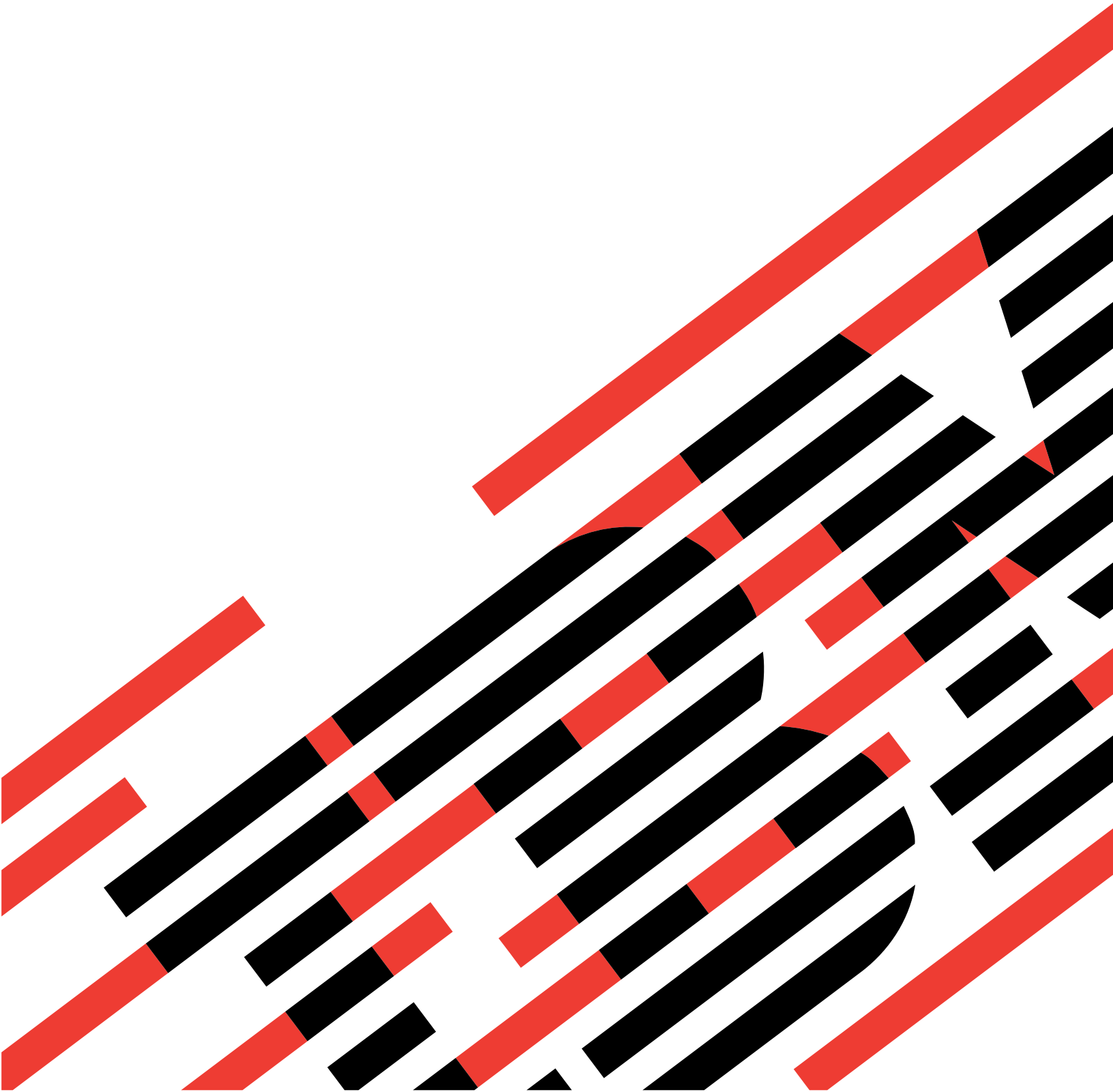
IBM

eserver

iSeries

Digital Certificate Manager



IBM

@server

iSeries

Digital Certificate Manager

Obsah

Časť 1. Správca digitálnych certifikátov

Digitálny certifikát je elektronické povolenie, ktoré môžete použiť na potvrdenie dôkazu identity v elektronickej transakcii. Používanie digitálnych certifikátov sa neustále rozširuje a poskytuje rozšírenú sieťovú bezpečnosť. Napríklad digitálne certifikáty sú nevyhnutné na konfigurovanie a používanie SSL (Secure Sockets Layer). Použitie SSL vám umožňuje vytvárať bezpečné spojenia medzi aplikáciami užívateľa a servera cez nedôveryhodnú sieť, akou je Internet. SSL poskytuje jedno z najlepších riešení na ochranu súkromia dôležitých informácií na Internete, ako sú mená užívateľov a heslá. Veľa služieb a aplikácií iSeries ako sú FTP, Telnet, HTTP Server for iSeries a mnohé ďalšie, poskytujú podporu SSL na zabezpečenie utajenia údajov.

iSeries poskytuje rozsiahlu podporu digitálnych certifikátov, ktorá vám umožňuje používať digitálne certifikáty ako oprávnenia v mnohých bezpečnostných aplikáciách. Okrem použitia certifikátov na konfiguráciu SSL, môžete ich použiť ako oprávnenia pre autentifikáciu klienta v SSL a VPN (súkromná virtuálna sieť) transakciách. Digitálne certifikáty a ich pridružené bezpečnostné kľúče môžete tiež používať na podpísanie objektov. Podpisovanie objektov vám umožňuje zistiť zmeny alebo možné zasahovanie do obsahu objektov overovaním podpisov na objektoch, čím sa zabezpečí ich integrita.

Využitie podpory iSeries pre certifikáty je jednoduché, ak na centralizované manažovanie certifikátov pre vaše aplikácie použijete Správcu digitálnych certifikátov (DCM), bezplatný doplnok iSeries. DCM vám umožňuje manažovať certifikáty, ktoré získate od ľubovoľnej Certifikačnej autority (CA). DCM môžete použiť aj na vytvorenie a prevádzkovanie vašej lokálnej CA, s ktorou môžete vydávať súkromné certifikáty aplikáciám a užívateľom vo vašej organizácii.

Správne naplánovanie a vyhodnotenie sú kľúčovými momentmi pre efektívne používanie certifikátov s ohľadom na ich pridané bezpečnostné výhody. Prečítajte si tieto témy, v ktorých sa dozviete o spôsobe fungovania certifikátov a o použití DCM na ich manažovanie, ako aj na manažovanie aplikácií, ktoré ich používajú:

Čo je nového pre V5R2
Z týchto informácií sa dozviete o zmenách v doplnku Správca digitálnych certifikátov a o zmenách v informačnej príručke pre túto verziu.

Vytlačte si túto tému
Na tejto stránke sa dozviete, ako vytlačiť celú príručku ako súbor PDF.

Migrovanie na DCM zo starších vydaní
Z týchto informácií sa dozviete, aké úlohy musíte vykonať a Ďalšie hľadiská, ktoré musíte pochopiť, ak migrujete existujúcu verziu DCM do aktuálnej verzie vydania.

Scenáre DCM
Tieto informácie použite na prehľad dvoch scenárov, ktoré ilustrujú typické implementačné schémy certifikátov, ktoré vám pomôžu naplánovať vašu vlastnú implementáciu certifikátov, ako časti vašej politiky bezpečnosti iSeries. Každý scenár poskytuje tiež všetky potrebné konfiguračné úlohy, ktoré musíte vykonať na použitie scenára tak, ako je opísaný.

Pojmy digitálnych certifikátov
Tento koncept a referenčné informácie vám bližšie vysvetlia, čo sú vlastne digitálne certifikáty a ako fungujú. Získajte informácie o rôznych typoch certifikátov a ako ich môžete použiť, ako časť vašej politiky bezpečnosti.

Plánovanie pre DCM
Tieto informácie vám pomôžu rozhodnúť, ako a kedy by ste mali používať digitálne certifikáty, aby ste vyhoveli svojim bezpečnostným cieľom. V týchto informáciách sa dozviete o predpokladoch, ktoré musíte nainštalovať, ako aj o ďalších požiadavkách, na ktoré musíte brať ohľad pred použitím DCM.

Konfigurovať DCM
V týchto informáciách sa dozviete, ako nakonfigurovať čokoľvek, čo potrebujete na zabezpečenie toho, aby ste mohli používať DCM na manažovanie vašich certifikátov a ich kľúčov.

Manažovať DCM
Tieto informácie vám ukážu, ako používať DCM na manažovanie certifikátov a aplikácií, ktoré ich používajú. Tiež sa dozviete o tom, ako digitálne podpisovať objekty a ako vytvoriť a prevádzkovať vlastnú Certifikačnú autoritu.

Odstraňovanie chýb DCM
Tieto informácie vám vysvetlia, ako odstrániť niektoré z najbežnejších chýb, na ktoré môžete naraziť pri používaní DCM.

Informácie súvisiace s DCM
Túto stránku použite na vyhľadanie odkazov na iné zdroje, z ktorých sa dozviete viac o digitálnych certifikátoch, infraštruktúre verejných kľúčov, Správcovi digitálnych certifikátov a ďalších súvisiacich informáciách.

Kapitola 1. Čo je nového pre V5R2

Vylepšenia v Správcovi digitálnych certifikátov (DCM) V5R2 a vybavení iSeries pre digitálne certifikáty zahŕňajú:

- **Funkcia priradenia certifikátu**
  Táto nová úloha DCM vám umožňuje rýchlejšie a ľahšie priradiť certifikát k jednej alebo viacerým aplikáciám. Na túto úlohu môžete pristupovať zo zoznamu úloh **Manažovať certifikáty**, alebo zo stránok zrýchleného prístupu **Pracovať so serverom a certifikátmi** a **Pracovať s certifikátmi na podpisovanie objektov**. Táto funkcia je dostupná len pre pamäte certifikátov *SYSTEM a *OBJECTSIGNING.
- **Podpisovať príkazová (*CMD) objekty**
  Teraz môžete používať DCM na vytvorenie elektronických podpisov na príkazové (*CMD) objekty na poskytnutie prostriedkov na kontrolu ich integrity. Taktiež môžete zvoliť rozsah podpisu pre *CMD objekty; môžete zvoliť, či sa má podpísať celý *CMD objekt, alebo iba základné komponenty *CMD objektov. Keď používate DCM na prezeranie podpisu na *CMD objektoch, DCM poskytne informácie o rozsahu podpisu.
- **API pre vytváranie užívateľských certifikátov, podpísaných lokálnou CA, bez použitia DCM**
  Teraz sú tu dva nové API, ktoré môžete používať na programové vydávanie certifikátov, podpísaných lokálnou certifikačnou autoritou (CA), pre užívateľov iných ako ako i-Series. Tieto API vám umožňujú na vydávanie certifikátov užívateľom bez užívateľských profilov iSeries a bez toho, aby museli užívatelia použiť DCM na individuálne získanie certifikátu na autentifikáciu klienta.

Nové alebo vylepšené informácie pre túto tému zahŕňajú:

- Dva nové scenáre, ktoré môžete použiť na to, aby vám pomohli pri zisťovaní, ako najlepšie uplatniť certifikáty na splnenie vašich bezpečnostných cieľov.
- Preorganizované informácie, ktoré vám zjednodušia rýchle vyhľadanie informácií, ktoré potrebujete na používanie DCM.

Na nájdenie ďalších informácií o tom, čo je nové alebo zmenené v tomto vydaní, si pozrite Poznámky pre užívateľov  .

Kapitola 2. Tlač tejto témy

Na zobrazenie alebo stiahnutie verzie PDF zvoľte Správca digitálnych certifikátov  (veľkosť súboru je okolo 468 KB alebo približne 110 strán).

Ak si chcete uložiť PDF na svojej pracovnej stanici za účelom prezerania alebo tlače:

1. Vo svojom prehliadači otvorte PDF (kliknite na predchádzajúci odkaz).
2. V ponuke svojho prehliadača kliknite na **Súbor**.
3. Kliknite na **Uložiť ako...**
4. Prejdite do adresára, do ktorého chcete uložiť dokument PDF.
5. Kliknite na **Uložiť**.

Ak na zobrazenie alebo vytlačenie PDF potrebujete Adobe Acrobat Reader, môžete si stiahnuť kópiu z web stránky Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Kapitola 3. Migrovať zo staršej verzie DCM

Keď migrujete z verzie V4R3 Správcu digitálnych certifikátov (DCM) do V5R2, DCM automaticky aktualizuje vašu existujúcu lokálnu certifikačnú autoritu (CA) a systémové súbory certifikačných kľúčov. DCM zaktualizuje tieto súbory, ktoré majú názov default.kyr, do zodpovedajúcich súborov pamäte certifikátov, ktoré majú názov default.kdb. DCM tiež migruje všetky platné certifikáty v súboroch kľúčov, spojených s HTTP (Hypertext Transfer Protocol) a LDAP (Lightweight Directory Access Protocol) servermi. DCM migruje platné certifikáty do pamäte certifikátov *SYSTEM (default.kdb).

Poznámka: Ak migrujete z verzie V4R4, V4R5, alebo V5R1 DCM, nepotrebujete vykonať žiadne migračné úlohy, lebo súbory certifikátov z týchto verzií sú kompatibilné s verziou V5R2 DCM.

Migrácia kľúčov do pamäte certifikátov – migrácia V4R3

Počas inštalácie V5R2 DCM systém migruje nasledovné súbory kľúčov:
- Štandardné súbory kľúčov DCM.
- Súbory kľúčov, používané konfiguračnými súbormi HTTP servera.
- Súbory kľúčov, používané konfiguračnými súbormi LDAP servera.

Ak používate .kyr súbor, ktorý DCM automaticky neaktualizuje, DCM ho skonvertuje do súboru kyr.kdb, keď s ním budete pracovať v DCM po prvýkrát. Napríklad, keď prvýkrát špecifikujete súbor secure.kyr v užívateľskom rozhraní DCM, DCM skonvertuje tento súbor do novej pamäte certifikátov s názvom súboru secure.kyr.kdb.

Poznámka: Súbory kľúčov sú odlišné od pamätí certifikátov, preto musíte skonvertovať súbory kľúčov, ktoré DCM automaticky neskonvertoval a to tak, že s nimi budete pracovať cez užívateľské rozhranie DCM. Ručná zmena rozšírení názvov súborov na .kdb má za následok chyby, keď sa následne pokúsite pracovať s týmito súbormi cez užívateľské rozhranie DCM.

Ak sa pokúsite zmazať súbor secure.kyr počas používania DCM, DCM ho v skutočnosti archivuje a vymaže súbor secure.kyr.kdb.

Štandardné heslo pamäte certifikátov

Ak existuje súbor /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR, systém migruje tento súbor kľúčov a mnohé ďalšie vhodné súbory kľúčov do pamäte certifikátov *SYSTEM. Pôvodné heslo, spojené so súborom /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR sa použije ako heslo pre pamäť certifikátov *SYSTEM.

Ak súbor /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR neexistuje, ale existujú iné vhodné súbory kľúčov na migráciu (napríklad, súbory kľúčov, ktoré používajú konfiguračné súbory HTTP Servera), systém vytvorí pamäť certifikátov *SYSTEM s heslom DEFAULT (všetky písmená sú veľké) a dokončí migráciu.

Informácie o chybách, ktoré sa môžu vyskytnúť počas procesu migrácie súborov a informácie o tom, ako ich vyriešiť, nájdete v: Chyby migrácie a riešenia obnovy.

Kapitola 4. Scenáre DCM

Správca digitálnych certifikátov a podpora digitálnych certifikátov, ktorú váš iSeries poskytuje, vám umožňuje používať certifikáty na rozšírenie vašej politiky bezpečnosti niekoľkými rôznymi spôsobmi. Ako sa rozhodnete certifikáty používať, závisí na vašich obchodných plánoch a bezpečnostných potrebách.

Použitie digitálnych certifikátov vám môže pomôcť zvýšiť vašu bezpečnosť niekoľkými spôsobmi. Digitálne certifikáty vám umožňujú používať Secure Sockets Layer (SSL) pre bezpečný prístup na Web stránky a iné služby Internetu. Digitálne certifikáty môžete používať na konfiguráciu vašich VPN (virtuálna súkromná sieť) spojení. Kľúč certifikátu tiež môžete použiť na digitálne podpisovanie objektov alebo na kontrolu digitálnych podpisov, ktoré zaručujú autenticitu objektov. Takéto elektronické podpisy zabezpečujú spoľahlivosť pôvodu objektu a ochraňujú integritu objektu.

Systémovú bezpečnosť môžete ďalej rozšíriť pomocou digitálnych certifikátov (namiesto užívateľských mien a hesiel) na autentifikáciu a autorizáciu relácií medzi serverom a užívateľmi. DCM môžete taktiež použiť na združovanie certifikátu užívateľa s jeho alebo jej užívateľským profilom iSeries. Tento certifikát má potom rovnaké oprávnenia a povolenia ako príslušný profil.

Preto to, ako sa rozhodnete použiť certifikáty, môže byť komplikované a závisí na rôznych faktoroch. Scenáre, poskytnuté v tejto kapitole, opisujú niektoré z bežnejších bezpečnostných cieľov digitálnych certifikátov v rámci typických obchodných súvislostí. Každý scenár taktiež opisuje všetky potrebné systémové a softvérové predpoklady a všetky konfiguračné úlohy, ktoré musíte vykonať na implementovanie scenára. Prezrite si tieto scenáre, aby vám pomohli zistiť, ako by mohlo použitie certifikátov pre zvýšenú bezpečnosť najlepšie vyhovovať vašim potrebám:

Scenár: Použite certifikáty na ochranu prístupu do verejných aplikácií a zdrojov
Tento scenár opisuje, kedy a ako použiť certifikáty na ochranu a obmedzenie prístupu verejných užívateľov na verejné alebo extranetové zdroje a aplikácie.

Scenár: Použite certifikáty na ochranu prístupu do interných aplikácií a zdrojov
Tento scenár opisuje, kedy a ako použiť certifikáty na ochranu a obmedzenie toho, na ktoré zdroje a aplikácie na vašich interných serveroch môžu interní užívatelia pristupovať.

Scenár: Použite certifikáty na ochranu prístupu do verejných aplikácií a zdrojov

Situácia

Pracujete pre poisťovňu (MyCo., Inc) a ste zodpovedný za údržbu rôznych aplikácií na intranetových a extranetových stránkach vašej spoločnosti. Jednou konkrétnou aplikáciou, za ktorú ste zodpovedný, je aplikácia na výpočet sadzieb, ktorá umožňuje stovkám nezávislých agentov generovať sadzby pre svojich klientov. Pretože informácie, ktoré táto aplikácia poskytuje, sú tak trocha citlivé, chcete zabezpečiť, aby ich mohli používať iba registrovaní agenti. Navyše chcete eventuálne poskytnúť bezpečnejšiu metódu prístupu užívateľov do aplikácie, ako je vaša súčasná metóda užívateľského mena a hesla. Obávate sa, že neoprávnení užívatelia by mohli zachytiť tieto informácie, keď sú prenášané cez nedôveryhodnú sieť. Taktiež by tieto informácie mohli medzi sebou zdieľať rôzni agenti bez oprávnenia k tomu, aby tak konali.

Po určitom prieskume ste sa rozhodli, že používanie digitálnych certifikátov vám môže poskytnúť bezpečnosť, ktorú potrebujete. Použitie certifikátov vám umožňuje použiť SSL (Secure Sockets Layer) na ochranu prenosu údajov sadzieb. Aj keď chcete, aby nakoniec všetci agenti používali na prístup do aplikácie certifikát, viete, že vaša spoločnosť a jej agenti budú potrebovať nejaký čas, kým bude tento cieľ dosiahnutý. V tomto čase plánujete pokračovať v súčasnej metóde autentifikácie užívateľským menom a heslom, lebo SSL chráni súkromie týchto citlivých údajov pri prenose.

Na základe type aplikácie a jej užívateľoch, ako aj vášho budúceho cieľa autentifikácie užívateľov certifikátom, ste sa rozhodli použiť verejný certifikát zo známej certifikačnej autority (CA) na nakonfigurovanie SSL pre vašu aplikáciu.

Výhody scenára

Tento scenár má nasledovné výhody:
- Použitie digitálnych certifikátov na nakonfigurovanie prístupu do vašej aplikácie na výpočet sadzieb cez SSL zabezpečí, že informácie, prenášané medzi serverom a klientom, sú chránené a súkromné.
- Použitie digitálnych certifikátov, kdekoľvek je to možné, na autentifikáciu klientov, poskytuje bezpečnejšiu metódu identifikovania autorizovaných užívateľov. Aj tam, kde to nie je možné, je autentifikácia klientov prostredníctvom užívateľského mena a hesla chránená a držaná súkromná reláciou SSL, čím sa výmena takýchto citlivých údajov stáva bezpečnejšou.
- Použitie *verejných* digitálnych certifikátov na obmedzenie alebo povolenie prístupu k vašim aplikáciám a údajom je praktická voľba pod týmito alebo podobnými podmienkami:
  - Vaše údaje a aplikácie vyžadujú rôzne stupne bezpečnosti.
  - Existuje vysoká miera zmien medzi vašimi dôveryhodnými užívateľmi.
  - Poskytujete verejný prístup na aplikácie a údaje, ako je miesto internetových web stránok alebo extranetová aplikácia.
  - Nechcete prevádzkovať vašu vlastnú certifikačnú autoritu (CA) kvôli veľkému počtu užívateľov, ktorí pristupujú na vaše aplikácie a zdroje, alebo pre iné administratívne dôvody.
- Použitie verejného certifikátu na konfigurovanie aplikácie na výpočet sadzieb pre SSL v tomto scenári znižuje objem konfigurácie, ktorý musia vykonať užívatelia na prístup k aplikácii. Väčšina klientskeho softvéru obsahuje certifikáty CA pre väčšinu známych CA.

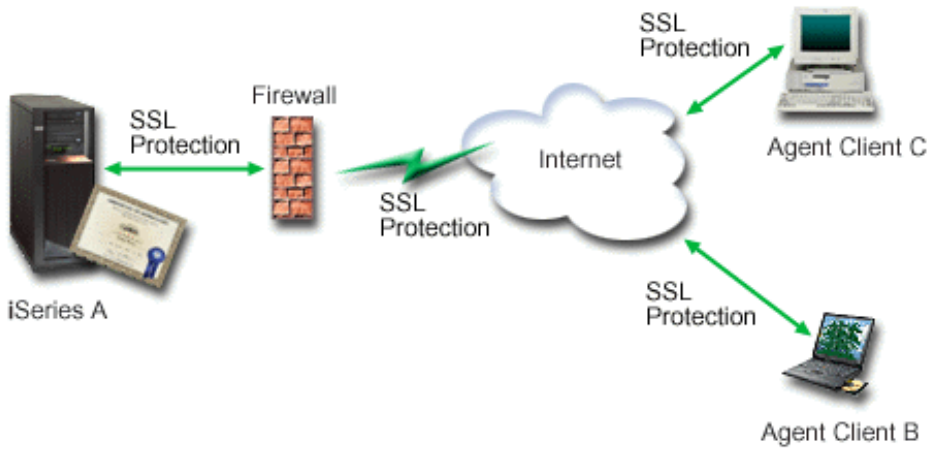
Ciele

V tomto scenári chce MyCo., Inc. používať digitálne certifikáty na ochranu informácií o výpočte sadzieb, ktoré jej aplikácia poskytuje autorizovaným verejným užívateľom. Spoločnosť tiež chce bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolené pristupovať na túto aplikáciu.

Ciele tohto scenára sú nasledovné:
- Verejná aplikácia spoločnosti na výpočet sadzieb musí používať SSL na ochranu utajenia údajov, ktoré poskytuje užívateľom.
- Konfigurácia SSL musí byť uskutočnená s verejnými certifikátmi zo známej verejnej internetovej certifikačnej autority (CA).
- Autorizovaní užívatelia musia poskytnúť platné užívateľské meno a heslo, aby dosiahli prístup na aplikáciu v režime SSL. Prípadne musia byť autorizovaní užívatelia schopní použiť jednu z dvoch metód bezpečnej autentifikácie, aby im bol povolený prístup k aplikácii. Agenti musia poskytnúť buď verejný digitálny certifikát zo známej certifikačnej autority (CA), alebo platné užívateľské meno a heslo.

Podrobnosti

Nasledujúci obrázok ilustruje konfiguráciu siete pre tento scenár:



Obrázok ilustruje nasledujúce informácie o situácii pre tento scenár:

Verejný server spoločnosti – iSeries A
- iSeries A je server, ktorý hosťuje aplikáciu spoločnosti na výpočet sadzieb.
- iSeries A beží na OS/400 Verzia 5 Vydanie 2 (V5R2).
- iSeries A má nainštalovaného poskytovateľa šifrovaného prístupu??? (5722–AC3).
- iSeries A má nainštalovaného a nakonfigurovaného Správcu digitálnych certifikátov (OS/400 voľba 34) a IBM HTTP Server for iSeries (5722–DG1).
- iSeries A prevádzkuje aplikáciu na výpočet sadzieb, ktorá je nakonfigurovaná tak, že:
  - Vyžaduje režim SSL.
  - Používa verejný certifikát zo známej certifikačnej autority (CA) pre konfiguráciu SSL.
  - Vyžaduje autentifikáciu užívateľov užívateľským menom a heslom.
- iSeries A predkladá svoj certifikát na inicializovanie relácie SSL, keď klienti B a C pristupujú na aplikáciu.
- Po inicializovaní relácie SSL iSeries A požiada, aby klienti B a C poskytli platné užívateľské meno a heslo pred povolením prístupu na aplikáciu na výpočet sadzieb.

Klientske systémy agentov – Klient B a Klient C
- Klienti B a C sú nezávislí agenti, ktorí pristupujú na aplikáciu na výpočet sadzieb.
- Klienti B a C majú kópiu certifikátu známej CA, ktorá vydala certifikát aplikácie, nainštalovaný v ich klientskom softvéri.
- Klienti B a C pristupujú do aplikácie na výpočet sadzieb na iSeries A, ktorý predkladá svoj certifikát do ich klientskeho softvéru na overenie jeho identity a spustenie relácie SSL.
- Klientsky softvér na klientoch B a C je nakonfigurovaný tak, aby akceptoval certifikát z iSeries A a relácia SSL začína.
- Po tom, ako začala relácia SSL, klienti B a C musia zadať platné užívateľské meno a heslo pred tým, ako im iSeries A povolí prístup do aplikácie na výpočet sadzieb.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:
1. Aplikácia na výpočet sadzieb na iSeries A je generická??? aplikácia, ktorá môže byť nakonfigurovaná na používanie SSL. Väčšina aplikácií, vrátane mnohých aplikácií iSeries, poskytuje podporu SSL. Konfiguračné kroky SSL sa u rôznych aplikácií líšia. Preto tento scenár neposkytuje presné inštrukcie na konfiguráciu aplikácie na výpočet sadzieb na používanie SSL. Tento scenár poskytuje inštrukcie pre konfiguráciu a správu certifikátov, ktoré sú potrebné pre akúkoľvek aplikáciu, aby používala SSL.
2. *Voliteľne*môže aplikácia na výpočet sadzieb poskytovať schopnosť vyžadovania certifikátov pre autentifikáciu klientov. Tento scenár poskytuje inštrukcie pre to, ako

používať Správcu digitálnych certifikátov (DCM) na nakonfigurovanie dôvery ???certifikátu pre tie aplikácie, ktoré poskytujú túto podporu. Pretože sa konfiguračné kroky pre autentifikáciu klientov medzi aplikáciami líšia tento scenár neposkytuje presné inštrukcie pre konfiguráciu autentifikácie klienta certifikátom pre aplikáciu na výpočet sadzieb.

3. iSeries A spĺňa požiadavky pre nainštalovanie a používanie Správcu digitálnych certifikátov (DCM).
4. Nikto v minulosti nekonfiguroval ani nepoužíval DCM na iSeries A.
5. Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
6. iSeries A nemá nainštalovaný IBM 4758-023 PCI Cryptographic Coprocessor.

Kroky úloh

Na implementovanie tohto scenára musíte vykonať tieto úlohy na iSeries A:

1. Dokončite všetky kroky podmienok na nainštalovanie a nakonfigurovanie všetkých potrebných produktov iSeries.
2. Použite Správcu digitálnych certifikátov (DCM) na vytvorenie požiadavky na serverovský certifikát.
3. Nakonfigurujte vašu aplikáciu na používanie Secure Sockets Layer (SSL).
4. Použite DCM na importovanie a priradenie podpísaného serverovského a klientskeho certifikátu k ID aplikácie pre vašu aplikáciu.
5. Spustite aplikáciu v režime SSL, ak je to potrebné.
6. *Voliteľné úlohy*: Použite DCM na definovanie zoznamu dôveryhodných CA na umožnenie autentifikácie klientov, založenej na certifikátoch pre aplikácie, ktoré poskytujú túto podporu.

   Poznámka: Situácia, ktorú tento scenár opisuje, nevyžaduje, aby aplikácia na výpočet sadzieb používala certifikáty pre autentifikáciu klientov. Mnoho aplikácií poskytuje podporu autentifikácie klientov certifikátom; ako nakonfigurujete túto podporu, závisí od aplikácií. Táto voliteľná úloha je poskytnutá na to, aby vám pomohla pochopiť, ako použiť DCM na aktivovanie dôvery v certifikát pre autentifikáciu klienta ako podklad pre konfigurovanie podpory autentifikácie klienta certifikátom vo vašej aplikácii.

Podrobnosti konfigurácie

Dokončite nasledovné kroky úloh na použitie certifikátov na konfigurovanie chráneného verejného prístupu do aplikácií a zdrojov, ako to popisuje tento scenár.

Krok 1: Dokončite úlohy predpokladov na nainštalovanie všetkých potrebných produktov iSeries

Pred tým, ako budete môcť vykonať špecifické konfiguračné úlohy pre implementovanie tohto scenára, musíte dokončiť všetky úlohy požiadaviek na nainštalovanie a konfiguráciu všetkých potrebných produktov iSeries.

Krok 2: Vytvoriť požiadavku na serverovský alebo klientsky certifikát

Na začatie procesu používania SSL (Secure Sockets Layer) na ochranu údajových komunikácií aplikácie, ako to popisuje tento scenár, musíte najprv získať digitálny certifikát z verejnej certifikačnej autority (CA). Použite Správcu digitálnych certifikátov (DCM) na vytvorenie informácií, ktoré verejná CA vyžaduje na vydanie certifikátu.

Na začatie procesu získavania vášho certifikátu dokončite tieto kroky:

1. Spustite DCM.
2. V navigačnej časti DCM vyberte **Vytvoriť novú pamäť certifikátov**, aby sa spustila úloha a mohli ste vyplniť sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia pamäte certifikátov a certifikátu, ktoré môžu vaše aplikácie použiť pre SSL relácie.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Zvoľte ***SYSTEM** ako pamäť certifikátov, ktorá sa má vytvoriť a kliknite na **Pokračovať**.
4. Vyberte **Áno**, aby sa certifikát vytvoril ako časť vytvárania pamäte certifikátov *SYSTEM a kliknite na **Pokračovať**.
5. Ako podpisovateľa nového certifikátu vyberte **VeriSign alebo iná internetová Certifikačná autorita (CA)** a kliknite na **Pokračovať**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačnú informácie pre nový certifikát.
6. Vyplňte formulár a kliknite na **Pokračovať**, aby sa zobrazila strana s potvrdením. Táto potvrdzovacia strana zobrazuje údaje požiadavky na certifikát, ktoré musíte poskytnúť verejnej Certifikačnej autorite (CA), ktorá vydá váš certifikát. Údaje CSR (Certificate Signing Request) obsahujú verejný kľúč a iné informácie, ktoré ste špecifikovali pre nový certifikát.
7. Pozorne skopírujte a vložte údaje CSR do aplikačného formulára certifikátu, alebo do samostatného súboru, ktoré požaduje verejná CA na vyžiadanie certifikátu. Musíte použiť všetky údaje CSR, vrátane riadkov Begin a End New Certificate Request. Keď odídete z tejto strany, údaje sa stratia a nedajú sa už obnoviť.
8. Pošlite tento aplikačný formulár alebo súbor do CA, ktorú ste vybrali na vydanie a podpísanie vášho certifikátu.
9. Počkajte, kým CA vráti podpísaný, dokončený certifikát pred tým, ako budete pokračovať ďalším krokom úlohy pre scenár.

Po tom, ako CA vráti podpísaný, dokončený certifikát, môžete nakonfigurovať vašu aplikáciu na používanie SSL, importovať certifikát do pamäte certifikátov *SYSTEM a priradiť ho vašej aplikácii na použitie pre SSL.

Krok 3: Nakonfigurujte aplikáciu na používanie SSL

Keď prijmete váš podpísaný certifikát späť z verejnej certifikačnej autorita (CA), môžete pokračovať v procese aktivovania komunikácií SSL (Secure Sockets Layer) pre vašu verejnú aplikáciu. Pred prácou s vaším podpísaným certifikátom by ste mali nakonfigurovať vašu aplikáciu na používanie SSL. Niektoré aplikácie, také ako HTTP Server for iSeries, generujú jedinečné ID aplikácie a registrujú ID so Správcom digitálnych certifikátov (DCM), keď konfigurujete aplikáciu na používanie SSL. Predtým, ako budete môcť použiť DCM na priradenie podpísaného certifikátu k ID aplikácie a dokončiť proces konfigurácie SSL, musíte ID aplikácie poznať.

To, ako nakonfigurujete vašu aplikáciu na používanie SSL, sa mení na základe aplikácie. Tento scenár nepredpokladá presný zdroj pre aplikáciu na výpočet sadzieb, ktorú opisuje, lebo je niekoľko spôsobov, ktorými by mohol MyCo., Inc. poskytnúť túto aplikáciu svojim agentom.

Na nakonfigurovanie vašej aplikácie na používanie SSL postupujte podľa inštrukcií, ktoré poskytne dokumentácia vašej aplikácie. Taktiež by ste sa mohli dozvedieť viac o konfigurovaní mnohých bežných aplikácií IBM na používanie SSL prezretím článku Zabezpečte aplikácie s SSL v Informačnom centre.

Krok 4: Importujte a priraďte podpísaný verejný certifikát

Po tom, čo nakonfigurujete vašu aplikáciu na používanie SSL, môžete použiť Správcu digitálnych certifikátov (DCM) na import vášho podpísaného certifikátu a jeho priradenie vašej aplikácii.

Na import vášho certifikátu a jeho priradenie vašej aplikácii na dokončenie procesu konfigurovania SSL postupujte podľa týchto krokov:

1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Importovať certifikát**, aby sa spustil proces importu podpísaného certifikátu do pamäte certifikátov *SYSTEM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
6. Ďalej zo zoznamu úloh **Manažovať certifikáty** vyberte **Priradiť certifikát** na zobrazenie zoznamu certifikátov pre aktuálnu pamäť certifikátov.
7. Vyberte certifikát zo zoznamu a kliknite na **Priradiť aplikáciám** na zobrazenie zoznamu definícií aplikácií pre aktuálnu pamäť certifikátov.
8. Vyberte vašu aplikáciu zo zoznamu a kliknite na **Pokračovať**. Zobrazí sa stránka s potvrdzovacou správou pre váš výber priradenia, alebo s chybovým hlásením, ak nastal problém.

Ak máte tieto úlohy dokončené, môžete spustiť vašu aplikáciu v režime SSL a začať s ochranou utajenia údajov, ktoré poskytuje.

Krok 5: Spustite aplikáciu v režime SSL

Po dokončení procesu importovania a priradenia certifikátu k vašej aplikácii môžete potrebovať ukončiť a reštartovať vašu aplikáciu v režime SSL. Je to v niektorých prípadoch nutné, lebo aplikácia nemusí byť schopná zistiť, že existuje priradenie certifikátu, kým aplikácia beží. Prezrite si dokumentáciu vašej aplikácie na zistenie, či ju potrebujete reštartovať, alebo pre iné špecifické informácie o spúšťaní aplikácie v režime SSL.

Voliteľná úloha 6: Definujte zoznam dôveryhodných CA pre aplikáciu, ktorá vyžaduje certifikáty pre autentifikáciu klientov

Aplikácie, ktoré podporujú použitie certifikátov na autentifikáciu klienta počas Secure Sockets Layer (SSL) relácie musia určiť, či budú akceptovať certifikát ako platný dôkaz identity. Jedným z kritérií, ktoré aplikácia používa na autentifikáciu certifikátu je to, či aplikácia dôveruje Certifikačnej autorite (CA), ktorá vydala daný certifikát.

Situácia, ktorú tento scenár opisuje, nevyžaduje, aby aplikácia na výpočet sadzieb používala certifikáty pre autentifikáciu klientov. Mnoho aplikácií poskytuje podporu autentifikácie klientov certifikátom; ako nakonfigurujete túto podporu, závisí od aplikácií. Táto voliteľná úloha je poskytnutá na to, aby vám pomohla pochopiť, ako použiť DCM na aktivovanie dôvery v certifikát pre autentifikáciu klienta ako podklad pre konfigurovanie vašich aplikácií na používanie certifikátov na autentifikáciu klientov.

Aby ste mohli zadefinovať zoznam dôveryhodných CA pre aplikáciu, musí byť splnených niekoľko podmienok:

- Aplikácia musí podporovať použitie certifikátov na autentifikáciu klientov.
- Definícia DCM pre aplikáciu musí určovať, že aplikácia používa zoznam dôveryhodných CA.

Ak definícia pre aplikáciu špecifikuje, že aplikácia používa zoznam dôveryhodných CA, tento zoznam musíte zadefinovať a až potom môže aplikácia úspešne vykonať autentifikáciu klientov. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Na použitie DCM na zadefinovanie zoznamu dôveryhodných CA vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Nastaviť stav CA** na zobrazenie zoznamu certifikátov CA.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
6. Vyberte zo zoznamu certifikát CA, ktorému by mala vaša aplikácia dôverovať a kliknite na **Povoliť** na zobrazenie zoznamu aplikácií, ktoré používajú zoznam dôveryhodných CA.
7. Vyberte zo zoznamu aplikáciu, ktorá by mala pridať zvolenú CA do svojho zoznamu dôveryhodných CA a kliknite na **OK**. Na vrchole stránky sa zobrazí správa, oznamujúca, že aplikácia, ktorú ste vybrali, bude dôverovať CA certifikátom, ktoré vydáva.

Teraz môžete nakonfigurovať vašu aplikáciu na vyžadovanie certifikátov na autentifikáciu klientov. Postupujte podľa inštrukcií, poskytnutých dokumentáciou pre vašu aplikáciu.

Scenár: Použite certifikáty na ochranu prístupu do interných aplikácií a zdrojov

Situácia

Ste správcom siete v spoločnosti (MyCo., Inc.), ktorej oddelenie ľudských zdrojov sa zaujíma o také otázky, ako právne záležitosti a utajenie záznamov. Zamestnanci spoločnosti žiadali, aby boli schopní pristupovať online ku svojim informáciám o osobných výhodách a starostlivosti o zdravie. Spoločnosť odpovedala na túto požiadavku vytvorením internej web stránky na poskytovanie týchto informácií zamestnancom. Vy ste zodpovedný za správu tejto internej web stránky.

Pretože sa zamestnanci nachádzajú v dvoch geograficky oddelených úradoch a niektorí zamestnanci často cestujú, obávate sa o udržanie utajenia týchto informácií, keďže prechádzajú internetom. Taktiež na obmedzenie prístupu k údajom spoločnosti tradične používate autentifikáciu užívateľským menom a heslom. Kvôli citlivej a súkromnej podstate týchto údajov si uvedomujete, že obmedzenie prístupu k nim, založené na heslách, nemusí byť dostačujúce. Okrem toho, ľudia môžu heslá zdieľať, zabudnúť, či dokonca ukradnúť.

Po určitom prieskume ste sa rozhodli, že používanie digitálnych certifikátov vám môže poskytnúť bezpečnosť, ktorú potrebujete. Použitie certifikátov vám umožňuje použiť SSL (Secure Sockets Layer) na ochranu prenosu údajov. Navyše môžete namiesto hesiel použiť certifikáty na bezpečnejšiu autentifikáciu užívateľov a limitovanie informácií o ľudských zdrojoch, ku ktorým môžu pristúpiť.

Z týchto dôvodov sa rozhodnete nastaviť súkromnú lokálnu certifikačnú autoritu (CA) a vydávať certifikáty všetkým zamestnancom a združiť ich certifikáty s ich užívateľskými profilmi iSeries. Tento typ implementácie súkromných certifikátov vám umožňuje presnejšie riadiť prístup k citlivým údajom, ako aj riadiť súkromie údajov prostredníctvom SSL. Na záver, keď budete vydávať certifikáty vy sami, máte zvýšenú pravdepodobnosť, že vaše údaje zostanú bezpečné a budú na ne pristupovať len konkrétne osoby.

Výhody scenára

Tento scenár má nasledovné výhody:
- Použitie digitálnych certifikátov na nakonfigurovanie prístupu na váš web server ľudských zdrojov cez SSL zabezpečí, že informácie, prenášané medzi serverom a klientom, budú chránené a súkromné.
- Použitie digitálnych certifikátov na autentifikáciu klientov poskytuje bezpečnejšiu metódu identifikovania autorizovaných užívateľov.
- Použitie *súkromných* digitálnych certifikátov na obmedzenie alebo povolenie prístupu k vašim aplikáciám a údajom je praktická voľba pod týmito alebo podobnými podmienkami:
  - Požadujete vysoký stupeň bezpečnosti, hlavne s ohľadom na autentifikáciu užívateľov.
  - Dôverujete jedincom, ktorým vydávate certifikáty.
  - Vaši užívatelia už majú užívateľské profily iSeries pre riadenie ich prístupu k aplikáciám a údajom.
  - Chcete prevádzkovať vlastnú Certifikačnú autoritu (CA).
- Používanie súkromných certifikátov na autentifikáciu klientov vám umožňuje ľahšie združovať certifikát s užívateľským profilom iSeries autorizovaného užívateľa. Toto združenie certifikátu s užívateľským profilom umožňuje serveru HTTP zistiť užívateľský profil vlastníka certifikátu počas autentifikácie. HTTP Server potom môže zmeniť naňho ??? a bežať pod týmto užívateľským profilom, alebo vykonať akcie pre tohto užívateľa na základe informácií v jeho užívateľskom profile.

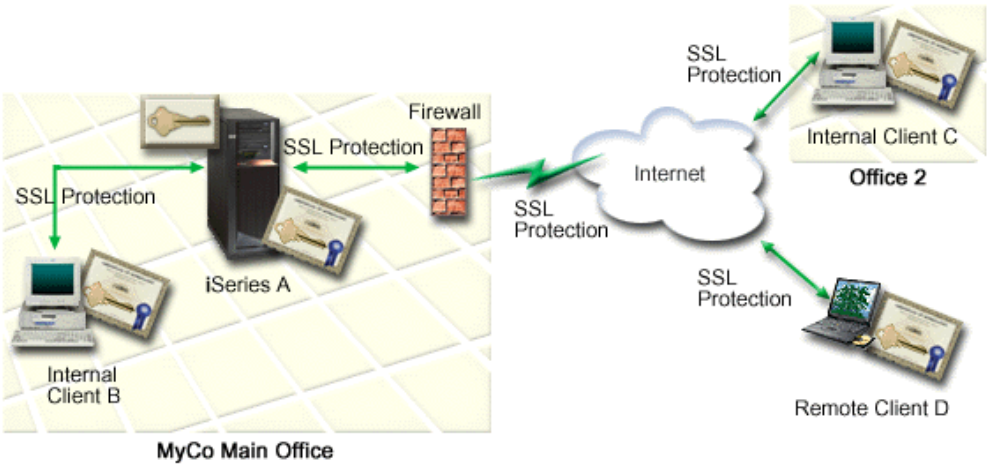
Ciele

V tomto scenári chce MyCo., Inc. používať digitálne certifikáty na ochranu citlivých osobných informácií, ktoré jej interná web stránka ľudských zdrojov poskytuje zamestnancom spoločnosti. Spoločnosť tiež chce bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolené pristupovať na túto web stránku.

Ciele tohto scenára sú nasledovné:
- Interná web stránka ľudských zdrojov spoločnosti musí používať SSL na ochranu utajenia údajov, ktoré poskytuje užívateľom.
- Konfigurácia SSL musí byť uskutočnená so súkromnými certifikátmi z internej lokálnej certifikačnej autority (CA).
- Autorizovaní užívatelia musia poskytnúť platný certifikát, aby dosiahli prístup na web stránku v režime SSL.

Podrobnosti

Nasledujúci obrázok ilustruje konfiguráciu siete pre tento scenár:



Obrázok ilustruje nasledujúce informácie o situácii pre tento scenár:

Web server ľudských zdrojov spoločnosti – iSeries A
- iSeries A je server, ktorý hosťuje web aplikáciu ľudských zdrojov spoločnosti.
- iSeries A beží na OS/400 Verzia 5 Vydanie 2 (V5R2).
- iSeries A má nainštalovaného poskytovateľa šifrovaného prístupu??? (5722–AC3).
- iSeries A má nainštalovaného a nakonfigurovaného Správcu digitálnych certifikátov (OS/400 voľba 34) a IBM HTTP Server for iSeries (5722–DG1).
- iSeries A prevádzkuje aplikáciu ľudských zdrojov, ktorá je nakonfigurovaná tak, že:
  - Vyžaduje režim SSL.
  - Používa súkromný certifikát z lokálnej certifikačnej autority (CA) pre konfiguráciu SSL.
  - Vyžaduje certifikáty pre autentifikáciu klientov.
- iSeries A predkladá svoj certifikát na inicializovanie relácie SSL, keď klienti B, C a D pristupujú na aplikáciu.
- Po inicializovaní relácie SSL iSeries A požiada, aby klienti B, C a D poskytli platný certifikát pred povolením prístupu na aplikáciu ľudských zdrojov. Táto výmena certifikátov je pre užívateľov klientov B, C a D transparentná.

Systémy klientov zamestnancov – klient B, klient C a klient D
- Klient B je zamestnanec, ktorý pracuje v hlavnom sídle MyCo, kde sa nachádza iSeries A.
- Klient C je zamestnanec, ktorý pracuje v sekundárnom sídle MyCo, ktoré je geograficky oddelené od hlavného sídla.
- Klient D je zamestnanec, ktorý pracuje vzdialene a často cestuje na obchody spoločnosti??? a musí byť schopný bezpečne pristupovať na web stránku ľudských zdrojov, bez ohľadu na to, kde sa fyzicky nachádza.
- Klienti B, C a D sú zamestnanci spoločnosti, ktorí pristupujú na aplikáciu ľudských zdrojov.
- Klienti B, C a D majú všetci kópiu certifikátu lokálnej CA, ktorý vydal certifikát aplikácie, nainštalovaný v ich klientskom softvéri.
- Klienti B, C a D pristupujú do aplikácie ľudských zdrojov na iSeries A, ktorý predkladá svoj certifikát do ich klientskeho softvéru na overenie jeho identity a spustenie relácie SSL.
- Klientsky softvér na klientoch B, C a D je nakonfigurovaný tak, aby akceptoval certifikát z iSeries A a relácia SSL začína.
- Po tom, ako začala relácia SSL, klienti B, C a D musia poskytnúť platný certifikát pred tým, ako im iSeries A povolí prístup do aplikácie a svojich zdrojov.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:

1. IBM HTTP Server for iSeries prevádzkuje aplikáciu ľudských zdrojov na iSeries A. Existujú dva typy HTTP Server for iSeries (originál a powered by Apache) a významne revised upravená verzia HTTP Servera bude dostupná po publikovaní týchto informácií. Preto tento scenár neposkytuje *presné* inštrukcie na konfiguráciu servera HTTP na používanie SSL. Tento scenár poskytuje inštrukcie pre konfiguráciu a správu certifikátov, ktoré sú potrebné pre akúkoľvek aplikáciu, aby používala SSL.
2. HTTP Server poskytuje schopnosť vyžadovania certifikátov pre autentifikáciu klientov. Tento scenár poskytuje inštrukcie pre použitie Správcu digitálnych certifikátov (DCM) na nakonfigurovanie požiadaviek manažmentu certifikátu pre tento scenár. Avšak tento scenár neposkytuje *presné* inštrukcie pre konfiguráciu autentifikácie klienta certifikátom pre server HTTP.
3. Server HTTP ľudských zdrojov na iSeries A už používa ochranu heslom.
4. iSeries A spĺňa požiadavky pre nainštalovanie a používanie Správcu digitálnych certifikátov (DCM).
5. Nikto v minulosti nekonfiguroval ani nepoužíval DCM na iSeries A.
6. Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
7. iSeries A nemá nainštalovaný IBM 4758-023 PCI Cryptographic Coprocessor.

Kroky úloh

Na implementovanie tohto scenára musíte dokončiť dve skupiny úloh: Jedna skupina úloh vám umožňuje nastaviť aplikáciu ľudských zdrojov na iSeries A na používanie SSL a vyžadovanie certifikátov na autentifikáciu užívateľov. Druhá skupina úloh umožňuje vašim užívateľom na klientoch B, C a D participovať v relácii SSL s aplikáciou ľudských zdrojov a získať certifikáty na autentifikáciu užívateľov.

Kroky úloh aplikácie web servera ľudských zdrojov

Na implementovanie tohto scenára musíte vykonať tieto úlohy na iSeries A:

1. Dokončite všetky kroky podmienok na nainštalovanie a nakonfigurovanie všetkých potrebných produktov iSeries.
2. Nakonfigurujte váš server HTTP ľudských zdrojov na používanie SSL a poznačte si ID aplikácie pre inštanciu servera.
3. Použite Správcu digitálnych certifikátov (DCM) na vytvorenie a prevádzkovanie lokálnej CA a použite ju na vydanie certifikátu pre server HTTP ľudských zdrojov. Táto riadená úloha taktiež zabezpečí, aby ste priradili certifikát aplikácii web servera a pridali CA do zoznamu tých, ktorým aplikácia dôveruje.
4. Nakonfigurujte web server ľudských zdrojov na vyžadovanie certifikátov na autentifikáciu klientov.
5. Spustite server HTTP ľudských zdrojov v režime SSL.

Kroky úloh konfigurácie klientov

Na implementovanie tohto scenára musí každý užívateľ (klienti B, C a D), ktorý bude pristupovať na web server ľudských zdrojov na iSeries A, vykonať tieto úlohy:

6. Nainštalovať kópiu certifikátu lokálnej CA do ich softvéru prehliadača.
7. Požiadať o certifikát z lokálnej CA.

Podrobnosti konfigurácie

Dokončite nasledovné kroky úloh na použitie certifikátov na konfigurovanie chráneného prístupu do interných aplikácií a zdrojov, ako to popisuje tento scenár.

Krok 1: Dokončite úlohy predpokladov na nainštalovanie všetkých potrebných produktov iSeries

Pred tým, ako budete môcť vykonať špecifické konfiguračné úlohy pre implementovanie tohto scenára, musíte dokončiť všetky úlohy požiadaviek na nainštalovanie a konfiguráciu všetkých potrebných produktov iSeries.

Krok 2: Nakonfigurujte server HTTP ľudských zdrojov na používanie SSL

Kroky konfigurácie SSL (Secure Sockets Layer) pre server HTTP ľudských zdrojov na iSeries A sa menia na základe toho, či používate originál, alebo verziu powered by Apache???.

Pozrite si časť Konfigurovať bezpečný server na HTTP Server, kde nájdete špecifické informácie o konfigurovaní servera HTTP (originálu) na používanie SSL.

Pozrite si kapitolu Scenár: JKL aktivuje ochranu SSL (Secure Sockets Layer) na ich serveri HTTP (powered by Apache), kde nájdete špecifické informácie o konfigurovaní servera HTTP (powered by Apache) na používanie SSL. Tento scenár poskytuje všetky kroky úloh pre vytvorenie virtuálneho hostiteľa a jeho nakonfigurovanie na použitie SSL. Pre špecifické kroky na konfigurovanie SSL si pozrite nadpis ″Aktivovať SSL pre virtuálneho hostiteľa.″

Ďalšie informácie o konfigurovaní aktuálnej aj budúcich verzií HTTP Server for iSeries (originál alebo powered by Apache) nájdete v téme Web serving.

Krok 3: Vytvorte a prevádzkujte lokálnu CA

Po tom, čo ste nakonfigurovali server HTTP ľudských zdrojov na používanie SSL (Secure Sockets Layer), musíte nakonfigurovať certifikát pre server, ktorý sa má používať na spustenie SSL. Na základe cieľov pre tento scenár ste sa rozhodli vytvoriť a prevádzkovať lokálnu certifikačnú autoritu (CA) na vydanie certifikátu serveru.

Keď použijete Správcu digitálnych certifikátov (DCM) na vytvorenie lokálnej CA, ste prevedený procesom, ktorý zabezpečí, že nakonfigurujete všetko, čo potrebujete na aktivovanie SSL pre vašu aplikáciu. To zahŕňa pridelenie certifikátu, ktorý vydáva lokálna CA, do vašej aplikácie web servera. Taktiež pridáte lokálnu CA do zoznamu dôveryhodných CA aplikácie web servera. Prítomnosť lokálnej CA v zozname dôveryhodných CA aplikácie zabezpečí, že aplikácia bude môcť rozoznať a autentifikovať užívateľov, ktorí predložia certifikát, ktorý vydá lokálna CA.

Na použitie Správcu digitálnych certifikátov (DCM) na vytvorenie a prevádzkovanie lokálnej CA a vydanie certifikátu serveru aplikácie ľudských zdrojov vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti DCM vyberte **Vytvoriť Certifikačnú autoritu**, aby sa zobrazila séria formulárov. Tieto formuláre vás prevedú procesom vytvorenia lokálnej CA a dokončením ďalších úloh, potrebných na začatie používania digitálnych certifikátov pre SSL, podpisovanie objektov a overovanie podpisov.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Vyplňte formuláre pre túto riadenú úlohu. Použitím týchto formulárov na vykonanie všetkých úloh, ktoré potrebujete na nastavenie fungujúcej lokálnej certifikačnej autority (CA):
   a. Poskytnite identifikačné informácie pre lokálnu CA.
   b. Nainštalujte certifikát lokálnej CA na váš PC alebo do vášho prehliadača, aby váš softvér mohol rozpoznať lokálnu CA a overiť certifikáty, ktoré lokálna CA vydá.

c. Zvoľte údaje politiky pre vašu lokálnu CA.

   Poznámka: Uistite sa, či ste označili, že lokálna CA môže vydávať užívateľské certifikáty.

d. Použite novú lokálnu CA na vydanie serverovského alebo klientskeho certifikátu, ktorý vaše aplikácie budú môcť použiť pre pripojenia SSL.

e. Vyberte aplikácie, ktoré môžu používať certifikát servera alebo klienta pre SSL spojenia.

   Poznámka: Ubezpečte sa, že ste vybrali ID aplikácie pre váš server HTTP ľudských zdrojov.

f. Použite novú lokálnu CA na vydanie certifikátu na podpisovanie objektov, ktorý aplikácie budú môcť použiť na elektronické podpisovanie objektov. Táto podúloha vytvorí pamäť certifikátov *OBJECTSIGNING; toto je pamäť certifikátov, ktorú používate na manažovanie certifikátov, podpisujúcich objekty.

   Poznámka: Aj keď tento scenár nepoužíva certifikáty na podpisovanie objektov, určite dokončite tento krok. Ak to prerušíte v tomto bode úlohy, úloha skončí a vy budete musieť vykonať oddelené úlohy na dokončenie konfigurácie vášho certifikátu SSL.

g. Zvoľte aplikácie, ktoré by mali dôverovať lokálnej CA.

   Poznámka: Ubezpečte sa, že ste vybrali ID aplikácie pre váš server HTTP ľudských zdrojov ako jednu z aplikácií, ktoré dôverujú lokálnej CA.

Teraz, keď ste dokončili konfiguráciu certifikátu, ktorý vaša aplikácia web servera potrebuje na používanie SSL, môžete nakonfigurovať aplikáciu web servera na vyžadovanie certifikátov pre autentifikáciu užívateľov.

Krok 4: Nakonfigurujte web server ľudských zdrojov na vyžadovanie certifikátov pre autentifikáciu klientov

Kroky konfigurácie SSL (Secure Sockets Layer) na vyžadovanie certifikátov pre autentifikáciu klientov pre server HTTP ľudských zdrojov na iSeries A sa menia na základe toho, či používate originál aplikácie, alebo verziu powered by Apache???.

Pozrite si časť Vytvoriť nastavenia ochrany na HTTP Server (originál), kde nájdete špecifickejšie informácie o konfigurovaní servera HTTP (originálu) na vyžadovanie certifikátov pre autentifikáciu klientov.

Pozrite si kapitolu Scenár: JKL aktivuje ochranu SSL (Secure Sockets Layer) na ich serveri HTTP (powered by Apache), kde nájdete špecifické informácie o konfigurovaní servera HTTP (powered by Apache) na vyžadovanie certifikátov pre autentifikáciu klientov. Tento scenár servera HTTP poskytuje všetky kroky úloh pre vytvorenie virtuálneho hostiteľa a jeho nakonfigurovanie na použitie SSL a certifikátov na autentifikáciu klientov. Pre špecifické kroky na konfigurovanie SSL a certifikátov na autentifikáciu klientov si pozrite nadpis ″Aktivovať SSL pre virtuálneho hostiteľa.″

Ďalšie informácie o konfigurovaní aktuálnej aj budúcich verzií HTTP Server for iSeries (originál alebo powered by Apache) nájdete v téme Web serving.

Krok 5: Spustite server HTTP ľudských zdrojov v režime SSL

Môžete potrebovať zastaviť a reštartovať váš server HTTP na zabezpečenie toho, že je server schopný zistiť, že existuje priradenie certifikátu a použiť ho na inicializáciu relácií SSL.

Na zastavenie a spustenie servera HTTP (originál) použite formuláre Konfigurácia a Administrácia a postupujte podľa týchto krokov:
1. Kliknite na **Administrácia**.
2. Kliknite na **Riadiť servery HTTP**.
3. Vyberte server.
4. Zadajte voliteľné parametre spustenia do poľa, ktoré je poskytnuté vo formulári.
5. Kliknite na **Spustiť**.

Poznámka: Ak server bežal, keď ste robili priradenia certifikátov, mali by ste Zastaviť a potom Spustiť server. Kliknutie na **Reštart** nezabezpečí vždy, že je server schopný zistiť zmeny certifikátov, ktoré nastali, kým bežal.

Na zastavenie a spustenie servera HTTP (powered by Apache) použite formuláre Konfigurácia a Administrácia a postupujte podľa týchto krokov:
1. Kliknite na **Administrácia**.
2. V ponuke vľavo kliknite na **Riadiť servery HTTP** pod **Všeobecná správa serverov**.
3. Vyberte server, s ktorým chcete pracovať, potom kliknite na **Spustiť** alebo **Zastaviť**. Pozrite si online pomoc pre viac informácií o spúšťacích parametroch.

Ďalšie informácie o riadení aktuálnej aj budúcich verzií HTTP Server for iSeries (originál alebo powered by Apache) nájdete v téme Web serving.

Ak máte tieto úlohy dokončené, môžete spustiť vašu aplikáciu ľudských zdrojov v režime SSL a začať s ochranou utajenia údajov, ktoré poskytuje.

Krok 6: Zariaďte, aby si užívatelia nainštalovali kópiu certifikátu lokálnej CA do svojho softvéru prehliadača.

Keď užívatelia pristúpia na server, ktorý poskytuje pripojenie SSL (Secure Sockets Layer), server predkladá certifikát do užívateľovho klientskeho softvéru ako dôkaz svojej identity. Klientsky softvér musí potom overiť platnosť certifikátu servera, predtým ako server vytvorí reláciu. Na overenie platnosti certifikátu servera musí mať klientsky softvér prístup k lokálne uloženej kópii certifikátu pre certifikačnú autoritu (CA), ktorá vydala certifikát servera. Ak server predkladá certifikát z verejnej internetovej CA, váš prehliadač alebo iný klientsky softvér by už mal mať kópiu tohto certifikátu CA. Ak, ako v tomto scenári, server predkladá certifikát zo súkromnej lokálnej CA, každý užívateľ musí použiť Správcu digitálnych certifikátov (DCM) na nainštalovanie kópie certifikátu lokálnej CA.

Každý užívateľ (klienti B, C a D) musí dokončiť tieto kroky na získanie kópie certifikátu lokálnej CA:
1. Spustite DCM.
2. V navigačnom rámci vyberte **Nainštalovať certifikát lokálnej CA na váš PC** na zobrazenie stránky, ktorá vám umožní stiahnuť certifikát lokálnej CA do vášho prehliadača, alebo ho uložiť do súboru na vašom systéme.
3. Vyberte voľbu na inštaláciu certifikátu. Táto voľba stiahne certifikát lokálnej CA ako dôveryhodný zdroj do vášho prehliadača. To zabezpečí, že váš prehliadač bude môcť vytvoriť bezpečné komunikačné relácie s web servermi, ktoré používajú certifikát z tejto CA. Váš prehliadač zobrazí sériu okien, ktoré vám pomôžu dokončiť inštaláciu.
4. Kliknite na **OK** na návrat na domovskú stránku Správcu digitálnych certifikátov.

Krok 7: Zariaďte, aby užívatelia požiadali o certifikát z lokálnej CA

V predošlých krokoch ste nakonfigurovali web server ľudských zdrojov, aby vyžadoval certifikáty na autentifikáciu klientov. Teraz musia užívatelia predložiť platný certifikát z lokálnej CA pred tým, ako im bude povolené pristúpiť na web server. Každý užívateľ musí

použiť Správcu digitálnych certifikátov (DCM) na získanie certifikátu prostredníctvom úlohy **Vytvoriť certifikát**. Na získanie certifikátu z lokálnej CA musí politika lokálnej CA umožniť CA vydať užívateľské certifikáty.

Každý užívateľ (klienti B, C a D) musí dokončiť tieto kroky na získanie certifikátu:

1. Spustite DCM.
2. V navigačnej časti vyberte **Vytvoriť certifikát**.
3. Ako typ certifikátu na vytvorenie vyberte **Užívateľský certifikát**. Zobrazí sa formulár, na ktorom môžete zadať identifikačné informácie pre certifikát.
4. Vyplňte formulár a kliknite na **Pokračovať**.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
5. Na tomto mieste spolupracuje DCM s vašim prehliadačom pri vytvorení súkromného a verejného kľúča pre certifikát. Váš prehliadač môže zobraziť okná, ktoré vás povedú týmto procesom. Postupujte podľa inštrukcií prehliadača pre tieto úlohy. Keď prehliadač vygeneruje kľúče, zobrazí sa potvrdzovacia strana, ktorá oznamuje, že DCM vytvoril certifikát.
6. Nainštalujte nový certifikát do vášho prehliadača. Váš prehliadač môže zobraziť okná, ktoré vás povedú týmto procesom. Aby ste dokončili túto úlohu, postupujte podľa inštrukcií, ktoré vám poskytne prehliadač.
7. Kliknite na **OK** na ukončenie úlohy.

Počas spracovania, Správca digitálnych certifikátov automaticky spojí certifikát s vašim užívateľským profilom iSeries.

Kapitola 5. Pojmy digitálnych certifikátov

Predtým, ako začnete používať digitálne certifikáty na vylepšenie systémovej a sieťovej bezpečnostnej politiky, mali by ste rozumieť tomu čo sú a aké bezpečnostné výhody poskytujú.

Digitálny certifikát predstavuje digitálne povoľovacie údaje, ktoré validujú vlastníka certifikátu viac, ako heslo. Dôveryhodná strana, nazývaná certifikačná autorita (CA), vydáva digitálne certifikáty užívateľom a aplikáciám serverov alebo klientov. Základom dôvery voči certifikátu ako platným povoľovacím údajom je dôvera v CA.

Ak sa chcete dozvedieť viac o pojmoch digitálnych certifikátov, prezrite si tieto témy:

Rozoznaný názov
Tieto informácie si prečítajte, aby ste sa dozvedeli viac o identifikačných charakteristikách digitálnych certifikátov.

Digitálne podpisy
Tieto informácie si prečítajte, aby ste sa dozvedeli, čo sú elektronické podpisy a ako pracujú na zabezpečení integrity objektov.

Pár verejný-súkromný kľúč
Tieto informácie si prečítajte, aby ste sa dozvedeli viac o bezpečnostných kľúčoch, združených s digitálnymi certifikátmi.

Certifikačná autorita (CA)
V týchto informáciách sa dozviete viac o CA, entitách, ktoré vydávajú digitálne certifikáty.

Umiestnenia CRL
V týchto informáciách sa dozviete, čo je Certificate Revocation List (CRL) a ako sa používa v procese validizácie a autentifikácie certifikátov.

Pamäte certifikátov
V týchto informáciách sa dozviete o tom, čo to je pamäť certifikátov a ako používať Správcu digitálnych certifikátov (DCM) na prácu s nimi a s certifikátmi, ktoré obsahujú.

Kryptografia
V týchto informáciách sa dočítate viac o tom, čo to je kryptografia a ako používajú digitálne certifikáty kryptografické funkcie na poskytovanie bezpečnosti.

Secure Sockets Layer (SSL)
V týchto informáciách sa nachádza stručný popis SSL.

Rozoznaný názov

Každá CA má politiku na určenie, aké identifikačné informácie vyžaduje CA na vydanie certifikátu. Niektoré verejné internetové Certifikačné autority môžu vyžadovať menej informácií, ako je meno a e-mailová adresa. Ostatné verejné CA môžu vyžadovať viac informácií a vyžadujú striktný dôkaz identifikačných informácií pred vydaním certifikátu. Napríklad, CA, ktoré podporujú štandardy Public Key Infrastructure Exchange (PKIX), môžu pred vydaním certifikátu požadovať od žiadateľa overenie informácií o identite cez Registračnú autoritu (RA). Následne, ak plánujete prijať a používať certifikáty ako povoľovacie údaje, mali by ste si pozrieť požiadavky na identifikáciu pre CA a určiť, či sa ich požiadavky hodia na vaše bezpečnostné potreby.

Rozoznaný názov (DN) je výraz, ktorý popisuje identifikačné informácie vlastníka certifikátu a je časťou samotného certifikátu. V závislosti na identifikačnej politiky CA, ktorá vydáva certifikát, DN môže obsahovať rôzna informácie. Správcu digitálnych certifikátov (DCM)

môžete použiť na prevádzkovanie súkromnej Certifikačnej autority a vydávanie súkromných certifikátov. DCM tiež môžete použiť na vygenerovanie informácií o DN a kľúčového páru pre certifikáty, ktoré vydá verejná internetová CA pre vašu organizáciu. Informácie o DN, ktoré môžete poskytnúť pre každý typ certifikátu môžu obsahovať:
- Normálne meno vlastníka certifikátu
- Organizácia
- Organizačná jednotka
- Mesto
- Štát
- Krajina

Keď používate DCM na vydávanie vlastných certifikátov, pre certifikát môžete poskytnúť dodatočné informácie o DN, ako:
- IP adresa verzie 4
- Plne kvalifikovaný názov domény
- E-mailová adresa

Tieto ďalšie informácie sú užitočné, ak plánujete použiť certifikát na konfiguráciu pripojenia VPN (virtual private network).

Elektronické podpisy

Elektronický podpis na elektronickom dokumente alebo inom objekte sa vytvorí použitím formy kryptografie a je ekvivalentný s osobným podpisom na písomných dokumentoch. Elektronický podpis poskytuje dôkaz o pôvode objektu a prostriedok, podľa ktorého sa dá overiť integrita objektu. Vlastník digitálneho certifikátu ″podpíše″ objekt použitím súkromného kľúča certifikátu. Prijímateľ objektu použije príslušný verejný kľúč certifikátu na dešifrovanie podpisu, ktorý kontroluje integritu podpísaného objektu a kontroluje odosielateľa ako zdroj.

Certifikačná autorita (CA) podpisuje certifikáty, ktoré vydáva. Tento podpis pozostáva z údajového reťazca, ktorý je zašifrovaný súkromným kľúčom Certifikačnej autority. Každý užívateľ môže potom overiť podpis na certifikáte pomocou verejného kľúča Certifikačnej autority na dešifrovanie podpisu.

Elektronický podpis je podpis, ktorý vy alebo aplikácia vytvára na objekte, použitím súkromného kľúča digitálneho certifikátu. Elektronický podpis na objekte poskytuje jedinečnú elektronickú väzbu identity podpisovateľa (vlastníka podpisovacieho kľúča) k pôvodu objektu. Keď pristúpite na objekt, ktorý obsahuje elektronický podpis. môžete overiť podpis na objekte na potvrdenie zdroja objektu ako platného (napríklad že aplikácia, ktorú sťahujete, skutočne pochádza z autorizovaného zdroja, ako je IBM). Tento overovací proces vám tiež umožňuje zistiť, či sa na objekte udiali nejaké neautorizované zmeny, odkedy bol podpísaný.

Príklad toho, ako pracuje elektronický podpis

Vývojár softvéru vytvoril aplikáciu iSeries, ktorú chce distribuovať cez internet ako pohodlný a cenovo efektívny spôsob pre svojich zákazníkov. Avšak vie, že zákazníci sú oprávnene obávajú sťahovania programov cez internet kvôli narastajúcemu problému s objektmi, ktoré sa tvária ako legitímne programy, ale v skutočnosti obsahujú škodlivé programy, ako sú vírusy.

Z tohto dôvodu sa rozhodne elektronicky podpísať aplikáciu, takže jeho zákazníci budú môcť overiť, že jeho spoločnosť je legitímnym zdrojom aplikácie. Na podpísanie aplikácie používa súkromný kľúč z digitálneho certifikátu, ktorý získal zo známej verejnej certifikačnej autority. Potom ho sprístupní na stiahnutie pre svojich zákazníkov. Ako časť balíka na stiahnutie zahŕňa kópiu digitálneho certifikátu, ktorý použil na podpísanie objektu. Keď zákazník stiahne balík aplikácie, môže použiť verejný kľúč certifikátu na overenie podpisu na aplikácii. Tento proces

zákazníkovi umožňuje identifikovať a overiť aplikáciu, ako aj uistiť sa, že obsah objektu aplikácie nebol od svojho podpísania zmenený.

Dvojica verejný-súkromný kľúč

Každý digitálny certifikát má so sebou spojený pár kryptografických kľúčov. Tento pár kľúčov sa skladá zo súkromného kľúča a verejného kľúča. (Výnimkou tohto pravidlá sú certifikáty na kontrolu podpisu, ktoré majú priradený len verejný kľúč.)

Verejný kľúč je časťou vlastníkovho digitálneho certifikátu a je dostupný na použitie pre každého. Súkromný kľúč je však chránený vlastníkom kľúča a je dostupný iba pre neho. Tento obmedzený prístup zaisťuje, že komunikácie používajúce tento kľúč sú bezpečné.

Vlastník certifikátu môže tieto kľúče použiť na využitie kryptografických bezpečnostných vlastností, ktoré kľúče poskytujú. Napríklad vlastník certifikátu môže použiť súkromný kľúč certifikátu na ″podpísanie″ a zašifrovanie údajov, odosielaných medzi užívateľmi a servermi, ako sú správy, dokumenty a kódové objekty. Príjemca podpísaného objektu potom môže použiť verejný kľúč, priložený v certifikáte podpisovateľa, na dešifrovanie podpisu. Takéto elektronické podpisy zabezpečujú spoľahlivosť pôvodu objektu a poskytujú prostriedok na kontrolu integrity objektu.

Certifikačná autorita (CA)

Certifikačná autorita (CA) je dôveryhodná centrálna administratívna entita, ktorá môže vydávať digitálne certifikáty užívateľom a serverom. Dôvera v CA je základom dôvery v certifikát ako platných povoľovacích údajov. CA používa svoj súkromný kľúč na vytváranie digitálneho podpisu na certifikáte, ktorý vydá, čím je možná validizácia pôvodu certifikátu. Ostatní môžu použiť verejný kľúč certifikátu Certifikačnej autority na kontrolu autenticity certifikátov, ktoré vydá a podpíše daná CA.

CA môže byť verejná komerčná entita, ako je VeriSign, alebo to môže byť súkromná entita, ktorú prevádzkuje organizácia pre interné potreby. Niekoľko podnikov poskytuje komerčné služby Certifikačnej autority pre užívateľov Internetu. Správca digitálnych certifikátov (DCM) vám umožňuje manažovať certifikáty od verejných aj súkromných CA.

DCM tiež môžete použiť na prevádzkovanie vlastnej CA na vydávanie súkromných certifikátov systémom a užívateľom. Keď CA vydá užívateľský certifikát, DCM automaticky združí certifikát s užívateľovým systémovým užívateľským profilom iSeries. Tým sa zabezpečí, že prístup a autorizačné privilégiá pre certifikát sú rovnaké ako tie, ktoré sú pre užívateľský profil vlastníka.

Stav dôveryhodného zdroja

Výraz dôveryhodný zdroj sa týka špeciálneho označenia, ktoré je dané certifikátu Certifikačnej autority. Toto označenie dôveryhodný zdroj umožňuje prehliadaču alebo inej aplikácii autentifikovať a akceptovať certifikáty, ktoré vydáva daná Certifikačná autorita (CA).

Keď stiahnete do svojho prehliadača certifikát Certifikačnej autority, prehliadač vám umožní označiť ho ako dôveryhodný zdroj. Ostatné aplikácie, ktoré používajú použitie certifikátov sa musia tiež nakonfigurovať tak, aby verili danej CA, aby mohli autentifikovať a dôverovať certifikátom, ktoré vydá konkrétna CA.

Na povolenie alebo zakázanie dôverovania certifikátu Certifikačnej autority (CA) v pamäti certifikátov môžete použiť DCM. Keď povolíte certifikát CA, môžete špecifikovať, že aplikácie ho môžu používať na autentifikáciu a akceptovanie certifikátov, ktoré vydá daná CA.

Keď zakážete certifikát CA, nemôžete špecifikovať, že aplikácie ho môžu používať na autentifikáciu a akceptovanie certifikátov, ktoré vydá daná CA.

Údaje politiky Certifikačnej autority

Keď vytvoríte Certifikačnú autoritu (CA) pomocou Správcu digitálnych certifikátov, môžete špecifikovať údaje politiky pre danú CA. Údaje politiky pre CA popisujú privilégiá podpisovania, ktoré má táto CA. Údaje o politike určujú:
- Či môže CA vydávať a podpisovať užívateľské certifikáty.
- Ako dlho sú platné certifikáty, ktoré vydá daná CA.

Umiestnenia Certificate Revocation List (CRL)

Certificate Revocation List (CRL) je súbor, ktorý obsahuje všetky neplatné a zrušené certifikáty pre konkrétnu Certifikačnú autoritu (CA). CA periodicky aktualizujú svoje CRL a sprístupňujú ich ostatným na zverejnenie v Lightweight Directory Access Protocol (LDAP) adresároch. Niektoré CA, ako je SSH vo Fínsku, zverejňujú ich CRL sami v LDAP adresároch, na ktoré môžete priamo pristúpiť. Ak CA zverejní svoj vlastný CRL, certifikát túto skutočnosť oznámi zahrnutím rozšírenia distribučného bodu CRL vo forme Uniform Resource Identifier (URI).

Správca digitálnych certifikátov (DCM) vám umožňuje definovať a manažovať informácie o umiestnení CRL na zabezpečenie prísnejšej autentifikácie pre certifikáty, ktoré používate alebo akceptujete od iných. Definícia umiestnenia CRL popisuje umiestnenie, prístupové informácie a Lightweight Directory Access Protocol (LDAP) server, ktorý obsahuje CRL.

Aplikácie, ktoré vykonávajú autentifikáciu certifikátov pristupujú na umiestnenie CRL pre konkrétnu CA, ak je definované, aby sa presvedčili, že táto CA nezrušila niektorý konkrétny certifikát. DCM vám umožňuje definovať a manažovať informácie o umiestnení CRL, ktoré potrebujú aplikácie na vykonávanie spracovania CRL počas autentifikácie certifikátu. Príkladmi aplikácií a procesov, ktoré môžu vykonávať spracovanie CRL na autentifikáciu certifikátov sú: VPN (virtuálna súkromná sieť) Internet Key Exchange (IKE) server, aplikácie s povoleným Secure Sockets Layer (SSL) a proces, ktorý podpisuje objekty. Keď definujete umiestnenie CRL a priradíte ho k certifikátu CA, DCM vykoná spracovanie CRL ako súčasť validačného procesu pre certifikáty, ktoré vydáva špecifikovaná CA .

Pamäte certifikátov

Pamäť certifikátov je špeciálny súbor databázy kľúčov, ktorý Správca digitálnych certifikátov (DCM) používa na uloženie digitálnych certifikátov. Pamäť certifikátov taktiež obsahuje súkromný kľúč certifikátu, ak namiesto nej na jeho uloženie nezvolíte Cryptographic Coprocessor 4758. DCM vám umožňuje vytvárať a manažovať niekoľko typov pamäte certifikátov. DCM riadi prístup do pamätí certifikátov cez heslá v kombinácii s riadením prístupu adresára IFS a súborov IFS, ktoré predstavujú pamäť certifikátov.

Pamäte certifikátov sú klasifikované podľa typov certifikátov, ktoré obsahujú. Úlohy manažmentu, ktoré môžete vykonávať na každej pamäti certifikátov sa menia podľa typu certifikátu, ktorý je v pamäti certifikátov. DCM poskytuje nasledovné preddefinované pamäte certifikátov, ktoré môžete vytvoriť a riadiť:

Lokálna certifikačná autorita (CA)
DCM používa túto pamäť certifikátov na uloženie certifikátu miestnej CA a jeho súkromného kľúča, ak vytvoríte miestnu CA. Certifikát v tejto pamäti certifikátov môžete používať na podpisovanie certifikátov, ktoré vydáva miestna CA. Keď miestna CA vydá certifikát, DCM vloží kópiu certifikátu CA (bez súkromného kľúča) do správnej pamäte certifikátov (napríklad, *SYSTEM) za účelom autentifikácie. Aplikácie používajú certifikáty CA na kontrolu pôvodu certifikátov, ktoré musia validovať ako časť dohody SSL na poskytnutie autorizácie na prostriedky.

***SYSTEM**
DCM poskytuje túto pamäť certifikátov pre manažovanie certifikátov servera a klienta, ktoré používajú aplikácie ako súčasť komunikačných relácií Secure Sockets Layer (SSL). Aplikácie IBM iSeries (a mnohé ďalšie aplikácie vývojárov softvéru) sú naprogramované iba na použitie certifikátov v pamäti certifikátov *SYSTEM. Ak používate DCM na vytvorenie lokálnej CA, DCM vytvorí túto pamäť certifikátov ako časť procesu. Ak sa rozhodnete získať certifikáty z verejnej CA, ako je VeriSign, pre použitie vašimi aplikáciami servera alebo klienta, musíte túto pamäť certifikátov vytvoriť.

***OBJECTSIGNING**
DCM poskytuje túto pamäť certifikátov pre manažovanie certifikátov, ktoré používate na digitálne podpisovanie objektov. Taktiež vám úlohy v tejto pamäti certifikátov umožnia vytvoriť elektronické podpisy na objektoch, ako aj prezerať a overovať podpisy na objektoch. Ak používate DCM na vytvorenie lokálnej CA, DCM vytvorí túto pamäť certifikátov ako časť procesu. Ak sa rozhodnete získať certifikáty z verejnej CA, ako je VeriSign, pre podpisovanie objektov, musíte túto pamäť certifikátov vytvoriť.

***SIGNATUREVERIFICATION**
DCM poskytuje túto pamäť certifikátov na manažovanie certifikátov, ktoré používate na overovanie autenticity elektronických podpisov na objektoch. Na overenie elektronického podpisu musí táto pamäť certifikátov obsahovať kópiu certifikátu, ktorým bol objekt podpísaný. Pamäť certifikátov musí tiež obsahovať kópiu certifikátu CA pre CA, ktorá vydala certifikát na podpísanie objektu. Tieto certifikáty získate exportovaním certifikátov na podpísanie objektov na aktuálny systém do pamäti, alebo importovaním certifikátov, ktoré prijmete od podpisovateľa objektu.

Iná systémová pamäť certifikátov
Táto pamäť certifikátov poskytuje alternatívne umiestnenie pamäte pre certifikáty servera alebo klienta, ktoré používate pre SSL relácie. Iné systémové pamäte certifikátov sú užívateľom definované sekundárne pamäte certifikátov pre SSL certifikáty. Voľba Iná systémová pamäť certifikátov vám umožňuje manažovať certifikáty pre aplikácie, ktoré napíšete vy alebo iní, ktoré používajú SSL_Init API na programovateľný prístup a použitie certifikátu na vytvorenie SSL relácie. Toto API umožňuje aplikácii použiť štandardný certifikát pre pamäť certifikátov namiesto certifikátu, ktorý konkrétne identifikujete. Najčastejšie budete túto pamäť certifikátov používať pri migrácii certifikátov z predchádzajúceho vydania DCM, alebo pri vytváraní špeciálnej podmnožiny certifikátov pre použitie so SSL.

Poznámka: Ak máte vo vašom serveri iSeries nainštalovaný 4758 PCI Cryptographic Coprocessor, môžete si vybrať iné voľby uloženia súkromného kľúča pre vaše certifikáty (s výnimkou certifikátov na podpisovanie objektov). Môžete rozhodnúť, že súkromný kľúč uložíte na samotnom koprocesore, alebo koprocesor môžete používať na zašifrovanie súkromného kľúča a môžete ho uložiť v špeciálnom súbore kľúčov, nie v pamäti certifikátov.

DCM riadi prístup do pamätí certifikátov cez heslá. DCM tiež obsluhuje riadenie prístupu adresára integrovaného súborového systému a súborov, ktoré tvoria pamäť certifikátov. Pamäte certifikátov Miestna Certifikačná autorita(CA), *SYSTEM, *OBJECTSIGNING a *SIGNATUREVERIFICATION musia byť umiestnené na špecifických cestách v integrovanom súborom systéme, Iné systémové pamäte certifikátov môžu byť umiestnené kdekoľvek v integrovanom súborovom systéme.

Kryptografia

Kryptografia je vedou na udržanie údajov v bezpečnosti. Kryptografia vám umožňuje ukladať informácie alebo komunikovať s inými stranami, pričom nezúčastneným stranám zakazuje čítať uložené informácie alebo sledovať komunikáciu. Šifrovanie transformuje zrozumiteľný text do nezrozumiteľných údajov (zašifrovaný text). Dešifrovanie obnovuje zrozumiteľný text z nezrozumiteľných údajov. Oba procesy zahŕňajú matematický vzorec alebo algoritmus a tajnú postupnosť údajov (kľúč).

Existujú dva typy kryptografie:

- V kryptografii so **zdieľaným alebo súkromným kľúčom (symetrickým)** je jeden kľúč zdieľaným tajomstvom medzi dvoma komunikujúcimi stranami. Šifrovanie a dešifrovanie používa rovnaký kľúč.
- V kryptografii s **verejným kľúčom (nesymetrickým)** sa na šifrovanie a dešifrovanie používajú odlišné kľúče. Účastníci majú dvojicu kľúčov, pozostávajúcu z verejného a súkromného kľúča. Verejný kľúč je distribuovaný voľne, zvyčajne v rámci digitálneho certifikátu, kým súkromný kľúč je bezpečne uložený u vlastníka. Oba kľúče sú matematicky spojené, ale je virtuálne nemožné oddeliť verejný kľúč od súkromného. Objekt, ako je správa, ktorý je zašifrovaný verejným kľúčom môže dešifrovať len niekto, kto má príslušný súkromný kľúč. Alternatívne, server alebo užívateľ môže použiť súkromný kľúč na ″podpísanie″ objektu a prijímateľ môže použiť príslušný súkromný kľúč na dešifrovanie súkromného podpisu a skontrolovať tak pôvod a integritu objektu.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL), pôvodne vytvorený spoločnosťou Netscape, je priemyselný štandard pre šifrovanie relácií medzi klientmi a servermi. SSL používa na šifrovanie relácie medzi serverom a klientom asymetrickú kryptografiu (s verejnými kľúčmi). Klientska a serverovská aplikácia dojednajú tento kľúč relácie počas vzájomnej výmeny digitálnych certifikátov. Tento kľúč automaticky exspiruje po 24 hodinách a proces SSL vytvorí odlišný kľúč pre každé spojenie server a každého klienta. Aj keď by neoprávnení užívatelia odchytili a dešifrovali kľúč relácie (čo je nepravdepodobné), nemôžu ho použiť na odpočúvanie neskorších relácií.

Kapitola 6. Plánovanie pre DCM

Na použitie Správcu digitálnych certifikátov (DCM) na efektívne spravovanie digitálnych certifikátov vašej spoločnosti musíte mať celkový plán toho, ako budete používať digitálne certifikáty ako časť vašej politiky bezpečnosti.

Ak sa chcete dozvedieť viac o tom, ako plánovať použitie DCM a lepšie pochopiť, ako sa môžu digitálne certifikáty hodiť do vašej politiky bezpečnosti, prezrite si tieto témy:

Požiadavky pre použitie DCM
Dozviete sa tu, aký softvér musíte nainštalovať a aké informácie potrebujete na nastavenie vášho systému na používanie DCM.

Typy digitálnych certifikátov
V týchto informáciách sa dozviete o rôznych typoch certifikátov, na ktorých správu môžete použiť DCM.

Verejné certifikáty verzus súkromné certifikáty
V týchto informáciách sa dozviete o tom, ako určiť typ certifikátov, ktorý sa najlepšie hodí na vaše firemné potreby, keď sa raz rozhodnete, že chcete používať certifikáty kvôli ich výhodám dodatočnej bezpečnosti. Môžete používať certifikáty od verejnej CA alebo si na vydávanie certifikátov môžete vytvoriť a prevádzkovať vlastnú CA. Ako sa rozhodnete získavať certifikáty záleží na tom, ako ich chcete používať.

Digitálne certifikáty pre komunikácie SSL (Secure Sockets Layer)
Tieto informácie vám ukážu, ako používať certifikáty, aby vaše aplikácie mohli vytvárať bezpečné komunikačné relácie.

Digitálne certifikáty na autentifikáciu užívateľov
V týchto informáciách sa dozviete o tom, ako používať certifikáty na zriadenie prostriedkov účinnejšej autentifikácie užívateľov, ktorí pristupujú na zdroje servera iSeries.

Digitálne certifikáty na autentifikáciu pripojení VPN (virtual private network)
V týchto informáciách sa dozviete, ako použiť certifikáty pri konfigurácii VPN spojenia.

Digitálne certifikáty na podpisovanie objektov
Tieto informácie vám vysvetlia, ako používať certifikáty na zaistenie integrity objektu, alebo ako skontrolovať digitálny podpis na objekte za účelom kontroly jeho autenticity.

Digitálne certifikáty pre overovanie podpisov objektov
V týchto informáciách sa dozviete, ako používať certifikáty na overovanie elektronického podpisu na objekte na overenie jeho autenticity.

Požiadavky nastavenia DCM

Správca digitálnych certifikátov (DCM) je bezplatný doplnok iSeries, ktorý vám umožňuje centrálne spravovať digitálne certifikáty pre vaše aplikácie. Na úspešné používanie DCM zabezpečte, že urobíte nasledovné:

- Nainštalujte licencovaný program poskytovateľa šifrovaného prístupu (5722–AC3). Tento šifrovací produkt zisťuje maximálnu dĺžku kľúča, ktorá je povolená pre šifrovacie algoritmy, založené na reguláciách exportu a importu. Tento produkt musíte nainštalovať pred tým, ako budete môcť vytvárať certifikáty.
- Nainštalujte voľbu 34 OS/400. Toto je DCM, založený na prehliadači.
- Nainštalujte IBM HTTP Server for iSeries (5722–DG1) a spustite inštanciu servera *ADMIN.
- Presvedčte sa, že na vašom systéme je nakonfigurovaný TCP, aby váš systém mohol používať web prehliadač, ako aj inštancia *ADMIN HTTP Servera na prístup k DCM.

Poznámka: Kým nenainštalujete všetky požadované produkty, nebudete môcť vytvárať certifikáty. Ak nie je nainštalovaný niektorý vyžadovaný produkt, DCM zobrazí chybovú správu s oznamom, že máte nainštalovať chýbajúci komponent.

Typy digitálnych certifikátov

Existuje niekoľko klasifikácii digitálnych certifikátov. Tieto klasifikácie opisujú, ako je certifikát použitý. Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie nasledovných typov certifikátov:

Certifikáty certifikačnej autority (CA)
Certifikát Certifikačnej autority predstavuje povoľovacie údaje, ktoré validujú identitu Certifikačnej autority (CA), ktorá vlastní tento certifikát. Certifikát certifikačnej autority obsahuje identifikačné informácie a certifikačnej autorite, ako aj jej verejný kľúč. Ostatní môžu použiť verejný kľúč certifikátu Certifikačnej autority na kontrolu autenticity certifikátov, ktoré vydá a podpíše daná CA. Certifikát Certifikačnej autority môže byť podpísaný inou CA, ako je VeriSign, alebo môže byť podpísaný sám sebou, ak je nezávislou entitou. Nezávislou entitou je CA, ktorú vytvoríte v Správcovi digitálnych certifikátov. Ostatní môžu použiť verejný kľúč certifikátu Certifikačnej autority na kontrolu autenticity certifikátov, ktoré vydá a podpíše daná CA. Na použitie certifikátu pre SSL, podpisovanie objektov, alebo overovanie podpisov objektov, musíte mať kópiu certifikátu CA pre CA, ktorá vydala certifikát.

Certifikáty servera alebo klienta
Certifikát servera alebo klienta predstavuje digitálne povoľovacie údaje, ktoré identifikujú aplikáciu servera alebo klienta, ktorá používa certifikát pre bezpečnú komunikáciu. Certifikáty servera alebo klienta identifikujú informácie o organizácii, ktorá vlastní aplikáciu, ako je rozoznaný názov systému. Certifikát tiež obsahuje verejný kľúč systému. Server musí mať digitálny certifikát, aby mohol používať Secure Sockets Layer (SSL) pre bezpečnú komunikáciu. Aplikácie, ktoré podporujú digitálne certifikáty môžu preskúšať certifikát servera a skontrolovať identitu servera, keď klient pristupuje na tento server. Aplikácie, potom môžu použiť autentifikáciu certifikát ako základ pre inicializovanie šifrovanej relácie pomocou SSL medzi klientom a serverom. Tieto typy certifikátov môžete manažovať iba pre pamäť certifikátov *SYSTEM.

Certifikáty na podpisovanie objektov
Certifikát na podpisovanie objektov je certifikát, ktorý používate na elektronické ″podpísanie″ objektu. Podpísaním objektu poskytujete spôsob, podľa ktorého môžete overiť integritu objektu a pôvod alebo vlastníctvo objektu. Certifikát môžete použiť na podpísanie množstva objektov, vrátane väčšiny objektov v integrovanom súborovom systéme (IFS) a *CMD objektov. V kapitole Podpisovanie objektov a overovanie podpisov môžete nájsť kompletný zoznam podpisovateľných objektov. Keď na podpísanie objektu použijete verejný kľúč certifikátu, podpisujúceho objekty, prijímateľ objektu musí mať prístup na kópiu príslušného certifikátu, podpisujúceho objekty, aby mohol správne autentifikovať podpis objektu. Tieto typy certifikátov môžete manažovať iba pre pamäť certifikátov *OBJECTSIGNING.

Certifikáty na overovanie podpisov
Certifikát na kontrolu podpisu je kópia certifikátu, podpisujúceho objekty, bez súkromného kľúča certifikátu. Verejný kľúč certifikátu na overovanie podpisov môžete použiť na overenie elektronického podpisu, vytvoreného certifikátom na podpisovanie objektov. Overenie podpisu vám umožňuje zistiť pôvod objektu a či bol zmenený odvtedy, ako bol podpísaný. Tieto typy certifikátov môžete manažovať iba pre pamäť certifikátov *SIGNATUREVERIFICATION.

Užívateľské certifikáty
Užívateľský certifikát predstavuje digitálne povoľovacie údaje, ktoré validujú identitu klienta alebo užívateľa, ktorý vlastní certifikát. Mnoho aplikácií poskytuje v súčasnosti podporu, ktorá vám umožňuje používať certifikáty na autentifikovanie užívateľov na prostriedky, namiesto používania mien užívateľov a hesiel. Správca digitálnych certifikátov (DCM) automaticky združuje užívateľské certifikáty, ktoré vydáva vaša súkromná CA, s užívateľovým užívateľským profilom iSeries. DCM môžete taktiež používať na združovanie užívateľských certifikátov, ktoré vydávajú iné certifikačné autority, s užívateľovým užívateľským profilom iSeries.

Keď na manažovanie svojich certifikátov používate Správcu digitálnych certifikátov (DCM), DCM ich organizuje podľa týchto klasifikácií a ukladá ich a ich príslušné súkromné kľúče do pamäte certifikátov.

Poznámka: Ak máte vo vašom serveri iSeries nainštalovaný IBM 4758 PCI Cryptographic Coprocessor, môžete si vybrať iné voľby uloženia súkromného kľúča pre vaše certifikáty (s výnimkou certifikátov na podpisovanie objektov). Môžete vybrať, aby sa súkromný kľúč uložil na samotnom koprocesore. Alebo, koprocesor môžete používať na zašifrovanie súkromného kľúča a môžete ho uložiť v špeciálnom súbore kľúčov, nie v pamäti certifikátov. Užívateľské certifikáty a ich súkromné kľúče sú uložené na systéme užívateľa buď v prehliadači alebo v súbore, aby ich mohli použiť iné klientske softvérové balíky.

Verejné certifikáty verzus súkromné certifikáty

Keď sa rozhodnete používať certifikáty, mali by ste si vybrať typ implementácie certifikátu, ktorý najlepšie vyhovuje vašim bezpečnostným potrebám. Na získavanie certifikátov máte nasledovné voľby:

- Zakúpenie vašich certifikátov od verejnej internetovej Certifikačnej autority (CA).
- Prevádzkovanie vlastnej CA na vydávanie súkromných certifikátov pre vašich užívateľov a aplikácie.
- Použitie kombinácie certifikátov od verejných internetových CA a vašej vlastnej CA.

Pre ktorú z týchto volieb sa rozhodnete závisí na množstve faktorov, pričom jedným z najhlavnejších je prostredie, v ktorom sa budú tieto certifikáty používať. Nasleduje niekoľko informácií, ktoré vám pomôžu rozhodnúť, ktorá voľba je tou pravou pre vaše firemné a bezpečnostné potreby.

Použitie verejných certifikátov

Verejné internetové CA vydávajú certifikáty všetkým, ktorí zaplatia potrebný poplatok. Pred vydaním certifikátu vyžaduje internetová CA nejaký dôkaz identity. Táto úroveň dôkazu sa mení podľa identifikačnej politiky danej CA. Mali by ste vyhodnotiť, či prísnosť identifikačnej politiky danej CA vyhovuje vašim bezpečnostným potrebám ešte predtým, ako sa rozhodnete získať certifikáty od tejto CA alebo dôverovať ňou vydaným certifikátom. Ako boli vyvinuté štandardy Public Key Infrastructure for X.509 (PKIX) niektoré novšie verejné CA už poskytujú oveľa prísnejšie identifikačné štandardy pre vydávanie certifikátov. Proces získania certifikátov od takýchto PKIX CA je trochu zložitejší, ale certifikáty, ktoré vydá takáto CA poskytujú väčšiu istotu pre zabezpečenia prístupu na aplikácie konkrétnymi užívateľmi. Správca digitálnych certifikátov (DCM) vám umožňuje používať a manažovať certifikáty od PKIX CA, ktoré používajú tieto nové štandardy pre certifikáty.

Musíte tiež uvážiť cenu, spojenú s použitím verejnej CA na vydanie certifikátov. Ak potrebujete certifikáty pre konečný počet aplikácií servera alebo klienta a užívateľov, cena nemusí byť rozhodujúcim faktorom. Cena však môže byť rozhodujúca, ak máte veľký počet *súkromných* užívateľov, ktorí potrebujú verejné certifikáty na autentifikáciu klientov. V tomto prípade by ste mali zohľadniť aj administratívne a programovacie úsilie, potrebné na konfiguráciu aplikácií servera na akceptovanie len konkrétnej podmnožiny certifikátov, ktoré vydáva daná verejná CA.

Použitie certifikátov od verejnej CA vám môže ušetriť čas a prostriedky, pretože veľa aplikácií servera, klienta a užívateľských aplikácií je nakonfigurovaných na rozpoznanie väčšiny dobre známych verejných CA. Iné spoločnosti a užívatelia môžu rozoznať a viac dôverovať certifikátom, ktoré vydá dobre známa verejná CA, ako tým, ktoré vydá vaša súkromná CA.

Použitie súkromných certifikátov

Ak vytvoríte vašu vlastnú lokálnu CA, môžete vydávať certifikáty systémom a užívateľom v rámci limitovanejšieho rozsahu, ako napr. v rámci vašej spoločnosti alebo organizácie. Vytváranie a udržiavanie vašej vlastnej CA vám umožní vydávať certifikáty iba tým užívateľom, ktorí sú dôveryhodnými členmi vašej skupiny. Poskytuje to lepšiu bezpečnosť, pretože môžete prísnejšie riadiť, kto má certifikáty a kto má prístup k vašim prostriedkom. Potenciálnou nevýhodou údržby vašej vlastnej lokálnej CA je množstvo času a prostriedkov, ktoré musíte investovať. Správca digitálnych certifikátov (DCM) však tento proces uľahčuje.

Keď používate lokálnu CA na vydávanie certifikátov užívateľom pre klientsku autentifikáciu, mali by ste sa rozhodnúť, či chcete, aby boli vaše certifikáty užívateľov združené s užívateľskými profilmi iSeries. Môžete zariadiť, aby užívatelia získali svoje certifikáty z lokálnej CA cez DCM, ak chcete, aby boli ich certifikáty združené s užívateľským profilom iSeries. Alebo, počínajúc V5R2, môžete používať API na programové vydávanie certifikátov užívateľom iným ako i-Series, takže títo užívatelia nemusia mať užívateľský profil iSeries na to, aby mohli používať súkromné certifikáty pre klientsku autentifikáciu.

Poznámka: Bez ohľadu na to, ktorú CA používate na vydávanie certifikátov, správca systému riadi, ktorým CA by mali dôverovať aplikácie na tomto systéme. Ak sa vo vašom prehliadači nájde kópia certifikátu pre dobre známu CA, váš prehliadač sa môže nastaviť tak, aby dôveroval certifikátom servera, ktoré boli vydané touto CA. Ak však tento certifikát CA nie je vo vašej pamäti certifikátov *SYSTEM, váš server nemôže dôverovať užívateľským certifikátom alebo certifikátom klienta, ktoré boli vydané touto CA. Ak chcete dôverovať užívateľským certifikátom, ktorá vydala táto CA, musíte si zaobstarať kópiu certifikátu CA z uvedenej CA. Musí byť v správnom formáte súborov a tento certifikát musíte pridať do svojej pamäte certifikátov DCM.

Môže byť pre vás užitočné prezrieť si niektoré všeobecné scenáre použitia certifikátov, ktoré vám pomôžu rozhodnúť sa, či sa vašim obchodným a bezpečnostným zámerom viac hodí použitie verejných, alebo súkromných certifikátov.

Súvisiace úlohy

Keď sa rozhodnete, ako chcete používať certifikáty a ktorý typ, pozrite si tieto procedúry, v ktorých sa dozviete viac o tom, ako použiť Správcu digitálnych certifikátov na zrealizovanie vašich plánov:

- Vytvorenie a prevádzkovanie súkromnej CA popisuje úlohy, ktoré musíte vykonať, ak sa rozhodnete pre prevádzkovanie súkromnej CA, ktorá bude vydávať súkromné certifikáty.
- Manažovanie certifikátov od verejných internetových CA popisuje úlohy, ktoré musíte vykonať, ak chcete používať certifikáty od dobre známej verejnej CA, vrátane PKIX CA.
- Použitie lokálnej CA na iných serveroch iSeries opisuje úlohy, ktoré musíte vykonať, ak chcete používať certifikáty zo súkromnej CA na viac ako jednom systéme.

Digitálne certifikáty pre bezpečné SSL komunikácie

Digitálne certifikáty môžete použiť na konfiguráciu aplikácií na používanie SSL (Secure Sockets Layer) pre relácie bezpečných komunikácií. Ak chcete vytvoriť SSL reláciu, váš server vždy predloží svoj certifikát na validizáciu klientovi, ktorý požaduje spojenie. Použitie SSL spojenia:

- Zaisťuje klientovi alebo koncovému užívateľovi autenticitu vášho servera.
- Poskytuje šifrovanú komunikačnú reláciu, ktorá zaisťuje súkromnosť informácií údajov pri prechode cez spojenie.

Aplikácie servera a klienta spolupracujú pri zaisťovaní súkromnosti údajov nasledovne:

1. Aplikácia servera predloží certifikát aplikácii klienta (užívateľa), ako dôkaz identity servera.
2. Aplikácia klienta skontroluje identitu servera pomocou kópie certifikátu vydávajúcej Certifikačnej autority. (Aplikácia klienta musí mať prístup na miestne uloženú kópiu potrebného certifikátu CA.)
3. Aplikácia servera aj klienta sa dohodnú na symetrickom kľúči na šifrovanie a používajú ho na šifrovanie komunikačnej relácie.
4. Voliteľne, server teraz môže požiadať od klienta dôkaz identity, až potom mu umožní prístup na požadované prostriedky. Na používanie certifikátov ako dôkaz identity musia komunikujúce aplikácie podporovať používanie certifikátov na autentifikáciu užívateľov.

SSL používa počas dohodovania SSL algoritmus asymetrického kľúča (verejný kľúč), ktorým dohodne symetrický kľúč, ktorý sa následne používa na šifrovanie a dešifrovanie údajov aplikácie pre túto konkrétnu SSL reláciu. To znamená, že váš server a klient používajú rôzne kľúče relácie, ktorým automaticky skončí platnosť po nastavenom časovom úseku pre každé spojenie. V nepravdepodobnom prípade odchytenia a dešifrovania konkrétneho kľúča relácie niekým iným sa tento kľúč relácie aj tak nedá použiť na určenie budúcich kľúčov.

Digitálne certifikáty na autentifikáciu užívateľov

Používatelia získavajú tradične prístup na prostriedky z aplikácie alebo systému podľa ich užívateľského mena a hesla. Systémovú bezpečnosť môžete ďalej rozšíriť pomocou digitálnych certifikátov (namiesto užívateľských mien a hesiel) na autentifikáciu a autorizáciu relácií medzi mnohými aplikáciami servera a užívateľmi. Taktiež môžete použiť Správcu digitálnych certifikátov (DCM) na združovanie užívateľových certifikátov s užívateľským profilom iSeries tohto užívateľa. Tento certifikát má potom rovnaké oprávnenia a povolenia ako príslušný profil. Od verzie V5R2 môžete používať API na programové používanie vašej súkromnej lokálnej certifikačnej autority na vydávanie certifikátov užívateľom iným ako i-Series. Tieto API vám poskytnú schopnosť vydávať súkromné certifikáty užívateľom, keď nechcete, aby mali títo užívatelia užívateľský profil iSeries.

Digitálny certifikát slúži ako elektronické povolenie a kontroluje, či osoba, ktorá ho predkladá, je naozaj tá osoba, za ktorú sa vydáva. V tomto ohľade je certifikát podobný normálnemu pasu. Oba dokazujú identitu osoby, obsahujú jedinečné číslo na účely identifikácie a majú rozoznateľnú vydávajúcu autoritu, ktorá prehlasuje dané povoľovacie údaje za autentické. V prípade certifikátu, ako dôveryhodná tretia strana, ktorá vydáva certifikát a prehlasuje ho za autentické povoľovacie údaje funguje Certifikačná autorita (CA).

Kvôli autentifikačným účelom používajú certifikáty verejný kľúč a s ním súvisiaci súkromný kľúč. Vydávajúca CA tieto dva kľúče zviaže dokopy spolu s ostatnými informáciami o vlastníkovi certifikátu do samotného certifikátu za účelom identifikácie.

Zvyšujúci sa počet súčasných aplikácií poskytuje podporu pre použitie certifikátov na autentifikáciu klientov počas SSL relácie. Aktuálne poskytujú podporu certifikátov na autentifikáciu klientov tieto aplikácie iSeries:
- Telnet server
- IBM HTTP Server (originál, aj powered by Apache)
- Directory Services (LDAP) server
- Management Central
- Client Access Express (vrátane iSeries Navigator)
- FTP server

Po čase môžu podporu certifikátov na autentifikáciu užívateľov poskytovať aj ďalšie aplikácie; prezrite si dokumentáciu na zistenie, či určité aplikácie poskytujú túto podporu.

Certifikáty môžu poskytovať silnejší spôsob autentifikovania užívateľov z niekoľkých dôvodov:

- Je istá pravdepodobnosť, že osoba zabudne svoje heslo. Používatelia sa preto musia učiť svoje heslá alebo si užívateľské mená a heslá niekam zapíšu, aby ich nezabudli. Výsledkom toho je, že neautorizovaní užívatelia môžu pomerne ľahko získať užívateľské mená a heslá od autorizovaných užívateľov. Pretože certifikáty sú uložené v súbore alebo na inom elektronickom mieste, prístup a prekladanie certifikátu na autentifikáciu riadia aplikácie klienta (namiesto samotných užívateľov). Toto zaisťuje, že je oveľa menej pravdepodobné, aby užívatelia zdieľali certifikáty s neautorizovanými užívateľmi, ak títo neautorizovaní užívatelia nemajú prístup na systém užívateľa. Certifikát sa tiež dá nainštalovať na smart card, čo predstavuje ďalší spôsob ochrany pred ich neautorizovaným použitím.
- Certifikát obsahuje súkromný kľúč, ktorý sa nikdy neposiela s certifikátom na identifikáciu. Namiesto toho systém používa tento kľúč počas procesu šifrovania a dešifrovania. Ostatní môžu používať príslušný verejný kľúč certifikátu, ktorým overia identitu odosielateľa objektov, ktoré sú podpísané súkromným kľúčom.
- Veľa systémov vyžaduje heslá, ktoré sú 8 znakové alebo kratšie, čo robí tieto heslá vhodnými na útoky formou hádania. Kryptografické kľúče certifikátu sú dlhé stovky znakov. Táto dĺžka spolu s ich náhodnou povahou má za následok to, že je oveľa ťažšie uhádnuť kryptografické kľúče než heslá.
- Kľúče digitálnych certifikátov poskytujú niekoľko možných použití, ktoré neposkytujú heslá, ako je integrita a súkromnosť údajov. Certifikáty a s nimi spojené kľúče môžete použiť na:
  - Zaistenie integrity údajov pomocou detekovania zmien v údajoch.
  - Dokázanie, že sa v skutočnosti vykonala nejaká konkrétna akcia. Toto sa nazýva nezamietnutie.
  - Zaistenie súkromnosti prenosov údajov pomocou Secure Sockets Layer (SSL) na šifrovanie komunikačných relácií.

Ak sa chcete dozvedieť viac o konfigurovaní aplikácií servera iSeries pre autentifikáciu klientov počas relácie SSL, pozrite si Zabezpečenie aplikácií s SSL.

Digitálne certifikáty pre VPN spojenia

Digitálne certifikáty môžete použiť ako prostriedok vytvorenia pripojenia iSeries VPN (virtual private network). Oba koncové body dynamického VPN spojenia musia byť schopné vzájomne sa autentifikovať pred aktivovaním spojenia. Autentifikácia koncového bodu sa vykonáva Internet Key Exchange (IKE) serverom na každom konci. Po úspešnej autentifikácii IKE servery dohodnú metódy šifrovania a algoritmy, ktoré použijú na zabezpečenie VPN spojenia.

V skorších verziách ako V5R1, IKE servery sa mohli vzájomne autentifikovať len pomocou predzdieľaného kľúča. Použitie predzdieľaného kľúča je menej bezpečné, pretože tento kľúč musíte ručne oznámiť správcovi opačného koncového bodu vašej VPN. Preto tu existuje možnosť, že niekto tento kľúč počas jeho oznamovania odhalí.

Tomuto riziku môžete zabrániť použitím digitálnych certifikátov na autentifikáciu koncových bodov namiesto použitie predzdieľaného kľúča. IKE server môže autentifikovať certifikát druhého servera a vytvoriť spojenie na dohodnutie metód a algoritmov šifrovania, ktoré použijú tieto servery na zabezpečenie spojenia.

Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie certifikátov, ktoré používa váš IKE server na vytvorenie dynamického VPN spojenia. Musíte sa najprv rozhodnúť, či chcete pre svoj IKE server používať verejné certifikáty alebo vydávať súkromné certifikáty.

Niektoré implementácie vyžadujú, aby certifikát okrem štandardnej informácii o rozoznanom názve obsahoval aj alternatívne informácie o predmete, ako je názov domény alebo e-mailová adresa. Keď používate na vydávanie certifikátov súkromnú CA z DCM, môžete pre certifikát špecifikovať alternatívne informácie o predmete. Zadanie týchto informácií zabezpečí, že vaše pripojenie iSeries VPN bude kompatibilné s inými implementáciami VPN, ktoré ich môžu vyžadovať pre autentifikáciu.

Ak sa chcete dozvedieť viac o manažovaní certifikátov pre vaše VPN spojenia, pozrite si tieto zdroje:

- Ak ste ešte nikdy nepoužívali DCM na manažovanie certifikátov, pomôžu vám tieto témy:
  - Vytvorenie a prevádzkovanie lokálnej, súkromnej CA opisuje, ako použiť DCM na vydanie súkromných certifikátov pre vaše aplikácie.
  - Manažovanie certifikátov od verejnej internetovej CA popisuje, ako použiť DCM na prácu s certifikátmi od verejnej CA.
- Ak súčasne používate DCM aj na manažovanie certifikátov pre iné aplikácie, pozrite si tieto zdroje, aby ste sa dozvedeli ako špecifikovať, aby aplikácia používala existujúci certifikát a ktoré certifikáty môže aplikácia akceptovať a autentifikovať:
  - Manažovanie priradenia certifikátov pre aplikáciu popisuje, ako použiť DCM na priradenie existujúceho certifikátu k aplikácii, ako je váš IKE server.
  - Definovanie zoznamu dôveryhodných CA pre aplikáciu popisuje, ako špecifikovať, ktorým CA môže aplikácia dôverovať, keď prijíma certifikáty na autentifikáciu klientov (alebo VPN).

Digitálne certifikáty na podpisovanie objektov

Od verzie V5R1 poskytuje OS/400 podporu pre používanie certifikátov na elektronické podpisovanie objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod. Podpora podpisovania objektov rozširuje tradičné systémové nástroje iSeries na riadenie, kto môže meniť objekty. Pri tradičnom riadení sa objekt nedal ochrániť pred neautorizovaným zásahom počas prenosu objektu cez Internet alebo inú nedôveryhodnú sieť, alebo keď je objekt uložený na inom ako iSeries systéme. Taktiež, tradičné riadenia nemôžu vždy zistiť, či na objekte nastali neautorizované zmeny alebo zásahy. Použitie elektronických podpisov na objektoch poskytuje spoľahlivý prostriedok na zistenie zmien na podpísaných objektoch.

Umiestnenie digitálneho podpis na objekt obsahuje použitie súkromného kľúča certifikátu na pridanie zašifrovanej matematického súčtu údajov v objekte. Podpis chráni údaje pred neautorizovanými zmenami. Samotný podpis objekt a jeho obsah nezašifruje, ani ho nespraví súkromným; spomenutý súčet je však zašifrovaný a zabraňuje neautorizovaným zmenám v objekte. Ak sa chce niekto presvedčiť, že objekt nebol pri prenose zmenený a pochádza o akceptovaného legitímneho zdroja, môže použiť verejný kľúč podpisujúceho certifikátu, ktorým overí pôvodný digitálny podpis. Ak sa podpis nezhoduje, údaje mohli byť zmenené. V takomto prípade môže príjemca zabrániť použitiu objektu a môže kontaktovať podpisovateľa, aby získal inú kópiu podpísaného objektu.

Ak sa rozhodnete, že použitie digitálnych podpisov vyhovuje vašim bezpečnostným potrebám, mali by ste vyhodnotiť, či by ste mali používať verejné certifikáty alebo vydávať súkromné certifikáty. Ak máte v úmysle distribuovať objekty užívateľom vo všeobecnej verejnosti, mali by ste zvážiť použitie certifikátov od známej verejnej certifikačnej autority (CA) na podpisovanie objektov. Použitie verejných certifikátov zaisťuje, že ostatní môžu ľahko a lacno overiť podpisy, ktoré dáte na objekty, ktoré im distribuujete. Ak však máte v úmysle distribuovať objekty výhradne v rámci vašej organizácie, môžete uprednostniť použitie Správcu digitálnych certifikátov (DCM) na prevádzkovanie vašej vlastnej lokálnej CA na

vydávanie certifikátov pre podpisovanie objektov. Použitie súkromných certifikátov z lokálnej CA na podpisovanie objektov je menej nákladné, ako zakúpenie certifikátov zo známej verejnej CA.

Podpis na objekte reprezentuje systém, ktorý podpísal objekt, nie konkrétneho užívateľa tohto systému (aj keď užívateľ musí mať príslušné oprávnenie na použitie certifikátu na podpísanie objektov). Používate Správcu digitálnych certifikátov (DCM) na manažovanie certifikátov, ktoré používate na podpisovanie objektov a na overovanie podpisov objektov. DCM môžete taktiež použiť na podpisovanie objektov a na overovanie podpisov objektov.

Digitálne certifikáty pre overovanie podpisov objektov

Od verzie V5R1 poskytuje iSeries podporu pre používanie certifikátov na overovanie elektronických podpisov na objektoch. Ktokoľvek, kto sa chce uistiť, že podpísaný objekt nebol počas prenosu zmenený a že objekt, ktorý odišiel z akceptovaného, legálneho zdroja, môže použiť verejný kľúč podpisujúceho certifikátu na overenie pôvodného elektronického podpisu. Ak sa podpis nezhoduje, údaje mohli byť zmenené. V takomto prípade môže príjemca zabrániť použitiu objektu a môže kontaktovať podpisovateľa, aby získal inú kópiu podpísaného objektu.

Podpis na objekte reprezentuje systém, ktorý podpísal objekt, nie konkrétneho užívateľa tohto systému. Ako súčasť procesu kontroly digitálnych podpisov musíte rozhodnúť, ktorým Certifikačným autoritám dôverujete a ktorým certifikátom dôverujete na podpisovanie objektov. Keď zvolíte dôveryhodnú CA, môžete rozhodnúť, či budete veriť podpisom, ktoré niekto vytvorí použitím certifikátu, ktorý vydala dôveryhodná CA. Keď sa rozhodnete nedôverovať CA, tiež sa rozhodnete nedôverovať certifikátom, ktoré vydala táto CA a ani podpisom, ktoré niekto vytvorí pomocou týchto certifikátov.

Systémová hodnota Verify object restore (QVFYOBJRST)

Ak sa rozhodnete vykonať overenie podpisu, jedno z prvých dôležitých rozhodnutí, ktoré musíte urobiť, je zistiť, nakoľko dôležité sú podpisy pre objekty, ktoré majú byť obnovované na vašom systéme. Toto riadite so systémovou hodnotou QVFYOBJRST. Štandardné nastavenie pre túto systémovú hodnotu umožňuje obnovu nepodpísaných objektov, ale zaisťuje, že podpísané objekty sa obnovia len vtedy, ak majú platný podpis. Systém definuje objekt ako podpísaný len vtedy, ak má objekt podpis, ktorému váš systém dôveruje; systém ignoruje ostatné, ″nedôveryhodné″ podpisy na objekte a takýto objekt berie ako nepodpísaný.

Pre systémovú hodnotu QVFYOBJRST môžete použiť niekoľko hodnôt v rozsahu od ignorovania všetkých podpisov po vyžadovanie platných podpisov pre všetky objekty, ktoré systém obnoví. Táto systémová hodnota ovplyvňuje len obnovované vykonateľné objekty, nie úložné súbory ani IFS súbory. Ak sa chcete dozvedieť viac o použití tejto alebo iných systémových hodnôt, pozrite si System Value Finder v Informačnom centre.

Správcu digitálnych certifikátov (DCM) používate na implementovanie vašich certifikátov a rozhodnutí o dôveryhodnosti CA, ako aj na manažovanie certifikátov, ktoré používate na overovanie podpisov objektov. DCM môžete taktiež používať na podpisovanie objektov a na overovanie podpisov objektov.

Kapitola 7. Konfigurovať DCM

Správca digitálnych certifikátov (DCM) poskytuje užívateľské rozhranie, založené na prehliadači, ktoré vám umožňuje manažovať digitálne certifikáty pre vaše aplikácie a užívateľov. Užívateľské rozhranie je rozdelené na dve hlavné časti: navigačná časť a úlohová časť.

Navigačnú časť používate na výber úloh na manažovanie certifikátov alebo aplikácií, ktoré ich používajú. Kým niektoré samostatné úlohy sa objavia priamo v hlavnej navigačnej časti, väčšina úloh v navigačnej časti je organizovaná do kategórií. Napríklad, **Manažovať certifikáty** je úloha, ktorá obsahuje rôzne samostatné úlohy, ako je Zobraziť certifikát, Obnoviť certifikát, Importovať certifikát, atď. Ak položka v navigačnej časti je kategória, ktorá obsahuje viac ako jednu úlohu, naľavo od nej sa zobrazí šípka. Táto šípka znamená, že keď vyberiete odkaz na túto kategóriu, zobrazí sa rozšírený zoznam úloh a vy si môžete vybrať úlohu, ktorú chcete vykonať.

S výnimkou kategórie **Rýchly spôsob**, každá kategória v navigačnej časti je úloha s návodom, ktorý vás rýchlo a jednoducho prevedie sériou krokov na dokončenie úlohy. Kategória Rýchly spôsob poskytuje zoskupenie funkcií na manažovanie certifikátov a aplikácií, ktoré umožňuje skúseným užívateľom DCM rýchlo pristupovať na rôzne súvisiace úlohy z centrálnej množiny strán.

Ktoré úlohy sú dostupné v navigačnej časti závisí na pamäti certifikátov, v ktorej pracujete. Taktiež kategória a počet úloh, ktoré vidíte v navigačnom rámci, sa mení v závislosti na oprávneniach, ktoré má váš užívateľský profil iSeries. Všetky úlohy pre prevádzkovanie CA, manažovanie certifikátov, ktoré aplikácie používajú a iné úlohy systémovej úrovne, sú dostupné iba pre bezpečnostných pracovníkov a správcov iSeries. Správcovia bezpečnosti alebo správcovia musia mať špeciálne oprávnenie *SECADM a *ALLOBJ, aby mohli vidieť a používať tieto úlohy. Používatelia bez týchto špeciálnych oprávnení majú prístup len na funkcie užívateľských certifikátov.

Ak sa chcete dozvedieť, ako nakonfigurovať DCM a ako ho začať používať na manažovanie vašich certifikátov, prezrite si tieto témy:

Spustenie DCM
Táto téma vás naučí, akým spôsobom pristúpiť na program Správca digitálnych certifikátov na vašom iSeries.

Nastaviť certifikáty po prvý krát
Táto téma vás naučí, ako začať s používaním DCM na nastavenie všetkého, čo potrebujete, keď používate certifikáty po prvý krát. Naučte sa, ako začať s manažovaním certifikátov z verejnej internetovej certifikačnej autority (CA), alebo ako vytvoriť a prevádzkovať súkromnú lokálnu CA na vydávanie certifikátov.

Ak by ste chceli náučnejšie informácie o používaní digitálnych certifikátov v prostredí internetu na zvýšenie bezpečnosti vášho systému a siete, vynikajúcim zdrojom je web stránka VeriSign. Web stránka VeriSign poskytuje rozsiahlu knižnicu s témami o digitálnych certifikátoch, ako aj množstvo iných tém o bezpečnosti v Internete. Do ich knižnice sa môžete dostať cez Sekciu pomoci VeriSign .

Spustiť Správcu digitálnych certifikátov

Aby ste mohli použiť ľubovoľnú z jeho funkcií, musíte spustiť Správcu digitálnych certifikátov (DCM). Aby ste zaistili úspešné spustenie DCM, vykonajte tieto kroky:

1. Nainštalujte voľbu 34 z 5722 SS1. To je Správca digitálnych certifikátov (DCM).

   Nainštalujte 5722 DG1. To je IBM HTTP Server for iSeries.

   Nainštalujte 5722 AC3. To je šifrovací produkt, ktorý DCM V5R2 používa na generovanie dvojice verejný-súkromný kľúč pre certifikáty, na zašifrovanie exportovaných súborov certifikátov a dešifrovanie importovaných súborov certifikátov.
2. Použite iSeries Navigator na spustenie inštancie *ADMIN pre HTTP Server:
   a. Spustite **iSeries Navigator**.
   b. Kliknite dvakrát na váš server iSeries v hlavnom stromovom pohľade.
   c. Spravte dvojité kliknutie na **Sieť**.
   d. Spravte dvojité kliknutie na **Servery**.
   e. Spravte dvojité kliknutie na **TCP/IP**.
   f. Pravým tlačidlom kliknite na **Správa HTTP**.
   g. Kliknite na **Spustiť**.
3. Spustite váš web prehliadač.
4. Použitím vášho prehliadača choďte na stránku Úlohy iSeries na vašom systéme na http://*názov_vášho_systému*:2001.
5. Vyberte **Správca digitálnych certifikátov** zo zoznamu produktov na stránke Úlohy iSeries na vstup do doplnok DCM.

Ak migrujete zo staršej verzie DCM, táto stránka vám poskytne podrobnosti, ktoré potrebujete na aktualizáciu vášho systému.

Nastaviť certifikáty po prvý krát

Ľavá časť Správcu digitálnych certifikátov (DCM) je navigačná časť úloh. Túto časť môžete použiť na výber širokého spektra úloh pre manažovanie certifikátov a aplikácií, ktoré ich používajú. Ktoré úlohy sú dostupné závisí na oprávnení vášho užívateľského profilu a na tom, ktorú pamäť certifikátov ste otvorili (ak vôbec nejakú). Väčšina úloh je dostupných len vtedy, ak máte špeciálne oprávnenia *ALLOBJ a *SECADM.

Keď použijete Správcu digitálnych certifikátov po prvýkrát, neexistuje žiadna pamäť certifikátov (ak ste nerobili prechod z predchádzajúcej verzie DCM). Ak máte potrebné opatrenia, navigačná časť zobrazí len tieto úlohy:

- Manažovať užívateľské certifikáty.
- Vytvoriť novú pamäť certifikátov
- Vytvoriť Certifikačnú autoritu (CA). (Poznámka: Ak vyberiete túto úlohu a vytvoríte súkromnú CA, táto úloha sa už v zozname neobjaví.)
- Manažovať miesta CRL.
- Manažovať umiestnenie požiadavky PKIX.

Aj keď na vašom systéme už existujú pamäte certifikátov (napríklad migrujete zo staršej verzie DCM), DCM v ľavom navigačnom rámci zobrazí iba obmedzený počet úloh alebo kategórií úloh. Aby ste mohli začať pracovať s väčšinou úloh manažmentu certifikátov a aplikácií, musíte najprv pristúpiť na príslušnú pamäť certifikátov. Ak chcete otvoriť konkrétnu pamäť certifikátov, v navigačnej časti kliknite na **Vybrať pamäť certifikátov**.

Navigačná časť DCM tiež poskytuje tlačidlo **Bezpečné spojenia**. Toto tlačidlo môžete použiť na to, aby sa otvorilo druhé okno prehliadača a inicializovalo sa bezpečné spojenie pomocou Secure Sockets Layer (SSL). Na úspešné používanie tejto funkcie musíte najprv nakonfigurovať IBM HTTP Server for iSeries na použitie SSL na prevádzku v bezpečnom

režime. Potom musíte spustiť HTTP Server v bezpečnom režime. Ak ste nenakonfigurovali a nespustili HTTP Server pre prevádzkovanie SSL, uvidíte chybové hlásenie a váš prehliadač nespustí zabezpečenú reláciu.

Začíname

Hoci možno chcete používať certifikáty na dosiahnutie mnohých bezpečnostných cieľov, čo urobíte ako prvé závisí od toho, ako plánujete získavať svoje certifikáty. Existujú dva hlavné spôsoby, pre ktoré sa môžete rozhodnúť pri prvom použití DCM a rozhodnúť sa musíte podľa toho, či chcete používať verejné certifikáty alebo súkromné certifikáty:

Vytvoriť a prevádzkovať lokálnu CA na vydávanie certifikátov vašim aplikáciám.

Manažovať certifikáty z verejnej internetovej CA pre používanie vašimi aplikáciami.

Vytvoriť a prevádzkovať lokálnu CA

Po dôslednom zhodnotení vašich bezpečnostných potrieb a politík ste sa rozhodli prevádzkovať lokálnu certifikačnú autoritu (CA) na vydávanie súkromných certifikátov pre vaše aplikácie. Môžete použiť Správcu digitálnych certifikátov (DCM) na vytvorenie a prevádzkovanie vašej vlastnej lokálnej CA. DCM vám poskytuje úlohy, ktoré vás prevedú procesom vytvorenia CA a jej použitia na vydanie certifikátov pre vaše aplikácie. Tieto úlohy zaistia, že máte všetko potrebné na začatie používania digitálnych certifikátov, na konfiguráciu aplikácií na používanie SSL, na podpisovanie objektov a kontrolu podpisov objektov.

Poznámka: Na použitie certifikátov s IBM HTTP Server for iSeries by ste mali vytvoriť a nakonfigurovať váš web server ešte pred prácou s DCM. Keď konfigurujete web server na používanie SSL, je vygenerované ID aplikácie pre server. Toto ID aplikácie si musíte zapamätať, aby ste mohli DCM použiť na špecifikáciu toho, ktorý certifikát má táto aplikácia použiť pre SSL.

Neukončujte a nereštartujte server, kým používate DCM na priradenie certifikátu k serveru. Ak ukončíte a reštartujete inštanciu *ADMIN web servera pred tým, ako k nemu priradíte certifikát, server sa nespustí vy nebudete schopný použiť DCM na priradenie u k serveru.

Na používanie DCM na vytvorenie a prevádzkovanie lokálnej CA postupujte podľa týchto krokov:

1. Spustite DCM.
2. V navigačnej časti DCM vyberte **Vytvoriť Certifikačnú autoritu**, aby sa zobrazila séria formulárov. Tieto formuláre vás prevedú procesom vytvorenia lokálnej CA a dokončením ďalších úloh, potrebných na začatie používania digitálnych certifikátov pre SSL, podpisovanie objektov a overovanie podpisov.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Vyplňte všetky formuláre pre túto úlohu. Použitím týchto formulárov na vykonanie všetkých úloh, ktoré potrebujete na nastavenie fungujúcej lokálnej certifikačnej autority (CA):
   a. Zvoľte, ako uložiť súkromný kľúč pre certifikát lokálnej CA. (Tento krok je zahrnutý, iba ak máte na vašom iSeries nainštalovaný IBM 4758–023 PCI Cryptographic Coprocessor. Ak váš systém nemá kryptografický procesor, DCM automaticky uloží certifikát a jeho súkromný kľúč do pamäte certifikátov Miestna Certifikačná autorita (CA).)
   b. Poskytnite identifikačné informácie pre lokálnu CA.

c. Nainštalujte certifikát lokálnej CA na váš PC alebo do vášho prehliadača, aby váš softvér mohol rozpoznať lokálnu CA a overiť certifikáty, ktoré CA vydá.
d. Zvoľte údaje politiky pre vašu lokálnu CA.
e. Použite novú lokálnu CA na vydanie serverovského alebo klientskeho certifikátu, ktorý vaše aplikácie budú môcť použiť pre pripojenia SSL. (Ak váš iSeries má nainštalovaný IBM 4758–023 PCI Cryptographic Coprocessor, tento krok vám umožní zvoliť, ako sa má uložiť súkromný kľúč pre serverovský alebo klientsky certifikát. Ak váš systém nemá koprocesor, DCM automaticky umiestni súkromný kľúč do pamäte certifikátov *SYSTEM. DCM vytvorí pamäť certifikátov *SYSTEM ako súčasť tejto podúlohy.)
f. Vyberte aplikácie, ktoré môžu používať certifikát servera alebo klienta pre SSL spojenia.

   Poznámka: Ak ste už v minulosti použili DCM na vytvorenie pamäte certifikátov *SYSTEM na manažovanie certifikátov pre SSL od verejnej internetovej CA, nemusíte vykonať tento ani predchádzajúci krok.
g. Použite novú lokálnu CA na vydanie certifikátu na podpisovanie objektov, ktorý aplikácie budú môcť použiť na elektronické podpisovanie objektov. Táto podúloha vytvorí pamäť certifikátov *OBJECTSIGNING; toto je pamäť certifikátov, ktorú používate na manažovanie certifikátov, podpisujúcich objekty.
h. Vyberte aplikácie, ktoré môžu používať certifikát, podpisujúci objekty, na digitálne podpisovanie objektov.

   Poznámka: Ak ste už v minulosti použili DCM na vytvorenie pamäte certifikátov *OBJECTSIGNING na manažovanie certifikátov, podpisujúcich objekty, od verejnej internetovej CA, nemusíte vykonať tento ani predchádzajúci krok.
i. Zvoľte aplikácie, ktoré by mali dôverovať vašej lokálnej CA.

Keď dokončíte túto úlohu, máte všetko, čo potrebujete na začatie konfigurovania aplikácií na použitie SSL pre bezpečnú komunikáciu.

Po tom, čo nakonfigurujete vaše aplikácie, musia užívatelia, ktorí pristupujú na aplikácie cez pripojenie SSL, použiť DCM na získanie kópie certifikátu lokálnej CA. Každý užívateľ musí mať kópiu certifikátu, aby ho klientsky softvér užívateľa mohol použiť na autentifikáciu identity servera ako súčasti procesu dohodovania SSL. Užívatelia môžu použiť DCM na skopírovanie certifikátu lokálnej CA do súboru, alebo na stiahnutie certifikátu do svojho prehliadača. Ako užívatelia uložia certifikátu lokálnej CA, závisí na klientskom softvére, ktorý používajú na vytvorenie pripojenia SSL do aplikácie.

Túto lokálnu CA môžete taktiež používať na vydanie certifikátov aplikáciám na iných systémoch iSeries vo vašej sieti.

Ak sa chcete dozvedieť viac o používaní DCM na manažovanie užívateľských certifikátov a o tom, ako môžu užívatelia získať kópiu certifikátu lokálnej CA na autentifikáciu certifikátov, ktoré lokálna CA vydáva, prezrite si tieto témy:

Manažovať užívateľské certifikáty
Naučte sa, ako môžu užívatelia používať DCM na získanie certifikátov, alebo združovať existujúce certifikáty s ich užívateľskými profilmi iSeries.

Použiť API na programové vydávanie certifikátov pre užívateľov iných ako i-Series
Naučte sa, ako môžete používať vašu lokálnu CA na vydávanie súkromných certifikátov užívateľom bez združovania certifikátu s užívateľským profilom iSeries.

Získať kópiu certifikátu súkromnej CA
Naučte sa, ako získať kópiu certifikátu súkromnej CA a ako ju nainštalovať do vášho PC tak, aby ste mohli autentifikovať akékoľvek serverovské certifikáty, ktoré CA vydáva.

Manažovať užívateľské certifikáty

Vy a vaši užívatelia môžu používať Správcu digitálnych certifikátov (DCM) na manažovanie certifikátov, ktoré potrebujú vaši užívatelia, aby mohli vytvárať Secure Sockets Layer (SSL) relácie.

Ak užívatelia pristupujú na vaše verejné alebo interné servery pomocou SSL spojenia, musia mať kópiu certifikátu Certifikačnej autority (CA), ktorá vydala certifikát servera. Musia mať certifikát CA, aby ich klientsky softvér mohol validovať autenticitu certifikátu servera na vytvorenie spojenia. Ak váš server používa certifikát od verejnej CA, softvér vašich užívateľov by už mal vlastniť kópiu tohto certifikátu CA. Aby vaši užívatelia mohli vytvoriť reláciu SSL, vy ako správca DCM, ani priamo vaši užívatelia, nemusíte vykonať žiadnu ďalšiu akciu. Avšak ak váš server používa certifikát zo súkromnej lokálnej CA, vaši užívatelia musia získať kópiu certifikátu lokálnej CA skôr, ako budú môcť so serverom vytvoriť reláciu SSL.

Okrem toho, ak aplikácia servera podporuje a vyžaduje autentifikáciu klientov cez certifikáty, užívatelia musia predložiť akceptovateľný certifikát užívateľa, aby sa dostali na prostriedky, ktoré poskytuje server. V závislosti od vašich potrieb bezpečnosti môžu užívatelia predložiť certifikát z verejnej internetovej CA, alebo taký, ktorý dostanú z lokálnej CA, ktorú prevádzkujete. Ak vaša serverovská aplikácia poskytuje prístup na prostriedky pre interných užívateľov, ktorí aktuálne majú užívateľské profily iSeries, môžete DCM použiť na pridanie ich certifikátov k ich užívateľským profilom. Toto priradenie zaisťuje, že predložení certifikátov majú užívatelia na prostriedky rovnaký prístup alebo obmedzenia, ako im poskytuje alebo zakazuje ich užívateľský profil.

Správca digitálnych certifikátov (DCM) vám umožňuje manažovať certifikáty, ktoré sú priradené k užívateľskému profilu iSeries. Ak máte užívateľský profil so špeciálnymi oprávneniami *SECADM a *ALLOBJ, môžete manažovať priradenia certifikátov užívateľských profilov sami pre seba alebo pre ostatných užívateľov. Keď nie je otvorená žiadna pamäť certifikátov, alebo keď je otvorená pamäť certifikátov Miestna Certifikačná autorita (CA), v navigačnej časti môžete vybrať **Manažovať užívateľské certifikáty**, aby ste mohli pristúpiť na príslušné úlohy. Ak je otvorená iná pamäť certifikátov, úlohy pre užívateľské certifikáty sú začlenené do úlohy pod **Manažovať certifikáty**.

Užívatelia bez mimoriadnych oprávnení užívateľského profilu *SECADM a *ALLOBJ môžu spravovať iba ich vlastné priradenia certifikátov. Môžu zvoliť **Manažovať užívateľské certifikáty** na prístup k úlohám, ktoré im umožnia prezerať certifikáty. združené s ich užívateľskými profilmi, odstrániť certifikát zo svojich užívateľských profilov, alebo priradiť certifikát z inej CA do svojich užívateľských profilov. Užívatelia môžu bez ohľadu na mimoriadne oprávnenia pre ich užívateľské profily získať užívateľský certifikát z lokálnej CA zvolením úlohy **Vytvoriť certifikát** v hlavnom navigačnom rámci.

Ak sa chcete dozvedieť viac o tom, ako používať DCM na správu a vytvorenie užívateľských certifikátov, prezrite si tieto témy:

Vytvoriť užívateľský certifikát
Použite tieto informácie na to, aby ste sa naučili, ako môžu užívatelia používať lokálnu CA na vydávanie certifikátu pre autentifikáciu klientov.

Priradiť užívateľský certifikát
V týchto informáciách sa dozviete o tom, ako spojiť vami vlastnený certifikát s vaším užívateľským profilom. certifikát môže byť zo súkromnej lokálnej CA na inom systéme, alebo zo známej internetovej CA. Aby ste mohli k svojmu užívateľskému profilu priradiť certifikát, server musí vydávajúcej CA dôverovať a certifikát nesmie byť už spojený s iným užívateľským profilom na systéme.

Vytvoriť užívateľský certifikát: Ak chcete použiť digitálne certifikáty na autentifikáciu užívateľa, užívatelia musia mať certifikáty. Ak používate Správcu digitálnych certifikátov (DCM) na prevádzkovanie lokálnej certifikačnej autority (CA), môžete lokálnu CA použiť na vydanie certifikátov pre každého užívateľa. Každý užívateľ musí použiť DCM na získanie certifikátu pomocou úlohy **Vytvoriť certifikát**. Na to, aby sa dal získať certifikát z lokálnej CA, musí politika CA umožniť CA vydať užívateľské certifikáty.

Na získanie certifikátu z lokálnej CA vykonajte tieto kroky:
1. Spustite DCM.
2. V navigačnej časti vyberte **Vytvoriť certifikát**.
3. Ako typ certifikátu na vytvorenie vyberte **Užívateľský certifikát**. Zobrazí sa formulár, na ktorom môžete zadať identifikačné informácie pre certifikát.
4. Vyplňte formulár a kliknite na **Pokračovať**.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
5. Na tomto mieste spolupracuje DCM s vašim prehliadačom pri vytvorení súkromného a verejného kľúča pre certifikát. Váš prehliadač môže zobraziť okná, ktoré vás povedú týmto procesom. Postupujte podľa inštrukcií prehliadača pre tieto úlohy. Keď prehliadač vygeneruje kľúče, zobrazí sa potvrdzovacia strana, ktorá oznamuje, že DCM vytvoril certifikát.
6. Nainštalujte nový certifikát do vášho prehliadača. Váš prehliadač môže zobraziť okná, ktoré vás povedú týmto procesom. Aby ste dokončili túto úlohu, postupujte podľa inštrukcií, ktoré vám poskytne prehliadač.
7. Kliknite na **OK** na dokončenie úlohy.

Počas spracovania Správca digitálnych certifikátov automaticky združí certifikát s vaším užívateľským profilom iSeries.

Ak chcete, aby mal certifikát z inej CA, ktorý užívateľ predkladá pre autentifikáciu klienta, rovnaké oprávnenia, ako jeho užívateľský profil, môže užívateľ použiť DCM na priradenie certifikátu k jeho užívateľskému profilu.

Priradiť užívateľský certifikát: Ak chcete použiť digitálne certifikáty na autentifikáciu užívateľa, užívatelia musia mať certifikáty. Ak vaši užívatelia musia predkladať certifikáty od verejnej internetovej Certifikačnej autority (CA), na priradenie týchto certifikátov k ich užívateľským profilom môžu použiť Správcu digitálnych certifikátov (DCM). Toto umožňuje vám a užívateľom použiť DCM na manažovanie týchto certifikátov.

Ak chcete použiť úlohu **Priradiť užívateľský certifikát**, musíte mať s HTTP Serverom vytvorenú bezpečnú reláciu cez ktorú pristupujete na Správcu digitálnych certifikátov (DCM). Či je vaša relácia bezpečná zistíte podľa čísla portu v URL, ktorý ste použili na prístup k DCM. Ak ste použili port 2001, čo je štandardný port pre prístup na DCM, nemáte bezpečnú reláciu. Pred tým, ako budete môcť prepnúť na bezpečnú reláciu, musí byť aj HTTP Server nakonfigurovaný na používanie SSL.

Keď vyberiete túto úlohu, zobrazí sa nové okno prehliadača. Ak nemáte bezpečnú reláciu, DCM vás požiada, aby ste klikli na **Priradiť užívateľský certifikát**, aby sa spustila. DCM potom inicializuje Secure Sockets Layer (SSL) dohody s vašim prehliadačom.

Ako časť týchto dohôd, váš prehliadať váš požiada o potvrdenie, či sa má dôverovať Certifikačnej autorite (CA), ktorá vydala certifikát, ktorý identifikuje HTTP Server. Váš prehliadač vás tiež môže požiadať o potvrdenie, či sa má akceptovať samotný certifikát servera.

Keď dovolíte vášmu prehliadaču dôverovať CA a akceptujete certifikát servera, server môže požadovať, aby ste predložili certifikát na autentifikáciu klienta. Podľa konfiguračných nastavení vášho prehliadača, váš prehliadač vás môže požiadať o výber certifikátu, ktorý sa predloží na autentifikáciu. Ak váš prehliadač predloží certifikát od CA, ktorý systém akceptuje ako dôveryhodný, DCM zobrazí informácie o certifikáte v samostatnom okne. Ak nepredložíte akceptovateľný certifikát, môže vás server za účelom autentifikácie, pred povolením prístupu, vyzvať na zadanie vášho užívateľského mena a hesla.

Keď vytvoríte bezpečnú reláciu, DCM sa pokúsi od vášho prehliadača získať certifikát, aby ho mohol spojiť s vašim užívateľským profilom. Ak DCM úspešne získa jeden alebo viac certifikátov, môžete zobraziť informácie o certifikáte a vybrať, že certifikát sa má spojiť s vašim užívateľským profilom.

Ak DCM nezobrazí informácie z certifikátu, neboli ste schopný predložiť certifikát, ktorý by mohol DCM priradiť k vášmu užívateľskému profilu. Môže to byť spôsobené jedným z niekoľkých problémov s užívateľskými certifikátmi. Napríklad, certifikát, ktorý obsahuje váš prehliadač už môže byť spojený s vašim užívateľským profilom.

Ak uprednostňujete použitie lokálnej CA na vydávanie certifikátov pre vašich užívateľov, musia namiesto toho užívatelia použiť úlohu vytvoriť užívateľský certifikát.

Použiť API na programové vydávanie certifikátov pre užívateľov iných ako i-Series

Počínajúc verziou V5R2 sú dostupné dva nové API, ktoré môžete používať na programové vydávanie certifikátov pre užívateľov iných ako i-Series. V predchádzajúcich vydaniach, ak ste používali vašu lokálnu certifikačnú autoritu (CA) na vydávanie certifikátov užívateľom, boli tieto certifikáty automaticky združené s ich užívateľskými profilmi iSeries. V dôsledku toho ak ste chceli použiť lokálnu CA na vydávanie certifikátu užívateľovi pre autentifikáciu klienta, museli ste tomu užívateľovi poskytnúť užívateľský profil iSeries. Taktiež keď užívateľ potreboval získať certifikát z lokálnej CA pre autentifikáciu klienta, musel každý užívateľ na vytvorenie potrebného certifikátu použiť Správcu digitálnych certifikátov (DCM). Z tohto dôvodu musí mať každý užívateľ užívateľský profil na serveri iSeries, ktorý hostuje DCM a platné prihlásenie na tento server iSeries.

Združovanie certifikátu s užívateľským profilom má svoje výhody, obzvlášť keď sa to týka interných užívateľov. Avšak tieto obmedzenia a požiadavky to robia menej praktickým pre použitie lokálnej CA na vydávanie užívateľských certifikátov pre veľký počet užívateľov, obzvlášť ak nechcete, aby títo užívatelia mali užívateľský profil iSeries. Aby ste sa vyhli poskytovaniu užívateľských profilov týmto užívateľom a chceli by ste vyžadovať certifikáty pre autentifikáciu užívateľov pre vašu aplikáciu, museli by ste požadovať od užívateľov, aby platili za certifikát zo známej CA.

Tieto dve nové API poskytujú podporu, ktorá vám umožní poskytnúť rozhranie pre vytváranie užívateľských certifikátov, podpísaných certifikátom lokálnej CA, pre akékoľvek užívateľské meno. Tento certifikát nebude združený s užívateľským profilom. Užívateľ nemusí existovať na serveri iSeries, ktorý hostuje DCM a užívateľ nemusí používať DCM na vytvorenie certifikátu.

Sú tu dva API, jeden pre každý z prevládajúcich prehliadačov, ktoré môžete vyvolať, keď používate Net.Data na vytvorenie programu na vydávanie certifikátov užívateľom. Aplikácia, ktorú vytvárate, musí poskytovať kód grafického užívateľského rozhrania (GUI), potrebný na vytvorenie užívateľského certifikátu a na zavolanie jedného z vhodných API na použitie lokálnej CA ma podpísanie certifikátu.

Viac informácií o použití týchto API nájdete na stránkach:
- API požiadavky na vygenerovanie a podpísanie užívateľského certifikátu (QYCUGSUC).

- API požiadavky na podpísanie užívateľského certifikátu (QYCUSUC).

Získať kópiu certifikátu súkromnej CA

Keď pristupujete na server, ktorý používa Secure Sockets Layer (SSL) spojenie, ako dôkaz svojej identity poskytne server vášmu klientskemu softvéru certifikát. Aby mohol server vytvoriť reláciu, váš klientsky softvér musí validovať certifikát servera. Aby sa dal validovať certifikát servera, váš klientsky softvér musí mať prístup na miestne uloženú kópiu certifikátu pre Certifikačnú autoritu (CA), ktorá vydala certifikát servera. Ak server predkladá certifikát z verejnej CA, váš prehliadač alebo iný klientsky softvér by už mal mať kópiu tohto certifikátu CA. Ak však server predkladá certifikát zo súkromnej lokálnej CA, musíte použiť Správcu digitálnych certifikátov (DCM) na získanie kópie certifikátu lokálnej CA.

DCM môžete použiť na stiahnutie certifikátu lokálnej CA priamo do vášho prehliadača, alebo môžete certifikát lokálnej CA skopírovať do súboru, aby k nemu mal iný klientsky softvér prístup a mohol ho použiť. Ak na bezpečné komunikácie používate prehliadač aj ďalšie aplikácie, môžete potrebovať na nainštalovanie certifikátu lokálnej CA použiť obidve metódy. Ak použijete obe metódy najprv nainštalujte certifikát do svojho prehliadača, až potom ho skopírujte a vložte do súboru.

Ak aplikácia servera vyžaduje, aby ste sa autentifikovali predložením certifikátu z lokálnej CA, mali by ste pred požiadaním o užívateľský certifikát z lokálnej CA stiahnuť certifikát lokálnej CA do vášho prehliadača.

Na použitie DCM na získanie kópie certifikátu lokálnej CA vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnom rámci vyberte **Nainštalovať certifikát lokálnej CA na váš PC** na zobrazenie stránky, ktorá vám umožní stiahnuť certifikát lokálnej CA do vášho prehliadača, alebo ho uložiť do súboru na vašom systéme.
3. Zvoľte metódu získanie certifikátu lokálnej CA.
   a. Zvoľte **Nainštalovať certifikát** na stiahnutie certifikátu lokálnej CA ako dôveryhodného zdroja do vášho prehliadača. Toto zaisťuje, že váš prehliadač môže vytvárať bezpečné komunikačné relácie so servermi, ktoré používajú certifikát od tejto CA. Váš prehliadač zobrazí sériu okien, ktoré vám pomôžu dokončiť inštaláciu.
   b. Zvoľte **Skopírovať a vložiť certifikát** na zobrazenie stránky, ktorá obsahuje špeciálne kódovanú kópiu certifikátu lokálnej CA. Skopírujte textový objekt, zobrazený na tejto strane do vašej odkladacej schránky. Neskôr musíte presunúť tieto informácie do súboru. Tento súbor je používaný obslužným programom PC (ako je MKKF alebo IKEYMAN) na ukladanie certifikátov pre použitie klientskymi programami na tomto PC. Pred tým, ako bude môcť vaša klientska aplikácia rozoznať a použiť certifikát lokálnej CA pre autentifikáciu, musíte aplikáciu nakonfigurovať tak, aby poznala certifikát ako dôveryhodný zdroj. Vytvorený súbor použite podľa inštrukcií, ktoré poskytujú tieto aplikácie.
4. Kliknite na **OK** na návrat na domovskú stránku Správcu digitálnych certifikátov.

Manažovať certifikáty z verejnej internetovej CA

Po pozornom prehodnotení vašich bezpečnostných potrieb a politík ste sa rozhodli, že chcete používať certifikáty od verejnej internetovej Certifikačnej autority (CA), ako je VeriSign. Napríklad, prevádzkujete verejné miesto web stránok a chcete používať Secure Sockets Layer (SSL) pre bezpečné komunikačné relácie, aby ste zaistili súkromnosť určitých informačných transakcií. Pretože miesto web stránok je dostupné širokej verejnosti, chcete používať certifikáty, ktoré môže ľahko rozoznať väčšina web prehliadačov.

Alebo, vyvíjate aplikácie pre externých zákazníkov a verejné certifikáty chcete používať na digitálne podpisovanie aplikačných balíkov. Podpísaním aplikačného balíka si môžu byť vaši zákazníci istý, že tento balík prišiel z vašej spoločnosti a počas prenosu nebol zmenený jeho obsah neautorizovanými stranami. Chcete použiť verejný certifikát, aby vaši zákazníci mohli

ľahko a lacno skontrolovať podpis na balíku. Tento certifikát tiež môžete použiť na kontrolu podpisu pre odoslaním balíka vašim zákazníkom.

Úlohy v Správcovi digitálnych certifikátov (DCM) môžete použiť na centrálne manažovanie týchto verejných certifikátov a aplikácií, ktoré ich používajú na vytváranie SSL spojení, podpisovanie objektov alebo kontrolu autenticity digitálnych podpisov na objektoch.

Manažovať verejné certifikáty

Keď použijete DCM na manažovanie certifikátov od verejnej internetovej CA, musíte najprv vytvoriť Internet. Pamäť certifikátov je špeciálny databázový súbor kľúčov, ktorý používa DCM na ukladanie digitálnych certifikátov a s nimi spojených súkromných kľúčov. DCM vám umožňuje vytvárať a manažovať niekoľko typov pamäte certifikátov, podľa typu certifikátov, ktoré obsahujú.

Typ pamäte certifikátov, ktorý vytvoríte a následné úlohy, ktoré musíte vykonať na manažovanie svojich certifikátov a aplikácií ktoré ich používajú, závisí na tom, ako plánujete používať svoje certifikáty. Ak sa chcete dozvedieť viac o použití DCM na vytvorenie príslušnej pamäte certifikátov a manažovaní vašich certifikátov pre vaše aplikácie, pozrite si tieto témy:

- Manažovať verejné internetové certifikáty pre relácie komunikácií SSL.
- Manažovať verejné internetové certifikáty pre podpisovanie objektov.
- Manažovať certifikáty pre overovanie podpisov objektov.

DCM vám tiež umožňuje manažovať certifikáty, ktoré získate z certifikačnej autority PKIX (Public Key Infrastructure for X.509).

Manažovať verejné internetové certifikáty pre relácie komunikácií SSL

Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov pre vaše aplikácie, aby na vytváranie bezpečných komunikačných relácií používali Secure Sockets Layer (SSL). Ak nepoužívate DCM na prevádzkovanie vašej vlastnej lokálnej certifikačnej autority (CA), musíte najprv vytvoriť príslušnú pamäť certifikátov na manažovanie verejných certifikátov, ktoré používate pre SSL. Tou je pamäť certifikátov *SYSTEM. Keď vytvoríte pamäť certifikátov, DCM vás prevedie procesom vytvorenia informácií na požiadanie o certifikát, ktoré musíte poskytnúť verejnej CA na získanie certifikátu.

Ak chcete použiť DCM na manažovanie a používanie verejných internetových certifikátov, aby mohli vaše aplikácie vytvárať komunikačné SSL relácie, vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti DCM vyberte **Vytvoriť novú pamäť certifikátov**, aby sa spustila úloha a mohli ste vyplniť sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia pamäte certifikátov a certifikátu, ktoré môžu vaše aplikácie použiť pre SSL relácie.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Zvoľte ***SYSTEM** ako pamäť certifikátov, ktorá sa má vytvoriť a kliknite na **Pokračovať**.
4. Vyberte **Áno**, aby sa certifikát vytvoril ako časť vytvárania pamäte certifikátov *SYSTEM a kliknite na **Pokračovať**.

5. Ako podpisovateľa nového certifikátu vyberte **VeriSign alebo iná internetová Certifikačná autorita (CA)** a kliknite na **Pokračovať**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačnú informácie pre nový certifikát.

   Poznámka: Ak váš iSeries má nainštalovaný IBM 4758–023 PCI Šifrovací koprocesor, DCM vám ako nasledujúcu úlohu umožní zvoliť, ako sa má uložiť súkromný kľúč pre certifikát. Ak váš systém nemá koprocesor, DCM automaticky umiestni súkromný kľúč do pamäte certifikátov *SYSTEM. Ak potrebujete pomoc pri výbere, ako sa má uložiť súkromný kľúč, pozrite si online pomoc v DCM.

6. Vyplňte formulár a kliknite na **Pokračovať**, aby sa zobrazila strana s potvrdením. Táto potvrdzovacia strana zobrazuje údaje požiadavky na certifikát, ktoré musíte poskytnúť verejnej Certifikačnej autorite (CA), ktorá vydá váš certifikát. Údaje CSR (Certificate Signing Request) obsahujú verejný kľúč a iné informácie, ktoré ste špecifikovali pre nový certifikát.
7. Pozorne skopírujte a vložte údaje CSR do aplikačného formulára certifikátu, alebo do samostatného súboru, ktoré požaduje verejná CA na vyžiadanie certifikátu. Musíte použiť všetky údaje CSR, vrátane riadkov Begin a End New Certificate Request. Keď odídete z tejto strany, údaje sa stratia a nedajú sa už obnoviť. Pošlite tento aplikačný formulár alebo súbor do CA, ktorú ste vybrali na vydanie a podpísanie vášho certifikátu.

   Poznámka: Aby sa dokončila táto procedúra, musíte počkať, kým CA nevráti podpísaný, dokončený certifikát.

   Poznámka: Na použitie certifikátov s HTTP Server for iSeries by ste mali vytvoriť a nakonfigurovať váš web server ešte pred prácou s DCM na prácu s podpísaným dokončeným certifikátom. Keď konfigurujete web server na používanie SSL, je vygenerované ID aplikácie pre server. Toto ID aplikácie si musíte zapamätať, aby ste mohli DCM použiť na špecifikáciu toho, ktorý certifikát má táto aplikácia použiť pre SSL.

   Neukončujte a nereštartujte server, kým používate DCM na priradenie podpísaného dokončeného certifikátu k serveru. Ak ukončíte a reštartujete inštanciu *ADMIN web servera pred tým, ako k nemu priradíte certifikát, server sa nespustí vy nebudete schopný použiť DCM na priradenie u k serveru.

8. Keď verejná CA vráti váš podpísaný certifikát, spustite DCM.
9. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
10. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
11. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
12. Zo zoznamu úloh vyberte **Importovať certifikát**, aby sa spustil proces importu podpísaného certifikátu do pamäte certifikátov *SYSTEM. Po dokončení importu certifikátu môžete špecifikovať aplikácie, ktoré by ho mali používať pre SSL komunikáciu.
13. V navigačnej časti okna vyberte **Manažovať aplikácie**, aby sa zobrazil zoznam úloh.
14. Zo zoznamu úloh vyberte **Zaktualizovať priradenie certifikátu**, aby sa zobrazil zoznam aplikácií s podporou SSL, ktorým chcete priradiť certifikát.
15. Vyberte niektorú aplikáciu zo zoznamu a kliknite na **Zaktualizovať priradenie certifikátu**.

16. Vyberte certifikát, ktorý ste naimportovali a kliknite na **Priradiť nový certifikát**. DCM zobrazí správu, ktorou potvrdí váš výber certifikátu pre aplikáciu.

    Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Ak chcete, aby aplikácia s touto podporou bola schopná autentifikovať certifikáty pred poskytnutím prístupu na prostriedky, musíte pre aplikáciu definovať zoznam dôveryhodných CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívateľ alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Keď dokončíte túto úlohu, máte všetko, čo potrebujete na začatie konfigurovania aplikácií na použitie SSL pre bezpečnú komunikáciu. Aby mohli užívatelia používať tieto aplikácie pomocou SSL, musia mať kópiu certifikátu CA pre CA, ktorá vydala certifikát servera. Ak je váš certifikát od dobre známej internetovej CA, klientsky softvér vašich užívateľov už môže mať kópiu potrebného certifikátu CA. Ak užívatelia potrebujú získať certifikát CA, mali by navštíviť web stránku danej CA a riadiť sa inštrukciami na tejto stránke.

Manažovať verejné internetové certifikáty pre podpisovanie objektov

Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov na digitálne podpisovanie objektov. Ak nepoužívate DCM na prevádzkovanie vašej vlastnej lokálnej certifikačnej autority (CA), musíte najprv vytvoriť príslušnú pamäť certifikátov na manažovanie verejných certifikátov, ktoré používate na podpisovanie objektov. Tou je pamäť certifikátov *OBJECTSIGNING. Keď vytvárate pamäť certifikátov, DCM vás prevedie procesom vytvárania informácií o požiadavke na certifikát, ktoré musíte poskytnúť verejnej internetovej CA na získanie certifikátu.

Ak chcete použiť certifikát na podpisovanie objektov, musíte najprv definovať ID aplikácie. Toto ID aplikácie riadi oprávnenie, ktoré musí mať niekto, kto chce podpísať objekty s konkrétnym certifikátom, a riadi ďalšiu úroveň riadenia prístupu okrem tej, ktorú poskytuje DCM. Štandardne, definícia aplikácie vyžaduje od užívateľa, aby mal špeciálne oprávnenie *ALLOBJ, ak chce použiť certifikát pre aplikáciu podpisujúce objekty. (Aj keď oprávnenie, ktoré ID aplikácie vyžaduje, môžete zmeniť prostredníctvom iSeries Navigator.)

Ak chcete použiť DCM na manažovanie a používanie verejných internetových certifikátov na podpisovanie objektov, vykonajte tieto kroky:

1. Spustite DCM.
2. V ľavej navigačnej časti DCM vyberte **Vytvoriť novú pamäť certifikátov**, aby sa spustila úloha a mohli vyplniť sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia pamäte certifikátov a certifikátu, ktorý môžete použiť na podpisovanie objektov.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Zvoľte ***OBJECTSIGNING** ako pamäť certifikátov, ktorá sa má vytvoriť a kliknite na **Pokračovať**.
4. Vyberte **Áno**, aby sa certifikát vytvoril ako časť vytvárania pamäte certifikátov a kliknite na **Pokračovať**.
5. Ako podpisovateľa nového certifikátu vyberte **VeriSign alebo iná internetová Certifikačná autorita (CA)** a kliknite na **Pokračovať**. Týmto sa zobrazí formulár, ktorý vám umožňuje zadať identifikačnú informácie pre nový certifikát.

6. Vyplňte formulár a kliknite na **Pokračovať**, aby sa zobrazila strana s potvrdením. Táto potvrdzovacia strana zobrazuje údaje požiadavky na certifikát, ktoré musíte poskytnúť verejnej Certifikačnej autorite (CA), ktorá vydá váš certifikát. Údaje CSR (Certificate Signing Request) obsahujú verejný kľúč a iné informácie, ktoré ste špecifikovali pre nový certifikát.
7. Pozorne skopírujte a vložte údaje CSR do aplikačného formulára certifikátu, alebo do samostatného súboru, ktoré požaduje verejná CA na vyžiadanie certifikátu. Musíte použiť všetky údaje CSR, vrátane riadkov Begin a End New Certificate Request. Keď odídete z tejto strany, údaje sa stratia a nedajú sa už obnoviť. Pošlite tento aplikačný formulár alebo súbor do CA, ktorú ste vybrali na vydanie a podpísanie vášho certifikátu.

   Poznámka: Aby sa dokončila táto procedúra, musíte počkať, kým CA nevráti podpísaný, dokončený certifikát.
8. Keď verejná CA vráti váš podpísaný certifikát, spustite DCM.
9. V ľavej navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***OBJECTSIGNING**.
10. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
11. V navigačnej časti okna vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
12. Zo zoznamu úloh vyberte **Importovať certifikát**, aby sa spustil proces importu podpísaného certifikátu do pamäte certifikátov *OBJECTSIGNING. Po dokončení importu certifikátu môžete vytvoriť definíciu aplikácie na používanie certifikátu na podpisovanie objektov.
13. Po zaktualizovaní obsahu ľavej navigačnej časti vyberte **Manažovať aplikácie**, aby sa zobrazil zoznam úloh.
14. Zo zoznamu úloh vyberte **Pridať aplikáciu**, aby sa spustil proces vytvorenia definície aplikácie, podpisujúcej objekty, na použitie s certifikátom na podpisovanie objektov.
15. Vyplnením formulára zadefinujte aplikáciu na podpisovanie objektov a kliknite na **Pridať**. Táto definícia aplikácie nepopisuje skutočnú aplikáciu, ale popisuje typ objektov, ktoré chcete podpisovať konkrétnym certifikátom. Pri vypĺňaní formuláru môžete použiť online pomoc.
16. Kliknite na **OK**, aby sa potvrdila správa o vytvorení definície a zobrazil úloh Manažovať aplikácie.
17. Zo zoznamu úloh vyberte **Aktualizovať priradenie certifikátu** a kliknite na **Pokračovať** na zobrazenie zoznamu ID aplikácií podpisujúcich objekty, pre ktoré chcete priradiť certifikát.
18. Zo zoznamu ID aplikácií vyberte svoju aplikáciu a kliknite na **Zaktualizovať priradenie certifikátu**.
19. Vyberte certifikát, ktorý ste naimportovali a kliknite na **Priradiť nový certifikát**.

Po dokončení týchto úloh máte všetko potrebné na začatie podpisovania objektov na zaručenie ich integrity.

Keď distribuujete podpísané objekty, tí, ktorí prijímajú tieto objekty, musia použiť V5R1 alebo novšie verzie DCM na overenie podpisu na objektoch na zabezpečenie, že sú údaje nezmenené a na overenie identity odosielateľa. Aby sa overil podpis, prijímateľ musí mať kópiu certifikátu na kontrolu podpisu. Tento certifikát by ste mali poskytnúť ako časť balíka podpísaných objektov.

Prijímateľ tiež musí mať kópiu certifikátu CA pre CA, ktorá vydala certifikát, ktorý ste použili na podpísanie objektu. Ak ste podpísali objekty s certifikátom od dobre známej internetovej CA, prijímateľova verzia DCM by už mala mať kópiu potrebného certifikátu CA. Ak si myslíte, že prijímateľ ešte nemá kópiu certifikátu CA, mali by ste ju poskytnúť spolu s

podpísanými objektmi. Napríklad mali by ste poskytnúť kópiu certifikátu lokálnej CA, ak ste podpísali objekty s certifikátom zo súkromnej lokálnej CA. Z bezpečnostných dôvodov by ste mali poskytnúť certifikát CA v samostatnom balíku alebo na požiadanie adresátov by ste mali tento certifikát CA spraviť verejne dostupným.

Manažovať certifikáty pre overovanie podpisov objektov

Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie certifikátov na kontrolu podpisov, ktoré používate na validovanie digitálnych podpisov na objektoch. Ak chcete podpísať objekt, na vytvorenie podpisu použijete súkromný kľúč certifikátu. Keď posielate tento podpísaný objekt ostatným, musíte poslať aj kópiu certifikátu, ktorý podpísal tento objekt. Urobíte to pomocou DCM a vyexportujete certifikát, podpisujúci objekty (bez súkromného kľúča certifikátu), ako certifikát na kontrolu podpisu. Certifikát na kontrolu podpisu môžete vyexportovať do súboru, ktorý potom môžete distribuovať ostatným. Alebo, ak chcete overiť podpisy, ktoré vytvoríte, môžete vyexportovať certifikát na kontrolu podpisu do pamäte certifikátov *SIGNATUREVERIFICATION.

Ak chcete validovať podpis na objekte, musíte mať kópiu certifikátu, ktorý podpísal objekt. Na kontrolu podpisu, ktorý bol vytvorený súkromným kľúčom používate verejný kľúč certifikátu, ktorý obsahuje certifikát. Aby ste teda mohli skontrolovať podpis na objekte, musíte získať kópiu podpisujúceho certifikátu od kohokoľvek, kto vám poskytol podpísané objekty.

Musíte tiež mať kópiu certifikátu Certifikačnej autority (CA) pre CA, ktorá vydala certifikát, ktorý podpísal objekt. Certifikát CA používate na kontrolu autenticity certifikátu, ktorý podpísal objekt. DCM poskytuje kópie certifikátov CA od dobre známych CA. Ak bol však objekt podpísaný certifikátom z inej verejnej CA alebo súkromnej lokálnej CA, pred tým, ako budete môcť overiť podpis objektu, budete musieť získať kópiu tohto certifikátu CA.

Ak chcete na kontrolu podpisov objektov používať DCM, musíte najprv vytvoriť vhodnú pamäť certifikátov na manažovanie potrebných certifikátov na kontrolu podpisu; jedná sa o pamäť certifikátov *SIGNATUREVERIFICATION. Keď vytvoríte túto pamäť certifikátov, DCM do nej automaticky uloží certifikáty väčšiny dobre známych verejných CA.

Poznámka: Ak chcete kontrolovať podpisy, ktoré ste vytvorili pomocou vlastných certifikátov, podpisujúcich objekty, musíte vytvoriť pamäť certifikátov *SIGNATUREVERIFICATION a skopírovať do nej certifikáty z pamäte certifikátov *OBJECTSIGNING. To platí aj vtedy, ak chcete vykonávať kontrolu podpisov pomocou pamäte certifikátov *OBJECTSIGNING.

Ak chcete na manažovanie svojich certifikátov na kontrolu podpisu použiť DCM, vykonajte tieto kroky:

1. Spustite DCM.
2. V ľavej navigačnej časti DCM vyberte **Vytvoriť novú pamäť certifikátov**, aby sa spustila úloha a mohli vyplniť sériu formulárov.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Zvoľte ***SIGNATUREVERIFICATION** ako pamäť certifikátov, ktorá sa má vytvoriť a kliknite na **Pokračovať**.

   Poznámka: Ak pamäť certifikátov *OBJECTSIGNING existuje, na tomto mieste vás DCM požiada o špecifikovanie, či sa majú do novej pamäte certifikátov skopírovať certifikáty, podpisujúce objekty, ako certifikáty na kontrolu podpisu. Ak chcete na kontrolu podpisov používať vlastné existujúce certifikáty, podpisujúce objekty, mali by ste vybrať **Áno** a kliknúť na

Pokračovať. Aby ste mohli skopírovať certifikáty z pamäte certifikátov *OBJECTSIGNING, musíte poznať heslo.

4. Špecifikujte heslo pre novú pamäť certifikátov a kliknite na **Pokračovať**, aby sa vytvorila pamäť certifikátov. Zobrazí sa potvrdzovacia stránka na naznačenie, že bola pamäť certifikátov úspešne vytvorená. Teraz môžete použiť túto pamäť manažovanie a použitie certifikátov na kontrolu podpisov objektov.

   Poznámka: Ak ste vytvorili túto pamäť, aby ste mohli kontrolovať podpisy na objektoch, ktoré ste podpísali, nerobte to. Keď vytvoríte nové certifikáty, podpisujúce objekty, mali by ste ich vyexportovať z pamäte certifikátov *OBJECTSIGNING do tejto pamäte certifikátov. Ak ich nevyexportujete, nebudete môcť kontrolovať podpisy, ktoré s nimi vytvoríte.

   Poznámka: Ak ste vytvorili tú pamäť certifikátov, aby ste mohli kontrolovať podpisy na objektoch, ktoré prijmete z iných zdrojov, mali by ste pokračovať v tejto procedúre, aby ste naimportovali potrebné certifikáty do pamäte certifikátov.
5. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SIGNATUREVERIFICATION**.
6. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
7. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
8. Zo zoznamu úloh vyberte **Importovať certifikát**. Táto riadená úloha vás prevedie procesom importovania certifikátov, ktoré potrebujete, do pamäte certifikátov, aby ste mohli overovať podpis na objektoch, ktoré ste prijali.
9. Vyberte typ certifikátu, ktorý chcete naimportovať. Zvoľte **Overovanie podpisu** na import certifikátu, ktorý ste prijali s podpísanými objektmi a dokončite importovaciu úlohu.

   Poznámka: Ak pamäť certifikátov ešte neobsahuje kópiu certifikátu CA pre CA, ktorá vydala certifikát na overovanie podpisu, musíte *najprv* naimportovať certifikát CA. Ak pred importovaním certifikátu na overovanie podpisu nenaimportujete certifikát CA, môžete prijať chybové hlásenie pri importovaní certifikátu na overovanie podpisu.

Teraz môžete používať tieto certifikáty na kontrolu podpisov objektov.

Kapitola 8. Manažovanie DCM

Po tom, čo ste nakonfigurovali Správcu digitálnych certifikátov (DCM) je tu niekoľko úloh na správu certifikátov, ktoré budete potrebovať vykonať. Ak sa chcete dozvedieť, ako používať DCM na správu digitálnych certifikátov, prezrite si tieto témy:

Použiť lokálnu CA na vydávanie certifikátov pre iné systémy iSeries
Naučte sa, ako používať súkromnú lokálnu CA na jednom systéme na vydávanie certifikátov pre použitie na iných systémoch iSeries.

Manažovať aplikácie v DCM
Naučte sa, ako používať DCM na prácu s definíciami aplikácií pre aplikácie, podporujúce SSL, alebo pre aplikácie na podpisovanie objektov. Táto téma poskytuje informácie o vytváraní definícií aplikácií a spôsobe manažovania priradenia certifikátov aplikáciám. Dozviete sa tu tiež o definovaný zoznamov dôveryhodných CA, ktoré používajú aplikácie ako základ pri akceptovaní certifikátov na autentifikáciu klienta.

Overiť platnosť certifikátov a aplikácií
Naučte sa, ako môžete overiť autenticitu určitého certifikátu pre tým, ako ho aplikácia použije alebo akceptuje.

Priradiť certifikáty
Naučte sa, ako môžete rýchlo priradiť certifikát k jednej alebo viacerým aplikáciám na použitie pre bezpečné funkcie.

Manažovať umiestnenia CRL Naučte sa, ako definovať a používať umiestnenia Zoznamu odmietaných certifikátov (CRL), ktoré môžu aplikácie používať na overenie, či sú certifikáty, ktoré akceptujú, platné.

Uložiť kľúče certifikátov na IBM 4758 Cryptographic Coprocessor
Naučte sa, ako používať nainštalovaný koprocesor na poskytnutie bezpečnejšieho uloženia pre súkromné kľúče vašich certifikátov.

Manažovať umiestnenie požiadavky pre PKIX CA
Naučte sa, ako môžete použiť DCM na manažovanie certifikátov, ktoré získate z verejných internetových CA, ktoré vydávajú certifikáty pod štandardmi PKIX (Public Key Infrastructure for X.509).

Podpisovať objekty
Naučte sa, ako používať DCM na správu certifikátov, ktoré používate na elektronické podpisovanie objektov na zabezpečenie ich integrity.

Overiť podpisy objektov
Naučte sa, ako používať DCM na overovanie autenticity elektronických podpisov na objektoch.

Použiť lokálnu CA na vydávanie certifikátov pre iné systémy iSeries

Možno už používate súkromnú lokálnu certifikačná autoritu (CA) na systéme iSeries vo vašej sieti. Teraz chcete rozšíriť použitie tejto lokálnej CA na ďalšie systémy iSeries vo vašej sieti. Napríklad chcete, aby vaša aktuálna lokálna CA vydala serverovský alebo klientsky certifikát pre aplikáciu na inom systéme iSeries na použitie pre relácie komunikácií SSL. Alebo chcete používať certifikáty z vašej lokálnej CA na jednom systéme na podpisovanie objektov, ktoré sú uložené na inom serveri iSeries.

Toto môžete dosiahnuť použitím Správcu digitálnych certifikátov (DCM). Vykonávate nejaké úlohy na iSeries, na ktorom prevádzkujete lokálnu CA a iné vykonávate na sekundárnom systéme iSeries, ktorý hosťuje aplikácie, pre ktoré chcete vydať certifikáty. Tento sekundárny systém sa nazýva cieľový systém. Úlohy, ktoré musíte vykonať na cieľovom systéme, závisia na úrovni vydania toho systému.

Poznámka: Môžete naraziť na problém, ak systém iSeries, na ktorom prevádzkujete lokálnu CA, používa produkt so silnejším šifrovaním, než má cieľový systém. (Pre V5R2 je jediný dostupný poskytovateľ šifrovaného prístupu 5722–AC3, ktorý je najsilnejším dostupným produktom. Avšak v starších vydaniach ste mohli nainštalovať iné, slabšie produkty (5722–AC1, alebo 5722–AC2), ktoré poskytujú nižšiu úroveň šifrovacej funkcie.) Keď vyexportujete certifikát (a jeho súkromným kľúčom), systém zašifruje tento súbor, aby ochránil jeho obsah. Ak systém používa silnejší kryptografický produkt ako cieľový systém, cieľový systém nemôže počas procesu importu tento súbor dešifrovať. Následne, import zlyhá alebo tento certifikát nebudete môcť použiť na vytvorenie SSL relácií. Toto platí aj v prípade, ak pre nový certifikát použijete veľkosť kľúča, ktorá je vhodná na použitie s kryptografickým produktom na cieľovom systéme.

Vašu lokálnu CA môžete použiť na vydávanie certifikátov iným systémom, ktoré potom môžete používať na podpisovanie objektov, alebo ktoré môžu aplikácie používať na vytváranie relácií SSL. Keď používate lokálnu CA na vytváranie certifikátu pre použitie na inom systéme iSeries, súbory, ktoré DCM vytvára, obsahujú kópiu certifikátu lokálnej CA, ako aj kópie certifikátov pre mnohé verejné internetové CA.

Úlohy, ktoré musíte vykonať v DCM, sa nepatrne líšia v závislosti na tom, ktorý typ certifikátu, ktorý vaša lokálna CA vydáva a na úrovni vydania a podmienkach na cieľovom systéme.

Vydať súkromný certifikát pre použitie na inom V5R2 alebo V5R1 systéme iSeries

Na používanie vašej lokálnej CA na vydávanie certifikátov pre použitie na inom V5R2 alebo V5R1 systéme iSeries vykonajte tieto kroky na systéme, ktorý hosťuje lokálnu CA:

1. Spustite DCM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
2. V navigačnom rámci zvoľte **Vytvoriť certifikát** na zobrazenie zoznamu typov certifikátov, na ktorých vytvorenie môžete použiť lokálnu CA.

   Aby ste dokončili túto úlohu, nemusíte otvoriť pamäť certifikátov. Tieto inštrukcie predpokladajú, že nepracujete v niektorej konkrétnej pamäti certifikátov a ani v pamäti certifikátov miestnej Certifikačnej autority (CA). Lokálna CA musí existovať na tomto systéme pred tým, ako budete môcť vykonať tieto úlohy.
3. Zvoľte typ certifikátu, ktorý chcete, aby lokálna CA vydala a kliknite na **Pokračovať** na spustenie riadenej úlohy a dokončenie série formulárov. Zvoľte vytvorenie **serverovského alebo klientskeho certifikátu pre iný iSeries** (pre relácie SSL), alebo **certifikát na podpisovanie objektov pre iný iSeries** (pre použitie na inom systéme).

   Poznámka: Ak vytvárate certifikát na podpisovanie objektov pre použitie iným systémom, na použitie certifikátu musí na tomto systéme bežať V5R1, alebo novšia verzia OS/400. Pretože cieľový systém musí mať verziu V5R1 alebo neskoršiu, DCM na hostiteľskom systéme vás nepožiada o výber formátu cieľového vydania pre nový certifikát, podpisujúci objekty.
4. Ak vytvárate serverovský alebo klientsky certifikát, vyberte úroveň vydania systému iSeries, pre ktorý vytvárate tento certifikát. Kliknite na **Pokračovať**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačné informácie pre nový certifikát.

   Poznámka: Vami vybraná úroveň vydania určuje formát, ktorý použije DCM na vytvorenie nového certifikátu. Množstvo a typ identifikačných informácií na

tomto formulári je rôzny, v závislosti od vami vybranej úrovne vydania. To zabezpečí, že súbory certifikátov sú kompatibilné so systémom iSeries, ktorý bude certifikát používať.

5. Vyplňte formulár a kliknite na **Pokračovať**, aby sa zobrazila strana s potvrdením.

   Poznámka: Ak na cieľovom systéme existuje pamäť certifikátov *OBJECTSIGNING alebo *SYSTEM, pre certifikát určite špecifikujte jedinečné označenie certifikátu a názov súboru. Špecifikovaním jedinečného označenia certifikátu sa zaistí, že tento certifikát môžete ľahko naimportovať do existujúcej pamäti certifikátov na cieľovom systéme.

   Táto potvrdzovacia strana zobrazuje názvy súborov, ktoré vytvoril DCM a ktoré treba preniesť do cieľového systému. DCM vytvorí tieto súbory podľa vami špecifikovanej úrovne vydania cieľového systému. DCM automaticky vloží do týchto súborov kópiu certifikátu lokálnej CA.

   Poznámka: DCM vytvorí nový certifikát vo svojej vlastnej pamäte certifikátov a vygeneruje dva súbory, ktoré máte preniesť: súbor pamäte certifikátov (prípona .KDB) a súbor požiadavky (prípona .RDB).

6. Na prenos týchto súborov do cieľového systému použite FTP (File Transfer Protocol) alebo inú metódu.

Vydať súkromný certifikát pre použitie na V4R4 alebo V4R5 systéme iSeries

Na používanie vašej lokálnej CA na vydávanie certifikátov pre použitie na V4R4 alebo V4R5 systéme iSeries vykonajte tieto kroky na systéme, ktorý hostuje lokálnu CA V5R2:

1. Spustite DCM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.

2. V navigačnom rámci zvoľte **Vytvoriť certifikát** na zobrazenie zoznamu typov certifikátov, na ktorých vytvorenie môžete použiť lokálnu CA.

   Aby ste dokončili túto úlohu, nemusíte otvoriť pamäť certifikátov. Tieto inštrukcie predpokladajú, že nepracujete v niektorej konkrétnej pamäti certifikátov a ani v pamäti certifikátov miestnej Certifikačnej autority (CA). Lokálna CA musí existovať na tomto systéme pred tým, ako budete môcť vykonať tieto úlohy.

3. Zvoľte typ certifikátu, ktorý chcete, aby lokálna CA vydala a kliknite na **Pokračovať** na spustenie riadenej úlohy a dokončenie série formulárov.

   Poznámka: Pretože tento certifikát vytvárate pre použitie na V4R4 alebo V4R5 systéme iSeries, musíte zvoliť **serverovský alebo klientsky certifikát pre iný iSeries**. Cieľové systémy so skorším vydaním ako V5R1 nemôžu používať certifikáty, podpisujúce objekty.

4. Vyberte úroveň vydania iSeries, pre ktorý vytvárate tento certifikát. Kliknite na **Pokračovať**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačné informácie pre nový certifikát.

   Poznámka: Vami vybraná úroveň vydania určuje formát, ktorý použije DCM na vytvorenie nového certifikátu. Množstvo a typ identifikačných informácií na tomto formulári je rôzny, v závislosti od vami vybranej úrovne vydania. To zabezpečí, že súbory certifikátov sú kompatibilné so systémom iSeries, ktorý bude certifikát používať.

5. Vyplňte formulár a kliknite na **Pokračovať**, aby sa zobrazila strana s potvrdením.

Poznámka: Ak na cieľovom systéme existuje pamäť certifikátov *SYSTEM, uistite sa, že zadávate jedinečné označenie certifikátu a jedinečný názov súboru pre certifikát. Špecifikovaním jedinečného označenia certifikátu sa zaistí, že tento certifikát môžete ľahko naimportovať do existujúcej pamäti certifikátov na cieľovom systéme.

Táto potvrdzovacia strana zobrazuje názvy súborov, ktoré vytvoril DCM a ktoré treba preniesť do cieľového systému. DCM vytvorí tieto súbory podľa vami špecifikovanej úrovne vydania cieľového systému. DCM automaticky vloží do týchto súborov kópiu certifikátu lokálnej CA.

Poznámka: DCM vytvorí nový certifikát vo svojej vlastnej pamäte certifikátov a vygeneruje dva súbory, ktoré máte preniesť: súbor pamäte certifikátov (prípona .KDB) a súbor požiadavky (prípona .RDB).

Poznámka: Ak plánujete používať certifikáty v týchto súboroch v existujúcej pamäti certifikátov *SYSTEM na cieľovom systéme V4R4 alebo V4R5, nemôžete importovať certifikát lokálnej CA priamo zo súborov .KDB a .RDB. Je to spôsobené tým, že certifikát CA nie je vo formáte, ktorý vie rozoznať a použiť funkcia importu v DCM. Namiesto toho musíte použiť hostiteľský systém na export kópie certifikátu lokálnej CA do oddeleného súboru na zabezpečenie toho, že certifikát CA bude vo formáte, ktorý bude fungovať s importovacou funkciou pre staršie vydania.

6. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
7. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali na hostiteľskom systéme a kliknite na **Pokračovať**.
8. V navigačnej časti okna vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
9. Zo zoznamu úloh vyberte **Exportovať certifikát**.
10. Ako typ certifikátu na export vyberte **Certifikačná autorita (CA)** a kliknite na **Pokračovať**, aby sa zobrazil zoznam certifikátov CA.
11. Vyberte certifikát lokálnej CA zo zoznamu certifikátov (napríklad LOCAL_CERTIFICATE_AUTHORITY). Kliknite na **Exportovať** na zobrazenie formulára, ktorý vám umožní zvoliť cieľ pre certifikát CA.
12. Vyberte **Súbor** a kliknite na **Pokračovať**.
13. Pre exportovaný súbor špecifikujte plne kvalifikovanú cestu a názov súboru a potom kliknite na **Pokračovať**. Zobrazí sa potvrdzovacia strana, ktorá oznamuje, že DCM úspešne vyexportoval súbor.

    Poznámka: Presvedčte sa, že súboru dáte jedinečný názov a rozšírenie. Napríklad, mohli by ste použiť súbor mycafile.exp. Pri pomenúvaní súboru nepoužívajte rozšírenia súborov: .TXT, .KDB, .RDB alebo .KYR. Použitie jedného z týchto typov prípon môže zapríčiniť problém, keď naimportujete súbor na cieľový systém.
14. Na prenos súborov pamätí certifikátov, ktoré ste vytvorili (.KDB a .RDB), na cieľový systém V4R4 alebo V4R5, použite binárny FTP (File Transfer Protocol), alebo inú metódu. Na prenos súboru, ktorý obsahuje exportovaný certifikát lokálnej CA, použite ASCII režim FTP.

Použiť prenesené súbory na cieľovom systéme

Po prenose súborov použite na prácu s prenesenými súbormi certifikátov na cieľovom systéme znovu DCM. Úlohy DCM, ktoré musíte vykonať závisia na úrovni vydania cieľového systému a na tom, ktoré pamäte certifikátov existujú na tomto cieľovom systéme. Úlohy, ktoré musíte

vykonať na cieľovom systéme tiež ovplyvňuje typ certifikátu, ktorý ste vytvorili. Ak sa chcete dozvedieť viac o použití DCM na cieľovom systéme na prácu s prenesenými súbormi certifikátov, pozrite si tieto témy:

- Použiť súkromný certifikát pre relácie SSL na cieľovom systéme V5R2.
- Použiť súkromný certifikát pre relácie SSL na cieľovom systéme V5R1.
- Použiť súkromný certifikát pre podpisovanie objektov na cieľovom systéme V5R2 alebo V5R1.
- Použiť súkromný certifikát pre podpisovanie objektov na cieľovom systéme V4R5 alebo V4R4.

Použiť súkromný certifikát pre relácie SSL na cieľovom systéme V5R2

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie z pamäte certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste ešte nikdy nepoužívali DCM na cieľovom systéme V5R2 na manažovanie certifikátov pre SSL, potom by táto pamäť certifikátov nemala na cieľovom systéme existovať. Úlohy pre použitie prenesených súborov pamäte certifikátov, ktorú ste vytvorili na hostiteľskom systéme lokálnej certifikačnej autority (CA), sa líšia na základe toho, či existuje pamäť certifikátov *SYSTEM. Ak pamäť certifikátov *SYSTEM neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie pamäte certifikátov *SYSTEM. Ak pamäť certifikátov *SYSTEM na cieľovom systéme V5R2 existuje, môžete prenesené súbory certifikátov použiť jedným z dvoch spôsobov:

- Použite prenesené súbory ako Pamäť certifikátov iného systému.
- Importujte prenesené súbory do existujúcej pamäte certifikátov *SYSTEM.

Pamäť certifikátov *SYSTEM neexistuje

Ak pamäť certifikátov *SYSTEM na systéme V5R2, na ktorom chcete používať prenesené súbory pamäte certifikátov, neexistuje, môžete prenesené súbory certifikátov použiť ako pamäť certifikátov *SYSTEM. Na vytvorenie pamäte certifikátov *SYSTEM a použitie súborov certifikátov na vašom cieľovom systéme V5R2 postupujte podľa týchto krokov:

1. Skontrolujte, či súbory pamäte certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) ktorú ste vytvorili na systéme, ktorý hostuje lokálnu CA, sú v adresári /QIBM/USERDATA/ICSS/CERT/SERVER.
2. Ak sú prenesené súbory certifikátu v adresári /QIBM/USERDATA/ICSS/CERT/SERVER, premenujte ich na DEFAULT.KDB a DEFAULT.RDB. Premenovaním týchto súborov v príslušnom adresári vytvoríte komponenty, ktoré tvoria pamäť certifikátov *SYSTEM pre cieľový systém. Súbory pamäte certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov pamäte certifikátov, keď ste ich vytvorili.

   Upozornenie: Ak váš cieľový systém už má súbory DEFAULT.KDB a DEFAULT.RDB v adresári /QIBM/USERDATA/ICSS/CERT/SERVER, pamäť certifikátov *SYSTEM už aktuálne existuje na tomto cieľovom systéme. Následne, prenesené súbory by ste nemali premenovať, ako bolo odporučené. Nahradením štandardných súborov vzniknú problémy pri používaní DCM, prenesenej pamäte certifikátov a jej obsahu. Namiesto toho by ste sa mali presvedčiť, že majú jedinečné názvy a prenesenú pamäť certifikátov by ste mali použiť ako **Inú systémovú pamäť certifikátov**. Ak použijete tieto súbory ako Inú systémovú pamäť certifikátov, na špecifikovanie aplikácií, ktoré by mali používať daný certifikát nemôžete použiť DCM.

3. Spustite DCM. Teraz musíte zmeniť heslo pre pamäť certifikátov *SYSTEM, ktorú ste vytvorili premenovaním prenesených súborov. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na pamäti certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
5. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre pamäť certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R2 a kliknite na **Pokračovať**.
6. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov. Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi. Ďalej môžete špecifikovať, ktoré aplikácie používajú certifikát pre SSL relácie.
7. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
8. Keď sa zobrazí stránka Pamäť certifikátu a heslo, zadajte nové heslo a kliknite na **Pokračovať**.
9. Po tom, čo sa navigačný rámec obnoví, zvoľte v ňom **Manažovať certifikáty** na zobrazenie zoznamu úloh.
10. Zo zoznamu úloh vyberte **Priradiť certifikát** na zobrazenie zoznamu certifikátov v aktuálnej pamäti certifikátov.
11. Vyberte certifikát, ktorý ste vytvorili na *hostiteľskom* systéme a kliknite na **Priradiť aplikácii** na zobrazenie zoznamu aplikácií, podporujúcich SSL, ku ktorým môžete priradiť certifikát.
12. Vyberte aplikáciu, ktorá by mala používať certifikát pre relácie SSL a kliknite na **Pokračovať**. DCM zobrazí správu na potvrdenie vášho výberu certifikátu pre aplikácie.

    Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Aplikácia s touto podporou musí byť schopná autentifikovať certifikáty predtým, ako poskytne prístup na prostriedky. Následne, pre aplikáciu musíte zadefinovať zoznam dôveryhodných CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Dokončením týchto úloh budú môcť aplikácie na cieľovom systéme používať certifikát, vydaný lokálnou CA na inom iSeries. Avšak pred tým, ako budete môcť začať používať SSL pre tieto aplikácie, musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým, ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát lokálnej CA musí byť skopírovaný do súboru na užívateľovom PC, alebo stiahnutý do prehliadača užívateľa, v závislosti na požiadavkách aplikácie s podporou SSL.

Pamäť certifikátov *SYSTEM existuje — súbory sa použijú ako Pamäť certifikátov iného systému

Ak cieľový systém V5R2 už má pamäť certifikátov *SYSTEM, musíte rozhodnúť, ako sa má pracovať so súbormi certifikátov. Môžete vybrať, aby sa prenesené súbory certifikátov použili ako **Iná systémová pamäť certifikátov**. Alebo môžete zvoliť importovať súkromný certifikát a jeho zodpovedajúci certifikát lokálnej CA do existujúcej pamäte certifikátov *SYSTEM.

Iné systémové pamäte certifikátov sú užívateľom definované sekundárne pamäte certifikátov pre SSL certifikáty. Môžete ich vytvoriť a používať na poskytovanie certifikátov pre

užívateľom napísané aplikácie s podporou SSL, ktoré nepoužívajú API DCM na registrovanie ID aplikácie s doplnkom DCM. Voľba Iná systémová pamäť certifikátov vám umožňuje manažovať certifikáty pre aplikácie, ktoré napíšete vy alebo iní, ktoré používajú SSL_Init API na programovateľný prístup a použitie certifikátu na vytvorenie SSL relácie. Toto API umožňuje aplikácii použiť štandardný certifikát pre pamäť certifikátov namiesto certifikátu, ktorý konkrétne identifikujete.

Aplikácie IBM iSeries (a mnohé ďalšie aplikácie vývojárov softvéru) sú naprogramované iba na použitie certifikátov v pamäti certifikátov *SYSTEM. Ak vyberiete používanie prenesených súborov ako Iná systémová pamäť certifikátov, na špecifikovanie aplikácií, ktoré by mali používať tento certifikát pre SSL relácie nemôžete použiť DCM. Následne teda nemôžete konfigurovať štandardné aplikácie iSeries s podporou SSL na používanie tohto certifikátu. Ak chcete certifikát používať pre aplikácie iSeries, musíte certifikát importovať z vašich prenesených súborov pamäte certifikátov do pamäte certifikátov *SYSTEM.

Ak chcete pristúpiť na prenesené súbory certifikátov a pracovať s nimi ako s Inou systémovou pamäťou certifikátov, vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre pamäť certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R2 a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi. Ďalej môžete špecifikovať, že certifikát v tejto pamäti sa použije ako štandardný certifikát.
5. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
6. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov, uveďte nové heslo a kliknite na **Pokračovať**.
7. Po tom, čo sa navigačný rámec obnoví, zvoľte **Manažovať pamäť certifikátov** a vyberte **Nastaviť predvolený certifikát** zo zoznamu úloh.

Teraz, keď ste vytvorili a nakonfigurovali Inú systémovú pamäť certifikátov, všetky aplikácie, ktoré používajú SSL_Init API môžu použiť certifikát z tejto pamäte na vytvorenie SSL relácií.

Pamäť certifikátov *SYSTEM existuje — použijú sa certifikáty v existujúcej pamäti certifikátov *SYSTEM

Môžete používať certifikáty v prenesených súboroch pamäte certifikátov v existujúcej pamäti certifikátov *SYSTEM na systéme V5R2. Ak tak chcete urobiť, musíte naimportovať certifikáty zo súborov pamäte certifikátov do existujúcej pamäte certifikátov *SYSTEM. Avšak nemôžete importovať certifikáty priamo zo súborov .KDB a .RDB, lebo nie sú vo formáte, ktorý vie importovacia funkcia DCM rozpoznať a použiť. Na použitie prenesených certifikátov v existujúcej pamäti certifikátov *SYSTEM musíte súbory otvoriť ako Pamäť certifikátov iného systému a exportovať ich do pamäte certifikátov *SYSTEM.

Na exportovanie certifikátov zo súborov pamäte certifikátov do pamäte certifikátov *SYSTEM vykonajte na cieľovom systéme V5R2 tieto kroky:

1. Spustite DCM.
2. V navigačnom rámci kliknite na **Vybrať pamäť certifikátov** a ako pamäť certifikátov, ktorá sa má otvoriť, zadajte **Pamäť certifikátov iného systému**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre pamäť certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R2 a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatické prihlasovanie, môžete naraziť na chyby pri exportovaní certifikátov z tejto pamäte do pamäte certifikátov *SYSTEM.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli pracovať s jej certifikátmi.
5. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
6. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov, uveďte nové heslo a kliknite na **Pokračovať**.
7. Po zaktualizovaní obsahu navigačného okna v ňom vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh a vyberte **Exportovať certifikát**.
8. Ako typ certifikátu na export vyberte **Certifikačná autorita (CA)** a kliknite na **Pokračovať**.

   Poznámka: Pred tým, ako budete exportovať serverovský alebo klientsky certifikát do pamäte certifikátov, by ste mali do pamäte certifikátov vyexportovať certifikát lokálnej CA. Ak exportujete najprv serverovský alebo klientsky certifikát, môžete naraziť na chybu, lebo v pamäti certifikátov neexistuje certifikát lokálnej CA.
9. Vyberte na export certifikát miestnej CA a kliknite na **Exportovať**.
10. Ako cieľ pre exportovaný certifikát vyberte **Pamäť certifikátov** a kliknite na **Pokračovať**.
11. Ako cieľovú pamäť certifikátov zadajte *SYSTEM, zadajte heslo pre pamäť certifikátov *SYSTEM a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá uvádza, že bol certifikát exportovaný úspešne, alebo poskytne informácie o chybe, ak proces exportu zlyhal.
12. Teraz môžete do pamäte certifikátov *SYSTEM exportovať serverovský alebo klientsky certifikát. Znova vyberte úlohu **Exportovať certifikát**.
13. Ako typ certifikátu na export vyberte **Serverovský alebo klientsky** a kliknite na **Pokračovať**.
14. Vyberte príslušný serverovský alebo klientsky certifikát na export a kliknite na **Exportovať**.
15. Ako cieľ pre exportovaný certifikát vyberte **Pamäť certifikátov** a kliknite na **Pokračovať**.
16. Ako cieľovú pamäť certifikátov zadajte *SYSTEM, zadajte heslo pre pamäť certifikátov *SYSTEM a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá uvádza, že bol certifikát exportovaný úspešne, alebo poskytne informácie o chybe, ak proces exportu zlyhal.
17. Teraz môžete certifikát priradiť aplikácii na použitie pre SSL. V navigačnom rámci kliknite na **Vybrať pamäť certifikátov** a ako pamäť certifikátov, ktorá sa má otvoriť, zadajte ***SYSTEM**.
18. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo pre pamäť certifikátov *SYSTEM a kliknite na **Pokračovať**.

19. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
20. Zo zoznamu úloh vyberte **Priradiť certifikát** na zobrazenie zoznamu certifikátov v aktuálnej pamäti certifikátov.
21. Vyberte certifikát, ktorý ste vytvorili na *hostiteľskom* systéme a kliknite na **Priradiť aplikácii** na zobrazenie zoznamu aplikácií, podporujúcich SSL, ku ktorým môžete priradiť certifikát.
22. Vyberte aplikáciu, ktorá by mala používať certifikát pre relácie SSL a kliknite na **Pokračovať**. DCM zobrazí správu na potvrdenie vášho výberu certifikátu pre aplikácie.

    Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Aplikácia s touto podporou musí byť schopná autentifikovať certifikáty predtým, ako poskytne prístup na prostriedky. Následne, pre aplikáciu musíte zadefinovať zoznam dôveryhodných CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Dokončením týchto úloh budú môcť aplikácie na cieľovom systéme používať certifikát, vydaný lokálnou CA na inom iSeries. Avšak pred tým, ako budete môcť začať používať SSL pre tieto aplikácie, musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým, ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát lokálnej CA musí byť skopírovaný do súboru na užívateľovom PC, alebo stiahnutý do prehliadača užívateľa, v závislosti na požiadavkách aplikácie s podporou SSL.

Použiť súkromný certifikát pre relácie SSL na cieľovom systéme V5R1

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie z pamäte certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste na manažovanie certifikátov pre SSL na cieľovom systéme V5R1 ešte nikdy nepoužívali DCM, na tomto systéme by nemala existovať ani pamäť certifikátov. Úlohy pre použitie prenesených súborov pamäte certifikátov, ktorú ste vytvorili na hostiteľskom systéme lokálnej certifikačnej autority (CA), sa líšia na základe toho, či existuje pamäť certifikátov *SYSTEM. Ak pamäť certifikátov *SYSTEM neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie pamäte certifikátov *SYSTEM. Ak pamäť certifikátov *SYSTEM na cieľovom systéme V5R1 existuje, môžete prenesené súbory certifikátov použiť jedným z dvoch spôsobov:

- Použite prenesené súbory ako Pamäť certifikátov iného systému.
- Importujte prenesené súbory do existujúcej pamäte certifikátov *SYSTEM.

Pamäť certifikátov *SYSTEM neexistuje

Ak pamäť certifikátov *SYSTEM neexistuje na systéme V5R1, na ktorom chcete používať prenesenú súbory pamäte certifikátov, ako pamäť certifikátov *SYSTEM môžete použiť prenesené súbory certifikátov. Na použitie súborov certifikátov na vašom cieľovom systéme V5R1 postupujte podľa týchto krokov:

1. Skontrolujte, či súbory pamäte certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) ktorú ste vytvorili na systéme, ktorý hosťuje lokálnu CA, sú v adresári /QIBM/USERDATA/ICSS/CERT/SERVER.
2. Ak sú prenesené súbory certifikátu v adresári /QIBM/USERDATA/ICSS/CERT/SERVER, premenujte ich na DEFAULT.KDB a DEFAULT.RDB. Premenovaním týchto súborov v príslušnom adresári vytvoríte

komponenty, ktoré tvoria pamäť certifikátov *SYSTEM pre cieľový systém. Súbor pamäte certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov pamäte certifikátov, keď ste ich vytvorili.

Upozornenie: Ak váš cieľový systém už má súbory DEFAULT.KDB a DEFAULT.RDB v adresári /QIBM/USERDATA/ICSS/CERT/SERVER, pamäť certifikátov *SYSTEM už aktuálne existuje na tomto cieľovom systéme. Následne, prenesené súbory by ste nemali premenovať, ako bolo odporučené. Nahradením štandardných súborov vzniknú problémy pri používaní DCM, prenesenej pamäte certifikátov a jej obsahu. Namiesto toho by ste sa mali presvedčiť, že majú jedinečné názvy a prenesenú pamäť certifikátov by ste mali použiť ako **Inú systémovú pamäť certifikátov**. Ak použijete tieto súbory ako Inú systémovú pamäť certifikátov, na špecifikovanie aplikácií, ktoré by mali používať daný certifikát nemôžete použiť DCM.

3. Spustite DCM. Teraz musíte zmeniť heslo pre pamäť certifikátov *SYSTEM, ktorú ste vytvorili premenovaním prenesených súborov. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na pamäti certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
5. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre pamäť certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R1 a kliknite na **Pokračovať**.
6. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov. Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi. Ďalej môžete špecifikovať, ktoré aplikácie používajú certifikát pre SSL relácie.
7. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SYSTEM**.
8. Keď sa zobrazí stránka Pamäť certifikátu a heslo, zadajte nové heslo a kliknite na **Pokračovať**.
9. Po tom, čo sa navigačný rámec obnoví, zvoľte v ňom **Manažovať aplikácie** na zobrazenie zoznamu úloh.
10. Zo zoznamu úloh vyberte **Zaktualizovať priradenie certifikátu**, aby sa zobrazil zoznam aplikácií s podporou SSL, ktorým chcete priradiť certifikát.
11. Vyberte niektorú aplikáciu zo zoznamu a kliknite na **Zaktualizovať priradenie certifikátu**.
12. Vyberte certifikát, ktorý vydala lokálna CA na *hostiteľskom* systéme a kliknite na **Priradiť nový certifikát**. DCM zobrazí správu, ktorou potvrdí váš výber certifikátu pre aplikáciu.

Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Aplikácia s touto podporou musí byť schopná autentifikovať certifikáty predtým, ako poskytne prístup na prostriedky. Následne, pre aplikáciu musíte zadefinovať zoznam dôveryhodných CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Dokončením týchto úloh budú môcť aplikácie na cieľovom systéme používať certifikát, vydaný lokálnou CA na inom iSeries. Avšak pred tým, ako budete môcť začať používať SSL pre tieto aplikácie, musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým, ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát CA sa musí skopírovať do súboru na PC užívateľa alebo stiahnuť do prehliadača užívateľa, podľa požiadaviek aplikácie s podporou SSL.

Pamäť certifikátov *SYSTEM existuje — súbory sa použijú ako Pamäť certifikátov iného systému

Ak cieľový systém V5R1 už má pamäť certifikátov *SYSTEM, musíte rozhodnúť, ako sa bude pracovať so súbormi certifikátov. Môžete vybrať, aby sa prenesené súbory certifikátov použili ako **Iná systémová pamäť certifikátov**. Alebo môžete zvoliť importovať súkromný certifikát a jeho zodpovedajúci certifikát lokálnej CA do existujúcej pamäte certifikátov *SYSTEM.

Iné systémové pamäte certifikátov sú užívateľom definované sekundárne pamäte certifikátov pre SSL certifikáty. Môžete ich vytvoriť a používať na poskytovanie certifikátov pre užívateľmi napísané aplikácie s podporou SSL, ktoré na registráciu ID aplikácie s pomocným programom DCM nepoužívajú API DCM. Voľba Iná systémová pamäť certifikátov vám umožňuje manažovať certifikáty pre aplikácie, ktoré napíšete vy alebo iní, ktoré používajú SSL_Init API na programovateľný prístup a použitie certifikátu na vytvorenie SSL relácie. Toto API umožňuje aplikácii použiť štandardný certifikát pre pamäť certifikátov namiesto certifikátu, ktorý konkrétne identifikujete.

Aplikácie IBM iSeries (a mnohé ďalšie aplikácie vývojárov softvéru) sú naprogramované iba na použitie certifikátov v pamäti certifikátov *SYSTEM. Ak vyberiete používanie prenesených súborov ako Iná systémová pamäť certifikátov, na špecifikovanie aplikácií, ktoré by mali používať tento certifikát pre SSL relácie nemôžete použiť DCM. Následne teda nemôžete konfigurovať štandardné aplikácie iSeries s podporou SSL na používanie tohto certifikátu. Ak chcete certifikát používať pre aplikácie iSeries, musíte certifikát importovať z vašich prenesených súborov pamäte certifikátov do pamäte certifikátov *SYSTEM.

Ak chcete pristúpiť na prenesené súbory certifikátov a pracovať s nimi ako s Inou systémovou pamäťou certifikátov, vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre pamäť certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R1 a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi. Ďalej môžete špecifikovať, že certifikát v tejto pamäti sa použije ako štandardný certifikát.
5. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
6. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov, uveďte nové heslo a kliknite na **Pokračovať**.
7. Po tom, čo sa navigačný rámec obnoví, zvoľte **Manažovať pamäť certifikátov** a vyberte **Nastaviť predvolený certifikát** zo zoznamu úloh.

Teraz, keď ste vytvorili a nakonfigurovali Inú systémovú pamäť certifikátov, všetky aplikácie, ktoré používajú SSL_Init API môžu použiť certifikát z tejto pamäte na vytvorenie SSL relácií.

Pamäť certifikátov *SYSTEM existuje — použijú sa certifikáty v existujúcej pamäti certifikátov *SYSTEM

Certifikáty v prenesených súboroch pamäte certifikátov môžete použiť v existujúcej pamäti certifikátov *SYSTEM na systéme V5R1. Ak tak chcete urobiť, musíte naimportovať certifikáty zo súborov pamäte certifikátov do existujúcej pamäte certifikátov *SYSTEM. Avšak nemôžete importovať certifikáty priamo zo súborov .KDB a .RDB, lebo nie sú vo formáte, ktorý vie importovacia funkcia DCM rozpoznať a použiť. Na použitie prenesených certifikátov v existujúcej pamäti certifikátov *SYSTEM musíte súbory otvoriť ako Pamäť certifikátov iného systému a exportovať ich do pamäte certifikátov *SYSTEM.

Poznámka: Táto procedúra popisuje, ako použiť Pamäť certifikátov iného systému na cieľovom systéme na exportovanie certifikátov z pôvodných súborov pamäte certifikátov do pamäte certifikátov *SYSTEM. Použitie tejto metódy na pridanie certifikátov do pamäte certifikátov *SYSTEM vám môže pomôcť zabrániť možným problémom, keď cieľový systém používa slabšieho produktu poskytovateľa šifrovaného prístupu (ako je 5722–AC2), ako hostiteľský systém.

Na exportovanie certifikátov zo súborov pamäte certifikátov do pamäte certifikátov *SYSTEM vykonajte na cieľovom systéme V5R1 tieto kroky:

1. Spustite DCM.
2. V navigačnom rámci kliknite na **Vybrať pamäť certifikátov** a ako pamäť certifikátov, ktorá sa má otvoriť, zadajte **Pamäť certifikátov iného systému**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre pamäť certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R1 a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatické prihlasovanie, môžete naraziť na chyby pri exportovaní certifikátov z tejto pamäte do pamäte certifikátov *SYSTEM.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi.
5. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
6. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov, uveďte nové heslo a kliknite na **Pokračovať**.
7. Po zaktualizovaní obsahu navigačného okna v ňom vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh a vyberte **Exportovať certifikát**.
8. Ako typ certifikátu na export vyberte **Certifikačná autorita (CA)** a kliknite na **Pokračovať**.

   Poznámka: Pred tým, ako budete exportovať serverovský alebo klientsky certifikát do pamäte certifikátov, by ste mali do pamäte certifikátov vyexportovať certifikát lokálnej CA. Ak exportujete najprv serverovský alebo klientsky certifikát, môžete naraziť na chybu, lebo v pamäti certifikátov neexistuje certifikát lokálnej CA.
9. Vyberte na export certifikát miestnej CA a kliknite na **Exportovať**.

10. Ako cieľ pre exportovaný certifikát vyberte **Pamäť certifikátov** a kliknite na **Pokračovať**.
11. Ako cieľovú pamäť certifikátov zadajte *SYSTEM, zadajte heslo pre pamäť certifikátov *SYSTEM a kliknite na **Pokračovať**.
12. Teraz môžete do pamäte certifikátov *SYSTEM exportovať serverovský alebo klientsky certifikát. Znova vyberte úlohu **Exportovať certifikát**.
13. Ako typ certifikátu na export vyberte **Serverovský alebo klientsky** a kliknite na **Pokračovať**.
14. Vyberte príslušný serverovský alebo klientsky certifikát na export a kliknite na **Exportovať**.
15. Ako cieľ pre exportovaný certifikát vyberte **Pamäť certifikátov** a kliknite na **Pokračovať**.
16. Ako cieľovú pamäť certifikátov zadajte *SYSTEM, zadajte heslo pre pamäť certifikátov *SYSTEM a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá uvádza, že bol certifikát exportovaný úspešne, alebo poskytne informácie o chybe, ak proces exportu zlyhal.
17. Teraz môžete certifikát priradiť aplikácii na použitie pre SSL. V navigačnom rámci kliknite na **Vybrať pamäť certifikátov** a ako pamäť certifikátov, ktorá sa má otvoriť, zadajte ***SYSTEM**.
18. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo pre pamäť certifikátov *SYSTEM a kliknite na **Pokračovať**.
19. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
20. Zo zoznamu úloh vyberte **Zaktualizovať priradenie certifikátu**, aby sa zobrazil zoznam aplikácií s podporou SSL, ktorým chcete priradiť certifikát.
21. Vyberte niektorú aplikáciu zo zoznamu a kliknite na **Zaktualizovať priradenie certifikátu**.
22. Vyberte certifikát, ktorý vydala lokálna CA na *hostiteľskom* systéme a kliknite na **Priradiť nový certifikát**. DCM zobrazí správu, ktorou potvrdí váš výber certifikátu pre aplikáciu.

    Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Aplikácia s touto podporou musí byť schopná autentifikovať certifikáty predtým, ako poskytne prístup na prostriedky. Následne, pre aplikáciu musíte zadefinovať zoznam dôveryhodných CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Dokončením týchto úloh budú môcť aplikácie na cieľovom systéme používať certifikát, vydaný lokálnou CA na inom iSeries. Pred začatím používa SSL pre tieto aplikácie však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým, ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát CA sa musí skopírovať do súboru na PC užívateľa alebo stiahnuť do prehliadača užívateľa, podľa požiadaviek aplikácie s podporou SSL.

Použiť súkromný certifikát pre podpisovanie objektov na cieľovom systéme V5R2 alebo V5R1

Certifikáty, ktoré používate na podpisovanie objektov z pamäte certifikátov *OBJECTSIGNING manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste na manažovanie certifikátov, podpisujúcich objekty, na cieľovom systéme ešte nikdy nepoužívali DCM, na tomto systéme by nemala existovať táto pamäť certifikátov. Úlohy, ktoré musíte vykonať na použitie prenesených súborov pamäte certifikátov, ktorú ste vytvorili na

hostiteľskom systéme lokálnej (CA), sa líšia na základe toho, či existuje pamäť certifikátov *OBJECTSIGNING. Ak pamäť certifikátov *OBJECTSIGNING neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie pamäte certifikátov *OBJECTSIGNING. Ak pamäť certifikátov *OBJECTSIGNING na cieľovom systéme existuje, musíte do nej prenesené certifikáty naimportovať.

Pamäť certifikátov *OBJECTSIGNING neexistuje

Úlohy, ktoré vykonáte na použitie súborov pamäte certifikátov, ktorú ste vytvorili na hostiteľskom systéme lokálnej (CA), sa líšia na základe toho, či ste už na cieľovom systéme niekedy použili DCM na manažovanie certifikátov na podpisovanie objektov.

Ak pamäť certifikátov *OBJECTSIGNING na cieľovom systéme V5R2 alebo V5R1 s prenesenými súbormi pamäte certifikátov neexistuje, postupujte podľa týchto krokov:

1. Skontrolujte, či súbory pamäte certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) ktorú ste vytvorili na systéme, ktorý hostuje lokálnu CA, sú v adresári /QIBM/USERDATA/ICSS/CERT/SIGNING.
2. Ak sú prenesené súbory certifikátu v adresári /QIBM/USERDATA/ICSS/CERT/SIGNING, premenujte ich na SGNOBJ.KDB a SGNOBJ.RDB. ak je to potrebné Premenovaním týchto súborov vytvoríte komponenty, ktoré vytvoria pamäť certifikátov *OBJECTSIGNING pre cieľový systém. Súbor pamäte certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov pamäte certifikátov, keď ste ich vytvorili.

   Pozor: Ak váš cieľový systém už má súbory SGNOBJ.KDB a SGNOBJ.RDB v adresári /QIBM/USERDATA/ICSS/CERT/SIGNING, pamäť certifikátov *OBJECTSIGNING už aktuálne existuje na tomto cieľovom systéme. Následne, prenesené súbory by ste nemali premenovať, ako bolo odporučené. Nahradením štandardných súborov, podpisujúcich objekty, vzniknú problémy pri používaní DCM, prenesenej pamäte certifikátov a jej obsahu. Certifikáty z týchto súborov môžete dostať do existujúcej pamäte certifikátov *OBJECTSIGNING jedným z dvoch spôsobov. Certifikáty v tomto súbore môžete vyexportovať do množiny súborov, z ktorých môžete naimportovať tieto certifikáty do existujúcej pamäte certifikátov *OBJECTSIGNING. Alebo, prenesené súbory môžete otvoriť ako Inú systémovú pamäť certifikátov a certifikáty vyexportovať priamo do pamäte certifikátov *OBJECTSIGNING, ako je popísané neskôr v tomto materiáli. V oboch prípadoch, musíte dostať certifikáty do pamäte certifikátov *OBJECTSIGNING, ak chcete manažovať aplikácie, ktoré ich používajú, ako to opisuje táto procedúra.
3. Spustite DCM. Musíte zmeniť heslo pre pamäť certifikátov *OBJECTSIGNING. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na pamäti certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***OBJECTSIGNING**.
5. Keď sa zobrazí strana na zadanie hesla, zadajte heslo, ktoré ste špecifikovali pre pamäť certifikátov pri jej vytváraní na hostiteľskom systéme a kliknite na **Pokračovať**.
6. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov. Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi. Ďalej môžete vytvoriť definíciu aplikácie na používanie certifikátu na podpisovanie objektov.
7. Po opätovnom otvorení pamäte certifikátov vyberte v navigačnej časti okna **Manažovať aplikácie**, aby sa zobrazil zoznam úloh.

8. Zo zoznamu úloh vyberte **Pridať aplikáciu**, aby sa spustil proces vytvorenia definície aplikácie, podpisujúcej objekty, na použitie s certifikátom na podpisovanie objektov.
9. Vyplnením formulára zadefinujte aplikáciu na podpisovanie objektov a kliknite na **Pridať**. Táto definícia aplikácie nepopisuje skutočnú aplikáciu, ale popisuje typ objektov, ktoré chcete podpisovať konkrétnym certifikátom. Pri vypĺňaní formuláru môžete použiť online pomoc.
10. Kliknite na **OK**, aby sa potvrdila správa o vytvorení definície a zobrazte si zoznam úloh **Manažovať aplikácie**.
11. Zo zoznamu úloh vyberte **Aktualizovať priradenie certifikátu** na zobrazenie zoznamu ID aplikácií podpisujúcich objekty, pre ktoré môžete priradiť certifikát.
12. Zo zoznamu ID aplikácií vyberte svoju aplikáciu a kliknite na **Zaktualizovať priradenie certifikátu**.
13. Vyberte certifikát, ktorý vytvorila lokálna CA na hostiteľskom systéme a kliknite na **Priradiť nový certifikát**.

Po dokončení týchto úloh máte všetko potrebné na začatie podpisovania objektov na zaručenie ich integrity.

Keď distribuujete podpísané objekty, tí, ktorí prijímajú objekty, musia použiť verzie DCM V5R2 alebo V5R1 na overenie podpisu na objektoch na zabezpečenie, že sú údaje nezmenené a na overenie identity odosielateľa. Aby sa validoval podpis, prijímateľ musí mať kópiu certifikát na kontrolu podpisu. Tento certifikát by ste mali poskytnúť ako časť balíka podpísaných objektov.

Prijímateľ tiež musí mať kópiu certifikátu CA pre CA, ktorý vydala certifikát, ktorý ste použili na podpísanie objektu. Ak ste podpísali objekty s certifikátom od dobre známej internetovej CA, prijímateľova verzia DCM by už mala mať kópiu potrebného certifikátu CA. Ak to je však potrebné, spolu s podpísanými objektmi by ste mali v samostatnom balíku poskytnúť kópiu certifikátu CA. Napríklad by ste mali poskytnúť kópiu certifikátu lokálnej CA, ak ste podpísali objekty certifikátom z lokálnej CA. Z bezpečnostných dôvodov by ste mali poskytnúť certifikát CA v samostatnom balíku alebo na požiadanie adresátov by ste mali tento certifikát CA spraviť verejne dostupným.

Pamäť certifikátov *OBJECTSIGNING existuje

Môžete používať certifikáty v prenesených súboroch pamäte certifikátov v existujúcej pamäti certifikátov *OBJECTSIGNING na systéme V5R2 alebo V5R1. Ak tak chcete urobiť, musíte naimportovať certifikáty zo súborov pamäte certifikátov do existujúcej pamäte certifikátov *OBJECTSIGNING. Avšak nemôžete importovať certifikáty priamo zo súborov .KDB a .RDB, lebo nie sú vo formáte, ktorý vie importovacia funkcia DCM rozpoznať a použiť. Certifikáty môžete do existujúcej pamäte certifikátov *OBJECTSIGNING pridať otvorením prenesených súborov ako Pamäť certifikátov iného systému na cieľovom systéme V5R2 alebo V5R1. Potom môžete vyexportovať tieto certifikáty priamo do pamäte certifikátov *OBJECTSIGNING. Musíte exportovať kópiu samotného certifikát na podpisovanie objektov aj certifikátu lokálnej CA z prenesených súborov.

Na exportovanie certifikátov zo súborov pamäte certifikátov priamo do pamäte certifikátov *OBJECTSIGNING vykonajte na cieľovom systéme V5R2 alebo V5R1 tieto kroky:
1. Spustite DCM.
2. V navigačnom rámci kliknite na **Vybrať pamäť certifikátov** a ako pamäť certifikátov, ktorá sa má otvoriť, zadajte **Pamäť certifikátov iného systému**.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súborov pamäte certifikátov. Taktiež uveďte heslo, ktoré ste použili, keď ste ich vytvárali na hostiteľskom systéme a kliknite na **Pokračovať**.

4. V navigačnej časti okna vyberte **Manažovať pamäť certifikátov** a zo zoznamu úloh vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatické prihlasovanie, môžete naraziť na chyby pri exportovaní certifikátov z tejto pamäte do pamäte certifikátov *OBJECTSIGNING.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi.
5. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte **Iná systémová pamäť certifikátov**.
6. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte úplnú cestu a názov súboru pamäte certifikátov, uveďte nové heslo a kliknite na **Pokračovať**.
7. Po zaktualizovaní obsahu navigačného okna v ňom vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh a vyberte **Exportovať certifikát**.
8. Ako typ certifikátu na export vyberte **Certifikačná autorita (CA)** a kliknite na **Pokračovať**.

   Poznámka: Štylizácia pre túto úlohu predpokladá, že keď pracujete s Pamäťou certifikátov iného systému, pracujete s certifikátmi servera alebo klienta. To je preto, lebo tento typ pamäte certifikátov je určený na použitie ako sekundárna pamäť certifikátov k pamäti certifikátov *SYSTEM. Avšak použitie exportovacej úlohy v tejto pamäti certifikátov je najjednoduchším spôsobom pridávania certifikátov z prenesených súborov do existujúcej pamäte certifikátov *OBJECTSIGNING.
9. Vyberte na export certifikát miestnej CA a kliknite na **Exportovať**.

   Poznámka: Pred tým, ako budete exportovať certifikát na podpisovanie objektov do pamäte certifikátov, by ste mali do pamäte certifikátov vyexportovať certifikát lokálnej CA. Ak exportujete najprv certifikát na podpisovanie objektov, môžete naraziť na chybu, lebo v pamäti certifikátov neexistuje certifikát lokálnej CA.
10. Ako cieľ pre exportovaný certifikát vyberte **Pamäť certifikátov** a kliknite na **Pokračovať**.
11. Ako cieľovú pamäť certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre pamäť certifikátov a kliknite na **Pokračovať**.
12. Teraz môžete vyexportovať certifikát, podpisujúci objekty, do pamäte certifikátov *OBJECTSIGNING. Znova vyberte úlohu **Exportovať certifikát**.
13. Ako typ certifikátu na export vyberte **Serverovský alebo klientsky** a kliknite na **Pokračovať**.
14. Vyberte príslušný certifikát na export a kliknite na **Exportovať**.
15. Ako cieľ pre exportovaný certifikát vyberte **Pamäť certifikátov** a kliknite na **Pokračovať**.
16. Ako cieľovú pamäť certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre pamäť certifikátov *OBJECTSIGNING a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá uvádza, že bol certifikát exportovaný úspešne, alebo poskytne informácie o chybe, ak proces exportu zlyhal.

    Poznámka: Na použitie tohto certifikátu na podpisovanie objektov musíte teraz priradiť certifikát aplikácii na podpisovanie objektov.

Použiť súkromný certifikát pre relácie SSL na cieľovom systéme V4R5 alebo V4R4

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie z pamäte certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste ešte nikdy nepoužívali DCM na cieľovom systéme V4R5 alebo V4R4 na manažovanie certifikátov pre SSL, potom by táto pamäť certifikátov nemala na cieľovom systéme existovať. Prenesené súbory pamäte certifikátov, ktorú ste vytvorili na hostiteľskom systéme lokálnej CA, obsahuje dva certifikáty. Tieto súbory sú serverovský alebo klientsky certifikát, ktorý ste vytvorili a certifikát súkromnej lokálnej CA, ktorý ste použili na jeho podpísanie.

Úlohy, ktoré musíte vykonať na použitie prenesených súborov pamäte certifikátov, sa líšia na základe toho, či existuje pamäť certifikátov *SYSTEM. Ak pamäť certifikátov *SYSTEM neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie pamäte certifikátov *SYSTEM. Ak pamäť certifikátov *SYSTEM na cieľovom systéme V5R1 existuje, môžete prenesené súbory certifikátov použiť jedným z dvoch spôsobov:

- Použiť prenesené súbory ako Pamäť certifikátov iného systému.
- Importovať prenesené súbory do existujúcej pamäte certifikátov *SYSTEM.

Pamäť certifikátov *SYSTEM neexistuje

Ak pamäť certifikátov *SYSTEM na systéme V4R5 alebo V4R4, na ktorom chcete používať prenesené súbory pamäte certifikátov, neexistuje, postupujte podľa týchto krokov:

1. Skontrolujte, či súbory pamäte certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) ktorú ste vytvorili na systéme, ktorý hosťuje lokálnu CA, sú v adresári /QIBM/USERDATA/ICSS/CERT/SERVER.
2. Ak sú prenesené súbory certifikátu v adresári /QIBM/USERDATA/ICSS/CERT/SERVER, premenujte ich na DEFAULT.KDB a DEFAULT.RDB. Premenovaním týchto súborov v príslušnom adresári vytvoríte komponenty, ktoré tvoria pamäť certifikátov *SYSTEM pre cieľový systém. Súbor pamäte certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov pamäte certifikátov, keď ste ich vytvorili.

   Upozornenie: Ak váš cieľový systém už má súbory DEFAULT.KDB a DEFAULT.RDB v adresári /QIBM/USERDATA/ICSS/CERT/SERVER, pamäť certifikátov *SYSTEM už aktuálne existuje na tomto cieľovom systéme. Následne, prenesené súbory by ste nemali premenovať, ako bolo odporučené. Nahradením štandardných súborov vzniknú problémy pri používaní DCM, prenesenej pamäte certifikátov a jej obsahu. Namiesto toho by ste sa mali presvedčiť, že majú jedinečné názvy a prenesené súbory pamäte certifikátov používate ako **Inú** pamäť certifikátov. Ak súbory používate ako Pamäť certifikátov iného systému, nemôžete použiť DCM na určenie, ktoré aplikácie by mali certifikát používať.
3. Spustite DCM. Musíte zmeniť heslo pre pamäť certifikátov *SYSTEM. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na pamäti certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnom okne skontrolujte, či je *SYSTEM zobrazená ako pamäť certifikátov v roletovom zozname a vyberte **Systémové certifikáty** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Pamäť certifikátov a heslo**.
5. Do príslušných polí pre pamäť certifikátov na otvorenie zadajte *SYSTEM a heslo, ktoré ste použili, keď ste vytvárali súbory použitím lokálnej CA Na hostiteľskom systéme. Teraz môžete zmeniť heslo pre pamäť certifikátov.
6. Zo zoznamu úloh v navigačnej časti okna vyberte **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov. Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi.

7. Po opätovnom otvorení pamäte certifikátov *SYSTEM vyberte zo zoznamu úloh **Pracovať s bezpečnými aplikáciami**, aby sa zobrazila strana, ktorá vám umožňuje manažovať certifikáty, spojené s konkrétnymi aplikáciami.
8. Zo zoznamu aplikácií vyberte aplikáciu, ktorá by mala používať prenesený súkromný certifikát pre SSL relácie.
9. Kliknite na **Pracovať so systémovým certifikátom** a vyberte certifikát, ktorý vydala lokálna CA na hostiteľskom systéme.
10. Kliknite na **Priradiť nový certifikát**, aby špecifikovaná aplikácia začala používať vybratý certifikát.

Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Použitie certifikátov na autentifikáciu klientov zaisťuje, že aplikácia pred umožnením prístupu na ňou riadené prostriedky prijme platný certifikát. Aplikácia s touto podporou sa musí nastaviť tak, aby verila CA, aby mohla autentifikovať certifikáty, ktoré vydá konkrétna CA. Použite stránku **Pracovať s certifikačnými autoritami** na zabezpečenie, že certifikát CA má v pamäti certifikátov stav dôveryhodný. Potom použite stránku **Pracovať s bezpečnými aplikáciami** na zabezpečenie, že aplikácie, ktoré certifikát používajú, dôverujú lokálnej CA, ktorá ho vydala. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Dokončením týchto úloh budú môcť aplikácie na cieľovom systéme V4R5 alebo V4R4 používať certifikát, vydaný lokálnou CA V5R2 na inom iSeries. Pred začatím používa SSL pre tieto aplikácie však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým, ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát CA sa musí skopírovať do súboru na PC užívateľa alebo stiahnuť do prehliadača užívateľa, podľa požiadaviek aplikácie s podporou SSL.

Pamäť certifikátov *SYSTEM existuje — súbory sa použijú ako Pamäť certifikátov iného systému

Ak cieľový systém V4R5 alebo V4R4 už má pamäť certifikátov *SYSTEM, musíte rozhodnúť, ako sa má pracovať so súbormi certifikátov. Prenesené súbory pamäte certifikátov obsahujú dva certifikáty: serverovský alebo klientsky certifikát, ktorý ste vytvorili a certifikát súkromnej lokálnej CA, ktorý ste použili na jeho podpísanie. Môžete vybrať, aby sa prenesené súbory certifikátov používali ako **Iná** systémová pamäť certifikátov. Alebo môžete zvoliť importovať súkromný certifikát a jeho zodpovedajúci certifikát CA do existujúcej pamäte certifikátov *SYSTEM.

Ak vyberiete používanie prenesených súborov ako **Iná** systémová pamäť certifikátov, na špecifikovanie aplikácií, ktoré by mali používať tento certifikát pre SSL relácie nemôžete použiť DCM. Môžete však určiť certifikát v tejto pamäti certifikátov ako štandardný certifikát pre pamäť certifikátov. Voľba Iná systémová pamäť certifikátov vám umožňuje manažovať certifikáty pre aplikácie, ktoré napíšete vy alebo iní, ktoré používajú SSL_Init API na programovateľný prístup a použitie certifikátu na vytvorenie SSL relácie. Toto API umožňuje aplikácii použiť štandardný certifikát pre pamäť certifikátov namiesto nejakého konkrétneho certifikátu.

Ak pamäť certifikátov *SYSTEM na systéme V4R5 alebo V4R4, na ktorom chcete používať prenesené súbory pamäte certifikátov, existuje, postupujte podľa týchto krokov:

1. Spustite DCM. Musíte zmeniť heslo pre pamäť certifikátov *OBJECTSIGNING. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na pamäti certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
2. V navigačnom okne skontrolujte, či je ako pamäť certifikátov v roletovom zozname zobrazené OTHER a vyberte **Systémové certifikáty** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Pamäť certifikátov a heslo**.
3. Do príslušných polí zadajte úplnú cestu a názov súboru pre pamäť certifikátov (prípona .KDB), ktorý ste preniesli z hostiteľského systému lokálnej CA. Zadajte heslo, ktoré ste použili, keď ste vytvárali súbory na *hostiteľskom* systéme. Teraz môžete zmeniť heslo pre pamäť certifikátov.
4. V navigačnej časti okna vyberte zo zoznamu úloh pre systémové certifikáty **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi. Ďalej môžete špecifikovať, že certifikát v tejto pamäti sa použije ako štandardný certifikát.
5. V navigačnej časti okna vyberte **Pracovať s certifikátmi**, aby sa zobrazila strana, ktorá vám umožňuje vykonať množstvo úloha manažmentu certifikátov.
6. Zo zoznamu certifikátov vyberte certifikát, ktorý chcete používať ako štandardný certifikát pre aktuálnu pamäť a kliknite na **Nastaviť ako štandard**.

teraz, keď ste vytvorili a nakonfigurovali Pamäť certifikátov iného systému, môže akákoľvek aplikácia, ktorá používa API SSL_Init, používať certifikát v nej na vytvorenie relácií SSL.

Pamäť certifikátov *SYSTEM existuje — importujú sa súbory do existujúcej pamäti certifikátov *SYSTEM

Predtým, ako budete môcť importovať certifikáty do *SYSTEM na cieľovom systéme V4R5 or V4R4, musíte najprv exportovať certifikáty z pamäte certifikátov, ktorú ste vytvorili do iného formátu súboru. Potom môžete naimportovať certifikáty do pamäte certifikátov *SYSTEM z nových súborov. Prenesené súbory pamäte certifikátov obsahujú dva certifikáty: serverovský alebo klientsky certifikát, ktorý ste vytvorili a certifikát súkromnej lokálnej CA, ktorý ste použili na jeho podpísanie. Do pamäte certifikátov *SYSTEM musíte naimportovať certifikát servera aj klienta, ktoré ste vytvorili, ako aj certifikát miestnej súkromnej CA.

Poznámka: Exportovacie funkcie, dostupné v DCM pre V4R5 a V4R4, nie sú tak dobre vyvinuté, ako tie pre V5R2 a môžete zaznamenať problémy, ak použijete cieľový systém na export certifikátu súkromnej lokálnej CA. Z tohto dôvodu by ste na export *ďalšej* kópie certifikátu lokálnej CA do oddeleného súboru mali radšej použiť hostiteľský systém V5R2, ako cieľový systém V4R4 alebo V4R5. Potom, ako vyexportujete certifikát lokálnej CA na hostiteľskom systéme V5R2, môžete exportový súbor certifikátu lokálnej CA manuálne preniesť do cieľového systému V4R4 alebo V4R5 a pokračovať krokmi, poskytnutými ďalej v tejto procedúre, na importovanie certifikátu lokálnej CA do pamäte certifikátov *SYSTEM. Certifikát miestnej CA musíte naimportovať *predtým*, ako naimportujete certifikát, ktorý ste s ním vytvorili. Ak importujete najprv súkromný certifikát, môžete naraziť na chybu, lebo v pamäti certifikátov neexistuje certifikát lokálnej CA.

Ak chcete vyexportovať certifikát zo súborov pamäte certifikátov, na cieľovom systéme V4R4 alebo V4R5 vykonajte tieto kroky:
1. Spustite DCM.

2. V navigačnom okne skontrolujte, či je ako pamäť certifikátov v roletovom zozname zobrazené OTHER a vyberte **Systémové certifikáty** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Pamäť certifikátov a heslo**.
3. Zadajte úplnú cestu a názov súboru prenesených súborov pamäte certifikátov, uveďte heslo, ktoré ste použili, keď ste ich vytvorili na *hostiteľskom* systéme a kliknite na **OK**. Teraz môžete zmeniť heslo pre pamäť certifikátov.
4. V navigačnom rámci vyberte zo zoznamu úloh systémových certifikátov **Zmeniť heslo**. Vyplňte formulár na zmenu hesla pre pamäť certifikátov.

   Poznámka: Uistite sa, že ste označili voľbu **Automatické prihlasovanie**, keď meníte heslo pre pamäť certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novej pamäti môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatické prihlasovanie, môžete naraziť na chyby pri exportovaní certifikátov z tejto pamäte.

   Po zmene hesla musíte nanovo otvoriť pamäť certifikátov, aby ste mohli spracovať s jej certifikátmi.
5. V navigačnej časti okna vyberte **Pracovať s certifikátmi**, aby sa zobrazil zoznam certifikátov.
6. Zo zoznamu vyberte požadovaný súkromný certifikát a kliknite na **Exportovať**, aby sa zobrazila strana Export certifikátu.
7. Vyplňte formulár Exportovať certifikát.

   Poznámka: Presvedčte sa, že súboru dáte jedinečný názov a príponu. Napríklad, mohli by ste použiť súbor myfile.exp. Keď pomenovávate súbor, nepoužívajte pre súbor jednu z týchto prípon: .TXT, .KDB, .RDB, alebo .KYR, pretože použitie jednej z týchto prípon môže spôsobiť chybu, keď importujete certifikát zo súboru. Vyberte vhodnú úroveň vydania pre cieľový systém, ktorý bude používať tento certifikát. Úroveň vydania, ktorú zvolíte, má vplyv na formát exportovaných certifikátov.
8. Kliknite na **OK**. Navrchu strany sa zobrazí správa, že DCM vyexportoval certifikát do vami špecifikovaného súboru.

V tomto bode by ste na export ďalšej kópie certifikátu lokálnej CA mali radšej použiť DCM na pôvodnom hostiteľskom systéme V5R2 a manuálne ich preniesť na cieľový systém V4R4 alebo V5R5. Tiež by ste mali použiť DCM na tomto cieľovom systéme na export súkromného serverovského alebo klientskeho certifikátu do súboru. Teraz ste pripravený na import týchto certifikátov do pamäte certifikátov *SYSTEM. Certifikát miestnej CA musíte naimportovať *predtým*, ako naimportujete certifikát, ktorý ste s ním vytvorili. Ak importujete najprv súkromný certifikát, môžete naraziť na chybu, lebo v pamäti certifikátov neexistuje certifikát lokálnej CA.

Ak chcete naimportovať certifikáty z týchto exportovaných súborov a špecifikovať, že ich používajú aplikácie s podporou SSL, na cieľovom systéme V4R4 alebo V4R5 vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnom okne skontrolujte, či je *SYSTEM zobrazená ako pamäť certifikátov v roletovom zozname a vyberte **Systémové certifikáty** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Pamäť certifikátov a heslo**.
3. Ako pamäť certifikátov na otvorenie špecifikujte *SYSTEM, zadajte heslo a kliknite na **Pokračovať**.
4. teraz musíte importovať certifikát lokálnej CA z exportovaného súboru, ktorý ste vytvorili na hostiteľskom systéme V5R2. V navigačnej časti okna vyberte **Prijať certifikát CA**, aby sa zobrazil formulár.

5. Vyplňte formulár a kliknite na **OK**, aby sa zobrazila strana Prijatie certifikátu bolo úspešné. Keď pracujete v pamäti certifikátov *SYSTEM, táto strana zobrazí zoznam aplikácií, ktoré môžete nastaviť tak, aby dôverovali naimportovanému certifikátu CA.

   Poznámka: Niektoré aplikácie s podporou SSL podporujú autentifikáciu klientov, založenú na certifikátoch. Použitie certifikátov na autentifikáciu klientov zaisťuje, že aplikácia pred umožnením prístupu na ňou riadené prostriedky prijme platný certifikát. Aplikácia s touto podporou sa musí nastaviť tak, aby verila CA, aby mohla autentifikovať certifikáty, ktoré vydá konkrétna CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.
6. Vyberte aplikácie, ktoré by mali dôverovať certifikátu CA a kliknite na **OK**. Zobrazí sa strana Stav bezpečných aplikácií na potvrdenie toho, že vybrané aplikácie sú nastavené tak, aby dôverovali tomuto novému certifikátu.
7. Teraz môžete importovať serverovský certifikát. V navigačnej časti okna vyberte **Pracovať s certifikátmi**, aby sa zobrazil zoznam certifikátov.
8. Kliknite na **Importovať**, aby sa zobrazila strana Import certifikátu.
9. Vyplňte formulár Importovať certifikát a kliknite na **OK** na návrat na stránku Pracovať s certifikátmi. Skontrolujte, či uvádzate názov súboru, ktorý obsahuje exportovaný serverovský alebo klientsky certifikát a že zadávate cieľové vydanie, ktoré zodpovedá tomu, ktoré ste zadali pri predchádzajúcom exportovaní certifikátu. Navrchu strany sa zobrazí správa, že DCM pridal certifikát do súčasnej pamäte certifikátov. Vami naimportovaný certifikát by sa mal zobraziť v zozname certifikátov.
10. Teraz musíte špecifikovať, ktoré aplikácie by mali používať naimportovaný certifikát pre SSL. V navigačnom rámci vyberte **Pracovať s bezpečnými aplikáciami** na zobrazenie stránky, ktorá vám umožní manažovať certifikáty, združené so špecifickými aplikáciami.
11. Vyberte aplikáciu zo zoznamu a kliknite na **Pracovať so systémovým certifikátom** na zobrazenie zoznamu certifikátov, ktoré môžete určiť na používanie zvolenej aplikácii pre vytvorenie relácií SSL.
12. Vyberte zo zoznamu certifikát a kliknite na **Priradiť nový certifikát**, aby sa vybratý certifikát priradil k špecifikovanej aplikácii. Navrchu strany sa zobrazí potvrdzovacia správa, ktorá označuje výber certifikátu.

Dokončením týchto úloh budú môcť aplikácie na cieľovom systéme V4R4 alebo V4R5 používať certifikát, vydaný lokálnou CA na inom iSeries. Pred začatím používa SSL pre tieto aplikácie však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým, ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát CA sa musí skopírovať do súboru na PC užívateľa alebo stiahnuť do prehliadača užívateľa, podľa požiadaviek aplikácie s podporou SSL.

Manažovať aplikácie v DCM

Správcu digitálnych certifikátov (DCM) môžete použiť na vykonávanie rôznych úloh pre aplikácie s podporou SSL a aplikácie, podpisujúce objekty. Napríklad, môžete manažovať, ktoré certifikáty používajú vaše aplikácie pre komunikačné relácie Secure Sockets Layer (SSL). Úlohy na správu aplikácie, ktoré môžete vykonať, sa menia v závislosti na type aplikácie a pamäte certifikátov, v ktorej pracujete. Môžete manažovať len aplikácie z pamäte certifikátov *SYSTEM alebo *OBJECTSIGNING.

Väčšina úloh manažmentu aplikácií, ktoré poskytuje DCM je ľahko pochopiteľná, je tu niekoľko úloh, ktoré nemusíte poznať. Informácie o týchto úlohách nájdete v týchto témach:

Vytvoriť definíciu aplikácie popisuje typy aplikácií, ktoré môžete definovať a s ktorými môžete pracovať.

Manažovať priradenia certifikátov opisuje, ako priradiť alebo zmeniť certifikát, ktorý aplikácia používa na vytvorenie relácie SSL alebo na podpisovanie objektov.

Definovať zoznam dôveryhodných CA popisuje, kedy môžete a kedy by ste mali definovať, ktorým certifikačným autoritám môže aplikácia dôverovať pri overovaní platnosti a akceptovaní certifikátov.

Informácie o ďalších úlohách DCM môžete nájsť v online pomoci.

Vytvoriť definície aplikácie

Existujú dva typy definícií aplikácií, s ktorými môžete pracovať v DCM: definície aplikácií pre aplikácie servera alebo klienta, ktoré používajú SSL a definície aplikácií, ktoré používate na podpisovanie objektov.

Ak chcete použiť DCM na prácu s definíciami aplikácií pre SSL a ich certifikátmi, aplikácia sa musí najprv zaregistrovať v DCM ako definícia aplikácie, aby mala jedinečné ID aplikácie. Vývojári aplikácií registrujú aplikácie s podporou SSL pomocou API (QSYRGAP, QsyRegisterAppForCertUse), aby sa v DCM vytvoril ID aplikácie automaticky. Všetky aplikácie IBM iSeries s povoleným SSL sú registrované s DCM, takže môžete jednoducho používať DCM na priradenie certifikátu k nim, tak, že budú môcť vytvoriť reláciu SSL. Pre aplikácie, ktoré napíšete alebo kúpite tiež môžete zadefinovať definíciu aplikácie a vytvoriť ID aplikácie v samotnom DCM. Aby ste mohli vytvoriť definíciu aplikácie SSL pre aplikáciu klienta alebo aplikáciu servera, musíte pracovať v pamäti certifikátov *SYSTEM.

Ak chcete použiť certifikát na podpisovanie objektov, musíte najprv zadefinovať aplikáciu, ktorú bude používať certifikát. Na rozdiel od definície aplikácie SSL, aplikácia, podpisujúca objekty, nepopisuje skutočnú aplikáciu. Vami vytvorená definícia aplikácie by mala popisovať typ alebo skupinu objektov, ktoré chcete podpísať. Aby ste mohli vytvoriť definíciu aplikácie, podpisujúcej objekty, musíte pracovať v pamäti certifikátov *OBJECTSIGNING.

Ak chcete vytvoriť definíciu aplikácie, vykonajte tieto kroky:
1. Spustite DCM.
2. Kliknite na **Vybrať pamäť certifikátov** a vyberte správnu pamäť certifikátov. (Je to buď pamäť certifikátov *SYSTEM alebo pamäť certifikátov *OBJECTSIGNING podľa toho, aký typ definície aplikácie vytvárate.)

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať aplikácie**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Pridať aplikáciu**, aby sa zobrazil formulár na zadefinovanie aplikácie.

   Poznámka: Ak pracujete v pamäti certifikátov *SYSTEM, DCM vás vyzve, aby ste zvolili, či sa bude pridávať definícia aplikácie servera alebo definícia aplikácie klienta.
6. Vyplňte formulár a kliknite na **Pridať**. Informácie, ktoré môžete špecifikovať pre definíciu aplikácie sa menia podľa typu aplikácie, ktorú definujete. Ak definujete aplikáciu servera, môžete tiež špecifikovať, či aplikácia môže používať certifikáty na autentifikáciu klientov a či má vyžadovať autentifikáciu klientov. Môžete tiež špecifikovať, že aplikácia musí pri autentifikovaní certifikátov používať zoznam dôveryhodných CA.

Manažovať priradenia certifikátu aplikácii

Aby mohla aplikácia vykonať bezpečnú funkciu, ako je vytvorenie Secure Sockets Layer (SSL) relácie alebo podpísanie objektu, musíte použiť Správcu digitálnych certifikátov a aplikácii priradiť nejaký certifikát. Ak chcete aplikácii priradiť certifikát alebo zmeniť priradenie certifikátu pre danú aplikáciu, vykonajte tieto kroky:

1. Spustite DCM.
2. Kliknite na **Vybrať pamäť certifikátov** a vyberte správnu pamäť certifikátov. (Je to buď pamäť certifikátov *SYSTEM alebo pamäť certifikátov *OBJECTSIGNING podľa typu aplikácie, ktorej priraďujete certifikát.)

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať aplikácie**, aby sa zobrazil zoznam úloh.
5. Ak ste v pamäti certifikátov *SYSTEM, zvoľte typ aplikácie, ktorá sa má manažovať. (Zvoľte **Serverovská** alebo **Klientska** aplikácia, ako je to vhodné.)
6. Zo zoznamu úloh vyberte **Zaktualizovať priradenie certifikátu**, aby sa zobrazil zoznam aplikácií, ktorým chcete priradiť certifikát.
7. Zo zoznamu vyberte nejakú aplikáciu a kliknite na **Zaktualizovať priradenie certifikátu**, aby sa zobrazil zoznam certifikátov, ktoré môžete priradiť aplikácii.
8. Zo zoznamu vyberte certifikát a kliknite na **Priradiť nový certifikát**. DCM zobrazí správu, ktorou potvrdí váš výber certifikátu pre aplikáciu.

   Poznámka: Ak priraďujete certifikát aplikácii s podporou SSL, ktorá podporuje použitie certifikátov na autentifikáciu klientov, pre túto aplikáciu musíte zadefinovať zoznam dôveryhodných CA. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Keď zmeníte alebo odstránite certifikát pre aplikáciu, aplikácia môže a nemusí rozpoznať zmenu, ak je v čase zmeny priradenia certifikátu spustená. Napríklad, Client Access Express servery použijú všetky zmeny priradenia certifikátov automaticky pri ich vykonaní. Avšak môžete potrebovať zastaviť a spustiť servery Telnet, IBM HTTP Server for iSeries, alebo iné aplikácie, aby mohli tieto aplikácie zaviesť vaše zmeny certifikátov.

Od verzie V5R2 môžete použiť úlohu Priradiť certifikát, keď chcete priradiť certifikát ku niekoľkým aplikáciám súčasne.

Definovať zoznam dôveryhodných CA pre aplikáciu

Aplikácie, ktoré podporujú použitie certifikátov na autentifikáciu klienta počas Secure Sockets Layer (SSL) relácie musia určiť, či budú akceptovať certifikát ako platný dôkaz identity. Jedným z kritérií, ktoré aplikácia používa na autentifikáciu certifikátu je to, či aplikácia dôveruje Certifikačnej autorite (CA), ktorá vydala daný certifikát.

Na definovanie CA, ktorej certifikátom má aplikácia dôverovať počas vykonávania autentifikácie klientov môžete použiť Správcu digitálnych certifikátov (DCM). CA, ktorým dôveruje aplikácia manažujete pomocou zoznamu dôveryhodných CA.

Aby ste mohli zadefinovať zoznam dôveryhodných CA pre aplikáciu, musí byť splnených niekoľko podmienok:

- Aplikácia musí podporovať použitie certifikátov na autentifikáciu klientov.

- Definícia pre aplikáciu musí špecifikovať, že aplikácia používa zoznam dôveryhodných CA.

Ak definícia pre aplikáciu špecifikuje, že aplikácia používa zoznam dôveryhodných CA, tento zoznam musíte zadefinovať a až potom môže aplikácia úspešne vykonať autentifikáciu klientov. Toto zaistí, že aplikácia môže validovať len certifikáty od tých CA, ktoré špecifikujete ako dôveryhodné. Ak užívatelia alebo aplikácia klienta predloží certifikát od CA, ktorá nie je špecifikovaná ako dôveryhodná, aplikácia ho nebude akceptovať ako základ pre kladnú validizáciu.

Keď pridáte do zoznamu dôveryhodných CA pre aplikáciu novú CA, musíte tiež zaistiť, že táto CA je povolená.

Ak chcete zadefinovať zoznam dôveryhodných CA pre aplikáciu, vykonajte tieto kroky:
1. Spustite DCM.
2. Kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte pamäť certifikátov *SYSTEM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
3. Keď sa zobrazí stránka Pamäť certifikátu a heslo, uveďte heslo, ktoré ste zadali pre pamäť certifikátov, keď ste ju vytvárali a kliknite na **Pokračovať**.
4. V navigačnej časti okna vyberte **Manažovať aplikácie**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Definovať zoznam dôveryhodných CA**.
6. Vyberte typ aplikácie (server alebo klient), pre ktorú chcete definovať zoznam a kliknite na **Pokračovať**.
7. Zo zoznamu vyberte nejakú aplikáciu a kliknite na **Pokračovať**, aby sa zobrazil zoznam certifikátov CA, ktoré použijete na zadefinovanie zoznamu dôveryhodných CA.
8. Vyberte všetky CA, ktorým má dôverovať aplikácia a kliknite na **OK**. DCM zobrazí správu, ktorou potvrdí váš výber pre zoznam dôveryhodných CA.

   Poznámka: Zo zoznamu môžete vybrať jednotlivé CA alebo môžete špecifikovať, že aplikácia by mala dôverovať všetkým alebo žiadnej z CA v zozname. Pred pridaním certifikátu CA do zoznamu dôveryhodných CA ho tiež môžete zobraziť alebo validovať.

Overiť platnosť certifikátov a aplikácií

Správcu digitálnych certifikátov (DCM) môžete použiť na validovanie jednotlivých certifikátov alebo aplikácií, ktoré ich používajú. Zoznam vecí, ktoré kontroluje DCM sa trochu odlišuje podľa toho, či validujete certifikát alebo aplikáciu.

validizácia aplikácie

Použitie DCM na validizáciu definície aplikácie pomáha predchádzať problémom s certifikátmi pre aplikáciu, keď vykonáva nejakú funkciu, ktorá vyžaduje certifikáty. Takéto problémy by mohli zabrániť aplikácii úspešne vytvoriť Secure Sockets Layer (SSL) reláciu alebo úspešne podpisovať objekty.

Keď validujete aplikáciu, DCM kontroluje, či existuje priradenie certifikátu pre aplikáciu a zaisťuje, že priradený certifikát je platný. Okrem toho, DCM zaisťuje, že ak je aplikácia nakonfigurovaná na použitie zoznamu dôveryhodných Certifikačných autorít (CA), tento zoznam dôveryhodných autorít obsahuje minimálne jeden certifikát CA. DCM potom skontroluje, či sú certifikáty CA v zozname dôveryhodných CA platné. Taktiež, ak definícia

aplikácie špecifikuje, že sa má vykonávať spracovanie Certificate Revocation List (CRL) a pre CA je definované umiestnenie CRL, DCM kontroluje dané CRL ako súčasť validačného procesu.

validizácia certifikátu

Keď validujete certifikát, DCM kontroluje množstvo položiek, týkajúcich sa certifikátu, aby zaistil autenticitu a platnosť tohto certifikátu. validizácia certifikátu zaisťuje, že aplikácie, ktoré používajú tento certifikát pre bezpečnú komunikáciu alebo na podpisovanie objektov, budú mať problémy pri používaní tohto certifikátu len veľmi nepravdepodobne.

Ako súčasť validačného procesu, DCM kontroluje, či vybraný certifikát nemá skončenú platnosť. DCM tiež kontroluje, či daný certifikát nie je uvedený v Certificate Revocation List (CRL) ako zrušený, ak pre danú CA, ktorá vydala tento certifikát existuje umiestnenie CRL. Okrem toho, DCM kontroluje, či certifikát CA pre vydávajúcu CA je v súčasnej pamäti certifikátov a či je tento certifikát CA povolený a preto dôveryhodný. Ak má certifikát súkromný kľúč (napríklad, certifikáty servera, klienta a na podpisovanie objektov), DCM tiež validuje pár verejný-súkromný kľúč, aby zaistil, že tento pár je správny. Inými slovami, DCM zašifruje údaje pomocou verejného kľúča a potom sa presvedčí, že sa dajú rozšifrovať pomocou súkromného kľúča.

Priradiť certifikát k aplikáciám

Počínajúc vo V5R2 vám nové rozšírenie Správcu digitálnych certifikátov (DCM) umožňuje priradiť certifikát rýchlo a jednoducho ku viacerým aplikáciám. Priradiť certifikát ku viacerým aplikáciám môžete iba v pamätiach certifikátov *SYSTEM or *OBJECTSIGNING.

Na vytvorenie priradenia certifikátu pre jednu alebo viacero aplikácií postupujte podľa týchto krokov:

1. Spustite DCM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár počas používania DCM, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
2. V navigačnom rámci kliknite na **Vybrať pamäť certifikátov** a vyberte ***OBJECTSIGNING** alebo ***SYSTEM**.
3. Zadajte heslo pre pamäť certifikátov a kliknite na **Pokračovať**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Priradiť certifikát** na zobrazenie zoznamu certifikátov pre aktuálnu pamäť certifikátov.
6. Vyberte certifikát zo zoznamu a kliknite na **Priradiť aplikáciám** na zobrazenie zoznamu definícií aplikácií pre aktuálnu pamäť certifikátov.
7. Vyberte jednu alebo viacero aplikácií zo zoznamu a kliknite na **Pokračovať**. Zobrazí sa stránka s potvrdzovacou správou pre váš výber priradenia, alebo s chybovým hlásením, ak nastal problém.

Manažovať umiestnenia CRL

Správca digitálnych certifikátov (DCM) vám umožňuje definovať a riadiť informácie o umiestnení Zoznamu odmietaných certifikátov (CRL) pre určitú certifikačnú autoritu (CA) na použitie ako časť procesu overovania platnosti certifikátu. DCM alebo aplikácia, ktorá vyžaduje spracovanie CRL môže použiť CRL na určenie, že CA, ktorá vydala konkrétny certifikát ho nezrušila. Keď definujete umiestnenie CRL pre určitú CA, aplikácie, ktoré podporujú použitie certifikátov na autentifikáciu klientov, môžu pristupovať na CRL.

Aplikácie, ktoré podporujú použitie certifikátov na autentifikáciu klientov môžu vykonať spracovanie CRL na zabezpečenie prísnejšej autentifikácie pre certifikáty, ktoré akceptujú ako platný dôkaz identity. Aby mohla aplikácia použiť definovaný CRL ako súčasť procesu validizácie certifikátov, definícia aplikácie v DCM musí vyžadovať, aby daná aplikácia vykonávala spracovanie CRL.

Ako funguje spracovanie CRL?

Keď použijete DCM na validovanie certifikátu alebo aplikácie, DCM vykoná štandardne spracovanie CRL ako súčasť procesu validizácie. Ak nie je zadefinované žiadne umiestnenie CRL pre CA, ktorá vydala certifikát, ktorý validujete, DCM nemôže vykonať kontrolu CRL. Avšak DCM sa môže pokúsiť overiť platnosť iných dôležitých informácií o certifikáte, také ako či je podpis CA na určitom certifikáte platný a či je CA, ktorá ho vydala, dôveryhodná.

Definovať umiestnenie CRL

Ak chcete definovať umiestnenie CRL pre konkrétnu CA, vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti okna vyberte **Manažovať umiestnenia CRL**, aby sa zobrazil zoznam úloh.
3. Zo zoznamu úloh vyberte **Pridať umiestnenie CRL**, aby sa zobrazil formulár, ktorý môžete použiť na popísanie umiestnenia CRL a ako má DCM alebo iná aplikácia pristupovať na toto umiestnenie.
4. Vyplňte formulár a kliknite na **OK**. Musíte dať umiestneniu CRL jedinečný názov, identifikovať server LDAP, ktorý hosťuje CRL a poskytnúť informácie o pripojení, ktoré opisujú, ako pristupovať na server LDAP.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár v tejto úlohe, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.

   Teraz potrebujete združiť definíciu umiestnenia CRL so špecifickou CA.
5. V navigačnom rámci vyberte **Manažovať certifikáty** na zobrazenie zoznamu úloh.
6. Zo zoznamu úloh vyberte **Aktualizovať priradenie umiestnenia CRL** na zobrazenie zoznamu certifikátov CA.
7. Vyberte zo zoznamu certifikát CA, ku ktorému chcete priradiť definíciu umiestnenia CRL, ktorú ste vytvorili a kliknite na **Aktualizovať priradenie umiestnenia CRL**. Zobrazí sa zoznam umiestnení CRL.
8. Vyberte zo zoznamu umiestnenie CRL, ktoré chcete združiť s CA a kliknite na **Aktualizovať priradenie**. Na vrchole stránky sa zobrazí správa, oznamujúca, že umiestnenie CRL bolo priradené certifikátu certifikačnej autority (CA).

Keď zadefinujete umiestnenie pre CRL pre konkrétnu CA, DCM alebo iné aplikácie ho môžu používať pri vykonávaní spracovania CRL. Aby fungovalo spracovanie CRL, Directory Services server musí obsahovať príslušný CRL. Taktiež musíte nakonfigurovať aplikácie Directory Services servera a klienta na používanie SSL a priradiť certifikát do aplikácií v DCM.

Ak sa chcete dozvedieť viac p konfigurovaní a používaní servera iSeries Directory Services (LDAP), prezrite si tieto témy Informačného centra:

- Directory Services (LDAP)
  Táto kapitola obsahuje všetko, čo potrebujete vedieť o konfigurovaní a používaní servera iSeries Directory Services (LDAP).
- Using Secure Sockets Layer (SSL) security with the LDAP directory server
  Táto téma vysvetľuje, čo potrebujete na konfiguráciu vášho LDAP servera na použitie SSL pre bezpečnú komunikáciu.

Uložiť kľúče certifikátov na IBM 4758 Cryptographic Coprocessor

Ak ste nainštalovali IBM 4758–023 PCI Cryptographic Coprocessor na váš iSeries, môžete použiť koprocesor na poskytovanie bezpečnejšieho uloženie pre súkromný kľúč certifikátu. Koprocesor môžete použiť na uloženie súkromného kľúča pre certifikát servera, certifikát klienta alebo certifikát miestnej Certifikačnej autority (CA). Koprocesor nemôžete použiť na uloženie súkromného kľúča užívateľského certifikátu, pretože tento kľúč musí byť uložený na systéme užívateľa. Koprocesor tiež nemôžete v súčasnosti použiť na uloženie súkromného kľúča pre certifikát, podpisujúci objekty.

Koprocesor môžete použiť na uloženie súkromného kľúča certifikátu jedným z dvoch spôsobov:
- Uloženie súkromného kľúča certifikátu priamo na samotnom koprocesore.
- Použitie hlavného kľúča koprocesora na zašifrovanie súkromného kľúča certifikátu na uloženie v špeciálnom súbore kľúčov.

Túto voľbu pamäte pre kľúč môžete vybrať ako súčasť procesu vytvárania alebo obnovy certifikátu. Ak použijete koprocesor na uloženie súkromného kľúča certifikátu, môžete zmeniť priradenie zariadenia koprocesora pre tento kľúč.

Ak chcete použiť koprocesor pre uloženie súkromného kľúča, musíte zaistiť, aby bol koprocesor spustený pred použitím Správcu digitálnych certifikátov (DCM). V opačnom prípade DCM neposkytne stranu na výber voľby uloženia ako súčasť procesu vytvorenia alebo obnovy certifikátu.

Ak vytvárate alebo obnovujete certifikát servera alebo klienta, voľbu uloženia súkromného kľúča vyberiete po výbere typu CA, ktorá podpísala súčasný certifikát. Ak vytvárate alebo obnovujete miestnu CA, voľbu uloženia súkromného kľúča vyberiete ako prvý krok v tomto procese.

Uložiť súkromný kľúč certifikátu priamo na koprocesore

Na silnejšiu ochranu prístupu na a použitie súkromného kľúča certifikátu sa môžete rozhodnúť uložiť kľúč priamo na IBM 4758–023 PCI Cryptographic Coprocessor. Túto voľbu pamäte pre kľúč môžete vybrať ako súčasť vytvárania alebo obnovy certifikátu v Správcovi digitálnych zariadení.

Ak chcete uložiť súkromný kľúč certifikátu priamo na koprocesore, vykonajte kroky zo strany **Výber umiestnenie uloženia kľúča**:
1. Ako voľbu ukladania vyberte **Hardvér**.
2. Kliknite na **Pokračovať**. Týmto sa zobrazí strana **Výber popisu kryptografického zariadenia**.
3. Zo zoznamu zariadení vyberte to, ktoré chcete použiť na uloženie súkromného kľúča certifikátu.
4. Kliknite na **Pokračovať**. DCM pokračuje v zobrazovaní strán pre túto úlohu, ako sú identifikačné informácie pre certifikát, ktorý vytvárate alebo obnovujete.

Použiť hlavný kľúč koprocesora na zašifrovanie súkromného kľúča certifikátu

Na silnejšiu ochranu prístupu na a použitie súkromného kľúča certifikátu sa môžete použiť hlavný kľúč IBM 4758–023 PCI Cryptographic Coprocessor na zašifrovanie súkromného kľúča a uloženie kľúča v špeciálnom súbore kľúčov. Túto voľbu pamäte pre kľúč môžete vybrať ako súčasť vytvárania alebo obnovy certifikátu v Správcovi digitálnych zariadení.

Pred tým, ako budete môcť túto voľbu úspešne použiť, musíte použiť web rozhranie konfigurácie IBM 4758–023 PCI Cryptographic Coprocessor na vytvorenie vhodného súboru

pamäte kľúčov. Toto web rozhranie na konfiguráciu koprocesora tiež musíte použiť na spojenie súboru kľúčov s popisom zariadenia koprocesora, ktorý používate. Na web rozhranie konfigurácie koprocesora môžete pristúpiť zo stránky Úlohy iSeries.

Ak má váš systéme nainštalované viac ako jedno zariadenie koprocesora, môžete vybrať zdieľanie súkromného kľúča certifikátu medzi viacerými zariadeniami. Aby popisy zariadení zdieľali súkromný kľúč, všetky tieto zariadenia musia mať rovnaký hlavný kľúč. Proces distribúcie rovnakého hlavného kľúča do viacerých zariadení sa nazýva *klonovanie*. Zdieľanie kľúča medzi zariadeniami vám umožňuje použiť vyváženie výkonu Secure Sockets Layer (SSL), ktoré môže zlepšiť výkon pre bezpečné relácie.

Ak chcete použiť hlavný kľúč koprocesora na zašifrovanie hlavného kľúča certifikátu a uložiť ho v špeciálnom súbore kľúčov, vykonajte kroky zo strany **Výber umiestnenia uloženia kľúča**:

1. Ako voľbu ukladania vyberte **Šifrovaný hardvérom**.
2. Kliknite na **Pokračovať**. Týmto sa zobrazí strana **Výber popisu kryptografického zariadenia**.
3. Zo zoznamu zariadení vyberte to, ktoré chcete použiť na šifrovanie súkromného kľúča certifikátu.
4. Kliknite na **Pokračovať**. Ak máte nainštalovaných a spustených viac zariadení koprocesora, zobrazí sa strana **Výber dodatočných popisov kryptografických zariadení**.

   Poznámka: Ak nemáte k dispozícii viac zariadení koprocesora, DCM pokračuje v zobrazovaní strán pre túto úlohu, ako sú identifikačné informácie pre certifikát, ktorý vytvárate alebo obnovujete.
5. Zo zoznamu zariadení vyberte názov jedného alebo viacerých popisov zariadení, na ktorých chcete zdieľať súkromný kľúč certifikátu.

   Poznámka: Vami vybraté popisy zariadení musia mať rovnaký hlavný kľúč ako zariadenie, ktoré ste vybrali na predchádzajúcej strane. Ak chcete skontrolovať, či je hlavný kľúč rovnaký na všetkých zariadeniach, použite úlohu Master Key Verification z web rozhrania 4758 Cryptographic Coprocessor Configuration. Na web rozhranie konfigurácie koprocesora môžete pristúpiť zo stránky Úlohy iSeries.
6. Kliknite na **Pokračovať**. DCM pokračuje v zobrazovaní strán pre túto úlohu, ako sú identifikačné informácie pre certifikát, ktorý vytvárate alebo obnovujete.

Manažovať umiestnenie požiadavky pre PKIX CA

Certifikačná autorita (CA) PKIX (Public Key Infrastructure for X.509) je CA, ktorá vydáva certifikáty založené na najnovších internetových štandardoch x.509 pre implementovanie infraštruktúry verejných kľúčov. Štandardy PKIX sú obsiahnuté v Request For Comments (RFC) 2560.

PKIX CA vyžaduje prísnejšiu identifikáciu pred vydaním certifikátu; zvyčajne vyžaduje, aby žiadateľ poskytol dôkaz identity cez Registračnú autoritu (RA). Keď žiadateľ poskytne dôkaz identity, ktorý vyžaduje RA, RA potvrdí žiadateľovu identitu. Buď RA, alebo žiadateľ, v závislosti na procedúre, zavedenej CA, odošle certifikovanú aplikáciu do pridruženej CA. Ako sa tieto štandardy prijímajú v širšom rozsahu, CA, ktoré sú v súlade so špecifikáciou PKIX sa stanú viac dostupnými. O použití CA, vyhovujúcej PKIX, by ste mali pouvažovať v prípade, že vaše bezpečnostné potreby vyžadujú prísne riadenie prístupu na prostriedky, ktoré poskytujú vaše aplikácie s podporou SSL užívateľom. Napríklad Lotus Domino poskytuje PKIX CA pre verejné použitie.

Ak sa rozhodnete, že certifikáty na použitie vašimi aplikáciami vám bude vydávať PKIX CA, na manažovanie týchto certifikátov môžete použiť Správcu digitálnych certifikátov (DCM). DCM použite na konfiguráciu URL pre PKIX CA. Keď tak vykonáte, Správca digitálnych certifikátov (DCM) poskytne PKIX CA ako voľbu pre získavanie podpísaných certifikátov.

Ak chcete použiť DCM na manažovanie certifikátov od PKIX CA, musíte nakonfigurovať DCM na použitie umiestnenia pre danú CA vykonaním nasledovných krokov:

1. Spustite DCM.
2. V navigačnej časti vyberte **Manažovať umiestnenia požiadavky PKIX**, aby sa zobrazil formulár, ktorý vám umožňuje špecifikovať URL pre PKIX CA alebo s ňou spojenú RA.
3. Zadajte plne kvalifikovaný URL pre PKIX CA, ktorý chcete použiť na požiadanie o certifikát; napríklad: http://www.thawte.com a kliknite na **Pridať**. Pridaním URL sa DCM nakonfiguruje na pridanie PKIX CA ako voľby pre získavanie podpísaných certifikátov.

Potom, ako pridáte umiestnenie požiadavky PKIX CA, DCM pridá PKIX CA ako voľbu pre určovanie typu CA, ktorý si môžete zvoliť pre vydanie certifikátu, keď používate úlohu **Vytvoriť certifikát**.

Podpisovať objekty

Na podpisovanie objektov môžete použiť tri metódy. Môžete napísať program, ktorý volá API podpísania objektu. Môžete použiť Správcu digitálnych certifikátov (DCM) na podpisovanie objektov. Alebo, počínajúc vo V5R2, môžete použiť doplnok iSeries Navigator Riadiaca centrála na podpisovanie objektov, ako ich budete baliť pre distribúciu na iných systémov iSeries.

Certifikáty, ktoré manažujete v DCM môžete použiť na podpísanie ľubovoľného objektu, ktorý uložíte do integrovaného súborového systému vášho systému, okrem objektov, ktoré sú uložené v knižnici. Môžete podpisovať len tieto objekty, ktoré sú uložené v súborovom systéme QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG *FILE (len úložný súbor). Nové vo V5R2, môžete tiež podpisovať príkazové (*CMD) objekty. Nemôžete podpisovať objekty, ktoré sú uložené na iných serveroch iSeries.

Môžete podpísať objekty s certifikátmi, ktoré zakúpite od verejnej internetovej certifikačnej autority (CA), alebo ktoré vytvoríte so súkromnou, lokálnou CA v DCM. Fungovanie podpisovacích certifikátov je rovnaké, bez ohľadu na to, či použijete verejné alebo súkromné certifikáty.

Požiadavky pre podpisovanie objektov

Pred použitím DCM (alebo Sign Object API) na podpisovanie objektov musíte zaistiť, že sú splnené určité vyžadované podmienky:

- Musíte mať vytvorenú pamäť certifikátov *OBJECTSIGNING, buď ako časť procesu vytvorenia lokálnej CA, alebo ako časť procesu manažovania certifikátu na podpisovanie objektov z verejnej internetovej CA.
- Pamäť certifikátov *OBJECTSIGNING musí obsahovať aspoň jeden certifikát, buď jeden, ktorý ste vytvorili prostredníctvom lokálnej CA, alebo jeden, ktorý ste získali z verejnej internetovej CA.
- Musíte mať vytvorenú definíciu aplikácie na podpisovanie objektov na použitie pre podpisovanie objektov.
- Musíte mať priradený certifikát k aplikácii na podpisovanie objektov, ktorú plánujete používať na podpisovanie objektov.

Použiť DCM na podpisovanie objektov

Na použitie DCM na podpísanie jedného alebo viacerých objektov postupujte podľa týchto krokov:

1. Spustite DCM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár počas používania DCM, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
2. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***OBJECTSIGNING**.
3. Zadajte heslo pre pamäť certifikátov *OBJECTSIGNING a kliknite na **Pokračovať**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať podpísateľné objekty**, aby sa zobrazil zoznam úloh.
5. Z tohto zoznamu úloh vyberte **Podpísať objekt**, aby sa zobrazil zoznam definícií aplikácií, ktoré môžete použiť na podpisovanie objektov.
6. Vyberte niektorú aplikáciu a kliknite na **Podpísať objekt**, aby sa zobrazil formulár na špecifikovanie umiestnenia objektov, ktoré chcete podpísať.

   Poznámka: Ak vami vybratá aplikácia so sebou nemá spojený žiadny certifikát, nemôžete ju použiť na podpísanie objektu. Musíte najprv použiť úlohu **Zaktualizovať priradenie certifikátu** z **Manažovať aplikácie**, ktorou priradíte k definícii aplikácií nejaký certifikát.
7. V poskytnutom poli zadajte plne kvalifikovanú cestu a názov súboru objektu alebo adresára objektov, ktoré chcete podpísať a kliknite na **Pokračovať**. Alebo, zadajte umiestnenie adresára a kliknite na **Prehľadať**, aby sa zobrazil obsah tohto adresára a mohli ste z neho vybrať objekty na podpísanie.

   Poznámka: Názov objektu musíte začať s úvodným lomítkom, inak narazíte na chybu. Na popísanie časti adresára, ktorú chcete podpísať tiež môžete použiť určité znaky náhrady. Tieto znaky náhrady sú hviezdička (*****, ktorá špecifikuje ″ľubovoľný počet znakov,″ a otáznik (**?**), ktorý špecifikuje ″ľubovoľný jeden znak.″ Napríklad, ak chcete podpísať všetky objekty v konkrétnom adresári, mali by ste zadať /mydirectory/*; ak chcete podpísať všetky programy v konkrétnej knižnici, mali by ste zadať /QSYS.LIB/QGPL.LIB/*.PGM. Tieto znaky náhrady môžete použiť len v poslednej časti názvu cesty; napríklad, /mydirectory*/filename bude mať za následok chybovú správu. Ak chcete na zobrazenie zoznamu obsahu knižnice alebo adresára použiť funkciu Prehľadať, mali by ste zadať znak náhrady ako časť názvu cesty ešte pred kliknutím na **Prehľadať**.
8. Vyberte voľby spracovania, ktoré chcete použiť pre podpísanie vybratého objektu alebo objektov a kliknite na **Pokračovať**.

   Poznámka: Ak vyberiete čakanie na výsledky úlohy, súbor výsledkov sa zobrazí priamo vo vašom prehliadači. Výsledky pre súčasnú úlohu sa pridávajú na koniec súboru výsledkov. Tento súbor môže obsahovať okrem výsledkov súčasnej úlohy obsahovať aj výsledky z ľubovoľných predchádzajúcich úloh. Môžete špecifikovať dátumové pole v súbore čím určíte, ktoré riadky v súbore sa aplikujú na súčasnú úlohu. Dátumové pole má formát RRRRMMDD. Prvé pole v súbore môže byť ID správy (ak počas spracovania objektu došlo k chybe) alebo dátumové pole (označujúce dátum spracovania úlohy).
9. Špecifikujte plne kvalifikovanú cestu a názov súboru, ktorý sa použije na ukladanie výsledkov pre operáciu podpisovania objektov a kliknite na **Pokračovať**. Alebo, zadajte umiestnenie adresára a kliknite na **Prehľadať**, aby sa zobrazil obsah tohto adresára a mohli ste z neho vybrať súbor na ukladanie výsledkov úlohy. Zobrazí sa správa, ktorá označuje spustenie úlohy na podpísanie objektov. Ak chcete pozrieť výsledky úlohy, si v protokole úloh si pozrite úlohu **QOBJSGNBAT**.

Overiť podpisy objektov

Na kontrolu autenticity podpisov objektov môžete použiť Správcu digitálnych certifikátov. Keď skontrolujete podpis, zaistíte tým, že údaje v tomto objekte neboli zmenené od podpísania objektu vlastníkom objektu.

Požiadavky pre kontrolu podpisov

Pred použitím DCM na kontrolu podpisov na objektoch musíte zaistiť, že sú splnené určité vyžadované podmienky:

- Musíte vytvoriť pamäť certifikátov *SIGNATUREVERIFICATION na manažovanie vašich certifikátov na kontrolu podpisu.

  Poznámka: Kontrolu podpisov môžete vykonať počas práce s pamäťou certifikátov *OBJECTSIGNING v prípade, že kontrolujete podpisy pre objekty, ktoré boli podpísané na rovnakom systéme. Kroky, ktoré vykonáte na kontrolu podpisu v DCM sú rovnaké pre obe pamäte certifikátov. Pamäť certifikátov *SIGNATUREVERIFICATION však musí existovať a musí obsahovať kópiu certifikátu, ktorý podpísal objekt, aj v prípade, že kontrolu podpisu robíte počas práce v pamäti certifikátov *OBJECTSIGNING.
- Pamäť certifikátov *SIGNATUREVERIFICATION musí obsahovať kópiu certifikátu, ktorý podpísal objekty.
- Pamäť certifikátov *SIGNATUREVERIFICATION musí obsahovať kópiu certifikátu CA, ktorá vydala certifikát, ktorý podpísal objekty.

Použiť DCM na overenie podpisov na objektoch

Ak chcete na kontrolu podpisu objektov používať DCM, vykonajte tieto kroky:

1. Spustite DCM.

   Poznámka: Ak máte otázky, ako vyplniť niektorý konkrétny formulár počas používania DCM, vyberte znak otáznika (**?**) z vrchnej časti strany, čím sa dostanete do online pomoci.
2. V navigačnej časti okna kliknite na **Vybrať pamäť certifikátov** a na otvorenie vyberte ***SIGNATUREVERIFICATION**.
3. Zadajte heslo pre pamäť certifikátov *SIGNATUREVERIFICATION a kliknite na **Pokračovať**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manažovať podpísateľné objekty**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Skontrolovať podpis objektu**, aby ste mohli špecifikovať umiestnenie objektov, ktorým chcete skontrolovať podpisy.
6. V poskytnutom poli zadajte plne kvalifikovanú cestu a názov súboru objektu alebo adresára objektov, ktorým chcete skontrolovať podpisy a kliknite na **Pokračovať**. Alebo, zadajte umiestnenie adresára a kliknite na **Prehľadať**, aby sa zobrazil obsah tohto adresára a mohli ste z neho vybrať objekty na kontrolu podpisu.

   Poznámka: Môžete použiť aj bežné náhradné znaky na popísanie časti adresára, ktorú chcete skontrolovať. Tieto znaky náhrady sú hviezdička (*****, ktorá špecifikuje ″ľubovoľný počet znakov,″ a otáznik (**?**), ktorý špecifikuje ″ľubovoľný jeden znak.″ Napríklad, ak chcete podpísať všetky objekty v konkrétnom adresári, mali by ste zadať /mydirectory/*; ak chcete podpísať všetky programy v konkrétnej knižnici, mali by ste zadať /QSYS.LIB/QGPL.LIB/*.PGM. Tieto znaky náhrady môžete použiť len v poslednej časti názvu cesty; napríklad, /mydirectory*/filename bude mať za následok chybovú správu. Ak chcete

na zobrazenie zoznamu obsahu knižnice alebo adresára použiť funkciu Prehľadať, mali by ste zadať znak náhrady ako časť názvu cesty ešte pred kliknutím na **Prehľadať**.

7. Zvoľte voľby spracovania, ktoré chcete použiť pre overenie podpisu na vybranom objekte alebo objektoch a kliknite na **Pokračovať**.

   Poznámka: Ak vyberiete čakanie na výsledky úlohy, súbor výsledkov sa zobrazí priamo vo vašom prehliadači. Výsledky pre súčasnú úlohu sa pridávajú na koniec súboru výsledkov. Tento súbor môže obsahovať okrem výsledkov súčasnej úlohy obsahovať aj výsledky z ľubovoľných predchádzajúcich úloh. Môžete špecifikovať dátumové pole v súbore čím určíte, ktoré riadky v súbore sa aplikujú na súčasnú úlohu. Dátumové pole má formát RRRRMMDD. Prvé pole v súbore môže byť ID správy (ak počas spracovania objektu došlo k chybe) alebo dátumové pole (označujúce dátum spracovania úlohy).
8. Špecifikujte plne kvalifikovanú cestu a názov súboru, ktorý sa použije na ukladanie výsledkov pre operáciu kontroly podpisov a kliknite na **Pokračovať**. Alebo, zadajte umiestnenie adresára a kliknite na **Prehľadať**, aby sa zobrazil obsah tohto adresára a mohli ste z neho vybrať súbor na ukladanie výsledkov úlohy. Zobrazí sa správa, ktorá označuje spustenie úlohy na kontrolu objektov. Ak chcete pozrieť výsledky úlohy, si v protokole úloh si pozrite úlohu **QOBJSGNBAT**.

Na zobrazenie informácií o certifikáte, ktorý podpísal objekt tiež môžete použiť DCM. Toto vám umožňuje pred začatím práce s týmto určiť, či objekt pochádza zo zdroja, ktorému veríte.

Kapitola 9. Odstraňovanie chýb DCM

Tieto stránky môžete použiť na nájdenie užitočných informácií, ktoré vám môžu pomôcť odstrániť niektoré bežnejšie problémy, na ktoré môžete naraziť počas práce so Správcom digitálnych certifikátov (DCM).

Pre informácie o problémoch a ich možných riešeniach si prezrite tieto stránky:

Odstrániť problémy s heslami a všeobecné problémy
V týchto informáciách sa dozviete viac o bežných problémoch s užívateľským rozhraním DCM, na ktoré môžete naraziť a o spôsobe, ako ich odstrániť.

Odstrániť problémy s pamäťou certifikátov a databázou kľúčov
V týchto informáciách sa dozviete viac o bežných problémoch s pamäťou certifikátov a databázou kľúčov, na ktoré môžete naraziť a o spôsobe, ako ich odstrániť.

Odstrániť problémy s prehliadačom
V týchto informáciách sa dozviete viac o bežných problémoch, na ktoré môžete naraziť pri používaní vášho prehliadača na prístup na DCM a o spôsobe, ako ich správne odstrániť.

Odstrániť problémy s HTTP Server for iSeries
V týchto informáciách sa dozviete viac o bežných problémoch s HTTP severom, na ktoré môžete naraziť a o spôsobe, ako ich odstrániť.

Chyby pri migrácii a ich odstránenie
V týchto informáciách sa dozviete viac o bežných problémoch, na ktoré môžete naraziť pri migrácii DCM z predchádzajúceho vydania a o spôsobe, ako ich správne odstrániť.

Odstraňovanie problémov pri priraďovaní užívateľského certifikátu
V týchto informáciách sa dozviete viac o bežných problémoch, na ktoré môžete naraziť pri použití DCM na registráciu užívateľského certifikátu a o spôsobe, ako ich správne odstrániť.

Odstrániť problémy s heslami a všeobecné problémy

Nasledujúcu tabuľku použite na nájdenie informácií, ktoré vám pomôžu odstrániť niektoré bežnejšie problémy s heslami a iné všeobecné problémy, na ktoré môžete naraziť počas práce so Správcom digitálnych certifikátov (DCM).

Problém	Možné riešenie
Nemôžete nájsť ďalšiu pomoc pre DCM.	V DCM kliknite na ikonu ″**?**″. Môžete tiež prehľadať Information Center a externé stránky na Internete.
Pri pokuse o otvorenie pamäte certifikátov narazíte na chybu NET.DATA.	Keď použijete **Vybrať pamäť certifikátov**, tlačidlo **Pokračovať** vyberte pomocou myši, nie pomocou klávesu **Enter** na klávesnici.
Vaše heslo pre pamäť certifikátov Miestna Certifikačná autorita (CA) a *SYSTEM nefunguje.	Heslá sú rozlišujú a veľkosť písmen. Presvedčte sa, či je preraďovač veľkosti písmen v tej istej polohe, ako keď ste špecifikovali heslo.
Váš pokus o reset hesla, keď ste použili úlohu Zvoliť pamäť certifikátov, zlyhal.	Funkcia vynulovania pracuje len vtedy, ak DCM uložil heslo. DCM ukladá heslo automaticky, keď vytvoríte pamäť certifikátov. Avšak ak zmeníte (alebo zresetujete) heslo pre Pamäť certifikátov iného systému, potom musíte označiť voľbu**Automatické prihlasovanie**, aby DCM pokračoval v ukladaní hesla.

Problém	Možné riešenie
	Taktiež ak presúvate pamäť certifikátov z jedného systému na druhý, musíte zmeniť heslo pre pamäť certifikátov na novom systéme, aby ste zaistili, že ho DCM uloží automaticky. Na zmenu hesla musíte zadať pôvodné heslo pre pamäť certifikátov, keď ju otvoríte v novom systéme. Voľbu resetovať heslo nemôžete použiť, kým máte otvorenú pamäť s pôvodným heslom a zmenili ste heslo, aby sa uložilo. Ak heslo nie je zmenené a uložené, DCM a SSL ho nemôžu automaticky obnoviť keď je potrebné pre rôzne funkcie. Ak presúvate pamäť certifikátov, ktorú budete používať ako Pamäť certifikátov iného systému, musíte označiť voľbu **Automatické prihlasovanie**, keď meníte heslo, na zabezpečenie, že DCM uloží nové heslo pre tento typ pamäte certifikátov.
	Skontrolujte hodnotu, priradenú atribútu ″Povoliť nové digitálne certifikáty″ pod voľbou Pracovať s bezpečnosťou systému zo Systémových servisných nástrojov (SST). Ak je tento atribút nastavený na 2 (Nie), potom heslo pamäte certifikátov nemôže byť resetované. Pozrieť alebo zmeniť hodnotu pre tento atribút môžete príkazom STRSST a zadaním užívateľského ID a hesla užívateľa Servisných nástrojov. Potom zvoľte voľbu ″Pracovať s bezpečnosťou systému″. ID užívateľa Servisných nástrojov je pravdepodobne ID užívateľa QSECOFR.
Nemôžete nájsť zdroj pre certifikát CA, aby ste ho získali do vášho systému iSeries.	Niektoré CA nesprístupňujú svoj certifikát. Ak nemôžete získať certifikát od CA, kontaktujte vášho VAR, ktorý možno vykonal špeciálne alebo peňažné dohody s CA.
Nemôžete nájsť pamäť certifikátov *SYSTEM.	Umiestnenie súboru pamäte certifikátov musí byť /qibm/userdata/icss/cert/server/default.kdb. Ak pamäť certifikátov neexistuje, musíte použiť na jeho vytvorenie DCM. Použite úlohu **Vytvoriť novú pamäť certifikátov**.
Dostali ste od DCM chybu a táto chyba sa ďalej vyskytuje potom, čo ste ju odstránili.	Vymažte vyrovnávaciu pamäť prehliadača. Nastavte veľkosť vyrovnávacej pamäte na 0, ukončite a opätovne spustite prehliadač.
Máte problém s LDAP serverom, ako napríklad, že priradenia certifikátov sa nezobrazia pri zobrazení informácií o bezpečnej aplikácii ihneď po priradení certifikátu. Tento problém sa objaví častejšie pri používaní iSeries Navigator s prehliadačom Netscape Communicator. Vaša preferencia pre cache pamäť prehliadača je nastavená na porovnávanie dokumentu v cache pamäti s dokumentom na sieti ″Once per session″???.	Zmeňte vašu štandardnú preferenciu, aby vždy kontrolovala ukladanie do vyrovnávacej pamäte.
Keď používate DCM na importovanie certifikátu, podpísaného externou CA, ako je Entrust, dostanete chybové hlásenie, že perióda platnosti nezahŕňa dnešok, alebo nespadá do periódy platnosti svojho vydávateľa.	Systém používa pre obdobie platnosti formát všeobecného času. Počkajte jeden deň a zopakujte pokus. Taktiež skontrolujte, či má váš iSeries správnu hodnotu pre offset UTC (dspsysval qutcoffset). Ak zaregistrujete letný čas, váš posun môže byť nastavený nesprávne.
Keď ste sa pokúšali importovať certifikát Entrust, prijali ste základnú chybu??? 64.	Certifikát má uvedené, že je v špeciálnom formáte, ako je formát PEM. Ak funkcia kopírovania vášho prehliadača nefunguje správne, možno kopírujete materiál navyše, ktorý nepatrí certifikátu, ako sú prázdne medzery na začiatku každého riadka. Ak je to tento prípad, potom certifikát nie je v správnom formáte, keď sa ho pokúšate použiť na iSeries. Tento problém môžu spôsobovať návrhy niektorých web stránok. Iné web stránky sú navrhnuté tak, aby sa tomuto problému vyhli. Určite porovnajte vzhľad pôvodného certifikátu a výsledkami vloženia, pričom vložené informácie by mali vyzerať rovnako.

Problém	Možné riešenie
Keď migrujete z verzie V4R3 DCM do verzie V5R2, migrácia neprijme systémové certifikáty s ukončenou platnosťou.	Systémový certifikát, ktorého platnosť sa skončila, je teraz nesprávny a nemôže sa dostať do pamäte certifikátov *SYSTEM. Pred migráciou odstráňte alebo premenujte staré súbory kľúčov z verzie V4R3 a ignorujte správu o zlyhaní migrácie alebo skúste opakovane vykonať migráciu.
Nemôžete nájsť vzorový kód na pridávanie certifikátov do validačných zoznamov.	Vzorový kód ešte nie je dostupný.

Odstrániť problémy s pamäťou certifikátov a databázou kľúčov

Nasledujúcu tabuľku použite na nájdenie informácií, ktoré vám pomôžu odstrániť niektoré bežnejšie problémy s pamäťami certifikátov a databázou kľúčov, na ktoré môžete naraziť počas práce so Správcom digitálnych certifikátov (DCM).

Problém	Možné riešenie
Systém nenašiel databázu kľúčov alebo zistil, že je neplatná.	Skontrolujte si svoje heslo a názov súboru, či neobsahuje typografické chyby. Presvedčte sa, či je súčasťou názvu súboru cesta, vrátane začiatočného lomítka.
Vytvorenie kľúčovej databázy zlyhalo.	Zistite, či nie je konflikt s názvom súboru. Tento konflikt môže byť v inom súbore, než je ten, ktorý ste žiadali.
Systém neakceptuje textový súbor CA, ktorý bol prenesený v binárnom režime z iného systému. Takýto súbor bude akceptovaný, keď sa prenáša v ASCII (American National Standard Code for Information Interchange).	Súbory kľúčov a databázy kľúčov sú binárne a preto sú odlišné. Na prenos textových súborov CA musíte použiť File Transfer Protocol (FTP) v ASCII režime a FTP v binárnom režime pre binárne súbory, ako sú súbory s týmito rozšíreniami: .kdb, .kyr, .sth, .rdb, atď.
Nemôžete zmeniť heslo databázy kľúčov. Certifikát v databáze kľúčov už neplatí.	Po overení toho, že problémom nie je nesprávne heslo, vyhľadajte a vymažte neplatný certifikát alebo certifikáty z pamäte certifikátov a potom sa pokúste zmeniť heslo. Ak máte vo svojej pamäti certifikátov certifikáty so skončenou platnosťou, sú neplatné. Keďže sú tieto certifikáty neplatné, funkcia zmeny hesla pre pamäť certifikátov nemusí povoliť zmenu hesla a proces šifrovania nezašifruje súkromné kľúče takéhoto neplatného certifikátu. To zabraňuje zmene hesla a systém môže nahlásiť, že jednou z príčin je poškodenie pamäte certifikátov. Neplatné certifikáty (so skončenou platnosťou) musíte z pamäte certifikátov odstrániť.
Certifikáty potrebujete používať pre internetového užívateľa a preto potrebujete použiť validačné zoznamy, ale DCM neposkytuje funkcie pre validačné zoznamy.	Obchodní partneri, vytvárajúci aplikácie, ktoré majú použiť validačné zoznamy, musia napísať ich kód, ktorý priradí validačný zoznam k ich aplikácii. Musia tiež napísať kód, ktorý určí, či je totožnosť internetového užívateľa riadne overená tak, aby sa do validačného zoznamu mohol pridať daný certifikát. Pozrite si tému v Information Center pre QsyAddVldlCertificate API. Pri konfigurovaní bezpečnej inštancie servera na používanie validačného zoznamu si pozrite Webmaster's Guide.

Odstrániť problémy s prehliadačom

Nasledujúcu tabuľku použite ako pomoc pri odstránení niektorých bežnejších problémov, týkajúcich sa prehliadačov, na ktoré môžete naraziť počas práce so Správcom digitálnych certifikátov (DCM).

Problém	Možné riešenie
Microsoft Internet Explorer vás nenechá vybrať iný certifikát, kým nespustíte novú reláciu prehliadača.	Spustite novú reláciu pre Internet Explorer.

Problém	Možné riešenie
Internet Explorer nezobrazí všetky dostupné certifikáty klienta/užívateľa vo výberovom zozname prehliadača. Internet Explorer zobrazí len certifikáty, vydané dôveryhodnou CA, ktoré môžete použiť na bezpečnom mieste.	CA musí byť v databáze kľúčov uvedená ako dôveryhodná, ako aj v bezpečnej aplikácii. Presvedčte sa, že ste na PC s prehliadačom Internet Explorer prihlásený s tým istým menom, ktoré je v užívateľskom certifikáte v prehliadači. Od systému, na ktorý pristupujete získajte iný užívateľský certifikát. Správca systému by sa mal presvedčiť, že pamäť certifikátov (databáza kľúčov) stále dôveruje CA, ktorá podpísala certifikáty užívateľa a systému.
Internet Explorer 5 prijme certifikát CA, ale nemôže otvoriť súbor alebo nájsť disk, na ktorý ste uložili certifikát.	Toto je nová funkcia prehliadača pre certifikáty, ktorý zatiaľ prehliadač Internet Explorer nedôveruje. Môžete použiť miesto na vašom PC.
Dostali ste varovanie od prehliadača, že názov systému a systémový certifikát sa nezhodujú.	Niektoré prehliadače vykonávajú odlišné porovnávanie veľkých a malých písmen v názvoch systémov. URL napíšte presne tak, ako uvádza systémový certifikát. Alebo, vytvorte systémový certifikát tak, aby sa zhodoval s tým, čo používa väčšina užívateľov. Ak neviete, čo vlastne robíte, najlepšie je ponechať názov systému alebo názov servera nezmenený. Mali by ste tiež skontrolovať správnosť vášho názvového servera domény.
Spustili ste Internet Explorer s HTTPS namiesto HTTP a dostali ste varovanie o zmiešaní bezpečnej a nebezpečnej relácii.	Toto varovanie môžete akceptovať alebo ignorovať; budúce vydania Internet Explorer tento problém odstránia.
Netscape Communicator 4.04 pre Windows skonvertoval hexadecimálne hodnoty A1 a B1 na B2 a 9A v poľskej kódovej stránke.	Jedná sa o chybu v prehliadači, ktorá ovplyvňuje NLS. Použite iný prehliadač, alebo použite hoci aj rovnakú verziu tohto prehliadača na inej platforme, ako je Netscape Communicator 4.04 pre AIX.
V užívateľskom profile, Netscape Communicator 4.04 zobrazil veľké NLS písmená užívateľského certifikátu správne, ale malé písmená zobrazil nesprávne.	Niektoré národné jazykové znaky, ktoré boli zadané správne ako jeden znak sa pri neskoršom zobrazení zobrazili inak. Napríklad vo verzii Netscape Communicator 4.04 pre Windows boli hexadecimálne hodnoty A1 a B1 skonvertované na B2 a 9A pre poľskú kódovú stránku, z čoho vyplynulo, že sa zobrazil iný znak NLS.
Prehliadač oznamuje koncovému užívateľovi, že daná CA nie je ešte dôveryhodná.	Na nastavenie **stavu CA** na povolený, čo označuje CA za dôveryhodnú, použite DCM.
Požiadavky Internet Explorer odmietajú spojenie pre HTTPS.	Toto je problém vo funkcii prehliadača alebo v jeho konfigurácii. Prehliadač rozhodol, že sa nepripojí na stránku, ktorá používa systémový certifikát, ktorý je pravdepodobne podpísaný sám sebou alebo je z iného dôvodu neplatný.
Prehliadač Netscape Communicator a produkty servera používajú hlavné certifikáty od spoločností, akou je VeriSign, ako povoľujúcu funkciu SSL komunikácie — konkrétne sa jedná o autentifikáciu. Všetkým hlavným certifikátom končí pravidelne platnosť. Niektorým hlavným certifikátom prehliadača Netscape a servera skončila platnosť medzi 25. decembrom 1999 a 31. decembrom 1999. Ak tento problém neopravíte najneskôr 14. decembra 1999, zobrazí sa chybová správa.	Skoršie verzie prehliadača (Netscape Communicator 4.05 alebo skorší) majú certifikáty, ktorým končí platnosť. Musíte zaktualizovať prehliadač na súčasnú verziu Netscape Communicator. Informácie o hlavných certifikátov prehliadača sú k dispozícii na mnohých stránkach, vrátane http://home.netscape.com/security/ a http://www.verisign.com/server/cus/rootcert/webmaster.html. Prehliadač si môžete stiahnuť zadarmo z adresy http://www.netcenter.com.

Odstrániť problémy s HTTP Server for iSeries

Nasledujúcu tabuľku použite na nájdenie informácií, ktoré vám pomôžu odstrániť niektoré bežnejšie problémy s HTTP Server for iSeries, na ktoré môžete naraziť počas práce so Správcom digitálnych certifikátov (DCM).

Problém	Možné riešenie
HTTPS (Hypertext Transfer Protocol Secure) nefunguje.	Presvedčte sa, či je HTTP Server správne nakonfigurovaný na použitie SSL. V V5R1 alebo novších verziách musí mať konfiguračný súbor nastavený **SSLAppName** prostredníctvom grafického užívateľského rozhrania (GUI) servera HTTP. Taktiež musí mať konfigurácia nakonfigurovaného virtuálneho hostiteľa, ktorý používa port SSL, s **SSLEnable** vnútri virtuálneho hostiteľa. Tiež musia existovať dve smernice načúvanie, určujúce dva odlišné porty, jeden pre SSL, druhý nie pre SSL. Skontrolujte, či je vytvorená inštancia servera a či je serverovský certifikát podpísaný.
Proces registrácie inštancie servera HTTP ako bezpečnej aplikácie potrebuje objasnenie.	Na vašom systéme iSeries choďte do web rozhrania servera HTTP na nastavenie konfigurácie pre váš server HTTP. Musíte najprv definovať, aby virtuálny hostiteľ povolil SSL. To sa dá urobiť na obrazovke Manažment kontextu. Virtuálny hostiteľ musí byť definovaný, aby používal port SSL, definovaný predtým v smernici načúvania. Ďalej musíte použiť obrazovku Všeobecné nastavenia SSL na zapnutie SSL na predtým nakonfigurovanom virtuálnom hostiteľovi. Všetky zmeny musia byť aplikované na konfiguračný súbor. Všimnite si, že registrovanie vašej inštancie nezvolí automaticky, ktoré certifikáty by mala inštancia používať. Musíte použiť DCM na priradenie určitého certifikátu k vašej aplikácii pred tým, ako sa pokúsite zastaviť a reštartovať vašu inštanciu servera.
Máte ťažkosti pri nastavovaní HTTP servera pre validačné zoznamy a nepovinnú autentifikáciu klientov.	Pozrite si HTTP Server Webmaster's Guide, kde nájdete voľby pre nastavovanie inštancie. Tieto informácie sú tiež dostupné v kapitole Web serving v Informačnom centre.
Netscape Communicator čaká na skončenie platnosti konfiguračnej direktívy v kóde HTTP Servera, až potom vám umožní vybrať iný certifikát.	Väčšia hodnota certifikátu sťažuje registráciu druhého certifikátu, pretože prehliadač stále používa prvý.
Pokúšate sa donútiť prehliadač, aby HTTP Serveru predložil certifikát X.509, aby ste mohli tento certifikát použiť ako vstup do QsyAddVldlCertificate API.	Musíte použiť **SSLEnable** a **SSLClientAuth ON**, aby server HTTP zaviedol premennú prostredia HTTPS_CLIENT_CERTIFICATE. Tieto API môžete nájsť v kapitole OS/400 APIs v Informačnom centre. Možno sa tiež budete chcieť pozrieť na tieto API pre validačné zoznamy a certifikáty: • QsyListVldlCertificates a QSYLSTVC • QsyRemoveVldlCertificate a QRMVVC • QsyCheckVldlCertificate a QSYCHKVC • QsyParseCertificate a QSYPARSC, atď.
Nemôžete nájsť súbor požiadaviek, ktorý sa vytvoril pri inštalácii HTTP servera. Systém používa tento súbor na označenie platných súborov kľúčov, nájdených v direktíve KEYFILE v konfiguračných súboroch v jeho adresári.	Pozrite si Migrovať na DCM zo starších vydaní pre viac informácií. Pre server HTTP je správnym súborom /qibm/userdata/httpsvr/keyring/keymreq.crt. Pre LDAP je správnym súborom /qibm/userdata/os400/dirsrv/qdirsrv.crt.
HTTP Serveru trvá pridlho návrat alebo nestihne vykonať vašu požiadavku o zoznam certifikátov vo validačnom zozname a je tam viac ako 10000 položiek.	Vytvorte dávkovú úlohu, ktorá vyhľadáva a vymazáva certifikáty na základe zhodnosti s určitými kritériami, napríklad tie, ktorým skončila platnosť alebo sú od určitej CA.
Spozorovali ste problém s vašimi pamäťami certifikátov po nainštalovaní V5R2 cez vydanie V4R3 a súbor /qibm/userdata/httpsvr/keyring/keymreq.crt alebo /qibm/usedata/os400/dirsrv/qdirsrv.crt teraz existuje. Systém nedokázal dokončiť automatickú migráciu súboru kľúčov do databázy kľúčov.	Špecifikujte staré súbory kľúčov ako pamäť certifikátov a nájdite a vymažte neplatný certifikát alebo certifikáty zo súborov kľúčov pre zavolaním qicss/qyepmgrt na zopakovanie pokusu o migráciu. Alebo, ignorujte alebo vymažte .crt súbor, ak sa migráciou presunuli všetky dôležité certifikáty.

Problém	Možné riešenie
Server HTTP sa nespustí úspešne s nastaveným **SSLEnable**, v protokole úlohy sa objaví chybová správa HTP8351. Chybový protokol pre server *ADMIN ukazuje chybu, že operácia inicializácie SSL zlyhala s návratovým kódom chyby 107, keď server HTTP zlyháva.	Chyba 107 znamená, že sa ukončila platnosť certifikátu. Ak je inštanciou servera server *ADMIN, potom dočasne nastavte **SSLDisable**, aby ste mohli používať DCM na serveri *ADMIN. Použite DCM na priradenie iného certifikátu k aplikácii; napríklad QIBM_HTTP_SERVER_ADMIN, ak je inštanciou servera server *ADMIN.

Chyby pri migrácii a ich odstránenie

Chyby a zotavenie po chybe

Nasledujúce indikátory váš upozorňujú na chyby, ktoré by sa mohli vyskytnúť počas migrácie:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
Prítomnosť tohto indikátora po úspešnom nainštalovaní voľby 34 a 5722-DG1 znamená, že 5722-DG1 sa pokúsil migrovať súbor kľúčov ale zlyhal. Možno budete musieť vykonať migráciu súboru kľúčov do pamäte certifikátov *SYSTEM.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
Prítomnosť tohto indikátora po tom, ako ste úspešne nainštalovali voľbu 34, znamená, že migrácia kľúčov pre server LDAP nebola úspešná.

Okrem zistených chýb, existujú možné chyby migrácie, ktoré systém nemusí zistiť. Napríklad, keď systém nájde súbory kľúčov, ktoré je potrebné migrovať do pamäte certifikátov *SYSTEM, môže tiež objaviť konflikty s existujúcimi údajovými súbormi užívateľa v integrovanom súborovom systéme. V takomto prípade nemusí systém dokončiť migráciu súboru kľúčov, aj keď ste inštaláciu dokončili úspešne.

Zriedkavo sa môže stať, že sa vykoná migrácia súboru kľúčov s čiastočným priradením systémových certifikátov a následné chyby zabránia dokončeniu migrácie. To môže spôsobiť chyby, keď spustíte inštanciu *ADMIN web servera IBM HTTP Server, ak SSLMODE je ON. Nasledujú možné vysvetlenia:

- Migrovaný súbor kľúčov mal nastavený ako štandard zlý systémový certifikát.
- DCM skončil migráciu, aby uchoval užívateľské dáta, ktoré už existovali v kritickom názve súboru.
- V migračnom kóde došlo k nepredvídateľnej chybe.

IBM HTTP Server môžete spustiť bez SSLMODE nastaveného na ON dočasným prepnutím SSLMODE na OFF pre inštanciu *ADMIN pred spustením inštancie *ADMIN. To vám umožní prešetriť pamäte certifikátov pomocou DCM a vyriešiť problém skôr, než ukončíte inštanciu *ADMIN. Keď ukončíte inštanciu *ADMIN, môžete vrátiť SSLMODE späť na ON a spustiť inštanciu *ADMIN, aby sa správne nainicializovalo SSL.

Po migrácii voľby 34 sa môžu chyby vyskytnúť počas normálnych požiadaviek DCM, ktoré používajú pamäte certifikátov. K týmto chybám dochádza v prehliadači. Príkladom takýchto chýb je:

```
Chyba databázy
Chyba čítania databázy
Chyba zapisovania databázy
Poškodenie databázy
Poškodenie databázovej tabuľky
```

Ďalej, systém môže mať súbor, ktorý nie je platnou pamäťou certifikátov, nazvaný default.kdb, v rovnakom adresári ako /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR alebo

/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. V tomto prípade musíte vykonať nasledovnú manuálnu migráciu pred použitím DCM na vytvorenie nových certifikátov:

Poznámka: Ak vyberiete, že sa nebudú migrovať súbory kľúčov a vytvoríte novú CA a systémový certifikát, nasledovnú procedúru manuálnej migrácie preskočte.

- Ak plánujete nainštalovať HTTP Server for iSeries (5722-DG1), nainštalujte ho teraz, pred tým, ako budete pokračovať.

  Poznámky:

  1. Inštalačný kód voľby 34 z 5722–SS1 sa nepokúsi o opätovnú migráciu po nainštalovaní voľby 34. Jednoducho opakovaná inštalácia voľby 34 nepomôže.
  2. Príslušné súbory sú umiestnené v adresároch užívateľských údajov, ktoré boli vytvorené s oprávnením PUBLIC *EXCLUDE. Zabezpečte, aby ste na ne mali riadne oprávnenie.

- Skontrolujte, či existujú tieto súbory:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Ak existujú, premenujte ich pomocou príkazu WRKLNK a vytvorte zálohy.
- Z užívateľského profilu, ktorý má oprávnenie *ALLOBJ zavolajte v príkazovom riadku program QICSS/QYEPMGRT, nasledovne:

  ```
  CALL QICSS/QYEPMGRT
  ```

  Ak je výsledok úspešný, presvedčte sa, či na vašom systéme existuje jeden z týchto súborov:
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

DCM si normálne ponechá záložnú kópiu užívateľských údajov, uloženú v súboroch, ktorých názvy sú odlišné od tých, ktoré používa DCM. Ak nasledujúce súbory neexistujú:

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

Ale existujú tieto súbory:

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

Potom systém sa ich pokúsi premenovať pridaním rozšírenia .OLD. Ak tieto súbory už tiež existujú, systém nevytvorí žiadne záložné kópie. Namiesto toho jednoducho prepíše existujúce .STH súbory.

Rôzne

Ak sú vaše pokusy vytvoriť CA a systémový certifikát aj naďalej neúspešné kvôli rozporom s názvom súborov, mohli ste naraziť na jedno z nasledujúceho:

- **Konflikt s iným názvom súboru** – DCM sa pokúša chrániť užívateľské údaje v adresároch, ktoré vytvára, aj ak tieto súbory bránia DCM úspešne vytvoriť súbory, keď ich musí vytvoriť. Vyriešte tento problém skopírovaním všetkých konfliktných súborov do iného adresára a ak to bude možné, použite funkcie DCM na vymazanie zodpovedajúcich súborov. Ak na to nemôžete použiť DCM, súbory vymažte manuálne z pôvodného adresára integrovaného súborového systému, kde robili konflikt s DCM. Zabezpečte, aby ste pri

presune súborov zaznamenali presne, ktoré súbory presúvate. Kópie vám umožňujú obnoviť súbory, ak zistíte, že ich stále potrebujete. Musíte vytvoriť novú CA potom, ako presuniete nasledujúce súbory:

```
/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
```

Po presune nasledovných súborov musíte vytvoriť novú pamäť certifikátov *SYSTEM a systémový certifikát:

```
/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
```

- **Chýba vyžadovaný komponent** – Presvedčte sa, že ste správne nainštalovali vyžadované licenčné programy (LPP).
- **Problém kódu** – Spojte sa s predstaviteľom servisu.

Odstrániť problémy s priradením užívateľského certifikátu

Keď používate úlohu **Priradiť užívateľský certifikát** Správca digitálnych certifikátov (DCM) vám zobrazí informácie o certifikáte, aby ste ho pred registrovaní certifikátu schválili. Ak nie je DCM schopný zobraziť certifikát, problém môže byť spôsobený jednou z týchto situácií:

1. Váš prehliadač nepožiadal, aby ste si vybrali certifikát, ktorý predkladáte serveru. Toto sa môže stať, ak prehliadač uložil predošlý certifikát (z prístupu do iného servera) do vyrovnávacej pamäte. Pokúste sa vymazať vyrovnávaciu pamäť prehliadača a zopakujte úlohu. Prehliadač by vás mal vyzvať, aby ste si vybrali certifikát.
2. Certifikát, ktorý chcete zaregistrovať, je už zaregistrovaný pomocou DCM.
3. Certifikačná autorita, ktorá vydala certifikát, nie je v systéme označená ako dôveryhodný zdroj. Preto je vami predložený certifikát neplatný. Spojte sa so správcom systému, aby stanovil, či je CA, ktorá vydala váš certifikát správna. Ak je CA správna, správy systému musí **naimportovať** tento certifikát CA do pamäte certifikátov *SYSTEM. Alebo

správcovia môžu na vyriešenie problému potrebovať použiť úlohu **Pracovať s certifikátmi CA** na aktivovanie CA na systéme ako dôveryhodný zdroj.

4. Nemáte certifikát na registráciu. Môžete skontrolovať užívateľské certifikáty vo vašom prehliadači, aby ste videli, či sa jedná o tento problém.
5. Certifikátu, ktorý sa pokúšate zaregistrovať, skončila platnosť alebo nie je úplný. Ak chcete vyriešiť problém, musíte buď obnoviť certifikát alebo kontaktovať CA, ktorá ho vydala.
6. IBM HTTP Server for iSeries nie je správne nastavený na vykonávanie registrácie certifikátov prostredníctvom SSL a autentifikácie klienta na bezpečnej serverovskej inštancii *ADMIN. Ak nefunguje žiadny z predošlých tipov na odstránenie problémov, spojte sa so správcom vášho systému a nahláste mu vzniknutý problém.

Ak chcete **Priradiť užívateľský certifikát**, musíte byť pripojený do Správcu digitálnych certifikátov (DCM) pomocou SSL relácie. Ak pri výbere úlohy **Priradiť užívateľský certifikát** nepoužívate SSL, DCM zobrazí správu, že musíte použiť SSL. Správa obsahuje tlačidlo, pomocou ktoré sa môžete pripojiť do DCM pomocou SSL. Ak sa správa zobrazí bez tlačidla, informujte o tomto probléme správcu systému. Možno sa musí reštartovať Web server, aby sa zabezpečilo, že sa aktivujú konfiguračné direktívy na použitie SSL.

Kapitola 10. Informácie súvisiace s DCM

Ako sa použitie digitálnych certifikátov stáva bežnejším, je k dispozícii čoraz viac zdrojov informácií. Tu je krátky zoznam iných zdrojov, ktoré si môžete pozrieť, ak sa chcete dozvedieť viac o digitálnych certifikátoch a o tom, ako ich môžete použiť na rozšírenie politiky bezpečnosti iSeries:

- **Web stránka VeriSign**
  Web stránka VeriSign poskytuje rozsiahlu knižnicu s témami o digitálnych certifikátoch, ako aj množstvo iných tém o bezpečnosti v Internete.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Tento IBM Redbook sa zameriava na rozšírenie bezpečnosti siete V5R1. Kniha pokrýva mnoho tém, vrátane spôsobu použitia schopností podpisovania objektov iSeries, Správcu digitálnych certifikátov (DCM), podpora 4758 Cryptographic Coprocessor pre SSL, atď.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  Táto kniha popisuje, čo môžete robiť s digitálnymi certifikátmi na serveri iSeries. Vysvetľuje, ako nastaviť rôzne servery a klientov na použitie certifikátov. Ďalej poskytuje informácie a vzorový kód použitia OS/400 API na riadenie a používanie digitálnych certifikátov v užívateľských aplikáciách.
- **Vyhľadávanie v indexoch RFC**
  Táto web stránka poskytuje prehľadávateľnú schránku RFC (Request for Comments). RFC popisujú štandardy pre internetové protokoly, ako je SSL, PKIX a iné, ktoré sa týkajú použitia digitálnych certifikátov.

Vytlačené v USA