările trebuie să fie aplicate fișierului de configurare. Luați aminte că înregistrarea instanței dumneavoastră nu alege automat care certificate vor fi folosite de instanță. Trebuie să folosiți DCM pentru a alocă un certificat specific aplicației dumneavoastră înainte să încercați să opriți și apoi să reporniți instanța server a dumneavoastră.
Dacă aveți dificultăți la setarea serverului HTTP pentru liste validarea listelor și autentificării opționale a clientului.	Vedeți documentația serverului HTTP pentru iSeries pentru opțiuni de setare a instanței.
Netscape Communicator așteaptă expirarea directivei de configurare din codul server HTTP înainte de a vă permite să selectați un alt certificat.	O valoare mare de certificat face dificilă înregistrarea unui al doilea certificat, dacă browser-ul îl mai folosește încă pe primul.

Problemă	Soluție posibilă
Încercați ca browser-ul să prezinte certificatul X.509 server-ului HTTP pentru a putea folosi certificatul ca intrare pentru API-urile QsyAddVldlCertificate.	Trebuie să folosiți SSLEnable și SSLClientAuth ON pentru a face ca Serverul HTTP să încarce variabila de mediu HTTPS_CLIENT_CERTIFICATE . Puteți localiza informația despre API-uri cu subiectul Căutător de API-uri din Centrul de informare. Ați putea de asemenea să vreți să vă uitați la aceste API-uri legate de liste de validare sau de certificate: <ul style="list-style-type: none"> • QsyListVldlCertificates și QSYLSTVC • QsyRemoveVldlCertificate și QRMVVC • QsyCheckVldlCertificate și QSYCHKVC • QsyParseCertificate și QSYPARSC ș.a.m.d.
Server-ului HTTP îi ia foarte mult timp să se întoarcă sau expiră dacă cereți o listă de certificate din lista de validare și sunt mai mult de 10.000 de elemente.	Creați un job batch ce caută și șterge 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 și mesajul de eroare HTP8351 apare în istoricul jobului. Istoricul erorii pentru serverul HTTP arată o eroare că operația de inițializare SSL a eșuat cu o eroare cod de returnare de 107 când serverul HTTP eșuează.	Eroarea 107 înseamnă că certificatul a expirat. Folosiți DCM pentru a alocă un certificat diferit aplicației; de exemplu, QIBM_HTTP_SERVER_MY_SERVER. Dacă instanța server care eșuează la pornire este serverul *ADMIN, atunci setați temporar SSL pe Dezactivat astfel încât să folosiți DCM pe serverul *ADMIN. Apoi folosiți DCM pentru a alocă un certificat diferit aplicației QIBM_HTTP_SERVER_ADMIN și încercați să setați SSL pe Activat din nou.

Depanarea alocării unui certificat utilizator

Când folosiți task-ul **Alocarea unui certificat utilizator**, Digital Certificate Manager (DCM) afișează informații despre certificat ca dumneavoastră să le aprobați înainte de a înregistra certificatul. Dacă DCM nu poate să afișeze un certificat, problema ar putea fi cauzată de una din următoarele situații:

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 ștergerea memoriei cache a browser-ului și apoi executarea din nou a procesului. Browser-ul vă va prompta să selectați un certificat.
2. Asta s-ar putea întâmpla de asemenea dacă configurați browser-ul dumneavoastră astfel încât să nu afișeze o listă de selecție și browser-ul conține doar un certificat de la o Autoritate de certificare din lista de CA-uri în care are încredere serverul. Verificați setările de configurare ale browser-ului și modificați-le dacă este necesar. Browser-ul dumneavoastră vă va prompta să selectați un certificat. Dacă nu puteți prezenta un certificat de la un CA pentru care serverul este setat să aibă încredere, nu puteți alocă un certificat. Contactați administratorul dumneavoastră DCM.
3. Certificatul care se dorește 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 aplicația în cauză. De aceea certificatul pe care îl prezentați nu este valid. Contactați-vă administratorul de sistem pentru a determina dacă CA care a emis certificatul este corect. Dacă CA este corectă, administratorul de sistem ar putea avea nevoie să **Importe** certificatul CA în depozitul de certificate *SYSTEM. Sau, administratorul ar putea avea nevoie să folosească task-ul **Setare stare CA** pentru a activa CA drept de încredere pentru a corecta problema.
5. Nu există un certificat pentru înregistrare. Se pot verifica certificatele client în browser pentru a vedea dacă este vreo problemă.
6. Certificatul care se dorește a fi înregistrat este expirat sau incomplet. Trebuie fie să reînnoiți certificatul sau să contactați 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 și autentificarea clientului pe instanța securizată Admin a serverului. Dacă nu funcționează nici unul dintre sfaturile de depanare propuse, contactați administratorul de sistem pentru a-i raporta problema.

Pentru **Atribuirea unui certificat utilizator**, trebuie să vă conectați la un DCM, folosind o sesiune SSL. Dacă nu folosiți SSL când selectați task-ul **Atribuirea unui certificat utilizator**, DCM va afișa un mesaj în care vă va spune că trebuie să folosiți SSL. Acest mesaj este însoțit de un buton prin care se poate face conectarea la DCM folosind SSL. Dacă butonul respectiv nu apare, informați 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.

Operații înrudite

“Alocarea unui certificat utilizator” la pagina 42





Puteți să alocați un certificat pe care îl dețineți la profilul utilizator i5/OS sau la altă identitate de utilizator.

Certificatul poate fi de la un CA local privat de pe alt sistem sau de la un CA din Internet binecunoscut. Pentru a aloca un certificat unei identități de utilizator, CA-ul emitent trebuie să fie de încredere pentru server și certificatul trebuie să nu fie deja asociat cu un profil de utilizator sau altă identitate de utilizator din sistem.

Informații înrudite pentru DCM

Revedeți această pagină pentru a găsi legături către alte resurse pentru a învăța mai mult despre certificatele digitale, infrastructura cheilor publice, Digital Certificate Manager și alte informații înrudite.

Cum folosirea certificatelor digitale a devenit mai răspândită, resursele informaționale au devenit de asemenea mai disponibile. Aici se află o listă scurtă de alte resurse pe care le puteți revizui pentru a învăța mai multe despre certificate digitale și cum pot fi folosite ele pentru a îmbunătăți polița de securitate:

- **Situl Web VeriSign Help Desk**  Situl Web VeriSign oferă o bibliotecă extensivă cu subiecte legate de certificate digitale, cum ar fi semnarea obiectelor, ca și alte subiecte de securitate a Internetului.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM și Cryptographic Enhancements**
SG24-6168  Acest manual IBM Redbook se concentrează pe îmbunătățirile de securitate ale rețelelor la V5R1 OS/400. Cartea Redbook include multe subiecte inclusiv cum să utilizați iSeries
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**  Această carte Redbook descrie ce puteți face cu certificatele digitale în serverul iSeries. Explică cum se setează diferitele servere și clienți care folosesc certificate. Oferă informații și exemple de coduri despre cum se folosesc API-urile OS/400 pentru a gestiona și folosi certificatele digitale în aplicațiile utilizatorilor.
- **RFC Index Search**  Acest sit Web oferă o magazie pentru căutarea RFC-urilor. RFC-urile descriu standardele pentru protocoale Internet, cum ar fi SSL, PKIX și altele care sunt înrudite cu folosirea certificatelor digitale.

Anexa. Observații

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

Este posibil ca IBM să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Luați legătura cu reprezentanța IBM locală pentru a obține informații cu privire la produsele și serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcțional și care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea și verificarea modului în care funcționează un produs, program sau serviciu non-IBM ține de responsabilitatea utilizatorului.

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

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

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

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

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor țări unde asemenea prevederi sunt incompatibile cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAȚIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANȚIE EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA GARANȚIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE CU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilității pentru garanțiile exprese sau implicite în anumite tranzacții și de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informații pot conține greșeli tehnice sau erori de tipar. Se efectuează modificări periodice la informațiile incluse aici; aceste modificări vor fi încorporate în noi ediții ale publicației. IBM poate aduce îmbunătățiri și/sau modificări produsului (produselor) și/sau programului (programelor) descrise în această publicație în orice moment, fără notificare.

Orice fel de referințe din aceste informații către situri Web non-IBM sunt furnizate doar pentru conveniență și nu servește în nici un caz ca aprobare a acelor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

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

Posesorii de licențe pentru acest program care doresc să obțină informații despre el în scopul de a permite: (I) schimbul de informații între programe create independent și alte programe (inclusiv acesta) și (II) utilizarea mutuală a informațiilor care au fost schimbate, vor contacta:

IBM Corporation

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

Aceste informații pot fi disponibile cu condiția respectării termenilor și condițiilor, iar în unele cazuri cu plata unor taxe.

- | Programul cu licență descris în aceste informații și toate materialele cu licență disponibile pentru acesta sunt furnizate
- | de către IBM conform termenilor din Contractul IBM cu Clientul, Contractul de Licență IBM pentru Programele
- | Internaționale, Contractul de Licență IBM pentru Codul Mașină, sau orice contract echivalent dintre noi.

Toate datele de performanță conținute aici au fost determinate într-un mediu controlat. Prin urmare, rezultatele obținute în alte medii de operare pot fi semnificativ diferite. Este posibil ca unele măsurători să fi fost realizate pe sisteme de nivel evoluat și nu există nici o garanție că aceste măsurători vor fi identice pe sisteme general disponibile. Mai mult, este posibil ca anumite măsurători să fi fost estimate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice datele aplicate pentru mediul lor specific.

Toate declarațiile referitoare la direcția sau intențiile viitoare ale IBM sunt subiectul modificării sau a retragerii fără aviz și reprezintă doar țeluri și obiective.

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

Aceste informații conțin exemple de date și rapoarte folosite în operații de afaceri zilnice. Pentru a le ilustra cât mai complet posibil, exemplele includ nume de persoane, companii, mărci și produse. Toate aceste nume sunt fictive și orice asemănare cu nume și adrese utilizate de o întreprindere reală este pur întâmplătoare.

LICENȚĂ DE COPYRIGHT:

Aceste informații cuprind exemple de programe de aplicație în limbaj sursă, care ilustrează tehnici de programare pe diverse platforme de operare. Puteți copia, modifica și distribui aceste programe-eșantion în orice formă fără necesitatea unei plăți către IBM, în scopul dezvoltării, utilizării, marketingului sau distribuirii programelor de aplicație în concordanță cu interfața de programare a aplicației pentru platforma de operare pentru care sunt scrise programele-eșantion. Aceste exemple nu au fost testate complet în toate condițiile. Prin urmare, IBM nu poate garanta sau sugera că aceste programe vor fi fiabile, practice sau funcționale.

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

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

Dacă vedeți aceste informații folosind o copie electronică, fotografiile și ilustrațiile color s-ar putea să nu apară.

Mărci comerciale

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

- | AIX
- | AS/400
- | Domino
- | eServer
- | i5/OS
- | IBM

- | iSeries
- | Lotus
- | Net.Data
- | OS/400

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

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

Termenii și condițiile

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

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

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

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

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

Nu puteți descărca, exporta sau reexporta aceste informații decât respectând integral legile și reglementările în vigoare, precum și legile și reglementările din Statele Unite privind exportul.

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



Tipărit în S.U.A.