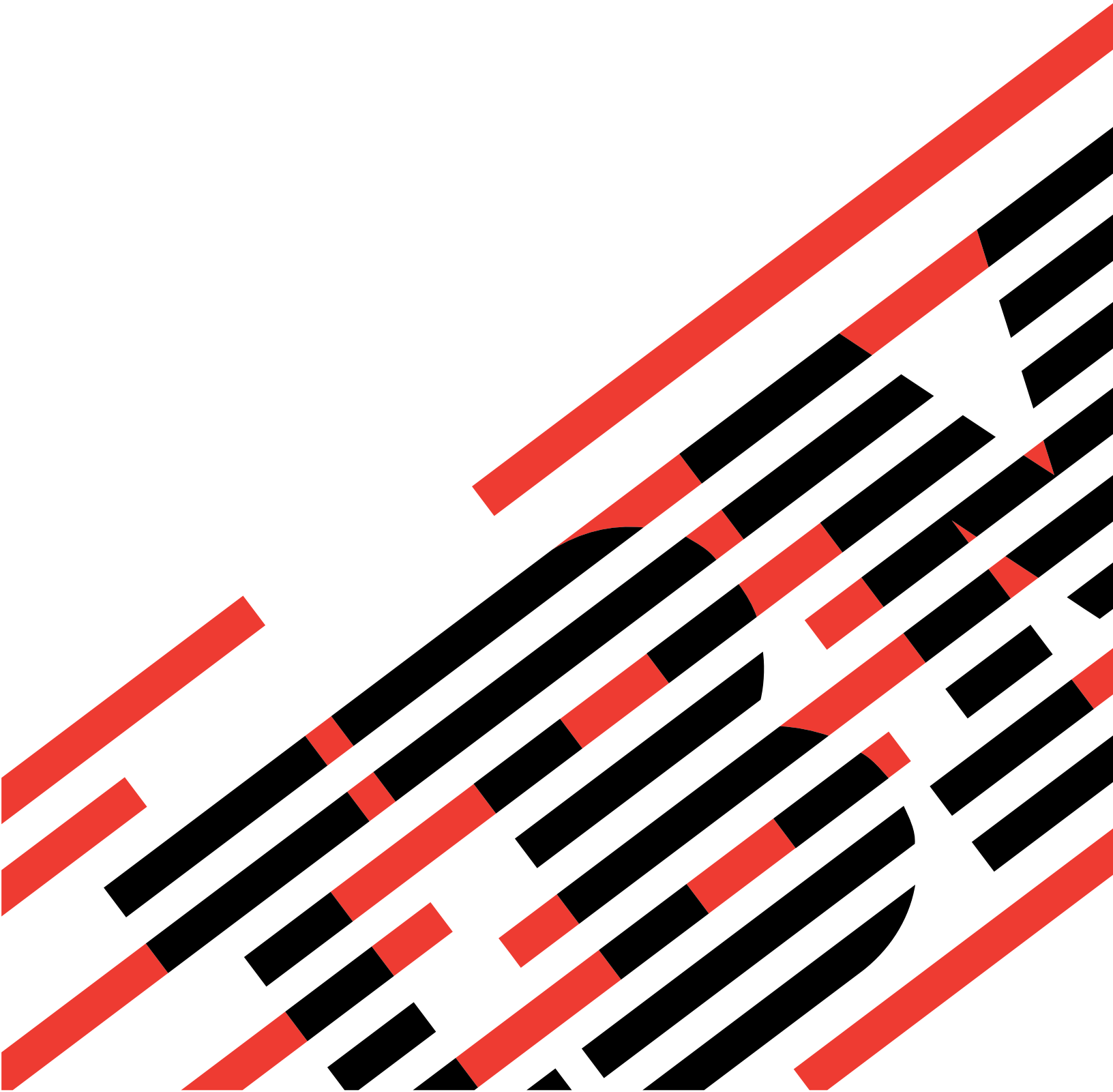
IBM

eserver

iSeries

Digital Certificate Manager

Verzia 5 Vydanie 3



IBM

@server

iSeries

Digital Certificate Manager

Verzia 5 Vydanie 3

Poznámka

Pred použitím týchto informácií a produktu, ktorý podporujú, si určite prečítajte informácie v časti “Vyhlásenia”, na strane 93.

Ôsme vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydanie 3, modifikácie 0 operačného systému IBM Operating System/400 (číslo produktu 5722–SS1) a všetkých následných vydaní a modifikácií pokiaľ nebude v nových vydaniach uvedené inak. Táto verzia nebeží na všetkých modeloch RISC (reduced instruction set computer) a nebeží ani na modeloch CISC.

Obsah

Kapitola 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. Množstvo služieb a aplikácií, ako sú FTP, Telnet, HTTP Server for iSeries a ďalšie, poskytuje podporu SSL na zabezpečenie utajenia údajov.

IBM poskytuje rozšírenú podporu digitálnych certifikátov, ktorá vám umožní používať v množstve bezpečnostných aplikácií digitálne certifikáty ako oprávnenia. Okrem použitia certifikátov na konfiguráciu SSL, môžete ich použiť ako oprávnenia pre autentifikáciu klienta v transakciách SSL a VPN (súkromná virtuálna sieť). 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 pre certifikáty je jednoduché, keď používate Správcu digitálnych certifikátov (DCM), ktorý je bezplatným komponentom slúžiacim na centrálny manažment certifikátov pre vaše aplikácie. DCM vám umožňuje manažovať certifikáty, ktoré získate od ľubovoľnej Certifikačnej autority (CA). DCM môžete použiť aj na vytvorenie a prevádzkovanie vašej vlastnej lokálnej CA, ak chcete vystavovať súkromné certifikáty pre aplikácie a užívateľov vo vašej organizácii.

Správne naplánovanie a vyhodnotenie sú kľúčovými momentmi pre efektívne používanie certifikátov s ohľadom na ich pridané bezpečnostné výhody. Ak si prečítate tieto témy, dozviete sa viac o fungovaní certifikátov a o tom, ako môžete používať DCM na ich manažovanie a na manažovanie aplikácií, ktoré ich používajú:

Novinky vo V5R3
Z týchto informácií sa dozviete o vylepšeniach Správcu digitálnych certifikátov (DCM) a zmenách v informačných témach, ktoré prináša toto vydanie.

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

Scenáre DCM
Tieto informácie použite na prehľad dvoch scenárov ilustrujúcich typické implementačné schémy certifikátov, ktoré vám pomôžu pri plánovaní vašej vlastnej implementácie certifikátu, v rámci vašej bezpečnostnej politiky. 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 možnosti ich použita, ako časti vašej bezpečnostnej politiky.

Plánovanie pre DCM
Použitie týchto informácií vám pomôže pri rozhodovaní, ako a kedy môžete použiť digitálne certifikáty na dosiahnutie vašich bezpečnostných zámerov. V týchto informáciách sa dozviete o predpokladoch, potrebných pri inštatalácii, 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.

Manažovanie DCM
Pomocou týchto informácií sa dozviete 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 2. Novinky vo V5R3

Vylepšenia Správcu digitálnych certifikátov V5R3 (DCM) a funkcií digitálnych certifikátov zahŕňajú:

- **Manage LDAP Location**
  Nová úloha Manage LDAP Location v úlohe DCM vám umožňuje ukladať užívateľské certifikáty, ktoré vystavuje lokálna Certifikačná autorita, do lokality LDAP (Lightweight Directory Access Protocol). Keď konfigurujete DCM na používanie tejto voľby, môžete použiť užívateľské certifikáty, uložené v tejto lokalite LDAP, s EIM (Enterprise Identity Mapping). Do tejto úlohy sa dostanete z hlavnej navigačnej ponuky DCM.
- **Vylepšenia úlohy Assign a user certificate pre EIM**
  Pri konfigurovaní DCM na prácu s EIM (Enterprise Identity Mapping) úloha Assign a user certificate ukladá priradené certifikáty do lokality LDAP (Lightweight Directory Access Protocol) a nie s užívateľským profilom. Ako DCM spracováva toto priradenie certifikátu, závisí od toho, či máte DCM nakonfigurovaný na používanie lokality LDAP (Lightweight Directory Access Protocol) na ukladanie certifikátov spolu s používaním EIM (Enterprise Identity Mapping).
- **Check certificate expiration**
  Táto nová funkcia vám umožňuje certifikáty rýchlo a ľahko zobraziť a manažovať na základe dátumu ukončenia ich platnosti. V prípade certifikátov servera alebo klienta a certifikátov na podpisovanie objektov môžete ukončenie platnosti certifikátov kontrolovať v lokálnom systéme. Môžete kontrolovať aj ukončenie platnosti užívateľských certifikátov. Ukončenie platnosti užívateľských certifikátov môžete kontrolovať buď pre konkrétny užívateľský profil, pre všetky užívateľské certifikáty v systéme alebo pre všetky užívateľské certifikáty v podniku, ak je v systéme nakonfigurované EIM.

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

Ako zistiť novinky alebo zmeny

Aby ste videli, kde došlo k technickým zmenám, táto informácia používa:

- » Obrázok na označenie, kde začínajú nové alebo zmenené informácie.
- « Obrázok na označenie, kde končia nové alebo zmenené informácie.

Kapitola 3. Tlač tejto témy

Ak chcete zobraziť alebo stiahnuť PDF verziu tejto témy, vyberte Digital Certificate Manager  (veľkosť súboru je asi 600 KB alebo asi 116 strán).

Ukladanie súborov PDF:

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

1. Pravým tlačidlom myši kliknite na PDF vo vašom prehliadači (pravým tlačidlom myši kliknite na vyššie uvedený odkaz).
2. Ak používate Internet Explorer, kliknite na **Save Target As...**. Ak používate Netscape Communicator, kliknite na **Save Link As...**.
3. Prejdite do adresára, do ktorého chcete uložiť dokument PDF.
4. Kliknite na **Save**.

Stiahnutie programu Adobe Acrobat Reader

Na prezeranie alebo tlač týchto PDF potrebujete program Adobe Acrobat Reader. Kópiu si môžete stiahnuť z webovej stránky Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Kapitola 4. Scenáre DCM

Digital Certificate Manager a systémová podpora digitálnych certifikátov vám umožňuje používať certifikáty na vylepšenie vašej bezpečnostnej politiky rozličnými 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 webové 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. Taktiež, podľa toho, ako nakonfigurujete DCM, môžete DCM používať na priradenie certifikátu užívateľa k jeho užívateľskému profilu alebo k identifikátoru EIM (Enterprise Identity Mapping). Tento certifikát má potom rovnaké oprávnenia a povolenia ako priradený užívateľský profil.

Preto to, ako sa rozhodnete použiť certifikáty, môže byť komplikované a závisí na rôznych faktoroch. Scenáre, uvedené v tejto téme, opisujú niektoré bežnejšie bezpečnostné účely digitálnych certifikátov pre bezpečnú komunikáciu v rámci typických firemných kontextov. Každý scenár taktiež opisuje všetky potrebné systémové a softvérové predpoklady a všetky konfiguračné úlohy, ktoré musíte vykonať na implementovanie scenára. **Poznámka:** Podrobné príklady o spôsobe používania digitálnych certifikátov na podpisovanie objektov na zabezpečenie ich integrity nájdete v téme Object signing scenarios v Informačnom centre iSeries.

Prezrite si tieto scenáre, aby vám pomohli zistiť, ako by mohlo použitie certifikátov pre zvýšenú bezpečnosť najlepšie vyhovovať vašim potrebám:

Scenár: Používanie certifikátov na externú autentifikáciu
Tento scenár opisuje, kedy a ako používať certifikáty ako autentifikačný mechanizmus na ochranu a na obmedzenie prístupu verejných užívateľov k verejným alebo extranetovým prostriedkom a aplikáciám.

Scenár: Používanie certifikátov na internú autentifikáciu
Tento scenár opisuje, kedy a ako používať certifikáty ako autentifikačný mechanizmus na ochranu a na vymedzenie prostriedkov a aplikácií, ku ktorým môžu mať interní užívatelia prístup na vašich interných serveroch.

Scenár: Používanie certifikátov na externú autentifikáciu

Situácia

Pracujete pre poisťovaciu spoločnosť MyCo, Inc a zodpovedáte za udržiavanie rozličných 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. Ďalej chcete pre aplikáciu asi poskytnúť bezpečnejšiu metódu autentifikácie užívateľa ako je vaše aktuálne meno užívateľa a heslo. Okrem toho vás znepokojuje, že neautorizovaní užívatelia by mohli zachytiť tieto informácie pri ich prenose cez nedôveryhodnú sieť. Znepokojuje vás aj to, že rozliční agenti by mohli navzájom zdieľať tieto informácie bez toho, aby na to mali oprávnenie.

Po preskúmaní tejto situácie sa rozhodnete, že používanie digitálnych certifikátov vám môže poskytnúť bezpečnosť, ktorú potrebujete na ochranu citlivých informácií, zadaných do a získaných z tejto aplikácie. Používanie certifikátov vám umožňuje na ochranu prenosu údajov o sadzbách používať SSL (Secure Sockets Layer). 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. Okrem používania certifikátu na autentifikáciu klienta plánujete naďalej bežne používať autentifikáciu pomocou mena užívateľa a hesla, pretože SSL chráni pri prenose súkromie týchto citlivých údajov.

Na základe typu aplikácie a jej užívateľov a vášho cieľa pre budúcnosť, ktorým je autentifikácia pomocou certifikátu pre všetkých užívateľov, sa rozhodnite, či budete na nakonfigurovanie SSL pre vašu aplikáciu používať verejný certifikát od všeobecne známej Certifikačnej autority (CA).

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. Dokonca aj v prípade, keď používanie digitálnych certifikátov nie je možné, relácia SSL chráni autentifikáciu klienta pomocou mena užívateľa a hesla a zabezpečuje jej súkromie, čím sa výmena takýchto citlivých údajov stane bezpečnejšou.
- Používanie *verejných* digitálnych certifikátov na autentifikáciu užívateľov pristupujúcich k vašim aplikáciám a údajom spôsobom, ktorý opisuje tento scenár, je praktickou voľbou za týchto alebo podobných podmienok:
  - Vaše údaje a aplikácie vyžadujú rôzne stupne bezpečnosti.
  - Existuje vysoká miera zmien medzi vašimi dôveryhodnými užívateľmi.
  - Poskytujete verejný prístup k aplikáciám a údajom, akými sú internetová webová stránka alebo extranetová aplikácia.
  - Nechcete prevádzkovať vašu vlastnú Certifikačnú autoritu (CA) z administračných dôvodov, akými sú veľký počet užívateľov zvonka, ktorí pristupujú k vašim aplikáciám a prostriedkom.
- Používanie verejného certifikátu na nakonfigurovanie aplikácie na výpočet sadzieb pre SSL v tomto scenári znižuje rozsah konfigurácie, ktorú musia užívatelia vykonať, aby mali bezpečný prístup k tejto aplikácii. Väčšina klientskeho softvéru obsahuje certifikáty CA pre väčšinu známych CA.

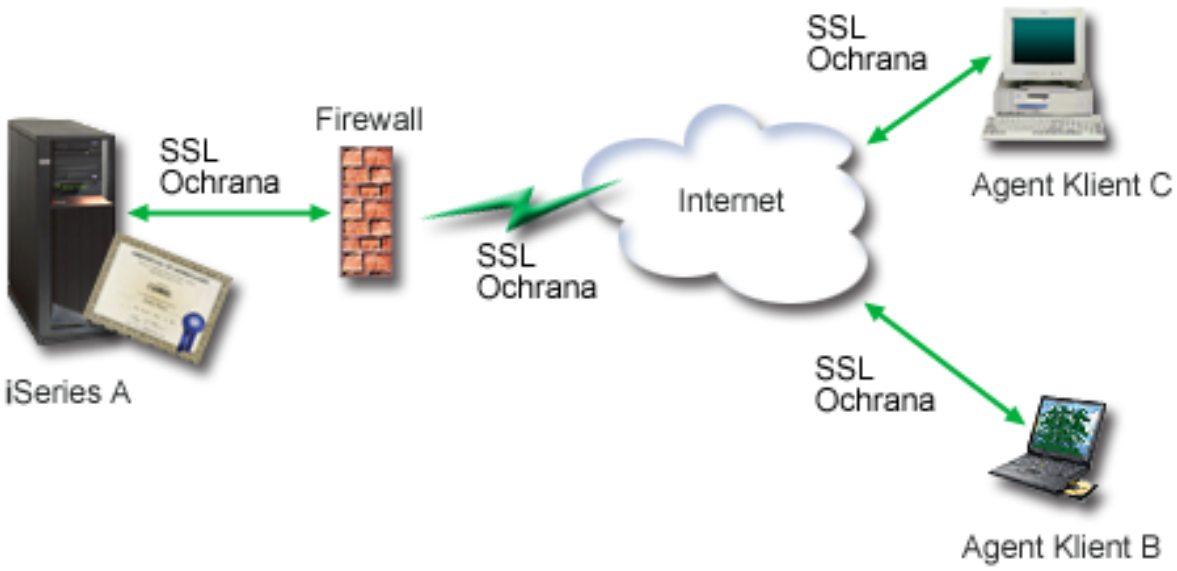
Ciele

V tomto scenári chce spoločnosť MyCo, Inc. používať digitálne certifikáty na ochranu informácií o výpočte sadzieb, ktoré poskytujú ich aplikácie autorizovaným verejným užívateľom. Táto spoločnosť chce podľa možnosti aj bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolený prístup k tejto aplikácii.

Ciele tohto scenára sú nasledovné:
- Verejná aplikácia na výpočet sadzieb musí na ochranu súkromia údajov, ktoré poskytuje užívateľom a ktoré od užívateľov dostáva, používať SSL.
- 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 predložiť jednak verejný digitálny certifikát od všeobecne známej Certifikačnej autority (CA) alebo platné meno užívateľa a heslo, ak certifikát nie je k dispozícii.

Detaily

Nasledujúci obrázok zobrazuje konfiguráciu siete v tomto scenári:



Obrázok ilustruje nasledujúce informácie o situácii pre tento scenár:

Verejný server spoločnosti – A
- Server A je server, ktorý hosťuje aplikáciu na výpočet sadzieb vašej spoločnosti.
- Na serveri A beží OS/400 Verzia 5 Vydanie 2 (V5R2). alebo vyššia.
- Server A má nainštalovaný Cryptographic Access Provider (5722–AC3).
- Na serveri A sú nainštalované a nakonfigurované programy Digital Certificate Manager (OS/400 voľba 34) a IBM HTTP Server for iSeries (5722–DG1).
- Na serveri A beží aplikácia na výpočet sadzieb, ktorá je nakonfigurovaná tak, že:
  – Vyžaduje režim SSL.
  – Na svoju vlastnú autentifikáciu k inicializácii relácie SSL používa verejný certifikát od všeobecne známej Certifikačnej autority (CA).
  – Vyžaduje autentifikáciu užívateľov užívateľským menom a heslom.
- Server A prezentuje svoje certifikáty na inicializáciu relácie SSL, keď klienti B a C pristupujú k aplikácii na výpočet sadzieb.
- Po inicializácii relácie SSL server A vyžaduje, aby klienti B a C zadali pred umožnením prístupu k aplikácii na výpočet sadzieb platný názov užívateľa a heslo.

Klientske systémy agentov – Klient B a Klient C
- Klienti B a C sú nezávislí agenti, ktorí pristupujú na aplikáciu na výpočet sadzieb.
- Klientsky softvér Klientov B a C má nainštalovanú kópiu certifikátu všeobecne známej CA, ktorá vystavila certifikát pre túto aplikáciu.
- Klienti B a C pristupujú k aplikácii na výpočet sadzieb na serveri A, ktorý prezentuje svoj certifikát ich klientskemu softvéru na autentifikáciu ich identity a inicializáciu relácie SSL.
- Klientsky softvér na klientoch B a C je nakonfigurovaný na akceptovanie certifikátu zo servera A za účelom inicializácie relácie SSL.
- Po začatí relácie SSL musia klienti B a C poskytnúť platný názov užívateľa a heslo predtým, ako server A povolí prístup k aplikácii.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:
1. Aplikácia na výpočet sadzieb na serveri A je generickou aplikáciou, ktorá môže byť nakonfigurovaná na používanie SSL. Väčšina aplikácií, vrátane množstva serverových aplikácií, poskytuje podporu SSL. Konfiguračné kroky SSL

sa u rôznych aplikácií líšia. Takže tento scenár neposkytuje konkrétne inštrukcie ku konfigurovaniu aplikácie na výpočet sadzieb, aby používala 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 k používaniu Správcu digitálnych certifikátov (DCM) na nakonfigurovanie dôveryhodnosti certifikátu pre 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. Server A vyhovuje požiadavkám na inštaláciu a používanie DCM (Digital Certificate Manager).
4. Na serveri A v minulosti ešte nikto nekonfiguroval ani nepoužíval DCM.
5. Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
6. Server A nemá nainštalovaný šifrovací koprocesor IBM.

Konfiguračné kroky

Ak chcete naimplementovať tento scenár, musíte vykonať na serveri A toto:

1. Vyplniť plánovacie pracovné listy
2. Dokončiť všetky vyžadované kroky na inštaláciu a konfiguráciu všetkých potrebných produktov
3. Na vytvorenie požiadavky na certifikát servera použiť Správcu digitálnych certifikátov (DCM)
4. Nakonfigurovanie aplikácie na používanie SSL (Secure Sockets Layer)
5. V prípade vašej aplikácie pomocou DCM naimportovať a priradiť podpísaný certifikát servera alebo klienta k identifikátoru aplikácie
6. V prípade potreby spustiť aplikáciu v režime SSL
7. **Voliteľné**. Pomocou DCM zadefinovať zoznam dôveryhodných CA na povolenie autentifikácie klienta na základe certifikátov pre aplikácie, ktoré poskytujú túto podporu

Poznámka: Situácia, ktorú opisuje tento scenár, nevyžaduje, aby aplikácia na výpočet sadzieb používala na autentifikáciu klientov certifikáty. 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: Vyplnenie plánovacích pracovných listov

Nasledujúce plánovacie pracovné listy názorne ukazujú informácie, ktoré potrebujete pozbierať a rozhodnutia, ktoré musíte prijať na prípravu implementácie digitálnych certifikátov, ktorú opisuje tento scenár. Ak chcete, aby sa implementácia určite podarila, musíte na všetky požadované položky odpovedať Áno a musíte mať pozbierané všetky požadované informácie predtým, než vykonáte akékoľvek konfiguračné úlohy.

Tabuľka 1. Plánovací pracovný list s požiadavkami na implementáciu certifikátu

Pracovný list s požiadavkami	Odpovede
Máte OS/400 V5R2 (5722-SS1) alebo novší ?	Áno
Je na vašom systéme nainštalovaný Cryptographic Access Provider (5722-AC3)?	Áno
Je na vašom systéme nainštalovaná voľba 34 OS/400 ?	Áno

Tabuľka 1. Plánovací pracovný list s požiadavkami na implementáciu certifikátu (pokračovanie)

Pracovný list s požiadavkami	Odpovede
Je na vašom systéme nainštalovaný IBM HTTP Server for iSeries (5722–DG1) a je spustená inštancia administračného servera ?	Áno
Je vo vašom systéme nakonfigurovaný TCP, aby ste mohli na prístup k DCM používať webový prehliadač a inštanciu administračného servera HTTP ?	Áno
Máte zvláštne oprávnenia *SECADM a *ALLOBJ ?	Áno

Aby ste vykonali konfiguračné úlohy potrebné na vykonanie implementácie, musíte pozbierať nasledujúce informácie o implementácii vašich digitálnych certifikátov:

Tabuľka 2. Plánovací pracovný list pre konfiguráciu implementácie certifikátov

Plánovací pracovný list pre server A	Odpovede
Budete prevádzkovať vašu vlastnú lokálnu CA alebo budete certifikáty pre vaše aplikácie získavať od verejnej CA ?	Získanie certifikátu od verejnej CA
Hosťuje server A aplikácie, ktoré chcete povoliť pre SSL?	Áno
Ktoré informácie o DN použijete pre CSR (certificate signing request), na vytvorenie ktorého používate DCM ? • **Veľkosť kľúča**: určuje silu šifrovacích kľúčov pre certifikát. • **Štítok certifikátu**: identifikuje certifikát pomocou jedinečného znakového reťazca. • **Bežný názov**: identifikuje vlastníka certifikátu, napríklad osobu, entitu alebo aplikáciu; súčasť DN predmetu tohto certifikátu. • **Organizačná jednotka**: identifikuje organizačnú sekciu alebo oblasť pre aplikáciu, ktorá bude používať tento certifikát. • **Názov organizácie**: identifikuje vašu spoločnosť alebo oddelenie pre aplikáciu, ktorá bude používať tento certifikát. • **Lokalita alebo mesto**: identifikuje vaše mesto alebo označenie lokality pre vašu organizáciu. • **Štát alebo provincia**: identifikuje štát alebo provinciu, v ktorej budete používať tento certifikát. • **Krajina alebo región**: pomocou označenia, zloženého z dvoch písmen, identifikuje krajinu alebo región, kde budete používať tento certifikát.	**Veľkosť kľúča**: 1024 **Štítok certifikátu**: Myco_public_cert **Bežný názov**: myco_rate_server@myco.com **Organizačná jednotka**: Rate dept **Názov organizácie**: myco **Lokalita alebo mesto**: Any_city **Štát alebo provincia**: Any **Krajina alebo región**: ZZ
Aké je ID aplikácie DCM pre aplikáciu, ktorú chcete nakonfigurovať na používanie SSL ?	mcyo_agent_rate_app
Nakonfigurujete aplikáciu, povolenú pre SSL, na používanie certifikátov na autentifikáciu klienta ? Ak áno, ktoré Certifikačné autority chcete pridať do zoznamu CA, ktorým táto aplikácia dôveruje ?	Nie

Krok 2: Dokončite nevyhnutné úlohy na inštaláciu všetkých potrebných produktov

Aby ste mohli vykonávať špecifické konfiguračné úlohy na implementáciu tohto scenára, musíte dokončiť všetky nevyhnutné úlohy na inštaláciu a konfiguráciu všetkých potrebných produktov.

Krok 3: Vytvorenie požiadavky na certifikát servera alebo klienta

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 **Create New Certificate Store**, aby sa spustila úloha a mohli ste vyplniť sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia skladu 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 sklad certifikátov, ktorý sa má vytvoriť a kliknite na **Continue**.
4. Vyberte **Yes**, aby sa certifikát vytvoril ako časť vytvárania skladu certifikátov *SYSTEM a kliknite na **Continue**.
5. Ako podpisovateľa nového certifikátu vyberte **VeriSign or other Internet Certificate Authority (CA)** a kliknite na **Continue**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačnú informácie pre nový certifikát.
6. Vyplňte formulár a kliknite na **Continue**, 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) sa skladajú z verejného kľúča, charakteristického názvu (DN) a ďalších informácií, 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. **Poznámka:** Ak túto stránku ukončíte, tieto údaje sa stratia a nemôžete ich 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 skladu certifikátov *SYSTEM a priradiť ho vašej aplikácii na použitie pre SSL.

Krok 4: Konfigurácia aplikácie na používanie SSL

Keď prijmete váš podpísaný certifikát späť z verejnej certifikačnej autority (CA), môžete pokračovať v procese aktivovania komunikácií SSL (Secure Sockets Layer) pre vašu verejnú aplikáciu. Vašu aplikáciu musíte nakonfigurovať na používanie SSL predtým, než začnete pracovať s vaším podpísaným certifikátom. Niektoré aplikácie, napríklad HTTP Server for iSeries, generujú jedinečné ID aplikácie a registrujú toto ID pomocou Správcu digitálnych certifikátov (DCM), keď túto aplikáciu nakonfigurujete 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 konkrétny zdroj pre aplikáciu na výpočet sadzieb, ktorú opisuje, pretože existuje veľa spôsobov, ktorými môže spoločnosť MyCo, Inc. poskytnúť túto aplikáciu svojim agentom.

| Na nakonfigurovanie vašej aplikácie na používanie SSL postupujte podľa inštrukcií, ktoré poskytne dokumentácia vašej
| aplikácie. O konfigurovaní mnohých bežných aplikácií IBM na používanie SSL sa dozviete viac aj v téme Secure
| Sockets Layer (SSL) v Informačnom centre iSeries.

| Keď pre vašu aplikáciu konfigurujete SSL, môžete pre túto aplikáciu nakonfigurovať podpísaný verejný certifikát, takže
| bude môcť iniciovať relácie SSL.

Krok 5: Importovanie a priradenie podpísaného verejného certifikátu

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 **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
3. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte heslo, ktoré ste uviedli pre sklad certifikátov pri jeho vytváraní a kliknite na **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Import certificate**, aby sa spustil proces importu podpísaného certifikátu do skladu 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 **Manage Certificates** vyberte **Assign certificate** na zobrazenie zoznamu certifikátov pre aktuálny sklad certifikátov.
7. Vyberte z tohto zoznamu váš certifikát a kliknite na **Assign to Applications**, čím zobrazíte zoznam definícií aplikácií pre aktuálny sklad certifikátov.
8. Vyberte vašu aplikáciu zo zoznamu a kliknite na **Continue**. 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 6: Spustenie aplikácie 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.

Ak chcete na autentifikáciu klienta používať certifikáty, pre túto aplikáciu môžete teraz zadefinovať zoznam dôveryhodných CA.

Krok 7 (Voliteľný): Zadefinovanie zoznamu dôveryhodných CA pre aplikáciu, ktorá vyžaduje certifikáty na autentifikáciu klienta

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 opisuje tento scenár, nevyžaduje, aby aplikácia na výpočet sadzieb používala na autentifikáciu klienta certifikáty, ale aby táto aplikácia bola schopná akceptovať certifikáty na autentifikáciu, keď sú k dispozícii. Mnohé aplikácie poskytujú podporu certifikátov na autentifikáciu klienta; ako túto podporu nakonfigurujete, sa v rámci aplikácií výrazne odlišuje. 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 validáciu.

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

1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
3. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte heslo, ktoré ste uviedli pre sklad certifikátov pri jeho vytváraní a kliknite na **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Set CA status** 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. Zo zoznamu vyberte jeden alebo viac certifikátov CA, ktorým bude vaša aplikácia dôverovať a kliknite na **Enable**, čím zobrazíte zoznam aplikácií, ktoré používajú zoznam dôveryhodných CA.
7. Z tohto zoznamu vyberte aplikáciu, pre ktorú treba do jej zoznamu dôveryhodných CA pridať vybratú 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: Používanie certifikátov na internú autentifikáciu

Situácia

Ste správca siete v spoločnosti (MyCo, Inc.), ktorej oddelenie ľudských zdrojov má na starosti napríklad právne materiály a záznamy o súkromí. Zamestnanci spoločnosti žiadali, aby boli schopní pristupovať online ku svojim informáciám o osobných výhodách a starostlivosti o zdravie. Spoločnosť na túto požiadavku odpovedala vytvorením internej webovej stránky, aby zamestnancom poskytla tieto informácie. Vy ste zodpovedný za správu tejto internej webovej stránky, ktorá beží na serveri IBM HTTP Server for iSeries (založený na Apache).

Pretože sa zamestnanci nachádzajú v dvoch geograficky oddelených úradoch a niektorí zamestnanci často cestujú, obávate sa o udržanie utajenia týchto informácií, keďže prechádzajú internetom. Užívateľov autentifikujete aj tradične, pomocou mena užívateľa a hesla, aby ste obmedzili prístup k firemným údajom. Pretože sú tieto údaje citlivé a súkromné, uvedomujete si, že obmedzenie prístupu k nim na základe autentifikácie pomocou hesla pravdepodobne nebude 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 pristupovať.

Z toho dôvodu ste sa rozhodli nastaviť súkromnú lokálnu certifikačnú autoritu (CA), vydať certifikáty všetkým zamestnancom a nechať zamestnancov priradiť ich certifikáty svojim užívateľským profilom. 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 k nim pristupovať len určité osoby.

Výhody scenára

Tento scenár má nasledovné výhody:

- Používanie digitálnych certifikátov na konfiguráciu prístupu SSL na váš webový server ľudských zdrojov zabezpečuje, že informácie, prenášané medzi týmto serverom a klientom, sú chránené a súkromné.
- Použitie digitálnych certifikátov na autentifikáciu klientov poskytuje bezpečnejšiu metódu identifikovania autorizovaných užívateľov.
- Používanie *súkromných* digitálnych certifikátov na autentifikáciu užívateľov pristupujúcich k vašim aplikáciám a údajom, je praktickou voľbou za týchto alebo podobných podmienok:
  - Požadujete vysoký stupeň bezpečnosti, hlavne s ohľadom na autentifikáciu užívateľov.

  - Dôverujete jedincom, ktorým vydávate certifikáty.
  - Vaši užívatelia už majú užívateľské profily na riadenie svojho prístupu k aplikáciám a údajom.
  - Chcete prevádzkovať vlastnú Certifikačnú autoritu (CA).
- Používanie súkromných certifikátov na autentifikáciu klienta vám umožňuje jednoduchšie priradenie certifikátu autorizovanému užívateľskému profilu. Toto združenie certifikátu s užívateľským profilom umožňuje serveru HTTP zistiť užívateľský profil vlastníka certifikátu počas autentifikácie. Server HTTP môže teda prejsť naň a bežať pod týmto užívateľským profilom alebo vykonávať akcie pre tohto užívateľa na základe informácií v užívateľskom profile.

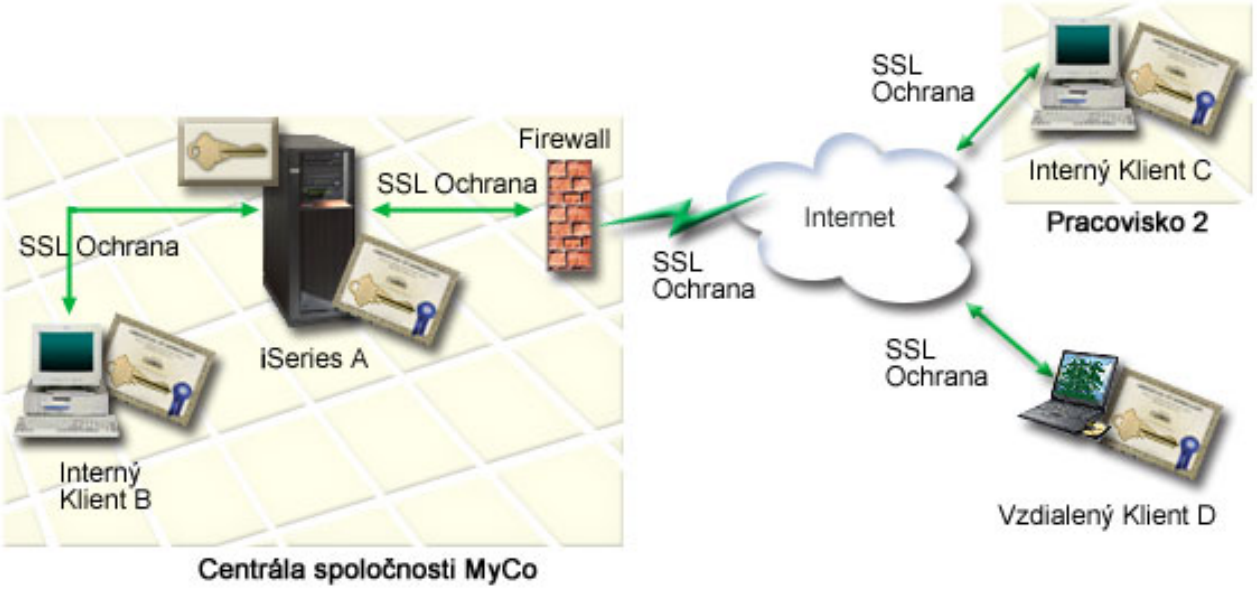
Ciele

V tomto scenári chce spoločnosť MyCo, Inc. používať digitálne certifikáty na ochranu citlivých osobných informácií, ktoré poskytuje jej interná webová stránka ľudských zdrojov zamestnancom spoločnosti. Táto spoločnosť chce aj bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolený prístup k tejto webovej stránke.

Ciele tohto scenára sú nasledovné:
- Interná webová stránka ľudských zdrojov tejto spoločnosti musí na ochranu súkromia tých údajov, ktoré poskytuje užívateľom, používať SSL.
- Konfigurácia SSL musí byť uskutočnená so súkromnými certifikátmi z internej lokálnej certifikačnej autority (CA).
- Autorizovaní užívatelia musia na prístup k webovej stránke ľudských zdrojov v režime SSL poskytnúť platný certifikát.

Detaily

Nasledujúci obrázok zobrazuje konfiguráciu siete v tomto scenári:



Obrázok ilustruje nasledujúce informácie o situácii pre tento scenár:

Webový server ľudských zdrojov spoločnosti – Server A
- Server A je server, ktorý hostuje webovú aplikáciu ľudských zdrojov vašej spoločnosti.
- Na serveri A beží OS/400 Verzia 5 Vydanie 2 (V5R2) alebo novšia verzia.
- Server A má nainštalovaný Cryptographic Access Provider (5722–AC3).
- Na serveri A sú nainštalované a nakonfigurované programy Digital Certificate Manager (OS/400 voľba 34) a IBM HTTP Server for iSeries (5722–DG1).
- Na serveri A beží aplikácia 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.
- Server A prezentuje svoj certifikát na inicializáciu relácie SSL, keď klienti B, C a D pristupujú k aplikácii.
- Po inicializácii relácie SSL server A vyžaduje, aby klienti B, C a D poskytli pred povolením prístupu k aplikácii ľudských zdrojov platný certifikát. 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 spoločnosti MyCo, kde sa nachádza aj server 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, často cestuje na služobné cesty a musí mať možnosť bezpečného prístupu na webovú 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 k aplikácii ľudských zdrojov na serveri A, ktorý prezentuje svoje certifikáty ich klientskemu softvéru na overenie jeho identity a inicializáciu relácie SSL.
- Klientsky softvér na klientoch B, C a D je nakonfigurovaný na akceptovanie certifikátu zo servera A a relácia SSL začína.
- Po začatí relácie SSL klienti B, C a D musia poskytnúť platný certifikát predtým, ako server A povolí prístup k aplikácii a jej prostriedkom.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:
1. IBM HTTP Server for iSeries (založený na Apache) spúšťa aplikáciu ľudských zdrojov na serveri A. Tento scenár neposkytuje *špecifické* pokyny na konfiguráciu HTTP servera 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 k používaniu Správcu digitálnych certifikátov (DCM) na nakonfigurovanie požiadaviek na manažovanie certifikátov v tomto scenári. Avšak tento scenár neposkytuje *presné* inštrukcie pre konfiguráciu autentifikácie klienta certifikátom pre server HTTP.
3. HTTP server ľudských zdrojov na serveri A už používa autentifikáciu pomocou hesla.
4. Server A vyhovuje požiadavkám na inštaláciu a používanie DCM (Digital Certificate Manager).
5. Na serveri A v minulosti ešte nikto nekonfiguroval ani nepoužíval DCM.
6. Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
7. Server A nemá nainštalovaný šifrovací koprocesor IBM.

Konfiguračné kroky

Existujú dve skupiny úloh, ktoré musíte pri implementáciu tohto scenára dokončiť: Jedna skupina úloh vám umožňuje nastaviť aplikáciu ľudských zdrojov na serveri A na používanie SSL a vyžaduje certifikáty na autentifikáciu užívateľa. 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 webového servera ľudských zdrojov

Ak chcete naimplementovať tento scenár, musíte vykonať na serveri A toto:
1. Vyplniť plánovacie pracovné listy tohto scenára
2. Dokončiť všetky vyžadované kroky na inštaláciu a konfiguráciu všetkých potrebných produktov
3. Nakonfigurovať server HTTP ľudských zdrojov tak, aby používal SSL a poznamenať si ID aplikácie pre inštanciu tohto servera
4. Na vytvorenie a prevádzkovanie lokálnej CA použiť Správcu digitálnych certifikátov (DCM)
5. Nakonfigurovať autentifikáciu klienta pre webový server ľudských zdrojov.
6. Spustenie servera HTTP ľudských zdrojov v režime SSL .

Kroky úloh konfigurácie klientov

Ak chcete naimplementovať tento scenár, každý užívateľ (klienti B, C a D) ktorý bude pristupovať na webový server ľudských zdrojov na serveri A musí vykonať toto:

7. Nainštalovať kópiu certifikátu lokálnej CA do softvéru svojho prehliadača
8. Vyžiadať certifikát od lokálnej CA

Podrobnosti konfigurácie

Ak chcete použiť certifikáty na nakonfigurovanie chráneného prístupu SSL k interným aplikáciám a prostriedkom a na autentifikáciu užívateľov tak, ako to opisuje tento scenár, vykonajte nasledujúce kroky úloh.

Krok 1: Vyplnenie plánovacích pracovných listov

Nasledujúce plánovacie pracovné listy názorne ukazujú informácie, ktoré potrebujete pozbierať a rozhodnutia, ktoré musíte prijať na prípravu implementácie digitálnych certifikátov, ktorú opisuje tento scenár. Ak chcete, aby sa implementácia určite podarila, musíte na všetky požadované položky odpovedať Áno a musíte mať pozbierané všetky požadované informácie predtým, než vykonáte akékoľvek konfiguračné úlohy.

Tabuľka 3. Plánovací pracovný list s požiadavkami na implementáciu certifikátu

Pracovný list s požiadavkami	**Odpovede**
Máte OS/400 V5R2 (5722-SS1) alebo novší ?	Áno
Je na vašom systéme nainštalovaný Cryptographic Access Provider (5722-AC3)?	Áno
Je na vašom systéme nainštalovaná voľba 34 OS/400 ?	Áno
Je na vašom systéme nainštalovaný IBM HTTP Server for iSeries (5722–DG1) a je spustená inštancia administračného servera ?	Áno
Je vo vašom systéme nakonfigurovaný TCP, aby ste mohli na prístup k DCM používať webový prehliadač a inštanciu administračného servera HTTP ?	Áno
Máte zvláštne oprávnenia *SECADM a *ALLOBJ ?	Áno

Na vykonanie konfiguračných úloh, potrebných na vykonanie implementácie, musíte pozbierať nasledujúce informácie o implementácii vašich digitálnych certifikátov:

Tabuľka 4. Plánovací pracovný list pre konfiguráciu implementácie certifikátov

Plánovací pracovný list pre server A	**Odpovede**
Budete prevádzkovať vašu vlastnú lokálnu CA alebo budete certifikáty pre vaše aplikácie získavať od verejnej CA ?	Vytvorenie lokálnej CA na vystavovanie certifikátov
Hosťuje server A aplikácie, ktoré chcete povoliť pre SSL?	Áno

Tabuľka 4. Plánovací pracovný list pre konfiguráciu implementácie certifikátov (pokračovanie)

Plánovací pracovný list pre server A	Odpovede
Ktoré informácie o DN použijete pre túto lokálnu CA ? • **Veľkosť kľúča**: určuje silu šifrovacích kľúčov pre certifikát. • **Názov Certifikačnej autority (CA)**: identifikuje CA a stane sa bežným názvom pre certifikát CA a charakteristickým názvom Vystavovateľa pre certifikáty, ktoré táto CA vystavuje. • **Organizačná jednotka**: identifikuje organizačnú sekciu alebo oblasť pre aplikáciu, ktorá bude používať tento certifikát. • **Názov organizácie**: identifikuje vašu spoločnosť alebo oddelenie pre aplikáciu, ktorá bude používať tento certifikát. • **Lokalita alebo mesto**: identifikuje vaše mesto alebo označenie lokality pre vašu organizáciu. • **Štát alebo provincia**: identifikuje štát alebo provinciu, v ktorej budete používať tento certifikát. • **Krajina alebo región**: pomocou označenia, zloženého z dvoch písmen, identifikuje krajinu alebo región, kde budete používať tento certifikát. • **Doba platnosti Certifikačnej autority**: špecifikuje počet dní, počas ktorých je certifikát Certifikačnej autority platný.	**Veľkosť kľúča**: 1024 **Názov Certifikačnej autority (CA)**: Myco_CA@myco.com **Organizačná jednotka**: Rate dept **Názov organizácie**: myco **Lokalita alebo mesto**: Any_city **Štát alebo provincia**: Any **Krajina alebo región**: ZZ **Doba platnosti Certifikačnej autority**: 1095
Chcete nastaviť údaje politiky pre lokálnu CA, aby mala povolené vystavovať užívateľské certifikáty na autentifikáciu klienta ?	Áno
Ktoré informácie o DN použijete pre certifikát servera, ktorý vystavuje lokálna CA ? • **Veľkosť kľúča**: určuje silu šifrovacích kľúčov pre certifikát. • **Štítok certifikátu**: identifikuje certifikát pomocou jedinečného znakového reťazca. • **Bežný názov**: identifikuje vlastníka certifikátu, napríklad osobu, entitu alebo aplikáciu; súčasť DN predmetu tohto certifikátu. • **Organizačná jednotka**: identifikuje organizačnú sekciu alebo oblasť pre aplikáciu, ktorá bude používať tento certifikát. • **Názov organizácie**: identifikuje vašu spoločnosť alebo oddelenie pre aplikáciu, ktorá bude používať tento certifikát. • **Lokalita alebo mesto**: identifikuje vaše mesto alebo označenie lokality pre vašu organizáciu. • **Štát alebo provincia**: identifikuje štát alebo provinciu, v ktorej budete používať tento certifikát. • **Krajina alebo región**: pomocou označenia, zloženého z dvoch písmen, identifikuje krajinu alebo región, kde budete používať tento certifikát.	**Veľkosť kľúča**: 1024 **Štítok certifikátu**: Myco_public_cert **Bežný názov**: myco_rate_server@myco.com **Organizačná jednotka**: Rate dept **Názov organizácie**: myco **Lokalita alebo mesto**: Any_city **Štát alebo provincia**: Any **Krajina alebo región**: ZZ
Aké je ID aplikácie DCM pre aplikáciu, ktorú chcete nakonfigurovať na používanie SSL ?	mcyo_agent_rate_app
Nakonfigurujete aplikáciu, povolenú pre SSL, na používanie certifikátov na autentifikáciu klienta ? Ak áno, ktoré Certifikačné autority chcete pridať do zoznamu CA, ktorým táto aplikácia dôveruje ?	Áno Myco_CA@myco.com

Krok 2: Dokončite nevyhnutné úlohy na inštaláciu všetkých potrebných produktov

Aby ste mohli vykonávať špecifické konfiguračné úlohy na implementáciu tohto scenára, musíte dokončiť všetky nevyhnutné úlohy na inštaláciu a konfiguráciu všetkých potrebných produktov.

Krok 3: Konfigurácia servera HTTP ľudských zdrojov na používanie SSL

| Konfigurácia SSL (Secure Sockets Layer) pre HTTP server ľudských zdrojov (založený na Apache) na serveri A zahŕňa
| množstvo úloh, ktoré závisia od aktuálnej konfigurácie vášho servera.

| Ak chcete server nakonfigurovať na používanie SSL, postupujte takto:
| 1. Spustite administračné rozhranie servera HTTP.
| 2. Ak chcete pracovať s konkrétnym serverom HTTP, na zobrazenie zoznamu všetkých nakonfigurovaných serverov HTTP vyberte na stránke tieto záložky **Manage —> All Servers —> All HTTP Servers** .
| 3. Zo zoznamu vyberte príslušný server a kliknite na **Manage Details**.
| 4. V navigačnom rámci vyberte **Security**.
| 5. Vo formulári vyberte záložku **SSL with Certificate Authentication**.
| 6. V poli **SSL** vyberte Enabled.
| 7. V poli **Server certificate application name** uveďte ID aplikácie, pod ktorým je známa inštancia tohto servera. Môžete ho vybrať aj zo zoznamu. Toto ID aplikácie je v tvare QIBM_HTTP_SERVER_[názov_servera], napríklad QIBM_HTTP_SERVER_MYCOTEST. **Poznámka:** Zapamätajte si toto ID aplikácie. Budete ho musieť znova vybrať v DCM.

| O celkovej konfigurácii, potrebnej pre váš server HTTP na používanie SSL, sa dozviete v téme Informácie o HTTP
| Server for iSeries, najmä v príklade, nazývanom Scenár: spoločnosť JKL povoľuje ochranu SSL (Secure Sockets Layer) na svojom serveri HTTP (založenom na Apache). Tento scenár poskytuje všetky kroky úloh pre vytvorenie virtuálneho hostiteľa a jeho nakonfigurovanie na používanie SSL, vrátane nasledujúcich úloh:
| 1. Nastavenie názvového virtuálneho hostiteľa.
| 2. Nastavenie direktívy Listen pre virtuálneho hostiteľa.
| 3. Nastavenie adresárov virtuálneho hostiteľa.
| 4. Nastavenie ochrany hesla pomocou základnej autentifikácie.
| 5. Povolenie SSL pre virtuálneho hostiteľa.

Ďalšie informácie o konfigurovaní aktuálnej aj budúcej verzie aplikácie HTTP Server for iSeries nájdete v téme HTTP Server for iSeries.

| Keď konfigurujete server HTTP na používanie SSL, môžete pomocou DCM nakonfigurovať podporu certifikátov, ktorú
| potrebujete pre SSL a autentifikáciu klienta.

Krok 4: Vytvorenie a prevádzkovanie lokálnej 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 pre server.

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. Toto zahrňuje priradenie certifikátu, ktorý lokálna CA vystavuje pre aplikáciu vášho webového servera. Lokálnu CA pridajte aj do zoznamu dôveryhodných CA tejto aplikácie webového servera. Prítomnosť lokálnej CA v zozname dôveryhodných CA aplikácie zabezpečí, že aplikácia bude môcť rozoznať a autentifikovať užívateľov, ktorí predložia certifikát vydaný lokálnou 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 **Create a Certificate Authority**, 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. Pri používaní týchto formulárov na vykonávanie všetkých úloh, potrebných pre nastavenie funkčnej lokálnej Certifikačnej autority (CA), postupujte nasledovne:
   a. Poskytnite identifikačné informácie pre lokálnu CA.
   b. Nainštalujte certifikát lokálnej CA na vaše 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 serverového 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 sklad certifikátov *OBJECTSIGNING; toto je sklad certifikátov, ktorý používate na manažovanie certifikátov, podpisujúcich objekty.

      Poznámka: Aj keď tento scenár nepoužíva certifikáty na podpisovanie objektov, určite dokončite tento krok. Ak úlohu v tomto bode prerušíte, táto úloha skončí a na vykonanie konfigurácie vášho certifikátu SSL musíte vykonať osobitné úlohy.
   g. Vyberte aplikácie, ktoré budú dôverovať lokálnej CA.

      Poznámka: Nezabudnite vybrať ID aplikácie pre váš server HTTP ľudských zdrojov, napríklad QIBM_HTTP_SERVER_MYCOTEST, ako jednu z aplikácií, ktoré dôverujú lokálnej CA.

Pri vykonávaní konfigurácie certifikátu, ktorý aplikácia vášho webového servera vyžaduje na používanie SSL, môžete webový server nakonfigurovať tak, aby na autentifikáciu užívateľov vyžadoval certifikáty.

Krok 5: Konfigurácia autentifikácie klienta pre webový server ľudských zdrojov

Keď určíte, že tento server HTTP vyžaduje na autentifikáciu certifikáty, musíte preň nakonfigurovať všeobecné nastavenia autentifikácie. Tieto nastavenia nakonfigurujte v rovnakom bezpečnostnom formulári, aký ste použili na konfiguráciu servera na používanie SSL (Secure Sockets Layer).

Ak chcete tento server nakonfigurovať tak, aby vyžadoval certifikáty na autentifikáciu klienta, postupujte nasledovne:

1. Spustite administračné rozhranie servera HTTP.
2. Ak chcete pracovať s konkrétnym serverom HTTP, na zobrazenie zoznamu všetkých nakonfigurovaných serverov HTTP vyberte na stránke tieto záložky **Manage —> All Servers —> All HTTP Servers** .
3. Zo zoznamu vyberte príslušný server a kliknite na **Manage Details**.
4. V navigačnom rámci vyberte **Security**.
5. Vo formulári vyberte záložku **Authentication**.
6. Vyberte **Use OS/400 profile of client**.
7. V poli **Authentication name or realm** uveďte názov pre oblasť autorizácie.
8. V poli **Process requests using client's authority** vyberte Enabled a kliknite na **Apply**.
9. Vo formulári vyberte záložku **Control Access**.
10. Vyberte **All authenticated users (valid user name and password)** a kliknite na **Apply**.
11. Vo formulári vyberte záložku **SSL with Certificate Authentication**.
12. Zabezpečte, aby v poli **SSL** bola vybratá hodnota Enabled.
13. Zabezpečte, aby v poli **Server certificate application name** bola špecifikovaná správna hodnota, napríklad QIBM_HTTP_SERVER_MYCOTEST.
14. Vyberte **Accept client certificate if available before making connection**. Kliknite na OK.

O celkovej konfigurácii, potrebnej pre váš server HTTP na používanie SSL, sa dozviete v téme Informácie o HTTP Server for iSeries, najmä v príklade, nazývanom Scenár: spoločnosť JKL povoľuje ochranu SSL (Secure Sockets Layer) na svojom serveri HTTP (založenom na Apache). Tento scenár poskytuje všetky kroky úloh pre vytvorenie virtuálneho hostiteľa a jeho nakonfigurovanie na použitie SSL.

Pri vykonávaní konfigurácie autentifikácie klienta môžete server HTTP znova spustiť v režime SSL a začať s ochranou súkromia údajov aplikácie ľudských zdrojov.

Krok 6: Spustenie webového servera 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.

Ak chcete zastaviť a spustiť server HTTP (založený na Apache), postupujte nasledovne:
1. V aplikácii **iSeries Navigator** rozviňte váš server.
2. Rozviňte **Network > Servers > TCP/IP > HTTP Administration**.
3. Kliknite na **Start**, čím spustíte administračné rozhranie servera HTTP.
4. Ak chcete zobraziť zoznam všetkých nakonfigurovaných serverov HTTP, kliknite na záložku **Manage**.
5. Zo zoznamu vyberte príslušný server a ak tento server beží, kliknite na **Stop**.
6. Ak chcete tento server znova spustiť, kliknite na **Start**. Viac informácií o parametroch spustenia získate v online pomoci.

Ďalšie informácie o manažovaní aktuálnej a budúcej verzie aplikácie HTTP Server for iSeries (originálny alebo založený na Apache) nájdete v téme HTTP Server for iSeries.

Skôr než užívatelia pristúpia k webovej aplikácii ľudských zdrojov, musia si najprv do softvéru svojho prehliadača nainštalovať kópiu certifikátu lokálnej CA.

Krok 7: Nechať užívateľov nainštalovať kópiu certifikátu lokálnej CA do softvéru ich 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 tento server predloží certifikát od verejnej internetovej CA, softvér užívateľovho prehliadača alebo iný klientsky softvér musí už mať kópiu certifikátu tejto 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 **Install Local CA Certificate on Your 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. Tým sa zabezpečí, že váš prehliadač môže vytvárať relácie bezpečných komunikácií s webovými servermi, ktoré používajú certifikát od tejto CA. Váš prehliadač zobrazí sériu okien, ktoré vám pomôžu dokončiť inštaláciu.
4. Kliknite na **OK** na návrat na domovskú stránku Správcu digitálnych certifikátov.

Aby teraz užívatelia mohli pristupovať na webový server ľudských zdrojov v režime SSL, musia byť schopní tomuto serveru predložiť príslušný certifikát na autentifikáciu. Musia teda získať užívateľský certifikát od lokálnej CA.

Krok 8: Nechať každého užívateľa vyžiadať certifikát od lokálnej CA

V predchádzajúcich krokoch ste webový server ľudských zdrojov nakonfigurovali tak, aby na autentifikáciu užívateľov vyžadoval certifikáty. Užívatelia musia teraz pred povolením prístupu na webový server predkladať platný certifikát od

lokálnej CA. Každý užívateľ musí použiť Správcu digitálnych certifikátov (DCM) na získanie certifikátu prostredníctvom úlohy **Create Certificate**. 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 **Create Certificate**.
3. Ako typ certifikátu na vytvorenie vyberte **User certificate**. Zobrazí sa formulár, na ktorom môžete zadať identifikačné informácie pre certifikát.
4. Vyplňte formulár a kliknite na **Continue**.

   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 priradí certifikát vášmu užívateľskému profilu.

Po vykonaní týchto úloh môžu k údajom na webovom serveri ľudských zdrojov pristupovať len autorizovaní užívatelia s platným certifikátom a tieto údaje počas prenosu chráni SSL.

Kapitola 5. Pojmy digitálnych certifikátov

Než začnete používať digitálne certifikáty na vylepšenie vášho systému a politiky sieťovej bezpečnosti, musíte pochopiť ich podstatu a akým prínosom sú pre bezpečnosť.

Digitálny certifikát predstavuje digitálne povoľovacie údaje, ktoré validujú vlastníka certifikátu viac ako heslo. Identifikačné informácie, ktoré poskytuje digitálny certifikát, sú známe ako charakteristický názov predmetu. Dôveryhodná strana, nazývaná Certifikačná autorita (CA), vystavuje digitálne certifikáty užívateľom alebo organizáciám. Dôvera v CA je základom dôvery v certifikát ako zdroj platných povoľovacích údajov.

Digitálny certifikát obsahuje aj verejný kľúč, ktorý je súčasťou páru, zloženého z verejného a súkromného kľúča. Celý rad bezpečnostných funkcií sa spolieha na používanie digitálnych certifikátov a k nim priradených párov kľúčov. Digitálne certifikáty môžete použiť na konfigurovanie relácií SSL (Secure Sockets Layer), aby ste zaistili súkromné a bezpečné komunikácie medzi užívateľmi a vašimi serverovými aplikáciami. Túto bezpečnosť môžete rozšíriť nakonfigurovaním mnohých aplikácií povolených pre SSL tak, aby na bezpečnejšiu autentifikáciu užívateľa vyžadovali certifikát namiesto mena užívateľa a hesla.

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

Rozšírenia certifikátov
V týchto informáciách sa dozviete, čo sú polia rozšírenia certifikátov a ako sa používajú.

Obnovenie platnosti certifikátov
V týchto informáciách sa dozviete o postupe, ktorý DCM používa na obnovenie platnosti serverových a klientskych certifikátov a certifikátov na podpisovanie objektov.

Rozoznaný názov
V týchto informáciách sa dozviete o identifikačných vlastnostiach 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
V týchto informáciách sa dozviete o bezpečnostných kľúčoch, priradených k digitálnym certifikátom.

Certifikačná autorita (CA)
V týchto informáciách sa dozviete o Certifikačných autoritách (CA), čo sú entity, ktoré vystavujú digitálne certifikáty.

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

Sklady certifikátov
V týchto informáciách sa dozviete o tom, čo to je sklad 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.

Koprocesory **IBM Cryptographic Coprocessor for iSeries**
V týchto informáciách sa dozviete, ako môžete používať DCM a šifrovacie koprocesory IBM na bezpečnejšie uloženie kľúčov.

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

Definície aplikácií
V týchto informáciách sa dozviete, čo sú definície aplikácií DCM a ako sa má s nimi pracovať v prípade konfigurácie SSL a podpisovania objektov.

Overenie platnosti
V týchto informáciách sa dozviete, ako funguje v DCM proces overovania platnosti v prípade aplikácií a certifikátov.

Rozšírenia certifikátov

Rozšírenia certifikátov sú informačné polia, ktoré poskytujú ďalšie informácie o certifikáte. Rozšírenia certifikátov poskytujú spôsob rozšírenia informačných štandardov originálneho certifikátu X.509. Kým v prípade niektorých rozšírení sa informácie poskytujú na rozšírenie identifikačných informácií pre certifikát, iné rozšírenia poskytujú informácie o šifrovacích schopnostiach certifikátu.

Nie všetky certifikáty používajú polia rozšírenia na rozšírenie charakteristického názvu a ďalších informácií. Počet a typ polí rozšírenia, ktoré certifikát používa, sa mení v rámci entít CA, ktoré vystavujú certifikáty.

Napríklad lokálna CA, ktorú poskytuje Správca digitálnych certifikátov (DCM), vám umožňuje používať len rozšírenia certifikátu Alternatívneho názvu subjektu. Tieto rozšírenia vám umožňujú priradiť k certifikátu konkrétnu IP adresu, plne kvalifikovaný názov domény alebo e-mailovú adresu. Ak chcete certifikát používať na identifikáciu koncového bodu pripojenia virtuálnej súkromnej siete (VPN), musíte zadať informácie pre tieto rozšírenia.

Obnovenie platnosti certifikátov

Proces obnovenia platnosti certifikátu, ktorý používa Správca digitálnych certifikátov (DCM), sa líši podľa typu Certifikačnej autority (CA), ktorá vystavila tento certifikát.

Ak na podpísanie certifikátu s obnovenou platnosťou použijete lokálnu CA, DCM použije vami poskytnuté informácie na vytvorenie nového certifikátu v aktuálnom sklade certifikátov a predchádzajúci certifikát si ponechá.

Ak na vystavenie certifikátu použijete všeobecne známu internetovú CA, obnovenie platnosti certifikátu môžete spracovať jedným z nasledujúcich spôsobov: certifikát s obnovenou platnosťou môžete naimportovať zo súboru, ktorý dostanete od podpisujúcej CA alebo necháte Správcu digitálnych certifikátov (DCM) vytvoriť pre tento certifikát nový pár kľúčov, zložený z verejného a súkromného kľúča. DCM poskytuje prvú možnosť v prípade, ak uprednostníte obnovenie platnosti certifikátu priamo Certifikačnou autoritou, ktorá ho vystavila.

Ak sa rozhodnete vytvoriť nový pár kľúčov, DCM spracuje obnovenie platnosti rovnakým spôsobom ako spracoval vytvorenie tohto certifikátu. DCM vytvorí pre certifikát s obnovenou platnosťou nový pár verejného a súkromného kľúča a vygeneruje CSR (Certificate Signing Request), ktorý sa skladá z verejného kľúča a ďalších informácií, ktoré poskytnete pre nový certifikát. CSR môžete použiť na vyžiadanie nového certifikátu od certifikačnej autority VeriSign alebo inej verejnej CA. Keď dostanete od CA podpísaný certifikát, pomocou DCM naimportujte tento certifikát do príslušného skladu certifikátov. Sklad certifikátov bude potom obsahovať obe kópie certifikátu, pôvodného aj novovystaveného certifikátu s obnovenou platnosťou.

Ak rozhodnete, že DCM nemá vygenerovať nový pár kľúčov, DCM vás prevedie procesom importovania podpísaného certifikátu s obnovenou platnosťou do skladu certifikátov z existujúceho súboru, ktorý ste dostali od CA. Naimportovaný certifikát s obnovenou platnosťou tak nahradí predchádzajúci certifikát.

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). Takže ak plánujete akceptovať a používať certifikáty ako oprávnenia, musíte si znova pozrieť identifikačné požiadavky pre CA, aby ste zistili, či sú ich požiadavky v súlade s vašimi bezpečnostnými potrebami.

DN (Distinguished name) je pojem, ktorý opisuje informácie o identifikácii v certifikáte a je súčasťou samotného certifikátu. Certifikát obsahuje informácie o DN v prípade vlastníka certifikátu aj žiadateľa o certifikát (nazýva sa DN predmetu) a v prípade CA, ktorá vystavuje certifikát (nazýva sa DN vystavovateľa). V závislosti na identifikačnej politiky CA, ktorá vydáva certifikát, DN môže obsahovať rôzne 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
- Lokalita alebo mesto
- Štát alebo provincia
- Krajina alebo región

Keď používate DCM na vystavovanie súkromných certifikátov, môžete použiť rozšírenia certifikátov, čím poskytnete pre certifikát ďalšie informácie o DN, vrátane:

- IP adresa verzie 4
- Plne kvalifikovaný názov domény
- E-mailová adresa

Tieto ďalšie informácie sú užitočné v prípade, že plánujete použiť tento certifikát na nakonfigurovanie 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 jedinečné elektronické spojenie identity podpisujúceho (vlastník kľúča na podpisovanie) so zdrojom 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 i5/OS, ktorú chce distribuovať cez internet. Tento spôsob distribúcie je výhodný a finančne nenáročný. Avšak vie, že zákazníci sa oprávnene obávajú sťahovania programov cez internet z dôvodu narastajúceho 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 administračná entita, ktorá môže vystavovať digitálne certifikáty užívateľom a serverom. Dôvera v CA je základom dôvery v certifikát ako zdroj platných povoľovacích údajov. CA používa svoj súkromný kľúč na vytváranie digitálneho podpisu na certifikáte, ktorý vydá, čím je možná validácia pôvodu certifikátu. Ostatní môžu použiť verejný kľúč certifikátu CA 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 môžete použiť aj na prevádzkovanie vašej vlastnej súkromnej lokálnej CA, ak chcete vystavovať súkromné certifikáty pre systémy a užívateľov. Keď lokálna CA vydá užívateľský certifikát, DCM automaticky priradí certifikátu užívateľský systémový profil alebo inú užívateľskú identitu. Či DCM priradí tento certifikát k užívateľskému profilu alebo k inej užívateľskej identite tohto užívateľa, závisí od toho, či nakonfigurujete DCM na prácu s EIM (Enterprise Identity Mapping). 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 dôverovali danej CA, aby mohli autentifikovať a dôverovať certifikátom, ktoré vydá konkrétna CA.

DCM môžete použiť na povolenie alebo zakázanie dôveryhodnosti pre certifikát Certifikačnej autority (CA). Keď povolíte certifikát CA, môžete špecifikovať, že aplikácie ho môžu používať na autentifikáciu a akceptovanie certifikátov, ktoré vydá daná CA. Ak zakážete certifikát CA, nemôžete špecifikovať, že aplikácie ho môžu používať na autentifikáciu a akceptovanie certifikátov, ktoré vydá daná CA.

Údaje politiky Certifikačnej autority

Keď vytvárate lokálnu Certifikačnú autoritu (CA) pomocou Správcu digitálnych certifikátov, pre túto lokálnu CA môžete uviesť údaje o politike. Údaje o politike pre lokálnu CA opisujú jej podpisové oprávnenia. Údaje o politike určujú:

- Či môže lokálna CA vystavovať a podpisovať užívateľské certifikáty.
- Dĺžku platnosti certifikátov, vystavovaných lokálnou 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 pristupovať. 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 .

Sklady certifikátov

Sklad certifikátov je špeciálny súbor databázy kľúčov, ktorý Správca digitálnych certifikátov (DCM) používa na uloženie digitálnych certifikátov. Sklad certifikátov obsahuje aj súkromný kľúč certifikátu, pokiaľ sa nerozhodnete namiesto toho použiť na uloženie kľúča šifrovací koprocesor IBM. DCM vám umožňuje vytvárať a manažovať niekoľko typov skladov certifikátov. DCM riadi prístup k skladom certifikátov prostredníctvom hesiel spolu s riadením prístupu k adresáru integrovaného súborového systému a k súborom, ktoré tvoria sklad certifikátov.

Sklady certifikátov sú klasifikované podľa typov certifikátov, ktoré obsahujú. Úlohy manažmentu, ktoré môžete vykonávať na každom sklade certifikátov sa menia podľa typu certifikátu, ktorý je v sklade certifikátov. DCM poskytuje nasledovné preddefinované sklady certifikátov, ktoré môžete vytvoriť a riadiť:

Lokálna certifikačná autorita (CA)
Ak vytvoríte lokálnu CA, DCM použije tento sklad certifikátov na uloženie certifikátu lokálnej CA a jeho súkromného kľúča. Certifikát v tomto sklade certifikátov môžete použiť na podpisovanie certifikátov, na vystavenie ktorých používate lokálnu CA. Keď lokálna CA vystaví certifikát, DCM dá kópiu certifikátu CA (bez súkromného kľúča) do príslušného skladu certifikátov (napríklad *SYSTEM) na účely autentifikácie. Aplikácie používajú certifikáty CA na kontrolu pôvodu certifikátov, ktoré musia validovať ako časť dohody SSL na poskytnutie autorizácie na prostriedky.

***SYSTEM**
DCM poskytuje tento sklad certifikátov pre manažovanie certifikátov servera a klienta, ktoré používajú aplikácie ako súčasť komunikačných relácií Secure Sockets Layer (SSL). Aplikácie IBM (a množstvo aplikácií od iných vývojárov) sú napísané tak, že používajú iba certifikáty nachádzajúce sa v sklade certifikátov *SYSTEM. Keď použijete DCM na vytvorenie lokálnej CA, DCM vytvorí tento sklad certifikátov ako súčasť uvedeného procesu. Ak sa rozhodnete získať certifikáty z verejnej CA, ako je VeriSign, pre použitie vašimi aplikáciami servera alebo klienta, musíte tento sklad certifikátov vytvoriť.

***OBJECTSIGNING**
DCM poskytuje tento sklad certifikátov pre manažovanie certifikátov, ktoré používate na digitálne podpisovanie objektov. Taktiež vám úlohy v tomto sklade certifikátov umožnia vytvoriť elektronické podpisy na objektoch, ako aj prezerať a overovať podpisy na objektoch. Keď použijete DCM na vytvorenie lokálnej CA, DCM vytvorí tento sklad certifikátov ako súčasť uvedeného procesu. Ak sa rozhodnete získať certifikáty z verejnej CA, ako je VeriSign, pre podpisovanie objektov, musíte tento sklad certifikátov vytvoriť.

***SIGNATUREVERIFICATION**
DCM poskytuje tento sklad certifikátov na manažovanie certifikátov, ktoré používate na overovanie autenticity elektronických podpisov na objektoch. Na overenie elektronického podpisu musí tento sklad certifikátov obsahovať kópiu certifikátu, ktorým bol objekt podpísaný. Sklad 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 skladu, alebo importovaním certifikátov, ktoré prijmete od podpisovateľa objektu.

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

Poznámka: Ak máte na svojom serveri nainštalovaný šifrovací koprocesor IBM, môžete si pre vaše certifikáty vybrať iné možnosti uloženia súkromných kľúčov (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 sklade certifikátov.

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

Kryptografia

Kryptografia je vedný odbor zaoberajúci sa zachovávaním bezpečnosti dát. 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. Strana má pár kľúčov, ktorý tvorí verejný a súkromný kľúč. Verejný kľúč sa distribuuje voľne, zvyčajne v digitálnom certifikáte, zatiaľ čo súkromný kľúč má bezpečne uschovaný jeho vlastník. Oba kľúče sú matematicky spojené, ale virtuálne je 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.

IBM Cryptographic Coprocessor for iSeries

IBM Cryptographic Coprocessor for iSeries

Používa šifrovacie koprocesory IBM a vysoko bezpečné schopnosti spracovania šifrovania pre váš server. Šifrovací koprocesor poskytuje pre vyvíjanie bezpečných aplikácií elektronického obchodu osvedčené šifrovacie služby, zabezpečujúce súkromie a integritu.

Ak máte vo vašom systéme nainštalovaný a aktivovaný šifrovací koprocesor, môžete ho použiť na poskytnutie bezpečnejšieho uloženia vašich súkromných kľúčov pre certifikáty.

Šifrovací koprocesor môžete použiť na uloženie súkromného kľúča pre certifikát servera alebo klienta a pre certifikát lokálnej Certifikačnej autority (CA). Šifrovací koprocesor však nemôžete použiť na uloženie súkromného kľúča pre užívateľský certifikát, pretože tento kľúč musí byť uložený v užívateľovom systéme. Koprocesor tiež nemôžete v súčasnosti použiť na uloženie súkromného kľúča pre certifikát podpisujúci objekty.

Súkromný kľúč pre certifikát môžete buď uložiť priamo v šifrovacom koprocesore, alebo na zašifrovanie tohto kľúča môžete použiť hlavný kľúč šifrovacieho koprocesora a zašifrovaný súkromný kľúč uložiť vo zvláštnom súbore kľúčov. Tieto možnosti uloženia kľúčov si môžete vybrať ako súčasť procesu vytvárania certifikátu alebo obnovenia jeho platnosti. Ak použijete koprocesor na uloženie súkromného kľúča certifikátu, môžete zmeniť priradenie zariadenia koprocesora pre tento kľúč.

Ak chcete šifrovací koprocesor použiť na uloženie súkromného kľúča, musíte zabezpečiť, aby bol tento koprocesor aktivovaný pred použitím Správcu digitálnych certifikátov (DCM). V opačnom prípade DCM neposkytne možnosť výberu úložnej lokality ako súčasť procesu vytvárania certifikátu alebo obnovenia platnosti certifikátu.

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 serverová 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 servera a každého klienta. Aj keď by neoprávnení užívatelia odchytili a dešifrovali kľúč relácie (čo je nepravdepodobné), nemôžu ho použiť na odpočúvanie neskorších relácií.

Definície aplikácií

Existujú dva typy definícií aplikácií, ktoré môžete manažovať v Správcovi digitálnych certifikátov (DCM):

- Definície klientskych alebo serverových aplikácií, ktoré používajú relácie komunikácií SSL (Secure Sockets Layer).
- Definície aplikácií na podpisovanie objektov, ktoré podpisujú objekty na zabezpečeniu integrity týchto 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, povolené pre SSL, pomocou API (QSYRGAP, QsyRegisterAppForCertUse), aby sa ID aplikácie vytvorilo v DCM automaticky. Všetky aplikácie IBM s povoleným SSL sú zaregistrované pomocou DCM, aby ste mohli jednoducho používať DCM na priradenie certifikátu týmto aplikáciám, aby mohli vytvoriť reláciu SSL. Tak isto v prípade aplikácií, ktoré zapisujete alebo kupujete, môžete zadefinovať definíciu aplikácie a vytvoriť pre ňu ID aplikácie v samotnom DCM. Aby ste mohli vytvoriť definíciu aplikácie SSL pre aplikáciu klienta alebo aplikáciu servera, musíte pracovať v sklade 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. Namiesto toho môže definícia aplikácie, ktorú vytvárate, opisovať typ alebo skupinu objektov, ktoré chcete podpísať. Aby ste mohli vytvoriť definíciu aplikácie, podpisujúcej objekty, musíte pracovať v sklade certifikátov *OBJECTSIGNING.

Overenie platnosti

Správca digitálnych certifikátov (DCM) poskytuje úlohy, ktoré vám umožňujú overovať platnosť certifikátu alebo aplikácie, aby ste mohli skontrolovať rôzne vlastnosti, ktoré certifikát aj aplikácia musia mať.

validácia certifikátu

Keď overujete platnosť certifikátu, Správca digitálnych certifikátov (DCM) overuje počet položiek, ktoré sú súčasťou tohto certifikátu, aby sa zabezpečila pravosť a platnosť tohto certifikátu. Validácia 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. DCM tiež kontroluje, či je certifikát CA pre vystavujúcu CA v aktuálnom sklade certifikátov a či je tento certifikát CA označený ako dôveryhodný. Ak má tento certifikát súkromný kľúč (napríklad certifikáty servera a klienta alebo certifikáty na podpisovanie objektov), DCM overí platnosť aj páru verejného a súkromného kľúča, aby bolo isté, že pár verejného a súkromného kľúča sa k sebe hodí. Inými slovami, DCM zašifruje údaje pomocou verejného kľúča a potom sa presvedčí, že sa dajú rozšifrovať pomocou súkromného kľúča.

validácia aplikácie

Keď overujete platnosť aplikácie, Správca digitálnych certifikátov (DCM) overuje, či má táto aplikácia priradený certifikát a zabezpečuje platnosť priradeného certifikátu. 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. Ak definícia aplikácie uvádza, že dochádza k spracovaniu CRL (Certificate Revocation List) a že pre CA existuje zadefinovaná lokalita CRL, DCM skontroluje CRL ako súčasť procesu overovania platnosti.

Overovanie platnosti aplikácie vám môže pomôcť tým, že vás upozorní na možné problémy, ktoré môže mať aplikácia pri vykonávaní funkcie, vyžadujúcej certifikát. Takéto problémy môžu aplikácii zabrániť v úspešnom zapojení do relácie SSL (Secure Sockets Layer) alebo v úspešnom podpisovaní objektov.

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 bezpečnostnej politiky.

Ak sa chcete dozvedieť viac o tom, ako plánovať použitie DCM a lepšie pochopiť, ako sa môžu digitálne certifikáty hodiť do vašej bezpečnostnej politiky, 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.

Úvahy o zálohovaní a obnove údajov DCM
Prečítajte si túto časť, kde sa dozviete, ako zabezpečiť, aby sa do plánu zálohovania a obnovy vášho systému pridali dôležité údaje 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, ak sa raz rozhodnete, že chcete používať certifikáty z dôvodu výhod 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)
Pomocou týchto informácií sa dozviete 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 a EIM (Enterprise Identity Mapping)
Prečítaním týchto informácií sa dozviete o používaní DCM spolu s EIM.

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

Digital Certificate Manager (DCM) je bezplatný komponent, ktorý vám umožňuje centrálne manažovať 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.
- Voľba inštalácie 34 i5/OS. Toto je DCM, založený na prehliadači.
- Nainštalujte IBM HTTP Server for iSeries (5722–DG1) a spustite inštanciu administračného servera.
- Presvedčte sa, či je vo vašom systéme nakonfigurovaný TCP, aby ste mohli na prístup k DCM používať webový prehliadač a inštanciu administračného servera HTTP.

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.

Úvahy o zálohovaní a obnove údajov DCM

Heslá zašifrovanej databázy kľúčov, ktoré používate na prístup ku skladom certifikátov uložených v Správcovi digitálnych certifikátov (DCM) sú uložené alebo *ukryté* na vašom serveri v špeciálnom bezpečnostnom súbore. Keď používate DCM na vytváranie skladu certifikátov vo vašom systéme, DCM automaticky ukryje heslo za vás. Musíte však manuálne zabezpečiť, aby DCM ukryl heslá skladu certifikátov za určitých okolností.

Príkladom takýchto okolností je situácia, keď použijete DCM na vytvorenie certifikátu pre iný server a vyberiete si použitie súborov certifikátov na cieľovom systéme na vytvorenie nového skladu certifikátov. V tejto situácii musíte otvoriť novovytvorený sklad certifikátov a použiť úlohu **Change password** na zmenu hesla pre sklad certifikátov v cieľovom systéme, čím zabezpečíte, že DCM ukryje nové heslo. Ak je týmto skladom certifikátov Other System Certificate Store, mali by ste uviesť aj to, že chcete pri zmene hesla použiť voľbu **Auto login**. Ak sa chcete dozvedieť viac o používaní DCM na vytváranie certifikátov pre iné servery, pozrite si Použitie lokálnej CA na vydávanie certifikátov pre iné servery.

Okrem toho musíte voľbu **Auto login** špecifikovať pri každej zmene alebo resetovaní hesla pre Other System Certificate Store.

Ak chcete zabezpečiť kompletné zálohovanie závažných údajov DCM, musíte postupovať nasledovne:

- Príkazom SAV (save) uložte všetky súbory .KDB a .RDB. Každý sklad certifikátov DCM tvoria dva súbory, jeden s rozšírením .KDB a jeden s rozšírením .RDB.
- Príkazmi SAVSYS (save system) a SAVSECDTA (save security data) uložte zvláštny bezpečnostný súbor, ktorý obsahuje heslá databázy kľúčov na prístup k skladu certifikátov. Na obnovu bezpečnostného súboru hesiel DCM použite príkaz RSTUSRPRF (restore user profiles) a pre voľbu užívateľského profilu (USRPRF) uveďte hodnotu *ALL.

Ďalšia úvaha o obnove sa týka použitia operácie SAVSECDTA a možnosti, že aktuálne heslá skladu certifikátov nebudú synchronizované s heslami v uloženom bezpečnostnom súbore hesiel DCM. Ak zmeníte heslo pre sklad certifikátov po vykonaní operácie SAVSECDTA, ale pred obnovením údajov z tejto operácie, aktuálne heslo skladu certifikátov nebude synchronizované s heslom v obnovenom súbore.

Ak sa chcete vyhnúť tejto situácii, musíte v DCM použiť úlohu **Change password** (v navigačnom rámci pod **Manage Certificate Store**) na zmenu hesiel skladu certifikátov po obnovení údajov z operácie SAVSECDTA, aby sa zabezpečilo, že heslá budú znova synchronizované. V tejto situácii však nepoužívajte tlačidlo **Reset Password**, ktoré sa zobrazí, keď vyberiete sklad certifikátov, ktorý sa má otvoriť. Pri pokuse o resetovanie hesla sa DCM pokúsi načítať ukryté heslo. Ak ukryté heslo nie je synchronizované s aktuálnym heslom, operácia resetovania zlyhá. Ak heslá skladu certifikátov nemeníte často, budete pravdepodobne uvažovať o vykonaní operácie SAVSECDTA pri každej zmene týchto hesiel, aby ste zabezpečili, že vždy, keď bude treba obnoviť tieto údaje, sa vám uloží najaktuálnejšia verzia hesiel.

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 o 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. Lokálna CA, ktorú vytvárate a s ktorou pracujete pomocou Správcu digitálnych certifikátov, je nezávislá entita. Ostatní môžu použiť verejný kľúč certifikátu Certifikačnej autority na kontrolu autenticity certifikátov, ktoré vydá a podpíše daná CA. Ak chcete použiť certifikát pre SSL, na podpisovanie objektov alebo overovanie podpisov na objektoch, musíte mať aj kópiu certifikátu vystavujúcej CA.

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 certifikátu ako základ pre inicializovanie šifrovanej relácie pomocou SSL medzi klientom a serverom. Tieto typy certifikátov môžete manažovať iba pre sklad 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 aj pôvod alebo vlastníctvo objektu. Tento certifikát môžete použiť na podpisovanie rôznych objektov, vrátane väčšiny objektov v integrovanom súborovom systéme a objektov *CMD. 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 sklad 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 sklad 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 priraďuje užívateľské certifikáty, ktoré vaša súkromná CA vydáva s užívateľským profilom. Taktiež môžete používať DCM na priradenie užívateľských certifikátov, ktoré vydajú iné certifikačné autority s užívateľským profilom.

Keď na manažovanie vašich certifikátov používate Správcu digitálnych certifikátov (DCM), DCM organizuje a ukladá tieto certifikáty a ich priradené súkromné kľúče do skladu certifikátov na základe týchto klasifikácií.

Poznámka: Ak máte na svojom serveri nainštalovaný šifrovací koprocesor IBM, môžete si pre vaše certifikáty vybrať iné možnosti uloženia súkromných kľúčov (s výnimkou certifikátov na podpisovanie objektov). Môžete sa rozhodnúť, že súkromný kľúč uložíte na samotnom šifrovacom koprocesore. Šifrovací koprocesor môžete prípadne použiť na zašifrovanie súkromného kľúča a môžete ho uložiť vo zvláštnom súbore a nie v sklade 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, musíte si vybrať typ implementácie certifikátov, ktorý najlepšie vyhovuje vašim požiadavkám na bezpečnosť. Na získavanie certifikátov máte nasledovné voľby:
- Zakúpenie vašich certifikátov od verejnej internetovej Certifikačnej autority (CA).
- Prevádzkovanie vašej vlastnej lokálnej CA na vystavovanie súkromných certifikátov pre vašich užívateľov a aplikácie.
- Používanie kombinácie certifikátov od verejných internetových CA a vašej vlastnej lokálnej 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. Než sa rozhodnete získať certifikáty od CA alebo dôverovať certifikátom, ktoré vystavuje, musíte zhodnotiť, či striktnosť identifikačnej politiky tejto CA vyhovuje vašim požiadavkám na bezpečnosť. Pretože vznikli štandardy PKIX (Public Key Infrastructure for X.509), niektoré verejné CA teraz poskytujú striktnejšie identifikačné štandardy pre vystavovanie 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 obmedzený počet serverových alebo klientskych aplikácií a užívateľov, cena nebude pre vás rozhodujúcim faktorom. Cena však môže byť rozhodujúca, ak máte veľký počet *súkromných* užívateľov, ktorí potrebujú verejné certifikáty na autentifikáciu klientov. V tomto prípade musíte vziať do úvahy aj administračné a programovacie úsilie, potrebné na nakonfigurovanie serverových aplikácií tak, aby akceptovali len konkrétnu podskupinu certifikátov, ktoré vystavuje 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. Rovnako ďalšie spoločnosti a užívatelia môžu viac uznávať a dôverovať certifikátom, ktoré vystavuje všeobecne známa verejná CA ako certifikátom, ktoré vystavuje vaša súkromná lokálna 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. Vytvorenie a udržiavanie vašej vlastnej lokálnej CA vám umožňuje vystavovať certifikáty len 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 na vystavovanie certifikátov užívateľom na autentifikáciu klienta používate lokálnu CA, musíte sa rozhodnúť, kde
| chcete tieto užívateľské certifikáty uložiť. Ak užívatelia získavajú svoje certifikáty od lokálnej CA prostredníctvom
| DCM, ich certifikáty sa štandardne ukladajú s užívateľským profilom. DCM môžete však nakonfigurovať na prácu s
| EIM (Enterprise Identity Mapping), aby sa ich certifikáty namiesto toho ukladali do lokality LDAP (Lightweight
| Directory Access Protocol). (Viac informácií o tom, ako DCM a EIM spolu pracujú, nájdete v Digital certificates and
| Enterprise Identity Mapping (EIM).) Ak uprednostníte, aby užívateľské certifikáty neboli žiadnym spôsobom priradené
| k užívateľskému profilu alebo s ním uložené, môžete pomocou API programovo vystavovať certifikáty užívateľom
| iného systému ako iSeries.

Poznámka: Systémový administrátor určuje, ktorým CA budú aplikácie v jeho systéme dôverovať bez ohľadu na to, ktorú CA používate na vystavovanie vašich certifikátov. 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. Administrátori stanovujú dôveryhodnosť pre certifikáty CA v príslušnom sklade certifikátov DCM, ktorý obsahuje kópie certifikátov od väčšiny všeobecne známych verejných CA. Ak však vo vašom sklade certifikátov certifikát CA nie je, váš server môže dôverovať užívateľským alebo klientskym certifikátom, ktoré vystavila táto CA, až keď získate a naimportujete kópiu tohto certifikátu CA. Tento certifikát CA musí byť v správnom súborovom formáte a vy ho musíte pridať do vášho skladu 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 opisuje úlohy, ktoré musíte vykonávať, ak sa rozhodnete na vystavovanie súkromných certifikátov prevádzkovať lokálnu CA.
- Manažovanie certifikátov od verejných internetových CA popisuje úlohy, ktoré musíte vykonať, ak chcete používať certifikáty od dobre známej verejnej CA, vrátane PKIX CA.
- Používanie lokálnej CA na iných serveroch opisuje úlohy, ktoré musíte vykonať, ak si želáte používať certifikáty zo súkromnej lokálnej 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 validáciu 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 bezpečnosti údajov nasledovne:

1. Aplikácia servera predloží certifikát aplikácii klienta (užívateľa) ako dôkaz identity servera.
2. Klientska aplikácia overuje identitu servera proti kópii certifikátu vystavujúcej Certifikačnej autority (CA). (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. 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 úvodného spracovania SSL algoritmus asymetrického kľúča (verejného kľúča) na dohodovanie symetrického kľúča, ktorý sa neskôr použije na šifrovanie a dešifrovanie údajov aplikácie pre túto konkrétnu reláciu SSL. 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. Správcu digitálnych certifikátov (DCM) môžete použiť aj na priradenie užívateľského certifikátu k užívateľskému profilu alebo inej

užívateľskej identite. Tento certifikát má teda rovnaké oprávnenia a povolenia ako priradená užívateľská identita alebo užívateľský profil. Prípadne môžete pomocou API programovo použiť vašu súkromnú lokálnu Certifikačnú autoritu na vystavovanie certifikátov pre užívateľov iného systému ako iSeries. Tieto API vám poskytujú možnosť vydať súkromné certifikáty užívateľom, ak si neželáte, aby títo užívatelia mali užívateľský profil alebo inú užívateľskú identitu.

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, funguje Certifikačná autorita (CA) ako dôveryhodná tretia strana, ktorá vydáva certifikát a prehlasuje ho za autentické povoľovacie údaje.

Na autentifikačné účely používajú certifikáty verejný kľúč a s ním súvisiaci súkromný kľúč. Vydávajúca CA tieto dva kľúče pripojí 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 tieto aplikácie poskytujú podporu certifikátov klientskej autentifikácie:
- Telnet server
- IBM HTTP Server (založený na Apache)
- IBM Directory Server
- iSeries Access for Windows (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:
- Existuje istá pravdepodobnosť, že osoba zabudne svoje heslo. Používatelia si preto musia zapamätať svoje heslá alebo si užívateľské mená a heslá niekam zapísať, 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 súkromia prenosov údajov pomocou Secure Sockets Layer (SSL) na šifrovanie komunikačných relácií.

Ak sa chcete dozvedieť viac o konfigurácii serverových aplikácií na používanie certifikátov pre autentifikáciu klienta počas relácie SSL, pozrite si tému SSL (Secure Sockets Layer) informačného centra iSeries.

Digitálne certifikáty a EIM (Enterprise Identity Mapping)

EIM (Enterprise Identity Mapping) je technológia eServer, ktorá vám umožňuje manažovať užívateľské identity vo vašom podniku, vrátane užívateľských profilov a užívateľských certifikátov. Najbežnejšou formou užívateľskej identity je meno užívateľa a heslo; inou formou užívateľskej identity sú certifikáty. Niektoré aplikácie sú nakonfigurované tak, aby užívatelia mohli byť autentifikovaní prostredníctvom užívateľského certifikátu a nie prostredníctvom mena užívateľa a hesla.

Pomocou EIM môžete vytvoriť mapovania medzi užívateľskými identitami, čo umožňuje užívateľovi preukázať sa s jednou užívateľskou identitou a pristupovať k prostriedkom inej užívateľskej identity bez toho, aby tento užívateľ musel poskytnúť potrebnú užívateľskú identitu. V EIM to uskutočníte zadefinovaním spojenia medzi jednou užívateľskou identitou a inou užívateľskou identitou. Užívateľské identity môžu mať rôzne formy, vrátane užívateľských certifikátov. Môžete vytvoriť aj individuálne spojenia medzi identifikátorom EIM a rôznymi užívateľskými identitami, ktoré patria k užívateľovi, reprezentovanému týmto identifikátorom EIM. Prípadne môžete vytvoriť priradenia politík, ktoré mapujú skupinu užívateľských identít do jednej cieľovej užívateľskej identity. Užívateľské identity môžu mať rôzne formy, vrátane užívateľských certifikátov. Pri vytváraní týchto priradení môžu byť užívateľské certifikáty mapované do príslušných identifikátorov EIM, v dôsledku čoho sa certifikáty ľahšie používajú na autentifikáciu.

Ak chcete túto vlastnosť EIM využiť na manažovanie užívateľských certifikátov, musíte pred vykonaním všetkých úloh konfigurácie DCM vykonať tieto úlohy konfigurácie EIM:

1. Na nakonfigurovanie EIM použite sprievodcu **EIM Configuration** v programe **iSeries Navigator**.
2. Vytvorte identifikátor EIM pre každého užívateľa, ktorého chcete mať zapojeného do EIM.
3. Vytvorte cieľové priradenie medzi každým identifikátorom EIM a užívateľským profilom užívateľa v lokálnom užívateľskom registri i5/OS tak, aby ľubovoľné užívateľské certifikáty, ktoré užívateľ priradí cez DCM alebo vytvorí v DCM, mohli byť namapované k užívateľskému profilu. Použite názov definície registra EIM pre lokálny užívateľský register i5/OS, ktorý ste zadali v sprievodcovi **EIM Configuration**. **Poznámka:** Viac informácií o konfigurovaní EIM nájdete v téme EIM.

Po vykonaní úloh, potrebných pre konfiguráciu EIM, musíte na nakonfigurovanie Správcu digitálnych certifikátov (DCM) použiť úlohu **Manage LDAP Location**, aby sa užívateľské certifikáty uložili v lokalite LDAP (Lightweight Directory Access Protocol) a nie s užívateľským profilom. Keď konfigurujete EIM a DCM tak, aby pracovali spolu, úloha **Create Certificate** pre užívateľské certifikáty a úloha **Assign a user certificate** spracovávajú certifikáty na používanie EIM a nie na priradenie certifikátu k užívateľskému profilu. DCM ukladá tento certifikát do nakonfigurovaného adresára LDAP a informácie o DN (distinguished name) tohto certifikátu používa na vytvorenie zdrojového priradenia pre príslušný identifikátor EIM. Toto umožňuje operačným systémom a aplikáciám používať tento certifikát ako zdroj vyhľadávacej operácie mapovania EIM na mapovanie z certifikátu do cieľovej užívateľskej identity, priradenej k rovnakému identifikátoru EIM.

Navyše, keď konfigurujete EIM a DCM tak, aby pracovali spolu, DCM môžete použiť na kontrolu ukončenia platnosti užívateľského certifikátu na podnikovej úrovni a nielen na úrovni systému.

Digitálne certifikáty pre pripojenia VPN

Digitálne certifikáty môžete používať ako prostriedok na vytvorenie spojenia virtuálnej súkromnej siete (VPN). 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.

Jednou metódou, ktorú môžu servery IKE používať na vzájomnú autentifikáciu, je predzdieľaný kľúč. Používanie predzdieľaného kľúča je však menej bezpečné, pretože tento kľúč musíte manuálne odovzdať administrátorovi druhého koncového bodu vo 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 použitia 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 na vystavovanie certifikátu

používate v DCM lokálnu CA, môžete pre tento certifikát špecifikovať alternatívne informácie o názve predmetu. Zadaním týchto informácií sa uistíte, že vaše spojenie VPN je kompatibilné s ostatnými 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

i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod. Podpora podpisovania objektov rozširuje tradičné systémové nástroje riadením, 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 systéme ako iSeries. 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 podpisu 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 z 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 používanie elektronických podpisov vyhovuje vašim požiadavkám na bezpečnosť a bezpečnostným politikám, musíte zhodnotiť, či potrebujete používať verejné certifikáty oproti vystavovaniu súkromných certifikátov. Ak máte v pláne distribuovať objekty užívateľom v širokej verejnosti, mali by ste zvážiť, či na podpisovanie objektov nebudete používať certifikáty od všeobecne známej verejnej Certifikačnej autority (CA). 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). Na manažovanie certifikátov, ktoré používate na podpisovanie objektov a na overovanie podpisov na objektoch používajte DCM. DCM môžete taktiež použiť na podpisovanie objektov a na overovanie podpisov objektov.

Digitálne certifikáty pre overovanie podpisov objektov

i5/OS poskytuje podporu používania certifikátov na overenie digitálnych 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 sa rozhodnete dôverovať Certifikačnej autorite (CA), môžete sa rozhodnúť, či budete dôverovať podpisom, ktoré niekto vytvára pomocou certifikátu, vystaveného touto dôveryhodnou 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, ako dôležité sú podpisy pre objekty, ktoré majú byť obnovované na vašom systéme. Toto zistíte pomocou systémovej hodnoty s názvom QVFYOBJRST (Verify object signatures during restore). 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 spustiteľné objekty, ktoré sa obnovujú a nie úložné súbory alebo súbory integrovaného súborového systému. Viac informácií o používaní tejto a ďalších systémových hodnôt nájdete v téme System Value Finder v Informačnom centre iSeries.

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 použiť na podpisovanie objektov a na overovanie podpisov objektov.

Kapitola 7. Konfigurácia 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, **Manage Certificates** 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 **Fast Path**, každá kategória v navigačnej časti je úloha s návodom, ktorý vás rýchlo a jednoducho prevedie sériou krokov na dokončenie úlohy. Kategória Fast Path poskytuje zoskupenie funkcií na manažovanie certifikátov a aplikácií, ktoré umožňuje skúseným užívateľom DCM rýchlo pristupovať na rôzne súvisiace úlohy z centrálnej množiny strán.

Dostupnosť úloh v navigačnej časti závisí od skladu certifikátov, v ktorom pracujete. Kategória a počet úloh, ktoré môžete vidieť v navigačnej časti, závisí od autorizácií vášho užívateľského profilu i5/OS. Všetky úlohy na prevádzkovanie CA, riadiace aplikáciami používané certifikáty a ďalšie úlohy systémovej úrovne sú k dispozícii iba správcom alebo správcom bezpečnosti. Správcovia bezpečnosti alebo správcovia musia mať špeciálne oprávnenie *SECADM a *ALLOBJ, aby mohli vidieť a používať tieto úlohy. Užívatelia 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
Toto si prečítajte, ak sa chcete dozvedieť viac o spôsobe prístupu k Správcovi digitálnych certifikátov na vašom serveri.

Prvé nastavenie certifikátov
Táto téma vás naučí, ako začať s používaním DCM na nastavenie všetkého, čo potrebujete, keď používate certifikáty prvýkrát. 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 máte záujem o ďalšie inštruktážne informácie o používaní digitálnych certifikátov v internetovom prostredí na zlepšenie bezpečnosti vášho systému a siete, vynikajúcim zdrojom je webová stránka certifikačnej autority VeriSign. Webová stránka certifikačnej autority VeriSign poskytuje rozsiahlu knižnicu tém o digitálnych certifikátoch, ako aj množstvo ďalších predmetov, týkajúcich sa bezpečnosti internetu. Do ich knižnice sa môžete dostať cez sekciu pomoci VeriSign .

Spustenie 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. Je to šifrovací produkt, ktorý DCM používa na generovanie páru verejného a súkromného kľúča pre certifikáty, ktorým sa šifrujú exportované súbory certifikátov a dešifrujú sa importované súbory certifikátov.
2. Na spustenie administračného servera HTTP Server použite program iSeries Navigator:

a. Spustite **iSeries Navigator**.
b. V hlavnom stromovom zobrazení kliknite dvakrát na váš server.
c. Rozviňte **Network > Servers > TCP/IP**.
d. Pravým tlačidlom kliknite na **HTTP Administration**.
e. Kliknite na **Start**.
3. Spustite váš webový prehliadač.
4. Pomocou prehliadača prejdite na stránku úloh vášho systému http://*názov_vášho_systému*:2001.
5. Zo zoznamu produktov na stránke úloh vyberte **Digital Certificate Manager** na sprístupnenie užívateľského rozhrania DCM.

Prvé nastavenie certifikátov

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. Aké úlohy sú k dispozícii, závisí od toho, s ktorým skladom certifikátov (ak existuje) pracujete a tiež od špeciálnych oprávnení vášho užívateľského profilu. Väčšina úloh je dostupných len vtedy, ak máte špeciálne oprávnenia *ALLOBJ a *SECADM. Ak chcete na overenie podpisov na objektoch použiť DCM, váš užívateľský profil musí mať aj špeciálne oprávnenie *AUDIT.

Ak používate Správcu digitálnych objektov (DCM) prvýkrát, sklady certifikátov neexistujú. Takže keď prvýkrát pristupujete do DCM, navigačný panel zobrazuje len nasledujúce úlohy a zobrazuje ich len v prípade, že máte potrebné špeciálne oprávnenia:

- Manažovanie užívateľských certifikátov.
- Vytvorenie nového skladu certifikátov
- Vytvorenie Certifikačnej autority (CA). (Poznámka: Po použití tejto úlohy na vytvorenie súkromnej lokálnej CA sa táto úloha už v zozname neobjaví.)
- Manažovanie miest CRL.
- Manažovanie lokality LDAP.
- Manažovanie umiestnenia požiadavky PKIX.
- Návrat na stránku úloh.

I keď sklady certifikátov vo vašom systéme už existujú (napríklad prechádzate zo staršej verzie DCM), DCM zobrazuje v ľavom navigačnom rámci len obmedzený počet úloh alebo kategórií úloh. Ktoré úlohy alebo kategórie DCM zobrazuje, sa mení na základe skladu certifikátov (ak existuje), ktorý je otvorený a od špeciálnych oprávnení vášho užívateľského profilu.

Aby ste mohli začať pracovať s väčšinou úloh manažmentu certifikátov a aplikácií, musíte najprv pristúpiť na príslušný sklad certifikátov. Ak chcete otvoriť konkrétny sklad certifikátov, v navigačnej časti kliknite na **Select a Certificate Store**.

Navigačná časť DCM tiež poskytuje tlačidlo **Secure Connection**. Toto tlačidlo môžete použiť na zobrazenie druhého okna prehliadača, ak chcete iniciovať bezpečné pripojenie pomocou SSL (Secure Sockets Layer). 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 na 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:

Vytvorenie a prevádzkovanie lokálnej CA na vydávanie certifikátov vašim aplikáciám.

Manažovanie certifikátov z verejnej internetovej CA pre používanie vašimi aplikáciami.

Vytvorenie a prevádzkovanie lokálnej 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: Ak chcete certifikáty používať s aplikáciou IBM HTTP Server for iSeries, musíte predtým, než začnete pracovať s DCM, vytvoriť a nakonfigurovať váš webový server. Pri konfigurovaní webového servera na používanie SSL sa pre tento server vygeneruje ID aplikácie. Toto ID aplikácie si musíte poznamenať, aby ste mohli pomocou DCM určiť, ktorý certifikát bude táto aplikácia používať pre SSL.

Server neukončujte a znova nespúšťajte, kým pomocou DCM nepriradíte k nemu certifikát. Ak ukončíte a znova spustíte inštanciu *ADMIN webového servera predtým, než k nemu priradíte certifikát, server sa nespustí a vy nebudete môcť pomocou DMC certifikát k nemu priradiť.

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

1. Spustite DCM.
2. V navigačnej časti DCM vyberte **Create a Certificate Authority**, 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 možný len v prípade, ak máte na vašom systéme iSeries nainštalovaný šifrovací koprocesor IBM. Ak váš systém nemá kryptografický procesor, DCM automaticky uloží certifikát a jeho súkromný kľúč do skladu certifikátov Miestna Certifikačná autorita (CA).)
   b. Poskytnite identifikačné informácie pre lokálnu CA.
   c. Nainštalujte certifikát lokálnej CA na vaše 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 serverového alebo klientskeho certifikátu, ktorý vaše aplikácie budú môcť použiť pre pripojenia SSL. (Ak je na vašom systéme iSeries nainštalovaný šifrovací koprocesor IBM, pomocou tohto kroku si môžete vybrať, ako máte uložiť súkromný kľúč pre certifikát servera alebo klienta. Ak váš systém nemá koprocesor, DCM automaticky umiestni súkromný kľúč do skladu certifikátov *SYSTEM. DCM vytvorí sklad 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 skladu 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 budú môcť aplikácie použiť na elektronické podpisovanie objektov. Táto podúloha vytvorí sklad certifikátov *OBJECTSIGNING; toto je sklad certifikátov, ktorý 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 skladu certifikátov *OBJECTSIGNING na manažovanie certifikátov, podpisujúcich objekty, od verejnej internetovej CA, nemusíte vykonať tento ani predchádzajúci krok.
   i. Vyberte aplikácie, ktoré budú 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 tohto certifikátu, aby ho užívateľov klientsky softvér mohol použiť na autentifikáciu identity servera ako súčasť procesu dohodovania SSL. Užívatelia môžu použiť DCM na skopírovanie certifikátu lokálnej CA do súboru alebo na stiahnutie certifikátu do svojho prehliadača. Ako užívatelia uložia certifikát lokálnej CA, závisí od klientskeho softvéru, 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:

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

Použitie 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.

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

Manažovanie užívateľských certifikátov

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

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 možno už vlastní kópiu 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 serverová 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. Ak nie je otvorený žiaden sklad certifikátov, alebo keď je otvorený sklad certifikátov Miestna Certifikačná autorita (CA), v navigačnej časti môžete vybrať **Manage User Certificates**, aby ste mohli pristupovať na príslušné úlohy. Ak je otvorený iný sklad certifikátov, úlohy pre užívateľské certifikáty sú začlenené do úlohy pod **Manage Certificates**.

Užívatelia bez mimoriadnych oprávnení užívateľského profilu *SECADM a *ALLOBJ môžu spravovať iba ich vlastné priradenia certifikátov. Môžu zvoliť **Manage User Certificates** 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 **Create Certificate** v hlavnom navigačnom rámci.

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

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

Priradenie užívateľského certifikátu
Z týchto informácií sa dozviete, ako máte priradiť certifikát, ktorý vlastníte, k vášmu užívateľskému profilu OS/400 alebo k inej užívateľskej identite. Certifikát môže byť zo súkromnej lokálnej CA na inom systéme alebo zo známej internetovej CA. Skôr než priradíte certifikát k užívateľskej identite, server musí vystavujúcej CA dôverovať a tento certifikát nesmie byť už priradený k užívateľskému profilu alebo k inej užívateľskej identite v systéme.

| **Manažovanie užívateľských certifikátov podľa ukončenia platnosti**
Z týchto informácií sa dozviete, ako máte zobrazovať a manažovať užívateľské certifikáty na základe dátumov ukončenia ich platnosti.

Vytvorenie užívateľského certifikátu: 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 **Create Certificate**. 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 **Create Certificate**.
3. Ako typ certifikátu na vytvorenie vyberte **User certificate**. Zobrazí sa formulár, na ktorom môžete zadať identifikačné informácie pre certifikát.
4. Vyplňte formulár a kliknite na **Continue**.

   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.

| **Priradenie užívateľského certifikátu:** Je možné, že niektorí užívatelia majú certifikáty od externej Certifikačnej
| autority (CA) alebo od lokálnej CA v inom systéme iSeries, ktoré vy, ako administrátor, budete chcieť sprístupniť pre
| Správcu digitálnych certifikátov (DCM). Umožňuje to vám a užívateľovi používať DCM na manažovanie týchto
| certifikátov, ktoré sa najčastejšie používajú na autentifikáciu klienta. Úloha **Assign a user certificate** poskytuje
| mechanizmus, ako umožniť užívateľovi vytvoriť priradenie DCM pre certifikát, získaný od externej CA.

| Keď užívateľ priraďuje certifikát, DCM má jeden z dvoch spôsobov spravovania priradeného certifikátu:

- Uloženie certifikátu lokálne na systém iSeries s užívateľským profilom tohto užívateľa.
  Keď pre DCM nie je zadefinovaná lokalita LDAP, úloha **Assign a user certificate** umožňuje užívateľovi priradiť k užívateľskému profilu OS/400 externý certifikát. Priradenie certifikátu k užívateľskému profilu zabezpečuje, že tento certifikát možno používať v systéme s aplikáciami, ktoré vyžadujú certifikáty na autentifikáciu klienta.
- Uloženie certifikátu v lokalite LDAP (Lightweight Directory Access Protocol) pre používanie s EIM (Enterprise Identity Mapping).
  Ak je zadefinovaná lokalita LDAP a systém iSeries je nakonfigurovaný na zapojenie do EIM, úloha **Assign a user certificate** umožňuje užívateľovi uložiť kópiu externého certifikátu do určeného adresára LDAP. DCM vytvára pre tento certifikát aj zdrojové priradenie v EIM. Uloženie certifikátu týmto spôsobom umožňuje administrátorovi EIM uznať tento certifikát ako platnú užívateľskú identitu, ktorá môže byť zapojená do EIM.

  Poznámka: Skôr než užívateľ priradí certifikát k užívateľskej identite v konfigurácii EIM, EIM musí byť pre tohto užívateľa primerane nakonfigurované. Táto konfigurácia EIM zahrňuje vytvorenie identifikátora EIM pre tohto užívateľa a vytvorenie cieľového priradenia medzi týmto identifikátorom EIM a užívateľským profilom. V opačnom prípade DCM nemôže pre tento certifikát vytvoriť zodpovedajúce zdrojové priradenie s identifikátorom EIM. Viac informácií o konfigurovaní EIM nájdete v téme EIM v Informačnom centre iSeries.

Ak chce užívateľ používať úlohu **Assign a user certificate**, musí splniť nasledujúce požiadavky:

1. Musíte mať bezpečnú reláciu so serverom HTTP, prostredníctvom ktorého pristupujete k 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 užívateľ vyberie túto úlohu, zobrazí sa nové okno prehliadača. Ak užívateľ nemá bezpečnú reláciu, DCM ho vyzve, aby klikol na **Assign a User Certificate**, čím túto reláciu spustí. DCM následne spustí dohodovania SSL (Secure Sockets Layer) s užívateľovým prehliadačom. Ako súčasť týchto dohodovaní sa môže prehliadač užívateľa opýtať, či má dôverovať Certifikačnej autorite (CA), ktorá vystavila certifikát, identifikujúci server HTTP. Prehliadač sa môže užívateľa tiež opýtať, či má akceptovať samotný certifikát servera.
2. Predložiť 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.
3. Mať v prehliadači certifikát, ktorý nie je už priradený k užívateľskej identite užívateľa, vykonávajúceho túto úlohu. (Prípadne, ak je DCM nakonfigurovaný na prácu spolu s EIM, užívateľ musí mať v prehliadači certifikát, ktorý už nie je uložený v lokalite LDAP pre DCM.)

   Po vytvorení bezpečnej relácie sa DCM pokúsi získať z vášho prehliadača príslušný certifikát, aby ho mohol priradiť k vašej užívateľskej identite. 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, znamená to, že ste nemohli poskytnúť certifikát, ktorý môže DCM priradiť k vašej užívateľskej identite. Môže to byť spôsobené jedným z niekoľkých problémov s užívateľskými certifikátmi. Napríklad certifikáty, ktoré obsahuje váš prehliadač, sú už pravdepodobne priradené k vašej užívateľskej identite.

Manažovanie užívateľských certifikátov podľa ukončenia platnosti: Správca digitálnych certifikátov (DCM) poskytuje podporu pre manažovanie ukončenia platnosti certifikátov, aby umožnil administrátorom kontrolovať dátumy ukončenia platnosti užívateľských certifikátov v lokálnom systéme iSeries. Podporu DCM pre manažovanie ukončenia platnosti certifikátov je možné používať spolu s EIM (Enterprise Identity Mapping), takže administrátori môžu DCM používať na kontrolu ukončenia platnosti užívateľských certifikátov na podnikovej úrovni.

Ak chcete využívať podporu manažovania ukončenia platnosti pre užívateľské certifikáty na podnikovej úrovni, v podniku musí byť nakonfigurované EIM a EIM musí obsahovať príslušné informácie o mapovaní pre užívateľské certifikáty. Na kontrolovanie ukončenia platnosti iných užívateľských certifikátov, než sú priradené k vášmu vlastnému užívateľskému profilu, musíte mať špeciálne oprávnenia *ALLOBJ a *SECADM.

Používanie DCM na zobrazovanie certifikátov na základe ukončenia ich platnosti vám umožňuje rýchlo a ľahko zistiť, ktorým certifikátom čoskoro skončí platnosť, takže týmto certifikátom je možné platnosť včas obnoviť.

Ak chcete zobrazovať alebo manažovať užívateľské certifikáty na základe dátumov ukončenia ich platnosti, postupujte nasledovne:

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 vyberte **Manage User Certificates**, čím zobrazíte zoznam úloh. **Poznámka:** Ak práve pracujete so skladom certifikátov, vyberte **Manage Certificates**, čím zobrazíte zoznam úloh, ďalej vyberte **Check expiration** a nakoniec vyberte **User**.
3. Ak má váš užívateľský profil špeciálne oprávnenia *ALLOBJ a *SECADM, môžete si zvoliť metódu, podľa ktorej budete vyberať užívateľské certifikáty, ktoré sa majú zobrazovať a manažovať na základe dátumov ukončenia ich platnosti. (Ak váš užívateľský profil nemá tieto špeciálne oprávnenia, DCM vás požiada o určenie rozsahu dátumov ukončenia platnosti, ako je opísané v nasledujúcom kroku.) Môžete vybrať jeden z nasledujúcich:
   - **User profile** na zobrazovanie a manažovanie užívateľských certifikátov, priradených ku konkrétnemu užívateľskému profilu OS/400. Uveďte **User profile name** a kliknite na **Continue**. **Poznámka:** Iný užívateľský profil než váš vlastný môžete uviesť len v prípade, že máte špeciálne oprávnenia *ALLOBJ a *SECADM.
   - **All user certificates** na zobrazovanie a manažovanie užívateľských certifikátov pre všetky užívateľské identity.
4. V poli **Expiration date range in days (1-365)** zadajte počet dní, pre ktoré chcete zobraziť užívateľské certifikáty na základe dátumu ukončenia ich platnosti a kliknite na **Continue**. DCM zobrazí všetky užívateľské certifikáty pre určený užívateľský profil, ktorých platnosť končí medzi dnešným dátumom a dátumom, ktorý zodpovedá počtu zadaných dní. DCM zobrazí aj všetky užívateľské certifikáty, ktorých dátumy ukončenia platnosti sú staršie ako dnešný dátum.
5. Vyberte užívateľský certifikát, ktorý chcete manažovať. Môžete si vybrať, či chcete zobraziť detailné informácie o certifikáte alebo chcete tento certifikát odstrániť z priradenej užívateľskej identity.
6. Po skončení práce s certifikátmi z tohto zoznamu kliknite na **Cancel**, čím úlohu ukončíte.

Použitie 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. Ak sa chcete vyhnúť poskytnutiu užívateľských profilov týmto užívateľom, môžete užívateľov požiadať, aby zaplatili za certifikát od všeobecne známej CA, ak ste chceli vyžadovať certifikáty na autentifikáciu užívateľov pre vaše aplikácie.

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.

Existujú dve API, pre každý z prevládajúcich programov prehliadača jedno, ktoré môžete zavolať, keď na vytvorenie programu na vystavovanie certifikátov pre užívateľov používate Net.Data. 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).

Získanie kópie certifikátu súkromnej CA

Keď pristupujete na server, ktorý používa spojenie Secure Sockets Layer (SSL), 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 tento server predloží certifikát od verejnej internetovej CA, softvér vášho prehliadača alebo iný klientsky softvér možno už má kópiu 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 serverová aplikácia vyžaduje, aby ste sami seba autentifikovali predložením certifikátu od lokálnej CA, musíte si ešte pred vyžiadaním užívateľského certifikátu od lokálnej CA stiahnuť do svojho prehliadača certifikát lokálnej CA.

Na použitie DCM na získanie kópie certifikátu lokálnej CA vykonajte tieto kroky:
1. Spustite DCM.
2. V navigačnom rámci vyberte **Install Local CA Certificate on Your 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 **Install certificate** 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 **Copy and paste certificate** 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.

Manažovanie 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 verejnú webovú stránku a na relácie bezpečnej komunikácie chcete používať SSL (Secure Sockets Layer), aby bolo zabezpečené súkromie určitých informačných transakcií. Pretože táto webová stránka je verejne všeobecne dostupná, chcete používať certifikáty, ktoré môže väčšina webových prehliadačov okamžite uznať.

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.

Manage public certificates

Keď použijete DCM na manažovanie certifikátov od verejnej internetovej CA, musíte najprv vytvoriť internet. Sklad 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 skladov certifikátov, podľa typu certifikátov, ktoré obsahujú.

Typ skladu 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 príslušného skladu certifikátov a manažovaní vašich certifikátov pre vaše aplikácie, pozrite si tieto témy:

- Manažovanie verejných internetových certifikátov pre relácie komunikácií SSL.
- Manažovanie verejných internetových certifikátov pre podpisovanie objektov.
- Manažovanie certifikátov na overovanie podpisov objektov.

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

Manažovanie verejných internetových certifikátov 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 príslušný sklad certifikátov na manažovanie verejných certifikátov, ktoré používate pre SSL. Tým je sklad certifikátov *SYSTEM. Keď vytvoríte sklad 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 **Create New Certificate Store**, aby sa spustila úloha a mohli ste vyplniť sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia skladu 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 sklad certifikátov, ktorý sa má vytvoriť a kliknite na **Continue**.
4. Vyberte **Yes**, aby sa certifikát vytvoril ako časť vytvárania skladu certifikátov *SYSTEM a kliknite na **Continue**.
5. Ako podpisovateľa nového certifikátu vyberte **VeriSign or other Internet Certificate Authority (CA)** a kliknite na **Continue**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačnú informáciu pre nový certifikát.

   Poznámka: Ak máte na vašom serveri nainštalovaný šifrovací procesor IBM, DCM vám umožní vybrať spôsob uloženia súkromného kľúča pre certifikát ako ďalšiu úlohu. Ak váš systém nemá koprocesor, DCM automaticky umiestni súkromný kľúč do skladu 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 **Continue**, 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. Ak opustíte túto stranu, 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 procedúra, musíte počkať, kým CA nevráti podpísaný dokončený certifikát.

Poznámka: Ak chcete certifikáty používať s aplikáciou HTTP Server for iSeries, musíte vytvoriť a nakonfigurovať váš webový server ešte pred prácou s DCM, aby ste mohli pracovať s podpísaným, úplným certifikátom. Pri konfigurovaní webového servera na používanie SSL sa pre tento server vygeneruje ID aplikácie. Toto ID aplikácie si musíte poznamenať, aby ste mohli pomocou DCM určiť, ktorý certifikát musí táto aplikácia používať pre SSL.

Server neukončujte a znova nespúšťajte, kým pomocou DCM nepriradíte k nemu podpísaný, úplný certifikát. Ak ukončíte a znova spustíte inštanciu *ADMIN webového servera predtým, než k nemu priradíte certifikát, server sa nespustí a vy nebudete môcť pomocou DMC certifikát k nemu priradiť.

8. Keď verejná CA vráti váš podpísaný certifikát, spustite DCM.
9. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
10. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali a kliknite na **Continue**.
11. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
12. Zo zoznamu úloh vyberte **Import certificate**, aby sa spustil proces importu podpísaného certifikátu do skladu certifikátov *SYSTEM. Po skončení importovania certifikátu môžete určiť aplikácie, ktoré ho musia používať v komunikáciách SSL.
13. V navigačnej časti okna vyberte **Manage Applications**, aby sa zobrazil zoznam úloh.
14. Zo zoznamu úloh vyberte **Update Certificate Assignment**, aby sa zobrazil zoznam aplikácií s podporou SSL, ktorým chcete priradiť certifikát.
15. Vyberte niektorú aplikáciu zo zoznamu a kliknite na **Update Certificate Assignment**.
16. Vyberte certifikát, ktorý ste naimportovali a kliknite na **Assign New Certificate**. 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 validáciu.

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 potrebujú užívatelia získať certifikát CA, musia navštíviť webovú stránku tejto CA a riadiť sa pokynmi na uvedenej stránke.

Manažovanie verejných internetových certifikátov 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 príslušný sklad certifikátov na manažovanie verejných certifikátov, ktoré používate na podpisovanie objektov. Tým je sklad certifikátov *OBJECTSIGNING. Keď vytvárate sklad 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 ľavom navigačnom rámci DCM vyberte **Create New Certificate Store**, čím spustíte riadenú úlohu a vyplníte sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia skladu 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 sklad certifikátov, ktorý sa má vytvoriť a kliknite na **Continue**.
4. Vyberte **Yes**, aby sa certifikát vytvoril ako časť vytvárania skladu certifikátov a kliknite na **Continue**.
5. Ako podpisovateľa nového certifikátu vyberte **VeriSign or other Internet Certificate Authority (CA)** a kliknite na **Continue**. Týmto sa zobrazí formulár, ktorý vám umožňuje zadať identifikačnú informácie pre nový certifikát.
6. Vyplňte formulár a kliknite na **Continue**, 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 ľavom navigačnom rámci kliknite na **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte ***OBJECTSIGNING**.
10. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali a kliknite na **Continue**.
11. V navigačnej časti okna vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
12. Zo zoznamu úloh vyberte **Import certificate**, aby sa spustil proces importu podpísaného certifikátu do skladu certifikátov *OBJECTSIGNING. Po dokončení importu certifikátu môžete vytvoriť definíciu aplikácie na používanie certifikátu na podpisovanie objektov.
13. Po obnovení ľavého navigačného rámca vyberte **Manage Applications**, čím zobrazíte zoznam úloh.
14. Zo zoznamu úloh vyberte **Add application**, 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 **Add**. 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 úloha Manage Applications.
17. Zo zoznamu úloh vyberte **Update certificate assignment** a kliknite na **Continue** na zobrazenie zoznamu ID aplikácií podpisujúcich objekty, pre ktoré chcete priradiť certifikát.
18. Zo zoznamu ID aplikácií vyberte svoju aplikáciu a kliknite na **Update Certificate Assignment**.
19. Vyberte certifikát, ktorý ste naimportovali a kliknite na **Assign New Certificate**.

Po dokončení týchto úloh máte všetko, čo potrebujete, aby ste mohli začať podpisovať objekty na zabezpečenie ich integrity.

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

Prijímateľ tiež musí mať kópiu certifikátu CA pre CA, ktorá vydala certifikát, ktorý ste použili na podpísanie objektu. Ak ste objekty podpísali s certifikátom od všeobecne známej internetovej CA, príjemcova verzia DCM už možno obsahuje kópiu potrebného certifikátu CA. Ak si však myslíte, že príjemca kópiu pravdepodobne nemá, kópiu

certifikátu CA môžete priložiť k podpísaným objektom. Kópiu certifikátu lokálnej CA musíte napríklad poskytnúť v prípade, že ste objekty podpísali s certifikátom od súkromnej lokálnej CA. Z bezpečnostných dôvodov musíte certifikát CA dodať v osobitnom balení alebo ho verejne sprístupniť na požiadanie tým, ktorí ho potrebujú.

Manažovanie certifikátov na 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 použite 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 skladu 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 vhodný sklad certifikátov na manažovanie potrebných certifikátov na kontrolu podpisu; ide o sklad certifikátov *SIGNATUREVERIFICATION. Keď vytvoríte tento sklad 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 sklad certifikátov *SIGNATUREVERIFICATION a skopírovať do neho certifikáty zo sklad certifikátov *OBJECTSIGNING. To platí aj vtedy, ak chcete vykonávať kontrolu podpisov pomocou skladu certifikátov *OBJECTSIGNING.

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

1. Spustite DCM.
2. V ľavom navigačnom rámci DCM vyberte **Create New Certificate Store**, čím spustíte riadenú úlohu a vyplníte 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 sklad certifikátov, ktorý sa má vytvoriť a kliknite na **Continue**.

   Poznámka: Ak sklad certifikátov *OBJECTSIGNING existuje, na tomto mieste vás DCM požiada o špecifikovanie, či sa majú do nového skladu certifikátov skopírovať certifikáty, podpisujúce objekty, ako certifikáty na kontrolu podpisu. Ak chcete na overenie podpisov použiť vaše existujúce certifikáty na podpisovanie objektov, vyberte **Yes** a kliknite na **Continue**. Aby ste mohli skopírovať certifikáty zo skladu certifikátov *OBJECTSIGNING, musíte poznať heslo.
4. Špecifikujte heslo pre nový sklad certifikátov a kliknite na **Continue**, aby sa vytvoril sklad certifikátov. Zobrazí sa potvrdzovacia stránka na naznačenie, že bol sklad certifikátov úspešne vytvorený. Teraz môžete použiť tento sklad na manažovanie a použitie certifikátov na kontrolu podpisov objektov.

   Poznámka: Ak ste vytvorili tento sklad, aby ste mohli kontrolovať podpisy na objektoch, ktoré ste podpísali, nerobte to. Pretože vytvárate nové certifikáty na podpisovanie objektov, musíte ich vyexportovať zo skladu certifikátov *OBJECTSIGNING do tohto skladu certifikátov. Ak ich nevyexportujete, nebudete môcť kontrolovať podpisy, ktoré s nimi vytvoríte.

Poznámka: Ak ste vytvorili tento sklad certifikátov, aby ste mohli overovať podpisy na objektoch, ktoré ste dostali z iných zdrojov, musíte v tejto procedúre pokračovať, aby ste do tohto skladu certifikátov mohli importovať certifikáty, ktoré potrebujete.

5. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SIGNATUREVERIFICATION**.
6. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali a kliknite na **Continue**.
7. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
8. Zo zoznamu úloh vyberte **Import certificate**. Táto riadená úloha vás prevedie procesom importovania certifikátov, ktoré potrebujete, do skladu certifikátov, aby ste mohli overovať podpis na objektoch, ktoré ste prijali.
9. Vyberte typ certifikátu, ktorý chcete naimportovať. Zvoľte **Signature verification** na import certifikátu, ktorý ste prijali s podpísanými objektmi a dokončite importovaciu úlohu.

   Poznámka: Ak sklad certifikátov ešte neobsahuje kópiu certifikátu CA pre CA, ktorý vydal certifikát na overovanie podpisu, musíte *najprv* naimportovať certifikát CA. Ak pred importovaním certifikátu na overovanie podpisov nenaimportujete certifikát CA, môžete pri importovaní certifikátu na overovanie podpisov dostať chybovú správu.

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:

Na vystavovanie certifikátov pre iné systémy iSeries použite lokálnu CA
Naučte sa, ako používať súkromnú lokálnu CA na jednom systéme na vydávanie certifikátov za účelom použitia na iných systémoch.

Manažovanie aplikácií 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 definovanýcjh zoznamoch dôveryhodných CA, ktoré používajú aplikácie ako základ pri akceptovaní certifikátov na autentifikáciu klienta.

Manažovanie certifikátov podľa ukončenia platnosti
Preštudujte si, ako máte používať DCM na zobrazovanie a manažovanie certifikátov na základe dátumu ukončenia ich platnosti.

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

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

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

Uloženie kľúčov certifikátov na šifrovací koprocesor IBM
Naučte sa, ako používať nainštalovaný koprocesor na poskytnutie bezpečnejšieho uloženia pre súkromné kľúče vašich certifikátov.

Manažovanie umiestnenia 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).

Manažovanie lokality LDAP pre užívateľské certifikáty
Preštudujte si, ako máte nakonfigurovať DCM na ukladanie užívateľských certifikátov do adresárovej lokality servera LDAP (Lightweight Directory Access Protocol), aby ste EIM (Enterprise Identity Mapping) mohli rozšíriť na prácu s užívateľskými certifikátmi.

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

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

Použitie lokálnej CA na vydávanie certifikátov pre iné systémy iSeries

Na serveri vo vašej sieti už pravdepodobne používate súkromnú lokálnu certifikačnú autoritu (CA). Teraz chcete rozšíriť používanie tejto lokálnej CA na ďalší server nachádzajúci sa vo vašej sieti. Napríklad chcete, aby vaša aktuálna lokálna CA vydala serverový alebo klientsky certifikát pre aplikáciu na ďalšom serveri na používanie pre komunikačné relácie SSL. Alebo chcete používať certifikáty z vašej lokálnej CA na jednom systéme na podpísanie objektov, ktoré ste uložili na inom serveri.

Toto môžete dosiahnuť použitím Správcu digitálnych certifikátov (DCM). Niektoré úlohy vykonáte na serveri, ktorý prevádzkuje lokálnu CA a ostatné vykonáte na sekundárnom serveri, 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: Problém môže nastať v prípade, keď server, na ktorom prevádzkujete lokálnu CA, používa produkt Cryptographic Access Provider, ktorý poskytuje lepšie šifrovanie ako cieľový systém. Pre V5R2 a novšie verzie OS/400 alebo i5/OS je dostupný len Cryptographic Access Provider 5722–AC3, ktorý je súčasne najsilnejším dostupným produktom. V starších vydaniach ste si však mohli nainštalovať iné, slabšie produkty poskytovateľa šifrovaného prístupu (5722–AC1 alebo 5722–AC2), ktoré poskytovali nižšie úrovne funkcie šifrovania. Keď exportujete certifikát (s jeho súkromným kľúčom), systém zašifruje tento súbor, aby bol jeho obsah chránený. 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. Ak používate lokálnu CA na vytvorenie certifikátu za účelom použitia na inom serveri, súbory vytvorené prostredníctvom DCM obsahujú kópiu certifikátu lokálnej CA a aj kópie certifikátov pre množstvo verejných internetových CA.

Úlohy, ktoré musíte vykonať v DCM, sa nepatrne líšia v závislosti od typu certifikátu vydávaný vašou lokálna CA a od úrovne vydania a podmienok na cieľovom systéme.

Vydajte súkromné certifikáty za účelom použitia na inom systéme V5R3, V5R2 alebo V5R1

Ak chcete svoju lokálnu CA použiť na vydanie certifikátov za účelom použitia na inom systéme V5R3, V5R2 alebo V5R1, vykonajte na systéme V5R3, ktorý hosťuje lokálnu CA tieto kroky:

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 **Create Certificate** na zobrazenie zoznamu typov certifikátov, na ktorých vytvorenie môžete použiť lokálnu CA.

   Na vykonanie tejto úlohy nemusíte otvoriť sklad certifikátov. Tieto inštrukcie predpokladajú, že nepracujete v niektorej konkrétnom sklade certifikátov a ani v sklade 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 **Continue** na spustenie riadenej úlohy a dokončenie série formulárov. Vyberte si buď vytvorenie **serverového alebo klientskeho certifikátu pre iný systém** (pre relácie SSL) alebo **certifikát podpisujúci objekty pre iný systém**.

   Poznámka: Ak vytvárate certifikát podpisujúci objekty pre iný systém, na tomto systéme musí bežať V5R1 alebo novšia verzia OS/400 alebo i5/OS, aby bolo možné tento certifikát používať. Pretože cieľový systém musí mať verziu V5R1 alebo novšiu, DCM v lokálnom hostiteľskom systéme vás nepožiada o výber formátu cieľového vydania pre nový certifikát na podpisovanie objektu.
4. Ak vytvárate serverový alebo klientsky certifikát, vyberte úroveň vydania servera, pre ktorý tento certifikát vytvárate. Kliknite na **Continue**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačné informácie pre nový certifikát.

   Poznámka: Vami vybratá 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. Toto zabezpečí kompatibilitu súborov certifikátu so serverom, ktorý bude tento certifikát používať.
5. Vyplňte formulár a kliknite na **Continue**, aby sa zobrazila strana s potvrdením.

Poznámka: Ak na cieľovom systéme existuje sklad 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 existujúceho skladu 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 svojom vlastnom sklade certifikátov a vygeneruje dva súbory, ktoré máte preniesť: súbor kladu certifikátov (prípona .KDB) a súbor požiadavky (prípona .RDB).

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

Vydajte súkromné certifikáty za účelom použitia na serveri V4R5

Ak chcete používať svoju lokálnu CA na vydávanie certifikátov za účelom použitia na serveri V4R5, vykonajte na systéme V5R3 hostujúcom lokálnu CA tieto kroky:

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 **Create Certificate** na zobrazenie zoznamu typov certifikátov, na ktorých vytvorenie môžete použiť lokálnu CA.

   Na vykonanie tejto úlohy nemusíte otvoriť sklad certifikátov. Tieto inštrukcie predpokladajú, že nepracujete v niektorej konkrétneho skladu certifikátov a ani v sklade certifikátov miestnej Certifikačnej autority (CA). Lokálna CA musí existovať na tomto systéme pred tým, ako budete môcť vykonať tieto úlohy.
3. Ako typ certifikátu, ktorý má vydať lokálna CA, vyberte **Server or client certificate for another server** a kliknite na **Continue**, čím spustíte riadenú úlohu a vyplníte sériu formulárov.

   Poznámka: Keďže tento certifikát vytvárate za účelom použitia na serveri V4R5, musíte vybrať **server or client certificate for another iSeries**. Cieľové systémy s vydaním starším ako V5R1 nemôžu používať certifikáty na podpisovanie objektov.
4. Vyberte úroveň vydania servera, pre ktorý tento certifikát vytvárate. Kliknite na **Continue**, aby sa zobrazil formulár, ktorý vám umožňuje zadať identifikačné informácie pre nový certifikát.

   Poznámka: Vami vybratá 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. Toto zabezpečí kompatibilitu súborov certifikátu so serverom, ktorý bude tento certifikát používať.
5. Vyplňte formulár a kliknite na **Continue**, aby sa zobrazila strana s potvrdením.

   Poznámka: Ak na cieľovom systéme existuje sklad 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 existujúceho skladu 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 svojom vlastnom sklade certifikátov a vygeneruje dva súbory, ktoré máte preniesť: súbor skladu certifikátov (prípona .KDB) a súbor požiadavky (prípona .RDB).

   Poznámka: Ak plánujete používať certifikáty v týchto súboroch v existujúcom sklade certifikátov *SYSTEM na cieľovom systéme V4R5, certifikát lokálnej CA nemôžete importovať priamo zo súborov .KDB a .RDB. Je to spôsobené tým, že certifikát CA nie je vo formáte, ktorý funkcia importu v DCM vie rozoznať a použiť. 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 **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
7. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali na hostiteľskom systéme a kliknite na **Continue**.
8. V navigačnej časti okna vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
9. Zo zoznamu úloh vyberte **Export certificate**.
10. Ako typ certifikátu na export vyberte **Certificate Authority (CA)** a kliknite na **Continue**, aby sa zobrazil zoznam certifikátov CA.
11. Vyberte certifikát lokálnej CA zo zoznamu certifikátov (napríklad LOCAL_CERTIFICATE_AUTHORITY). Kliknite na **Export** na zobrazenie formulára, ktorý vám umožní zvoliť cieľ pre certifikát CA.
12. Vyberte **File** a kliknite na **Continue**.
13. Pre exportovaný súbor špecifikujte plne kvalifikovanú cestu a názov súboru a potom kliknite na **Continue**. Zobrazí sa potvrdzovacia strana, ktorá oznamuje, že DCM úspešne vyexportoval súbor.

    Poznámka: Presvedčte sa, že súboru dáte jedinečný názov a príponu. Súboru môžete dať napríklad názov 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 skladu certifikátov, ktoré ste vytvorili (.KDB a .RDB), do cieľového systému V4R5 použite binárny FTP (File Transfer Protocol) alebo inú metódu. Na prenos súboru, ktorý obsahuje exportovaný certifikát lokálnej CA, použite ASCII režim FTP.

Použitie prenesených súborov v cieľovom systéme

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

- Použitie súkromného certifikátu pre relácie SSL v cieľovom systéme V5R3 alebo V5R2
- Použitie súkromného certifikátu pre relácie SSL na cieľovom systéme V5R1
- Použitie súkromného certifikátu na podpisovanie objektov v cieľovom systéme V5R3, V5R2 alebo V5R1
- Použitie súkromného certifikátu pre relácie SSL v cieľovom systéme V4R5

Použitie súkromného certifikátu pre relácie SSL v cieľovom systéme V5R3 alebo V5R2

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie zo skladu certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste v cieľovom systéme V5R3 alebo V5R2 nikdy nepoužili DCM na manažovanie certifikátov pre SSL, v tomto cieľovom systéme nebude tento sklad certifikátov existovať. Úlohy pre použitie prenesených súborov skladu certifikátov, ktorú ste vytvorili na hostiteľskom systéme lokálnej certifikačnej autority (CA), sa líšia na základe toho, či existuje sklad certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie skladu certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM v cieľovom systéme V5R3 alebo V5R2 existuje, prenesené súbory certifikátov môžete používať jedným z dvoch spôsobov:

- Použite prenesené súbory ako sklad certifikátov iného systému.
- Importujte prenesené súbory do existujúceho skladu certifikátov *SYSTEM.

Sklad certifikátov *SYSTEM neexistuje

Ak sklad certifikátov *SYSTEM neexistuje v systéme V5R3 alebo V5R2, v ktorom chcete používať prenesené súbory skladu certifikátov, ako sklad certifikátov *SYSTEM môžete použiť prenesené súbory certifikátov. Ak chcete vytvoriť sklad certifikátov *SYSTEM a súbory certifikátov používať vo vašom cieľovom systéme V5R3 alebo V5R2, postupujte nasledovne:

1. Skontrolujte, či súbory skladu 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 sklad certifikátov *SYSTEM pre cieľový systém. Súbory skladu certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM ich pridal, ako aj kópiu certifikátu lokálnej CA, do súborov skladu 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, sklad certifikátov *SYSTEM už aktuálne existuje na tomto cieľovom systéme. Prenesené súbory nesmiete teda premenovať. Nahradením štandardných súborov vzniknú problémy pri používaní DCM, preneseného skladu certifikátov a jeho obsahu. Namiesto toho musíte zabezpečiť, aby mali jedinečné názvy a sklad prenesených certifikátov musíte použiť ako **Other System Certificate Store**. Ak použijete tieto súbory ako sklad certifikátov iného systému, na určenie, ktoré aplikácie budú certifikát používať, nemôžete použiť DCM.
3. Spustite DCM. Teraz musíte zmeniť heslo pre sklad certifikátov *SYSTEM, ktorý ste vytvorili premenovaním prenesených súborov. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na sklade certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
5. Keď sa zobrazí stránka Certificate Store and Password, zadajte heslo, ktoré ste uviedli v *hostiteľskom* systéme pre sklad certifikátov pri vytváraní certifikátu pre cieľový systém V5R3 alebo V5R2 a kliknite na **Continue**.
6. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Potom môžete určiť, ktoré aplikácie budú používať tento certifikát pre relácie SSL.
7. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
8. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte nové heslo a kliknite na **Continue**.
9. Po tom, čo sa navigačný rámec obnoví, zvoľte v ňom **Manage Certificates** na zobrazenie zoznamu úloh.
10. Zo zoznamu úloh vyberte **Assign certificate** na zobrazenie zoznamu certifikátov v aktuálnom sklade certifikátov.
11. Vyberte certifikát, ktorý ste vytvorili na *hostiteľskom* systéme a kliknite na **Assign to Applications** na zobrazenie zoznamu aplikácií, podporujúcich SSL, ku ktorým môžete priradiť certifikát.
12. Vyberte aplikácie, ktoré budú používať tento certifikát pre relácie SSL a kliknite na **Continue**. 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 validáciu.

Po dokončení týchto krokov môžu aplikácie na cieľovom systéme používať certifikát, vydaný lokálnou CA na inom serveri. Pred začatím používania SSL pre tieto aplikácie však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým ako bude môcť užívateľ pristupovať 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.

Sklad certifikátov *SYSTEM existuje — používanie týchto súborov ako sklad certifikátov iného systému

Ak cieľový systém V5R3 alebo V5R2 už má sklad certifikátov *SYSTEM, musíte sa rozhodnúť, ako budete pracovať so súbormi certifikátov, ktoré ste preniesli do tohto cieľového systému. Môžete vybrať, aby sa prenesené súbory certifikátov použili ako **Other System Certificate Store**. Alebo môžete zvoliť importovať súkromný certifikát a jeho zodpovedajúci certifikát lokálnej CA do existujúceho skladu certifikátov *SYSTEM.

Iné systémové sklady certifikátov sú užívateľom definované sekundárne sklady 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 Other System Certificate Store 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 sklad certifikátov namiesto certifikátu, ktorý konkrétne identifikujete.

Aplikácie IBM iSeries (a mnohé ďalšie aplikácie vývojárov softvéru) sú naprogramované iba na použitie certifikátov v sklade certifikátov *SYSTEM. Ak sa rozhodnete, že prenesené súbory použijete ako sklad certifikátov iného systému, na určenie, ktoré aplikácie budú tento certifikát používať pre relácie SSL, nemôžete použiť DCM. Preto nemôžete nakonfigurovať štandardné aplikácie s povoleným SSL na používanie tohto certifikátu. Ak chcete certifikát používať pre aplikácie iSeries, musíte certifikát importovať z vašich prenesených súborov skladu certifikátov do skladu certifikátov *SYSTEM.

Ak chcete pristupovať na prenesené súbory certifikátov a pracovať s nimi ako s Iným systémovým skladom certifikátov, vykonajte tieto kroky:
1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre sklad certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R2 a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM.

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Ďalej môžete špecifikovať, že certifikát v temto sklade sa použije ako štandardný certifikát.
5. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
6. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte plne kvalifikovanú cestu a názov súboru skladu certifikátov, zadajte nové heslo a kliknite na **Continue**.
7. Po tom, čo sa navigačný rámec obnoví, zvoľte **Manage Certificate Store** a vyberte **Set default certificate** zo zoznamu úloh.

Teraz, keď ste vytvorili a nakonfigurovali Iný systémový sklad certifikátov, všetky aplikácie, ktoré používajú SSL_Init API môžu použiť certifikát z tohoto skladu na vytvorenie SSL relácií.

Sklad certifikátov *SYSTEM existuje — používanie certifikátov v existujúcom sklade certifikátov *SYSTEM

V systéme V5R3 alebo V5R2 môžete certifikáty v prenesených súboroch skladu certifikátov používať v existujúcom sklade certifikátov *SYSTEM. Ak tak chcete urobiť, musíte naimportovať certifikáty zo súborov skladu certifikátov do existujúceho skladu 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 existujúcom sklade certifikátov *SYSTEM musíte súbory otvoriť ako sklad certifikátov iného systému a exportovať ich do skladu certifikátov *SYSTEM.

Na exportovanie certifikátov zo súborov skladu certifikátov do skladu certifikátov *SYSTEM vykonajte na cieľovom systéme V5R2 tieto kroky:
1. Spustite DCM.
2. V navigačnom rámci kliknite na **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, zadajte **Other System Certificate Store**.

3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre sklad certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R2 a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatic login, môžete naraziť na chyby pri exportovaní certifikátov z tohto skladu do skladu certifikátov *SYSTEM.

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi.
5. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
6. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte plne kvalifikovanú cestu a názov súboru skladu certifikátov, zadajte nové heslo a kliknite na **Continue**.
7. Po zaktualizovaní obsahu navigačného okna v ňom vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh a vyberte **Export certificate**.
8. Ako typ certifikátu na export vyberte **Certificate Authority (CA)** a kliknite na **Continue**.

   Poznámka: Pred vyexportovaním certifikátu servera alebo klienta do skladu certifikátov musíte do tohto skladu certifikátov vyexportovať certifikát lokálnej CA. Ak exportujete najprv serverový alebo klientsky certifikát, môžete naraziť na chybu, lebo v sklade certifikátov neexistuje certifikát lokálnej CA.
9. Vyberte na export certifikát miestnej CA a kliknite na **Export**.
10. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
11. Ako cieľový sklad certifikátov zadajte *SYSTEM, zadajte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**. Zobrazí sa správa, ktorá uvádza, že certifikát bol exportovaný úspešne, alebo poskytne informácie o chybe, ak proces exportu zlyhal.
12. Teraz môžete do skladu certifikátov *SYSTEM exportovať serverový alebo klientsky certifikát. Znova vyberte úlohu **Export certificate**.
13. Ako typ certifikátu na export vyberte **Server or client** a kliknite na **Continue**.
14. Vyberte príslušný serverový alebo klientsky certifikát na export a kliknite na **Export**.
15. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
16. Ako cieľový sklad certifikátov zadajte *SYSTEM, zadajte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**. Zobrazí sa správa, ktorá uvádza, že certifikát bol úspešne exportovaný, alebo poskytne informácie o chybe, ak proces exportu zlyhal.
17. Teraz môžete certifikát priradiť aplikácii na použitie pre SSL. V navigačnom rámci kliknite na **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, zadajte ***SYSTEM**.
18. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**.
19. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
20. Zo zoznamu úloh vyberte **Assign certificate** na zobrazenie zoznamu certifikátov v aktuálnom sklade certifikátov.
21. Vyberte certifikát, ktorý ste vytvorili na *hostiteľskom* systéme a kliknite na **Assign to Applications** na zobrazenie zoznamu aplikácií, podporujúcich SSL, ku ktorým môžete priradiť certifikát.
22. Vyberte aplikácie, ktoré budú používať tento certifikát pre relácie SSL a kliknite na **Continue**. 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 validáciu.

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 pristupovať 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.

Použitie súkromného certifikátu pre relácie SSL na cieľovom systéme V5R1

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie zo skladu certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste v cieľovom systéme V5R1 nikdy nepoužili DCM na manažovanie certifikátov pre SSL, v tomto cieľovom systéme nebude tento sklad certifikátov existovať. Úlohy pre použitie prenesených súborov skladu certifikátov, ktorý ste vytvorili na hostiteľskom systéme lokálnej certifikačnej autority (CA), sa líšia na základe toho, či existuje sklad certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie skladu certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM na cieľovom systéme V5R1 existuje, môžete prenesené súbory certifikátov použiť jedným z dvoch spôsobov:

- Použite prenesené súbory ako sklad certifikátov iného systému.
- Importujte prenesené súbory do existujúceho skladu certifikátov *SYSTEM.

Sklad certifikátov *SYSTEM neexistuje

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

1. Skontrolujte, či súbory skladu certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) ktorý 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 sklad certifikátov *SYSTEM pre cieľový systém. Súbory skladu certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov skladu 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, sklad certifikátov *SYSTEM už aktuálne existuje na tomto cieľovom systéme. Prenesené súbory nesmiete teda premenovať. Nahradením štandardných súborov vzniknú problémy pri používaní DCM, preneseného skladu certifikátov a jeho obsahu. Namiesto toho musíte zabezpečiť, aby mali jedinečné názvy a sklad prenesených certifikátov musíte použiť ako **Other System Certificate Store**. Ak použijete tieto súbory ako sklad certifikátov iného systému, na určenie, ktoré aplikácie budú certifikát používať, nemôžete použiť DCM.
3. Spustite DCM. Teraz musíte zmeniť heslo pre sklad certifikátov *SYSTEM, ktorý ste vytvorili premenovaním prenesených súborov. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na sklade certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
5. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre sklad certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R1 a kliknite na **Continue**.
6. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Potom môžete určiť, ktoré aplikácie budú používať tento certifikát pre relácie SSL.
7. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
8. Keď sa zobrazí stránka Certificate Store and Password, zadajte nové heslo a kliknite na **Continue**.
9. Po tom, čo sa navigačný rámec obnoví, zvoľte v ňom **Manage Applications** na zobrazenie zoznamu úloh.

10. Zo zoznamu úloh vyberte **Update Certificate Assignment**, aby sa zobrazil zoznam aplikácií s podporou SSL, ktorým chcete priradiť certifikát.
11. Vyberte niektorú aplikáciu zo zoznamu a kliknite na **Update Certificate Assignment**.
12. Vyberte certifikát, ktorý vydala lokálna CA na *hostiteľskom* systéme a kliknite na **Assign New Certificate**. 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 validáciu.

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 pristupovať 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.

Sklad certifikátov *SYSTEM existuje — používanie týchto súborov ako sklad certifikátov iného systému

Ak cieľový systém V5R1 už má sklad certifikátov *SYSTEM, musíte rozhodnúť, ako sa bude pracovať so súbormi certifikátov. Môžete vybrať, aby sa prenesené súbory certifikátov použili ako **Other System Certificate Store**. Alebo môžete zvoliť importovať súkromný certifikát a jeho zodpovedajúci certifikát lokálnej CA do existujúceho skladu certifikátov *SYSTEM.

Iné systémové sklady certifikátov sú užívateľom definované sekundárne sklady 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 Other System Certificate Store 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 sklad certifikátov namiesto certifikátu, ktorý konkrétne identifikujete.

Aplikácie IBM iSeries (a mnohé ďalšie aplikácie vývojárov softvéru) sú naprogramované iba na použitie certifikátov v sklade certifikátov *SYSTEM. Ak sa rozhodnete, že prenesené súbory použijete ako sklad certifikátov iného systému, na určenie, ktoré aplikácie budú tento certifikát používať pre relácie SSL, nemôžete použiť DCM. Takže štandardné aplikácie iSeries, povolené pre SSL, nemôžete nakonfigurovať na používanie tohto certifikátu. Ak chcete certifikát používať pre aplikácie iSeries, musíte certifikát importovať z vašich prenesených súborov skladu certifikátov do skladu certifikátov *SYSTEM.

Ak chcete pristupovať na prenesené súbory certifikátov a pracovať s nimi ako s Iným systémovým skladom certifikátov, vykonajte tieto kroky:
1. Spustite DCM.
2. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre sklad certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R1 a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM.

Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Ďalej môžete špecifikovať, že certifikát v tomto sklade sa použije ako štandardný certifikát.

5. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
6. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov, uveďte nové heslo a kliknite na **Continue**.
7. Po tom, čo sa navigačný rámec obnoví, zvoľte **Manage Certificate Store** a vyberte **Set default certificate** zo zoznamu úloh.

Teraz, keď ste vytvorili a nakonfigurovali Iný systémový sklad certifikátov, všetky aplikácie, ktoré používajú SSL_Init API môžu použiť certifikát z tohto skladu na vytvorenie SSL relácií.

Sklad certifikátov *SYSTEM existuje — používanie certifikátov v existujúcom sklade certifikátov *SYSTEM

Certifikáty v prenesených súboroch sklade certifikátov môžete použiť v existujúcom sklade certifikátov *SYSTEM na systéme V5R1. Ak tak chcete urobiť, musíte naimportovať certifikáty zo súborov skladu certifikátov do existujúceho skladu 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 existujúcom sklade certifikátov *SYSTEM musíte súbory otvoriť ako sklad certifikátov iného systému a exportovať ich do skladu certifikátov *SYSTEM.

Poznámka: Táto postup popisuje, ako použiť Other System Certificate Store na cieľovom systéme na exportovanie certifikátov z pôvodných súborov skladu certifikátov do skladu certifikátov *SYSTEM. Použitie tejto metódy na pridanie certifikátov do skladu certifikátov *SYSTEM vám môže pomôcť zabrániť možným problémom, keď cieľový systém používa slabší produkt poskytovateľa šifrovaného prístupu (ako je 5722–AC2) ako hostiteľský systém.

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

1. Spustite DCM.
2. V navigačnom rámci kliknite na **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, zadajte **Other System Certificate Store**.
3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Taktiež uveďte heslo, ktoré ste zadali na *hostiteľskom* systéme pre sklad certifikátov, keď ste vytvárali certifikát pre cieľový systém V5R1 a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatic login, môžete naraziť na chyby pri exportovaní certifikátov z tohto skladu do skladu certifikátov *SYSTEM.

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi.
5. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
6. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov, uveďte nové heslo a kliknite na **Continue**.
7. Po zaktualizovaní obsahu navigačného okna v ňom vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh a vyberte **Export certificate**.
8. Ako typ certifikátu na export vyberte **Certificate Authority (CA)** a kliknite na **Continue**.

   Poznámka: Pred vyexportovaním certifikátu servera alebo klienta do skladu certifikátov musíte do tohto skladu certifikátov vyexportovať certifikát lokálnej CA. Ak exportujete najprv serverový alebo klientsky certifikát, môžete naraziť na chybu, lebo v sklade certifikátov neexistuje certifikát lokálnej CA.
9. Vyberte na export certifikát miestnej CA a kliknite na **Export**.

10. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
11. Ako cieľový sklad certifikátov zadajte *SYSTEM, zadajte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**.
12. Teraz môžete do skladu certifikátov *SYSTEM exportovať serverový alebo klientsky certifikát. Znova vyberte úlohu **Export certificate**.
13. Ako typ certifikátu na export vyberte **Server or client** a kliknite na **Continue**.
14. Vyberte príslušný serverový alebo klientsky certifikát na export a kliknite na **Export**.
15. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
16. Ako cieľový sklad certifikátov zadajte *SYSTEM, zadajte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**. 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 **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, zadajte ***SYSTEM**.
18. Keď sa zobrazí stránka Certificate Store and Password, uveďte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**.
19. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
20. Zo zoznamu úloh vyberte **Update Certificate Assignment**, aby sa zobrazil zoznam aplikácií s podporou SSL, ktorým chcete priradiť certifikát.
21. Vyberte niektorú aplikáciu zo zoznamu a kliknite na **Update Certificate Assignment**.
22. Vyberte certifikát, ktorý vydala lokálna CA na *hostiteľskom* systéme a kliknite na **Assign New Certificate**. 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 validáciu.

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 pristupovať 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.

Použitie súkromného certifikátu na podpisovanie objektov v cieľovom systéme V5R3, V5R2 alebo V5R1

Certifikáty, ktoré používate na podpisovanie objektov zo skladu certifikátov *OBJECTSIGNING manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste v cieľovom systéme nikdy nepoužili DCM na manažovanie certifikátov na podpisovanie objektov, v tomto cieľovom systéme nebude tento sklad certifikátov existovať. Úlohy, ktoré musíte vykonať na použitie prenesených súborov skladu certifikátov, ktorú ste vytvorili na hostiteľskom systéme lokálnej (CA), sa líšia na základe toho, či existuje sklad certifikátov *OBJECTSIGNING. Ak sklad certifikátov *OBJECTSIGNING neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie skladu certifikátov *OBJECTSIGNING. Ak sklad certifikátov *OBJECTSIGNING na cieľovom systéme existuje, musíte do nej prenesené certifikáty naimportovať.

Sklad certifikátov *OBJECTSIGNING neexistuje

Úlohy, ktoré vykonáte na použitie súborov skladu 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 v cieľovom systéme V5R3, V5R2 alebo V5R1 s prenesenými súbormi skladu certifikátov neexistuje sklad certifikátov *OBJECTSIGNING, postupujte nasledovne:

1. Skontrolujte, či súbory skladu certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB), ktorý ste vytvorili na systéme, ktorý hosťuje 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 sklad certifikátov *OBJECTSIGNING pre cieľový systém. Súbory skladu certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov skladu certifikátov, keď ste ich vytvorili.

   Upozornenie: Ak váš cieľový systém už má súbory SGNOBJ.KDB a SGNOBJ.RDB v adresári /QIBM/USERDATA/ICSS/CERT/SIGNING, sklad certifikátov *OBJECTSIGNING už aktuálne existuje na tomto cieľovom systéme. Prenesené súbory nesmiete teda premenovať. Nahradením štandardných súborov, podpisujúcich objekty, vzniknú problémy pri používaní DCM, preneseného skladu certifikátov a jeho obsahu. Ak sklad certifikátov *OBJECTSIGNING už existuje, musíte použiť iný postup k tomu, aby ste tieto certifikáty dostali do existujúceho skladu certifikátov.
3. Spustite DCM. Musíte zmeniť heslo pre sklad certifikátov *OBJECTSIGNING. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na sklade certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***OBJECTSIGNING**.
5. Keď sa zobrazí strana na zadanie hesla, zadajte heslo, ktoré ste špecifikovali pre sklad certifikátov pri jeho vytváraní na hostiteľskom systéme a kliknite na **Continue**.
6. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Ďalej môžete vytvoriť definíciu aplikácie na používanie certifikátu na podpisovanie objektov.
7. Po opätovnom otvorení skladu certifikátov vyberte v navigačnej časti okna **Manage Applications**, aby sa zobrazil zoznam úloh.
8. Zo zoznamu úloh vyberte **Add application**, 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 **Add**. 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 **Manage Applications**.
11. Zo zoznamu úloh vyberte **Update certificate assignment** na zobrazenie zoznamu ID aplikácií podpisujúcich objekty, pre ktoré môžete priradiť certifikát.
12. Zo zoznamu ID aplikácií vyberte svoju aplikáciu a kliknite na **Update Certificate Assignment**.
13. Vyberte certifikát, ktorý vytvorila lokálna CA na hostiteľskom systéme a kliknite na **Assign New Certificate**.

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

Keď distribuujete podpísané objekty, ich príjemcovia musia na overovanie podpisu na týchto objektoch používať verziu V5R3, V5R2 alebo V5R1 Správcu digitálnych certifikátov (DCM), aby bolo isté, že údaje nie sú zmenené a aby overili identitu odosielateľa. Aby sa validoval podpis, prijímateľ musí mať kópiu certifikátu na kontrolu podpisu. Kópiu tohto certifikátu musíte poskytnúť ako súčasť balíka podpísaných objektov.

Prijímateľ tiež musí mať kópiu certifikátu CA pre CA, ktorý vydala certifikát, ktorý ste použili na podpísanie objektu. Ak ste objekty podpísali s certifikátom od všeobecne známej internetovej CA, príjemcova verzia DCM už bude mať kópiu potrebného certifikátu CA. Kópiu certifikátu CA však musíte v prípade potreby poskytnúť v osobitnom balení spolu s podpísanými objektmi. Ak ste napríklad objekty podpísali s certifikátom od lokálnej CA, musíte poskytnúť kópiu certifikátu tejto lokálnej CA. Z bezpečnostných dôvodov musíte certifikát CA dodať v osobitnom balení alebo ho verejne sprístupniť na požiadanie tým, ktorí ho potrebujú.

Sklad certifikátov *OBJECTSIGNING existuje

V systéme V5R3, V5R2 alebo V5R1 môžete certifikáty v prenesených súboroch skladu certifikátov používať v existujúcom sklade certifikátov *OBJECTSIGNING. Ak tak chcete urobiť, musíte naimportovať certifikáty zo súborov

skladu certifikátov do existujúceho skladu 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. V cieľovom systéme V5R3, V5R2 alebo V5R1 môžete certifikáty do existujúceho skladu certifikátov *OBJECTSIGNING pridávať otvorením prenesených súborov ako Skladu certifikátov iného systému. Potom môžete vyexportovať tieto certifikáty priamo do skladu certifikátov *OBJECTSIGNING. Musíte exportovať kópiu samotného certifikátu na podpisovanie objektov, a aj certifikátu lokálnej CA z prenesených súborov.

Na vyexportovanie certifikátov zo súborov skladu certifikátov priamo do skladu certifikátov *OBJECTSIGNING vykonajte v cieľovom systéme V5R3, V5R2 alebo V5R1 nasledujúce kroky:

1. Spustite DCM.
2. V navigačnom rámci kliknite na **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, zadajte **Other System Certificate Store**.
3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súborov skladu certifikátov. Taktiež uveďte heslo, ktoré ste použili, keď ste ich vytvárali na hostiteľskom systéme a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatic login, môžete naraziť na chyby pri exportovaní certifikátov z tohto skladu do skladu certifikátov *OBJECTSIGNING.

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi.
5. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte **Other System Certificate Store**.
6. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov, uveďte nové heslo a kliknite na **Continue**.
7. Po zaktualizovaní obsahu navigačného okna v ňom vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh a vyberte **Export certificate**.
8. Ako typ certifikátu na export vyberte **Certificate Authority (CA)** a kliknite na **Continue**.

   Poznámka: Znenie tejto úlohy predpokladá, že keď pracujete s Other System Certificate Store, pracujete s certifikátmi servera alebo klienta. To je preto, lebo tento typ skladu certifikátov je určený na použitie ako sekundárny sklad certifikátov k skladu certifikátov *SYSTEM. Avšak použitie exportovacej úlohy v tomto sklade certifikátov je najjednoduchším spôsobom pridávania certifikátov z prenesených súborov do existujúceho skladu certifikátov *OBJECTSIGNING.
9. Vyberte na export certifikát miestnej CA a kliknite na **Export**.

   Poznámka: Pred vyexportovaním certifikátu na podpisovanie objektov do skladu certifikátov musíte do tohto skladu certifikátov vyexportovať certifikát lokálnej CA. Ak exportujete najprv certifikát na podpisovanie objektov, môžete naraziť na chybu, lebo v sklade certifikátov neexistuje certifikát lokálnej CA.
10. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
11. Ako cieľový sklad certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**.
12. Teraz môžete vyexportovať certifikát podpisujúci objekty, do skladu certifikátov *OBJECTSIGNING. Znova vyberte úlohu **Export certificate**.
13. Ako typ certifikátu na export vyberte **Server or client** a kliknite na **Continue**.
14. Vyberte príslušný certifikát na export a kliknite na **Export**.
15. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
16. Ako cieľový sklad certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**. 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.

Použitie súkromného certifikátu pre relácie SSL v cieľovom systéme V4R5

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie zo skladu certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste v cieľovom systéme V4R5 nikdy nepoužili DCM na manažovanie certifikátov pre SSL, v tomto cieľovom systéme nebude tento sklad certifikátov existovať. Prenesené súbory skladu certifikátov, ktorý ste vytvorili na hostiteľskom systéme lokálnej CA, obsahuje dva certifikáty. Tieto súbory sú serverový 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 skladu certifikátov, sa líšia na základe toho, či existuje sklad certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM neexistuje, môžete prenesené súbory certifikátov použiť ako prostriedok na vytvorenie skladu certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM na cieľovom systéme V5R1 existuje, môžete prenesené súbory certifikátov použiť jedným z dvoch spôsobov:

- Použitie prenesených súborov ako sklad certifikátov iného systému.
- Importovať prenesené súbory do existujúceho skladu certifikátov *SYSTEM.

Sklad certifikátov *SYSTEM neexistuje

Ak sklad certifikátov *SYSTEM neexistuje v systéme V4R5, v ktorom chcete použiť prenesené súbory skladu certifikátov, postupujte nasledovne:

1. Skontrolujte, či súbory skladu certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) ktorý 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 sklad certifikátov *SYSTEM pre cieľový systém. Súbory skladu certifikátov už obsahujú kópie certifikátov pre mnohé verejné internetové CA. DCM pridal tieto, ako aj kópiu certifikátu lokálnej CA, do súborov skladu 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, sklad certifikátov *SYSTEM už aktuálne existuje na tomto cieľovom systéme. Prenesené súbory nesmiete teda premenovať. Nahradením štandardných súborov vzniknú problémy pri používaní DCM, preneseného skladu certifikátov a jeho obsahu. Namiesto toho musíte zabezpečiť, aby mali jedinečné názvy a prenesené súbory skladu certifikátov použiť ako **Other** sklad certifikátov. Ak tieto súbory použijete ako Iný sklad certifikátov, na určenie, ktoré aplikácie budú tento certifikát používať, nemôžete použiť DCM.
3. Spustite DCM. Musíte zmeniť heslo pre sklad certifikátov *SYSTEM. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na sklade certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
4. V navigačnom okne skontrolujte, či je *SYSTEM zobrazená ako sklad certifikátov v roletovom zozname a vyberte **System Certificates** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Certificate Store and Password**.
5. Do príslušných polí pre sklad 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 sklad certifikátov.
6. Zo zoznamu úloh v navigačnej časti okna vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi.
7. Po opätovnom otvorení skladu certifikátov *SYSTEM vyberte zo zoznamu úloh **Work with secure applications**, aby sa zobrazila strana, ktorá vám umožňuje manažovať certifikáty, spojené s konkrétnymi aplikáciami.
8. Zo zoznamu aplikácií vyberte aplikáciu, ktorá bude pre relácie SSL používať prenesený súkromný certifikát.
9. Kliknite na **Work with system certificate** a vyberte certifikát, ktorý vydala lokálna CA na hostiteľskom systéme.
10. Kliknite na **Assign New Certificate**, 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 dôverovala CA, aby mohla autentifikovať certifikáty, ktoré vydá konkrétna CA. Použite stránku **Work with Certificate Authorities** na zabezpečenie, že certifikát CA má v sklade certifikátov stav dôveryhodný. Potom použite stránku **Work with secure applications** 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 validáciu.

Po vykonaní týchto úloh môžu aplikácie v cieľovom systéme V4R5 používať certifikát, vystavený lokálnou CA systému V5R3 v inom systéme iSeries. Pred začatím používania SSL pre tieto aplikácie však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým ako bude môcť užívateľ pristupovať 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.

Sklad certifikátov *SYSTEM existuje — používanie súborov ako Skladu certifikátov iného systému

Ak cieľový systém V4R5 už má sklad certifikátov *SYSTEM, musíte sa rozhodnúť, ako budete pracovať so súbormi certifikátov, ktoré ste preniesli do tohto cieľového systému. Prenesené súbory skladu certifikátov obsahujú dva certifikáty: serverový 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 **Other** systémový sklad certifikátov. Alebo môžete zvoliť importovať súkromný certifikát a jeho zodpovedajúci certifikát CA do existujúceho skladu certifikátov *SYSTEM.

Ak sa rozhodnete prenesené súbory použiť ako Sklad certifikátov **iného** systému, na určenie, ktoré aplikácie budú tento certifikát používať pre relácie SSL, nemôžete použiť DCM. Môžete však určiť certifikát v tomto sklade certifikátov ako štandardný certifikát pre sklad certifikátov. Voľba Other System Certificate Store 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 sklad certifikátov namiesto nejakého konkrétneho certifikátu.

Ak sklad certifikátov *SYSTEM existuje v systéme V4R5, v ktorom chcete použiť prenesené súbory skladu certifikátov, postupujte nasledovne:

1. Spustite DCM. Musíte zmeniť heslo pre sklad certifikátov *OBJECTSIGNING. Zmenou hesla sa umožní DCM uložiť nové heslo, aby ste na sklade certifikátov mohli použiť všetky funkcie manažmentu certifikátov DCM.
2. V navigačnom okne skontrolujte, či je ako sklad certifikátov v roletovom zozname zobrazené OTHER a vyberte **System Certificates** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Certificate Store and Password**.
3. Do príslušných polí zadajte úplnú cestu a názov súboru pre sklad 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 sklad certifikátov.
4. V navigačnej časti okna vyberte zo zoznamu úloh pre systémové certifikáty **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM.

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Ďalej môžete špecifikovať, že certifikát v tomto sklade sa použije ako štandardný certifikát.
5. V navigačnej časti okna vyberte **Work with certificates**, aby sa zobrazila strana, ktorá vám umožňuje vykonať množstvo úloh manažmentu certifikátov.
6. Zo zoznamu certifikátov vyberte certifikát, ktorý chcete používať ako štandardný certifikát pre aktuálny sklad kliknite na **Set default**.

Teraz, keď ste vytvorili a nakonfigurovali Other System Certificate Store, môže akákoľvek aplikácia, ktorá používa API SSL_Init, používať certifikát v nej na vytvorenie relácií SSL.

Sklad certifikátov *SYSTEM existuje — Importovanie súborov do existujúceho skladu certifikátov *SYSTEM

Než naimportujete certifikáty do skladu certifikátov *SYSTEM v systéme V4R5, musíte najprv vyexportovať tieto certifikáty zo skladu certifikátov, ktorý ste vytvorili, do iného súborového formátu. Potom môžete naimportovať certifikáty do skladu certifikátov *SYSTEM z nových súborov. Prenesené súbory skladu certifikátov obsahujú dva certifikáty: serverový alebo klientsky certifikát, ktorý ste vytvorili a certifikát súkromnej lokálnej CA, ktorý ste použili na jeho podpísanie. Do skladu certifikátov *SYSTEM musíte naimportovať certifikát servera aj klienta, ktoré ste vytvorili, ako aj certifikát miestnej súkromnej CA.

Poznámka: Funkcie exportovania, dostupné v DCM pre V4R5, nie sú vyvinuté tak dobre ako funkcie pre V5R3 a ak na exportovanie certifikátu súkromnej lokálnej CA použijete cieľový systém, môžete zaznamenať problémy. Na vyexportovanie *ďalšej* kópie certifikátu lokálnej CA do osobitného súboru musíte preto použiť hostiteľský systém V5R3 a nie cieľový systém V4R5. Po vyexportovaní certifikátu lokálnej CA na hostiteľskom systéme V5R3 môžete manuálne preniesť súbor exportu certifikátu lokálnej CA do cieľového systému V4R5 a vykonať kroky, uvedené ďalej v tejto procedúre, na naimportovanie certifikátu lokálnej CA do skladu 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 sklade certifikátov neexistuje certifikát lokálnej CA.

Na vyexportovanie certifikátu zo súborov skladu certifikátov vykonajte v cieľovom systéme V4R5 nasledujúce kroky:

1. Spustite DCM.
2. V navigačnom okne skontrolujte, či je ako sklad certifikátov v roletovom zozname zobrazené OTHER a vyberte **System Certificates** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Certificate Store and Password**.
3. Zadajte úplnú cestu a názov súboru prenesených súborov skladu certifikátov, uveďte heslo, ktoré ste použili, keď ste ich vytvorili na *hostiteľskom* systéme a kliknite na **OK**. Teraz môžete zmeniť heslo pre sklad certifikátov.
4. V navigačnej časti okna vyberte zo zoznamu úloh pre systémové certifikáty **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

   Poznámka: Skontrolujte, či ste označili voľbu **Automatic login**, keď meníte heslo pre sklad certifikátov. Použitie tejto voľby zaistí, že DCM uloží nové heslo, takže na novom sklade môžete použiť všetky funkcie manažmentu certifikátov DCM. Ak heslo nezmeníte a označíte voľbu Automatic login, môžete naraziť na chyby pri exportovaní certifikátov z tohto sklacu.

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi.
5. V navigačnej časti okna vyberte **Work with certificates**, aby sa zobrazil zoznam certifikátov.
6. Zo zoznamu vyberte požadovaný súkromný certifikát a kliknite na **Export**, aby sa zobrazila strana Export certifikátu.
7. Vyplňte formulár Export certificate.

   Poznámka: Presvedčte sa, že súboru dáte jedinečný názov a príponu. Súboru môžete dať napríklad názov 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 ste museli používať DCM v pôvodnom hostiteľskom systéme V5R3 na exportovanie ďalšej kópie certifikátu lokálnej CA a manuálne ju prenášať v režime ASCII do cieľového systému V4R5. DCM ste museli v tomto cieľovom systéme používať aj na exportovanie súkromného certifikátu servera alebo klienta do súboru. Teraz ste pripravený na import týchto certifikátov do skladu 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 sklade certifikátov neexistuje certifikát lokálnej CA.

Ak chcete certifikáty naimportovať z týchto súborov exportu a určiť, že aplikácie povolené pre SSL ich používajú, v cieľovom systéme V4R5 vykonajte nasledujúce kroky:

1. Spustite DCM.

2. V navigačnom okne skontrolujte, či je *SYSTEM zobrazená ako sklad certifikátov v roletovom zozname a vyberte **System Certificates** na zobrazenie zoznamu dostupných úloh. Zobrazí sa okno **Certificate Store and Password**.
3. Ako sklad certifikátov na otvorenie špecifikujte *SYSTEM, zadajte heslo a kliknite na **Continue**.
4. Certifikát lokálnej CA musíte teraz naimportovať zo súboru exportu, ktorý ste vytvorili v hostiteľskom systéme V5R3. V navigačnej časti okna vyberte **Receive a CA certificate**, aby sa zobrazil formulár.
5. Vyplňte formulár a kliknite na **OK**, aby sa zobrazila strana Receive Certificate Successful. Keď pracujete v sklade 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 dôverovala 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 validáciu.
6. Vyberte aplikácie, ktoré budú dôverovať certifikátu od CA a kliknite na **OK**. Zobrazí sa strana Secure Applications Status na potvrdenie toho, že vybrané aplikácie sú nastavené tak, aby dôverovali tomuto novému certifikátu.
7. Teraz môžete importovať serverový certifikát. V navigačnej časti okna vyberte **Work with certificates**, aby sa zobrazil zoznam certifikátov.
8. Kliknite na **Import**, aby sa zobrazila strana Import Certificate.
9. Vyplňte formulár Import Certificate a kliknite na **OK**, čím sa vrátite na stránku **Work with Certificates**. Skontrolujte, či uvádzate názov súboru, ktorý obsahuje exportovaný serverový 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 súčasného skladu certifikátov. V zozname certifikátov sa objaví aj certifikát, ktorý ste naimportovali.
10. Teraz musíte určiť, ktoré aplikácie budú používať tento naimportovaný súkromný certifikát pre relácie SSL. V navigačnom rámci vyberte **Work with secure applications** na zobrazenie stránky, ktorá vám umožní manažovať certifikáty, združené so špecifickými aplikáciami.
11. Vyberte aplikáciu zo zoznamu a kliknite na **Work with system certificate** na zobrazenie zoznamu certifikátov, ktoré môžete určiť na používanie zvolenej aplikácii pre vytvorenie relácií SSL.
12. Vyberte zo zoznamu certifikát a kliknite na **Assign New Certificate**, aby sa vybratý certifikát priradil k špecifikovanej aplikácii. Navrchu strany sa zobrazí potvrdzovacia správa, ktorá označuje výber certifikátu.

Po dokončení týchto krokov môžu aplikácie na cieľovom systéme V4R5 používať certifikát, vydaný lokálnou CA na inom serveri. Pred začatím používa SSL pre tieto aplikácie však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým ako bude môcť užívateľ pristupovať 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.

Manažovanie aplikácií 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 skladu certifikátov, v ktorom pracujete. Môžete manažovať len aplikácie zo skladu 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:

Vytvorenie definície aplikácie popisuje typy aplikácií, ktoré môžete definovať a s ktorými môžete pracovať.

Manažovanie priradenia certifikátu pre aplikáciu opisuje, ako treba priradiť alebo zmeniť certifikát, ktorý aplikácia používa na vytvorenie relácie SSL alebo na podpisovanie objektov.

Definovanie zoznamu dôveryhodných CA pre aplikáciu opisuje, kedy môžete a kedy musíte zadefinovať, ktorým Certifikačným autoritám môže aplikácia dôverovať v prípade overovania platnosti a akceptovania certifikátov.

Informácie o ďalších úlohách DCM môžete nájsť v online pomoci.

Vytvorenie definícií 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, povolené pre SSL, pomocou API (QSYRGAP, QsyRegisterAppForCertUse), aby sa ID aplikácie vytvorilo v DCM automaticky. Všetky aplikácie IBM s povoleným SSL sú zaregistrované pomocou DCM, aby ste mohli jednoducho používať DCM na priradenie certifikátu týmto aplikáciám, aby mohli 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 sklade 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. Namiesto toho môže definícia aplikácie, ktorú vytvárate, opisovať typ alebo skupinu objektov, ktoré chcete podpísať. Aby ste mohli vytvoriť definíciu aplikácie, podpisujúcej objekty, musíte pracovať v sklade certifikátov *OBJECTSIGNING.

Ak chcete vytvoriť definíciu aplikácie, vykonajte tieto kroky:
1. Spustite DCM.
2. Kliknite na **Select a Certificate Store** a vyberte správny sklad certifikátov. (Je to buď sklad certifikátov *SYSTEM alebo sklad 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 Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Applications**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Add application**, aby sa zobrazil formulár na zadefinovanie aplikácie.

   Poznámka: Ak pracujete v sklade 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 **Add**. Informácie, ktoré môžete špecifikovať pre definíciu aplikácie sa menia podľa typu aplikácie, ktorú definujete. Ak definujete serverovú aplikáciu, môžete tiež určiť, či môže táto aplikácia používať certifikáty na autentifikáciu klienta a či autentifikáciu klienta musí vyžadovať. Môžete tiež špecifikovať, že aplikácia musí pri autentifikovaní certifikátov používať zoznam dôveryhodných CA.

Manažovanie priradení 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 priradiť aplikácii certifikát. Ak chcete aplikácii priradiť certifikát alebo zmeniť priradenie certifikátu pre danú aplikáciu, vykonajte tieto kroky:
1. Spustite DCM.
2. Kliknite na **Select a Certificate Store** a vyberte správnu sklad certifikátov. (Je to buď sklad certifikátov *SYSTEM alebo sklad 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 Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Applications**, aby sa zobrazil zoznam úloh.
5. Ak ste v sklade certifikátov *SYSTEM, zvoľte typ aplikácie, ktorá sa má manažovať. (Zvoľte **Server** alebo **Client** aplikácia, ako je to vhodné.)
6. Zo zoznamu úloh vyberte **Update Certificate Assignment**, aby sa zobrazil zoznam aplikácií, ktorým chcete priradiť certifikát.
7. Zo zoznamu vyberte nejakú aplikáciu a kliknite na **Update Certificate Assignment**, aby sa zobrazil zoznam certifikátov, ktoré môžete priradiť aplikácii.
8. Zo zoznamu vyberte certifikát a kliknite na **Assign New Certificate**. 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 validáciu.

Keď zmeníte alebo odstránite certifikát pre aplikáciu, aplikácia môže a nemusí rozpoznať zmenu, ak je v čase zmeny priradenia certifikátu spustená. Napríklad servery iSeries Access for Windows budú automaticky používať všetky zmeny v certifikáte, ktoré vykonáte. Môžete však 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 Assign certificate, ak chcete priradiť certifikát ku niekoľkým aplikáciám súčasne.

Definovanie zoznamu dôveryhodných CA pre aplikáciu

Aplikácie, ktoré podporujú použitie certifikátov na autentifikáciu klienta počas relácie Secure Sockets Layer (SSL) 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 validáciu.

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 **Select a Certificate Store** a na otvorenie vyberte sklad 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 Certificate Store and Password, uveďte heslo, ktoré ste zadali pre sklad certifikátov, keď ste ho vytvárali a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Applications**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Define CA trust list**.
6. Vyberte typ aplikácie (server alebo klient), pre ktorú chcete definovať zoznam a kliknite na **Continue**.
7. Zo zoznamu vyberte nejakú aplikáciu a kliknite na **Continue**, aby sa zobrazil zoznam certifikátov CA, ktoré použijete na zadefinovanie zoznamu dôveryhodných CA.
8. Vyberte CA, ktorým bude aplikácia dôverovať a kliknite na **OK**. DCM zobrazí správu, ktorou potvrdí váš výber pre zoznam dôveryhodných CA.

Poznámka: Jednotlivé CA môžete jednak vybrať zo zoznamu, alebo môžete stanoviť, že aplikácia bude dôverovať všetkým alebo žiadnej CA v tomto zozname. Pred pridaním certifikátu CA do zoznamu dôveryhodných CA ho tiež môžete zobraziť alebo validovať.

Manažovanie certifikátov podľa ukončenia platnosti

Správca digitálnych certifikátov (DCM) poskytuje podporu pre manažovanie ukončenia platnosti certifikátov, aby umožnil administrátorom manažovať serverové alebo klientske certifikáty, certifikáty podpisovania objektov a užívateľské certifikáty podľa dátumu ukončenia platnosti na lokálnom serveri. Okrem toho, ak DCM nakonfigurujete na prácu s EIM (Enterprise Identity Mapping), užívateľské certifikáty môžete manažovať podľa dátumu ukončenia platnosti v celom podniku.

Používanie DCM na zobrazovanie certifikátov na základe dátumu ukončenia ich platnosti vám umožňuje rýchlo a ľahko zistiť, ktorým certifikátom čoskoro skončí platnosť, takže týmto certifikátom je možné platnosť včas obnoviť.

Poznámka: Pretože certifikát na overovanie podpisu môžete na overovanie podpisu použiť aj v prípade, ak tomuto certifikátu skončila platnosť, DCM neposkytuje podporu pre kontrolovanie doby platnosti týchto certifikátov.

Ak chcete zobrazovať a manažovať certifikáty servera alebo klienta alebo certifikáty na podpisovanie objektov na základe dátumov ukončenia ich platnosti, postupujte nasledovne:

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 **Select a Certificate Store** a vyberte ***OBJECTSIGNING** alebo ***SYSTEM**.
3. Zadajte heslo pre sklad certifikátov a kliknite na **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Check expiration**.
6. Vyberte typ certifikátu, ktorý chcete skontrolovať. Ak ste v sklade certifikátov *SYSTEM, vyberte **Server or client**; ak ste v sklade certifikátov *OBJECTSIGNING, vyberte **Object signing**.
7. V poli **Expiration date range in days (1-365)** zadajte počet dní, pre ktoré chcete zobraziť certifikáty na základe dátumu ukončenia ich platnosti a kliknite na **Continue**. DCM zobrazí všetky certifikáty, ktorých platnosť končí medzi dnešným dátumom a dátumom, ktorý zodpovedá počtu zadaných dní. DCM zobrazí aj všetky certifikáty, ktorých dátumy ukončenia platnosti sú staršie ako dnešný dátum.
8. Vyberte certifikát, ktorý chcete manažovať. Môžete si vybrať, či chcete zobraziť detailné informácie o certifikáte, či chcete certifikát vymazať alebo chcete obnoviť jeho platnosť.
9. Po skončení práce s certifikátmi z tohto zoznamu kliknite na **Cancel**, čím úlohu ukončíte.

Overenie platnosti 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.

validácia aplikácie

Použitie DCM na validáciu definície aplikácie pomáha predchádzať problémom s certifikátmi pre aplikáciu, ak vykonáva nejakú funkciu, ktorá vyžaduje certifikáty. Takéto problémy môžu aplikácii zabrániť v úspešnom zapojení do relácie SSL (Secure Sockets Layer) alebo v úspešnom podpisovaní objektov.

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.

validácia certifikátu

Keď validujete certifikát, DCM kontroluje množstvo položiek, týkajúcich sa certifikátu, aby zaistil autenticitu a platnosť tohto certifikátu. validácia 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 súčasnom sklade 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.

Priradenie certifikátu 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 skladoch 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 **Select a Certificate Store** a vyberte ***OBJECTSIGNING** alebo ***SYSTEM**.
3. Zadajte heslo pre sklad certifikátov a kliknite na **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Assign certificate** na zobrazenie zoznamu certifikátov pre aktuálny sklad certifikátov.
6. Vyberte certifikát zo zoznamu a kliknite na **Assign to Applications** na zobrazenie zoznamu definícií aplikácií pre aktuálny sklad certifikátov.
7. Vyberte jednu alebo viacero aplikácií zo zoznamu a kliknite na **Continue**. Zobrazí sa stránka s potvrdzovacou správou pre váš výber priradenia alebo s chybovým hlásením, ak nastal problém.

Manažovanie umiestnení 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 validácie 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 validácie. 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.

Definovanie umiestnenia CRL

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

1. Spustite DCM.
2. V navigačnej časti okna vyberte **Manage CRL Locations**, aby sa zobrazil zoznam úloh.
3. Zo zoznamu úloh vyberte **Add CRL location** na zobrazenie formulára, ktorý môžete použiť na opis lokality CRL a spôsobu, akým sa DCM alebo aplikácia dostane do tejto lokality.
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 **Manage Certificates** na zobrazenie zoznamu úloh.
6. Zo zoznamu úloh vyberte **Update CRL location assignment** na zobrazenie zoznamu certifikátov CA.
7. Vyberte zo zoznamu certifikát CA, ku ktorému chcete priradiť definíciu umiestnenia CRL, ktorú ste vytvorili a kliknite na **Update CRL Location Assignment**. Zobrazí sa zoznam umiestnení CRL.
8. Vyberte zo zoznamu umiestnenie CRL, ktoré chcete združiť s CA a kliknite na **Update Assignment**. Navrchu 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 adresárový server (LDAP), a aj klientske aplikácie na používanie SSL a v DCM k týmto aplikáciám priradiť certifikát..

O konfigurovaní a používaní adresárového servera (LDAP) iSeries sa dozviete v týchto témach Informačného centra:

- IBM Directory Server for iSeries (LDAP)
  V tejto téme sa dozviete všetko, čo potrebujete vedieť o konfigurovaní a používaní adresárového servera iSeries.
- Povolenie SSL na adresárovom serveri
  Táto téma vysvetľuje, čo musíte urobiť, ak chcete nakonfigurovať váš adresárový server tak, aby ste mohli na bezpečné komunikácie používať SSL.

Uloženie kľúčov certifikátov na šifrovací koprocesor IBM

Ak máte na vašom systéme iSeries nainštalovaný šifrovací koprocesor IBM, pomocou tohto koprocesora môžete bezpečnejšie uložiť 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 tento koprocesor použiť na uloženie súkromného kľúča, musíte zabezpečiť, aby bol tento koprocesor aktivovaný 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.

Uloženie súkromného kľúča certifikátu priamo na koprocesore

Ak chcete prístup k súkromnému kľúču certifikátu a používanie tohto kľúča ešte viac chrániť, môžete si zvoliť uloženie tohto kľúča priamo na šifrovací koprocesor IBM. 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 **Select a Key Storage Location**:
1. Ako voľbu ukladania vyberte **Hardware**.
2. Kliknite na **Continue**. Týmto sa zobrazí strana **Select a Cryptographic Device Description**.
3. Zo zoznamu zariadení vyberte to, ktoré chcete použiť na uloženie súkromného kľúča certifikátu.
4. Kliknite na **Continue**. DCM pokračuje v zobrazovaní strán pre túto úlohu, ako sú identifikačné informácie pre certifikát, ktorý vytvárate alebo obnovujete.

Použitie hlavného kľúča koprocesora na zašifrovanie súkromného kľúča certifikátu

Ak chcete prístup k súkromnému kľúču certifikátu a používanie tohto kľúča ešte viac chrániť, na zašifrovanie súkromného kľúča a jeho uloženie do špeciálneho súboru kľúčov môžete použiť hlavný kľúč šifrovacieho koprocesora IBM. Túto voľbu pamäte pre kľúč môžete vybrať ako súčasť vytvárania alebo obnovy certifikátu v Správcovi digitálnych zariadení.

Predtým, než sa vám podarí použiť túto voľbu, musíte použiť webové rozhranie konfigurácie šifrovacieho koprocesora IBM , aby ste mohli vytvoriť vhodný súbor na uloženie kľúčov. Webové rozhranie konfigurácie koprocesora musíte použiť aj na priradenie súboru na uloženie kľúčov k opisu zariadenia koprocesora, ktorý chcete použiť. K webovému rozhraniu konfigurácie koprocesora sa dostanete zo stránky iSeries Tasks.

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 **Select a Key Storage Location**:

1. Ako voľbu ukladania vyberte **Hardware encrypted**.
2. Kliknite na **Continue**. Týmto sa zobrazí strana **Select a Cryptographic Device Description**.
3. Zo zoznamu zariadení vyberte to, ktoré chcete použiť na šifrovanie súkromného kľúča certifikátu.
4. Kliknite na **Continue**. Ak máte nainštalovaných a spustených viac zariadení koprocesora, zobrazí sa strana **Select Additional Cryptographic Device Descriptions**.

   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 na týchto zariadeniach rovnaký, použite úlohu Master Key Verification vo webovom rozhraní konfigurácie šifrovacieho koprocesora 4758. K webovému rozhraniu konfigurácie koprocesora sa dostanete zo stránky iSeries Tasks.
6. Kliknite na **Continue**. DCM pokračuje v zobrazovaní strán pre túto úlohu, ako sú identifikačné informácie pre certifikát, ktorý vytvárate alebo obnovujete.

Manažovanie miestnenia požiadavky pre PKIX CA

Certifikačná autorita (CA) PKIX (Public Key Infrastructure for X.509) je CA, ktorá vystavuje certifikáty na základe najnovších noriem X.509 pre internet na implementovanie infraštruktúry verejného kľúča. 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. Keďže sa tieto štandardy prijímajú v širšom rozsahu, CA, ktoré sú v súlade so špecifikáciou PKIX sa stanú viac dostupnými. Pomocou CA, kompatibilnej s PKIX, môžete zisťovať, či vaše požiadavky na bezpečnosť vyžadujú striktné riadenie prístupu k prostriedkom, ktoré poskytujú užívateľom vaše aplikácie, povolené pre SSL. 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 **Manage PKIX Request Location**, 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 **Add**. 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 **Create Certificate**.

Manažovanie lokality LDAP pre užívateľské certifikáty

Štandardne Správca digitálnych certifikátov (DCM) ukladá užívateľské certifikáty, ktoré vydáva lokálna certifikačná autorita (CA) s užívateľskými profilmi i5/OS. Správcu digitálnych certifikátov (DCM) môžete však nakonfigurovať spolu s EIM (Enterprise Identity Mapping), takže keď lokálna Certifikačná autorita (CA) vystaví užívateľské certifikáty, verejná kópia certifikátu sa uloží do konkrétnej adresárovej lokality servera LDAP (Lightweight Directory Access Protocol). Kombinovaná konfigurácia EIM s DCM vám umožňuje ukladať užívateľské certifikáty do adresárovej lokality LDAP, aby tieto certifikáty boli jednoducho dostupné pre ďalšie aplikácie. Táto kombinovaná konfigurácia vám umožňuje aj používanie EIM na manažovanie užívateľských certifikátov ako typu užívateľskej identity v rámci vášho podniku.

Poznámka: Ak chcete, aby užívateľ uložil do lokality LDAP certifikát od inej CA, tento užívateľ musí vykonať úlohu **Assign a user certificate**.

EIM je technológia eServer, ktorá vám umožňuje vo vašom podniku manažovať užívateľské identity, vrátane užívateľských profilov a certifikátov i5/OS. Ak chcete EIM používať na manažovanie užívateľských certifikátov, musíte pred vykonaním všetkých úloh konfigurácie DCM vykonať tieto úlohy konfigurácie EIM:

1. Na nakonfigurovanie EIM použite sprievodcu **EIM Configuration** v programe **iSeries Navigator**.
2. Vytvorte identifikátor EIM pre každého užívateľa, ktorého chcete mať zapojeného do EIM.
3. Vytvorte cieľové priradenie medzi každým identifikátorom EIM a užívateľským profilom v lokálnom užívateľskom registri i5/OS. Použite názov definície registra EIM pre lokálny užívateľský register i5/OS, ktorý ste zadali v sprievodcovi **EIM Configuration**. **Poznámka:** Viac informácií o konfigurovaní EIM nájdete v téme EIM v Informačnom centre iSeries.

Po vykonaní úloh, potrebných pre konfiguráciu EIM, musíte na dokončenie celkovej konfigurácie na spoločné používanie EIM a DCM vykonať nasledujúce úlohy:

1. V DCM použite úlohu **Manage LDAP Location** na určenie adresára LDAP, ktorý DCM použije na uloženie užívateľského certifikátu, vytvoreného lokálnou CA. Lokalita LDAP sa nemusí nachádzať na lokálnom serveri a ani to nemusí byť rovnaký LDAP server, ktorý používa EIM. Keď konfigurujete lokalitu LDAP v DCM, DCM používa určený adresár LDAP na uloženie všetkých užívateľských certifikátov, ktoré vystavuje lokálna CA. DCM používa lokalitu LDAP aj na uloženie užívateľských certifikátov, spracovaných úlohou **Assign a user certificate**, namiesto uloženia certifikátu s užívateľským profilom.
2. Spustite príkaz CVTUSRCERT (**Convert User Certificates**) . Tento príkaz skopíruje existujúce užívateľské certifikáty do príslušnej lokality adresára LDAP. Tento príkaz však kopíruje len certifikáty pre užívateľa, ktorý mal vytvorené cieľové priradenie medzi identifikátorom EIM a užívateľským profilom. Príkaz potom vytvorí zdrojové priradenie medzi každým certifikátom a priradeným identifikátorom EIM. Príkaz používa na zadefinovanie názvu užívateľskej identity pre zdrojové priradenie charakteristický názov (DN) predmetu certifikátu, DN vystavovateľa a hash týchto DN spolu s verejným kľúčom certifikátu .

Podpisovanie objektov

Na podpisovanie objektov môžete použiť tri metódy. Môžete napísať program, ktorý volá API podpísania objektu. Môžete použiť Správcu digitálnych certifikátov (DCM) na podpisovanie objektov. Od verzie V5R2 môžete na podpisovanie objektov, keď ich balíte pre distribúciu na iné server, použiť aj funkciu Management Central navigátora iSeries Navigator.

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 je, že môžete tiež podpisovať príkazové (*CMD) objekty. Nemôžete podpisovať objekty, ktoré sú uložené na iných serveroch.

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 vytvorený sklad certifikátov *OBJECTSIGNING, buď ako časť procesu vytvorenia lokálnej CA, alebo ako časť procesu manažovania certifikátu na podpisovanie objektov z verejnej internetovej CA.
- Sklad 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.

Použitie 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 **Select a Certificate Store** a na otvorenie vyberte ***OBJECTSIGNING**.
3. Zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Signable Objects**, aby sa zobrazil zoznam úloh.
5. Z tohto zoznamu úloh vyberte **Sign an object**, aby sa zobrazil zoznam definícií aplikácií, ktoré môžete použiť na podpisovanie objektov.
6. Vyberte niektorú aplikáciu a kliknite na **Sign an object**, 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 **Update Certificate Assignment** z **Manage Applications**, 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 **Continue**. Alebo zadajte umiestnenie adresára a kliknite na **Browse**, aby sa zobrazil obsah tohto adresára a mohli ste z neho vybrať objekty na podpísanie.

   Poznámka: Názov objektu musíte začať s úvodnou lomkou, inak narazíte na chybu. Na popísanie časti adresára, ktorú chcete podpísať tiež môžete použiť určité zástupné znaky. Tieto zástupné znaky sú hviezdička (*****, ktorá špecifikuje ″ľubovoľný počet znakov,″ a otáznik (**?**), ktorý špecifikuje ″ľubovoľný jeden znak.″ Ak chcete napríklad podpísať všetky objekty v konkrétnom adresári, môžete zadať /mydirectory/*; ak chcete podpísať všetky programy v konkrétnej knižnici, môžete zadať /QSYS.LIB/QGPL.LIB/*.PGM. Tieto zástupné znaky môžete použiť len v poslednej časti názvu cesty; napríklad výsledkom zadania /mydirectory*/názov súboru je chybová správa. Ak chcete na prezeranie zoznamu obsahov knižníc alebo adresárov použiť funkciu Browse, pred kliknutím na **Browse** musíte ako súčasť názvu cesty zadať zástupný znak.
8. Vyberte voľby spracovania, ktoré chcete použiť pre podpísanie vybratého objektu alebo objektov a kliknite na **Continue**.

   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 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 **Continue**. Alebo zadajte umiestnenie adresára a kliknite na **Browse**, 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, v protokole úloh si pozrite úlohu **QOBJSGNBAT**.

Overenie podpisov 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 sklad certifikátov *SIGNATUREVERIFICATION na manažovanie vašich certifikátov na kontrolu podpisu.

  Poznámka: Kontrolu podpisov môžete vykonať počas práce so skladom 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 oba sklady certifikátov. Sklad certifikátov *SIGNATUREVERIFICATION však musí existovať a musí obsahovať kópiu certifikátu, ktorý podpísal objekt, aj v prípade, že kontrolu podpisu robíte počas práce v sklade certifikátov *OBJECTSIGNING.
- Sklad certifikátov *SIGNATUREVERIFICATION musí obsahovať kópiu certifikátu, ktorý podpísal objekty.
- Sklad certifikátov *SIGNATUREVERIFICATION musí obsahovať kópiu certifikátu CA, ktorá vydala certifikát, ktorý podpísal objekty.

Použitie 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 **Select a Certificate Store** a na otvorenie vyberte ***SIGNATUREVERIFICATION**.
3. Zadajte heslo pre sklad certifikátov *SIGNATUREVERIFICATION a kliknite na **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Signable Objects**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Verify object signature**, 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 **Continue**. Alebo zadajte umiestnenie adresára a kliknite na **Browse**, aby sa zobrazil obsah tohto adresára a mohli ste z neho vybrať objekty na kontrolu podpisu.

   Poznámka: Môžete použiť aj bežné zástupné znaky na popísanie časti adresára, ktorú chcete skontrolovať. Tieto zástupné znaky sú hviezdička (*****, ktorá špecifikuje ″ľubovoľný počet znakov,″ a otáznik (**?**), ktorý špecifikuje ″ľubovoľný jeden znak.″ Ak chcete napríklad podpísať všetky objekty v konkrétnom adresári, môžete zadať /mydirectory/*; ak chcete podpísať všetky programy v konkrétnej knižnici, môžete zadať /QSYS.LIB/QGPL.LIB/*.PGM. Tieto zástupné znaky môžete použiť len v poslednej časti názvu cesty; napríklad výsledkom zadania /mydirectory*/názov súboru je chybová správa. Ak chcete na prezeranie zoznamu obsahov knižníc alebo adresárov použiť funkciu Browse, pred kliknutím na **Browse** musíte ako súčasť názvu cesty zadať zástupný znak.
7. Zvoľte voľby spracovania, ktoré chcete použiť pre overenie podpisu na vybranom objekte alebo objektoch a kliknite na **Continue**.

   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 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 **Continue**. Alebo zadajte umiestnenie adresára a kliknite na **Browse**, 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, 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

Pri práci so Správcom digitálnych certifikátov (DCM) a s certifikátmi môžete zaznamenať chyby, ktoré vám bránia v realizácii vašich úloh a cieľov. Veľa bežných chýb alebo problémov, ktoré môžete spozorovať, spadá do mnohých kategórií, akými sú napríklad:

Odstránenie problémov 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.

Odstránenie problémov so skladom certifikátov a databázou kľúčov
V týchto informáciách sa dozviete viac o bežných problémoch so skladom certifikátov a databázou kľúčov, na ktoré môžete naraziť a o spôsobe, ako ich odstrániť.

Odstránenie problémov 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.

Odstránenie problémov s HTTP serverom
V týchto informáciách sa dozviete viac o bežných problémoch s HTTP severom, na ktoré môžete naraziť a o spôsobe, ako ich odstrániť.

Odstránenie problémov v úlohe Assign a user certificate
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.

Odstránenie problémov 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 prehľadať aj Informačné centrum a externé webové stránky IBM na internete.
Vaše heslo pre sklad certifikátov Miestna Certifikačná autorita (CA) a *SYSTEM nefunguje.	Heslá rozlišujú veľkosť písmen. Presvedčte sa, či je preraďovač veľkosti písmen v tej istej polohe, ako keď ste špecifikovali heslo.
Keď ste použili úlohu **Select a Certificate Store**, váš pokus o resetovanie hesla zlyhal.	Funkcia vynulovania pracuje len vtedy, ak DCM uložil heslo. DCM ukladá heslo automaticky, keď vytvoríte sklad certifikátov. Avšak ak zmeníte (alebo zresetujete) heslo pre Other System Certificate Store, potom musíte označiť voľbu **Automatic login**, aby DCM pokračoval v ukladaní hesla.
	Taktiež ak presúvate sklad certifikátov z jedného systému na druhý, musíte zmeniť heslo pre sklad certifikátov na novom systéme, aby ste zaistili, že ho DCM uloží automaticky. Na zmenu hesla musíte zadať pôvodné heslo pre sklad certifikátov, keď ju otvoríte v novom systéme. Voľbu resetovať heslo nemôžete použiť, kým máte otvorený sklad 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 sklad certifikátov, ktorý budete používať ako sklad certifikátov iného systému, musíte označiť voľbu **Automatic login**, keď meníte heslo, na zabezpečenie, že DCM uloží nové heslo pre tento typ skladu certifikátov.

Problém	Možné riešenie
	V SST (System Service Tools) pod voľbou **Work with system security** označte hodnotu, priradenú k atribútu **Allow new digital certificates**. Ak je tento atribút nastavený na 2 (Nie), potom heslo skladu certifikátov nemôže byť resetované. Hodnotu pre tento atribút môžete zobraziť alebo zmeniť príkazom STRSST a zadaním hesla a užívateľského ID pre servisné nástroje. Potom vyberte voľbu **Work with system security**. ID užívateľa Servisných nástrojov je pravdepodobne ID užívateľa QSECOFR.
Nemôžete nájsť zdroj pre certifikát CA na jeho prijatie do systému.	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 sklad certifikátov *SYSTEM.	Umiestnenie súboru skladu certifikátov musí byť /qibm/userdata/icss/cert/server/default.kdb. Ak sklad certifikátov neexistuje, musíte použiť na jeho vytvorenie DCM. Použite úlohu **Create New Certificate Store**.
Dostali ste od DCM chybovú správu a táto chyba sa ďalej vyskytuje potom, čo ste ju odstránili.	Vymažte pamäť cache prehliadača. Nastavte veľkosť pamäte cache na 0, ukončite a opätovne spustite prehliadač.
Máte problém s adresárovým serverom (LDAP), napríklad keď sa bezprostredne po priradení certifikátu zobrazia informácie o bezpečnej aplikácii, priradenia certifikátov sa nezobrazujú. Tento problém sa objaví častejšie pri používaní iSeries Navigator s prehliadačom Netscape Communicator. Vaša preferencia pre cache pamäť prehliadača je nastavená tak, aby dokument v cache pamäti porovnávala s dokumentom v sieti **Once per session**.	Zmeňte vašu štandardnú preferenciu, aby vždy kontrolovala ukladanie do pamäte cache.
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 overte, či má váš server správnu hodnotu ofsetu UTC (dspsysval qutcoffset). Ak zaregistrujete letný čas, váš posun môže byť nastavený nesprávne.
Keď ste sa pokúšali importovať certifikát Entrust, dostali ste základnú chybovú správu 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 toto nastane, certifikát nebude v správnom formáte, keď sa ho pokúsite použiť na serveri. Tento problém riešia úpravy niektorých webových stránok. Iné webové stránky sú navrhnuté tak, aby sa tomuto problému vyhli. Musíte porovnať zobrazenie originálneho certifikátu s výsledkami vloženia, pretože vložené informácie musia vyzerať rovnako.

Odstránenie problémov so skladom certifikátov a databázou kľúčov

Nasledujúcu tabuľku použite na nájdenie informácií, ktoré vám pomôžu odstrániť niektoré bežnejšie problémy so skladmi 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 začiatočnej lomky.

Problém	Možné riešenie

Zlyhalo vytvorenie databázy kľúčov alebo vytvorenie lokálnej CA.	Zistite, či nie je konflikt s názvom súboru. Tento konflikt môže byť v inom súbore, než je ten, ktorý ste žiadali. DCM sa pokúša chrániť užívateľské údaje v adresároch, ktoré vytvára, aj keď mu tieto súbory zabraňujú úspešne vytvárať súbory, keď to potrebuje.
	
	Vyriešte tento problém skopírovaním všetkých konfliktných súborov do iného adresára a ak to bude možné, použite funkcie DCM na vymazanie príslušných súborov. Ak na to nemôžete použiť DCM, súbory vymažte manuálne z pôvodného adresára integrovaného súborového systému, kde spôsobovali 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. Potrebujete vytvoriť novú lokálnu CA po presunutí nasledujúcich súborov:
	`/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 nový sklad 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`

	Pravdepodobne vám chýba LPP (prerequisite licensed program), ktorého nainštalovanie vyžaduje DCM. Skontrolujte zoznam požiadaviek DCM a zabezpečte, aby boli všetky licenčné programy správne nainštalované.
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.

Problém	Možné riešenie
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 zo skladu certifikátov a potom sa pokúste zmeniť heslo. Ak máte vo svojom sklade certifikátov certifikáty so skončenou platnosťou, sú neplatné. Keďže sú tieto certifikáty neplatné, funkcia zmeny hesla pre sklad 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 skladu certifikátov. Neplatné certifikáty (so skončenou platnosťou) musíte zo skladu 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. Preštudovanie dokumentácie k aplikácii HTTP Server for iSeries vám pomôže pri konfigurovaní bezpečnej inštancie servera HTTP na používanie validačného zoznamu.

Odstránenie problémov 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.
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 pod tým istým menom, ktoré je v užívateľskom certifikáte v prehliadači. Od systému, na ktorý pristupujete získajte iný užívateľský certifikát. Systémový administrátor musí mať istotu, že sklad certifikátov (databáza kľúčov) stále dôveruje Certifikačnej autorite, ktorá podpísala užívateľské a systémové certifikáty.
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. Musíte tiež skontrolovať, či je váš server názvov domén správne nastavený.
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.	Ide 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.

Problém	Možné riešenie
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 užívateľovi stále hlási, že táto CA ešte nemá dôveru.	Pomocou DCM nastavte **CA status** na **enabled**, aby mohla byť táto CA označená ako dôveryhodná.
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 ide 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.

Odstránenie problémov s HTTP Server for iSeries

V nasledujúcej tabuľke môžete nájsť informácie, ktoré vám pomôžu pri odstraňovaní niektorých častých problémov s HTTP serverom, ktoré môžu nastať 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. Konfiguračný súbor vo V5R1 alebo neskorších verziách musí mať **SSLAppName** nastavené pomocou administračného rozhrania servera HTTP. Aj konfigurácia musí mať nakonfigurovaného virtuálneho hostiteľa, ktorý používa port SSL, s **SSL** nastaveným pre virtuálneho hostiteľa na **Enabled**. Musia tam byť aj dve direktívy **Listen**, určujúce dva rozličné porty, jeden pre SSL a druhý nie pre SSL. Tieto sa nastavujú na stránke **General Settings**. Skontrolujte, či je vytvorená inštancia servera a či je serverový certifikát podpísaný.
Proces registrácie inštancie servera HTTP ako bezpečnej aplikácie potrebuje objasnenie.	Na serveri prejdite do rozhrania HTTP Server Administration, kde môžete nastaviť konfiguráciu HTTP servera. Najprv musíte zadefinovať virtuálneho hostiteľa, aby ste mohli povoliť SSL. Po zadefinovaní virtuálneho hostiteľa musíte uviesť, že tento virtuálny hostiteľ používa port SSL, zadefinovaný predtým v direktíve **Listen** (na stránke **General Settings**). Potom musíte na povolenie SSL v predtým nakonfigurovanom virtuálnom hostiteľovi použiť stránku **SSL with Certificate Authentication** pod **Security**. Všetky zmeny musia byť aplikované na konfiguračný súbor. Uvedomte si, že registrovanie vašej inštancie nevyberá automaticky, ktoré certifikáty bude táto inštancia používať. Predtým, než sa pokúsite ukončiť a potom znova spustiť inštanciu vášho servera, musíte pomocou DCM priradiť k vašej aplikácii konkrétny certifikát.
Máte ťažkosti pri nastavovaní HTTP servera pre validačné zoznamy a nepovinnú autentifikáciu klientov.	Možnosti nastavenia tejto inštancie nájdete v dokumentácii k aplikácii HTTP Server for iSeries.

Problém	Možné riešenie
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 HTTP server zaviedol premennú prostredia HTTPS_CLIENT_CERTIFICATE. Tieto API môžete nájsť v téme informačného centra i5/OS APIs. Pravdepodobne si budete chcieť pozrieť aj tento validačný zoznam alebo API, ktoré sa týkajú certifikátov: • QsyListVldlCertificates a QSYLSTVC • QsyRemoveVldlCertificate a QRMVVC • QsyCheckVldlCertificate a QSYCHKVC • QsyParseCertificate a QSYPARSC, atď.
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.
Server HTTP sa nepodarí spustiť s **SSL**, nastaveným na **Enabled** a v protokole úloh sa zobrazí chybová správa HTP8351. Pri zlyhaní servera HTTP chybový protokol pre server HTTP ukáže chybu, že operácia inicializácie SSL zlyhala, s návratovým kódom chyby 107.	Chyba 107 znamená, že sa ukončila platnosť certifikátu. Pomocou DCM priraďte k aplikácii iný certifikát; napríklad QIBM_HTTP_SERVER_MY_SERVER. Ak inštancia servera, ktorá sa nedá spustiť, je server *ADMIN, **SSL** dočasne nastavte na **Disabled**, aby ste na serveri *ADMIN mohli používať DCM. Potom pomocou DCM priraďte iný certifikát k aplikácii QIBM_HTTP_SERVER_ADMIN a znova skúste **SSL** nastaviť na **Enable**.

Odstránenie problémov s priradením užívateľského certifikátu

Keď používate úlohu **Assign a user certificate** Správca digitálnych certifikátov (DCM) vám zobrazí informácie o certifikáte, aby ste ho pred registrovaní certifikátu schválili. Ak DCM nemôže certifikát zobraziť, môže to byť spôsobené jednou z nasledujúcich 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 pamäte cache. Pokúste sa vymazať pamäť cache prehliadača a zopakujte úlohu. Prehliadač vás požiada o vybratie certifikátu.
2. K tomuto môže dôjsť aj v prípade, ak váš prehliadač nakonfigurujete tak, že nezobrazuje zoznam výberov a tento prehliadač obsahuje len jeden certifikát od Certifikačnej autority (CA) v zozname certifikačných autorít, ktorým server dôveruje. Skontrolujte konfiguračné nastavenia vášho prehliadača a v prípade potreby ich zmeňte. Váš prehliadač vás potom požiada o vybratie certifikátu. Ak nemôžete predložiť certifikát od CA, ktorej server dôveruje, certifikát nemôžete priradiť. Spojte sa s vaším administrátorom DCM.
3. Certifikát, ktorý chcete zaregistrovať, je už zaregistrovaný pomocou DCM.
4. Certifikačná autorita, ktorá vystavila tento certifikát, nie je pre príslušný systém alebo aplikáciu označená ako dôveryhodná. 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 skladu certifikátov *SYSTEM. Alebo bude administrátor pravdepodobne musieť použiť úlohu **Set CA status**, aby túto CA povolil ako dôveryhodnú a tým odstránil tento problém.
5. Nemáte certifikát na registráciu. Môžete skontrolovať užívateľské certifikáty vo vašom prehliadači, aby ste videli, či ide o tento problém.
6. 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.
7. IBM HTTP Server aktuálne nie je nastavený na vykonávanie registrácie certifikátov pomocou SSL a klientskej autentifikácie na zabezpečenej inštancii administračného servera. Ak nefunguje žiadny z predošlých tipov na odstránenie problémov, spojte sa so správcom vášho systému a nahláste mu vzniknutý problém.

Ak chcete **Assign a user certificate**, musíte byť pripojený do Správcu digitálnych certifikátov (DCM) pomocou SSL relácie. Ak pri výbere úlohy **Assign a user certificate** nepoužívate SSL, DCM zobrazí správu, že musíte použiť SSL.

Správa obsahuje tlačidlo, pomocou ktorého 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 môžete vidieť krátky zoznam ostatných zdrojov, z ktorých sa môžete naučiť viac o digitálnych certifikátoch a spôsobe ich použitia na vylepšenie vašej bezpečnostnej politiky:

- **Webová stránka VeriSign**
  Webová stránka certifikačnej autority VeriSign Web poskytuje rozsiahlu knižnicu tém, zaoberajúcich sa digitálnymi certifikátmi ako aj mnohými ďalšími predmetmi, týkajúcimi sa bezpečnosti internetu.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Príručka IBM Redbook sa zameriava na rozšírenie bezpečnosti siete V5R1. Táto príručka Redbook obsahuje mnoho tém, vrátane spôsobu používania funkcií podpisovania objektov, DCM (Digital Certificate Manager), podpory 4758 Cryptographic Coprocessor pre SSL, atď.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  Táto publikácia Redbook popisuje, čo všetko môžete robiť s digitálnymi certifikátmi na vašom serveri. Vysvetľuje, ako nastaviť rôzne servery a klientov na použitie certifikátov. Ďalej uvádza príklady kódu a informácie o spôsobe používania i5/OS API na manažovanie a používanie digitálnych certifikátov v užívateľských aplikáciách.
- **RFC Index Search**
  Táto webová stránka poskytuje prehľadávateľný archív RFC (Request for Comments). RFC popisujú štandardy pre internetové protokoly, ako je SSL, PKIX a iné, ktoré sa týkajú použitia digitálnych certifikátov.

Príloha. Vyhlásenia

Tieto informácie boli vytvorené pre produkty a služby ponúkané v USA.

IBM nemusí produkty, služby alebo komponenty, o ktorých sa hovorí v tomto dokumente, ponúkať vo všetkých krajinách. Informácie o produktoch a službách, aktuálne dostupných vo vašej krajine, môžete získať od zástupcu spoločnosti IBM. Žiadne odkazy na produkt, program alebo službu spoločnosti IBM neznamenajú, ani z nich nevyplýva, že musí byť použitý len tento produkt, program alebo služba spoločnosti IBM. Môžete použiť ľubovoľný funkčne ekvivalentný produkt, program alebo službu, ktoré neporušujú práva duševného vlastníctva IBM. Užívateľ však zodpovedá za to, aby zhodnotil a overil používanie takéhoto produktu, programu alebo služby.

Spoločnosť IBM môže vlastniť patenty alebo patenty v schvaľovacom konaní pokrývajúce predmetné záležitosti opísané v tomto dokumente. Text tohto dokumentu vám nedáva žiadne licencie na tieto patenty. Informácie o licenciách získate u výrobcu na adrese:

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

Požiadavky na licencie ohľadne dvojbajtových (DBCS) informácií získate od IBM Intellectual Property Department vo svojej krajine alebo ich zašlite písomne na:

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

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE", BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nepovoľujú zrieknutie sa výslovných ani mlčky predpokladaných záruk v určitých operáciách, preto sa na vás toto vyhlásenie nemusí vzťahovať.

Tento dokument môže obsahovať technické nepresnosti alebo tlačové chyby. Informácie uvedené v tomto dokumente podliehajú priebežným zmenám; tieto zmeny budú zapracované do nových vydaní. IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch opísaných v tejto publikácii.

Akékoľvek odkazy v tejto publikácii na iné webové stránky, než stránky firmy IBM, sú poskytované len pre vaše pohodlie a v žiadnom prípade neslúžia ako súhlas s týmito webovými stránkami. Materiály na týchto webových stránkach nie sú súčasťou materiálov k tomuto produktu firmy IBM a ich použitie je na vaše vlastné riziko.

| Spoločnosť IBM môže použiť alebo distribuovať ľubovoľné vami poskytnuté informácie vhodným zvoleným spôsobom
| bez toho, aby tým voči vám vznikli akékoľvek záväzky.

Držitelia licencií tohto programu, ktorí si želajú mať informácie o tomto programe kvôli povoleniu: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto programu) a (ii) spoločného používania vymenených informácií by mali kontaktovať:

| IBM Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť v niektorých prípadoch dostupné až po zaplatení príslušného poplatku.

Licenčný program spomínaný v týchto informáciách a všetky pre tento program dostupné licenčné materiály poskytuje spoločnosť IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement alebo ľubovoľnej ekvivalentnej zmluvy medzi nami.

Akékoľvek tu uvedené údaje o výkone, boli určené v kontrolovanom prostredí. Preto sa môžu výsledky získané v iných prevádzkových prostrediach výrazne odlišovať. Niektoré merania boli vykonané vo vývojovom systéme a preto nie je žiadna záruka, že budú tieto merania rovnaké aj na všeobecne dostupných systémoch. Navyše, niektoré merania mohli byť vykonané extrapoláciou. Aktuálne výsledky sa môžu rôzniť. Užívatelia týchto dokumentov by si mali overiť príslušné údaje pre svoje konkrétne prostredie.

Všetky vyhlásenia týkajúce sa budúceho smerovania a zámerov spoločnosti IBM sa môžu zmeniť alebo odvolať bez predchádzajúceho upozornenia a predstavujú len ciele a plány spoločnosti IBM.

Tieto informácie obsahujú príklady údajov a hlásení, používaných v každodenných obchodných operáciách. S cieľom čo najväčšej zrozumiteľnosti tieto príklady obsahujú mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s názvami a adresami skutočných obchodných spoločností je čisto náhodná.

Ochranné známky

Nasledujúce pojmy sú ochrannými známkami spoločnosti International Business Machines Corporation v USA alebo iných krajinách:

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

Lotus, Freelance a WordPro sú ochranné známky spoločnosti International Business Machines Corporation a Lotus Development Corporation v USA alebo iných krajinách.

Microsoft, Windows, Windows NT a logo Windows sú ochrannými známkami spoločnosti Microsoft Corporation v v USA alebo iných krajinách.

Ostatné názvy spoločností, produktov a služieb môžu byť ochrannými známkami alebo servisnými známkami iných spoločností.

Podmienky sťahovania a tlače publikácií

Povolenie na používanie vybratých publikácií, ktoré si chcete stiahnuť, je podmienené vaším súhlasom s nasledujúcimi podmienkami.

Osobné použitie: Tieto publikácie môžete kopírovať len na svoje osobné nekomerčné použitie pod podmienkou, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto publikácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce, bez výslovného súhlasu spoločnosti IBM.

Komerčné použitie: V rámci vášho podniku môžete kopírovať, distribuovať a prezentovať tieto publikácie len za predpokladu, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto publikácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce mimo vášho podniku bez výslovného súhlasu spoločnosti IBM.

Okrem povolení výslovne vyjadrených v tomto dokumente, nie sú pre uvedené publikácie alebo informácie, údaje, softvér alebo iné duševné vlastníctvo v nich obsiahnuté, udelené žiadne iné výslovné alebo mlčky predpokladané povolenia, oprávnenia alebo práva.

IBM si vyhradzuje právo vypovedať oprávnenia uvádzané v tomto dokumente kedykoľvek, ak usúdi, že používanie týchto publikácií poškodzuje jej záujmy alebo ak spoločnosť IBM zistí, že vyššie uvedené inštrukcie nie sú náležite dodržiavané.

Stiahnuť, exportovať a re-exportovať môžete tieto informácie len v tom prípade, ak vyhovujú všetkým platným zákonom a predpisom, vrátane zákonov a predpisov USA týkajúcich sa exportu. IBM NEPOSKYTUJE ŽIADNU ZÁRUKU NA OBSAH TÝCHTO PUBLIKÁCIÍ. TIETO PUBLIKÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL

Všetky materiály sú chránené autorským právom IBM Corporation.

Stiahnutím alebo vytlačením publikácie z týchto stránok vyjadrujete svoj súhlas s týmito podmienkami.

Vytlačené v USA