Systémy IBM - iSeries

Bezpečnosť
Správca digitálnych certifikátov

Verzia 5, vydanie 4

Systémy IBM - iSeries

Bezpečnosť
Správca digitálnych certifikátov

Verzia 5, vydanie 4

Poznámka

Pred použitím týchto informácií a produktu, ktorý podporujú, si určite prečítajte informácie v “Vyhlásenia”, na strane 79.

Deviate vydanie (február 2006)

Toto vydanie sa týka verzie 5, vydania 4, modifikácie 0 produktu IBM i5/OS (číslo produktu 5722-SS1) a všetkých nasledujúcich vydaní a modifikácií, ak nie je v nových vydaniach určené inak. Táto verzia nebeží na všetkých modeloch RISC (reduced instruction set computer) a nebeží ani na modeloch CISC.

Obsah

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. Mnoho služieb a aplikácií iSeries, napríklad server FTP, Telnet a HTTP poskytuje podporu SSL na zabezpečenie dôvernosti údajov.

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

Ak na centrálne manažovanie certifikátov pre vaše aplikácie použijete bezplatnú vlastnosť Správca digitálnych certifikátov (DCM), využitie podpory certifikátov v iSeries je jednoduché. 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 V5R4

Táto téma opisuje, ktoré informácie sú v tomto vydaní nové alebo výrazne zmenené.

Nové informácie o obnove certifikátov

Tieto nové informácie podrobne opisujú proces obnovy existujúcich certifikátov pomocou lokálneho alebo internetového CA.

- “Obnova existujúceho certifikátu” na strane 51

Nové informácie o importovaní certifikátov

Tieto nové informácie podrobne opisujú proces importovania certifikátov, ktoré sa nachádzajú v súboroch vo vašom serveri alebo v súboroch z iného servera.

- “Importovanie certifikátu” na strane 52

Rozšírenie informácií o zoznamoch zrušených certifikátov (CRL) a protokole LDAP (Lightweight Directory Access Protocol)

Tieto témy boli zaktualizované a obsahujú informácie o vytváraní anonymnej väzby k serveru LDAP za účelom spracovania CRL.

- “Manažovanie umiestnení CRL” na strane 65
- “Riadenie umiestenia LDAP pre užívateľské certifikáty” na strane 68
- “Umiestnenia Zoznamu odmietaných certifikátov (CRL)” na strane 6

Ako určiť, čo je nové alebo zmenené

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.

Ak chcete nájsť ďalšie informácie o novinkách alebo zmenách v tomto vydaní, pozrite si časť Poznámka pre užívateľov.

Vytlačiteľné súbory PDF

Na tejto stránke sa dozviete, ako vytlačiť celú príručku ako súbor PDF.

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

Uloženie 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 hore uvedený odkaz).
2. Ak používate prehliadač Internet Explorer, kliknite na **Save Target As**. Ak používate prehliadač Netscape Communicator, kliknite na **Save Link As**.
3. Prejdite do adresára, do ktorého chcete uložiť dokument PDF.
4. Kliknite na **Save**.

Prevzatie programu Adobe Acrobat Reader

Na prezeranie alebo tlač týchto PDF potrebujete program Adobe Acrobat Reader. Jeho kópiu môžete prevziať z webovej lokality spoločnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Koncepty DCM

Tieto informácie si pozrite, ak sa chcete lepšie oboznámiť s digitálnymi certifikátmi a s ich fungovaním. Získajte informácie o rôznych typoch certifikátov a možnosti ich použita, ako časti vašej bezpečnostnej politiky.

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 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

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 rozlišovacieho názvu a iných 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 používať certifikát na identifikovanie koncového bodu pripojenia virtuálnej súkromnej siete (VPN) iSeries, musíte zadať informácie pre tieto rozšírenia.

Súvisiace koncepty

"Charakteristický názov"
Tieto informácie vás oboznámia s identifikačnými charakteristikami digitálnych certifikátov.

Obnovenie platnosti certifikátov

Proces obnovenia platnosti certifikátu, ktorý používa Správca digitálnych certifikátov (DCM), je rôzny na základe 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 novo vystaveného 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.

Charakteristický názov

Tieto informácie vás oboznámia s identifikačnými charakteristikami digitálnych certifikátov.

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 vydávanie súkromných certifikátov, môžete pomocou rozšírení poskytnúť pre certifikát dodatočné informácie o DN, vrátane:

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

Súvisiace koncepty

“Rozšírenia certifikátov” na strane 3
Rozšírenia certifikátov sú informačné polia, ktoré poskytujú ďalšie informácie o certifikáte.

Digitálne podpisy

Digitálny podpis elektronického dokumentu alebo iného objektu sa vytvára pomocou istého typu kryptografie a je ekvivalentný osobnému podpisu na písanom dokumente.

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 pristupujete k objektu obsahujúcemu digitálny podpis, môžete podpis objektu overiť, aby ste skontrolovali platnosť zdroja objektu (napríklad či preberaná aplikácia 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, aby to bolo pre jeho zákazníkov nenákladné a pohodlné. 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.

Súvisiace koncepty

"Certifikačná autorita (CA)"
Certifikačná autorita (CA) je dôveryhodná centrálna administračná entita, ktorá môže vystavovať digitálne certifikáty užívateľom a serverom.

"Kryptografia" na strane 8
Tieto informácie vás oboznámia s kryptografiou a s tým, ako digitálne certifikáty pomocou kryptografických funkcií poskytujú bezpečnosť.

"Dvojica verejného a súkromného kľúča"
Každý digitálny certifikát má priradený pár kryptografických kľúčov, ktorý pozostáva zo súkromného a verejného kľúča.

Dvojica verejného a súkromného kľúča

Každý digitálny certifikát má priradený pár kryptografických kľúčov, ktorý pozostáva zo súkromného a verejného kľúča.

Poznámka: Certifikáty na kontrolu podpisov predstavujú výnimku z tohto pravidla a 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. Tieto digitálne podpisy zabezpečujú spoľahlivosť pôvodu objektu a poskytujú prostriedky na kontrolu integrity objektu.

Súvisiace koncepty

"Digitálne podpisy" na strane 4
Digitálny podpis elektronického dokumentu alebo iného objektu sa vytvára pomocou istého typu kryptografie a je ekvivalentný osobnému podpisu na písanom dokumente.

"Certifikačná autorita (CA)"
Certifikačná autorita (CA) je dôveryhodná centrálna administračná entita, ktorá môže vystavovať digitálne certifikáty užívateľom a serverom.

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 platných povoľovacích údajov. CA používa svoj súkromný kľúč na vytvorenie digitálneho podpisu certifikátu, ktorý vydáva na overovanie pôvodu certifikátu. Ostatní môžu používať verejný kľúč certifikátu CA na overovanie autenticity certifikátov, ktoré CA vydáva a podpisuje.

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 lokálne CA vydá certifikát, DCM ho automaticky priradí k užívateľskému profilu systému iSeries alebo k identite iného užívateľa. 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.

Súvisiace koncepty

“Digitálne podpisy” na strane 4
Digitálny podpis elektronického dokumentu alebo iného objektu sa vytvára pomocou istého typu kryptografie a je ekvivalentný osobnému podpisu na písanom dokumente.

“Dvojica verejného a súkromného kľúča” na strane 5
Každý digitálny certifikát má priradený pár kryptografických kľúčov, ktorý pozostáva zo súkromného a verejného kľúča.

Umiestnenia Zoznamu odmietaných certifikátov (CRL)

Certificate Revocation List (CRL) je súbor, ktorý obsahuje všetky neplatné a zrušené certifikáty pre konkrétnu Certifikačnú autoritu (CA).

Certifikačné autority periodicky aktualizujú svoje zoznamy CRL a sprístupňujú ich ostatným na zverejnenie do adresárov LDAP (Lightweight Directory Access Protocol). Niektoré CA, ako je SSH vo Fínsku, zverejňujú ich CRL sami v LDAP adresároch, na ktoré môžete priamo pristúpiť. Ak CA zverejní svoj vlastný CRL, certifikát túto skutočnosť oznámi zahrnutím rozšírenia distribučného bodu CRL vo forme Uniform Resource Identifier (URI).

Správca digitálnych certifikátov (DCM) vám umožňuje definovať a manažovať informácie o umiestnení CRL, aby ste zabezpečili prísnejšiu autentifikáciu pre certifikáty, ktoré používate alebo akceptujete od ostatných. Definícia umiestnenia CRL popisuje umiestnenie, prístupové informácie a Lightweight Directory Access Protocol (LDAP) server, ktorý obsahuje CRL.

Pri pripájaní k serveru LDAP musíte zadať DN a heslo, aby sa zabránilo anonymnej väzbe k serveru LDAP. Anonymná väzba k serveru LDAP neposkytuje potrebnú úroveň oprávnení na prístup k atribútom typu ″critical”, napríklad CRL. V takom prípade môže DCM validovať certifikát s odvolanou platnosťou, pretože nemôže z CRL získať správny stav. Ak chcete k LDAP pristupovať anonymne, musíte použiť webový administratívny nástroj pre adresárový server a pomocou úlohy ″Manažovať schému″ zmeniť triedu bezpečnosti (označovanú tiež ako ″trieda prístupu″) atribútov **certificateRevocationList** a **authorityRevocationList** z hodnoty ″critical″ na ″normal″.

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 .

Súvisiace koncepty

"Overenie platnosti certifikátov a aplikácií" na strane 64
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.

Súvisiace úlohy

"Manažovanie umiestnení CRL" na strane 65
Správca digitálnych certifikátov (DCM) vám umožňuje definovať a manažovať informácie o umiestnení zoznamu zrušených certifikátov (CRL) špecifickej certifikačnej autority, ktoré sa použijú v rámci procesu validácie certifikátu.

Sklady certifikátov

Sklad certifikátov je špeciálny súbor databázy kľúčov, ktorý Správca digitálnych certifikátov (DCM) používa na uloženie digitálnych certifikátov.

Sklad certifikátov obsahuje súkromný kľúč certifikátu, pokiaľ ste na ukladanie kľúča nezvolili použitie kryptografického koprocesora 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 iSeries (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.

Sklad certifikátov iného systému
Tento sklad certifikátov poskytuje alternatívne umiestnenie skladu pre certifikáty servera alebo klienta, ktoré používate pre SSL relácie. 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 SSL relácie. 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 vo vašom systéme nainštalovaný kryptografický koprocesor IBM, môžete pre certifikáty vybrať iné možnosti uloženia súkromných kľúčov (s výnimkou certifikátov podpisujúcich objekty). 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.

Súvisiace koncepty

“Typy digitálnych certifikátov” na strane 27
Tieto informácie vás oboznámia s rôznymi typmi digitálnych certifikátov a ich použitím v Správcovi digitálnych certifikátov (DCM).

Kryptografia

Tieto informácie vás oboznámia s kryptografiou a s tým, ako digitálne certifikáty pomocou kryptografických funkcií poskytujú bezpečnosť.

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 môže server alebo užívateľ použiť súkromný kľúč na ″podpísanie″ objektu a príjemca môže použiť zodpovedajúci verejný kľúč na dešifrovanie digitálneho podpisu a overenie zdroja a integrity objektu.

Súvisiace koncepty

"Digitálne podpisy" na strane 4
Digitálny podpis elektronického dokumentu alebo iného objektu sa vytvára pomocou istého typu kryptografie a je ekvivalentný osobnému podpisu na písanom dokumente.

"SSL (Secure Sockets Layer)"
Secure Sockets Layer (SSL), pôvodne vytvorený spoločnosťou Netscape, je priemyselný štandard pre šifrovanie relácií medzi klientmi a servermi.

Kryptografické koprocesory IBM pre iSeries

Šifrovací koprocesor poskytuje pre vyvíjanie bezpečných aplikácií elektronického obchodu osvedčené šifrovacie služby, zabezpečujúce súkromie a integritu.

Použitie kryptografických koprocesorov IBM pre iSeries pridáva do vášho systému schopnosť kryptografického spracovania s vysokou bezpečnosťou. Ak máte vo vašom systéme nainštalovaný a aktivovaný šifrovací koprocesor, môžete ho použiť na poskytnutie bezpečnejšieho uloženia vašich súkromných kľúčov pre certifikáty.

Kryptografický 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.

Súvisiace koncepty

"Ukladanie kľúčov certifikátov v kryptografickom koprocesore IBM" na strane 66
Dozviete sa tu, ako pomocou nainštalovaného koprocesora poskytnúť bezpečnejší úložný priestor pre súkromné kľúče vašich certifikátov.

SSL (Secure Sockets Layer)

Secure Sockets Layer (SSL), pôvodne vytvorený spoločnosťou Netscape, je priemyselný štandard pre šifrovanie relácií medzi klientmi a servermi.

SSL šifruje pomocou asymetrickej kryptografie (alebo kryptografie s verejnými kľúčmi) relácie medzi serverom a klientom. 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 server a každého klienta. Aj keď by neoprávnení užívatelia odchytili a dešifrovali kľúč relácie (čo je nepravdepodobné), nemôžu ho použiť na odpočúvanie neskorších relácií.

Súvisiace koncepty

"Kryptografia" na strane 8
Tieto informácie vás oboznámia s kryptografiou a s tým, ako digitálne certifikáty pomocou kryptografických funkcií poskytujú bezpečnosť.

"Typy digitálnych certifikátov" na strane 27
Tieto informácie vás oboznámia s rôznymi typmi digitálnych certifikátov a ich použitím v Správcovi digitálnych certifikátov (DCM).

Definície aplikácií

Tieto informácie vás oboznámia s definíciami aplikácií v DCM a s ich používaním na konfigurovanie SSL a podpisovanie objektov.

V Správcovi digitálnych certifikátov (DCM) môžete manažovať dva typy definícií aplikácií:

- 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 iSeries s povoleným SSL sa registrujú v DCM, takže k nim môžete pomocou DCM jednoducho priradiť certifikát, aby mohli vytvárať relácie 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.

Súvisiace koncepty

“Manažovanie aplikácií v DCM” na strane 60
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.

Súvisiace úlohy

“Vytvorenie definícií aplikácie” na strane 61
V tejto téme sa dozviete o dvoch rôznych typoch aplikácií, ktoré môžete definovať a pracovať s nimi.

Overenie platnosti

Správca digitálnych certifikátov (DCM) poskytuje úlohy, ktoré vám umožnia validovať certifikát alebo aplikáciu na overenie rôznych vlastností, ktoré 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 zaručuje, že v aplikáciách, ktoré používajú certifikát na bezpečnú komunikáciu alebo podpisovanie objektov, by nemalo dôjsť k problémom pri používaní certifikátu.

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.

| Ak nakonfigurujete mapovanie LDAP (Lightweight Directory Access Protocol) na používanie CRL, Správca
| digitálnych certifikátov pri validovaní certifikátu kontrolujte CRL, aby sa uistil, že sa certifikát v CRL nenachádza.
| Aby však proces validácie správne skontroloval CRL, adresárový server (server LDAP), nakonfigurovaný pre
| mapovanie LDAP, musí obsahovať požadované CRL. V opačnom prípade nebude validácia certifikátu správna. Aby ste
| zabránili validácii certifikátu s odvolanou platnosťou, musíte zadať DN a heslo pre vytvorenie väzby. Taktiež, ak pri
| konfigurovaní mapovania LDAP nezadáte DN a heslo, väzba k serveru LDAP bude anonymná. Anonymná väzba k
| serveru LDAP neposkytuje potrebnú úroveň oprávnenia na prístup k atribútom typu ″critical” a CRL je typu “critical”.
| V takom prípade môže DCM validovať certifikát s odvolanou platnosťou, pretože nemôže z CRL získať správny stav.

Ak chcete k LDAP pristupovať anonymne, musíte použiť webový administratívny nástroj pre adresárový server a pomocou úlohy ″Manažovať schému″ zmeniť triedu bezpečnosti (označovanú tiež ako ″trieda prístupu″) atribútov **certificateRevocationList** a **authorityRevocationList** z hodnoty ″critical″ na ″normal″.

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.

Súvisiace koncepty

“Overenie platnosti certifikátov a aplikácií” na strane 64
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.

Scenáre DCM

Tu môžete nájsť dva scenáre, ktoré ilustrujú typické schémy implementácie certifikátov a ktoré vám pomôžu naplánovať vašu vlastnú implementáciu certifikátov ako súčasť bezpečnostnej politiky iSeries. Každý scenár poskytuje tiež všetky potrebné konfiguračné úlohy, ktoré musíte vykonať na použitie scenára tak, ako je opísaný.

Správca digitálnych certifikátov a podpora digitálnych certifikátov v systéme iSeries vám umožňuje pomocou certifikátov viacerými spôsobmi zlepšiť vašu bezpečnostnú politiku. 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 pristupovať k webovým lokalitám a iným internetovým službám pomocou SSL (Secure Sockets Layer). 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. V závislosti od konfigurácie DCM môžete pomocou neho tiež priradiť certifikát užívateľa k jeho užívateľskému profilu iSeries 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 požiadavky na systém a softvér a všetky úlohy konfigurovania, ktoré musíte vykonať pri realizácii scenára.

Súvisiace informácie

Scenáre pre podpisovanie objektov

Scenár: Používanie certifikátov na externú autentifikáciu

V tomto scenári sa naučíte, kedy a ako používať certifikáty ako autentifikačný mechanizmus na ochranu a obmedzenie prístupu verejných užívateľov k verejným alebo extranetovým prostriedkom a aplikáciám.

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

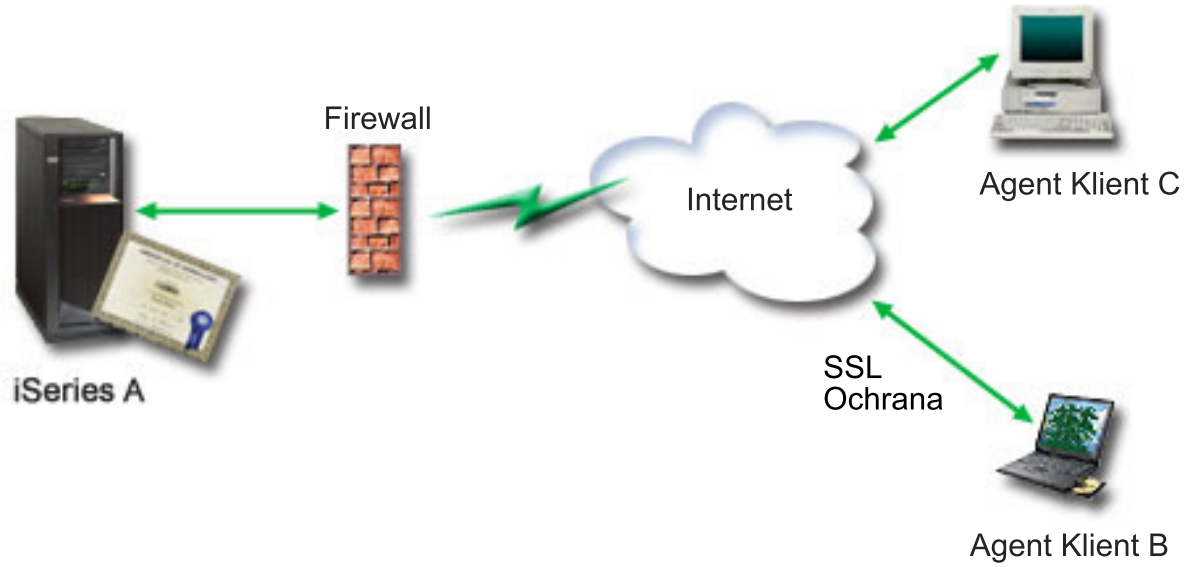
V tomto scenári chce spoločnosť MyCo, Inc. používať digitálne certifikáty na ochranu informácií o výpočte sadzieb, ktoré poskytujú ich aplikácie autorizovaným verejným užívateľom. Táto spoločnosť chce podľa možnosti aj bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolený prístup k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

- iSeries A je server, ktorý hosťuje aplikáciu spoločnosti na výpočet sadzieb.
- iSeries A používa i5/OS verzia 5 vydanie 4 (V5R4).
- iSeries A má nainštalovaný a nakonfigurovaný produkt Správca digitálnych certifikátov (voľba i5/OS 34) a produkt IBM HTTP Server for i5/OS (5722–DG1).
- V iSeries A sa vykonáva aplikácia na výpočet sadzieb, ktorá je nakonfigurovaná takto:
  - 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.
- Keď klienti B a C pristupujú k aplikácii na výpočet sadzieb, iSeries A poskytuje svoj certifikát na zriadenie relácie SSL.

- Po inicializácii relácie SSL požiada systém iSeries A klientov B a C o poskytnutie platného mena užívateľa a hesla, aby im povolil prístup k aplikácii na výpočet sadzieb.

Klientske systémy agentov - klient B a klient C

- Klienti B a C sú nezávislí agenti, ktorí pristupujú na aplikáciu na výpočet sadzieb.
- 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 v systéme iSeries A, ktorý poskytuje svoj certifikát ich klientskemu softvéru, aby autentifikoval svoju identitu a inicializoval reláciu SSL.
- Klientsky softvér v klientoch B a C je nakonfigurovaný tak, aby za účelom inicializovania relácie SSL akceptoval certifikát zo systému iSeries A.
- Po začatí relácie SSL musia klienti B a C poskytnúť platné meno užívateľa a heslo, aby im systém iSeries A povolil prístup k aplikácii.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:

- Aplikácia na výpočet sadzieb v iSeries A je generická aplikácia, ktorú je možné nakonfigurovať na používanie SSL. Väčšina aplikácií, vrátane mnohých aplikácií iSeries, 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.
- Aplikácia na výpočet sadzieb môže vyžadovať certifikáty na 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.
- Systém iSeries A spĺňa požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
- V iSeries predtým ešte nikto nenakonfiguroval ani nepoužíval DCM.
- Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
- iSeries A nemá nainštalovaný kryptografický koprocesor IBM.

Úlohy konfigurovania

Súvisiace úlohy

“Spustenie Správcu digitálnych certifikátov” na strane 37
Dozviete sa tu, ako pristupovať k vlastnosti Správca digitálnych certifikátov (DCM) vo vašom systéme.

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
Je váš systém i5/OS vydania V5R42 (5722-SS1)?	Áno
Je vo vašom systéme nainštalovaná voľba 34 systému i5/OS?	Áno
Je vo vašom systéme nainštalovaný produkt IBM HTTP Server for i5/OS (5722–DG1) a je spustená inštancia servera Správa?	Áno

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

Pracovný list s požiadavkami	Odpovede
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 mohli vykonať potrebné úlohy na dokončenie vašej implementácie certifikátov, musíte o nej získať tieto informácie:

Tabuľka 2. Plánovací pracovný list pre konfiguráciu implementácie certifikátov

Plánovací pracovný list pre iSeries A	Odpovede
Budete prevádzkovať vašu vlastnú lokálnu CA alebo budete certifikáty pre vaše aplikácie získavať od verejnej CA ?	Získanie certifikátu od verejnej CA
Hosťuje systém iSeries A aplikácie, pre ktoré chcete povoliť 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 **Označenie certifikátu**: ver_cert_mojaspol **Bežný názov**: mojaspol_uctvony_server@mojaspol.com **Organizačná jednotka**: Účtovné oddelenie **Názov organizácie**: mojaspol **Lokalita alebo mesto**: Ľubovoľné_mesto **Štát alebo provincia**: Ľubovoľný **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

Vytvorenie požiadavky o certifikát servera alebo klienta

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 autora podpisu pre nový certifikát vyberte **VeriSign alebo inú internetovú certifikačnú autoritu (CA)** a kliknutím na **Pokračovať** zobrazte formulár pre zadanie identifikačných informácií 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: Keď zatvoríte túto stránku, údaje sa stratia a nebude ich možné obnoviť.
8. Keď zatvoríte túto stránku, údaje sa stratia a nebude ich možné obnoviť.
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.

Konfigurácia aplikácie na používanie SSL

Keď prijmete váš podpísaný certifikát späť z verejnej certifikačnej autorita (CA), môžete pokračovať v procese aktivovania komunikácií SSL (Secure Sockets Layer) pre vašu verejnú aplikáciu. Vašu aplikáciu musíte nakonfigurovať na používanie SSL predtým, než začnete pracovať s vaším podpísaným certifikátom. Keď konfigurujete niektoré aplikácie, napríklad HTTP Server for iSeries, na používanie SSL, tieto aplikácie vygenerujú jedinečné ID aplikácie a zaregistrujú ho v Správcovi digitálnych certifikátov (DCM). 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. Taktiež, ak sa chcete dozvedieť viac o konfigurovaní množstva bežných aplikácií IBM na používanie SSL, pozrite si tému SSL (Secure Sockets Layer) v Informačné centrum iSeries.

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

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 **Sklad certifikátov a heslo**, zadajte heslo, ktoré ste zadali pri vytváraní skladu certifikátov a kliknite na **Pokračovať**.
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.

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.

(Voliteľné): Definovanie zoznamu dôveryhodných certifikačných autorít pre vyžadujúcu aplikáciu

Aplikácie, ktoré podporujú používanie certifikátov na autentifikáciu klientov počas relácie SSL (Secure Sockets Layer), musia určiť, či akceptujú 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 **Sklad certifikátov a heslo**, zadajte heslo, ktoré ste zadali pri vytváraní skladu certifikátov a kliknite na **Pokračovať**.
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

V tomto scenári sa naučíte používať certifikáty ako autentifikačný mechanizmus na ochranu a obmedzenie prostriedkov a aplikácií vo vašich interných serveroch, ktoré môžu používať interní užívatelia.

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. Ste zodpovedný za spravovanie tejto internej webovej lokality, ktorej fungovanie zabezpečuje IBM HTTP Server for i5/OS (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 pristúpiť.

Preto sa rozhodnete nastaviť súkromnú lokálnu certifikačnú autoritu (CA) a všetkým zamestnancom vydať certifikáty, ktoré si zamestnanci priradia k svojim užívateľským profilom iSeries. Tento typ implementácie súkromných certifikátov vám umožňuje presnejšie riadiť prístup k citlivým údajom, ako aj riadiť súkromie údajov prostredníctvom SSL. Na záver, keď budete vydávať certifikáty vy sami, máte zvýšenú pravdepodobnosť, že vaše údaje zostanú bezpečné a budú na ne pristupovať len konkrétne osoby.

Výhody scenára

Tento scenár má nasledovné výhody:

- 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 iSeries na riadenie prístupu k aplikáciám a údajom.
  - Chcete prevádzkovať vlastnú Certifikačnú autoritu (CA).

- Použitie certifikátov na autentifikáciu klientov vám umožňuje jednoduchšie priradenie certifikátu k užívateľskému profilu autorizovaného užívateľa iSeries. 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

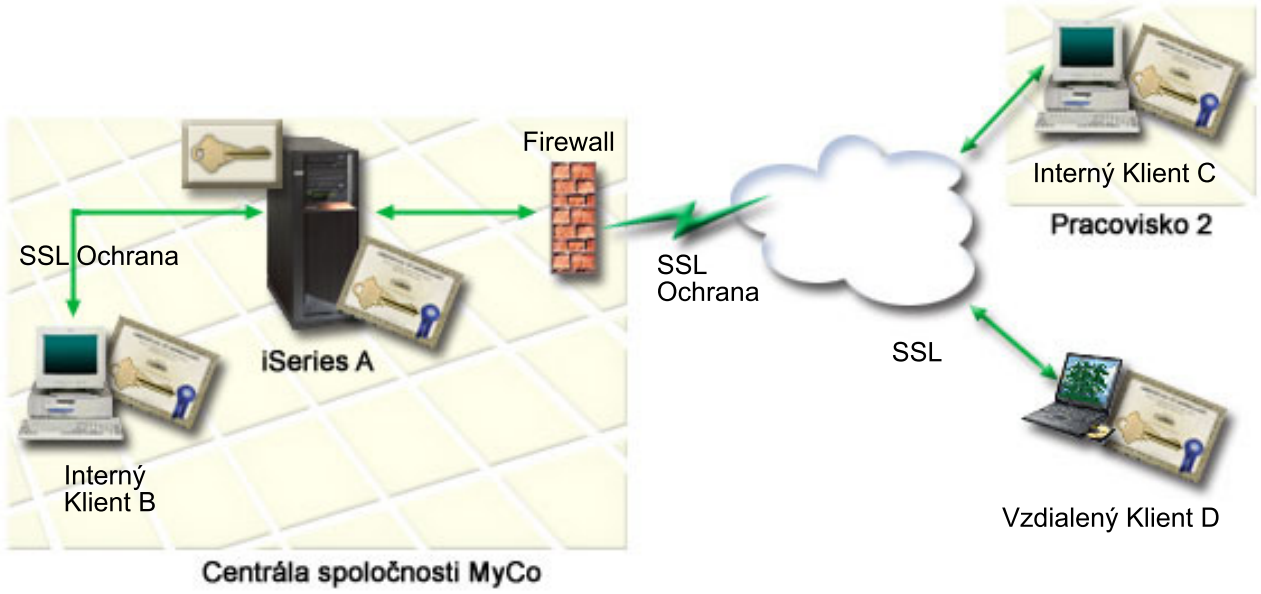
V tomto scenári chce spoločnosť MyCo, Inc. používať digitálne certifikáty na ochranu citlivých osobných informácií, ktoré poskytuje jej interná webová stránka ľudských zdrojov zamestnancom spoločnosti. Táto spoločnosť chce aj bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolený prístup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

Verejný server spoločnosti - iSeries A

- iSeries A je server, ktorý hostuje aplikáciu spoločnosti na výpočet sadzieb.
- iSeries A používa i5/OS verzia 5 vydanie 4 (V5R4).
- iSeries A má nainštalovaný a nakonfigurovaný produkt Správca digitálnych certifikátov (voľba i5/OS 34) a produkt IBM HTTP Server for i5/OS (5722–DG1).
- V iSeries A sa vykonáva aplikácia na výpočet sadzieb, ktorá je nakonfigurovaná takto:
  - 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.

- Keď klienti B a C pristupujú k aplikácii na výpočet sadzieb, iSeries A poskytuje svoj certifikát na zriadenie relácie SSL.
- Po inicializácii relácie SSL požiada systém iSeries A klientov B a C o poskytnutie platného mena užívateľa a hesla, aby im povolil prístup k aplikácii na výpočet sadzieb.

Klientske systémy agentov - klient B a klient C

- Klienti B a C sú nezávislí agenti, ktorí pristupujú na aplikáciu na výpočet sadzieb.
- 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 v systéme iSeries A, ktorý poskytuje svoj certifikát ich klientskemu softvéru, aby autentifikoval svoju identitu a inicializoval reláciu SSL.
- Klientsky softvér v klientoch B a C je nakonfigurovaný tak, aby za účelom inicializovania relácie SSL akceptoval certifikát zo systému iSeries A.
- Po začatí relácie SSL musia klienti B a C poskytnúť platné meno užívateľa a heslo, aby im systém iSeries A povolil prístup k aplikácii.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:

- V systéme iSeries A sa používa produkt IBM HTTP Server for i5/OS (založený na Apache), ktorý zabezpečuje fungovanie aplikácie pre ľudské zdroje. Tento scenár neobsahuje špecifické pokyny pre konfiguráciu servera HTTP na používanie SSL. Tento scenár poskytuje inštrukcie pre konfiguráciu a správu certifikátov, ktoré sú potrebné pre akúkoľvek aplikáciu, aby používala SSL.
- 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. Tento scenár však neobsahuje špecifické kroky konfigurácie pre server HTTP na konfiguráciu autentifikácie klientov pomocou certifikátov.
- Server HTTP pre ľudské zdroje v systéme iSeries A už používa autentifikáciu pomocou hesiel.
- Systém iSeries A spĺňa požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
- V iSeries predtým ešte nikto nenakonfiguroval ani nepoužíval DCM.
- Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
- iSeries A nemá nainštalovaný kryptografický koprocesor IBM.

Úlohy konfigurovania

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
Je váš systém i5/OS vydania V5R4 (5722-SS1)?	Áno
Je vo vašom systéme nainštalovaná voľba 34 systému i5/OS?	Áno
Je vo vašom systéme nainštalovaný produkt IBM HTTP Server for i5/OS (5722–DG1) a je spustená inštancia servera Správa?	Áno

Tabuľka 3. Plánovací pracovný list s požiadavkami na implementáciu certifikátu (pokračovanie)

Pracovný list s požiadavkami	**Odpovede**
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 mohli vykonať potrebné úlohy na dokončenie vašej implementácie certifikátov, musíte o nej získať tieto informácie:

Tabuľka 4. Plánovací pracovný list pre konfiguráciu implementácie certifikátov

Plánovací list pre iSeries 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 systém iSeries A aplikácie, pre ktoré chcete povoliť SSL?	Áno
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)**: pojaspol_CA@mojaspol.com **Organizačná jednotka**: Účtovné oddelenie **Názov organizácie**: mojaspol **Lokalita alebo mesto**: Ľubovoľné_mesto **Štát alebo provincia**: Ľubovoľný **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

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

Plánovací list pre iSeries A	Odpovede
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 **Označenie certifikátu**: ver_cert_mojaspol **Bežný názov**: mojaspol_uctvony_server@mojaspol.com **Organizačná jednotka**: Účtovné oddelenie **Názov organizácie**: mojaspol **Lokalita alebo mesto**: Ľubovoľné_mesto **Štát alebo provincia**: Ľubovoľný **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 ?	Ánomojaspol_CA@mojaspol.com

Konfigurácia servera HTTP pre ľudské zdroje na používanie SSL

Konfigurácia SSL (Secure Sockets Layer) pre server HTTP (založený na Apache) pre ľudské zdroje v systéme iSeries A zahŕňa viacero úloh, ktoré sa líšia podľa aktuálnej konfigurácie vášho servera.

Ak chcete server nakonfigurovať na používanie SSL, postupujte takto:

1. Spustite administračné rozhranie servera HTTP.
2. Ak chcete pracovať so špecifickým serverom HTTP, vyberte záložku **Manažovať —> Všetky servery —> Všetky servery HTTP**, aby sa zobrazil zoznam všetkých nakonfigurovaných serverov HTTP.
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.

Viac o celkovej konfigurácii, ktorá je potrebná pre váš server pri používaní SSL, sa môžete dozvedieť v téme Informačného centra HTTP Server for iSeries, najmä v príklade s názvom Scenár: JKL povolí v serveri HTTP (založenom na Apache) ochranu pomocou SSL (Secure Sockets Layer). 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.

Viac informácií o konfigurovaní aktuálnej aj budúcich verzií produktu 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.

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 serveru.

Keď použijete Správcu digitálnych certifikátov (DCM) na vytvorenie lokálnej CA, ste prevedený procesom, ktorý zabezpečí, že nakonfigurujete všetko, čo potrebujete na aktivovanie SSL pre vašu aplikáciu. 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. Pomocou nového lokálneho CA vydajte certifikát podpisujúci objekty, ktorý môžu používať aplikácie na digitálne 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.

Konfigurácia autentifikácie klientov pre webový server pre ľudské zdroje

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. Pomocou vášho prehliadača prejdite na stránku Úlohy i5/OS vášho systému na adrese http://nazov_vasho_systemu:2001.
3. Vyberte **IBM Web Administration for i5/OS**.
4. Ak chcete pracovať so špecifickým serverom HTTP, vyberte záložku **Manažovať → Všetky servery → Všetky servery HTTP**, aby sa zobrazil zoznam všetkých nakonfigurovaných serverov HTTP.
5. Zo zoznamu vyberte príslušný server a kliknite na **Manage Details**.
6. V navigačnom rámci vyberte **Security**.
7. Vo formulári vyberte záložku **Authentication**.
8. Vyberte voľbu **Použiť profil i5/OS klienta**.
9. V poli **Authentication name or realm** uveďte názov pre oblasť autorizácie.
10. V poli **Spracovať požiadavky pomocou oprávnenia klienta** vyberte hodnotu Povolené a kliknite na **Použiť**.
11. Vo formulári vyberte záložku **Control Access**.
12. Vyberte **All authenticated users (valid user name and password)** a kliknite na **Apply**.
13. Vo formulári vyberte záložku **SSL with Certificate Authentication**.
14. Skontrolujte, že je v poli **SSL** vybratá hodnota Povolené.
15. Zabezpečte, aby v poli **Server certificate application name** bola špecifikovaná správna hodnota, napríklad QIBM_HTTP_SERVER_MYCOTEST.
16. Vyberte **Accept client certificate if available before making connection**. Kliknite na **OK**.

Viac o celkovej konfigurácii, ktorá je potrebná pre váš server pri používaní SSL, sa môžete dozvedieť v téme Informačného centra HTTP Server for iSeries, najmä v príklade s názvom Scenár: JKL povolí v serveri HTTP (založenom na Apache) ochranu pomocou SSL (Secure Sockets Layer). 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.

Spustenie webového servera pre ľudské zdroje 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 Navigátor iSeries rozviňte váš systém.
2. Rozviňte **Sieť → Servery → TCP/IP → Správa HTTP**.
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.

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

Súvisiace informácie

Prehľad Informačného centra pre HTTP

Skopírovanie kópie certifikátu lokálneho CA do prehliadačov užívateľov

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 navigačnej časti vyberte voľbu **Nainštalovať certifikát lokálneho CA do vášho PC**, aby sa zobrazila stránka, ktorá vám umožní prevziať certifikát lokálneho CA do vášho prehliadača alebo ho uložiť do súboru vo 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 pristúpiť 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.

Požiadavky užívateľov o certifikát od lokálnej certifikačnej autority

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 k vášmu užívateľskému profilu iSeries.

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

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.

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 nastavenia DCM

Túto tému si pozrite, ak chcete skontrolovať, že máte nainštalované vyžadované voľby na používanie Správcu digitálnych certifikátov (DCM).

DCM je bezplatná vlastnosť iSeries, ktorá vám umožňuje centrálne manažovať digitálne certifikáty pre vaše aplikácie. Na úspešné používanie DCM zabezpečte, že urobíte nasledovné:

- Nainštalujte voľbu 34 systému i5/OS. Toto je DCM, založený na prehliadači.
- Nainštalujte produkt IBM HTTP Server for i5/OS (5722–DG1) a spustite inštanciu servera Správa.
- 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

Dozviete sa tu, ako zabezpečiť, že sa dôležité údaje DCM pridajú do plánu pre zálohovanie a obnovu vášho systému.

Zašifrované heslá databázy kľúčov, ktoré používate na prístup k skladom certifikátov v Správcovi digitálnych certifikátov (DCM), sú vo vašom systéme uložené, alebo *ukryté*, 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 môže byť situácia, keď pomocou DCM vytvoríte certifikát pre iný systém **iSeries** a súbory s certifikátmi chcete použiť na vytvorenie nového skladu certifikátov v cieľovom systéme. V tomto prípade musíte otvoriť novo vytvorený sklad certifikátov a pomocou úlohy **Zmeniť heslo** musíte zmeniť heslo pre sklad certifikátov v cieľovom systéme, čo zabezpečí, 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 vytváraní certifikátov pre iné systémy iSeries pomocou DCM, pozrite si časť Vydávanie certifikátov pre iné systémy iSeries pomocou lokálneho CA.

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.

Súvisiace úlohy

“Vydávanie certifikátov pre iné systémy iSeries pomocou lokálneho CA” na strane 53
Dozviete sa tu, ako pomocou súkromného lokálneho CA v jednom systéme vydávať certifikáty, ktoré sa budú používať v iných systémoch iSeries.

Typy digitálnych certifikátov

Tieto informácie vás oboznámia s rôznymi typmi digitálnych certifikátov a ich použitím v Správcovi digitálnych certifikátov (DCM).

Pomocou DCM môžete manažovať tieto typy certifikátov:

Certifikáty certifikačných autorít (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 používať verejný kľúč certifikátu CA na overovanie autenticity certifikátov, ktoré CA vydáva a podpisuje. 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 používať verejný kľúč certifikátu CA na overovanie autenticity certifikátov, ktoré CA vydáva a podpisuje. Ak chcete používať certifikát pre SSL, podpisovanie objektov alebo overovanie podpisov objektov, musíte mať tiež kópiu certifikátu vydávajúceho CA.

Certifikáty serverov alebo klientov
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. Na bezpečnú komunikáciu pomocou SSL (Secure Sockets Layer) musí mať server

digitálny certifikát. 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 podpisujúce objekty
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 kontrolu podpisu
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. Užívateľské certifikáty, ktoré vydá vaše súkromné CA, Správca digitálnych certifikátov (DCM) automaticky priradí k užívateľskému profilu iSeries. Pomocou DCM môžete k užívateľskému profilu iSeries priradiť tiež užívateľské certifikáty, ktoré vydajú iné certifikačné autority.

Keď pomocou Správcu digitálnych certifikátov (DCM) manažujete vaše certifikáty, DCM ich organizuje a spolu s ich priradenými súkromnými kľúčmi ich na základe týchto klasifikácií ukladá ich do skladu certifikátov.

Poznámka: Ak máte vo vašom systéme nainštalovaný kryptografický koprocesor IBM, môžete pre certifikáty vybrať iné možnosti uloženia súkromných kľúčov (s výnimkou certifikátov podpisujúcich objekty). 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.

Súvisiace koncepty

“SSL (Secure Sockets Layer)” na strane 9
Secure Sockets Layer (SSL), pôvodne vytvorený spoločnosťou Netscape, je priemyselný štandard pre šifrovanie relácií medzi klientmi a servermi.

“Sklady certifikátov” na strane 7
Sklad certifikátov je špeciálny súbor databázy kľúčov, ktorý Správca digitálnych certifikátov (DCM) používa na uloženie digitálnych certifikátov.

Verejné certifikáty verzus súkromné certifikáty

Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

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.Keď vyberiete typ CA na vydávanie certifikátov, musíte zvoliť 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. Keď užívatelia získajú pomocou DCM svoj certifikát od lokálneho CA, ich certifikát sa štandardne uloží spolu 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). Ak nechcete, aby mali užívatelia certifikát priradený alebo uložený s užívateľským profilom, môžete pomocou rozhraní API programovo vydávať certifikáty užívateľom iným ako užívateľom 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 pozrieť si niektoré bežné scenáre použitia certifikátov, ktoré vám pomôžu určiť, či vašim obchodným a bezpečnostným požiadavkám lepšie vyhovujú verejné alebo súkromné certifikáty.

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:

- Téma Vytvorenie a sprevádzkovanie súkromného CA opisuje úlohy, ktoré musíte vykonať, ak sa rozhodnete používať na vydávanie súkromných certifikátov lokálne CA.
- Téma Manažovanie certifikátov od verejného internetového CA opisuje úlohy, ktoré musíte vykonať, ak chcete používať všeobecne známe verejné CA, vrátane CA PKIX.
- Téma Použitie lokálneho CA v iných serveroch iSeries opisuje úlohy, ktoré musíte vykonať, ak chcete používať certifikáty od súkromného lokálneho CA vo viac než jednom systéme.

Súvisiace koncepty

“Manažovanie certifikáty z verejnej internetovej CA” na strane 45
Dozviete sa tu, ako pomocou vytvorenia skladu certifikátov manažovať certifikáty od verejného internetového CA.

“Verejné certifikáty verzus súkromné certifikáty” na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

“Nastavenie certifikátov po prvý krát” na strane 37
Tieto informácie vám ukážu, ako začať s manažovaním certifikátov od verejnej internetovej certifikačnej autority (CA) alebo ako vytvoriť a sprevádzkovať súkromnú lokálnu certifikačnú autoritu na vydávanie certifikátov.

“Digitálne certifikáty na podpisovanie objektov” na strane 34
Tieto informácie vám vysvetlia, ako používať certifikáty na zaistenie integrity objektu, alebo ako skontrolovať digitálny podpis na objekte za účelom kontroly jeho autenticity.

Súvisiace úlohy

“Digitálne certifikáty a architektúra Enterprise Identity Mapping (EIM)” na strane 32
Spoločné používanie EIM (Enterprise Identity Mapping) a Správcu digitálnych certifikátov (DCM) vám umožňuje použiť certifikát ako zdroj pre operáciu vyhľadávania mapovaní EIM na namapovanie certifikátu na cieľovú identitu užívateľa, priradenú k rovnakému identifikátoru EIM.

“Vytvorenie užívateľského certifikátu” na strane 41
Dozviete sa tu, ako môžu vaši užívatelia pomocou lokálneho CA vydávať certifikáty na autentifikáciu klientov.

“Vytvorenie a prevádzkovanie lokálnej CA” na strane 38
Tieto informácie opisujú spôsob vytvorenia a sprevádzkovania lokálnej certifikačnej autority (CA) na vydávanie súkromných certifikátov pre vaše aplikácie.

“Vydávanie certifikátov pre iné systémy iSeries pomocou lokálneho CA” na strane 53
Dozviete sa tu, ako pomocou súkromného lokálneho CA v jednom systéme vydávať certifikáty, ktoré sa budú používať v iných systémoch iSeries.

Súvisiaci odkaz

“Použitie API na programové vydávanie certifikátov pre užívateľov iných ako i-Series” na strane 44
Dozviete sa tu, ako môžete pomocou vášho lokálneho CA vydávať súkromné certifikáty pre užívateľov bez toho, aby ste certifikát priradili k užívateľskému profilu iSeries.

Digitálne certifikáty pre bezpečnú SSL komunikáciu

Pomocou týchto informácií sa dozviete ako používať certifikáty, aby vaše aplikácie mohli vytvárať bezpečné komunikačné relácie.

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. Ak chcete používať certifikáty ako dôkaz identity, komunikujúca aplikácia musí podporovať autentifikáciu užívateľov pomocou certifikátov.

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.

Súvisiace koncepty

"Digitálne certifikáty na autentifikáciu užívateľov"
Dozviete sa tu o používaní certifikátov ako prostriedkov na bezpečnejšiu autentifikáciu užívateľov, ktorí pristupujú k systémovým prostriedkom iSeries.

Digitálne certifikáty na autentifikáciu užívateľov

Dozviete sa tu o používaní certifikátov ako prostriedkov na bezpečnejšiu autentifikáciu užívateľov, ktorí pristupujú k systémovým prostriedkom iSeries.

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. Pomocou Správcu digitálnych certifikátov (DCM) môžete tiež priradiť užívateľský certifikát k užívateľskému profilu iSeries daného užívateľa alebo k identite iného užívateľa. Tento certifikát má teda rovnaké oprávnenia a povolenia ako priradená užívateľská identita alebo užívateľský profil. Prípadne môžete použiť rozhrania API na programové vydávanie certifikátov pomocou lokálnej certifikačnej autority pre užívateľov iných ako užívatelia iSeries. Tieto rozhrania API vám poskytujú možnosť vydávať súkromné certifikáty užívateľom, keď nechcete, aby títo užívatelia mali užívateľský profil iSeries alebo internú identitu užívateľa.

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. Podporu autentifikácie klientov pomocou certifikátov aktuálne poskytujú tieto aplikácie iSeries:

- Telnet server
- IBM HTTP Server for i5/OS (založený na Apache)

- IBM Directory Server
- iSeries Access for Windows (vrátane Navigátora Navigátor iSeries)
- 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 konfigurovaní aplikácií iSeries na používanie certifikátov pre autentifikáciu klientov počas relácie SSL, pozrite si tému SSL (Secure Sockets Layer) v Informačnom centre Navigátor iSeries.

Súvisiace koncepty

“Digitálne certifikáty pre bezpečnú SSL komunikáciu” na strane 30
Pomocou týchto informácií sa dozviete ako používať certifikáty, aby vaše aplikácie mohli vytvárať bezpečné komunikačné relácie.

Súvisiaci odkaz

“Použitie API na programové vydávanie certifikátov pre užívateľov iných ako i-Series” na strane 44
Dozviete sa tu, ako môžete pomocou vášho lokálneho CA vydávať súkromné certifikáty pre užívateľov bez toho, aby ste certifikát priradili k užívateľskému profilu iSeries.

Digitálne certifikáty a architektúra Enterprise Identity Mapping (EIM)

Spoločné používanie EIM (Enterprise Identity Mapping) a Správcu digitálnych certifikátov (DCM) vám umožňuje použiť certifikát ako zdroj pre operáciu vyhľadávania mapovaní EIM na namapovanie certifikátu na cieľovú identitu užívateľa, priradenú k rovnakému identifikátoru EIM.

EIM je technológia @server , ktorá vám umožňuje manažovať identity užívateľov vo vašej spoločnosti, vrátane užívateľských profilov a certifikátov užívateľov. 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. Pomocou sprievodcu **Konfigurácia EIM** v **Navigátore iSeries** nakonfigurujte EIM.
2. Vytvorte identifikátor EIM pre každého užívateľa, ktorého chcete mať zapojeného do EIM.
3. Vytvorte cieľové priradenie medzi každým identifikátorom EIM a profilom daného užívateľa v lokálnom registri užívateľov i5/OS, aby bolo možné každý certifikát, ktorý užívateľ priradí alebo vytvorí pomocou DCM, namapovať na profil užívateľa. Pre lokálny register užívateľov **i5/OS** použite názov definície registra EIM, ktorý ste zadali v sprievodcovi **Konfigurácia 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.

Okrem toho, keď nakonfigurujete EIM a DCM na vzájomnú spoluprácu, môžete pomocou DCM kontrolovať exspiráciu užívateľských certifikátov na úrovni podniku, nie len na úrovni systému.

Súvisiace koncepty

“Verejné certifikáty verzus súkromné certifikáty” na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

Súvisiace úlohy

“Manažovanie užívateľských certifikátov podľa ukončenia platnosti” na strane 43
Správca digitálnych certifikátov (DCM) poskytuje podporu pre manažovanie exspirácie, aby umožnil administrátorom kontrolovať v lokálnom systéme iSeries dátumy exspirácie užívateľských certifikátov. Podporu manažovania exspirácie užívateľských certifikátov v DCM je možné použiť spolu s EIM, takže administrátori môžu pomocou DCM kontrolovať exspiráciu užívateľských certifikátov na úrovni podniku.

“Riadenie umiestenia LDAP pre užívateľské certifikáty” na strane 68
Dozviete sa tu, ako nakonfigurovať DCM na ukladanie užívateľských certifikátov do adresárovej lokality servera LDAP (Lightweight Directory Access Protocol), aby mohlo EIM (Enterprise Identity Mapping) pracovať s užívateľskými certifikátmi.

Súvisiace informácie

Téma Informačného centra pre EIM

Digitálne certifikáty pre pripojenia VPN

Dozviete sa tu o používaní certifikátov ako súčasti konfigurácie pripojenia virtuálnej súkromnej siete (VPN).

Digitálne certifikáty môžete použiť ako prostriedok na vytvorenie pripojenia VPN v iSeries. 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. Najprv sa musíte rozhodnúť, či budete pre váš server IKE 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).

Súvisiace informácie

Konfigurácia pripojenia VPN

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.

IBM i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod. Podpisovanie objektov rozširuje tradičné nástroje systému iSeries na riadenie, kto môže meniť objekty. Pri tradičnom riadení sa objekt nedal ochrániť pred neautorizovaným zásahom počas prenosu objektu cez internet alebo inú nedôveryhodnú sieť, alebo keď je objekt uložený na inom ako iSeries systéme. Taktiež, tradičné riadenia nemôžu vždy zistiť, či na objekte nastali neautorizované zmeny alebo zásahy. Použitie elektronických podpisov na objektoch poskytuje spoľahlivý prostriedok na zistenie zmien na podpísaných objektoch.

Umiestnenie digitálneho 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 digitálnych podpisov vyhovuje vašim bezpečnostným požiadavkám a politikám, musíte určiť, či potrebujete používať verejné certifikáty alebo vydávať súkromné certifikáty. 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. Pomocou DCM môžete tiež podpisovať objekty a overovať podpisy objektov.

Súvisiace koncepty

"Verejné certifikáty verzus súkromné certifikáty" na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

"Digitálne certifikáty pre overovanie podpisov objektov"
Tieto informácie opisujú spôsob používania certifikátov na overovanie digitálneho podpisu objektu za účelom overenia jeho autenticity.

Súvisiace úlohy

"Overenie podpisov objektov" na strane 70
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.

"Manažovanie verejných internetových certifikátov pre podpisovanie objektov" na strane 47
Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov na digitálne podpisovanie objektov.

"Manažovanie certifikátov na overovanie podpisov objektov" na strane 49
Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie certifikátov na kontrolu podpisov, ktoré používate na validovanie digitálnych podpisov na objektoch.

Digitálne certifikáty pre overovanie podpisov objektov

Tieto informácie opisujú spôsob používania certifikátov na overovanie digitálneho podpisu objektu za účelom overenia jeho autenticity.

IBM i5/OS poskytuje podporu používania certifikátov na overovanie digitálnych podpisov objektov. Ľubovoľný užívateľ, ktorý chce skontrolovať, že podpísaný objekt nebol pri prenose zmenený a že objekt pochádza z akceptovaného zdroja, môže pomocou verejného kľúča podpisujúceho certifikátu overiť 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.

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. Ak sa chcete dozvedieť viac o používaní tejto a iných systémových hodnôt, pozrite si Vyhľadávač systémových hodnôt v Informačnom centre Informačné centrum 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. Pomocou DCM môžete tiež podpisovať objekty a overovať podpisy objektov.

Súvisiace koncepty

“Digitálne certifikáty na podpisovanie objektov” na strane 34
Tieto informácie vám vysvetlia, ako používať certifikáty na zaistenie integrity objektu, alebo ako skontrolovať digitálny podpis na objekte za účelom kontroly jeho autenticity.

Súvisiace informácie

Vyhľadávač systémových hodnôt

Konfigurácia 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.

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.

Dostupné úlohy v navigačnej časti sa líšia podľa skladu certifikátov, s ktorým pracujete. Taktiež kategória a počet úloh zobrazených v navigačnej časti sa líšia v podľa autorizácií, ktoré má váš užívateľský profil i5/OS. Všetky úlohy pre prácu s CA, manažovanie certifikátov, ktoré používajú aplikácie a iné úlohy na úrovni systému sú dostupné len správcom bezpečnosti alebo administrátorom iSeries. 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:

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

Dozviete sa tu, ako pristupovať k vlastnosti Správca digitálnych certifikátov (DCM) vo vašom systéme.

Pred používaním funkcií Správcu digitálnych certifikátov ho musíte spustiť. Aby ste zaistili úspešné spustenie DCM, vykonajte tieto kroky:

1. Nainštalujte voľbu 34 z 5722 SS1. To je Správca digitálnych certifikátov (DCM).
2. Nainštalujte 5722 DG1. To je IBM HTTP Server for i5/OS.
3. Pomocou Navigátora Navigátor iSeries spustite inštanciu Správa servera HTTP:
   a. Spustite **Navigátor iSeries** .
   b. V hlavnom stromovom zobrazení spravte dvojité kliknutie na váš systém.
   c. Rozviňte **Sieť > Servery > TCP/IP**.
   d. Pravým tlačidlom kliknite na **HTTP Administration**.
   e. Kliknite na **Start**.
4. Spustite váš webový prehliadač.
5. Pomocou prehliadača prejdite na stránku Úlohy iSeries vášho systému na adrese http://*nazov_vasho_systemu*:2001.
6. Zo zoznamu produktov na stránke Úlohy iSeries vyberte voľbu **Správca digitálnych certifikátov**, aby sa zobrazilo užívateľské rozhranie DCM.

Súvisiace koncepty

“Scenár: Používanie certifikátov na externú autentifikáciu” na strane 12
V tomto scenári sa naučíte, kedy a ako používať certifikáty ako autentifikačný mechanizmus na ochranu a obmedzenie prístupu verejných užívateľov k verejným alebo extranetovým prostriedkom a aplikáciám.

Nastavenie certifikátov po prvý krát

Tieto informácie vám ukážu, ako začať s manažovaním certifikátov od verejnej internetovej certifikačnej autority (CA) alebo ako vytvoriť a sprevádzkovať súkromnú lokálnu certifikačnú autoritu na vydávanie 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) po prvý raz, sklady certifikátov neexistujú. Takže keď po prvý raz 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 k Úlohám iSeries.

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). Ak chcete úspešne použiť túto funkciu, musíte najprv nakonfigurovať produkt IBM HTTP Server for i5/OS, aby používal SSL na prevádzku v bezpečnom režime. Potom musíte spustiť HTTP Server v bezpečnom režime. Ak ste nenakonfigurovali a nespustili HTTP Server pre prevádzkovanie SSL, uvidíte chybové hlásenie a váš prehliadač nespustí zabezpečenú reláciu.

Začíname

Hoci možno chcete používať certifikáty na dosiahnutie mnohých bezpečnostných cieľov, čo urobíte ako prvé závisí od toho, ako plánujete získavať svoje certifikáty. Pri prvom použití DCM sa môžete vydať dvoma základnými smermi podľa toho, či chcete používať verejné certifikáty alebo vydávať súkromné certifikáty.

Súvisiace koncepty

“Verejné certifikáty verzus súkromné certifikáty” na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

Vytvorenie a prevádzkovanie lokálnej CA

Tieto informácie opisujú spôsob vytvorenia a sprevádzkovania lokálnej certifikačnej autority (CA) na vydávanie súkromných certifikátov pre vaše aplikácie.

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 vo vašom systéme používať certifikáty s produktom IBM HTTP Server for i5/OS, váš webový server musíte vytvoriť a nakonfigurovať skôr, než budete pracovať s DCM. 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 voľbu Vytvoriť certifikačnú autoritu (CA), aby sa zobrazila skupina 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 týkajúce sa vypĺňania špecifického formulára v tejto riadenej úlohe, vyberte otáznik (?) 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 sa vykonáva len v prípade, že máte vo vašom systéme nainštalovaný kryptografický 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 má váš systém nainštalovaný kryptografický koprocesor IBM, tento krok vám umožní vybrať spôsob uloženia súkromného kľúča 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. Pomocou nového lokálneho CA vydajte certifikát podpisujúci objekty, ktorý môžu používať aplikácie na digitálne 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 riadenú úlohu, budete mať všetko potrebné na začatie konfigurovania vašich aplikácií na používanie 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.

Pomocou tohto lokálneho CA môžete tiež vydávať certifikáty pre aplikácie v 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:

Súvisiace koncepty

“Verejné certifikáty verzus súkromné certifikáty” na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

“Manažovanie užívateľských certifikátov” na strane 40
Pomocou Správcu digitálnych certifikátov (DCM) môžete získať certifikáty s SSL alebo priradiť existujúce certifikáty k ich užívateľským profilom iSeries.

Súvisiace úlohy

"Vydávanie certifikátov pre iné systémy iSeries pomocou lokálneho CA" na strane 53
Dozviete sa tu, ako pomocou súkromného lokálneho CA v jednom systéme vydávať certifikáty, ktoré sa budú používať v iných systémoch iSeries.

"Získanie kópie certifikátu súkromnej CA" na strane 44
Dozviete sa tu, ako získať kópiu certifikátu súkromného CA a nainštalovať ju do PC, aby ste mohli autentifikovať všetky certifikáty serverov, ktoré vydalo toto CA.

Súvisiaci odkaz

"Použitie API na programové vydávanie certifikátov pre užívateľov iných ako i-Series" na strane 44
Dozviete sa tu, ako môžete pomocou vášho lokálneho CA vydávať súkromné certifikáty pre užívateľov bez toho, aby ste certifikát priradili k užívateľskému profilu iSeries.

Manažovanie užívateľských certifikátov:

Pomocou Správcu digitálnych certifikátov (DCM) môžete získať certifikáty s SSL alebo priradiť existujúce certifikáty k ich užívateľským profilom iSeries.

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. Ak však váš server používa certifikát od súkromného lokálneho CA, vaši užívatelia musia pred vytvorením relácie SSL s vašim serverom získať kópiu certifikátu lokálneho CA.

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 aplikácia servera poskytuje prístup k prostriedkom pre interných užívateľov, ktorí aktuálne majú užívateľské profily iSeries, môžete k ich užívateľským profilom pomocou DCM pridať ich certifikáty. Toto priradenie zaisťuje, že predložení certifikátov majú užívatelia na prostriedky rovnaký prístup alebo obmedzenia, ako im poskytuje alebo zakazuje ich užívateľský profil.

Správca digitálnych certifikátov (DCM) vám umožňuje manažovať certifikáty, ktoré sú priradené k užívateľskému profilu iSeries. Ak máte užívateľský profil so špeciálnymi oprávneniami *SECADM a *ALLOBJ, môžete manažovať priradenia certifikátov užívateľských profilov sami pre seba alebo pre ostatných užívateľov. Keď nie je otvorený žiadny sklad certifikátov alebo keď je otvorený sklad certifikátov lokálnej certifikačnej autority (CA), môžete v navigačnej časti vybrať voľbu **Manažovať užívateľské certifikáty** a pristupovať k požadovaným úlohám. 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:

Súvisiace úlohy

"Vytvorenie a prevádzkovanie lokálnej CA" na strane 38
Tieto informácie opisujú spôsob vytvorenia a sprevádzkovania lokálnej certifikačnej autority (CA) na vydávanie súkromných certifikátov pre vaše aplikácie.

"Získanie kópie certifikátu súkromnej CA" na strane 44
Dozviete sa tu, ako získať kópiu certifikátu súkromného CA a nainštalovať ju do PC, aby ste mohli autentifikovať všetky certifikáty serverov, ktoré vydalo toto CA.

Vytvorenie užívateľského certifikátu:

Dozviete sa tu, ako môžu vaši užívatelia pomocou lokálneho CA vydávať certifikáty na autentifikáciu klientov.

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 priradí certifikát k vášmu užívateľskému profilu iSeries.

Ak chcete, aby mal certifikát od iného CA, ktorý poskytuje užívateľ na autentifikáciu klienta, rovnaké oprávnenia ako jeho užívateľský profil, užívateľ môže pomocou DCM priradiť certifikát k svojmu užívateľskému profilu.

Súvisiace koncepty

"Verejné certifikáty verzus súkromné certifikáty" na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

Súvisiace úlohy

"Priradenie užívateľského certifikátu"
Užívateľský certifikát, ktorý vlastníte, môžete priradiť k vášmu vlastnému užívateľskému profilu i5/OS alebo k identite iného užívateľa. 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.

"Získanie kópie certifikátu súkromnej CA" na strane 44
Dozviete sa tu, ako získať kópiu certifikátu súkromného CA a nainštalovať ju do PC, aby ste mohli autentifikovať všetky certifikáty serverov, ktoré vydalo toto CA.

Priradenie užívateľského certifikátu:

Užívateľský certifikát, ktorý vlastníte, môžete priradiť k vášmu vlastnému užívateľskému profilu i5/OS alebo k identite iného užívateľa. 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.

Niektorí užívatelia môžu mať certifikáty od externej certifikačnej autority (CA) alebo lokálnej certifikačnej autority v inom systéme iSeries, ktoré chcete (ako administrátor) sprístupniť v Správcovi digitálnych certifikátov (DCM). Umožňuje to vám a užívateľovi používať DCM na manažovanie týchto certifikátov, ktoré sa najčastejšie používajú na autentifikáciu klienta. Úloha **Priradenie užívateľského certifikátu** 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:

- Lokálne uloženie certifikátu v systéme iSeries spolu s užívateľským profilom. Keď pre DCM nie je definované umiestnenie LDAP, úloha **Priradenie užívateľského certifikátu** umožňuje užívateľovi priradiť externý certifikát k užívateľskému profilu i5/OS. 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). Keď je definované umiestnenie LDAP a systém iSeries je nakonfigurovaný, aby sa zúčastňoval v EIM, úloha **Priradenie užívateľského certifikátu** umožňuje užívateľovi uložiť kópiu externého certifikátu do zadaného 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.

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. Príčinou môže byť jeden z niekoľkých problémov s užívateľským certifikátom. Napríklad certifikáty, ktoré obsahuje váš prehliadač, sú už pravdepodobne priradené k vašej užívateľskej identite.

Súvisiace úlohy

“Vytvorenie užívateľského certifikátu” na strane 41
Dozviete sa tu, ako môžu vaši užívatelia pomocou lokálneho CA vydávať certifikáty na autentifikáciu klientov.

“Odstránenie problémov s priradením užívateľského certifikátu” na strane 77

Súvisiace informácie

Prehľad Informačného centra pre EIM

Manažovanie užívateľských certifikátov podľa ukončenia platnosti:

Správca digitálnych certifikátov (DCM) poskytuje podporu pre manažovanie exspirácie, aby umožnil administrátorom kontrolovať v lokálnom systéme iSeries dátumy exspirácie užívateľských certifikátov. Podporu manažovania exspirácie užívateľských certifikátov v DCM je možné použiť spolu s EIM, takže administrátori môžu pomocou DCM kontrolovať exspiráciu užívateľských certifikátov na úrovni podniku.

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 aktuálne pracujete so skladom certifikátov, vyberte voľbu **Manažovať certifikáty**, aby sa zobrazil zoznam úloh, potom vyberte **Skontrolovať exspiráciu** a vyberte **Užívateľ**.
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:
   - **Užívateľský profil**, ak chcete zobraziť a manažovať užívateľské certifikáty, ktoré sú priradené k špecifickému užívateľskému profilu i5/OS. Uveďte **User profile name** a kliknite na **Continue**.

     Poznámka: Užívateľský profil iný ako váš môžete zadať 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.

Súvisiace úlohy

"Digitálne certifikáty a architektúra Enterprise Identity Mapping (EIM)" na strane 32
Spoločné používanie EIM (Enterprise Identity Mapping) a Správcu digitálnych certifikátov (DCM) vám umožňuje použiť certifikát ako zdroj pre operáciu vyhľadávania mapovaní EIM na namapovanie certifikátu na cieľovú identitu užívateľa, priradenú k rovnakému identifikátoru EIM.

Súvisiace informácie

Prehľad Informačného centra pre EIM

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

Dozviete sa tu, ako môžete pomocou vášho lokálneho CA vydávať súkromné certifikáty pre užívateľov bez toho, aby ste certifikát priradili k užívateľskému profilu iSeries.

V systéme i5/OS V5R3 alebo novšom sú dostupné dve rozhrania API, ktoré môžete použiť na programové vydávanie certifikátov užívateľom iným ako užívateľom iSeries. Keď ste v predošlých vydaniach pomocou vašej lokálnej certifikačnej autority (CA) vydávali certifikáty pre užívateľov, tieto certifikáty sa automaticky priradili k ich užívateľským profilom iSeries. Aby ste mohli pomocou lokálneho CA vydať užívateľovi certifikát na autentifikáciu klienta, museli ste pre daného užívateľa vytvoriť 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). Každý užívateľ musí mať preto v serveri iSeries, ktorý hostuje DCM, užívateľský profil a platné prihlásenie k tomuto serveru iSeries.

Združovanie certifikátu s užívateľským profilom má svoje výhody, obzvlášť keď sa to týka interných užívateľov. Tieto obmedzenia a požiadavky však spôsobili, že používanie lokálneho CA na vydávanie certifikátov pre veľký počet užívateľov bolo nepraktické, obzvlášť v prípade, že ste nechceli, 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 v serveri iSeries, ktorý hostuje DCM a užívateľ nemusí na vytvorenie certifikátu použiť DCM.

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).

Súvisiace koncepty

"Verejné certifikáty verzus súkromné certifikáty" na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

"Digitálne certifikáty na autentifikáciu užívateľov" na strane 31
Dozviete sa tu o používaní certifikátov ako prostriedkov na bezpečnejšiu autentifikáciu užívateľov, ktorí pristupujú k systémovým prostriedkom iSeries.

Súvisiace úlohy

"Vytvorenie a prevádzkovanie lokálnej CA" na strane 38
Tieto informácie opisujú spôsob vytvorenia a sprevádzkovania lokálnej certifikačnej autority (CA) na vydávanie súkromných certifikátov pre vaše aplikácie.

Získanie kópie certifikátu súkromnej CA:

Dozviete sa tu, ako získať kópiu certifikátu súkromného CA a nainštalovať ju do PC, aby ste mohli autentifikovať všetky certifikáty serverov, ktoré vydalo toto 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 aplikácia servera vyžaduje, aby ste sa autentifikovali pomocou certifikátu od lokálneho CA, musíte pred požiadaním o užívateľský certifikát od lokálneho CA prevziať certifikát CA do vášho prehliadača.

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

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

Súvisiace koncepty

"Manažovanie užívateľských certifikátov" na strane 40
Pomocou Správcu digitálnych certifikátov (DCM) môžete získať certifikáty s SSL alebo priradiť existujúce certifikáty k ich užívateľským profilom iSeries.

Súvisiace úlohy

"Vytvorenie a prevádzkovanie lokálnej CA" na strane 38
Tieto informácie opisujú spôsob vytvorenia a sprevádzkovania lokálnej certifikačnej autority (CA) na vydávanie súkromných certifikátov pre vaše aplikácie.

"Vytvorenie užívateľského certifikátu" na strane 41
Dozviete sa tu, ako môžu vaši užívatelia pomocou lokálneho CA vydávať certifikáty na autentifikáciu klientov.

Manažovanie certifikáty z verejnej internetovej CA

Dozviete sa tu, ako pomocou vytvorenia skladu certifikátov manažovať certifikáty od verejného internetového 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.

Poznámka: DCM vám umožňuje tiež manažovať certifikáty, ktoré získate od certifikačnej autority z infraštruktúry verejných kľúčov pre X.509 (PKIX).

Ak sa chcete dozvedieť viac o použití DCM na vytvorenie príslušného skladu certifikátov a manažovaní vašich certifikátov pre vaše aplikácie, pozrite si tieto témy:

Súvisiace koncepty

"Verejné certifikáty verzus súkromné certifikáty" na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

Súvisiace úlohy

"Manažovanie miestnenia požiadavky pre PKIX CA" na strane 67
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.

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 autora podpisu pre nový certifikát vyberte **VeriSign alebo inú internetovú certifikačnú autoritu (CA)** a kliknutím na **Pokračovať** zobrazte formulár pre zadanie identifikačných informácií pre nový certifikát.

   Poznámka: Ak je vo vašom systéme nainštalovaný kryptografický koprocesor IBM, DCM vám ako ďalšiu úlohu umožní vybrať spôsob uloženia súkromného kľúča pre certifikát. 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. Keď zatvoríte túto stránku, údaje sa stratia a nebude ich možné 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.

   Ak chcete vo vašom systéme používať certifikáty so serverom HTTP, váš webový server musíte vytvoriť a nakonfigurovať skôr, než budete pomocou DCM pracovať s hotovým podpísaným 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 riadenú úlohu, budete mať všetko potrebné na začatie konfigurovania vašich aplikácií na používanie 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. (Pomocou Navigátora Navigátor iSeries však môžete zmeniť oprávnenie, ktoré vyžaduje ID aplikácie.)

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 zatvoríte túto stránku, údaje sa stratia a nebude ich možné 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 vyberte **Manažovať certifikáty**, 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. Vyplňte formulár na definovanie vašej aplikácie na podpisovanie objektov a kliknite na **Pridať**. Táto definícia aplikácie nepopisuje skutočnú aplikáciu, ale popisuje typ objektov, ktoré chcete podpisovať konkrétnym certifikátom. Pri vypĺňaní formuláru môžete použiť online pomoc.

16. Kliknite na **OK**, aby sa potvrdila správa o vytvorení definície a zobrazil 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 na podpisovanie objektov na zabezpečenie ich integrity.

Keď distribuujete podpísané objekty, ich príjemcovia musia pomocou DCM pre systém OS/400 V5R1 alebo novší skontrolovať podpis objektu, aby overili, že údaje nie sú zmenené a aby skontrolovali identitu odosielateľa. Aby mohol príjemca skontrolovať podpis, musí mať kópiu certifikátu na kontrolu podpisu. Kópiu tohto certifikátu musíte poskytnúť ako súčasť balíka podpísaných objektov.

Príjemca musí mať tiež kópiu certifikátu certifikačnej autority, ktorá vydala certifikát použitý 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.

Súvisiace koncepty

"Digitálne certifikáty na podpisovanie objektov" na strane 34
Tieto informácie vám vysvetlia, ako používať certifikáty na zaistenie integrity objektu, alebo ako skontrolovať digitálny podpis na objekte za účelom kontroly jeho autenticity.

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.

Pri podpisovaní objektov vytvoríte podpis pomocou súkromného kľúča 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. 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 kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, 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 certifikačnej autority, ktorá vydala certifikát na kontrolu podpisu, musíte *najprv* importovať certifikát CA. Ak pred importovaním certifikátu na overovanie podpisov nenaimportujete certifikát CA, môžete pri importovaní certifikátu na overovanie podpisov dostať chybovú správu.

Teraz môžete pomocou certifikátov overovať podpisy objektov.

Súvisiace koncepty

"Digitálne certifikáty na podpisovanie objektov" na strane 34
Tieto informácie vám vysvetlia, ako používať certifikáty na zaistenie integrity objektu, alebo ako skontrolovať digitálny podpis na objekte za účelom kontroly jeho autenticity.

Súvisiace úlohy

"Overenie podpisov objektov" na strane 70
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.

Obnova existujúceho certifikátu

Proces obnovenia platnosti certifikátu, ktorý používa Správca digitálnych certifikátov (DCM), je rôzny na základe typu Certifikačnej autority (CA), ktorá vystavila tento certifikát.

Certifikát môžete obnoviť pomocou lokálneho alebo internetového CA.

Obnova certifikátu od lokálnej certifikačnej autority

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 chcete obnoviť certifikát pomocou lokálneho CA, vykonajte tieto kroky:

1. V navigačnej časti kliknite na **Vybrať sklad certifikátov**, potom vyberte sklad certifikátov obsahujúci certifikát, ktorý chcete obnoviť.
2. V navigačnej časti vyberte **Manažovať certifikáty**.
3. V navigačnej časti vyberte **Obnoviť certifikát**.
4. Vyberte certifikát, ktorý chcete obnoviť a kliknite na **Obnoviť**.
5. Vyberte voľbu **Lokálna certifikačná autorita (CA)** a kliknite na **Pokračovať**.
6. Vyplňte formulár na identifikáciu certifikátu. Pole **Nové označenie certifikátu** musíte zmeniť, ale ostatné polia môžu ostať pôvodné.
7. Vyberte aplikácie, ktoré majú používať obnovený certifikát a kliknutím na **Pokračovať** dokončite obnovu certifikátu.

   Poznámka: Aby ste mohli používať certifikát, nemusíte vybrať aplikáciu.

Obnova certifikátu od internetovej certifikačnej autority

Ak na vydanie certifikátu používate všeobecne známu internetovú certifikačnú autoritu, môžete obnovu certifikátu vykonať dvoma rôznymi spôsobmi.

Certifikát môžete obnoviť priamo pomocou internetového CA a potom importovať obnovený certifikát zo súboru, ktorý získate od podpisujúceho CA. Alebo môžete pomocou DCM vytvoriť pre certifikát nový pár verejného a súkromného kľúča a požiadavku o podpísanie certifikátu (CSR) a potom tieto informácie odoslať internetovej certifikačnej autorite, aby ste získali nový certifikát. Keď od CA prijmete tento certifikát späť, môžete dokončiť proces obnovenia.

Importovanie a obnova certifikátu získaného priamo od internetovej certifikačnej autority:

Ak chcete importovať a obnoviť certifikát, ktorý ste získali priamo od internetového CA, vykonajte tieto kroky:

1. V navigačnej časti kliknite na **Vybrať sklad certifikátov**, potom vyberte sklad certifikátov obsahujúci certifikát, ktorý chcete obnoviť.

   Poznámka: Kliknite na "?" pre ľubovoľný panel, ak chcete získať odpovede na vaše otázky týkajúce sa vypĺňania údajov v paneli.
2. V navigačnej časti vyberte **Manažovať certifikáty**.
3. V navigačnej časti kliknite na **Obnoviť certifikát**.
4. Vyberte certifikát, ktorý chcete obnoviť a kliknite na **Obnoviť**.
5. Vyberte **VeriSign** alebo inú **Internetovú certifikačnú autoritu (CA)** a kliknite na **Pokračovať**.
6. Vyberte voľbu **Nie - Importovať obnovený podpísaný certifikát z existujúceho súboru**.
7. Dokončite riadenú úlohu, aby ste importovali certifikát. Keď zvolíte obnovu certifikátu priamo pomocou vydávajúceho CA, toto CA vám vráti obnovený certifikát v súbore. Pri importovaní certifikátu skontrolujte, že ste zadali správnu absolútnu cestu k súboru, v ktorom je v serveri uložený certifikát. Súbor obsahujúci obnovený certifikát môže byť uložený v ľubovoľnom adresári integrovaného súborového systému (IFS).
8. Kliknite na **OK** na ukončenie úlohy.

Obnova certifikátu vytvorením nového páru verejného a súkromného kľúča a CSR pre certifikát:

Ak chcete obnoviť certifikát pomocou internetového CA vytvorením nového páru verejného a súkromného kľúča a CSR pre certifikát, vykonajte tieto kroky:

1. V navigačnej časti kliknite na **Vybrať sklad certifikátov**, potom vyberte sklad certifikátov obsahujúci certifikát, ktorý chcete obnoviť.

   Poznámka: Kliknite na "?" pre ľubovoľný panel, ak chcete získať odpovede na vaše otázky týkajúce sa vypĺňania údajov v paneli.
2. V navigačnej časti vyberte **Manažovať certifikáty**.
3. V navigačnej časti kliknite na **Obnoviť certifikát**.
4. Vyberte certifikát, ktorý chcete obnoviť a kliknite na **Obnoviť**.
5. Vyberte **VeriSign** alebo inú **Internetovú certifikačnú autoritu (CA)** a kliknite na **Pokračovať**.
6. Kliknite na voľbu **Áno - Vytvoriť pre tento certifikát nový pár kľúčov** a kliknite na **Pokračovať**.
7. Vyplňte formulár na identifikáciu certifikátu. Pole Nové označenie certifikátu musíte zmeniť, ale ostatné polia môžu ostať pôvodné. Poznámka: Kliknite na "?" pre ľubovoľný panel, ak chcete získať odpovede na vaše otázky týkajúce sa vypĺňania údajov v paneli.
8. Kliknite na **OK** na ukončenie úlohy.

Importovanie certifikátu

Dozviete sa tu, ako môžete pomocou Správcu digitálnych certifikátov (DCM) importovať certifikáty, ktoré sa nachádzajú v súboroch vo vašom serveri.

Namiesto opakovaného vytvorenia certifikátu v aktuálnom serveri môžete certifikát tiež importovať z iného servera. Napríklad v systéme iSeries A ste pomocou lokálneho CA vytvorili certifikát vašej webovej obchodnej aplikácie, ktorý sa používa na inicializáciu pripojení SSL. Vaša spoločnosť sa nedávno rozrástla a vy ste nainštalovali nový server iSeries (iSeries B), ktorý bude hosťovať viac inštancií tejto vyťaženej obchodnej aplikácie. Chcete, aby všetky inštancie obchodnej aplikácie používali na identifikáciu a inicializáciu pripojení SSL identický certifikát. Následne môžete pomocou lokálneho CA v iSeries A vytvoriť nový, odlišný certifikát, ktorý bude používať iSeries B. Namiesto toho sa môžete rozhodnúť, že importujete certifikát lokálneho CA a certifikát servera zo systému iSeries A do systému iSeries B.

Ak chcete pomocou DCM importovať certifikát, vykonajte tieto kroky:

1. V ľavej navigačnej časti okna kliknite na **Vybrať sklad certifikátov** a vyberte sklad certifikátov, do ktorého chcete importovať certifikát. Sklad certifikátov, do ktorého chcete importovať certifikát, musí obsahovať certifikáty rovnakého typu, ako certifikát, ktorý ste exportovali v druhom systéme. Ak importujete napríklad certifikát servera (typ), musíte ho importovať do skladu certifikátov, ktorý obsahuje certifikáty serverov ako *SYSTEM, alebo do skladu certifikátov iného servera.
2. V navigačnej časti vyberte **Manažovať certifikáty**.
3. V navigačnej časti vyberte **Importovať certifikát**.
4. Vyberte typ certifikátu, ktorý chcete importovať a vyberte **Pokračovať**. Typ importovaného certifikátu musí byť rovnaký ako typ certifikátu, ktorý ste exportovali. Ak ste napríklad exportovali certifikát servera, zvoľte import certifikátu servera.

   Poznámka: Keď DCM exportuje certifikát vo formáte pkcs12, do exportovaného reťazca certifikátov sa zahrnie vydávajúce CA, takže keď DCM importuje samotný certifikát do skladu certifikátov, automaticky sa importuje aj certifikát vydávajúceho CA. Ak však certifikát nebol exportovaný vo formáte pkcs12 a v sklade certifikátov, do ktorého importujete, nemáte certifikát CA, pred importom certifikátu musíte importovať certifikát vydávajúceho CA.
5. Dokončite riadenú úlohu, aby ste importovali certifikát. Pri importovaní certifikátu skontrolujte, že ste zadali správnu absolútnu cestu, kde sa v serveri nachádza certifikát.

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.

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:

Vydávanie certifikátov pre iné systémy iSeries pomocou lokálneho CA

Dozviete sa tu, ako pomocou súkromného lokálneho CA v jednom systéme vydávať certifikáty, ktoré sa budú používať v iných systémoch iSeries.

V systéme vo vašej sieti už možno používate súkromnú lokálnu certifikačnú autoritu (CA). Teraz chcete rozšíriť použitie tohto lokálneho CA na iný systém v sieti. Chcete napríklad, aby aktuálne lokálne CA vydalo certifikát servera alebo klienta pre aplikáciu v inom systéme, ktorá ju bude používať 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 z úloh vykonáte v systéme, v ktorom prevádzkujete lokálne CA a ostatné v sekundárnom systéme, 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: Ak systém, v ktorom prevádzkujete lokálne CA, používa produkt kryptografického poskytovateľa prístupu, ktorý poskytuje silnejšie šifrovanie ako cieľový systém, môže dôjsť k problému. Pre OS/400 V5R2 a OS/400 V5R3 je jediným dostupným kryptografickým poskytovateľom prístupu produkt 5722–AC3, čo je najsilnejší dostupný produkt. V starších vydaniach však bolo možné nainštalovať iné, slabšie produkty kryptografických poskytovateľov prístupu (5722–AC1 alebo 5722–AC2), ktoré poskytujú nižšie úrovne kryptografických funkcií. Keď exportujete certifikát (s jeho súkromným kľúčom), systém zašifruje súbor, aby chránil jeho obsah. Ak systém používa silnejší kryptografický produkt ako cieľový systém, cieľový systém nemôže počas procesu importu tento súbor dešifrovať. Následne, import zlyhá alebo tento certifikát nebudete môcť použiť na vytvorenie SSL relácií. Toto platí aj v prípade, ak pre nový certifikát použijete veľkosť kľúča, ktorá je vhodná na použitie s kryptografickým produktom na cieľovom systéme.

Vašu lokálnu CA môžete použiť na vydávanie certifikátov iným systémom, ktoré potom môžete používať na podpisovanie objektov, alebo ktoré môžu aplikácie používať na vytváranie relácií SSL. Keď pomocou lokálneho CA vytvoríte certifikát, ktorý bude používať iný systém, súbory vytvorené v DCM budú obsahovať kópiu certifikátu lokálneho CA, ako aj kópie certifikátov pre mnoho verejných internetových certifikačných autorít.

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.

Vydávanie súkromných certifikátov, ktoré sa budú používať v inom systéme iSeries

Ak chcete pomocou vášho lokálneho CA vydávať certifikáty, ktoré bude používať iný systém, v systéme hosťujúcom lokálne CA vykonajte tieto kroky:

1. Spustenie DCM
2. V navigačnom rámci zvoľte **Create Certificate** na zobrazenie zoznamu typov certifikátov, na ktorých vytvorenie môžete použiť lokálnu CA.

   Poznámka: Na vykonanie tejto úlohy nemusíte otvoriť sklad certifikátov. Tieto pokyny predpokladajú, že nepracujete v špecifickom sklade certifikátov alebo že pracujete v sklade certifikátov lokálnej certifikačnej autority (CA). Lokálna CA musí existovať na tomto systéme pred tým, ako budete môcť

vykonať tieto úlohy. 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 typ certifikátu, ktorý chcete, aby lokálna CA vydala a kliknite na **Continue** na spustenie riadenej úlohy a dokončenie série formulárov.
4. Vyberte, či chcete vytvoriť **certifikát servera alebo klienta pre iný systém iSeries** (pre relácie SSL) alebo **certifikát podpisujúci objekty pre iný systém iSeries** (pre použitie v inom systéme).

   Poznámka: Ak vytvárate certifikát podpisujúci objekty pre použitie v inom systéme, tento systém musí používať operačný systém OS/400 V5R1 alebo novší, inak nebude možné certifikát použiť. Cieľový systém musí byť OS/400 V5R1 alebo novší, preto vás DCM v lokálnom systéme nevyzve na zadanie formátu cieľového vydania pre nový certifikát podpisujúci objekty.
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.

   DCM vytvorí certifikát vo vlastnom sklade certifikátov a vygeneruje dva súbory, ktoré musíte preniesť: súbor skladu certifikátov (rozšírenie .KDB) a súbor požiadaviek (rozšírenie .RDB).
6. Na prenos týchto súborov do cieľového systému použite FTP (File Transfer Protocol) alebo inú metódu.

Súvisiace koncepty

"Úvahy o zálohovaní a obnove údajov DCM" na strane 26
Dozviete sa tu, ako zabezpečiť, že sa dôležité údaje DCM pridajú do plánu pre zálohovanie a obnovu vášho systému.

"Verejné certifikáty verzus súkromné certifikáty" na strane 28
Dozviete sa tu, ako určiť, ktorý typ certifikátu (verejný alebo súkromný) najlepšie vyhovuje vašim obchodným potrebám.

Súvisiace úlohy

"Vytvorenie a prevádzkovanie lokálnej CA" na strane 38
Tieto informácie opisujú spôsob vytvorenia a sprevádzkovania lokálnej certifikačnej autority (CA) na vydávanie súkromných certifikátov pre vaše aplikácie.

Použitie súkromného certifikátu pre SSL

Certifikáty, ktoré používajú vaše aplikácie pre SSL relácie zo skladu certifikátov *SYSTEM manažujete v Správcovi digitálnych certifikátov (DCM). Ak ste v cieľovom systéme pomocou DCM nikdy nemanažovali certifikáty pre SSL, tento sklad certifikátov v ňom nebude existovať.

Úlohy pre použitie prenesených súborov skladu certifikátov, ktoré ste vytvorili v hostiteľskom systéme lokálnej certifikačnej autority (CA), sa líšia podľa toho, či existuje sklad certifikátov *SYSTEM. Ak sklad certifikátov *SYSTEM neexistuje, môžete na jeho vytvorenie použiť prenesené súbory skladu certifikátov. Ak v cieľovom systéme existuje sklad certifikátov *SYSTEM, môžete prenesené súbory použiť ako sklad certifikátov iného systému alebo ich importovať do existujúceho skladu certifikátov *SYSTEM.

Sklad certifikátov *SYSTEM neexistuje:

Ak v systéme, v ktorom chcete použiť prenesené súbory skladu certifikátov, neexistuje sklad certifikátov *SYSTEM, môžete tieto súbory použiť ako sklad certifikátov *SYSTEM. Ak chcete vytvoriť sklad certifikátov *SYSTEM a použiť súbory certifikátov v cieľovom systéme, vykonajte tieto kroky:

1. Skontrolujte, že sa súbory skladu certifikátov (dva súbory, jeden s príponou .KDB a jeden s príponou .RDB) vytvorené v systéme, ktorý hosťuje lokálne CA, nachádzajú 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 spolu s kópiou certifikátu lokálneho CA pridal do súborov skladu certifikátov pri ich vytvorení.

   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 Other System Certificate Store, 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 Sklad certifikátov a heslo, zadajte heslo, ktoré ste zadali pre sklad certifikátov v *hostiteľskom* systéme pri vytváraní certifikátu pre cieľový systém a kliknite na **Pokračovať**.
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 v *hostiteľskom* systéme a kliknite na **Priradiť k aplikáciám**, aby sa zobrazil zoznam aplikácií s povoleným SSL, ku ktorým môžete certifikát priradiť.
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 úloh môžu aplikácie v cieľovom systéme používať certifikát, ktorý vydalo lokálne CA v inom systéme. Pred začatím používania SSL v týchto aplikáciách však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát 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 - použitie súborov ako sklad certifikátov iného systému:

Ak už cieľový systém obsahuje sklad certifikátov *SYSTEM, musíte sa rozhodnúť, ako použijete súbory certifikátov, ktoré ste do tohto systému preniesli. 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 množstvo aplikácií od iných vývojárov) sú napísané tak, že používajú iba certifikáty nachádzajúce sa v sklade certifikátov *SYSTEM. Ak sa rozhodnete, že prenesené súbory použijete ako Other System Certificate Store, na určenie, ktoré aplikácie budú tento certifikát používať pre relácie SSL, nemôžete použiť DCM. Preto štandardné aplikácie iSeries s povoleným SSL nemôžete nakonfigurovať na používanie tohto certifikátu. Ak chcete používať certifikát pre aplikácie iSeries, musíte certifikát z prenesených súborov skladu certifikátov importovať do skladu certifikátov *SYSTEM.

Ak chcete pristúpiť na prenesené súbory certifikátov a pracovať s nimi ako s Iným systémovým skladom certifikátov, vykonajte tieto kroky:

1. Spustite DCM.
2. V navigačnej časti kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte **Sklad certifikátov iného systému**.
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. Zadajte tiež heslo, ktoré ste zadali pre sklad certifikátov v *hostiteľskom* systéme pri vytváraní certifikátu pre cieľový systém a kliknite na **Pokračovať**.
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 určiť, aby sa certifikát v tomto sklade používal ako predvolený 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 sklad certifikátov iného systému, všetky aplikácie používajúce API SSL_Init môžu pomocou certifikátu z tohto skladu vytvárať relácie SSL.

*Sklad certifikátov *SYSTEM existuje - použitie certifikátov v existujúcom sklade certifikátov *SYSTEM:*

Certifikáty z prenesených súborov skladu certifikátov môžete použiť v existujúcom sklade certifikátov *SYSTEM v systéme. 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 Other System Certificate Store a exportovať ich do skladu certifikátov *SYSTEM.

Ak chcete certifikáty zo súborov skladu certifikátov exportovať do skladu certifikátov *SYSTEM, vykonajte v cieľovom systéme 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. Zadajte tiež heslo, ktoré ste zadali pre sklad certifikátov v *hostiteľskom* systéme pri vytváraní certifikátu pre cieľový systém a kliknite na **Pokračovať**.
4. 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.

   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.
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 oznamujúca, že certifikát sa úspešne exportoval, alebo v prípade zlyhania procesu exportovania sa zobrazí správa s informáciami o chybe.
12. Teraz môžete do skladu certifikátov *SYSTEM exportovať serverový alebo klientsky certifikát. Znova vyberte úlohu **Exportovať certifikát**.
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 oznamujúca, že certifikát sa úspešne exportoval, alebo v prípade zlyhania procesu exportovania sa zobrazí správa s informáciami o chybe.
17. Teraz môžete certifikát priradiť aplikácii na použitie pre SSL. V navigačnej časti kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte ***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 v *hostiteľskom* systéme a kliknite na **Priradiť k aplikáciám**, aby sa zobrazil zoznam aplikácií s povoleným SSL, ku ktorým môžete certifikát priradiť.
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.

Po dokončení týchto úloh môžu aplikácie v cieľovom systéme používať certifikát, ktorý vydalo lokálne CA v inom systéme. Pred začatím používania SSL v týchto aplikáciách však musíte nakonfigurovať aplikácie na používanie SSL.

Pred tým ako bude môcť užívateľ pristúpiť na zvolené aplikácie cez pripojenie SSL, musí použiť DCM na získanie kópie certifikátu lokálnej CA z hostiteľského systému. Certifikát 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 na podpisovanie objektov v cieľovom systéme

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 na jeho vytvorenie použiť prenesené súbory s certifikátmi. Ak v cieľovom systéme existuje sklad certifikátov *OBJECTSIGNING, musíte doň importovať prenesené certifikáty.

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 s prenesenými súbormi skladu certifikátov neexistuje sklad certifikátov *OBJECTSIGNING, vykonajte tieto kroky:

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 kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte ***OBJECTSIGNING**.
5. Keď sa zobrazí stránka s heslom, zadajte heslo, ktoré ste zadali pri vytváraní skladu certifikátov v hostiteľskom systéme a kliknite na **Pokračovať**.

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. Vyplňte formulár na definovanie vašej aplikácie na podpisovanie objektov a kliknite na **Pridať**. Táto definícia aplikácie nepopisuje skutočnú aplikáciu, ale popisuje typ objektov, ktoré chcete podpisovať konkrétnym certifikátom. Pri vypĺňaní formuláru môžete použiť online pomoc.
10. Kliknite na **OK**, aby sa potvrdila správa o vytvorení definície a zobrazte si zoznam úloh **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, čo potrebujete na podpisovanie objektov na zabezpečenie ich integrity.

Keď distribuujete podpísané objekty, ich príjemcovia musia pomocou DCM skontrolovať podpis objektu, aby overili, že údaje nie sú zmenené a aby skontrolovali identitu odosielateľa. Aby mohol príjemca skontrolovať podpis, musí mať kópiu certifikátu na kontrolu podpisu. Kópiu tohto certifikátu musíte poskytnúť ako súčasť balíka podpísaných objektov.

Príjemca musí mať tiež kópiu certifikátu certifikačnej autority, ktorá vydala certifikát použitý 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:

Certifikáty z prenesených súborov skladu certifikátov môžete použiť v existujúcom sklade certifikátov *OBJECTSIGNING v systéme. 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. Certifikáty môžete do existujúceho skladu certifikátov *OBJECTSIGNING pridať tak, že v cieľovom systéme otvoríte prenesené súbory ako sklad 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.

Ak chcete certifikáty zo súborov skladu certifikátov exportovať priamo do skladu certifikátov *OBJECTSIGNING, vykonajte v cieľovom systéme tieto kroky:

1. Spustite DCM.
2. V navigačnej časti kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte **Sklad certifikátov iného systému**.
3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súborov skladu certifikátov. Zadajte tiež heslo, ktoré ste použili pri ich vytváraní v hostiteľskom systéme a kliknite na **Pokračovať**.
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 **Exportovať certifikát**.
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 **Sklad certifikátov** a kliknite na **Pokračovať**.
16. Ako cieľový sklad certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**. Zobrazí sa správa oznamujúca, že certifikát sa úspešne exportoval, alebo v prípade zlyhania procesu exportovania sa zobrazí správa s informáciami o chybe.

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

Manažovanie aplikácií v DCM

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.

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:

Súvisiace koncepty

"Definície aplikácií" na strane 10
Tieto informácie vás oboznámia s definíciami aplikácií v DCM a s ich používaním na konfigurovanie SSL a podpisovanie objektov.

Vytvorenie definícií aplikácie

V tejto téme sa dozviete o dvoch rôznych typoch aplikácií, ktoré môžete definovať a pracovať s nimi.

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 iSeries s povoleným SSL sa registrujú v DCM, takže k nim môžete pomocou DCM jednoducho priradiť certifikát, aby mohli vytvárať relácie 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 **Vybrať sklad certifikátov** a vyberte vhodný 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.

Súvisiace koncepty

"Definície aplikácií" na strane 10
Tieto informácie vás oboznámia s definíciami aplikácií v DCM a s ich používaním na konfigurovanie SSL a podpisovanie objektov.

Manažovanie pridelenia certifikátu k 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 **Vybrať sklad certifikátov** a vyberte vhodný 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 automaticky aplikujú všetky vykonané zmeny certifikátov. Aby vaše aplikácie aplikovali všetky zmeny certifikátov, možno budete musieť zastaviť a znova spustiť servery Telnet, IBM HTTP Server for i5/OS a iné.

V systéme OS/400 V5R2 alebo novšom môžete na priradenie certifikátu k viacerým aplikáciám naraz použiť úlohu Priradiť certifikát.

Definovanie zoznamu dôveryhodných CA pre aplikáciu

Aplikácie, ktoré podporujú používanie certifikátov na autentifikáciu klientov počas relácie SSL (Secure Sockets Layer), musia určiť, či akceptujú 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 **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte ***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 exspirácie, aby administrátorom umožnil pomocou dátumu exspirácie v lokálnom systéme manažovať certifikáty serverov a klientov, certifikáty podpisujúce objekty a užívateľské certifikáty.

Poznámka: Ak nakonfigurujete Správcu digitálnych certifikátov, aby spolupracoval s EIM (Enterprise Identity Mapping), môžete vo vašej spoločnosti riadiť užívateľské certifikáty pomocou dátumu exspirácie.

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: Certifikát na kontrolu podpisu môžete použiť na kontrolu podpisov objektov aj keď certifikát exspiroval, preto DCM neposkytuje podporu pre kontrolu exspirácie 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.
2. V navigačnom rámci kliknite na **Select a Certificate Store** a vyberte ***OBJECTSIGNING** alebo ***SYSTEM**.

   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.
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. 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.

validácia certifikátu

Keď validujete certifikát, DCM kontroluje množstvo položiek, týkajúcich sa certifikátu, aby zaistil autenticitu a platnosť tohto certifikátu. Validácia certifikátu zaručuje, že v aplikáciách, ktoré používajú certifikát na bezpečnú komunikáciu alebo podpisovanie objektov, by nemalo dôjsť k problémom pri používaní certifikátu.

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.

Súvisiace koncepty

“Umiestnenia Zoznamu odmietaných certifikátov (CRL)” na strane 6
Certificate Revocation List (CRL) je súbor, ktorý obsahuje všetky neplatné a zrušené certifikáty pre konkrétnu Certifikačnú autoritu (CA).

“Overenie platnosti” na strane 10
Správca digitálnych certifikátov (DCM) poskytuje úlohy, ktoré vám umožnia validovať certifikát alebo aplikáciu na overenie rôznych vlastností, ktoré musia mať.

Priradenie certifikátu aplikáciám

Správca digitálnych certifikátov (DCM) vám umožňuje jednoducho a rýchlo priradiť certifikát k 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.
2. V navigačnom rámci kliknite na **Select a Certificate Store** a vyberte ***OBJECTSIGNING** alebo ***SYSTEM**.

   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.
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 manažovať informácie o umiestnení zoznamu zrušených certifikátov (CRL) špecifickej certifikačnej autority, ktoré sa použijú v rámci procesu validácie 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 **Manažovanie umiestnení CRL**, aby sa zobrazil zoznam úloh.

   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. 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. Teraz musíte priradiť definíciu umiestnenia CRL k špecifickému CA.
5. V navigačnej časti vyberte **Manažovať certifikáty**, aby sa zobrazil zoznam 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).

Poznámka: Ak chcete vytvoriť anonymnú väzbu k serveru LDAP pre spracovanie CRL, musíte použiť webový administratívny nástroj pre adresárový server a pomocou úlohy ″Manažovať schému″ zmeniť triedu bezpečnosti (označovanú tiež ako ″trieda prístupu″) atribútov certificateRevocationList a authorityRevocationList z hodnoty ″critical″ na ″normal″ a ponechať polia **Rozlišovací názov pre prihlásenie** a **Heslo** prázdne.

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..

Súvisiace koncepty

"Umiestnenia Zoznamu odmietaných certifikátov (CRL)" na strane 6
Certificate Revocation List (CRL) je súbor, ktorý obsahuje všetky neplatné a zrušené certifikáty pre konkrétnu Certifikačnú autoritu (CA).

Súvisiace informácie

IBM Directory Server for iSeries (LDAP)

Povolenie SSL v adresárovom serveri

Ukladanie kľúčov certifikátov v kryptografickom koprocesore IBM

Dozviete sa tu, ako pomocou nainštalovaného koprocesora poskytnúť bezpečnejší úložný priestor pre súkromné kľúče vašich certifikátov.

Ak máte vo vašom systéme nainštalovaný kryptografický koprocesor IBM, môžete ho použiť na bezpečnejšie uloženie súkromného kľúča 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 v samotnom koprocesore.
- Zašifrovanie súkromného kľúča certifikátu pomocou hlavného kľúča koprocesora za účelom jeho uloženia 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.

Súvisiace koncepty

"Kryptografické koprocesory IBM pre iSeries" na strane 9
Šifrovací koprocesor poskytuje pre vyvíjanie bezpečných aplikácií elektronického obchodu osvedčené šifrovacie služby, zabezpečujúce súkromie a integritu.

Uložiť súkromné kľúče certifikátov priamo na koprocesore

Ak chcete zvýšiť bezpečnosť pri ochrane prístupu k súkromnému kľúču certifikátu a pri jeho používaní, môžete kľúč uložiť priamo do kryptografického koprocesora 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 zvýšiť bezpečnosť pri ochrane prístupu k súkromnému kľúču certifikátu a pri jeho používaní, môžete súkromný kľúč zašifrovať pomocou hlavného kľúča kryptografického koprocesora IBM a kľúč uložiť do špeciálneho súboru kľúčov. Túto voľbu pamäte pre kľúč môžete vybrať ako súčasť vytvárania alebo obnovy certifikátu v Správcovi digitálnych zariadení.

Skôr, než budete môcť úspešne použiť túto voľbu, musíte pomocou webového konfiguračného rozhrania kryptografického koprocesora IBM 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. Webové konfiguračné rozhranie je prístupné zo stránky Úlohy iSeries.

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

Ak chcete použiť hlavný kľúč koprocesora na zašifrovanie hlavného kľúča certifikátu a uložiť ho v špeciálnom súbore kľúčov, vykonajte kroky zo strany **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. Webové konfiguračné rozhranie je prístupné zo stránky Úlohy iSeries.
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.

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. Registračná autorita alebo žiadateľ (v závislosti od používanej procedúry certifikačnej autority) predloží certifikovanú aplikáciu priradenej certifikačnej autorite. 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**.

Poznámka: Štandardy PKIX sú obsiahnuté v Request For Comments (RFC) 2560.

Súvisiace koncepty

"Manažovanie certifikáty z verejnej internetovej CA" na strane 45
Dozviete sa tu, ako pomocou vytvorenia skladu certifikátov manažovať certifikáty od verejného internetového CA.

Riadenie umiestenia LDAP pre užívateľské certifikáty

Dozviete sa tu, ako nakonfigurovať DCM na ukladanie užívateľských certifikátov do adresárovej lokality servera LDAP (Lightweight Directory Access Protocol), aby mohlo EIM (Enterprise Identity Mapping) pracovať s užívateľskými certifikátmi.

Správca digitálnych certifikátov (DCM) štandardne ukladá užívateľské certifikáty, ktoré vydá lokálna certifikačná autorita (CA), spolu 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 umiestnenia v LDAP certifikát od iného CA, užívateľ musí vykonať úlohu **Priradenie užívateľského certifikátu**.

EIM je technológia @server , ktorá vám umožňuje manažovať identity užívateľov vo vašej spoločnosti, vrátane užívateľských profilov i5/OS a certifikátov užívateľov. Ak chcete EIM používať na manažovanie užívateľských certifikátov, musíte pred vykonaním všetkých úloh konfigurácie DCM vykonať tieto úlohy konfigurácie EIM:

1. Pomocou sprievodcu **Konfigurácia EIM** v Navigátore Navigátor iSeries nakonfigurujte EIM.
2. V doméne EIM, ktorá sa má používať pre priradenia certifikátov, vytvorte register X.509.
3. Vyberte voľbu ponuky Vlastnosti pre zložku Konfigurácia v doméne EIM a zadajte názov registra X.509.
4. Vytvorte identifikátor EIM pre každého užívateľa, ktorého chcete mať zapojeného do EIM.
5. Vytvorte cieľové priradenie medzi každým identifikátorom EIM a profilom daného užívateľa v lokálnom registri užívateľov i5/OS. Pre lokálny register užívateľov i5/OS použite názov definície registra EIM, ktorý ste zadali v sprievodcovi **Konfigurácia EIM**.

   Poznámka: Informácie o konfigurovaní EIM nájdete v téme EIM.

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. Umiestnenie LDAP nemusí byť v lokálnom systéme iSeries, ani nemusí ísť o rovnaký server LDAP ako 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. Vykonajte 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 .

Poznámka: Ak chcete vytvoriť anonymnú väzbu k serveru LDAP pre spracovanie CRL, musíte použiť webový administratívny nástroj pre adresárový server a pomocou úlohy ″Manažovať schému″ zmeniť triedu bezpečnosti (označovanú tiež ako ″trieda prístupu″) atribútov certificateRevocationList a authorityRevocationList z hodnoty ″critical″ na ″normal″ a ponechať polia **Rozlišovací názov pre prihlásenie** a **Heslo** prázdne.

Súvisiace úlohy

“Digitálne certifikáty a architektúra Enterprise Identity Mapping (EIM)” na strane 32
Spoločné používanie EIM (Enterprise Identity Mapping) a Správcu digitálnych certifikátov (DCM) vám umožňuje použiť certifikát ako zdroj pre operáciu vyhľadávania mapovaní EIM na namapovanie certifikátu na cieľovú identitu užívateľa, priradenú k rovnakému identifikátoru EIM.

Podpisovanie objektov

Dozviete sa tu, ako pomocou DCM manažovať certifikáty, ktoré používate na digitálne podpisovanie objektov na zabezpečenie ich integrity.

Na podpisovanie objektov môžete použiť tri metódy. Môžete napísať program, ktorý volá API podpísania objektu. Môžete použiť Správcu digitálnych certifikátov (DCM) na podpisovanie objektov. V systéme OS/400 V5R2 alebo novšom môžete pomocou vlastnosti Riadiaca centrála z Navigátor iSeries podpisovať objekty pri ich balení za účelom distribúcie do iných systémov.

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). V systéme OS/400 V5R2 alebo novšom môžete tiež podpisovať objekty príkazov (*CMD). Objekty, ktoré sú uložené v iných systémoch, nemôžete podpisovať.

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. Spustenie DCM
2. V navigačnej časti kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte ***OBJECTSIGNING**.

   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.
3. Zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Pokračovať**.
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 špecifickom adresári, môžete zadať hodnotu /mojadresar/*; ak chcete podpísať všetky programy v špecifickej knižnici, môžete zadať hodnotu /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 pomocou funkcie Prehľadať zobraziť obsah knižnice alebo adresára, musíte pred kliknutím na tlačidlo **Prehľadať** zadať ako súčasť názvu cesty 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:

- Museli ste 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.
2. V navigačnej časti kliknite na **Vybrať sklad certifikátov** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte ***SIGNATUREVERIFICATION**.

   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.
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 pomocou funkcie Prehľadať zobraziť obsah knižnice alebo adresára, musíte pred kliknutím na tlačidlo **Prehľadať** zadať ako súčasť názvu cesty 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.

Súvisiace koncepty

"Digitálne certifikáty na podpisovanie objektov" na strane 34
Tieto informácie vám vysvetlia, ako používať certifikáty na zaistenie integrity objektu, alebo ako skontrolovať digitálny podpis na objekte za účelom kontroly jeho autenticity.

Súvisiace úlohy

"Manažovanie certifikátov na overovanie podpisov objektov" na strane 49
Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie certifikátov na kontrolu podpisov, ktoré používate na validovanie digitálnych podpisov na objektoch.

Odstránenie problémov DCM

Dozviete sa tu, ako riešiť niektoré bežné chyby, ku ktorým môže dôjsť pri používaní 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

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 ikonu pomoci - "**?**". Môžete tiež prehľadať Informačné centrum a externé webové lokality 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.
Pri pokuse o otvorenie skladu certifikátov sa zobrazí chybová správa, informujúca o exspirovaní vášho hesla.	Musíte si zmeniť heslo pre sklad certifikátov. Kliknutím na tlačidlo **OK** zmeňte heslo.
Váš pokus o opakované nastavenie hesla pri použití úlohy **Výber skladu certifikátov** 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 Other System Certificate Store, musíte označiť voľbu **Automatic login**, keď meníte heslo, na zabezpečenie, že DCM uloží nové heslo pre tento typ skladu certifikátov.

Problém	Možné riešenie
	Skontrolujte hodnotu priradenú k atribútu **Povoliť nové digitálne certifikáty** pod voľbou **Práca s bezpečnosťou systému** v Systémových servisných nástrojoch (SST). 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. K tomuto problému dochádza častejšie, keď na prístup k prehliadaču Netscape Communications používate Navigátor iSeries. 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 skontrolujte, či má váš systém správne nastavenú hodnotu pre posun od 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 sa v takomto prípade pokúsite v systéme použiť certifikát, nebude mať správny formát. 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.
Serverové produkty a prehliadač Netscape Communicator využívajú koreňové certifikáty od spoločností, vrátane (ale nie len) VeriSign, ako vlastnosť na povolenie komunikácie SSL - konkrétne 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 koreňových certifikátoch prehliadačov sú dostupné na viacerých 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.

Odstraňovanie problémov s produktom HTTP Server for iSeries

Problém	Možné riešenie
HTTPS (Hypertext Transfer Protocol Secure) nefunguje.	Presvedčte sa, či je HTTP Server správne nakonfigurovaný na použitie SSL. Vo vydaní V5R1 alebo novšom musí mať konfiguračný súbor pomocou rozhrania Správa servera HTTP nastavenú hodnotu **SSLAppName**. 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.	Vo vašom systéme prejdite do rozhrania Správa servera HTTP a nastavte konfiguráciu vášho servera HTTP. 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.
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.

Problém	Možné riešenie
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. Informácie o týchto rozhraniach API môžete nájsť v téme Vyhľadávač API v Informačnom centre. 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 nie je možné spustiť inštanciu servera *ADMIN, dočasne nastavte voľbu **SSL** na hodnotu Deaktivované, aby ste pre server *ADMIN mohli použiť 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. Produkt IBM HTTP Server for i5/OS nie je správne nastavený na vykonávanie registrácie certifikátov pomocou SSL a autentifikácie klientov v bezpečnej inštancii servera Správa. 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.

Súvisiace úlohy

"Priradenie užívateľského certifikátu" na strane 41
Užívateľský certifikát, ktorý vlastníte, môžete priradiť k vášmu vlastnému užívateľskému profilu i5/OS alebo k identite iného užívateľa. 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.

Informácie súvisiace s DCM

Na tejto stránke nájdete odkazy na iné zdroje, kde sa dozviete viac o digitálnych certifikátoch, infraštruktúre verejných kľúčov, Správcovi digitálnych certifikátov, ako aj iné súvisiace informácie.

Ako sa použitie digitálnych certifikátov stáva bežnejším, je k dispozícii čoraz viac zdrojov informácií. Nasleduje krátky zoznam iných zdrojov, ktoré si môžete pozrieť, ak sa chcete dozvedieť viac o digitálnych certifikátoch a o ich použití na vylepšenie bezpečnostnej politiky vašich systémov.

- **Webová lokalita VeriSign Help Desk** Webová lokalita VeriSign poskytuje rozsiahlu knižnicu informácií týkajúcich sa digitálnych certifikátov, ako aj množstvo iných tém z oblasti internetovej bezpečnosti.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168** Tento dokument IBM Redbook sa zameriava na vylepšenia bezpečnosti siete v OS/400 V5R1. Dokument Redbook pokrýva množstvo tém, vrátane opisu použitia schopností podpisovania objektov v iSeries, Správcu digitálnych certifikátov (DCM), podpory kryptografického koprocesora 4758 a podobne.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)** Tento dokument Redbook opisuje, čo môžete robiť s digitálnymi certifikátmi v serveri iSeries. Vysvetľuje, ako nastaviť rôzne servery a klientov na použitie certifikátov. Ďalej poskytuje informácie a vzorový kód pre používanie rozhraní API OS/400 na manažovanie a používanie digitálnych certifikátov v užívateľských aplikáciách.
- **RFC Index Search** Táto webová lokalita poskytuje archív dokumentov RFC (Request for Comments) s možnosťou vyhľadávania. 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 ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Ak chcete získať informácie o produktoch a službách, ktoré sú aktuálne dostupné vo vašej oblasti, kontaktujte lokálneho zástupcu spoločnosti IBM. Žiadny odkaz na produkt, službu alebo program IBM nemá za účelom naznačiť, že je možné použiť len tento produkt, službu alebo program IBM. Namiesto toho je možné použiť ľubovoľný funkčne ekvivalentný produkt, službu alebo program, ktorý neporušuje právo na intelektuálne vlastníctvo spoločnosti IBM. Užívateľ však zodpovedá za to, aby zhodnotil a overil používanie takéhoto produktu, programu alebo služby.

Spoločnosť IBM môže vlastniť patenty alebo mať podané žiadosti o patenty, ktoré sa týkajú predmetu opísaného v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Informácie o licenciách získate u výrobcu na adrese:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
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 106-0032, 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. Spoločnosť 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 lokalitách nie sú súčasťou materiálov pre tento produkt IBM a použitie týchto webových lokalít je na vlastné riziko.

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 YBWA
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 opísaný v týchto informáciách a všetok licenčný materiál preň dostupný poskytuje IBM za podmienok Zákazníckej zmluvy IBM, Medzinárodnej licenčnej zmluvy pre program IBM, Licenčnej zmluvy IBM pre strojový kód, alebo akejkoľvek 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.

Všetky ceny IBM sú navrhované predajné ceny stanovené spoločnosťou IBM, sú aktuálne a sú predmetom zmeny bez ohlásenia. Dílerské ceny sa môžu líšiť.

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.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez poplatku pre IBM, za účelom vývoja, používania, predaja alebo distribúcie aplikačných programov, vyhovujúcich aplikačnému programovému rozhraniu pre operačnú platformu, pre ktorú sú tieto programy napísané. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. IBM preto nemôže garantovať ani implikovať spoľahlivosť, prevádzkyschopnosť ani funkčnosť týchto programov.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (názov vašej spoločnosti) (rok). Časti tohto kódu sú odvodené zo vzorových programov spoločnosti IBM. © Copyright IBM Corp. _zadajte rok, alebo roky_. Všetky práva vyhradené.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

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

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

| Lotus
| Net.Data
| OS/400

Microsoft, Windows a logo Windows sú ochranné známky spoločnosti Microsoft Corporation v USA alebo iných krajinách.

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

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne 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. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA