System i

Bezpečnosť
Správca digitálnych certifikátov - DCM

Verzia 6, vydanie 1

System i

Bezpečnosť
Správca digitálnych certifikátov - DCM

Verzia 6, vydanie 1

Poznámka

Pred použitím týchto informácií a produktu, ktorý podporujú, si prečítajte informácie v časti “Vyhlásenia”, na strane 85.

Toto vydanie platí pre verziu 6, vydanie 1, modifikáciu 0 produktu IBM i5/OS (číslo produktu 5761-SS1) a všetky ďalšie vydania a modifikácie, pokiaľ nie je v nových vydaniach uvedené inak. Táto verzia nebeží na všetkých modeloch RISC (reduced instruction set computer) a nebeží ani na modeloch CISC.

Obsah

Správca digitálnych certifikátov

Správca digitálnych certifikátov (DCM) umožňuje riadiť digitálne certifikáty pre vašu sieť a používať SSL (Secure Sockets Layer) s cieľom povoliť bezpečnú komunikáciu pre viaceré aplikácie.

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. Digitálne certifikáty sú napríklad nevyhnutné na konfiguráciu a používanie SSL. 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. Viaceré platformy a aplikácie System i, napríklad FTP, Telnet a HTTP Server poskytujú podporu SSL na zabezpečenie súkromia údajov.

System i 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. Na podpisovanie objektov môžete použiť aj digitálne certifikáty a ich priradené bezpečnostné kľúče. Podpisovanie objektov vám umožňuje zistiť zmeny alebo možné zasahovanie do obsahu objektov overovaním podpisov na objektoch, čím sa zabezpečí ich integrita.

Získanie podpory System i pre certifikáty je jednoduché, keď používate správcu digitálnych certifikátov, ktorý je bezplatnou funkciou slúžiacou na centrálne riadenie certifikátov pre vaše aplikácie. DCM vám umožňuje manažovať certifikáty, ktoré získate od ľubovoľnej certifikačnej autority (CA). DCM môžete použiť aj na vytvorenie a prevádzku svojej vlastnej lokálnej CA, ktorá vydáva 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:

Súvisiace informácie

SSL (Secure Sockets Layer)

Podpisovanie objektov a overovanie podpisov

Čo je nové vo vydaní V6R1

Prečítajte si kolekciu tém o nových alebo zásadne zmenených informáciách pre správcu digitálnych certifikátov (DCM) pre i5/OS.

Nové informácie pre riadenie certifikátov podľa dátumu uplynutia platnosti

Tieto nové informácie vysvetľujú, ako riadiť certifikáty servera alebo klienta, certifikáty podpisujúce objekty, certifikáty certifikačnej autority a užívateľské certifikáty podľa dátumu uplynutia platnosti v lokálnom systéme.

- “Riadenie certifikátov podľa dátumu ukončenia platnosti” na strane 67

Nové informácie na spúšťanie DCM

Tieto nové informácie vysvetľujú krok za krokom proces spúšťania DCM vo vašom systéme. Nový proces zahŕňa použitie nového rozhrania webovej konzoly na porte 2001 s názvom IBM Systems Director Navigator for i5/OS .

- “Spúšťanie správcu digitálnych certifikátov” na strane 41

Ako určiť, čo je nové alebo zmenené

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

- Značka , ktorá označuje, kde začínajú nové alebo zmenené informácie.
- Značka , ktorá označuje, kde nové alebo zmenené informácie končia.

Ak chcete nájsť ďalšie informácie o tom, čo je v tomto vydaní nové alebo zmenené, pozrite si Poznámky pre užívateľov.

Súbor PDF pre DCM

Súbor PDF s týmito informáciami môžete zobraziť a vytlačiť.

Ak chcete zobraziť alebo stiahnuť PDF verziu tejto témy, vyberte Digital Certificate Manager (približne 1 100 KB).

Uloženie súborov PDF

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

1. Pravým tlačidlom myši kliknite na odkaz PDF vo vašom prehliadači.
2. Vyberte voľbu, ktorá ukladá súbor PDF lokálne.
3. Prejdite do adresára, do ktorého chcete tento súbor PDF uložiť.
4. Kliknite na **Save**.

Stiahnutie programu Adobe Acrobat Reader

Ak chcete zobrazovať alebo tlačiť tieto súbory PDF, potrebujete Adobe Acrobat Reader. Kópiu si môžete stiahnuť z webovej stránky spoločnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Koncepty DCM

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 správca digitálnych certifikátov (DCM) poskytuje, umožňuje používať len rozšírenia certifikátu Subject Alternative Name. 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) System i, musíte zadať informácie pre tieto rozšírenia.

Súvisiace koncepty

"Charakteristický názov"
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.

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 používate lokálnu CA na podpis obnoveného certifikátu, DCM použije informácie, ktoré poskytnete, na vytvorenie nového certifikátu v aktuálnom sklade certifikátov a uchová predchádzajúci certifikát.

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

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.

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.

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 alebo 6
- Plne kvalifikovaný názov domény
- E-mailová adresa

Súvisiace koncepty

“Rozšírenia certifikátov” na strane 2
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"
Certifikačná autorita (CA) je dôveryhodná centrálna administračná entita, ktorá môže vystavovať digitálne certifikáty užívateľom a serverom.

"Kryptografia" na strane 8
Zdieľané a verejné kľúče sú dva rozdielne typy šifrovacích funkcií používaných digitálnymi certifikátmi na poskytovanie bezpečnosti.

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

Certifikačná autorita

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 tiež použiť na prevádzku svojej vlastnej súkromnej lokálnej CA na vydávanie súkromných certifikátov systémom a užívateľom. Keď lokálna CA vydá užívateľský certifikát, DCM automaticky priradí certifikát k užívateľskému profilu System i užívateľa alebo inej užívateľskej identite. 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.

Certificate Authority policy data

Keď vytvárate lokálnu certifikačnú autoritu (CA) pomocou správcu digitálnych certifikátov, môžete zadať údaje politiky pre lokálnu CA. Údaje politiky pre lokálnu CA popisujú podpisovacie privilégiá CA. Údaje o politike určujú:

- Či môže lokálna CA vydávať a podpisovať užívateľské certifikáty.
- Ako dlho platia certifikáty vydané 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 CRL (Certificate Revocation List)

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. Nasledujú príklady aplikácií a procesov, ktoré môžu vykonávať spracúvanie CRL pre

autentifikáciu certifikátov: pripojenia VPN (Virtual Private Networking), server IKE (Internet Key Exchange), aplikácie povolené so SSL (Secure Sockets Layer) a proces podpisovania objektov. 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

"Overovanie platnosti certifikátov a aplikácií" na strane 68
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

"Riadenie umiestnení CRL" na strane 69
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 ukladanie certifikátu lokálnej CA a jej súkromného kľúča. Certifikát z tohto skladu certifikátov môžete použiť na podpisovanie certifikátov, na vydávanie ktorých používate lokálnu CA. Keď lokálna CA vydá certifikát, DCM umiestni kópiu certifikátu CA (bez súkromného kľúča) z autentifikačných dôvodov do príslušného skladu certifikátov (napríklad *SYSTEM). 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 System i (a mnoho ďalších aplikácií vývojárov softvéru) sú napísané tak, že používajú len certifikáty zo skladu certifikátov *SYSTEM. Keď používate DCM na vytvorenie lokálnej CA, DCM ako súčasť procesu vytvorí tento sklad certifikátov. 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 používate DCM na vytvorenie lokálnej CA, DCM ako súčasť procesu vytvorí tento sklad certifikátov. 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 lokálnej certifikačnej autority (CA), *SYSTEM, *OBJECTSIGNING a *SIGNATUREVERIFICATION sa musia nachádzať na špecifických cestách v integrovanom súborovom systéme, ostatné systémové sklady certifikátov sa môžu nachádzať kdekoľvek v integrovanom súborovom systéme.

Súvisiace koncepty

“Typy digitálnych certifikátov” na strane 31
Keď používate správcu digitálnych certifikátov (DCM) na riadenie vašich certifikátov, DCM ich organizuje a ukladá spolu s ich priradenými súkromnými kľúčmi do skladu certifikátov podľa typu certifikátu.

Kryptografia

Zdieľané a verejné kľúče sú dva rozdielne typy šifrovacích funkcií používaných digitálnymi certifikátmi na poskytovanie bezpečnosti.

Kryptografia je vedný odbor zaoberajúci sa zachovávaním bezpečnosti dát. Kryptografia umožňuje ukladať informácie alebo komunikovať s druhými stranami, pričom zabráni nezúčastneným stranám porozumieť uloženým informáciám alebo komunikácii. 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.

"Secure Sockets Layer"
SSL (The Secure Sockets Layer) je priemyselný štandard na šifrovanie relácie medzi klientmi a servermi.

Kryptografické koprocesory IBM pre System i

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

Použitie kryptografického koprocesora IBM pre platformu System i pridáva do vášho systému schopnosť vysoko bezpečného kryptografického spracovania. 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 certifikátu v kryptografickom koprocesore IBM" na strane 70
Ak máte vo vašom systéme nainštalovaný kryptografický koprocesor IBM, môžete ho používať na poskytnutie bezpečnejšieho úložného priestoru pre súkromný kľúč certifikátu. Koprocesor môžete použiť na uloženie súkromného kľúča pre certifikát servera, certifikát klienta alebo certifikát miestnej certifikačnej autority (CA).

Secure Sockets Layer

SSL (The Secure Sockets Layer) je priemyselný štandard na šifrovanie relácie 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
Zdieľané a verejné kľúče sú dva rozdielne typy šifrovacích funkcií používaných digitálnymi certifikátmi na poskytovanie bezpečnosti.

"Typy digitálnych certifikátov" na strane 31
Keď používate správcu digitálnych certifikátov (DCM) na riadenie vašich certifikátov, DCM ich organizuje a ukladá spolu s ich priradenými súkromnými kľúčmi do skladu certifikátov podľa typu certifikátu.

Definície aplikácií

Správca digitálnych certifikátov (DCM) umožňuje riadiť definície aplikácií, ktoré budú pracovať s konfiguráciami SSL a podpisovaním objektov.

Existujú dva typy definícií aplikácií, ktoré môžete v DCM riadiť:

- 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 System i 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

“Riadenie aplikácií v DCM” na strane 64
Správca digitálnych certifikátov (DCM) umožňuje vytvoriť definície aplikácie a riadiť priraďovanie certifikátov aplikácie. Môžete tiež definovať zoznamy dôveryhodných CA, ktoré aplikácia používa ako základ pre akceptovanie certifikátov na autentifikáciu klienta.

Súvisiace úlohy

“Vytváranie definície aplikácie” na strane 65
V správcovi digitálnych certifikátov (DCM) môžete vytvoriť a používať tieto dva typy definícií aplikácií: aplikácie klienta alebo servera používajúce SSL a definície aplikácií, ktoré používate na podpisovanie objektov.

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

"Overovanie platnosti certifikátov a aplikácií" na strane 68
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

Tieto scenáre zobrazujú typické schémy implementácie certifikátov na pomoc pri plánovaní implementácie vašich vlastných certifikátov ako súčasť vašej bezpečnostnej politiky System i. Každý scenár poskytuje tiež všetky potrebné konfiguračné úlohy, ktoré musíte vykonať, aby bol scenár splnený.

Správca digitálnych certifikátov (DCM) povoľuje používať certifikáty na zlepšenie bezpečnostnej politiky viacerými spôsobmi. Ako sa rozhodnete certifikáty používať, závisí na vašich obchodných plánoch a bezpečnostných potrebách.

Použitie digitálnych certifikátov vám môže pomôcť zvýšiť vašu bezpečnosť niekoľkými spôsobmi. Digitálne certifikáty vám umožňujú 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 System i 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: Použitie 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.

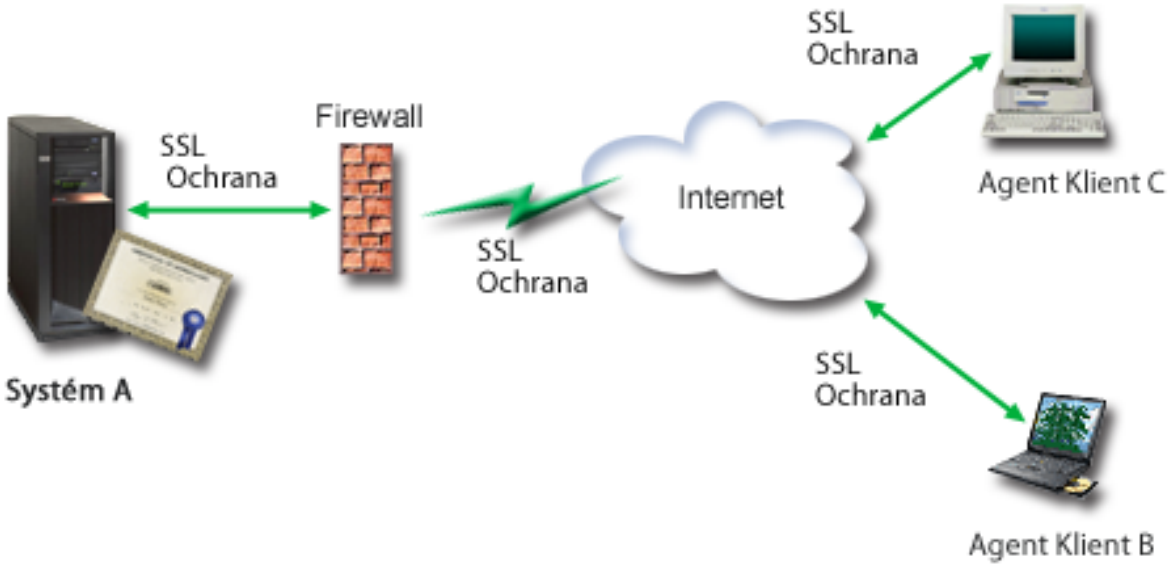
Ciele tohto scenára sú nasledovné:

- 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 - systém A

- Systém A je server, ktorý hostí aplikáciu na výpočet sadzieb spoločnosti.
- Systém A používa i5/OS verziu 5, vydanie 4 (V5R4) alebo novšie verzie.
- Systém A má nainštalovaného a nakonfigurovaného správcu digitálnych certifikátov IBM HTTP Server for i5/OS.
- System A spustí aplikáciu výpočtu sadzieb, ktorá je nakonfigurovaná tak, že:
  - Vyžaduje režim SSL.
  - Na svoju vlastnú autentifikáciu k inicializácii relácie SSL používa verejný certifikát od všeobecne známej certifikačnej autority (CA).
  - Vyžaduje autentifikáciu užívateľov užívateľským menom a heslom.
- Systém A poskytne svoj certifikát na inicializáciu relácie SSL, keď klienti B a C používajú aplikáciu na výpočet sadzieb.
- Po inicializácii relácie SSL systém A požiada klienta B a C o poskytnutie platného mena užívateľa a hesla a potom povolí prístup do aplikácie 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 používajú aplikáciu na výpočet sadzieb v systéme A, ktorý poskytne svoj certifikát softvéru ich klienta na autentifikáciu jeho identity a inicializáciu relácie SSL.
- Softvér klienta na klientoch B a C je nakonfigurovaný na akceptáciu certifikátu zo systému A za účelom inicializácie relácie SSL.
- Po začatí relácie SSL musia klienti B a C poskytnúť platné meno užívateľa a heslo a systém A potom poskytne aplikácii prístup.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:

- Aplikácia na výpočet sadzieb v systéme A je generická aplikácia, ktorú môžete nakonfigurovať na použitie SSL. Väčšina aplikácií, vrátane mnohých aplikácií System i, 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 A musí spĺňať tieto “Požiadavky nastavenia DCM” na strane 30 na inštaláciu a používanie správcu digitálnych certifikátov (DCM)
- V minulosti ešte nikto nenakonfiguroval ani nepoužíval DCM v systéme A.
- Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
- Systém A nemá nainštalovaný kryptografický koprocesor IBM.

Úlohy konfigurovania

Súvisiace úlohy

“Spúšťanie správcu digitálnych certifikátov” na strane 41
Aby ste mohli vykonávať funkcie správcu digitálnych certifikátov (DCM), musíte ho vo vašom systéme spustiť.

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
Používa váš systém i5/OS V5R4 alebo novšiu verziu?	Áno
Máte vo vašom systéme nainštalovaného správcu digitálnych certifikátov?	Áno
Je vo vašom systéme nainštalovaný IBM HTTP Server for i5/OS a spustená inštancia administračného servera?	Áno
Je vo vašom systéme nakonfigurovaný TCP, aby ste mohli na prístup k DCM používať webový prehliadač a inštanciu administračného servera HTTP ?	Áno
Máte zvláštne oprávnenia *SECADM a *ALLOBJ ?	Áno

Aby ste 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 systém A	**Odpovede**
Budete prevádzkovať vlastnú lokálnu CA alebo budete získavať certifikáty pre vaše aplikácie od verejnej CA?	Získanie certifikátu od verejnej CA
Hosťuje systém A aplikácie, ktoré chcete povoliť pre SSL?	Áno
Ktoré informácie o DN použijete pre CSR (certificate signing request), na vytvorenie ktorého používate DCM ? • **Veľkosť kľúča**: určuje silu šifrovacích kľúčov pre certifikát. • **Štítok certifikátu**: identifikuje certifikát pomocou jedinečného znakového reťazca. • **Skutočný 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

Vytváranie žiadosti o certifikát servera alebo klienta

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. Výberom **Vytvoriť nový sklad certifikátov** v navigačnom rámci DCM, spustite riadenú úlohu a vyplňte sériu formulárov. Tieto formuláre vás prevedú procesom vytvorenia skladu certifikátov a certifikátu, ktoré môžu vaše aplikácie použiť pre SSL relácie.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu stránky a dostanete sa k online pomoci.
3. Zvoľte ***SYSTEM** ako sklad certifikátov, ktorý sa má vytvoriť a kliknite na **Continue**.
4. Vyberte **Yes**, aby sa certifikát vytvoril ako časť vytvárania skladu certifikátov *SYSTEM a kliknite na **Continue**.
5. Ako podpisovateľa nového certifikátu označte **VeriSign or other Internet Certificate Authority (CA)** a kliknutím na **Continue** zobrazte formulár, ktorý vám umožní vytvoriť identifikačné údaje nového certifikátu.
6. Vyplňte formulár a kliknutím na **Continue** zobrazte potvrdzovaciu stránku. Na tejto potvrdzovacej stránke sú zobrazené údaje na žiadosť o certifikát, ktoré musíte poskytnúť 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. Starostlivo nakopírujte a vložte údaje CSR formulára žiadosti o certifikát, alebo do osobitného súboru, ktorý verejná CA pri žiadosti o certifikát požaduje. Musíte použiť všetky údaje CSR, vrátane riadkov Začiatku a Ukončenia žiadosti o nový certifikát.

   Poznámka: Keď túto stránku zavriete, údaje sa stratia a ich obnova nie je možná.
8. Keď túto stránku zavriete, údaje sa stratia a ich obnova nie je možná.
9. Kým pokročíte k ďalším krokom tohoto scenára, počkajte, kým vám CA vráti podpísaný certifikát.

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 aplikácií 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. Niektoré aplikácie, napríklad IBM HTTP Server for i5/OS, vygenerujú jedinečný ID aplikácie a zaregistrujú ho pomocou správcu digitálnych certifikátov (DCM) pri konfigurácii aplikácie na používanie SSL. Predtým, ako budete môcť použiť DCM na priradenie podpísaného certifikátu k ID aplikácie a dokončiť proces konfigurácie SSL, musíte ID aplikácie poznať.

To, ako nakonfigurujete vašu aplikáciu na používanie SSL, sa mení na základe aplikácie. Tento scenár nepredpokladá konkrétny zdroj pre aplikáciu na výpočet sadzieb, ktorú opisuje, pretože existuje veľa spôsobov, ktorými môže spoločnosť MyCo, Inc. poskytnúť túto aplikáciu svojim agentom.

Na nakonfigurovanie vašej aplikácie na používanie SSL postupujte podľa inštrukcií, ktoré poskytne dokumentácia vašej aplikácie. Keď pre vašu aplikáciu konfigurujete SSL, môžete pre túto aplikáciu nakonfigurovať podpísaný verejný certifikát, takže bude môcť iniciovať relácie SSL.

Súvisiace informácie

Bezpečnosť aplikácie so SSL

Import a priraďovanie 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. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
3. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte heslo, ktoré ste zadali pri vytváraní skladu certifikátov a kliknite na **Continue**.
4. Po obnovení navigačného rámca 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 si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu stránky a dostanete sa k 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. Označte v zozname svoju aplikáciu a kliknite na **Continue**. Zobrazí sa stránka buď so správou potvrdenia pre váš výber priradenia, alebo chybové hlásenie, ak sa vyskytol problém.

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

Spúšťanie aplikácií 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. Pozrite si dokumentáciu pre vašu aplikáciu a zistite, či musíte aplikáciu reštartovať alebo v nej vyhľadajte ďalšie konkrétne 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 dôveryhodného zoznamu CA pre aplikáciu, ktorá ho vyžaduje

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. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
3. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte heslo, ktoré ste zadali pri vytváraní skladu certifikátov a kliknite na **Continue**.
4. Po obnovení navigačného rámca vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
5. Zo zoznamu úloh vyberte **Set CA status** na zobrazenie zoznamu certifikátov CA.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu stránky a dostanete sa k 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 rozhodnite vytvoriť súkromnú lokálnu certifikačnú autoritu (CA), vydávať certifikáty všetkým zamestnancom a umožniť zamestnancom, aby priradili svoje certifikáty k svojim užívateľským profilom System i. 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 System i 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 System i. 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

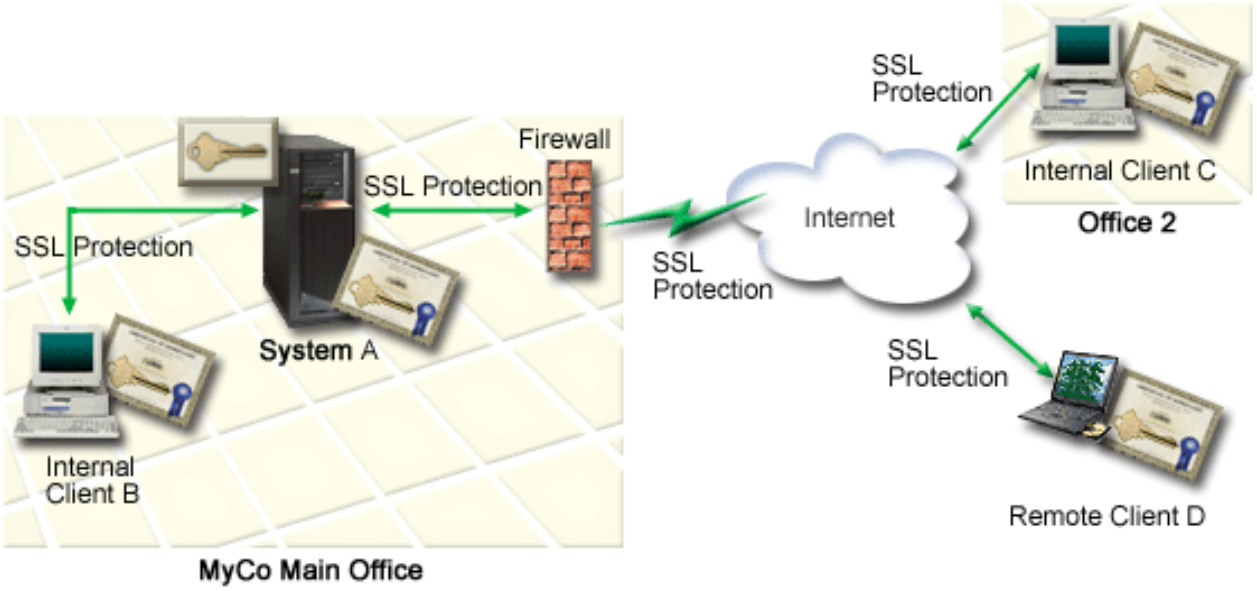
V tomto scenári chce spoločnosť MyCo, Inc. používať digitálne certifikáty na ochranu citlivých osobných informácií, ktoré poskytuje jej interná webová stránka ľudských zdrojov zamestnancom spoločnosti. Táto spoločnosť chce aj bezpečnejšiu metódu autentifikácie tých užívateľov, ktorí majú povolený prístup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

- Systém A je server, ktorý hostí aplikáciu na výpočet sadzieb spoločnosti.
- Systém A používa i5/OS verziu 5, vydanie 4 (V5R4) alebo novšie verzie.
- Systém A má nainštalovaného a nakonfigurovaného správcu digitálnych certifikátov IBM HTTP Server for i5/OS.
- Systém A spustí aplikáciu výpočtu sadzieb, ktorá je nakonfigurovaná tak, že:
  - Vyžaduje režim SSL.
  - Na svoju vlastnú autentifikáciu k inicializácii relácie SSL používa verejný certifikát od všeobecne známej certifikačnej autority (CA).
  - Vyžaduje autentifikáciu užívateľov užívateľským menom a heslom.
- Systém A poskytne svoj certifikát na inicializáciu relácie SSL, keď klienti B a C používajú aplikáciu na výpočet sadzieb.

- Po inicializácii relácie SSL systém A požiada klientov B a C o poskytnutie platného mena užívateľa a hesla a potom povolí prístup do aplikácie 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 používajú aplikáciu na výpočet sadzieb v systéme A, ktorý poskytne svoj certifikát softvéru ich klienta na autentifikáciu jeho identity a inicializáciu relácie SSL.
- Softvér klienta na klientoch B a C je nakonfigurovaný na akceptáciu certifikátu zo systému A za účelom inicializácie relácie SSL.
- Po začatí relácie SSL musia klienti B a C poskytnúť platné meno užívateľa a heslo a systém A potom poskytne aplikácii prístup.

Požiadavky a predpoklady

Tento scenár závisí na nasledovných požiadavkách a predpokladoch:

- IBM HTTP Server for i5/OS (napájaný z Apache) spúšťa na systéme A aplikáciu ľudských zdrojov. Tento scenár neobsahuje špecifické pokyny na konfiguráciu servera HTTP na používanie SSL. Tento scenár poskytuje inštrukcie pre konfiguráciu a správu certifikátov, ktoré sú potrebné pre akúkoľvek aplikáciu, aby používala SSL.
- HTTP Server poskytuje schopnosť vyžadovania certifikátov pre autentifikáciu klientov. Tento scenár obsahuje pokyny na používanie DCM na konfiguráciu požiadaviek správcu certifikátov pre tento scenár. Tento scenár však neobsahuje špecifické kroky konfigurácie pre server HTTP na konfiguráciu autentifikácie klientov pomocou certifikátov.
- Server HTTP pre ľudské zdroje v systéme A už používa autentifikáciu prostredníctvom hesla.
- Systém A spĺňa požiadavky na inštaláciu a používanie DCM.
- V minulosti ešte nikto nenakonfiguroval ani nepoužíval DCM v systéme A.
- Ktokoľvek, kto používa DCM na vykonávanie úloh v tomto scenári, musí mať mimoriadne oprávnenia *SECADM a *ALLOBJ pre svoj užívateľský profil.
- Systém 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**
Používa váš systém i5/OS V5R4 alebo novšiu verziu?	Áno
Máte vo vašom systéme nainštalovaného správcu digitálnych certifikátov?	Áno
Je vo vašom systéme nainštalovaný IBM HTTP Server for i5/OS a spustená inštancia administračného servera?	Áno
Je vo vašom systéme nakonfigurovaný TCP, aby ste mohli na prístup k DCM používať webový prehliadač a inštanciu administračného servera HTTP ?	Áno
Máte zvláštne oprávnenia *SECADM a *ALLOBJ ?	Áno

Aby ste 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 pracovný list pre systém A	**Odpovede**
Budete prevádzkovať vlastnú lokálnu CA alebo budete získavať certifikáty pre vaše aplikácie od verejnej CA?	Vytvorenie lokálnej CA na vydávanie certifikátov
Hosťuje systém A aplikácie, ktoré chcete povoliť pre SSL?	Áno
Aké informácie charakteristického názvu budete používať pre lokálnu CA? • **Key size**: 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 mohla vydávať užívateľské certifikáty na autentifikáciu klienta?	Áno
Aké informácie charakteristického názvu budete používať pre certifikát servera vydaného lokálnou 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

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

Plánovací pracovný list pre systém A	Odpovede
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 HTTP servera ľudských zdrojov na používanie SSL

Konfigurácia SSL (Secure Sockets Layer) pre HTTP server ľudských zdrojov (napájaný pomocou Apache) v systéme A zahŕňa množstvo úloh, ktoré sa líšia v závislosti od toho, ako je váš server aktuálne nakonfigurovaný.

Ak chcete server nakonfigurovať na používanie SSL, postupujte takto:

1. Spustite administračné rozhranie servera HTTP.
2. Ak chcete pracovať so špecifickým HTTP serverom, vyberte tieto karty **Manage → All Servers → All HTTP Servers** pre zobrazenie zoznamu všetkých nakonfigurovaných HTTP serverov.
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.

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

Súvisiace informácie

IBM HTTP Server for i5/OS

Vytváranie a prevádzka 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. Podľa cieľov tohto scenára ste si vybrali vytvorenie a prevádzku lokálnej certifikačnej autority (CA) na vydávanie certifikátov pre server.

Keď používate správcu digitálnych certifikátov (DCM) na vytvorenie lokálnej CA, pomocou sprievodcu sa oboznámite s procesom, ktorý zabezpečí, že nakonfigurujete všetko potrebné na povolenie SSL pre vašu aplikáciu. Tento proces zahŕňa priradenie certifikátu vydaného lokálnou CA k vašej aplikácii webového servera. Pridáte tiež lokálnu CA do dôveryhodného zoznamu CA aplikácie webového servera. Ak máte lokálnu CA v dôveryhodnom zozname CA aplikácie, je tým zabezpečené, že aplikácia môže rozpoznať a autentifikovať užívateľov poskytujúcich certifikáty vydávané lokálnou CA.

Ak chcete používať správcu digitálnych certifikátov (DCM) na vytvorenie a prevádzku lokálnej CA a vydať certifikát vašej serverovej aplikácii ľudských zdrojov, vykonajte tieto kroky:

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnej časti DCM vyberte **Create a Certificate Authority**, aby sa zobrazila séria formulárov. Tieto formuláre vás oboznámia s procesom vytvárania lokálnej CA a vykonaním ostatných úloh potrebných na začatie používania digitálnych certifikátov pre SSL, na podpisovanie objektov a overovanie platnosti podpisov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu stránky a dostanete sa k online pomoci.

3. Vyplňte formuláre pre túto riadenú úlohu. Pri používaní týchto formulárov na vykonanie všetkých úloh potrebných na nastavenie funkčnej lokálnej certifikačnej autority postupujte nasledovne:
   a. Poskytnite identifikačné informácie pre lokálnu CA.
   b. Nainštalujte certifikát lokálnej CA na váš PC alebo do prehliadača, aby váš softvér mohol rozpoznať lokálnu CA a overiť platnosť certifikátov, ktoré táto lokálna CA vydáva.
   c. Vyberte údaje politiky pre vašu lokálnu CA.

      Poznámka: Skontrolujte, či ste vybrali, aby mohla lokálna CA vydávať užívateľské certifikáty.
   d. Použite novú lokálnu CA na vydanie certifikátu servera alebo klienta, ktorý môžu vaše aplikácie používať 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 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 podpisujúce objekty, vykonajte 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: Skontrolujte, či ste vybrali ID aplikácie pre váš HTTP server ľudských zdrojov, napríklad QIBM_HTTP_SERVER_MYCOTEST, ako jednu z aplikácií, ktorá dôveruje 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 klienta pre webový server ľudských zdrojov

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

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

1. Spustite administračné rozhranie servera HTTP.
2. Otvorte webový prehliadač a zadajte adresu http://your_system_name:2001 na zavedenie úvodnej stránky IBM Systems Director Navigator for i5/OS.
3. Z úvodnej stránky kliknite na odkaz **i5/OS Tasks Page**.
4. Vyberte **IBM Web Administration for i5/OS**.
5. Ak chcete pracovať so špecifickým HTTP serverom, vyberte tieto karty **Manage → All Servers → All HTTP Servers** pre zobrazenie zoznamu všetkých nakonfigurovaných HTTP serverov.
6. Zo zoznamu vyberte príslušný server a kliknite na **Manage Details**.
7. V navigačnom rámci vyberte **Security**.
8. Vo formulári vyberte záložku **Authentication**.
9. Vyberte voľbu **Použiť profil i5/OS klienta**.
10. V poli **Authentication name or realm** uveďte názov pre oblasť autorizácie.
11. V poli **Process requests using client's authority** vyberte hodnotu Enabled a kliknite na **Apply**.
12. Vo formulári vyberte záložku **Control Access**.
13. Vyberte **All authenticated users (valid user name and password)** a kliknite na **Apply**.
14. Vo formulári vyberte záložku **SSL with Certificate Authentication**.

15. Skontrolujte, že je v poli **SSL** vybratá hodnota Povolené.
16. Zabezpečte, aby v poli **Server certificate application name** bola špecifikovaná správna hodnota, napríklad QIBM_HTTP_SERVER_MYCOTEST.
17. Vyberte **Accept client certificate if available before making connection**. Kliknite na **OK**.

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

Súvisiace informácie

IBM HTTP Server for i5/OS

Spúšťanie webového servera ľudských zdrojov v režime SSL

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

Ak chcete zastaviť a spustiť server HTTP (založený na Apache), postupujte nasledovne:

1. V System i Navigator rozviňte **system → Network → Servers → TCP/IP → HTTP Administration**
2. Kliknite na **Start**, čím spustíte administračné rozhranie servera HTTP.
3. Ak chcete zobraziť zoznam všetkých nakonfigurovaných serverov HTTP, kliknite na záložku **Manage**.
4. Zo zoznamu vyberte príslušný server a ak tento server beží, kliknite na **Stop**.
5. Ak chcete tento server znova spustiť, kliknite na **Start**. Viac informácií o parametroch spustenia získate v online pomoci.

Užívatelia musia najprv nainštalovať kópiu certifikátu lokálnej CA do softvéru svojho prehliadača a potom môžu vstupovať do webovej aplikácie ľudských zdrojov.

Súvisiace informácie

Prehľad Informačného centra pre HTTP

Inštalácia kópie certifikátu lokálnej CA do prehliadača

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

Všetci užívatelia (klienti B, C a D), ktorí chcú získať kópiu certifikátu lokálnej CA, musia vykonať tieto kroky:

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnom rámci vyberte **Install local CA Certificate on Your PC** na zobrazenie stránky, ktorá umožňuje stiahnutie certifikátu lokálnej CA do vášho prehliadača alebo jeho uloženie do súboru vo vašom systéme.
3. Vyberte voľbu na inštaláciu certifikátu. Táto voľba stiahne certifikát lokálnej CA do vášho prehliadača ako dôveryhodný koreň. 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. Následne musia získať užívateľský certifikát od lokálnej CA.

Vyžadovanie certifikátu od lokálnej CA

V predchádzajúcich krokoch ste webový server ľudských zdrojov nakonfigurovali tak, aby na autentifikáciu užívateľov vyžadoval certifikáty. Pred povolením prístupu k webovému serveru musia teraz užívatelia poskytnúť platný certifikát od lokálnej CA. Každý užívateľ musí použiť Správcu digitálnych certifikátov (DCM) na získanie certifikátu prostredníctvom úlohy **Create Certificate**. Aby ste mohli získať certifikát od lokálnej CA, politika lokálnej CA musí umožňovať, aby CA vydávala užívateľské certifikáty.

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

1. Spustite DCM. Pozrite si kapitolu Spúšťanie 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 si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu stránky a dostanete sa k 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 System i.

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.

Scenár: Nastavenie certifikačnej autority pomocou správcu digitálnych certifikátov

Pred nastavením certifikačnej autority (CA) musí administrátor pobočky zabezpečiť splnenie niekoľkých úloh plánovania. Pred vykonaním týchto úloh skontrolujte, či sú všetky nevyhnutné podmienky tohto scenára splnené.

Vyplnenie plánovacích pracovných listov pre správcu digitálnych certifikátov

Spoločnosť MyCo, Inc. vyplní plánovacie pracovné listy na pomoc pri nastavovaní digitálnych certifikátov, ktoré sa majú vydávať jej obchodným partnerom.

Tabuľka 5. Plánovacie pracovné listy na vytvorenie certifikačnej autority (CA) pomocou správcu digitálnych certifikátov (DCM)

Otázky	**Odpovede**
Aká veľkosť klúčov bude použitá na generovanie verejných a súkromných kľúčov pre certifikát?	1024
Aké je heslo skladu certifikátov?	secret **Dôležité:** Všetky heslá použité v tomto scenári slúžia len ako príklad. Nepoužívajte ich v žiadnej skutočnej konfigurácii.
Aký je názov certifikačnej autority?	mycoca
Aký je názov vašej organizácie?	myco

Tabuľka 5. Plánovacie pracovné listy na vytvorenie certifikačnej autority (CA) pomocou správcu digitálnych certifikátov (DCM) (pokračovanie)

Otázky	Odpovede
Koľko dní má byť certifikačná autorita v platnosti?	1095 (3 roky)
Aký prehliadač používate?	Windows Internet Explorer verziu 6.0
Budete vydávať certifikáty užívateľom v sieti?	Nie

Tabuľka 6. Plánovací pracovný list digitálneho certifikátu pre systém A

Otázky	Odpovede
Aká veľkosť klúčov bude použitá na generovanie verejných a súkromných kľúčov pre certifikát?	1024
Aké je heslo skladu certifikátov?	secret **Dôležité:** Všetky heslá použité v tomto scenári slúžia len ako príklad. Nepoužívajte ich v žiadnej skutočnej konfigurácii.
Aký je názov návestia certifikátu?	mycocert
Aké je skutočný názov vášho certifikátu?	mycocert
Aký je názov vašej organizácie?	MyCo, Inc
Aká je IP adresa vášho systému?	192.168.1.2 (2001:DB8::2 v IPv6) **Dôležité:** IP adresy použité v tomto scenári slúžia len ako príklad. Tieto IP adresy neodrážajú schému IP adresovania a nemali by byť použité v žiadnej skutočnej konfigurácii. Pri vykonávaní týchto úloh použite svoje vlastné IP adresy.
Aký je úplný názov hostiteľa vášho systému?	systema.myco.min.com

Tabuľka 7. Plánovací pracovný list pre digitálne certifikáty pre systém B

Otázky	Odpovede
Aká veľkosť klúčov bude použitá na generovanie verejných a súkromných kľúčov pre certifikát?	1024
Aký je názov návestia certifikátu?	corporatecert
Aké je skutočný názov vášho certifikátu?	corporatecert
Aká je cesta a názov súboru skladu certifikátov?	/tmp/systemb.kdb
Aké je heslo skladu certifikátov?	secret2 **Dôležité:** Všetky heslá použité v tomto scenári slúžia len ako príklad. Nepoužívajte ich v žiadnej skutočnej konfigurácii.
Aký je skutočný názov digitálneho certifikátu?	corporatecert
Aký je názov organizácie, ktorá vlastní tento certifikát?	MyCo, Inc

Tabuľka 7. Plánovací pracovný list pre digitálne certifikáty pre systém B (pokračovanie)

Otázky	Odpovede
Aká je IP adresa vášho systému?	172.16.1.3 (2002:DD8::3 v IPv6) **Dôležité:** IP adresy použité v tomto scenári slúžia len ako príklad. Tieto IP adresy neodrážajú schému IP adresovania a nemali by byť použité v žiadnej skutočnej konfigurácii. Pri vykonávaní týchto úloh použite svoje vlastné IP adresy.
Aký je úplný názov hostiteľa vášho systému?	systemb.myco.wis.com

Spúšťanie IBM HTTP Server for i5/OS v systéme A

Na spustenie IBM HTTP Server for i5/OS v systéme A použite túto procedúru.

Pre prístup na rozhranie správcu digitálnych certifikátov (DCM) musíte spustiť administratívnu inštanciu servera HTTP vykonaním nasledujúcich úloh.

1. Zo systému A sa prihláste na znakové rozhranie.
2. Do príkazového riadka napíšte strtcpsvr server(*HTTP) httpsvr(*admin). Tento príkaz spustí administračný systém servera HTTP.

Konfigurácia systému A ako certifikačnej autority

Na konfiguráciu systému A ako certifikačnej autority (CA) použite tento postup:

1. Otvorte webový prehliadač a zadajte adresu http://your_system_name:2001 na zavedenie úvodnej stránky IBM Systems Director Navigator for i5/OS.
2. Prihláste sa s menom a heslom užívateľského profilu systému A.
3. Z úvodnej stránky kliknite na odkaz **i5/OS Tasks Page**.
4. Vyberte **Digital Certificate Manager**.
5. Z ľavého navigačného podokna vyberte **Create a Certificate Authority (CA)**.
6. Na stránke vytvorenia certifikačnej autority (CA) zadajte do povinných polí informácie z pracovného listu plánovania DCM:
   - **Veľkosť kľúča:** 1024
   - **Heslo skladu certifikátov:** secret
   - **Potvrdiť heslo:** secret

     Dôležité: Všetky heslá použité v tomto scenári slúžia len ako príklad. Nepoužívajte ich v žiadnej skutočnej konfigurácii.
   - **Názov certifikačnej autority:** mycoca
   - **Názov organizácie:** MyCo, Inc
   - **Štát alebo provincia:** min
   - **Krajina alebo región:** us
   - **Doba platnosti certifikačnej autority (2-7300):** 1095
7. Kliknite na **Continue**.
8. Na stránke **Install Local CA certificate** kliknite na **Continue**.
9. Na stránke **Certificate Authority (CA) Policy Data** vyberte tieto voľby:
   - **Allow creation of user certificates:** Yes
   - **Validity period of certificates that are issued by this Certificate Authority (1-2000):** 365

10. Na stránke akceptovania údajov politiky si prečítajte zobrazené správy a kliknutím na **Continue** vytvorte predvolený sklad certifikátov servera (*SYSTEM) a certifikát servera podpísaný vašou CA. Prečítajte si potvrdzovaciu správu a kliknite na **Continue**.
11. Na stránke vytvorenia certifikátu servera alebo klienta zadajte tieto informácie:
    - **Veľkosť kľúča:** 1024
    - **Návestie certifikátu:** mycocert
    - **Heslo skladu certifikátov:** secret
    - **Potvrdiť heslo:** secret

      Dôležité: Všetky heslá použité v tomto scenári slúžia len ako príklad. Nepoužívajte ich v žiadnej skutočnej konfigurácii.
    - **Skutočný názov:** mycocert
    - **Názov organizácie:** myco
    - **Štát alebo provincia:** min
    - **Krajina alebo región:** us
    - **IP adresa verzia 4:** 192.168.1.2
    - **IP adresa verzia 6:** 2001:DB8::3

      Poznámka: IP adresy použité v tomto scenári slúžia len ako príklad. Tieto IP adresy neodrážajú schému IP adresovania a nemali by byť použité v žiadnej skutočnej konfigurácii. Pri vykonávaní týchto úloh použite svoje vlastné IP adresy.
    - **Úplný názov domény:** systema.myco.min.com
    - **E-mailová adresa:** administrator@myco.min.com
12. Kliknite na **Continue**.
13. Na stránke výberu aplikácie kliknite na **Continue**.

    Tip: Sprievodca novým pripojením VPN automaticky priradí práve vytvorený certifikát aplikácii manažéra kľúčov VPN i5/OS. Ak máte iné aplikácie, ktoré by mohli tento certifikát používať, môžete ich vybrať na tejto stránke. Keďže tento scenár používa len certifikáty pre pripojenia VPN, nemusíte vyberať žiadne ďalšie aplikácie.
14. Na stránke stavu aplikácie si prečítajte zobrazené správy a kliknite na **Cancel**. Vytvorené zmeny budú akceptované.

    Poznámka: Ak chcete vytvoriť sklad certifikátov, ktorý má obsahovať certifikáty používané na podpisovanie objektov, vyberte **Continue**.
15. Po obnove rozhrania DCM vyberte **Select a Certificate Store**.
16. Na stránke výberu skladu certifikátov vyberte ***SYSTEM**. Kliknite na **Continue**.
17. Na stránke skladu certifikátov a hesla zadajte secret. Kliknite na **Continue**.
18. V ľavom navigačnom rámci vyberte **Manage Applications**.
19. Na stránke riadenia aplikácií vyberte **Define CA trust list**. Kliknite na **Continue**.
20. Na stránke definovania dôveryhodného zoznamu CA vyberte **Server**. Kliknite na **Continue**.
21. Vyberte **i5/OS VPN Key Manager**. Kliknite na **Define CA Trust List**.
22. Na stránke definovania dôveryhodného zoznamu CA vyberte **LOCAL_CERTIFICATE_AUTHORITY**. Kliknite na **OK**.

Vytvorenie digitálneho certifikátu pre systém B

Na vytvorenie digitálneho certifikátu pre systém B použite tento postup:

1. V ľavom navigačnom okne kliknite na **Create Certificate** a vyberte **Server or client certificate for another System i**.
2. Kliknite na **Continue**.

3. Na stránke vytvorenia certifikátu servera alebo klienta pre ďalší System i vyberte **V5R3**. Ide o úroveň vydania pre systém B. Kliknite na **Continue**.
4. Na stránke vytvorenia certifikátu servera alebo klienta zadajte tieto informácie:
   - **Veľkosť kľúča:** 1024
   - **Návestie certifikátu:** corporatecert
   - **Cesta a názov súboru skladu certifikátov:** /tmp/systemb.kdb
   - **Heslo skladu certifikátov:** secret2
   - **Potvrdiť heslo:** secret2

     Poznámka: Všetky heslá použité v tomto scenári slúžia len ako príklad. Nepoužívajte ich v žiadnej skutočnej konfigurácii.
   - **Všeobecný názov:** corporatecert
   - **Názov organizácie:** MyCo, Inc
   - **Štát alebo provincia:** wis
   - **Krajina alebo región:** us
   - **IP adresa verzia 4:** 172.16.1.3
   - **IP adresa verzia 6:** 2002:DD8::3

     Dôležité: IP adresy použité v tomto scenári slúžia len ako príklad. Tieto IP adresy neodrážajú schému IP adresovania a nemali by byť použité v žiadnej skutočnej konfigurácii. Pri vykonávaní týchto úloh použite svoje vlastné IP adresy.
   - **Úplný názov hostiteľa:** systemb.myco.wis.com
   - **E-mailová adresa:** administrator@myco.wis.com
5. Kliknite na **Continue**. Dostanete potvrdzovaciu správu, ktorá overí, že certifikát servera bol vytvorený v systéme A pre systém B. Ako správca siete pobočky zašlete tieto súbory podnikovému správcovi siete prostredníctvom zašifrovanej elektronickej pošty. Podnikový správca siete musí teraz presunúť a premenovať súbor skladu certifikátov (.KDB) a súbor požiadaviek (.RDB) do systému B. Ďalej bude musieť presunúť tieto súbory do adresára /QIBM/USERDATA/ICSS/CERT/SERVER v integrovanom súborovom systéme pomocou binárneho FTP. Po vykonaní tejto úlohy musí premenovať uvedené súbory v príslušnom adresári.

Premenovanie súborov .KDB a .RDB v systéme B

Na premenovanie súborov .KDB a .RDB v systéme B použite túto procedúru.

Keďže sa v systéme B nenachádza sklad certifikátov *SYSTEM, správca podnikovej siete musí premenovať súbory systemb.kdb a systemb.RDB na DEFAULT.KDB a DEFAULT.RDB s použitím týchto prenesených súborov ako skladu certifikátov *SYSTEM v systéme B.

1. V System i Navigator rozviňte **System B → File Systems → Integrated File System → Qibm → UserData → ICSS → Cert → Server** a skontrolujte, či sú súbory systemb.kdb a systemb.RDB vypísané v zozname tohto adresára.
2. Do príkazového riadka napíšte wrklnk ('/qibm/userdata/icss/cert/server').
3. Na stránke práce s objektmi odkazov, vyberte voľbu 7 (Rename) na premenovanie súboru systemb.kdb. Stlačte kláves Enter.
4. Na stránke premenovania objektu zadajte DEFAULT.KDB v poli **New Object**. Stlačte kláves Enter.
5. Na premenovanie súboru systemb.RDB na DEFAULT.RDB zopakujte kroky 3 a 4.
6. Skontrolujte, či sa tieto súbory zmenili obnovením System i Navigator a rozvinutím ***System B*** **→ File Systems → Integrated File System → Qibm → UserData → ICSS → Cert → Server**. Súbory DEFAULT.KDB a DEFAULT.RDB musia byť vypísané v adresári.

Zmena hesla skladu certifikátov v systéme B

Na zmenu hesla skladu certifikátov v systéme B použite túto procedúru.

Správca podnikovej siete musí zmeniť heslo pre nový sklad certifikátov *SYSTEM vytvorený zároveň so súbormi DEFAULT.KDB a DEFAULT.RDB.

Poznámka: Musíte zmeniť heslo skladu certifikátov *SYSTEM. Po zmene je heslo uložené tak, aby ho mohla aplikácia automaticky obnoviť, otvoriť sklad certifikátov a dostať sa k certifikátom.

1. Otvorte webový prehliadač a zadajte adresu http://your_system_name:2001 na zavedenie úvodnej stránky IBM Systems Director Navigator for i5/OS.
2. Z úvodnej stránky kliknite na odkaz **i5/OS Tasks Page**.
3. Vyberte **Digital Certificate Manager**.
4. V ľavom navigačnom podokne kliknite na **Select a Certificate Store**
5. Vyberte ***SYSTEM Certificate Store** a zadajte secret2 pre heslo. Ide o heslo, ktoré zadal správca pobočky pri vytváraní certifikátu servera pre systém B. Kliknite na **Continue**.
6. V ľavom navigačnom rámci vyberte **Manage Certificate Store**, potom vyberte **Change Password** a kliknite na **Continue**.
7. Na stránke zmeny hesla pre sklad certifikátov zadajte corporatepwd do polí **New password** a **Confirm password**.
8. Vyberte **Password does not expire** pre politiku uplynutia platnosti. Kliknite na **Continue**. Zavedie sa potvrdzovacia stránka. Kliknite na **OK**.
9. Na potvrdzovacej stránke zmeny hesla skladu certifikátov si prečítajte správu na obrazovke a kliknite na **OK**.
10. Na stránke zmeny hesla skladu certifikátov, ktorá sa znovu zavedie, zadajte coporatepwd do poľa **Certificate Store Password**. Kliknite na **Continue**.

Definovanie dôveryhodnej CA pre správcu kľúčov i5/OS VPN v systéme B

Na zadefinovanie dôveryhodnej CA pre správcu kľúčov VPN v systéme B použite túto procedúru.

1. V ľavom navigačnom rámci vyberte **Manage Applications**.
2. Na stránke riadenia aplikácií vyberte **Define CA trust list**. Kliknite na **Continue**.
3. Na stránke definovania dôveryhodného zoznamu CA vyberte **Server**. Kliknite na **Continue**.
4. Vyberte **i5/OS VPN Key Manager**. Kliknite na **Define CA Trust List**.
5. Na stránke definovania dôveryhodného zoznamu CA vyberte **LOCAL_CERTIFICATE_AUTHORITY**. Kliknite na **OK**.

Teraz môžu správcovia pobočky a podniku začať s konfiguráciou VPN.

Plánovanie pre DCM

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

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

Požiadavky nastavenia DCM

Ak chcete, aby správca digitálnych certifikátov (DCM) fungoval správne, musíte mať nainštalované určité produkty a nakonfigurovanú aplikáciu.

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

- Nainštalujte správcu digitálnych certifikátov. Toto je DCM, založený na prehliadači.
- Nainštalujte IBM HTTP Server for i5/OS a spustite inštanciu administratívneho servera.
- Presvedčte sa, či je vo vašom systéme nakonfigurovaný TCP, aby ste mohli na prístup k DCM používať webový prehliadač a inštanciu administračného servera HTTP.

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

Úvahy o zálohovaní a obnove údajov DCM

Zašifrované heslá databázy kľúčov používané na prístup do skladov certifikátov v správcovi digitálnych certifikátov (DCM) sú uložené alebo uschované v špeciálnom súbore bezpečnosti vo vašom systéme. 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.

Jednou z uvedených okolností je, keď používate DCM na vytvorenie certifikátu pre ďalší model System i a rozhodnete sa použiť súbory certifikátov v cieľovom systéme na vytvorenie nového skladu certifikátov. V tomto prípade musíte otvoriť novo vytvorený sklad certifikátov a pomocou úlohy **Change password** 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**.

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

"Používanie lokálnej CA na vydávanie certifikátov pre ostatné modely System i" na strane 57
Pomocou správcu digitálnych certifikátov (DCM) môžete nakonfigurovať súkromnú lokálnu CA na jednom systéme, aby vydávala certifikáty na používanie na iných platformáchSystem i.

Typy digitálnych certifikátov

Keď používate správcu digitálnych certifikátov (DCM) na riadenie vašich certifikátov, DCM ich organizuje a ukladá spolu s ich priradenými súkromnými kľúčmi do skladu certifikátov podľa typu certifikátu.

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 vytvorená a prevádzkovaná 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 System i. Pomocou DCM môžete k užívateľskému profilu System i priradiť tiež užívateľské certifikáty, ktoré vydajú iné certifikačné autority.

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

“Secure Sockets Layer” na strane 9
SSL (The Secure Sockets Layer) je priemyselný štandard na šifrovanie relácie 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

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).
- Prevádzka vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vašich užívateľov a aplikácie.
- Použitie kombinácie certifikátov z 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. Aj iné spoločnosti a užívatelia môžu uznávať a dôverovať certifikátom vydaným známou verejnou CA viac, než certifikátom vydaným vašou súkromnou lokálnou CA.

Použitie súkromných certifikátov

Ak vytvárate svoju vlastnú lokálnu CA, môžete vydávať certifikáty pre systémy a užívateľov v obmedzenejšom rozsahu, napríklad vo svojej firme alebo organizácii. Vytvorenie a údržba vlastnej lokálnej CA umožňuje vydávať certifikáty len pre užívateľov, ktorí sú dôveryhodnými členmi vašej skupiny. Poskytuje to lepšiu bezpečnosť, pretože môžete prísnejšie riadiť, kto má certifikáty a kto má prístup k vašim prostriedkom. Možnou nevýhodou údržby vlastnej lokálnej CA je čas a prostriedky, ktoré musíte investovať. Správca digitálnych certifikátov (DCM) však tento proces uľahčuje.

Keď používate lokálnu CA na vydávanie certifikátov užívateľom na autentifikáciu klienta, musíte sa rozhodnúť, kde chcete užívateľské certifikáty uložiť. Keď užívatelia získajú svoje certifikáty z lokálnej CA prostredníctvom DCM, ich certifikáty budú štandardne uložené 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 v žiadnom prípade nechcete užívateľské certifikáty priraďovať ani ukladať s užívateľským profilom, môžete použiť rozhrania API na programové vydávanie certifikátov užívateľom s výnimkou užívateľov System i.

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:

- Vytvorenie a prevádzka súkromných CA opisuje úlohy, ktoré musíte vykonať, ak sa rozhodnete prevádzkovať lokálnu CA na vydávanie súkromných certifikátov.
- Téma Manažovanie certifikátov od verejného internetového CA opisuje úlohy, ktoré musíte vykonať, ak chcete používať všeobecne známe verejné CA, vrátane CA PKIX.
- Použitie lokálnej CA na iných modeloch System i opisuje úlohy, ktoré musíte vykonať, ak chcete používať certifikáty zo súkromnej lokálnej CA na viacerých systémoch.

Súvisiace koncepty

“Riadenie certifikátov z verejnej internetovej CA” na strane 49
Keď používate správcu digitálnych certifikátov (DCM) na riadenie certifikátov z verejnej internetovej CA, musíte najprv vytvoriť sklad certifikátov. Sklad certifikátov je špeciálny databázový súbor kľúčov, ktorý používa DCM na ukladanie digitálnych certifikátov a s nimi spojených súkromných kľúčov.

“Verejné certifikáty verzus súkromné certifikáty” na strane 33
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.

“Úvodné nastavenie certifikátov” na strane 41
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.

“Digitálne certifikáty na podpisovanie objektov” na strane 38
i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod.

Súvisiace úlohy

“Digitálne certifikáty a mapovanie podnikovej identity (Enterprise Identity Mapping)” na strane 36
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.

“Vytváranie užívateľského certifikátu” na strane 44
Ak chcete použiť digitálne certifikáty na autentifikáciu užívateľa, užívatelia musia mať certifikáty. Ak na prevádzku súkromnej lokálnej certifikačnej autority (CA) používate správcu digitálnych certifikátov (DCM), môžete na vydávanie certifikátov každému užívateľovi používať lokálnu CA.

“Vytváranie a prevádzka lokálnej CA” na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

“Používanie lokálnej CA na vydávanie certifikátov pre ostatné modely System i” na strane 57
Pomocou správcu digitálnych certifikátov (DCM) môžete nakonfigurovať súkromnú lokálnu CA na jednom systéme, aby vydávala certifikáty na používanie na iných platformáchSystem i.

Súvisiaci odkaz

“Používanie API na programové vydávanie certifikátov užívateľom s výnimkou užívateľov System i” na strane 48
Lokálna CA môže užívateľom vydávať súkromné certifikáty bez priraďovania týchto certifikátov k užívateľským profilom System i.

Digitálne certifikáty pre bezpečnú SSL komunikáciu

Ak chcete vytvoriť SSL reláciu, váš server vždy predloží svoj certifikát na validáciu klientovi, ktorý požaduje spojenie.

Použitie pripojenia SSL presvedčí klienta alebo koncového užívateľa o autentickosti vašej lokality, poskytne reláciu zašifrovanej komunikácie a zabezpečí, že údaje prechádzajúce pripojením, zostanú súkromné.

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”
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.

Digitálne certifikáty na autentifikáciu užívateľov

Používatelia získavajú tradične prístup na prostriedky z aplikácie alebo systému podľa ich užívateľského mena a hesla. Systémovú bezpečnosť môžete ďalej rozšíriť pomocou digitálnych certifikátov (namiesto užívateľských mien a hesiel) na autentifikáciu a autorizáciu relácií medzi mnohými aplikáciami servera a užívateľmi.

Môžete použiť správcu digitálnych certifikátov (DCM) na priradenie užívateľovho certifikátu k užívateľskému profilu užívateľského System i alebo inej užívateľskej identite. Tento certifikát má teda rovnaké oprávnenia a povolenia ako priradená užívateľská identita alebo užívateľský profil. Alternatívne môžete použiť rozhrania API na programové použitie súkromnej lokálnej certifikačnej autority (CA) na vydanie certifikátov užívateľom s výnimkou užívateľov System i. Tieto API poskytujú schopnosť vydávať súkromné certifikáty užívateľom, keď nechcete, aby títo užívatelia mali užívateľský profil System i alebo inú internú užívateľskú identitu.

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

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. Nasledujú aplikácie System i, ktoré v súčasnosti poskytujú podporu certifikátov na autentifikáciu klientov:

- Telnet server
- IBM HTTP Server for i5/OS (založený na Apache)
- IBM Tivoli Directory Server for i5/OS
- System i Access for Windows (vrátane Navigátora System i Navigator)
- FTP server

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

Certifikáty môžu poskytovať silnejší spôsob autentifikovania užívateľov z niekoľkých dôvodov:

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

Súvisiace koncepty

"Digitálne certifikáty pre bezpečnú SSL komunikáciu" na strane 35
Ak chcete vytvoriť SSL reláciu, váš server vždy predloží svoj certifikát na validáciu klientovi, ktorý požaduje spojenie.

Súvisiaci odkaz

"Používanie API na programové vydávanie certifikátov užívateľom s výnimkou užívateľov System i" na strane 48
Lokálna CA môže užívateľom vydávať súkromné certifikáty bez priraďovania týchto certifikátov k užívateľským profilom System i.

Digitálne certifikáty a mapovanie podnikovej identity (Enterprise Identity Mapping)

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 umožňuje riadiť užívateľské identity vo vašom podniku vrátane užívateľských profilov a užívateľských certifikátov. Najbežnejšou formou užívateľskej identity je meno užívateľa a heslo; inou formou užívateľskej identity sú certifikáty. Niektoré aplikácie sú nakonfigurované tak, aby užívatelia mohli byť autentifikovaní prostredníctvom užívateľského certifikátu a nie prostredníctvom mena užívateľa a hesla.

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

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

1. Pomocou sprievodcu **EIM Configuration** v navigátore **System i Navigator** 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 **EIM Configuration**.

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 33
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.

Súvisiace úlohy

"Riadenie užívateľských certifikátov podľa dátumu ukončenia platnosti" na strane 47
Správca digitálnych certifikátov (DCM) poskytuje podporu riadenia uplynutia platnosti certifikátov s cieľom umožniť administrátorom kontrolovať dátumy uplynutia platnosti užívateľských certifikátov na lokálnom modeli System i. Podpora riadenia uplynutia platnosti užívateľských certifikátov pomocou DCM sa môže použiť v spojení s mapovaním podnikovej identity (EIM) s cieľom umožniť administrátorom používať DCM na kontrolu uplynutia platnosti užívateľských certifikátov na podnikovej úrovni.

"Riadenie umiestnenia LDAP pre užívateľské certifikáty" na strane 72
Správcu digitálnych certifikátov (DCM) môžete použiť na ukladanie užívateľských certifikátov do umiestnenia adresára servera LDAP (Lightweight Directory Access Protocol) s cieľom rozšíriť mapovanie podnikovej identity (EIM) na prácu s užívateľskými certifikátmi.

Súvisiace informácie

Téma Informačného centra pre EIM

Digitálne certifikáty pre pripojenia VPN

Digitálne certifikáty môžete použiť ako prostriedok na vytvorenie pripojenia VPN v System i. 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 v DCM používate lokálnu CA na vydávanie certifikátu, môžete pre certifikát zadať alternatívne informácie o názve subjektu. Zadaním týchto informácií sa uistíte, že vaše spojenie VPN je kompatibilné s ostatnými implementáciami VPN, ktoré ich môžu vyžadovať pre autentifikáciu.

Súvisiace koncepty

“Riadenie certifikátov z verejnej internetovej CA” na strane 49
Keď používate správcu digitálnych certifikátov (DCM) na riadenie certifikátov z verejnej internetovej CA, musíte najprv vytvoriť sklad certifikátov. Sklad certifikátov je špeciálny databázový súbor kľúčov, ktorý používa DCM na ukladanie digitálnych certifikátov a s nimi spojených súkromných kľúčov.

Súvisiace úlohy

“Vytváranie a prevádzka lokálnej CA” na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

“Definovanie zoznamu dôveryhodných CA pre aplikáciu” na strane 66
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.

Súvisiace informácie

Konfigurácia pripojenia VPN

Digitálne certifikáty na podpisovanie objektov

i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod.

Podpora podpisovania objektov rozširuje tradičné nástroje modelu System i s cieľom riadiť osoby, ktoré môžu meniť objekty. Tradičné ovládacie prvky nemôžu ochrániť objekt pred neoprávneným zásahom počas presunu objektu cez internet či inú nedôveryhodnú sieť alebo, keď je objekt uložený v inom systéme s výnimkou platformy System i. 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 vo vašej organizácii, možno uprednostníte používanie správcu digitálnych certifikátov (DCM) na prevádzku vlastnej lokálnej CA vydávajúcej certifikáty na podpisovanie objektov. Používanie súkromných certifikátov z lokálnej CA na podpisovanie objektov je lacnejšie ako nákup 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 33
Môžete používať certifikáty od verejnej CA alebo si na vydávanie certifikátov môžete vytvoriť a prevádzkovať vlastnú CA. Ako sa rozhodnete získavať certifikáty záleží na tom, ako ich chcete používať.

“Digitálne certifikáty pre overovanie podpisov objektov”
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.

Súvisiace úlohy

“Overovanie platnosti podpisov objektov” na strane 75
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.

“Riadenie verejných internetových certifikátov na podpisovanie objektov” na strane 52
Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov na digitálne podpisovanie objektov.

“Riadenie certifikátov na overovanie podpisov objektov” na strane 53
Pri podpisovaní objektov vytvoríte podpis pomocou súkromného kľúča certifikátu. Keď posielate tento podpísaný objekt ostatným, musíte poslať aj kópiu certifikátu, ktorý podpísal tento objekt.

Digitálne certifikáty pre overovanie podpisov objektov

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.

Je niekoľko rôznych hodnôt, ktoré môžeme pre systémovú hodnotu QVFYOBJRST použiť, od ignorovania všetkých podpisov, po vyžadovanie platných podpisov pre všetky objekty, ktoré systém obnovuje. 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 i5/OS .

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 38
i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod.

Súvisiace informácie

Vyhľadávač systémovej hodnoty

Systémová hodnota QVFYOBJRST

Konfigurácia DCM

Správca digitálnych certifikátov (DCM) poskytuje užívateľské rozhranie založené na prehliadači, ktoré môžete použiť na riadenie a konfiguráciu digitálnych certifikátov 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 zobrazenie certifikátov, obnovenie certifikátov, importovanie certifikátov, 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 System i. Všetky úlohy pre prácu s CA, manažovanie certifikátov, ktoré používajú aplikácie a iné úlohy na úrovni systému sú dostupné len správcom bezpečnosti alebo administrátorom System i. 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 .

Spúšťanie správcu digitálnych certifikátov

Aby ste mohli vykonávať funkcie správcu digitálnych certifikátov (DCM), musíte ho vo vašom systéme spustiť.

Na úspešné spustenie DCM vykonajte tieto úlohy:

1. Nainštalujte správcu digitálnych certifikátov.
2. Nainštalujte IBM HTTP Server for i5/OS.
3. Pomocou Navigátora System i Navigator spustite inštanciu Správa servera HTTP:
   a. V System i Navigator rozviňte váš **system → Network → Servers → TCP/IP**.
   b. Pravým tlačidlom kliknite na **HTTP Administration**.
   c. Vyberte **Start**.
4. Otvorte webový prehliadač a zadajte http://your_system_name:2001 na zavedenie webovej konzoly IBM Systems Director Navigator for i5/OS.
5. Z úvodnej stránky kliknite na odkaz **i5/OS Tasks Page**.
6. Zo zoznamu produktov na stránke Úlohy i5/OS vyberte voľbu **Digital Certificate Manager**, aby sa zobrazilo užívateľské rozhranie DCM.

Súvisiace koncepty

"Scenár: Použitie certifikátov na externú autentifikáciu" na strane 11
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.

Úvodné nastavenie certifikátov

Ľavá časť Správcu digitálnych certifikátov (DCM) je navigačná časť úloh. Túto časť môžete použiť na výber širokého spektra úloh pre manažovanie certifikátov a aplikácií, ktoré ich používajú.

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

Ak používate Správcu digitálnych objektov (DCM) 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: Ak túto úlohu použijete na vytvorenie súkromnej lokálnej CA, úloha sa už v zozname nezobrazí.)
- Manažovanie miest CRL.
- Manažovanie lokality LDAP.
- Manažovanie umiestnenia požiadavky PKIX.
- Návrat na stránku úloh i5/OS

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 zobrazí, závisí od skladu certifikátov, ktorý je otvorený a mimoriadnych oprávnení pre váš užívateľský profil.

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 33
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.

Vytváranie a prevádzka lokálnej CA

Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

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.

Ak chcete použiť DCM na vytvorenie a prevádzku lokálnej CA, postupujte podľa týchto krokov:

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnej časti DCM vyberte voľbu Vytvoriť certifikačnú autoritu (CA), aby sa zobrazila skupina formulárov. Tieto formuláre vás oboznámia s procesom vytvárania lokálnej CA a vykonaním ostatných 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. Ak používate tieto formuláre na vykonávanie všetkých úloh potrebných na nastavenie fungujúcej lokálnej certifikačnej autority (CA):
   a. Rozhodnite sa, ako budete uchovávať súkromný kľúč pre certifikát lokálnej CA. (Tento krok sa vykonáva len v prípade, že máte vo vašom systéme nainštalovaný kryptografický koprocesor IBM). Ak ho váš systém neobsahuje, DCM automaticky uloží certifikát a jeho súkromný kľúč do skladu certifikátov lokálnej certifikačnej autority (CA)).
   b. Poskytnite identifikačné informácie pre lokálnu CA.
   c. Nainštalujte certifikát lokálnej CA na váš PC alebo prehliadač, aby váš softvér mohol rozoznať lokálnu CA a overiť certifikáty, ktoré CA vydáva.
   d. Vyberte údaje politiky pre vašu lokálnu CA.
   e. Použite novú lokálnu CA na vydanie certifikátu servera alebo klienta, ktorý môžu vaše aplikácie používať 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 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 dôverujú vašej lokálnej CA.

Po dokončení úlohy za pomoci sprievodcu máte všetko, čo potrebujete na začatie konfigurácie svojich aplikácií na použitie SSL na bezpečnú komunikáciu.

Po nakonfigurovaní aplikácií užívatelia, ktorí ich používajú prostredníctvom pripojenia SSL, musia 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 kopírovanie certifikátu lokálnej CA do súboru alebo na stiahnutie certifikátu do svojho prehliadača. Spôsob uchovávania certifikátu lokálnej CA užívateľmi závisí od softvéru klienta používaného na vytvorenie pripojenia SSL k aplikácii.

Túto lokálnu CA môžete použiť aj na vydanie certifikátov aplikáciám na iných modeloch System i vo vašej sieti.

Ak sa chcete dozvedieť viac o používaní DCM na riadenie užívateľských certifikátov a spôsobe, akým užívatelia môžu získať kópiu certifikátu lokálnej CA na autentifikáciu certifikátov vydávaných lokálnou CA, pozrite si tieto témy:

Súvisiace koncepty

“Verejné certifikáty verzus súkromné certifikáty” na strane 33
Môžete používať certifikáty od verejnej CA alebo si na vydávanie certifikátov môžete vytvoriť a prevádzkovať vlastnú CA. Ako sa rozhodnete získavať certifikáty záleží na tom, ako ich chcete používať.

“Digitálne certifikáty pre pripojenia VPN” na strane 37
Digitálne certifikáty môžete použiť ako prostriedok na vytvorenie pripojenia VPN v System i. Oba koncové body dynamického VPN spojenia musia byť schopné vzájomne sa autentifikovať pred aktivovaním spojenia.

“Riadenie užívateľských certifikátov” na strane 44
Pomocou Správcu digitálnych certifikátov (DCM) môžete získať certifikáty s SSL alebo priradiť existujúce certifikáty k ich užívateľským profilom System i.

Súvisiace úlohy

“Používanie lokálnej CA na vydávanie certifikátov pre ostatné modely System i” na strane 57
Pomocou správcu digitálnych certifikátov (DCM) môžete nakonfigurovať súkromnú lokálnu CA na jednom systéme, aby vydávala certifikáty na používanie na iných platformáchSystem i.

“Získavanie kópie certifikátu súkromnej CA” na strane 48
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.

“Podpisovanie objektov” na strane 74
Na podpisovanie objektov môžete použiť tri rozdielne metódy. Na podpísanie objektu môžete napísať program, ktorý zavolá API na podpisovanie objektov, použiť správcu digitálnych certifikátov (DCM) alebo funkciu centrálneho riadenia System i Navigator pre balíky, ktoré distribuujete do iných systémov.

Súvisiaci odkaz

"Používanie API na programové vydávanie certifikátov užívateľom s výnimkou užívateľov System i" na strane 48
Lokálna CA môže užívateľom vydávať súkromné certifikáty bez priraďovania týchto certifikátov k užívateľským profilom System i.

Riadenie užívateľských certifikátov:

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

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 ale váš server používa certifikát zo súkromnej lokálnej CA, vaši užívatelia musia získať kópiu certifikátu lokálnej CA a až potom budú môcť vytvoriť so serverom reláciu SSL.

Okrem toho, ak aplikácia servera podporuje a vyžaduje autentifikáciu klientov cez certifikáty, užívatelia musia predložiť akceptovateľný certifikát užívateľa, aby sa dostali na prostriedky, ktoré poskytuje server. V závislosti od vašich bezpečnostných potrieb môžu užívatelia poskytnúť certifikát z verejnej internetovej CA alebo certifikát získaný z lokálnej CA, ktorú prevádzkujete. Ak vaša aplikácia servera poskytuje prístup k prostriedkom pre interných užívateľov, ktorí aktuálne majú užívateľské profily System i, 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 System i. Ak máte užívateľský profil so špeciálnymi oprávneniami *SECADM a *ALLOBJ, môžete manažovať priradenia certifikátov užívateľských profilov sami pre seba alebo pre ostatných užívateľov. Ak nie je otvorený žiadny sklad certifikátov alebo, ak je otvorený sklad certifikátov lokálnej certifikačnej autority (CA), môžete v navigačnom rámci vybrať **Manage User Certificates** na prístup k príslušným 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 svoje užívateľské profily získať užívateľský certifikát z lokálnej CA výberom 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

"Vytváranie a prevádzka lokálnej CA" na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

"Získavanie kópie certifikátu súkromnej CA" na strane 48
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.

Vytváranie užívateľského certifikátu:

Ak chcete použiť digitálne certifikáty na autentifikáciu užívateľa, užívatelia musia mať certifikáty. Ak na prevádzku súkromnej lokálnej certifikačnej autority (CA) používate správcu digitálnych certifikátov (DCM), môžete na vydávanie certifikátov každému užívateľovi používať lokálnu CA.

Každý užívateľ musí použiť DCM na získanie certifikátu pomocou úlohy **Create Certificate**. Ak chcete získať certifikát z lokálnej CA, politika CA musí umožňovať CA vydávať užívateľské certifikáty.

Ak chcete získať certifikát z lokálnej CA, vykonajte tieto kroky:

1. Spustite DCM. Pozrite si kapitolu Spúšťanie 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 System i.

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 33
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.

Súvisiace úlohy

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

"Získavanie kópie certifikátu súkromnej CA" na strane 48
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.

Priraďovanie užívateľského certifikátu:

Užívateľský certifikát, ktorý vlastníte, môžete priradiť k vášmu vlastnému užívateľskému profilu i5/OS alebo k identite iného užívateľa. Certifikát môže pochádzať 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 z vonkajšej certifikačnej autority (CA) alebo lokálnej CA na inom systéme iSeries a vy, ako administrátor, chcete, aby boli k dispozícii pre správcu digitálnych certifikátov (DCM). Umožňuje to

vám a užívateľovi používať DCM na manažovanie týchto certifikátov, ktoré sa najčastejšie používajú na autentifikáciu klienta. Úloha **Assign a user certificate** poskytuje mechanizmus, ako umožniť užívateľovi vytvoriť priradenie DCM pre certifikát, získaný od externej CA.

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

- Lokálne uloženie certifikátu v systéme System i spolu s užívateľským profilom. Keď pre DCM nie je definované umiestnenie LDAP, úloha **Assign a user certificate** 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). Ak je zadané umiestnenie LDAP a model System i je nakonfigurovaný na účasť v EIM, potom úloha **Assign a user certificate** povoľuje užívateľovi uložiť kópiu vonkajšieho certifikátu v zadanom adresári 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

   “Vytváranie užívateľského certifikátu” na strane 44
   Ak chcete použiť digitálne certifikáty na autentifikáciu užívateľa, užívatelia musia mať certifikáty. Ak na prevádzku súkromnej lokálnej certifikačnej autority (CA) používate správcu digitálnych certifikátov (DCM), môžete na vydávanie certifikátov každému užívateľovi používať lokálnu CA.

   “Odstraňovanie problémov s priradením užívateľského certifikátu” na strane 82
   Nasledujúce kroky vám pomôžu pri odstraňovaní akýchkoľvek problémov, s ktorými sa môžete stretnúť pri pokuse o priradenie užívateľského certifikátu pomocou správcu digitálnych certifikátov (DCM).

Súvisiace informácie

Prehľad Informačného centra pre EIM

Riadenie užívateľských certifikátov podľa dátumu ukončenia platnosti:

Správca digitálnych certifikátov (DCM) poskytuje podporu riadenia uplynutia platnosti certifikátov s cieľom umožniť administrátorom kontrolovať dátumy uplynutia platnosti užívateľských certifikátov na lokálnom modeli System i. Podpora riadenia uplynutia platnosti užívateľských certifikátov pomocou DCM sa môže použiť v spojení s mapovaním podnikovej identity (EIM) s cieľom umožniť administrátorom používať DCM na kontrolu uplynutia platnosti užívateľských certifikátov na podnikovej úrovni.

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

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

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

1. Spustite DCM. Pozrite si kapitolu Spúšťanie 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 **Manage Certificates**, aby sa zobrazil zoznam úloh, potom vyberte **Check expiration** a vyberte **User**.
3. Ak má váš užívateľský profil špeciálne oprávnenia *ALLOBJ a *SECADM, môžete si zvoliť metódu, podľa ktorej budete vyberať užívateľské certifikáty, ktoré sa majú zobrazovať a manažovať na základe dátumov ukončenia ich platnosti. (Ak váš užívateľský profil nemá tieto špeciálne oprávnenia, DCM vás požiada o určenie rozsahu dátumov ukončenia platnosti, ako je opísané v nasledujúcom kroku.) Môžete vybrať jeden z nasledujúcich:
   - **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 mapovanie podnikovej identity (Enterprise Identity Mapping)” na strane 36
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.

“Riadenie certifikátov podľa dátumu ukončenia platnosti” na strane 67
Správca digitálnych certifikátov (DCM) poskytuje podporu riadenia uplynutia platnosti certifikátov, čo má administrátorom umožniť riadenie certifikátov servera alebo klienta, certifikátov podpisujúcich objekty, certifikátov certifikačnej autority a užívateľských certifikátov podľa uplynutia platnosti na lokálnom systéme.

Súvisiace informácie

Prehľad Informačného centra pre EIM

Používanie API na programové vydávanie certifikátov užívateľom s výnimkou užívateľov System i:

Lokálna CA môže užívateľom vydávať súkromné certifikáty bez priraďovania týchto certifikátov k užívateľským profilom System i.

| API QYCUGSUC (Generate and Sign User Certificate Request) a API QYCUSUC (Sign User Certificate Request)
| umožňuje programovo vydávať certifikáty užívateľom s výnimkou užívateľov System i. Priradenie certifikátov k
| užívateľským profilom System i má určité výhody, najmä v súvislosti s internými užívateľmi. Kvôli týmto
| obmedzeniam a požiadavkám je však používanie lokálnej CA na vydávanie užívateľských certifikátov veľkému počtu
| užívateľov menej praktické, najmä ak nechcete, aby títo užívatelia mali užívateľský profil System i. 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 API podporujú poskytovanie rozhrania na vytváranie užívateľských certifikátov podpísaných certifikátom lokálnej CA pre akékoľvek meno užívateľa. Tento certifikát nebude združený s užívateľským profilom. Užívateľ nemusí existovať v systéme hosťujúcom DCM a nemusí používať DCM na vytváranie certifikátov.

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. Vytvorená aplikácia musí poskytovať kód grafického užívateľského rozhrania (GUI) potrebný na vytvorenie užívateľského certifikátu a na zavolanie vhodného API, ktoré použije lokálnu CA na podpísanie certifikátu.

Súvisiace koncepty

“Verejné certifikáty verzus súkromné certifikáty” na strane 33
Môžete používať certifikáty od verejnej CA alebo si na vydávanie certifikátov môžete vytvoriť a prevádzkovať vlastnú CA. Ako sa rozhodnete získavať certifikáty záleží na tom, ako ich chcete používať.

“Digitálne certifikáty na autentifikáciu užívateľov” na strane 35
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.

Súvisiace úlohy

“Vytváranie a prevádzka lokálnej CA” na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

Súvisiace informácie

API požiadavky na vygenerovanie a podpis užívateľského certifikátu (QYCUGSUC)

API požiadavky na podpis užívateľského certifikátu (QYCUSUC)

Získavanie kópie certifikátu súkromnej CA:

Keď pristupujete na server, ktorý používa spojenie Secure Sockets Layer (SSL), ako dôkaz svojej identity poskytne server vášmu klientskemu softvéru certifikát. Aby mohol server vytvoriť reláciu, váš klientsky softvér musí validovať certifikát servera.

Aby sa dal validovať certifikát servera, váš klientsky softvér musí mať prístup na miestne uloženú kópiu certifikátu pre certifikačnú autoritu (CA), ktorá vydala certifikát servera. Ak tento server predloží certifikát od verejnej internetovej

CA, softvér vášho prehliadača alebo iný klientsky softvér možno už má kópiu certifikátu CA. Ak však server poskytuje certifikát zo súkromnej lokálnej CA, na získanie kópie certifikátu lokálnej CA musíte použiť správcu digitálnych certifikátov (DCM).

DCM môžete použiť na stiahnutie certifikátu lokálnej CA priamo do vášho prehliadača, alebo môžete skopírovať certifikát lokálnej CA do súboru, aby k nemu mal softvér iného klienta prístup a mohol ho používať. Ak na zabezpečenie komunikácií používate prehliadač aj ostatné aplikácie, na nainštalovanie certifikátu lokálnej CA budete musieť použiť obe 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 poskytnutím certifikátu z lokálnej CA, musíte ho stiahnuť do svojho prehliadača skôr, ako požiadate o užívateľský certifikát od lokálnej CA.

Ak chcete na získanie kópie certifikátu lokálnej CA použiť DCM, vykonajte tieto kroky:

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnom rámci vyberte **Install local CA Certificate on Your PC** na zobrazenie stránky, ktorá umožňuje stiahnutie certifikátu lokálnej CA do vášho prehliadača alebo jeho uloženie do súboru vo vašom systéme.
3. Vyberte metódu získavania certifikátu lokálnej CA.
   a. Vyberte **Install certificate** na stiahnutie certifikátu lokálnej CA ako dôveryhodného koreňa do svojho 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. Vyberte **Copy and paste certificate** na zobrazenie stránky, ktorá obsahuje špeciálne zakódovanú 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. Aby mohli aplikácie klienta rozpoznávať a používať certifikát lokálnej CA na autentifikáciu, musíte aplikácie nakonfigurovať na rozpoznávanie certifikátu ako dôveryhodného koreňa. Vytvorený súbor použite podľa inštrukcií, ktoré poskytujú tieto aplikácie.
4. Kliknite na **OK** na návrat na domovskú stránku Správcu digitálnych certifikátov.

Súvisiace koncepty

“Riadenie užívateľských certifikátov” na strane 44
Pomocou Správcu digitálnych certifikátov (DCM) môžete získať certifikáty s SSL alebo priradiť existujúce certifikáty k ich užívateľským profilom System i.

Súvisiace úlohy

“Vytváranie a prevádzka lokálnej CA” na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

“Vytváranie užívateľského certifikátu” na strane 44
Ak chcete použiť digitálne certifikáty na autentifikáciu užívateľa, užívatelia musia mať certifikáty. Ak na prevádzku súkromnej lokálnej certifikačnej autority (CA) používate správcu digitálnych certifikátov (DCM), môžete na vydávanie certifikátov každému užívateľovi používať lokálnu CA.

Riadenie certifikátov z verejnej internetovej CA

Keď používate správcu digitálnych certifikátov (DCM) na riadenie certifikátov z verejnej internetovej CA, musíte najprv vytvoriť sklad certifikátov. Sklad certifikátov je špeciálny databázový súbor kľúčov, ktorý používa DCM na ukladanie digitálnych certifikátov a s nimi spojených súkromných kľúčov.

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.

V DCM môžete použiť úlohy so sprievodcom na centrálne riadenie týchto verejných certifikátov a aplikácií, ktoré ich používajú na vytváranie pripojení SSL, podpisovanie objektov alebo overovanie autentickosti 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 33
Môžete používať certifikáty od verejnej CA alebo si na vydávanie certifikátov môžete vytvoriť a prevádzkovať vlastnú CA. Ako sa rozhodnete získavať certifikáty záleží na tom, ako ich chcete používať.

"Digitálne certifikáty pre pripojenia VPN" na strane 37
Digitálne certifikáty môžete použiť ako prostriedok na vytvorenie pripojenia VPN v System i. Oba koncové body dynamického VPN spojenia musia byť schopné vzájomne sa autentifikovať pred aktivovaním spojenia.

Súvisiace úlohy

"Riadenie umiestnenia požiadaviek pre PKIX CA" na strane 72
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.

Riadenie 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 prevádzku svojej vlastnej lokálnej certifikačnej autority (CA), musíte najprv vytvoriť príslušný sklad certifikátov na riadenie verejných certifikátov, ktoré použijete 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. Pozrite si kapitolu Spúšťanie 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 or other Internet Certificate Authority (CA)** a kliknutím na **Continue** 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.

Po dokončení úlohy za pomoci sprievodcu máte všetko, čo potrebujete na začatie konfigurácie svojich aplikácií na použitie SSL na 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.

Riadenie verejných internetových certifikátov na podpisovanie objektov:

Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov na digitálne podpisovanie objektov.

Ak nepoužívate DCM na prevádzku svojej vlastnej lokálnej certifikačnej autority (CA), musíte najprv vytvoriť príslušný sklad certifikátov na riadenie verejných certifikátov, ktoré použijete 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 System i Navigator 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. Pozrite si kapitolu Spúšťanie 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 **Manage certificates**, aby sa zobrazil zoznam úloh.
12. Zo zoznamu úloh vyberte **Import certificate**, aby sa spustil proces importu podpísaného certifikátu do skladu certifikátov *OBJECTSIGNING. Po dokončení importu certifikátu môžete vytvoriť definíciu aplikácie na používanie certifikátu na podpisovanie objektov.
13. Po obnovení ľavého navigačného rámca vyberte **Manage Applications**, čím zobrazíte zoznam úloh.

14. Zo zoznamu úloh vyberte **Add application**, aby sa spustil proces vytvorenia definície aplikácie, podpisujúcej objekty, na použitie s certifikátom na podpisovanie objektov.
15. Vyplňte formulár na definovanie vašej aplikácie na podpisovanie objektov a kliknite na **Add**. Táto definícia aplikácie nepopisuje skutočnú aplikáciu, ale popisuje typ objektov, ktoré chcete podpisovať konkrétnym certifikátom. Pri vypĺňaní formuláru môžete použiť online pomoc.
16. Kliknite na **OK**, aby sa potvrdila správa o vytvorení definície a zobrazil úloha Manage Applications.
17. Zo zoznamu úloh vyberte **Update certificate assignment** a kliknite na **Continue** na zobrazenie zoznamu ID aplikácií podpisujúcich objekty, pre ktoré chcete priradiť certifikát.
18. Zo zoznamu ID aplikácií vyberte svoju aplikáciu a kliknite na **Update Certificate Assignment**.
19. Vyberte certifikát, ktorý ste naimportovali a kliknite na **Assign New Certificate**.

Po dokončení týchto úloh máte všetko, čo potrebujete na podpisovanie objektov na zabezpečenie ich integrity.

Keď vykonávate distribúciu podpísaných objektov, osoby, ktoré dostanú tieto objekty, musia používať OS/400 V5R1 alebo novšiu verziu DCM na overenie platnosti podpisu na objektoch, aby zabezpečili, že údaje nie sú zmenené a aby overili 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. Ak ste napríklad podpísali objekty certifikátom zo súkromnej lokálnej CA, musíte poskytnúť kópiu certifikátu 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 38
i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod.

Súvisiace úlohy

“Overovanie platnosti podpisov objektov” na strane 75
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.

“Podpisovanie objektov” na strane 74
Na podpisovanie objektov môžete použiť tri rozdielne metódy. Na podpísanie objektu môžete napísať program, ktorý zavolá API na podpisovanie objektov, použiť správcu digitálnych certifikátov (DCM) alebo funkciu centrálneho riadenia System i Navigator pre balíky, ktoré distribuujete do iných systémov.

Riadenie certifikátov na overovanie podpisov objektov:

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, musíte najprv získať kópiu certifikátu CA a potom môžete overiť podpis objektu.

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. Pozrite si kapitolu Spúšťanie 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 **Select a Certificate Store** 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 38
i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod.

Súvisiace úlohy

“Overovanie platnosti podpisov objektov” na strane 75
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 existujúcich certifikátov

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 lokálnej CA alebo pomocou internetovej CA.

Obnova certifikátu z lokálnej CA

Ak používate lokálnu CA na podpis obnoveného certifikátu, DCM používa poskytnuté informácie na vytvorenie nového certifikátu v aktuálnom sklade certifikátov a uchováva predošlý certifikát.

Ak chcete obnoviť certifikát pomocou lokálnej CA, postupujte podľa týchto krokov:

1. V navigačnej časti kliknite na **Select a Certificate Store**, potom vyberte sklad certifikátov obsahujúci certifikát, ktorý chcete obnoviť.
2. V navigačnej časti vyberte **Manage Certificates**.
3. V navigačnej časti vyberte **Renew certificate**.
4. Vyberte certifikát, ktorý chcete obnoviť a kliknite na **Renew**.
5. Vyberte **local Certificate Authority (CA)** a kliknite na **Continue**.
6. Vyplňte formulár na identifikáciu certifikátu. Pole **New certificate label** musíte zmeniť, ale ostatné polia môžu ostať pôvodné.
7. Vyberte aplikácie, ktoré majú používať obnovený certifikát a kliknutím na **Continue** dokončite obnovu certifikátu.

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

Obnova certifikátu z internetovej CA

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. Ďalším spôsobom, ako môžete obnoviť certifikát je použitie DCM na vytvorenie nového verejno-súkromného páru kľúčov a CSR (Certificate Signing Request) pre certifikát a potom tieto informácie poslať do internetovej CA, 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 **Select a Certificate Store**, 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 **Manage Certificates**.
3. V navigačnej časti kliknite na **Renew certificate**.
4. Vyberte certifikát, ktorý chcete obnoviť a kliknite na **Renew**.

5. Vyberte **VeriSign** alebo inú **Internet Certificate Authority (CA)** a kliknite na **Continue**.
6. Vyberte voľbu **No - Import the renewed signed certificate from an existing file**.
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 **Select a Certificate Store**, 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 **Manage Certificates**.
3. V navigačnej časti kliknite na **Renew certificate**.
4. Vyberte certifikát, ktorý chcete obnoviť a kliknite na **Renew**.
5. Vyberte **VeriSign** alebo inú **Internet Certificate Authority (CA)** a kliknite na **Continue**.
6. Kliknite na voľbu **Yes - Create a new key pair for this certificate** a kliknite na **Continue**.
7. Vyplňte formulár na identifikáciu certifikátu. Pole New certificate label 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.

Import certifikátov

Na import certifikátov umiestnených v súboroch vášho systému môžete použiť správcu digitálnych certifikátov (DCM). Namiesto opakovaného vytvorenia certifikátu v aktuálnom serveri môžete certifikát tiež importovať z iného servera.

V systéme A ste napríklad používali lokálnu CA na vytvorenie certifikátu na použitie vašou maloobchodnou webovou aplikáciou na iniciáciu spojení SSL. Váš podnik sa v poslednej dobe rozrástol a tak ste nainštalovali nový model System i (systém B), aby ste mohli hostiť viacero inštancií tejto veľmi často používanej maloobchodnej aplikácie. Chcete, aby všetky inštancie obchodnej aplikácie používali na identifikáciu a inicializáciu pripojení SSL identický certifikát. Následne sa môžete rozhodnúť naimportovať certifikát lokálnej CA aj certifikát servera zo systému A na systém B a nepoužívať lokálnu CA v systéme A na vytvorenie nového odlišného certifikátu pre systém B.

Ak chcete pomocou DCM importovať certifikát, vykonajte tieto kroky:

1. V ľavej navigačnej časti okna kliknite na **Select a Certificate Store** 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 **Manage Certificates**.
3. V navigačnej časti vyberte **Import certificate**.
4. Vyberte typ certifikátu, ktorý chcete importovať a vyberte **Continue**. 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.

Riadenie DCM

Po tom, čo ste nakonfigurovali Správcu digitálnych certifikátov (DCM) je tu niekoľko úloh na správu certifikátov, ktoré budete potrebovať vykonať.

Ak sa chcete dozvedieť, ako používať DCM na správu digitálnych certifikátov, prezrite si tieto témy:

Používanie lokálnej CA na vydávanie certifikátov pre ostatné modely System i

Pomocou správcu digitálnych certifikátov (DCM) môžete nakonfigurovať súkromnú lokálnu CA na jednom systéme, aby vydávala certifikáty na používanie na iných platformáchSystem i.

Možno už používate súkromnú lokálnu certifikačnú autoritu (CA) v systéme vašej siete. Teraz chcete používanie tejto lokálnej CA rozšíriť na ďalší systém vo vašej sieti. Chcete napríklad, aby vaša aktuálna lokálna CA vydávala certifikát servera alebo klienta pre aplikáciu na inom systéme na používanie komunikačných relácií SSL. Alebo chcete používať certifikáty z lokálnej CA na jednom systéme na podpisovanie objektov uložených na inom serveri.

Tento cieľ môžete splniť pomocou DCM. Niektoré z úloh vykonáte na systéme, na ktorom prevádzkujete lokálnu CA a ostatné úlohy vykonáte na sekundárnom systéme hosťujúcom aplikácie, pre ktoré chcete vydávať certifikáty. Tento sekundárny systém sa nazýva cieľový systém. Úlohy, ktoré musíte vykonať na cieľovom systéme, závisia na úrovni vydania toho systému.

Poznámka: Problém môže nastať, ak systém, na ktorom prevádzkujete lokálnu CA používa produkt poskytovateľa kryptografického prístupu, ktorý poskytuje silnejšie šifrovanie než cieľový systém. Keď exportujete certifikát (s jeho súkromným kľúčom), systém zašifruje súbor na ochranu jeho obsahu. 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.

Lokálnu CA môžete použiť na vydávanie certifikátov iným systémom, ktoré potom môžete používať na podpisovanie objektov alebo použiť aplikácie na vytváranie relácií SSL. Keď používate lokálnu CA na vytváranie certifikátu na použitie na inom systéme, súbory vytvorené správcom digitálnych certifikátov obsahujú kópiu certifikátu lokálnej CA a tiež kópie certifikátov pre mnohé verejné internetové CA.

Úlohy, ktoré musíte vykonať v DCM sa mierne odlišujú v závislosti od typu certifikátu vydávaného vašou lokálnou CA a úrovne vydania a podmienok na cieľovom systéme.

Vydávať súkromné certifikáty na používanie na inom modeli System i

Ak chcete používať lokálnu CA na vydávanie certifikátov na používanie na inom systéme, na systéme hosťujúcom lokálnu CA vykonajte tieto kroky:

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnom rámci vyberte **Create Certificate** na zobrazenie zoznamu typov certifikátov, na vytváranie ktorých môžete použiť vašu 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). Aby ste mohli vykonávať tieto úlohy, musí na tomto systéme existovať lokálna CA. 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. Vyberte typ certifikátu, ktorý chcete aby lokálna CA vydávala a kliknite na **Continue** na začatie úloh so sprievodcom a vyplnenie série formulárov.
4. Vyberte vytvorenie **certifikátu klienta alebo servera pre iný System i** (pre relácie SSL) alebo **certifikátu podpisujúceho objekty pre iný System i** (pre používanie na inom systéme).
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 do týchto súborov automaticky vloží 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 31
Zašifrované heslá databázy kľúčov používané na prístup do skladov certifikátov v správcovi digitálnych certifikátov (DCM) sú uložené alebo uschované v špeciálnom súbore bezpečnosti vo vašom systéme. 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.

"Verejné certifikáty verzus súkromné certifikáty" na strane 33
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.

Súvisiace úlohy

"Vytváranie a prevádzka lokálnej CA" na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

Používanie 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 používanie prenesených súborov skladu certifikátov vytvorených na hostiteľskom systéme lokálnej certifikačnej autority (CA) sa líšia v závislosti od 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, či sa súbory skladu certifikátov (dva súbory: jeden s príponou .KDB a druhý s príponou .RDB) vytvorené v systéme, ktorý hostí lokálnu 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 pridal tieto kópie, ako aj kópiu certifikátu lokálnej CA do súborov skladu certifikátov pri ich vytváraní.

   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. Po zobrazení stránky skladu certifikátov a hesla poskytnite heslo zadané na hostiteľskom systéme pre sklad certifikátov, keď ste vytvárali certifikát pre cieľový systém a kliknite na **Continue**.
6. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Potom môžete určiť, ktoré aplikácie budú používať tento certifikát pre relácie SSL.
7. V navigačnej časti okna kliknite na **Select a Certificate Store** a na otvorenie vyberte ***SYSTEM**.
8. Keď sa zobrazí stránka **Certificate Store and Password**, zadajte nové heslo a kliknite na **Continue**.
9. Po tom, čo sa navigačný rámec obnoví, zvoľte v ňom **Manage Certificates** na zobrazenie zoznamu úloh.
10. Zo zoznamu úloh vyberte **Assign certificate** na zobrazenie zoznamu certifikátov v aktuálnom sklade certifikátov.
11. Vyberte certifikát, ktorý ste vytvorili v *hostiteľskom* systéme a kliknite na **Assign to Applications**, 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 na cieľovom systéme používať certifikát vydaný lokálnou CA na inom systéme. Pred začatím používania SSL v týchto aplikáciách však musíte nakonfigurovať aplikácie na používanie SSL.

Užívateľ musí najprv použiť DCM na získanie kópie certifikátu lokálnej CA z hosťujúceho systému a potom mu bude udelený prístup k vybraným aplikáciám prostredníctvom pripojenia SSL. Certifikát lokálnej CA musí byť skopírovaný do súboru na užívateľovom PC alebo stiahnutý do užívateľovho prehliadača v závislosti od požiadaviek aplikácie povolenej pomocou SSL.

Sklad certifikátov *SYSTEM existuje - použitie súborov ako skladu 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 si môžete vybrať import súkromného certifikátu a príslušného certifikátu 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 System i (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 System i s povoleným SSL nemôžete nakonfigurovať na používanie tohto certifikátu. Ak chcete používať certifikát pre aplikácie System i, 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 **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte **Other System Certificate Store**.
3. Keď sa zobrazí stránka Certificate Store and Password, uveďte úplnú cestu a názov súboru skladu certifikátov (toho s príponou .KDB), ktorý ste preniesli z hostiteľského systému. Zadajte tiež heslo, ktoré ste zadali pre sklad certifikátov v *hostiteľskom* systéme pri vytváraní certifikátu pre cieľový systém a kliknite na **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

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

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Ďalej môžete 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 **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. 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: Musíte najprv vyexportovať certifikát lokálnej CA do skladu certifikátov a potom môžete vyexportovať certifikát servera alebo klienta do skladu certifikátov. Ak najprv vyexportujete certifikát servera alebo klienta, môže nastať chyba, pretože certifikát lokálnej CA v sklade certifikátov neexistuje.
9. Vyberte certifikát lokálnej CA, ktorý chcete vyexportovať 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 **Export certificate**.
13. Ako typ certifikátu na export vyberte **Server or client** a kliknite na **Continue**.
14. Vyberte príslušný serverový alebo klientsky certifikát na export a kliknite na **Export**.
15. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
16. Ako cieľový sklad certifikátov zadajte *SYSTEM, zadajte heslo pre sklad certifikátov *SYSTEM a kliknite na **Continue**. Zobrazí sa správa 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 **Select a Certificate Store** 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 **Assign to Applications**, 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 na cieľovom systéme používať certifikát vydaný lokálnou CA na inom systéme. Pred začatím používania SSL v týchto aplikáciách však musíte nakonfigurovať aplikácie na používanie SSL.

Užívateľ musí najprv použiť DCM na získanie kópie certifikátu lokálnej CA z hosťujúceho systému a potom môže mať prístup k vybraným aplikáciám pomocou pripojenia SSL. Certifikát lokálnej CA musí byť skopírovaný do súboru na užívateľovom PC alebo stiahnutý do užívateľovho prehliadača v závislosti od požiadaviek aplikácie povolenej pomocou SSL.

Používanie súkromných certifikátov na podpisovanie objektov na 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 používanie prenesených súborov skladu certifikátov vytvorených na hostiteľskom systéme lokálnej CA, sa líšia v závislosti od 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 musíte vykonať na používanie súborov skladu certifikátov vytvorených na hostiteľskom systéme lokálnej CA, sa líšia v závislosti od toho, či ste už na cieľovom systéme používali DCM na riadenie certifikátov podpisujúcich objekty.

Ak v cieľovom systéme s prenesenými súbormi skladu certifikátov neexistuje sklad certifikátov *OBJECTSIGNING, vykonajte tieto kroky:

1. Skontrolujte, či sa súbory skladu certifikátov (dva súbory: jeden s príponou .KDB a jeden s príponou .RDB) vytvorené v systéme, ktorý hostí lokálnu CA, nachádzajú 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 kópie a tiež kópiu certifikátu lokálnej CA do súborov skladu certifikátov v čase ich vytvorenia.

   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 **Select a Certificate Store** 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 **Continue**.
6. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov. Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi. Ďalej môžete vytvoriť definíciu aplikácie na používanie certifikátu na podpisovanie objektov.

7. Po opätovnom otvorení skladu certifikátov vyberte v navigačnej časti okna **Manage Applications**, aby sa zobrazil zoznam úloh.
8. Zo zoznamu úloh vyberte **Add application**, aby sa spustil proces vytvorenia definície aplikácie, podpisujúcej objekty, na použitie s certifikátom na podpisovanie objektov.
9. Vyplňte formulár na definovanie vašej aplikácie na podpisovanie objektov a kliknite na **Add**. Táto definícia aplikácie nepopisuje skutočnú aplikáciu, ale popisuje typ objektov, ktoré chcete podpisovať konkrétnym certifikátom. Pri vypĺňaní formuláru môžete použiť online pomoc.
10. Kliknite na **OK**, aby sa potvrdila správa o vytvorení definície a zobrazte si zoznam úloh **Manage Applications**.
11. Zo zoznamu úloh vyberte **Update certificate assignment** na zobrazenie zoznamu ID aplikácií podpisujúcich objekty, pre ktoré môžete priradiť certifikát.
12. Zo zoznamu ID aplikácií vyberte svoju aplikáciu a kliknite na **Update Certificate Assignment**.
13. Vyberte certifikát, ktorý vytvorila lokálna CA na hostiteľskom systéme a kliknite na **Assign New Certificate**.

Po dokončení týchto úloh máte všetko, 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 podpísali objekty certifikátom z lokálnej CA, musíte poskytnúť kópiu certifikátu 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. Z prenesených súborov musíte vyexportovať kópiu samotného certifikátu podpisujúceho objekty aj certifikát lokálnej CA.

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 **Select a Certificate Store** a ako sklad certifikátov, ktorý sa má otvoriť, vyberte **Other System Certificate Store**.
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 **Continue**.
4. V navigačnej časti okna vyberte **Manage Certificate Store** a zo zoznamu úloh vyberte **Change password**. Vyplňte formulár na zmenu hesla pre sklad certifikátov.

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

   Po zmene hesla musíte nanovo otvoriť sklad certifikátov, aby ste mohli pracovať s jeho certifikátmi.

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

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

   Poznámka: Certifikát lokálnej CA musíte do skladu certifikátov vyexportovať predtým, ako doň vyexportujete certifikát podpisujúci objekty. Ak najprv vyexportujete certifikát podpisujúci objekty, môžete nastať chyba, pretože certifikát lokálnej CA v sklade certifikátov neexistuje.
10. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
11. Ako cieľový sklad certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**.
12. Teraz môžete vyexportovať certifikát podpisujúci objekty, do skladu certifikátov *OBJECTSIGNING. Znova vyberte úlohu **Export certificate**.
13. Ako typ certifikátu na export vyberte **Server or client** a kliknite na **Continue**.
14. Vyberte príslušný certifikát na export a kliknite na **Export**.
15. Ako cieľ pre exportovaný certifikát vyberte **Certificate store** a kliknite na **Continue**.
16. Ako cieľový sklad certifikátov zadajte *OBJECTSIGNING, zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**. Zobrazí sa správa 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.

Riadenie aplikácií v DCM

Správca digitálnych certifikátov (DCM) umožňuje vytvoriť definície aplikácie a riadiť priraďovanie certifikátov aplikácie. Môžete tiež definovať zoznamy dôveryhodných CA, ktoré aplikácia používa ako základ pre akceptovanie certifikátov na autentifikáciu klienta.

DCM môžete použiť na vykonanie rôznych riadiacich úloh pre aplikácie povolené pomocou SSL (Secure Socket Layer) a aplikácie podpisujúce objekty. Môžete napríklad riadiť, ktoré certifikáty budú vaše aplikácie používať na komunikačné relácie 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 9
Správca digitálnych certifikátov (DCM) umožňuje riadiť definície aplikácií, ktoré budú pracovať s konfiguráciami SSL a podpisovaním objektov.

Vytváranie definície aplikácie

V správcovi digitálnych certifikátov (DCM) môžete vytvoriť a používať tieto dva typy definícií aplikácií: aplikácie klienta alebo servera používajúce 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 System i 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. Pozrite si kapitolu Spúšťanie DCM.
2. Kliknite na **Select a Certificate Store** 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 9
Správca digitálnych certifikátov (DCM) umožňuje riadiť definície aplikácií, ktoré budú pracovať s konfiguráciami SSL a podpisovaním objektov.

Súvisiace informácie

QSYRGAP, QsyRegisterAppForCertUse API

Riadenie priraďovania certifikátov 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. Pozrite si kapitolu Spúšťanie DCM.
2. Kliknite na **Select a Certificate Store** 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 System i 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.

Súvisiace úlohy

“Riadenie umiestnení CRL” na strane 69
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.

“Priraďovanie certifikátu aplikáciám” na strane 69
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.

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. Pozrite si kapitolu Spúšťanie DCM.
2. Kliknite na **Select a Certificate Store** 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.

Súvisiace koncepty

"Digitálne certifikáty pre pripojenia VPN" na strane 37
Digitálne certifikáty môžete použiť ako prostriedok na vytvorenie pripojenia VPN v System i. Oba koncové body dynamického VPN spojenia musia byť schopné vzájomne sa autentifikovať pred aktivovaním spojenia.

Riadenie certifikátov podľa dátumu ukončenia platnosti

Správca digitálnych certifikátov (DCM) poskytuje podporu riadenia uplynutia platnosti certifikátov, čo má administrátorom umožniť riadenie certifikátov servera alebo klienta, certifikátov podpisujúcich objekty, certifikátov certifikačnej autority a užívateľských certifikátov podľa uplynutia platnosti na lokálnom systéme.

Poznámka: Ak nakonfigurujete DCM na prácu s mapovaním podnikovej identity (EIM), môžete riadiť užívateľské certifikáty podľa dátumu uplynutia platnosti v celom podniku.

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

Poznámka: 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. Ak už DCM nie je spustený, pozrite si kapitolu Spúšťanie 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.

Poznámka: Ak chcete skontrolovať dátum ukončenia platnosti certifikátov klienta alebo servera, musíte sa nachádzať v sklade certifikátov *SYSTEM alebo iného systému. Ak chcete skontrolovať dátum uplynutia platnosti certifikátov podpisujúcich objekty, musíte sa nachádzať v sklade certifikátov *OBJECTSIGNING. Dátum uplynutia platnosti certifikátov certifikačnej autority môžete skontrolovať vo všetkých skladoch certifikátov okrem skladu certifikátov lokálnej certifikačnej autority. Dátum uplynutia platnosti užívateľských certifikátov môžete skontrolovať v ktoromkoľvek sklade certifikátov. Ak chcete zistiť dátum uplynutia platnosti jedného certifikátu lokálnej CA, musíte ho zobraziť.

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.

Súvisiace úlohy

"Riadenie užívateľských certifikátov podľa dátumu ukončenia platnosti" na strane 47
Správca digitálnych certifikátov (DCM) poskytuje podporu riadenia uplynutia platnosti certifikátov s cieľom umožniť administrátorom kontrolovať dátumy uplynutia platnosti užívateľských certifikátov na lokálnom modeli System i. Podpora riadenia uplynutia platnosti užívateľských certifikátov pomocou DCM sa môže použiť v spojení s mapovaním podnikovej identity (EIM) s cieľom umožniť administrátorom používať DCM na kontrolu uplynutia platnosti užívateľských certifikátov na podnikovej úrovni.

Overovanie 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 CRL (Certificate Revocation List)” 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.

Priraďovanie 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. Pozrite si kapitolu Spúšťanie 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.

Súvisiace úlohy

“Riadenie priraďovania certifikátov aplikácii” na strane 65
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.

Riadenie 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. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnej časti okna vyberte **Manage CRL Locations**, 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 **Manage certificates**, 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 **Login distinguished name** a **Password** 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. Musíte tiež nakonfigurovať adresárový server (LDAP) a aplikácie klienta na používanie SSL a priradiť certifikát aplikáciám v DCM.

Súvisiace koncepty

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

Súvisiace úlohy

“Riadenie priraďovania certifikátov aplikácii” na strane 65
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.

Súvisiace informácie

IBM Directory Server for iSeries (LDAP)

Povolenie SSL v adresárovom serveri

Ukladanie kľúčov certifikátu v kryptografickom koprocesore IBM

Ak máte vo vašom systéme nainštalovaný kryptografický koprocesor IBM, môžete ho používať na poskytnutie bezpečnejšieho úložného priestoru pre súkromný kľúč certifikátu. Koprocesor môžete použiť na uloženie súkromného kľúča pre certifikát servera, certifikát klienta alebo certifikát miestnej certifikačnej autority (CA).

Koprocesor nemôžete používať na ukladanie súkromného kľúča užívateľského certifikátu, pretože tento kľúč musí byť uložený v 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 System i" na strane 9
Šifrovací koprocesor poskytuje pre vyvíjanie bezpečných aplikácií elektronického obchodu osvedčené šifrovacie služby, zabezpečujúce súkromie a integritu.

Súvisiace informácie

Prehľad kryptografie

Používanie 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.

Aby ste mohli túto voľbu úspešne používať, musíte použiť webové konfiguračné rozhranie kryptografického koprocesora IBM na vytvorenie príslušného súboru skladu 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 System i.

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 koprocesora je prístupné z webovej konzoly IBM Systems Director Navigator for i5/OS.

6. Kliknite na **Continue**. DCM pokračuje v zobrazovaní strán pre túto úlohu, ako sú identifikačné informácie pre certifikát, ktorý vytvárate alebo obnovujete.

Súvisiace informácie

Prehľad kryptografie

Práca s IBM Systems Director Navigator for i5/OS

Riadenie umiestnenia požiadaviek 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. Pozrite si kapitolu Spúšťanie 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

"Riadenie certifikátov z verejnej internetovej CA" na strane 49
Keď používate správcu digitálnych certifikátov (DCM) na riadenie certifikátov z verejnej internetovej CA, musíte najprv vytvoriť sklad certifikátov. Sklad certifikátov je špeciálny databázový súbor kľúčov, ktorý používa DCM na ukladanie digitálnych certifikátov a s nimi spojených súkromných kľúčov.

Riadenie umiestnenia LDAP pre užívateľské certifikáty

Správcu digitálnych certifikátov (DCM) môžete použiť na ukladanie užívateľských certifikátov do umiestnenia adresára servera LDAP (Lightweight Directory Access Protocol) s cieľom rozšíriť mapovanie podnikovej identity (EIM) na prácu s užívateľskými certifikátmi.

DCM štandardne ukladá užívateľské certifikáty vydávané lokálnou certifikačnou autoritou (CA) spolu s užívateľskými profilmi i5/OS. Môžete však nakonfigurovať správcu digitálnych certifikátov (DCM) v spojení s mapovaním podnikovej identity (EIM) tak, aby sa pri vydávaní užívateľských certifikátov lokálnou certifikačnou autoritou (CA)

ukladala verejná kópia certifikátu do špecifického umiestnenia adresára 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 **Assign a user certificate**.

EIM je technológia eServer, 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 **EIM Configuration** v navigátore System i Navigator 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 **EIM Configuration**.

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 zadanie adresára LDAP, ktorý bude DCM používať na uloženie užívateľského certifikátu vytvoreného lokálnou CA. Umiestnenie LDAP sa nemusí nachádzať na lokálnom modeli System i a nemusí byť ani na tom istom serveri LDAP, ktorý používa EIM. Keď nakonfigurujete umiestnenie LDAP v DCM, DCM použije zadaný adresár LDAP na ukladanie všetkých užívateľských certifikátov vydávaných lokálnou CA. DCM používa lokalitu LDAP aj na uloženie užívateľských certifikátov, spracovaných úlohou **Assign a user certificate**, namiesto uloženia certifikátu s užívateľským profilom.
2. Spustite príkaz **Convert User Certificates** (CVTUSRCERT). 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 **Login distinguished name** a **Password** prázdne.

Súvisiace úlohy

“Digitálne certifikáty a mapovanie podnikovej identity (Enterprise Identity Mapping)” na strane 36
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

Príkaz CVTUSRCERT (Convert User Certificate)

Enterprise Identity Mapping (EIM)

Podpisovanie objektov

Na podpisovanie objektov môžete použiť tri rozdielne metódy. Na podpísanie objektu môžete napísať program, ktorý zavolá API na podpisovanie objektov, použiť správcu digitálnych certifikátov (DCM) alebo funkciu centrálneho riadenia System i Navigator pre balíky, ktoré distribuujete 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). Môžete tiež podpisovať objekty príkazu (*CMD). Nemôžete podpisovať objekty uložené na iných systémoch.

Objekty môžete podpisovať pomocou certifikátov zakúpených od verejnej internetovej certifikačnej autority (CA) alebo certifikátov, ktoré vytvoríte pomocou súkromnej lokálnej 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 ako súčasť procesu vytvárania lokálnej CA alebo ako súčasť procesu riadenia certifikátov podpisujúcich objekty z verejnej internetovej CA.
- Sklad certifikátov *OBJECTSIGNING musí obsahovať aspoň jeden certifikát, vytvorený pomocou lokálnej CA alebo získaný z verejnej internetovej CA.
- Musíte mať vytvorenú definíciu aplikácie na podpisovanie objektov na použitie pre podpisovanie objektov.
- Musíte mať priradený certifikát k aplikácii na podpisovanie objektov, ktorú plánujete používať na podpisovanie objektov.

Použitie DCM na podpisovanie objektov

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

1. Spustite DCM. Pozrite si kapitolu Spúšťanie DCM.
2. V navigačnej časti kliknite na **Select a Certificate Store** 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 **Continue**.
4. Po zaktualizovaní obsahu navigačnej časti vyberte **Manage Signable Objects**, aby sa zobrazil zoznam úloh.
5. Z tohto zoznamu úloh vyberte **Sign an object**, aby sa zobrazil zoznam definícií aplikácií, ktoré môžete použiť na podpisovanie objektov.
6. Vyberte niektorú aplikáciu a kliknite na **Sign an object**, aby sa zobrazil formulár na špecifikovanie umiestnenia objektov, ktoré chcete podpísať.

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

   Poznámka: Názov objektu musíte začať s úvodnou lomkou, inak narazíte na chybu. Na popísanie časti adresára, ktorú chcete podpísať tiež môžete použiť určité zástupné znaky. Tieto zástupné znaky sú hviezdička (*****, ktorá špecifikuje ″ľubovoľný počet znakov,″ a otáznik (**?**), ktorý špecifikuje ″ľubovoľný jeden znak.″ Ak chcete napríklad podpísať všetky objekty v 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**.

Súvisiace úlohy

"Vytváranie a prevádzka lokálnej CA" na strane 42
Na vytvorenie a prevádzku svojej vlastnej lokálnej CA na vydávanie súkromných certifikátov pre vaše aplikácie môžete použiť správcu digitálnych certifikátov (DCM).

"Riadenie verejných internetových certifikátov na podpisovanie objektov" na strane 52
Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov na digitálne podpisovanie objektov.

Súvisiace informácie

API podpísania objektu

Scenár: Použitie Centrálneho riadenia Navigátora System i na podpisovanie objektov

Scenár: Použitie DCM na podpisovanie objektov a overovanie podpisov

Overovanie platnosti podpisov objektov

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

Požiadavky pre kontrolu podpisov

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

- Musíte mať vytvorený sklad certifikátov *SIGNATUREVERIFICATION, ktorý bude riadiť vaše certifikáty na overovanie platnosti podpisov.

  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. Pozrite si Spúšťanie DCM.
2. V navigačnej časti kliknite na **Select a Certificate Store** 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 38
i5/OS poskytuje podporu používania certifikátov na digitálne ″podpisovanie″ objektov. Elektronické podpisovanie objektov poskytuje spôsob na overenie integrity obsahu objektu aj jeho pôvod.

Súvisiace úlohy

“Riadenie verejných internetových certifikátov na podpisovanie objektov” na strane 52
Správcu digitálnych certifikátov (DCM) môžete použiť na manažovanie verejných internetových certifikátov na digitálne podpisovanie objektov.

“Riadenie certifikátov na overovanie podpisov objektov” na strane 53
Pri podpisovaní objektov vytvoríte podpis pomocou súkromného kľúča certifikátu. Keď posielate tento podpísaný objekt ostatným, musíte poslať aj kópiu certifikátu, ktorý podpísal tento objekt.

Odstraňovanie problémov s DCM

Na vyriešenie niektorých základných problémov, s ktorými sa môžete stretnúť počas konfigurácie a používania správcu digitálnych certifikátov (DCM), použite nasledujúce metódy odstraňovania problémov.

Pri práci s DCM a certifikátmi sa môžete stretnúť s chybami, ktoré zabránia splneniu vašich úloh a cieľov. Veľa bežných chýb alebo problémov, ktoré môžete spozorovať, spadá do mnohých kategórií, akými sú napríklad:

Odstraňovanie všeobecných problémov a problémov s heslami

Nasledujúca tabuľka pomáha pri odstraňovaní niektorých bežných problémov s heslami a ostatných všeobecných problémov, ktoré sa môžu vyskytnúť pri práci so správcom digitálnych certifikátov (DCM).

Problém	**Možné riešenie**
Nemôžete nájsť ďalšiu pomoc pre DCM.	V DCM kliknite ikonu pomoci - ″**?**″. Môžete tiež hľadať Informačné centrum i5/OS a externé webové stránky spoločnosti IBM na internete.
Vaše heslo pre lokálnu certifikačnú autoritu (CA) a sklady certifikátov *SYSTEM nefunguje.	Heslá rozlišujú veľkosť písmen. Presvedčte sa, či je prerađovač 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.
	Skontrolujte hodnotu priradenú k atribútu **Allow new digital certificates** pod voľbou **Work with system security** 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.

Problém	Možné riešenie
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 System i Navigator. 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.

Odstraňovanie problémov so skladom certifikátov alebo databázou kľúčov

Nasledujúca tabuľka pomáha pri odstraňovaní niektorých bežných problémov so skladom certifikátov alebo databázou kľúčov, ktoré môžete zaznamenať pri práci 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 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. Po presune nasledujúcich súborov vytvorte novú lokálnu CA:
	`/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 “Požiadavky nastavenia DCM” na strane 30 a tiež správnosť inštalácie všetkých licenčných programov.
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. Bližšie informácie nájdete v téme Informačné centrum i5/OS QsyAddVldlCertificate API. Pozrite si dokumentáciu k IBM HTTP Server for i5/OS, kde nájdete pomoc pri konfigurácii bezpečnej inštancie servera HTTP na používanie zoznamu overovania platnosti.

Odstraňovanie 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 servera HTTP pre i5/OS

Nasledujúca tabuľka pomáha pri odstraňovaní problémov servera HTTP, s ktorými sa môžete stretnúť pri práci so správcom digitálnych certifikátov (DCM).

Problém	Možné riešenie
HTTPS (Hypertext Transfer Protocol Secure) nefunguje.	Presvedčte sa, či je HTTP Server správne nakonfigurovaný na použitie SSL. 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.	Voľby nastavenia inštancie nájdete v dokumentácii k IBM HTTP Server for i5/OS.

Problém	Možné riešenie
Netscape Communicator čaká na skončenie platnosti konfiguračnej direktívy v kóde HTTP Servera, až potom vám umožní vybrať iný certifikát.	Väčšia hodnota certifikátu sťažuje registráciu druhého certifikátu, pretože prehliadač stále používa prvý.
Pokúšate sa donútiť prehliadač, aby HTTP Serveru predložil certifikát X.509, aby ste mohli tento certifikát použiť ako vstup do QsyAddVldlCertificate API.	Musíte použiť **SSLEnable** a **SSLClientAuth ON**, aby HTTP server zaviedol premennú prostredia HTTPS_CLIENT_CERTIFICATE. Informácie o týchto API môžete vyhľadať pomocou témy API finder v Informačné centrum i5/OS . 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**.

Odstraňovanie problémov s priradením užívateľského certifikátu

Nasledujúce kroky vám pomôžu pri odstraňovaní akýchkoľvek problémov, s ktorými sa môžete stretnúť pri pokuse o priradenie užívateľského certifikátu pomocou správcu digitálnych certifikátov (DCM).

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

"Priraďovanie užívateľského certifikátu" na strane 45
Užívateľský certifikát, ktorý vlastníte, môžete priradiť k vášmu vlastnému užívateľskému profilu i5/OS alebo k identite iného užívateľa. Certifikát môže pochádzať 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

Publikácie IBM Redbooks a webové stránky obsahujú informácie týkajúce sa kolekcie tém správcu digitálnych certifikátov (DCM). Každý súbor PDF môžete zobraziť alebo vytlačiť.

Dokumenty IBM Redbook

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

Webové stránky

- **Webová stránka VeriSign Help Desk** Táto webová stránka poskytuje rozsiahlu knižnicu tém o digitálnych certifikátoch a tiež veľa ďalších týkajúcich sa internetovej bezpečnosti.
- **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 tomto dokumente a všetky preň dostupné licenčné materiály poskytuje spoločnosť IBM na základe podmienok zákazníckej zmluvy IBM, medzinárodnej zmluvy IBM na licenčné programy, licenčnej zmluvy IBM pre počítačový kód alebo inej porovnateľnej zmluvy medzi zmluvnými stranami.

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. _uveďte rok alebo roky_. Všetky práva vyhradené.

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

Informácie o programovom rozhraní

Tento manažér digitálnych certifikátov dokumentuje plánované programové rozhrania, ktoré umožňujú zákazníkovi napísať programy na získanie služieb IBM i5/OS.

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
| Redbook
| System i

| Adobe, logo Adobe, PostScript a logo PostScript sú registrované ochranné známky alebo ochranné známky spoločnosti
| Adobe Systems Incorporated v Spojených štátoch amerických a/alebo iných krajinách.

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.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ IBM NERUČÍ ZA 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